SPECIAL REPORT

Worldwide Infrastructure Security Report

Volume X

ARBOR NETWORKS

About Arbor Networks

Arbor Networks, Inc. helps secure the world's largest enterprise and service provider networks from DDoS attacks and advanced threats. Arbor is the world's leading provider of DDoS protection in the enterprise, carrier and mobile market segments, according to Infonetics Research. Arbor's advanced threat solutions deliver complete network visibility through a combination of packet capture and NetFlow technology, enabling the rapid detection and mitigation of malware and malicious insiders. Arbor also delivers market-leading analytics for dynamic incident response, historical analysis, visualization and forensics. Arbor strives to be a "force multiplier," making network and security teams the experts. Our goal is to provide a richer picture into networks and more security context–so customers can solve problems faster and reduce the risk to their business. To learn more about Arbor products and services, please visit our website at arbornetworks.com. Arbor's research, analysis and insight, together with data from the ATLAS global threat intelligence system, can be found at the ATLAS Threat Portal.

Contents

Overview 6

Survey Methodology 7

Key Findings 8

Demographics of Survey Respondents 13

Figure 1
Respondent Organization's Primary Business Function 14

Figure 2
Organization's Geographic Information 14

Figure 3
Organization's Services Offered 15

Figure 4
Respondent's Role 15

Figure 5
SOC Type 16

Figure 6
Dedicated Security Personnel 16

Figure 7
Dedicated Security Personnel 16

ATLAS Introduction 17

Figure A1
ATLAS IPv4 Tracked Traffic 17

Figure A2
Participant Geographic Distribution 18

Figure A3
Participant Operator Types 18

Most Significant Operational Threats: Service Providers 19

Figure 8
Service Provider Experienced Threats 20

Figure 9
Service Provider Experienced Threats 21

Figure 10
Demand for DDoS Detection/Mitigation Services 21

Figure 11
Business Verticals for DDoS Services 22

Scale and Targeting of DDoS Attacks 23

Figure 12
Survey Peak Attack Size Year Over Year 24

Figure 13
Protocols Used for Reflection/Amplification 25

Figure 14
Target of Largest Attack 25

Figure 15
Attack Target Mix 26

Figure 16
Attack Target Customer Vertical 26

Figure 17
Attacks Targeting Cloud Services 27

Figure 18
CGN DDoS Attack Impact 27

ATLAS Attack Sizes 29

Figure A4
ATLAS Peak Attack Sizes Month by Month (Gbps) 29

Figure A5
Large Attack Breakout Month by Month 30

ATLAS Attack Durations 31

Figure A6
ATLAS Attack Duration Breakout 31

ATLAS Targeted Services 32

Figure A7
ATLAS Attack Port Breakout 32

ATLAS Targeted Services 33

Figure A8
Anatomy of an NTP Reflection Attack. 34

Figure A9
Example of NTP Server Monlist Response 35

Figure A10
ATLAS NTP Traffic Level 35

Figure A11
ATLAS NTP Attack Proportions 36

Figure A12
ATLAS SSDP Traffic Levels 37

Figure A13
ATLAS SSDP Traffic Levels 37

Table A1
Exploited Protocols 38

Type, Frequency and Motivation of DDoS Attacks 39

Figure 19
DDoS Attack Types 40

Figure 20
Multi-Vector DDoS Attacks 41

Figure 21
Targets of Application-Layer Attacks 41

Figure 22
Types of Attacks Targeting Encrypted Services 42

Figure 23
Application-Layer Attack Tools 43

Figure 24
Attack Frequency 44

Figure 25
Longest Attack Duration 44

Figure 26
Attack Motivations 44

Network, Customer and Service Threat Detection 45

Figure 27
Threat Detection Tools 46

Figure 28
Layer 7 Flow 46

Figure 29
Effectiveness of Threat Detection Tools 47

Attack Mitigation Techniques 49

Figure 30
Attack Mitigation Techniques 50

Figure 31
Time to Mitigate 50

Figure 32
Outbound Mitigation Mechanisms 51

Service Provider Corporate Network Threats 53

Figure 33
Incident Response Posture 54

Figure 34
Incident Response Assistance 54

Figure 35
Internal Network Security Threats 55

Figure 36
Internal Network Security Concerns 55

Table 1
Incident Response Time 56

Figure 37
Rate of Internal Network Incidents 56

Figure 38
Incident Response Preparedness 57

Figure 39
Incident Response Improvements 57

Figure 40
Internal Network Threat Detection Mechanisms 58

Figure 41
Actual Detection Methods and Sources 58

Figure 42
Incident Response 59

Figure 43
Social Media on Internal Networks 59

Figure 44
Identification of Employee-Owned Devices 60

Figure 45
BYOD Access Restrictions 61

Figure 46
BYOD Security Breach 61

Service Provider IPv6 63

Figure 47
Subscriber IPv6 Usage 64

Figure 48
Business Customer IPv6 Service Usage 64

Figure 49
IPv6 Flow Telemetry 65

Figure 50
IPv6 Traffic Growth 65

Figure 51
IPv6 Security Concerns 66

Figure 52
IPv6 Mitigation Capabilities 66

ATLAS IPv6 67

Figure A14
ATLAS Participants Providing Native IPv6 Data 67

Figure A15
ATLAS IPv6 Traffic 67

Data Center 69

Figure 53
Data Center Traffic Visibility 70

Figure 54
Data Center Anti-Spoofing Filters 70

Figure 55
Data Center Threat Protection 71

Figure 56
Data Center DDoS Attack Frequency 71

Figure 57
Data Center Attack Targets 72

Figure 58
Data Center DDoS Business Impact 72

Figure 59
Data Center DDoS Defenses 73

Figure 60
Data Center Firewall Failures Due to DDoS 73

Mobile Network Operators 75

Figure 61
Number of Subscribers 76

Figure 62
Radio Technologies 77

Figure 63
LTE Deployment 77

Figure 64
Security Incidents 77

Figure 65
Security Measures 78

Figure 66
Visibility in Packet Core 79

Figure 67
Visibility Mechanism 79

Figure 68
Roaming Data Monitoring 80

Figure 69
Poorly Implemented Application Impact 80

Figure 70
DDoS Attacks from Mobile Users 81

Figure 71
Outbound Attack Mitigation 81

Figure 72
DDoS Attacks on Mobile Infrastructure or Users 82

Figure 73
Mobile Resources Affected by DDoS Attacks 82

Figure 74
Number DDoS Attacks on Mobile Infrastructure 83

Figure 75
Visibility at (Gi/SGi) IP Backbone 83

Figure 76
Visibility Mechanism 84

Figure 77
DDoS Impact on IP Infrastructure 84

Enterprise, Government and Education Network Security 85

Figure 78
Most Significant Operational Threats 86

Figure 79
Operational Security Concerns 87

Table 2
Incident Response Time 87

Figure 80
Incident Response Posture 88

Figure 81
Use of External Organizations for Incident Response 88

Figure 82
Incident Response Rate 89

Figure 83
Incident Response Preparedness 89

Figure 84
Incident Response Improvements 90

Figure 85
Internal Network Threat Detection Mechanisms 90

Figure 86
Actual Detection Methods and Sources 91

Figure 87
Social Media on Internal Networks 91

Figure 88
Identification of Employee-Owned Devices 92

Figure 89
BYOD Access Restrictions 93

Figure 90
BYOD Security Breaches 93

Enterprise, Government and Education DDoS Attacks 95

Figure 91
Targets of DDoS Attacks 96

Figure 92
Firewalls and IPS Affected by DDoS Attacks 96

Figure 93
DDoS Attack Duration 97

Figure 94
Business Impact of DDoS Attacks 97

Figure 95
Attack Category Breakout 98

Figure 96
Targets of Application-Layer Attacks 98

Figure 97
Encrypted Application-Layer Attacks 99

Figure 98
Multi-Vector Attacks 99

Figure 99
DDoS Attack Motivations 100

Figure 100
DDoS Mitigation Techniques 101

Figure 101
DDoS Attack Mitigation Time 101

Enterprise IPv6 103

Figure 102
IPv6 Service Availability 104

Figure 103
IPv6 Flow Telemetry 105

Figure 104
IPv6 Security Concerns 105

Measuring IPv6 Adoption 107

Figure SIG1
Seven Measures of IPv6 Adoption Over Five Years 107

Figure SIG2
Traffic per Customer and Ratios for Peak and Average Datasets 108

Table 3
IPv6 Growth 108

Table 4
Comparison of IPv6 Application Breakdown and Convergence at Similar Ratios as IPv4 Signaling Adoption . . . 109

Figure SIG3
Regional IPv6 vs. IPv4 Ratios 109

DNS Operators 111

Figure 105
DNS Security Responsibility 112

Figure 106
DNS Traffic Visibility 112

Figure 107
Attacks Targeting Authoritative Servers 113

Figure 108
Attacks Targeting Recursive Servers 113

Figure 109
DDoS Protection Mechanisms 113

Organizational Security Practices 115

Figure 110
Infrastructure Best Current Practices 116

Figure 111
DDoS Attack Simulations 117

Figure 112
BGP Route Filtering 117

Figure 113
Route Hijack Monitoring 117

Figure 114
Participation in OPSEC Community 118

Conclusion 119

About the Authors 120

Glossary 121

OVERVIEW

Welcome to our tenth annual *Worldwide Infrastructure Security Report* (WISR). The data within this document is based on the collective experiences, observations and concerns of the global operational security community. Arbor has collected this data through a survey conducted in October 2014.

For the past 10 years, Arbor has produced the WISR – collecting detailed information on the threats and concerns of a variety of network operators, collating this data and then presenting it as a free-to-access repository of information. This document is intended to highlight the key trends in the threats and concerns facing today's organizations, and the ways in which these organizations are mitigating those threats.

Since its inception, the WISR has been based upon survey data collected from those who are directly involved in day-to-day operational security, and this is our continued approach. The WISR has changed immeasurably in terms of its scope and scale over 10 years, but the core goal is still to provide real insight into infrastructure security from an operational perspective.

Survey Methodology

The 2014 Infrastructure Security Survey is comprised of 182 free-form and multiple choice questions, a significant increase over the 131 of last year. However, the greater number of questions belies the fact that this year's survey has specific logic flows that enable service providers and government/enterprise/education respondents to see a different set of questions depending upon their self-classification. This change has proved necessary as the number of non-service-provider respondents continues to grow. The questions we need to ask diverge depending upon the nature of the respondent, and we are addressing feedback from last year to reduce the number of irrelevant questions asked to each respondent.

As in previous years, we have modified the survey questions to reflect changes in the threat landscape and technology and to address responses from last year's survey. The survey is divided into sections that address specific topics such as DDoS attacks, corporate network security, IPv6, data centers, mobile networking, etc. Each section establishes the observations and concerns of respondents and, where appropriate, the mechanisms put in place to manage their concerns.

Arbor distributes the WISR survey using an email list that specifically targets people within the operational security community to get as accurate a picture as possible. We saw a significant increase in the number of respondents to this year's survey, up to 287 from 220 last year, which in turn was up from 130 in 2012. Looking back to 10 years ago (which we do throughout this year's report), we had only 36 respondents—so the data now presented in the WISR is significantly more representative across a broader range of geographies and network operator types.

Key Findings

Service Provider Threats and Attacks

- DDoS attacks against customers remain the number one operational threat to service providers. Attacks against infrastructure continue to grow in prominence.
- Respondents see more demand for DDoS detection and mitigation services, with cloud/hosting organizations joining the top tier of verticals interested in these services.
- End-user subscribers and e-commerce organizations are the most commonly targeted DDoS attack victims, with government in the third spot.
- Attackers continue to use reflection/amplification techniques to create gigantic attacks. The largest reported attack was 400 Gbps, with other respondents reporting attacks of 300 Gbps, 200 Gbps and 170 Gbps. Another six respondents reported events that exceeded the 100 Gbps threshold.
- Although nearly two-thirds of attacks were volumetric in nature this year, almost all respondents reported application-layer attacks and 42 percent saw multi-vector attacks.
- More respondents reported a high frequency of attacks this year. Last year just over a quarter of respondents indicated they had seen more than 21 attacks per month. This year that number increased dramatically to 38 percent.
- The proportion of respondents seeing application-layer attacks targeting encrypted web services (HTTPS) has unexpectedly declined to 42 percent from 54 percent last year (but is still above the 37 percent seen in 2012).
- The proportion of respondents seeing attacks targeting cloud-based services has grown significantly.
- The top three motivations behind attacks remain nihilism vandalism, online gaming and ideological hacktivism—all of which have been in the top three for the past few years. Gaming has gained in percentage, which is no surprise given the number of high-profile, gaming-related attack campaigns this year.
- NetFlow analyzers are viewed as the most effective way of detecting threats. However, firewall logs—the second most commonly used detection mechanism—rank sixth in terms of effectiveness.
- The percentage of respondents using intelligent DDoS mitigation systems (IDMS) to mitigate DDoS attacks has moved ahead of ACLs for the first time this year.
- Over half of respondents saw an increase in security incidents on their corporate network. However, just under half say they are at least reasonably prepared with a similar number only somewhat prepared and a further 8 percent completely unprepared.
- Internet congestion due to DDoS attacks is by far the most common threat seen for service provider corporate networks.

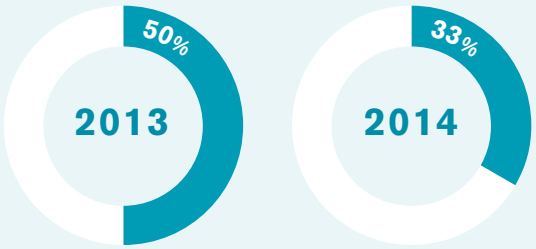
Enterprise, Government and Education Threats and Attacks

- The most frequently observed threats on enterprise networks are DDoS attacks, accidental data loss and botted or otherwise compromised hosts—all garnering around a third of respondents.
- Nearly half of respondents saw DDoS attacks during the survey period, with almost 40 percent of those seeing their Internet connectivity saturated.
- Respondents reported that 29 percent of attacks targeted the application layer, significantly higher than the 20 percent reported by service providers. This may be due to the fact that service providers are not aware of all the application-layer attacks going on, given their macroscopic network view.
- Eighty-one percent of respondents saw application-layer attacks targeting HTTP, and nearly 60 percent saw attacks against HTTPS and DNS.
- Over a third of organizations had their firewall or IPS devices experience a failure or contribute to an outage during a DDoS attack.
- Operational expenses, reputation damage and revenue loss are the top business impacts of DDoS attacks.
- Diversion to cover compromise or data exfiltration is the third highest perceived DDoS attack motivation.
- Nearly a fifth of respondents indicated that APTs have targeted their organizations during the survey period.
- Just over a third of respondents indicated an increase in security incidents this year, with about half indicating similar levels to last year. Fewer than half of respondents feel reasonably or well-prepared for a security incident, with 15 percent indicating that they have no plans or resources in place.
- Firewalls/IPS/UTP systems and NetFlow analyzers represent the most common threat detection mechanisms.

Security Practices

- The proportion of organizations that practice DDoS attack and defense simulations continued to decrease again this year.
- The challenges facing organizations as they build and maintain security teams remain the same, with the top two being lack of headcount and difficulty hiring and retaining skilled personnel. It should be noted that there has been a 14 percent increase in respondents reporting the latter, which indicates that the skills shortage within the security industry is not abating.

The proportion of respondents implementing BCP 38/84 anti-spoofing has dropped from around half last year to just over a third this year. Given that the lack of anti-spoofing filters at the Internet edge is one of the key reasons why reflection/amplification DDoS attacks are possible, it was expected that this proportion would have increased. **This is bad news.**



DNS

- Fewer companies have dedicated security groups responsible for DNS.
- No real change has occurred in the percentage of respondents implementing the best practice of restricting DNS recursive lookups.
- Respondents reported fewer DDoS attacks against DNS infrastructure that resulted in a customer-visible outage.

IPv6

- Over two-thirds of service provider respondents indicated that they have deployed IPv6 within their networks, or plan to deploy it within the next 12 months. Only a third of enterprise, government and educational respondents indicated the same.
- Nearly three-quarters of service provider respondents now have subscribers utilizing IPv6 services, but IPv6 service take-up rates for both subscribers and business customers are still mostly under 25 percent.
- Sixty-four percent of service providers have IPv6 traffic visibility, an encouraging jump from just over half last year. Fifty-five percent of enterprise, government and education respondents have IPv6 traffic visibility.
- Nearly half of the service provider respondents indicated that attacks over IPv6 impacting IPv4 services on dual-stack devices are a major or moderate concern.
- The top IPv6-related security concern for enterprise, government and education respondents, by a significant margin, is inadequate IPv4/IPv6 feature parity.
- IPv6 traffic growth continues to outstrip expected levels.

Mobile Network Operators

- Over 75 percent of MNO respondents indicated that they already have LTE equipment deployed, with a further 16 percent planning to deploy it in 2015.
- Seventeen percent of respondents indicated that they have experienced a security incident on the mobile packet core that led to a customer-visible outage, down from just over 20 percent last year and around a third in 2012.
- iACLs and NAT/PAT technology are still the most common protective measures used by MNOs to protect their packet core. There has been a significant increase in the use of both of these technologies.
- Four out of five mobile operators participating in the survey do not support the use of IPv6 in either the subscriber devices or mobile infrastructure on their networks.
- The percentage of respondents seeing between 51 and 100 attacks a month, targeting their end-users or mobile packet core, more than doubled this year.
- The frequency of DDoS attacks on the mobile Internet (Gi/SGi) is down significantly from last year.

Data Centers

- Over a third of data center operators saw DDoS attacks that exhausted their Internet bandwidth.
- Operational expense is the top cost attributed by data center operators to DDoS events. Revenue losses due to DDoS attacks are up sharply.
- Firewalls, application firewalls and IPS are still the top three deployed security mechanisms in the data center. Respondents reported big increases in the use of both IDMS and iACLs.
- Just under half of respondents indicated that their firewalls experienced or contributed to an outage due to DDoS. Load balancers also saw issues, with over a third of respondents seeing these fail due to DDoS in the last year.

Over 75 percent of mobile network operators indicated that they already have LTE equipment deployed, with a further 16 percent planning to deploy it in 2015.

Operational expense is by far the top cost attributed by data center operators to DDoS events.

1 Demographics of Survey Respondents

The number of respondents to the WISR survey continues to grow strongly. This year 60 percent of respondents are service providers, a lower proportion than we have seen previously. This is mainly due to increased participation by government and education organizations. Enterprise participation stays strong at 18 percent, similar to last year. The United States and Canada now represent the lead region for participation at just over a third of respondents, slightly ahead of Western, Central and Eastern Europe. Most respondents offer multiple services, with managed security services now tying for the second most commonly offered service—demonstrating the growth in this key market. Over 90 percent of respondents now have some dedicated security resources; this is the highest proportion we have ever seen and indicates continued focus on security across all types of network operators.

As in previous years, the majority of respondent organizations continue to be service providers from a primary function perspective (Figure 1). However, the proportion of service provider respondents dropped from just over 68 percent to 60 percent this year—mainly due to increased participation by government and education organizations. It should be noted that the actual number of tier-1 and tier-2/3 service providers participating in the survey has stayed relatively static.

Respondent Organization's Primary Business Function

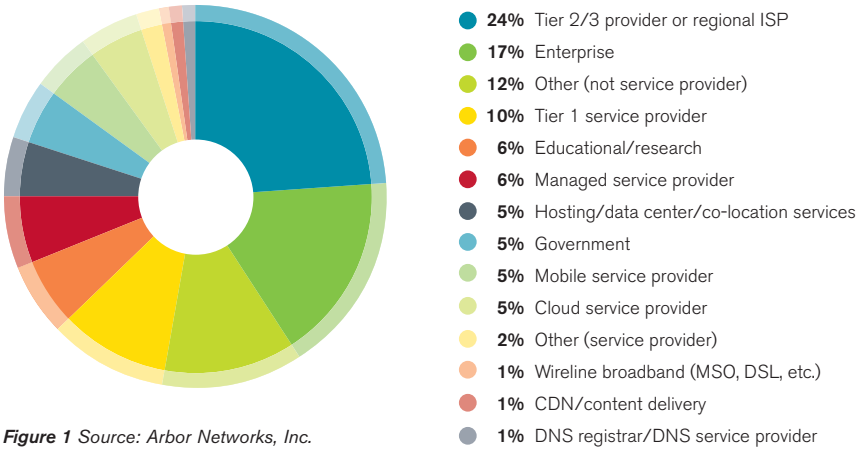


Figure 1 *Source: Arbor Networks, Inc.*

Last year we saw a big jump in the proportion of enterprise respondents to the survey—up to 18 percent from 8 percent in 2012. This year the percentage of enterprise respondents has stayed at approximately the same level, with small increases in the proportions of government and educational respondents. This is a marked contrast to 10 years ago when *all* respondents were service providers.

The WISR represents data collected from organizations that are headquartered—and that operate networks—all around the world (Figure 2). This year the highest proportions of respondents are headquartered either in the United States and Canada or in Western, Central and Eastern Europe. Many respondents offer services in multiple regions around the globe (Figure 2), with nearly half of respondents offering services either in the United States and Canada or in Western, Central and Eastern Europe.

Organization's Geographic Information

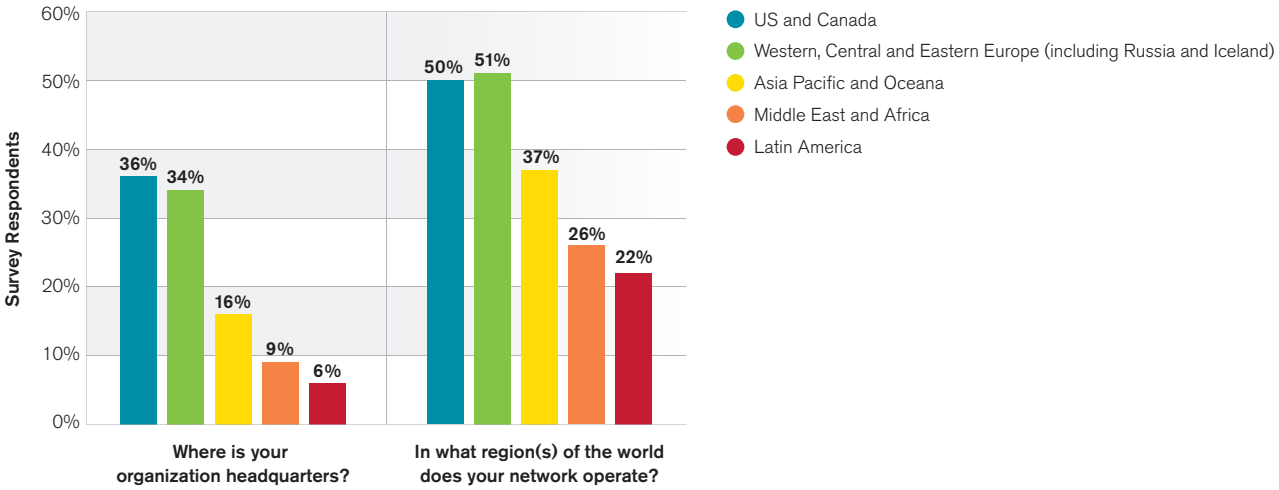


Figure 2 *Source: Arbor Networks, Inc.*

The survey also queried participating network operators about the services they offer (Figure 3). For those who provide services, most respondents offer multiple services—with the most common being business Internet access, hosting/co-location services and managed security services. Business Internet and hosting/co-location services were the top two in last year's survey, but managed security services has moved up from sixth place to tie for second this year. This indicates continued growth in the need for security services. What is interesting this year is that the proportion of respondents offering each type of service has dropped in all cases. This may indicate that respondents are narrowing their focus and reducing the spread of services they offer.

Organization's Services Offered

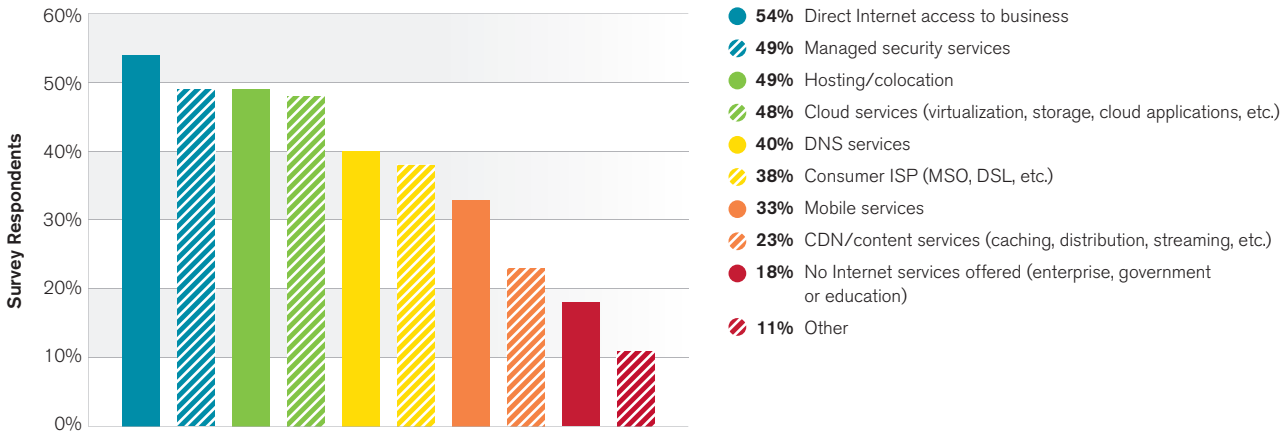


Figure 3 *Source: Arbor Networks, Inc.*

This year nearly three-quarters of respondents are security, network or operations professionals (Figure 4)—up from just over half last year. The remainder are managers, directors or executives focused within the security and networking space.

Just over half of respondents maintain an internal security operations center (SOC), with a further 13 percent taking a hybrid approach (Figure 5). Outsourcing this function remains unpopular, with only 5 percent of respondents taking this approach—down from 8 percent last year. A full quarter of respondents indicated that they have no SOC provision at all. Hybrid SOCs are a mix of internal SOC resources supplemented by third-party SOC resources primarily for additional coverage on off hours and weekends. This is a growing trend that enables organizations to achieve 24x7 coverage, even if they are not staffed to perform this.

Respondent's Role

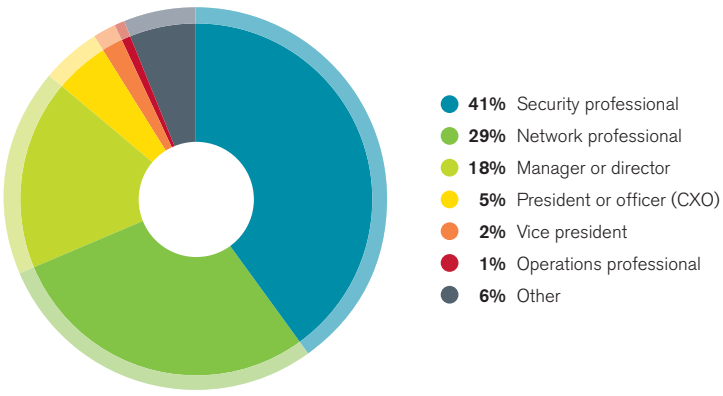
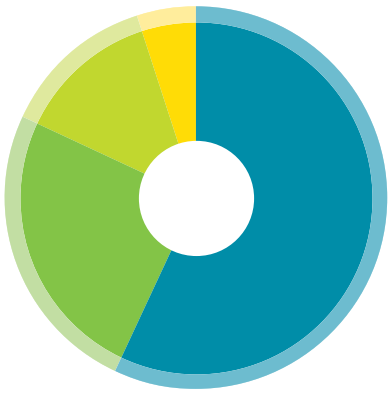


Figure 4 *Source: Arbor Networks, Inc.*

Looking more generally at dedicated security resources, 94 percent of respondents indicated they have personnel in place (Figure 6). This is a large and welcome increase from 81 percent last year and is higher than our previous record of 85 percent back in 2011. However, most organizations continue to work with relatively small teams of dedicated security personnel. Just over half of respondents have fewer than 10 dedicated resources—an almost identical percentage to last year. We have again seen an increase in the proportion of respondents with very large security teams (over 30 engineers)—up to one-quarter this year from 21 percent last year and 10 percent the year before. Interestingly, a significant number of these organizations self-categorize themselves as enterprises, accounting for the largest proportion behind tier-1 and tier-2/3 service providers.

SOC Type



- **57%** Internal SOC team
- **25%** No SOC rsources
- **13%** Internal SOC with supplemental third-party (hybrid)
- **5%** Third-party SOC (outsourced)

Figure 5 *Source: Arbor Networks, Inc.*

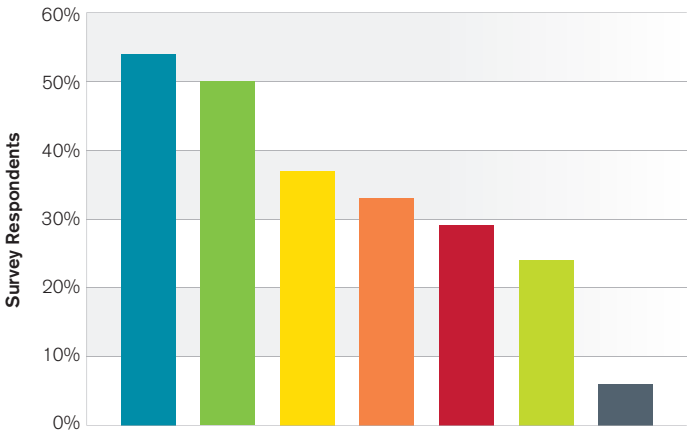
Dedicated Security Personnel

- **6%** 0
- **36%** 1-5
- **15%** 6-10
- **8%** 11-15
- **5%** 16-20
- **5%** 21-30
- **25%** More than 30

Figure 6 *Source: Arbor Networks, Inc.*

The challenges facing organizations as they build and maintain security teams remain the same (Figure 7), with the top two being lack of headcount and difficulty of hiring and retaining skilled personnel. It should be noted that there has been a 14 percent increase in respondents reporting the latter, which indicates that the skills shortage within the security industry is not abating.

Dedicated Security Personnel



- **54%** Lack of headcount or resources
- **50%** Difficulty of hiring and retaining skilled personnel
- **37%** Operational expenditure (OPEX) funding
- **33%** Capital expenditure (CAPEX) funding
- **29%** Lack of management support
- **24%** Lack of internal stakeholder support
- **6%** Other

Figure 7 *Source: Arbor Networks, Inc.*

Introduction

Arbor is incorporating data in this report from its ATLAS® Active Threat Level Analysis System. ATLAS is unique, as it is the only globally scoped threat analysis system in existence. ATLAS leverages Arbor's service-provider customer base, the Arbor Security Engineering & Response Team (ASERT) and relationships with other organizations in the security community to collate and correlate information pertaining to current security threats.

This report makes use of ATLAS data for comparison and correlation with survey responses. ATLAS data relies upon (at time of writing) 330+ Peakflow® customers from around the world anonymously sharing statistics on a peak of over 120 Tbps of traffic during 2014 (Figures A1, A2 and A3).

The data shared includes information on the traffic crossing the boundaries of the participating network operators, and anonymized details on the DDoS attacks they are detecting. The received data is collated and trended to deliver a detailed picture of the way in which Internet traffic and DDoS attacks are evolving.

ATLAS IPv4 Tracked Traffic

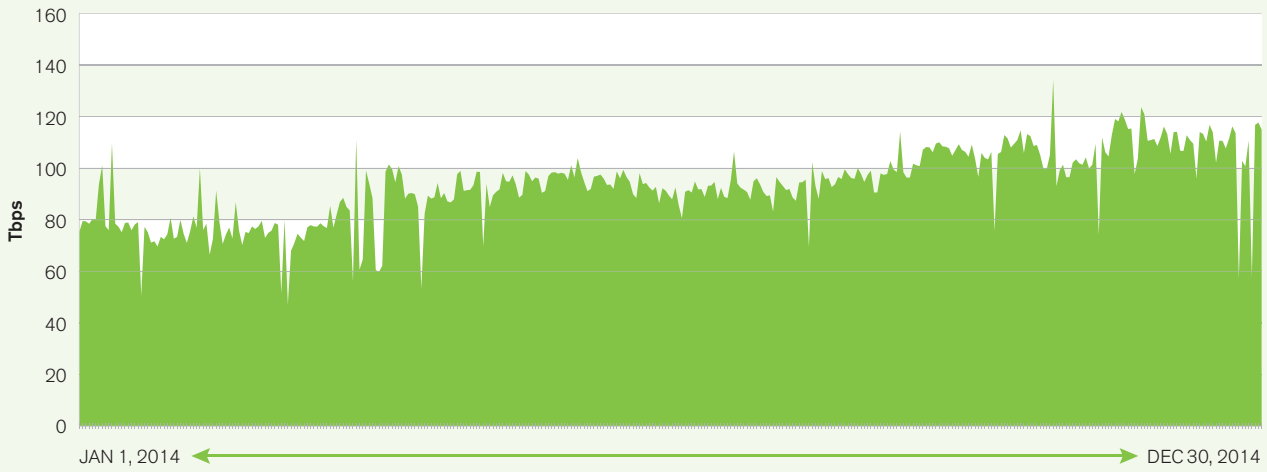


Figure A1 *Source: Arbor Networks, Inc.*

Participant Geographic Distribution

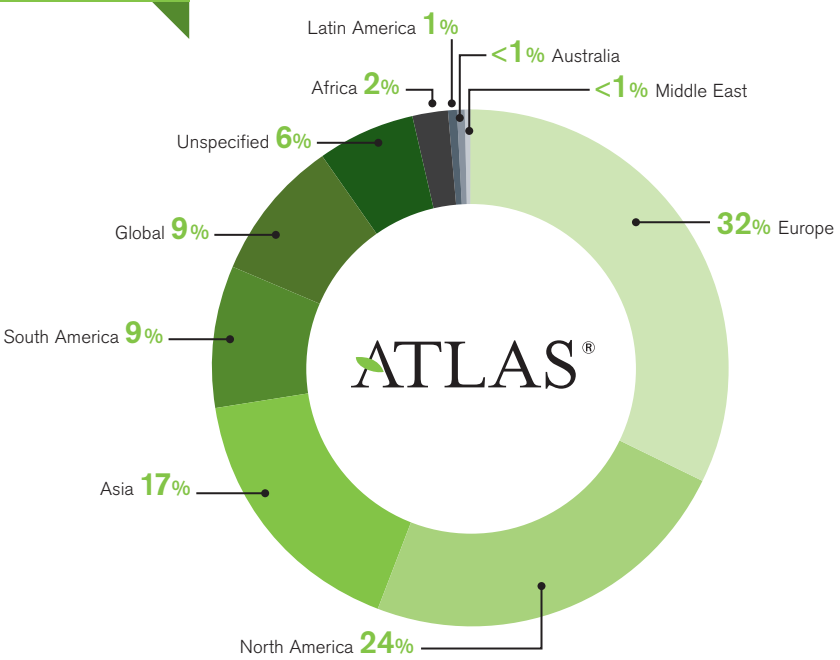


Figure A2
Source: Arbor Networks, Inc.

Participant Operator Types

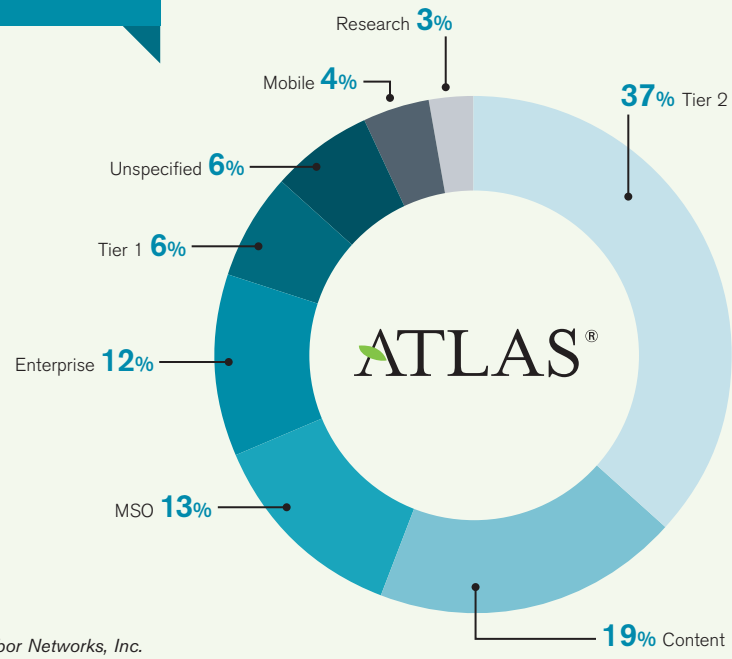


Figure A3
Source: Arbor Networks, Inc.

2 Most Significant Operational Threats: Service Providers

DDoS attacks against customers remain the number one operational threat. A higher proportion of respondents are seeing DDoS attacks against infrastructure this year. Demand for DDoS detection and mitigation services increased again, with the top verticals interested in these services being cloud/hosting providers, finance, government and e-commerce. Just under half of respondents plan to use SDN/NFV in a production environment within two years.

As in previous iterations of this report, DDoS attacks against customers are the most commonly experienced security threat for respondents (Figure 8). The percentage of respondents seeing these attacks returned to the 2012 level of around 75 percent after dropping last year to 64 percent. In fact, the proportions of respondents seeing DDoS attacks targeting services also rebounded to around the 2012 level. Attacks targeting infrastructure were slightly higher this year at 55 percent. This ties in with anecdotal information Arbor has received that seems to indicate that attackers are more regularly targeting infrastructure due to improved DDoS protection for specific customers and services.

Service Provider Experienced Threats

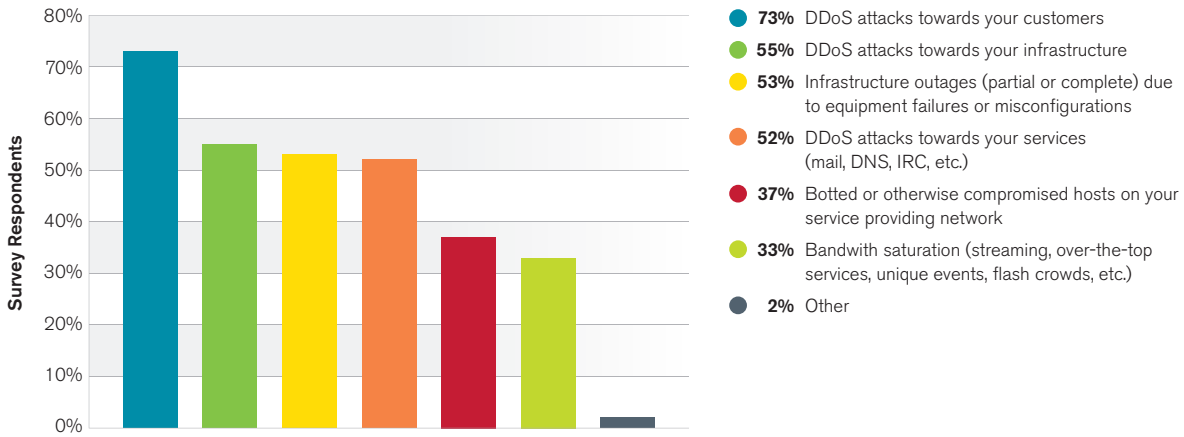


Figure 8 *Source: Arbor Networks, Inc.*

Looking at other threats, the number of respondents experiencing bandwidth saturation has declined this year to around one-third, mid-way between the 2012 and 2013 results. More interestingly, we are seeing a declining trend in the percentage of those experiencing infrastructure outages due to equipment failures or misconfiguration. This has dropped from the number two position to number three, with the percentage falling over the past few years from 60 percent, to 55 percent, and now 53 percent. This is very encouraging.

Looking at security concerns for the next 12 months (Figure 9), DDoS attacks take the top three positions as in last year's report, but with percentages up across the board. Almost three-quarters of respondents now see DDoS attacks against infrastructure as their top concern, up from two-thirds last year. This reinforces the point made earlier about current attack trends. DDoS attacks against customers are also more of a concern—up 9 percent. However, we have seen some decline in the proportion of respondents concerned about bandwidth saturation and infrastructure outages due to equipment failures or misconfiguration. The former is likely due to the lower proportion of respondents who have experienced this issue in the last 12 months. The latter may be indicative of a rise in configuration automation.

Service Provider Experienced Threats

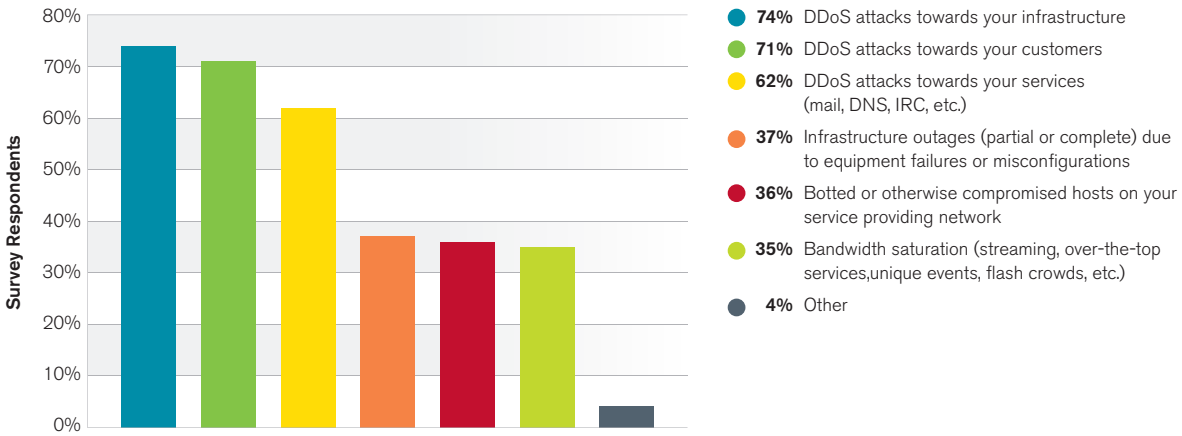


Figure 9 *Source: Arbor Networks, Inc.*

This year we again have an increase in the proportion of respondents who see more demand for DDoS detection and mitigation services, up 8 percent from last year (Figure 10). This should come as no surprise given both the results presented earlier in this section, and the increased enterprise focus and awareness around availability threats. We drilled into the demand for these services in more detail to try and establish which verticals are driving this increase (Figure 11).

Demand for DDoS Detection/Mitigation Services

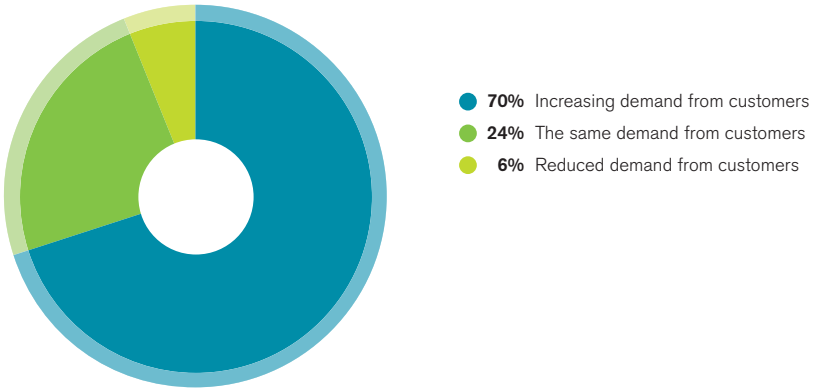


Figure 10 *Source: Arbor Networks, Inc.*

As last year, government and finance are in the top tier of verticals interested in these services. This year they are joined by e-commerce and cloud/hosting providers. This latter category is especially interesting given the increased adoption of cloud-based data and application services seen across a broad spread of industries. Cloud services can offer significant business advantages, but to exploit those advantages the services must be reachable. It looks as if cloud/hosting providers may become a key consumer of availability protection services to ensure this is the case. Also interesting is the broad spread of verticals with relatively high percentages. This indicates that a wide variety of organizations are now aware of—and looking for—solutions to the DDoS threat.

As new technologies evolve, mature and start to gain acceptance, Arbor adds questions to the WISR survey to assess levels of adoption and perceived risks. SDN and NFV are being discussed more and more by vendors, end-users and technology consultants alike as these technologies can offer significant cost and service agility benefits. In light of this, we asked respondents when or if they are planning on implementing SDN/NFV in a production environment.

Interestingly just over 10 percent of respondents indicated that they are already using SDN or NFV in their production environments, with a further one-third planning to use these technologies within the next two years. In terms of the locations within networks where these technologies are seeing the most interest, data centers are the clear leader. Over two-thirds of respondents planning to deploy these technologies are looking to use them in their data center. However, over a third of respondents also indicated that they plan to use SDN or NFV within their fixed-line infrastructure and/or within their value-added service infrastructure.

Business Verticals for DDoS Services

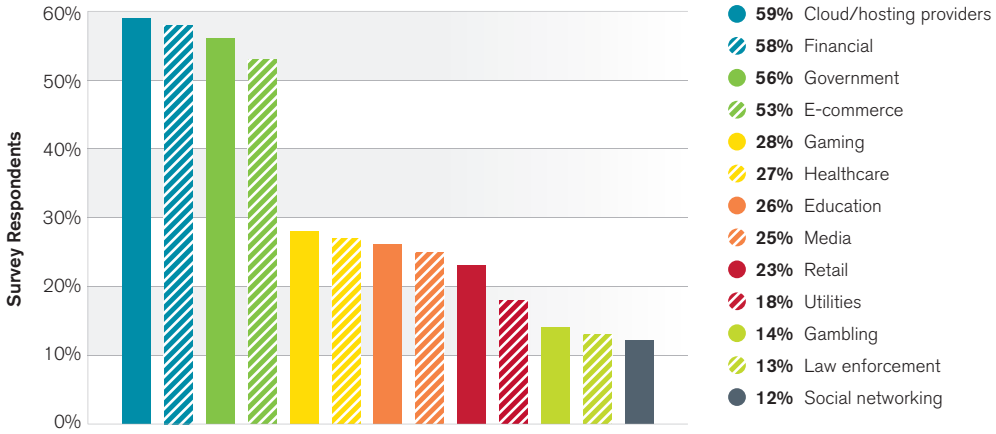


Figure 11 *Source: Arbor Networks, Inc.*

3 Scale and Targeting of DDoS Attacks

The largest attack reported by a respondent this year was 400 Gbps, with other respondents reporting attacks of 300 Gbps, 200 Gbps and 170 Gbps. Nearly three-quarters of respondents saw their customers being the target of their largest monitored attack. Customers remain the number one target, with over two-thirds of attacks targeting them. Service infrastructure is in second place. This year, the proportion of respondents seeing attacks targeting cloud-based services has grown significantly to 29 percent—up from 14 percent two years ago and 19 percent last year.

Through this survey period attackers appear to have continued the 2013 trend of using volumetric attacks to congest their targets' connectivity to the point where their goal is achieved. The largest attack reported by a respondent this year was 400 Gbps, with other respondents reporting attacks of 300 Gbps, 200 Gbps and 170 Gbps. Another six respondents reported events that exceeded the 100 Gbps threshold. In fact, almost 20 percent of respondents reported peak attack sizes over 50 Gbps during this survey period. Some of these attacks were a part of the plague of NTP reflection/amplification attacks in the first half of 2014, one of which was the largest attack ever tracked by the ATLAS system. Please reference the "ATLAS: A Time for Reflection" section of this report for more details. At 325 Gbps, this was slightly larger than the Spamhaus event in 2013, which weighed in at 309 Gbps.

It should be noted that a couple of years ago, a DDoS attack above 100 Gbps was a very rare occurrence. That is not so today. Based on conversations outside of this survey, Arbor is aware that many operators who reported large attacks also saw multiple such attacks throughout the year (i.e., they were not unique events). This is corroborated by ATLAS data. Please see the "ATLAS Attack Sizes" section of this report for more Arbor insight in this area.

Ten years ago, the first iteration of the WISR described peak attack sizes ranging from 5 Gbps to 8 Gbps. The peak attack size this year—400 Gbps—represents 4,900 percent growth over that 10-year period, illustrating how the DDoS threat has escalated. All of the largest reported attacks used UDP traffic targeted at NTP, DNS, SNMP, HTTP or HTTPS ports—likely indicating the use of a reflection/amplification mechanism to generate the traffic.

Survey Peak Attack Size Year Over Year

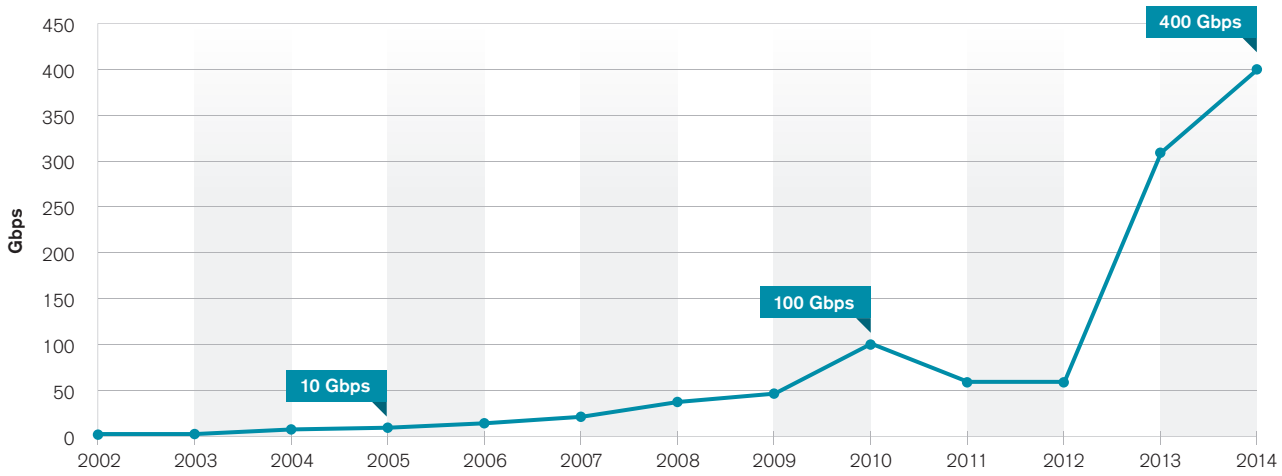


Figure 12 *Source: Arbor Networks, Inc.*

This year's survey asked a specific question about the protocols used for reflection/amplification (Figure 13). DNS remains the most commonly used protocol, with NTP not far behind. However, the results also show significant use of Chargen, SSDP and SNMP. Attackers are leveraging poorly configured or protected infrastructure to magnify their capabilities. The volumes of traffic generated can be significant, causing congestion problems for the target of the attacks and creating bottlenecks within the service provider's backbone and peering infrastructure. Please see the "ATLAS: A Time for Reflection" section of this report for more details.

Protocols Used for Reflection/Amplification

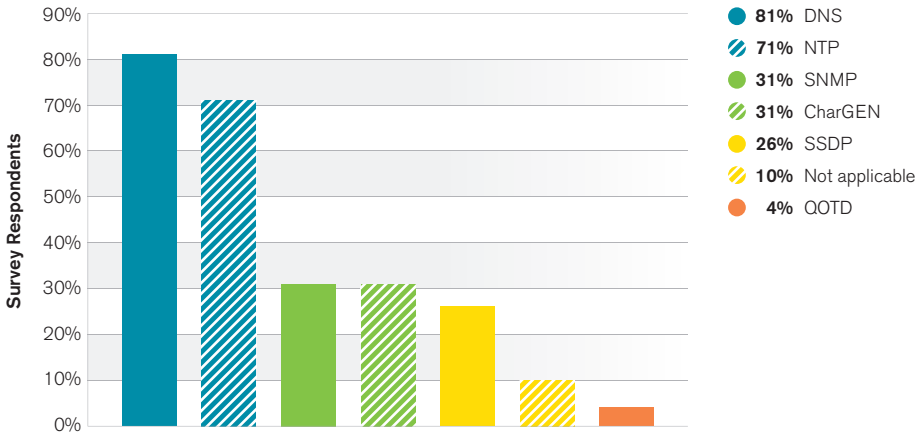


Figure 13 *Source: Arbor Networks, Inc.*

Regarding the targets of the largest attacks (Figure 14), nearly three-quarters of respondents saw their customers being hit—an increase from just under two-thirds last year. The proportion of respondents seeing infrastructure being the target has also stayed high at 15 percent, down from 20 percent last year but significantly up from the 8 percent seen in 2012. Attackers are continuing to target infrastructure with large volumetric attacks to achieve their goals—reducing the effectiveness of single-layer, on-premise defenses.

Target of Largest Attack

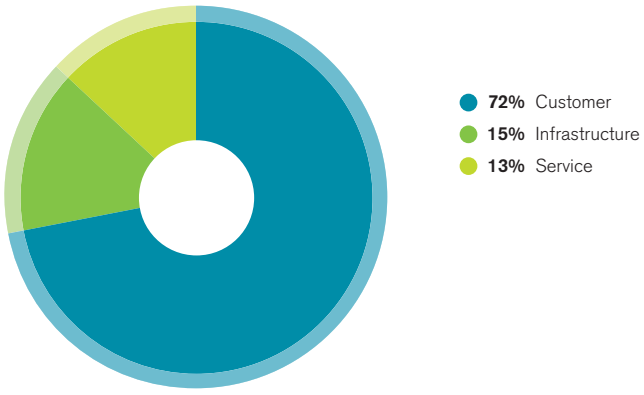


Figure 14 *Source: Arbor Networks, Inc.*

Looking more generally at the targets of the attacks monitored by survey participants (Figure 15), the results are very similar to last year and the year before. Customers remain the number one target, with over two-thirds of attacks targeting them. Service infrastructure is in second place. However, the percentage of attacks targeting service infrastructure has fallen from 25 percent to 19 percent. The proportion of attacks targeting network infrastructure has remained the same at 17 percent.

Attack Target Mix

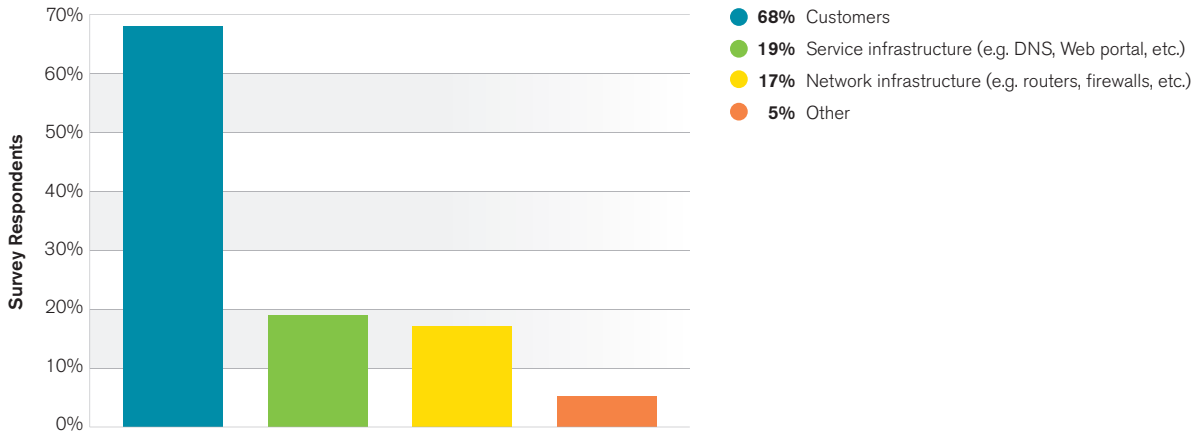


Figure 15 *Source: Arbor Networks, Inc.*

Based on feedback from last year's survey, we broadened the range of options available to survey respondents when specifying the "types" of customers they have seen being targeted (Figure 16). As last year, end-user subscribers and e-commerce organizations take the top two spots as the most common types of customer targeted. Finance, which was in third place last year, has moved down to fifth position behind both government and gaming. This shift may be due to the storm of attacks targeting gaming operators at the start of 2014, combined with the fact that Operation Ababil is no longer actively targeting financial institutions. Some of the additions to the options available have also seen significant results, with more than a quarter of respondents seeing attacks targeting customers in the hosting and education sectors.

Attack Target Customer Vertical

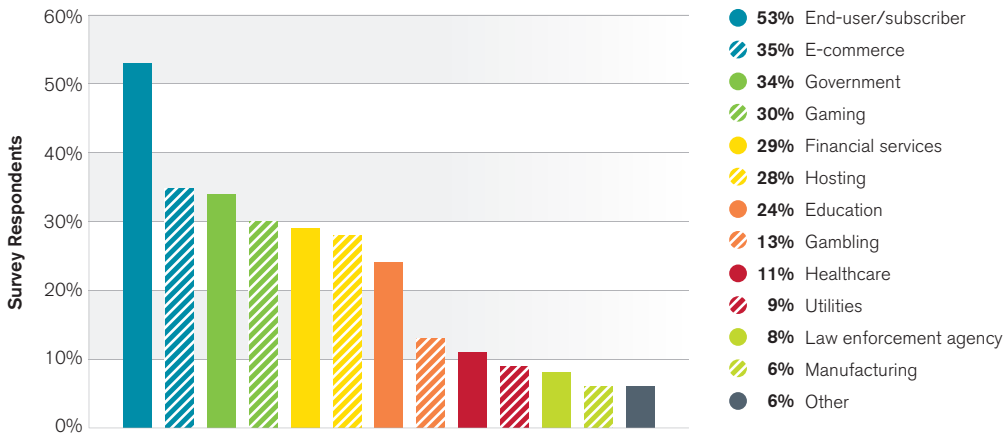


Figure 16 *Source: Arbor Networks, Inc.*

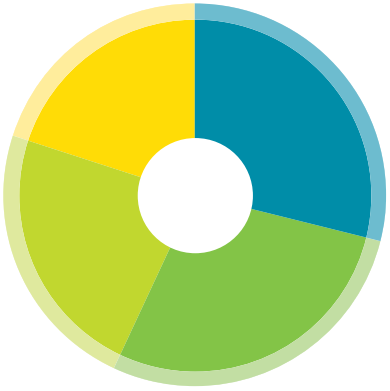
The adoption of cloud-based services is accelerating. Cloud services can offer significant performance, flexibility and cost advantages to business. However, they are generally reached via the Internet (even if a VPN is in place) and are therefore susceptible to DDoS attacks targeting their connectivity. When users cannot reach a cloud-based service, all of the business benefits are irrelevant. This year the proportion of respondents seeing attacks targeting cloud-based services has grown significantly (Figure 17), up from 14 percent two years ago, to 19 percent last year and 29 percent this year.

In terms of the types of cloud services being targeted, just over two-thirds of respondents saw attacks targeting IaaS services, with roughly one-third seeing attacks targeting SaaS and PaaS services.

Given that cloud services are frequent targets of attacks, they warrant protection from the DDoS threat, especially given the multi-tenant nature of some infrastructure. Attacks targeting one customer can impact others and cause collateral damage if appropriate defenses are not in place. This can lead to significant and potentially costly problems for the service provider.

When asked about their CGN NAT deployments, around half of this year's respondents indicated that they have CGN infrastructure deployed—about the same proportion as last year. In terms of how DDoS attacks impact this infrastructure, 19 percent of respondents have seen attacks causing either a full or partial outage—double last year's percentage (Figure 18). DDoS attacks can target any infrastructure that maintains a lot of per connection state. To reduce the threat surface of their network, organizations need to defend such infrastructure appropriately.

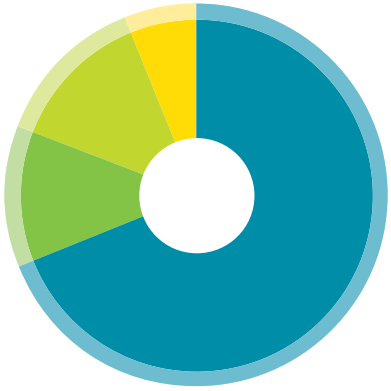
Attacks Targeting Cloud Services



- **29%** Yes
- **28%** Not applicable
- **23%** No
- **20%** Do not know

Figure 17 *Source: Arbor Networks, Inc.*

CGN DDoS Attack Impact



- **69%** No attacks
- **12%** Yes, but no impact
- **13%** Yes, with a partial outage
- **6%** Yes, with a significant outage

Figure 18 *Source: Arbor Networks, Inc.*

ARBOR ATLAS

Attack Sizes

The Arbor ATLAS system gathers statistics from 330+ Peakflow SP customers all around the world. These statistics include anonymized details of the DDoS attacks monitored by participants and summary information on the traffic crossing their network boundaries. Arbor's ASERT team collates and analyzes this unique data set to determine key trends in DDoS attack activity. This data is then released quarterly to the broader operational security community, and referenced within the WISR on an annual basis.

Again this year, the size of the largest attack reported by WISR participants increased substantially, and this has also been the case when looking at ATLAS data. This year the largest ATLAS monitored and verified attack was 325.05 Gbps, significantly up from last year's high of 245 Gbps. In fact, January, February, August and December 2014 all saw attacks that were larger than last year's peak (Figure A4).

ATLAS Peak Attack Sizes Month by Month (Gbps)

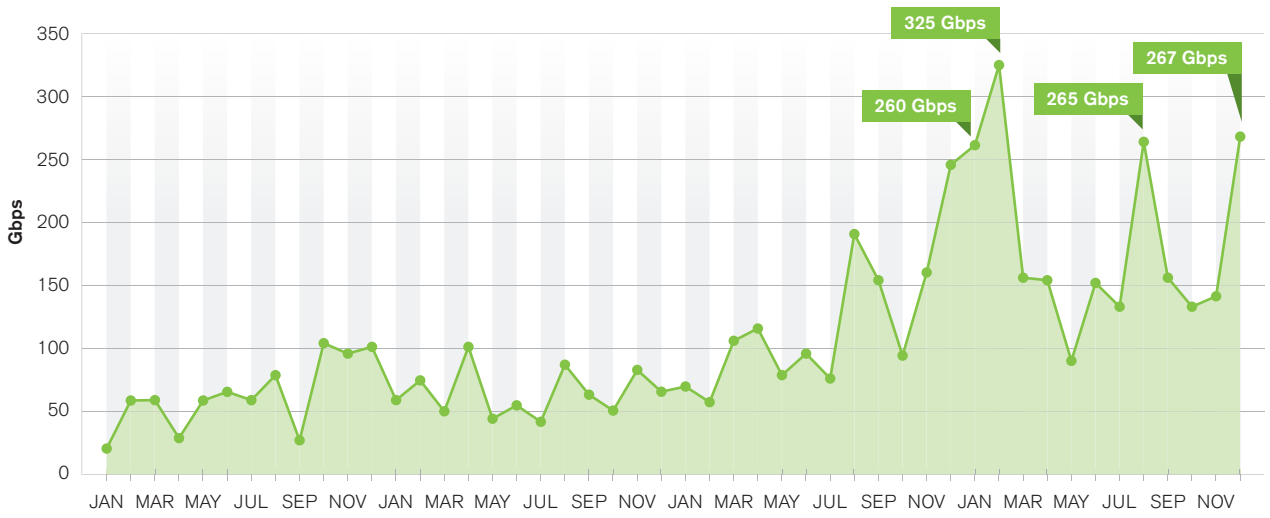


Figure A4 *Source: Arbor Networks, Inc.*

Again as last year, the very largest attacks were the product of reflection/amplification attack vectors. NTP reflection was responsible for most of the largest attacks, rather than DNS as in previous years. Please see the "ATLAS: A Time for Reflection" section of this report for further details. What is both interesting and very concerning this year is the sheer number of attacks over 100 Gbps. In 2013 ATLAS recorded 39 attacks over the 100 Gbps threshold. In 2014, we monitored 159 events—more than a fourfold increase. It should also be noted that the majority of the attacks over 100 Gbps that occurred in 2013 were in Q4 and were a part of the initial wave of NTP reflection attacks targeting gaming operators that continued through 2014. Figure A5 shows a graphical representation of the attack-size breakouts for this year month by month, clearly illustrating how frequently large attacks are now occurring.

The increased frequency and scale of large attacks and the continued use of varying reflection/amplification mechanisms to generate attack traffic are key concerns. Service providers need to scale their mitigation infrastructure and processes to deal with attacks of over 100 Gbps. Otherwise network operators could face significant collateral damage as peering and backbone capacity congests due to attack traffic.

Large Attack Breakout Month by Month

Figure A5 *Source: Arbor Networks, Inc.*

Attack Durations

In addition to tracking attack sizes, ATLAS also allows Arbor to track the duration of attacks monitored by participating network operators. During this survey period, attack durations have continued to fall.

Last year ATLAS data showed that 88 percent of events lasted less than one hour (up from 78 percent in 2012). This year that percentage has steadily increased in the first three quarters—reaching 90.1 percent in Q1 2014, 90.6 percent in Q2 and 91.2 percent in Q3—before dropping back to 87.7 percent in Q4 (Figure A3). To further emphasize this, the percentage of events lasting longer than 12 hours has fallen consistently through 2014—from 1.48 percent in Q1, to 1.38 percent in Q2 and 1.23 percent in Q3. Given the transient nature of attacks and the potential for extended service impact due to continued infrastructure failure, it is imperative for defenses to react quickly to any detected event. The trend in the WISR data shows that network operators are getting faster at mitigating attacks, with 68 percent of survey respondents indicating that they can mitigate attacks within 20 minutes.

ATLAS Attack Duration Breakout

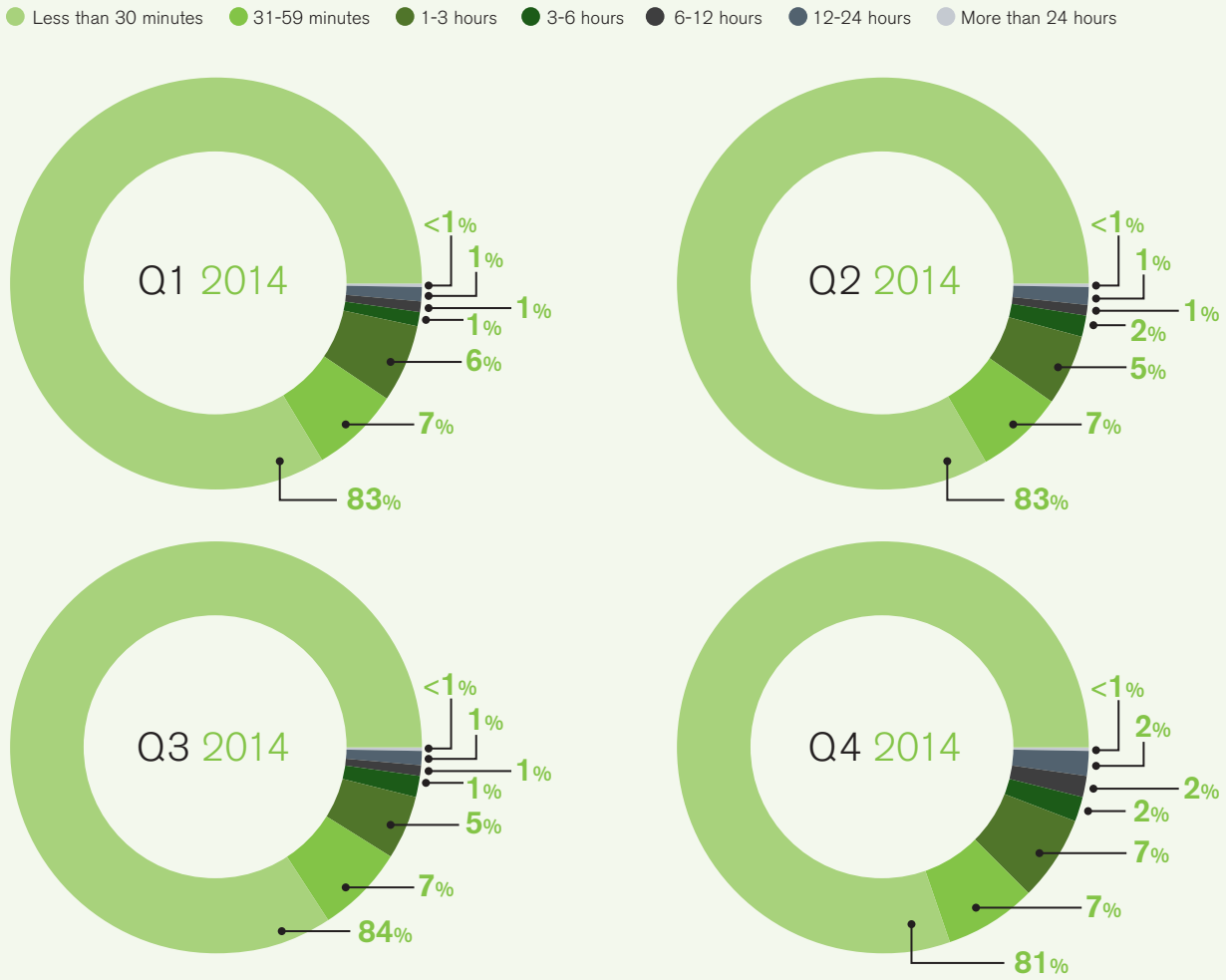


Figure A6 *Source: Arbor Networks, Inc.*

Targeted Services

In the first three quarters of 2014 ATLAS showed a steady increase in the proportion of attacks utilizing fragments. This is possibly due to the prevalence of reflection/amplification attack vectors. In Q1 2014, 21.8 percent of attacks used fragments, but this increased to just over 25 percent by the end of Q3 (Figure A7). However, in Q4 the proportion of attacks using fragments fell back to 18.4 percent—this may be due to ATLAS tracking a significantly higher number of small attacks (<500 Mbps) in Q4 (648875 in Q4 vs 509395 in Q3).

The top service port targeted during the survey period was HTTP, as in previous years. The percentage of attacks targeting port 80 grew throughout 2014 to just nearly a-quarter by the end of Q4. The proportion of attacks targeting encrypted web services (HTTPS) stayed nearly flat across the year, with a spike to 3.4 percent of attacks in Q3 (up from the normal levels of around 2.5 percent).

ATLAS Attack Port Breakout

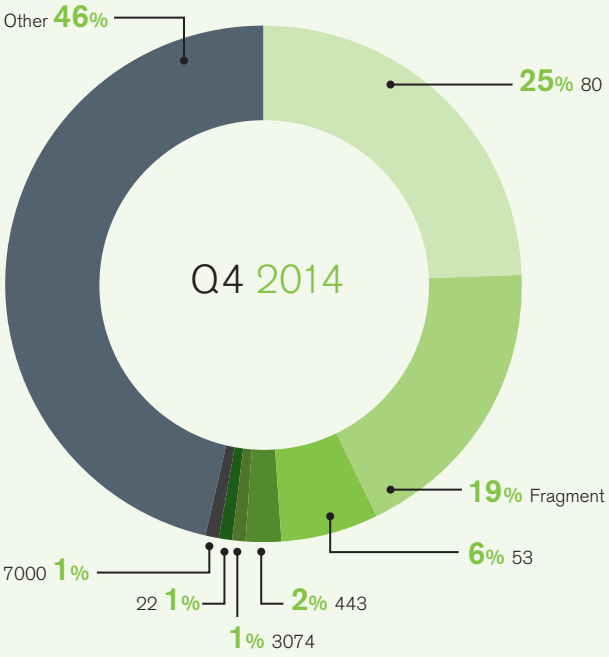


Figure A7 *Source: Arbor Networks, Inc.*

A Time for Reflection

During this survey period, ATLAS monitored possibly the most concentrated storm of large volumetric DDoS attacks ever seen on the Internet. These attacks were mainly generated using a reflection technique that leveraged poorly secured or configured NTP servers on the Internet.

Reflection/amplification techniques are not new where large DDoS attacks are concerned; they have been responsible for the largest attacks seen on the Internet for many years. Before 2013, the largest attacks were typically generated using the DNS protocol and peaked at about 100 Gbps. In 2013 we saw attacks become much larger, such as the DNS reflection/amplification attack targeting Spamhaus at 309 Gbps. Unfortunately, during this survey period attackers have started to more frequently leverage other UDP protocols to magnify their capabilities and achieve their goals—often causing collateral damage along the way. NTP is just one of the protocols that attackers can abuse in this way. In fact, NTP was responsible for the largest attack that ATLAS has ever monitored (325 Gbps), which targeted a destination in France on February 10, 2014.

Reflection/amplification techniques rely on two key factors:

1

Many service providers do not implement ingress anti-spoofing filters at their network edge. This year, for example, only 37 percent of WISR respondents indicated that they have these filters in place.

2

Large populations of poorly configured or secured devices on the Internet offer UDP services where a significant amplification factor between a query and response is possible.

Anatomy of an NTP Reflection Attack

The attacker sends requests to a publicly accessible, improperly secured, UDP-based service from a network that—inappropriately—allows the attacker to modify the source IP address of the request packets. The attacker changes the source IP address to that of the victim. This process is called spoofing, which causes the UDP-based services to return unsolicited "responses" to the victim. Since the attacker can issue large numbers of small queries to numerous servers, and the relatively large responses are returned to the victim, it is easy to overwhelm the bandwidth or other resources available to the victim.

The term **reflection** derives from the fact that the attacker "bounces" the attack off the intermediate servers. This action, when combined with the spoofed source address, serves to disguise the identity of the attacker.

Anatomy of an NTP Reflection Attack

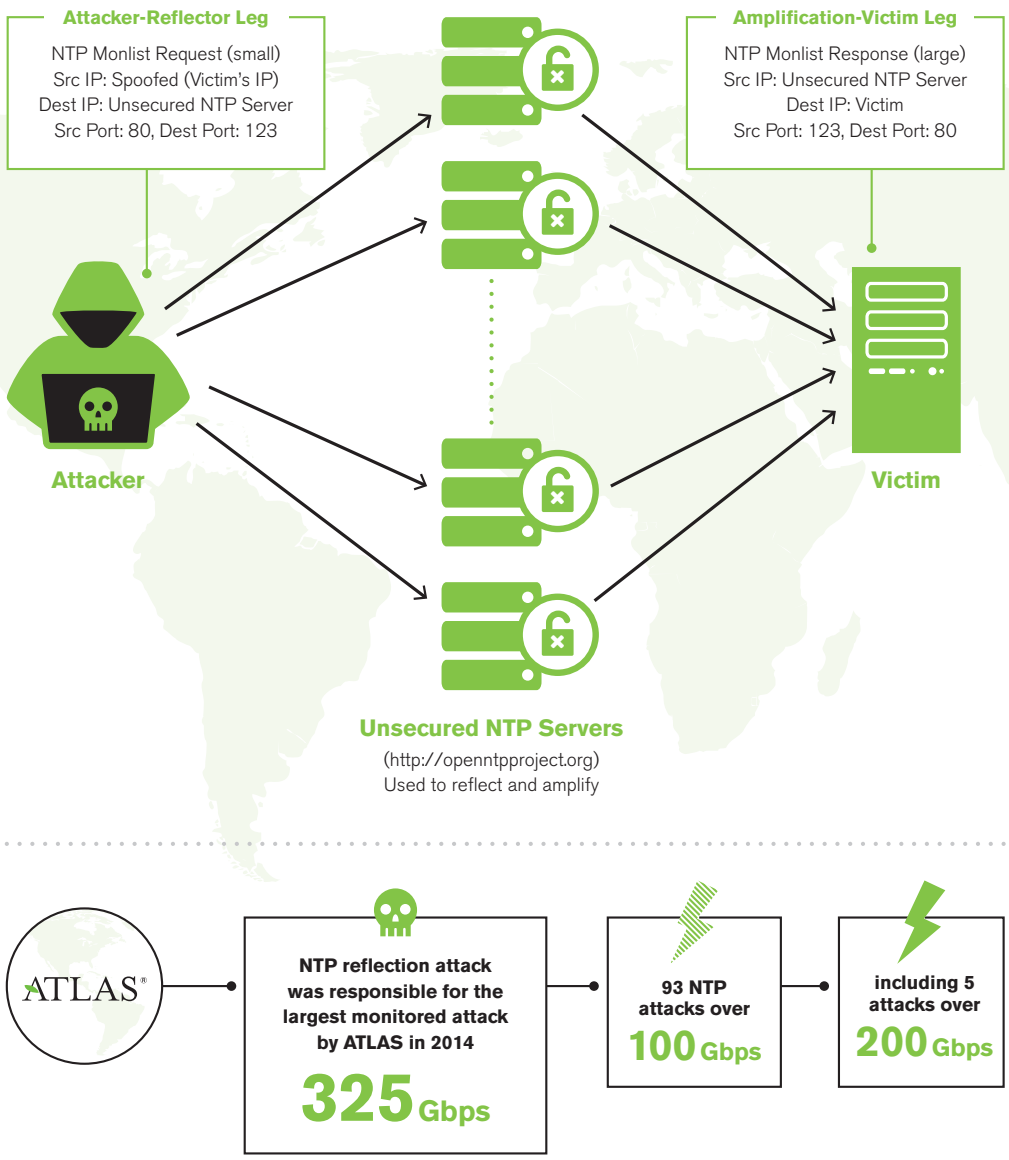


Figure A8 *Source: Arbor Networks, Inc.*

The term **amplification** derives from the fact that the size of the responses can far exceed the size of the original request. For example, the use of the NTP "monlist" command is popular in the recent spate of NTP attacks. When an NTP server receives a small, single-packet monlist request, the server can return a much larger set of information. Figure A9 shows a single monlist query returning the IP address, source port, NTP version and other information for several NTP clients that have recently connected to the NTP server.

Example of NTP Server Monlist Response

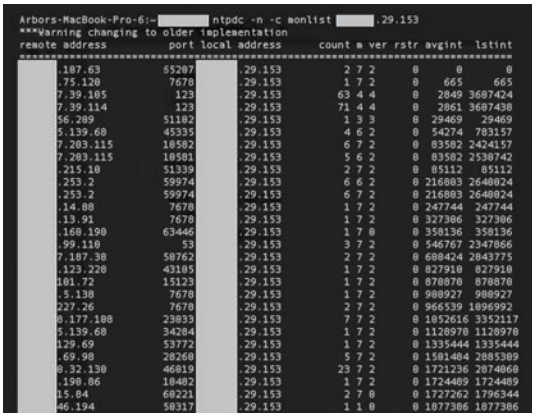


Figure A9 *Source: Arbor Networks, Inc.*

The NTP Storm

The storm of NTP reflection attacks seen during this survey period started in October 2013 and targeted various gaming organizations. The Derp hacker group claimed responsibility for some of these attacks. All of the attacks, as well as subsequent assaults, garnered significant media coverage.

Although the use of NTP as a reflection/amplification attack vector is not new, the publicity around the attacks mentioned above—some of which focused on the attack vector itself—led to widespread adoption within the attacker community. Cybercriminals developed and shared attack tools; built capabilities into botnets; launched DDoS services that offered NTP reflection as an attack option; and made available lists of exploitable servers (please see ASERT Threat Intelligence Brief 2014-5 for more details). These activities led to an explosion in NTP reflection/amplification attack activity.

A look at NTP traffic levels on the Internet during the survey period (Figure A10) clearly illustrates this point. The Arbor ATLAS system tracks data on the traffic crossing the boundaries of the 330+ participating network operators. This graph shows a clear rise in the amount of NTP traffic monitored, with the highest traffic levels recorded in February, March and April 2014 before a decline to a lower level throughout the rest of the year.

ATLAS NTP Traffic Level

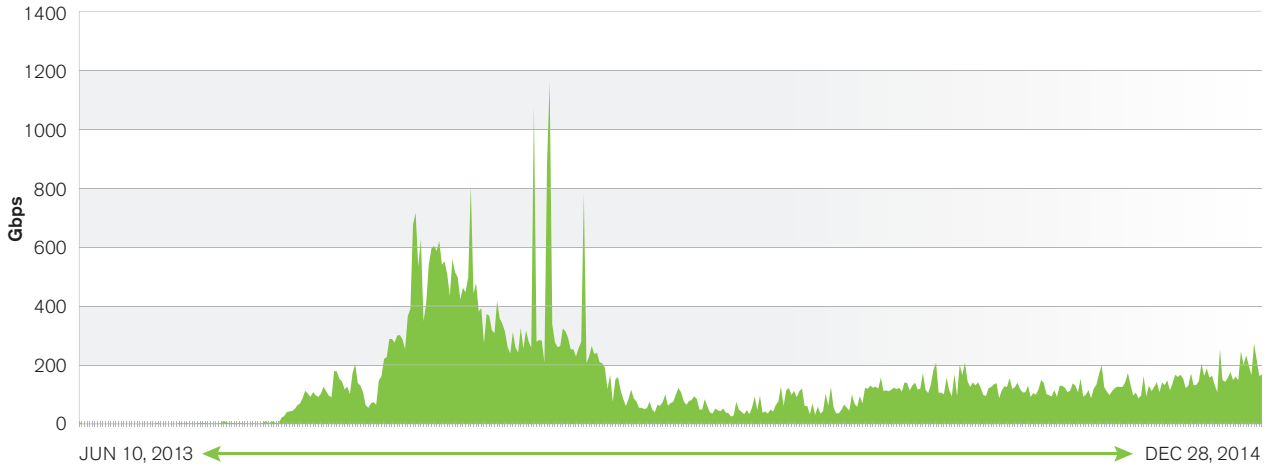


Figure A10 *Source: Arbor Networks, Inc.*

If we consider the October 2013 traffic level as our baseline, prior to the proliferation of NTP attacks, the average NTP traffic monitored for that month was 1.01 Gbps cumulatively across all ATLAS participants. The average for February 2014 was 466.46 Gbps, with March and April showing a gradual decrease (376.65 Gbps and 298.89 Gbps respectively). By October 2014, the level had decreased to an average of around 120 Gbps, but this is still 100x the level monitored in October 2013. This growth is purely due to attack traffic.

As mentioned earlier, NTP reflection was responsible for the largest DDoS attack ever monitored by ATLAS, at 325 Gbps. This year ATLAS has tracked 93 NTP attacks over the 100 Gbps threshold, including five over 200 Gbps. In fact, NTP refection was responsible for a significant proportion of attack activity throughout the year (Figure A11).

ATLAS NTP Attack Proportions

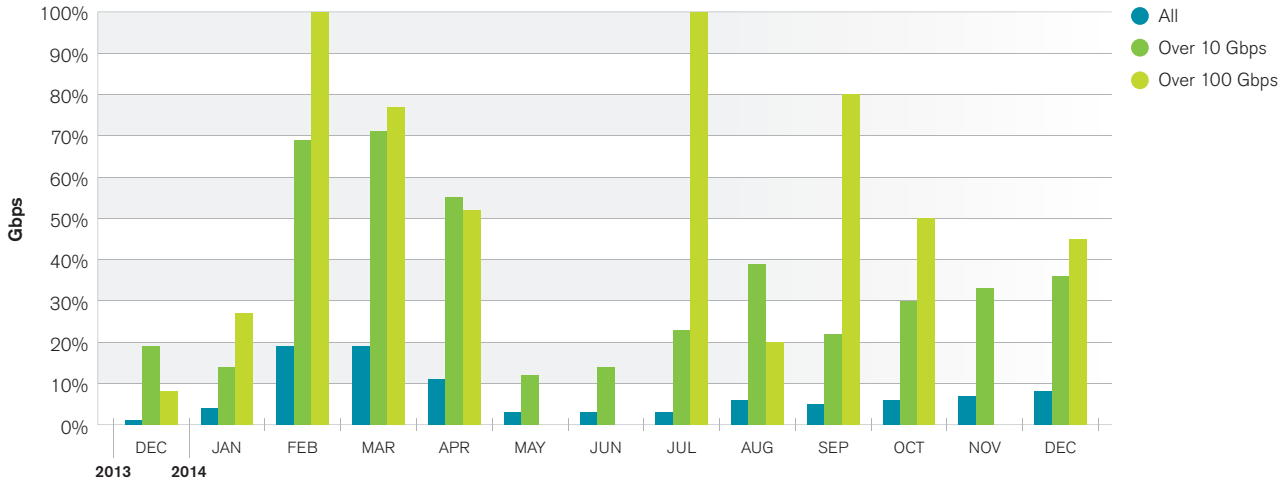


Figure A11 *Source: Arbor Networks, Inc.*

The Rise of SSDP

NTP and DNS are just two of the protocols that attackers can use to amplify their attack traffic; others include Chargen, SSDP, DVMRP and SNMP. Up until this year, DNS had been the most prevalent. But to some degree, cybercriminals have used all of these protocols for many years to launch attacks, it is just their levels of popularity and accessibility that have changed. In early Q3 2014, SSDP gained significantly in prominence, with traffic levels and numbers of attacks blooming. Figure A12 shows the swell of SSDP traffic monitored across ATLAS participants. In June of this year ATLAS monitored almost no SSDP traffic on the Internet. By October 2014, however, the average traffic level had risen to 150.42 Gbps.

ATLAS SSDP Traffic Levels

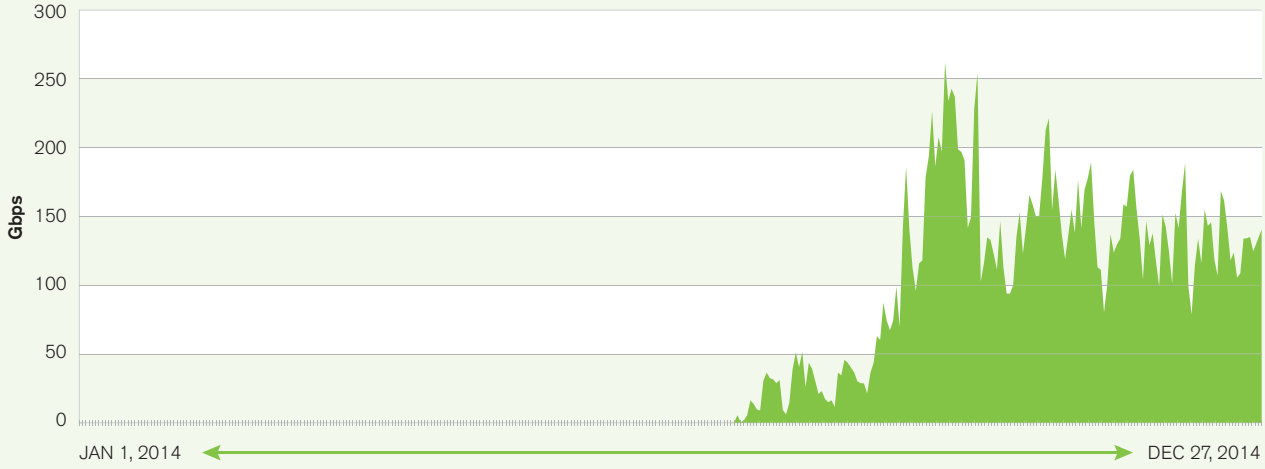


Figure A12 *Source: Arbor Networks, Inc.*

SSDP is primarily used for the discovery and advertisement of network services, and is the basis of the uPnP discovery mechanism. SSDP should only be seen within home and small office networks and NOT on the Internet. However, many home gateway devices incorrectly respond to SSDP queries to their Internet interfaces—creating a significant, exploitable capability within the Internet for attackers to use. Attacks leveraging SSDP as a reflection/amplification mechanism have ramped up quickly, as can be seen above. Prior to July of 2014, ATLAS monitored only a handful of attacks per month. In July this number increased to 241 attacks, and in each of October, November and December 2014 more than 25,000 attacks were monitored. Some SSDP reflection attacks have been large, the biggest so far—recorded at 131 Gbps—occurred in October of 2014 and targeted a Swedish destination. In September and October of 2014, SSDP was responsible for more than a third of the events over 10 Gbps recorded by ATLAS (Figure A13).

ATLAS SSDP Traffic Levels

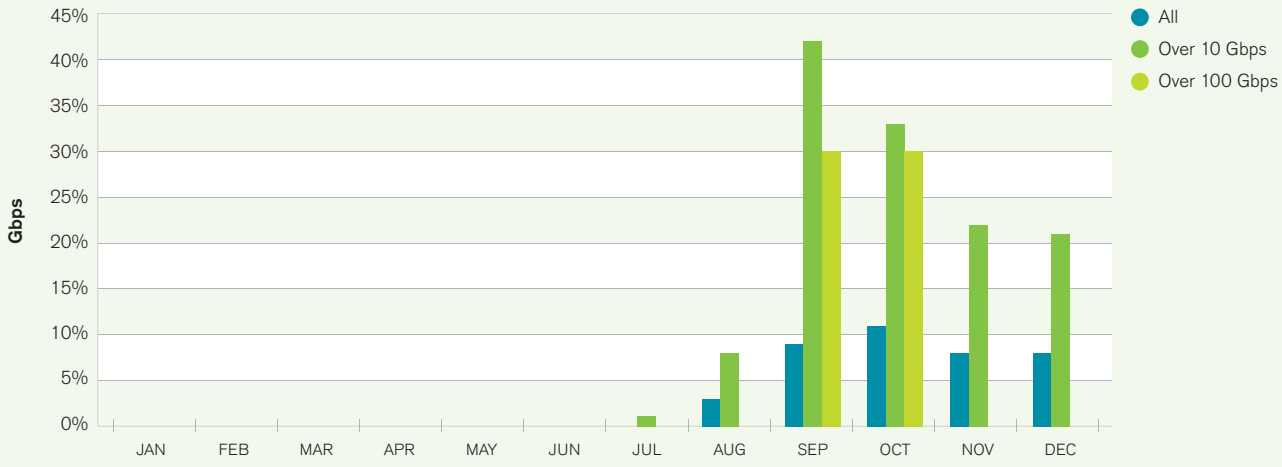


Figure A13 *Source: Arbor Networks, Inc.*

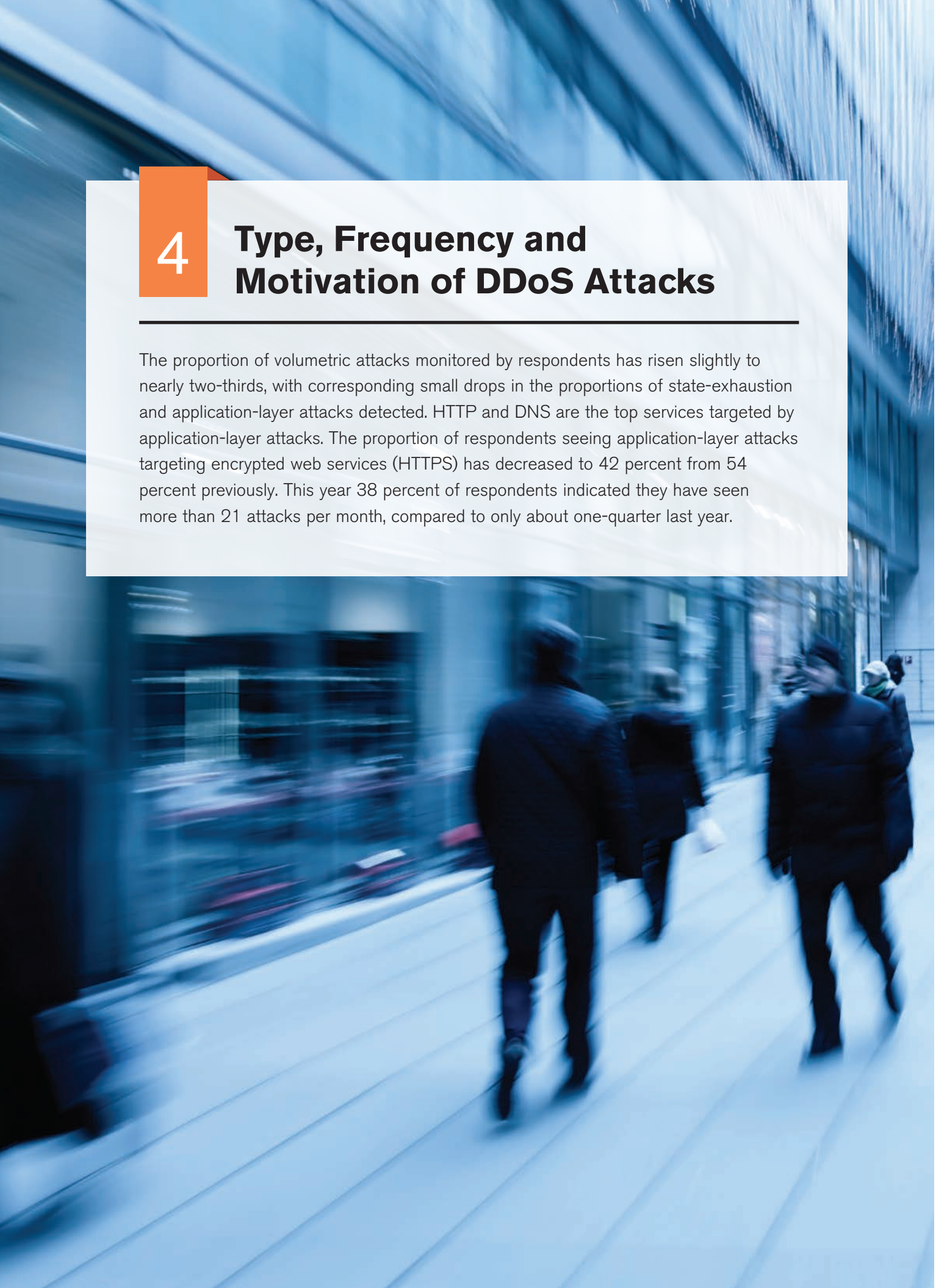
Other Protocols

Although NTP, DNS and SSDP are responsible for significant proportions of reflection/amplification activity in 2014, there are concerns that attackers could exploit other protocols such as Chargen, SNMP and DVMRP even more widely. 2014 has certainly been the busiest year yet for reflection/amplification attacks, both in terms of size and frequency, but 2015 could see these attacks become even larger and more damaging.

Exploited Protocols

Protocol	Overall % Q1	Overall % Q2	Overall % Q3	Overall % Q4	Max Attack
DNS (53)	2%	4%	4%	Less than 1%	104.28 Gbps
NTP (123)	14%	6%	5%	7%	325.05 Gbps
SSDP (1900)	Less than 1%	Less than 1%	4%	9%	131.2 Gbps
SNMP (161)	Less than 1%	Less than 1%	Less than 1%	Less than 1%	18.61 Gbps
Chargen (19)	1%	1%	2%	1%	96.27 Gbps

Table A1 *Source: Arbor Networks, Inc.*



4 Type, Frequency and Motivation of DDoS Attacks

The proportion of volumetric attacks monitored by respondents has risen slightly to nearly two-thirds, with corresponding small drops in the proportions of state-exhaustion and application-layer attacks detected. HTTP and DNS are the top services targeted by application-layer attacks. The proportion of respondents seeing application-layer attacks targeting encrypted web services (HTTPS) has decreased to 42 percent from 54 percent previously. This year 38 percent of respondents indicated they have seen more than 21 attacks per month, compared to only about one-quarter last year.

Now we will move on to look at attack types. DDoS attack vectors vary significantly, and attackers are constantly evolving the methodologies they use to evade defenses and achieve their goals. Attack vectors tend to fall into one of three broad categories:

1

Volumetric Attacks
These attacks attempt to consume the bandwidth either within the target network or service, or between the target network or service and the rest of the Internet. These attacks are simply about causing congestion.

2

TCP State-Exhaustion Attacks
These attacks attempt to consume the connection state tables that are present in many infrastructure components, such as load balancers, firewalls, IPS and the application servers themselves. They can take down even high-capacity devices capable of maintaining state on millions of connections.

3

Application-Layer Attacks
These target some aspect of an application or service at Layer 7. They are the most sophisticated and stealthy attacks because they can be very effective with as few as one attacking machine generating traffic at a low rate. This makes these attacks very difficult to proactively detect with traditional flow-based monitoring solutions. To effectively detect and mitigate this type of attack in real time, it is necessary to deploy an in-line or other packet-based component to your DDoS defense.

Looking at the split of attack types experienced by our survey participants (Figure 19), we can see that volumetric attacks are still the most common type of attack. In last year's report, we highlighted that volumetric attacks had seen a resurgence in 2013. This has continued and escalated in 2014, with more and larger volumetric attacks. This year's results show that the proportion of volumetric attacks has risen slightly to nearly two-thirds, with corresponding small drops in the proportions of state-exhaustion and application-layer attacks. However, it should be noted that while the proportion of more sophisticated application-layer attacks has declined from 24 percent to 20 percent, over 90 percent of this year's respondents said that they have seen some application-layer attacks. This is up from 86 percent last year.

DDoS Attack Types

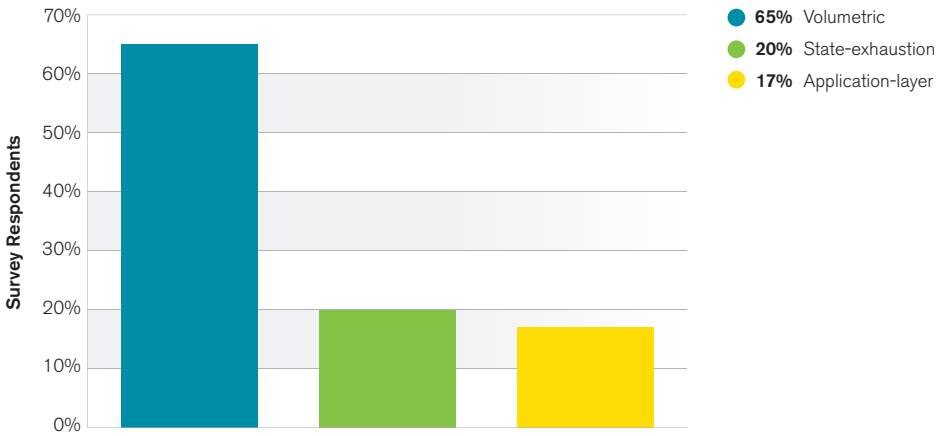


Figure 19 *Source: Arbor Networks, Inc.*

Rather than just using a single attack vector, some attackers direct multiple and different attack techniques at the same time toward a target—making it more difficult for defenses to mitigate the attack. This year we have a slight increase in the proportion of respondents seeing multi-vector attacks on their networks (Figure 20), up to 42 percent from 39 percent last year. As mentioned above, multi-vector attacks are more difficult to deal with, and layered defenses are the best solution. A layered defense lets you proactively deal with more stealthy attacks closer to the target, while the higher magnitude portions of an attack are handled inside the service provider or cloud infrastructure where sufficient capacity is available.

Multi-Vector DDoS Attacks

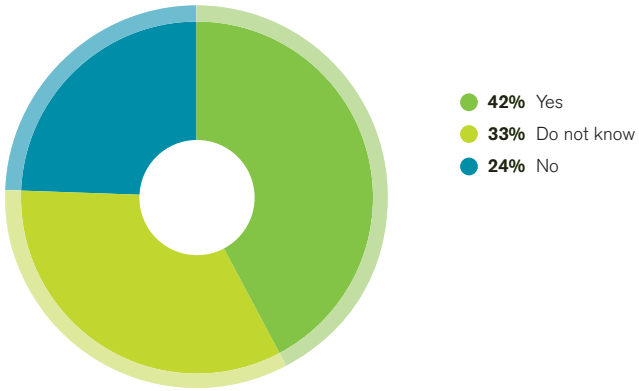


Figure 20 *Source: Arbor Networks, Inc.*

Looking at the services targeted by the more stealthy application-layer attacks (Figure 21) this year, we have two services sharing first place—HTTP and DNS. HTTP has been the top targeted service for the past few years, with DNS gaining ground year over year. Three-quarters of respondents are now seeing application-layer attacks targeting both of these services.

Targets of Application-Layer Attacks

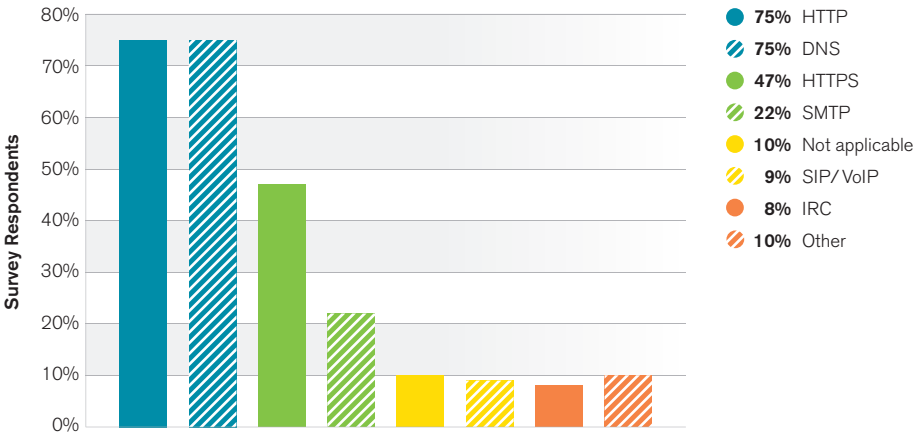


Figure 21 *Source: Arbor Networks, Inc.*

What is especially interesting in these results—and perhaps contrary to general perception—is the decreasing proportion of respondents seeing application-layer attacks targeting encrypted web services (HTTPS). This proportion decreased to 47 percent this year, compared to 54 percent last year (although this is still above the 37 percent seen in 2012). The decrease this year may, to some degree, be due to both the increasing use of reflection/amplification DDoS attacks and the end of the Operation Ababil attack campaign, which generated a lot of attacks targeting encrypted web services. For more details on the services targeted by volumetric attacks, please see the "ATLAS Targeted Services" section of this report.

Looking in more detail at the attacks targeting encrypted services (Figure 22), we can organize them into four different categories:

1. Attacks that target the SSL/TLS negotiation.
2. Attacks that target connection state (number of connections).
3. Volumetric attacks that simply flood traffic at service ports.
4. Application-layer attacks that target the underlying service directly over fully negotiated SSL/TLS connections.

As you can see from this year's survey results, roughly one-fifth of respondents are experiencing attacks in at least one category—but nearly two-thirds do not know what kind of attacks are happening. This latter statistic is a concern, as it may indicate limited visibility and detection for encrypted traffic. Given that these services are often used in financial and e-commerce applications, a successful attack can have significant financial and reputational impact. Deploying the appropriate defense mechanisms is very important.

Types of Attacks Targeting Encrypted Services

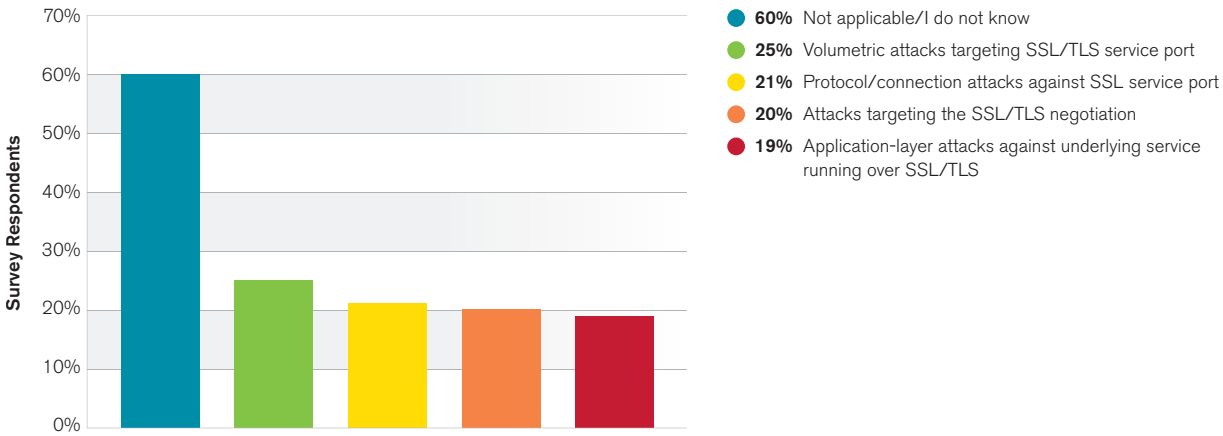


Figure 22 *Source: Arbor Networks, Inc.*

Drilling down into the attack techniques being used to target web services at the application-layer (Figure 23), HTTP GET floods remain the most common attack vector. In fact, the top four attack techniques remain the same as last year in terms of their order. However, the percentage of respondents identifying individual attack techniques has fallen across the board. For example, fewer than 50 percent of respondents identified HTTP GET floods this year, down from 78 percent last year. There is no clear reason for this in the data.

Application-Layer Attack Tools

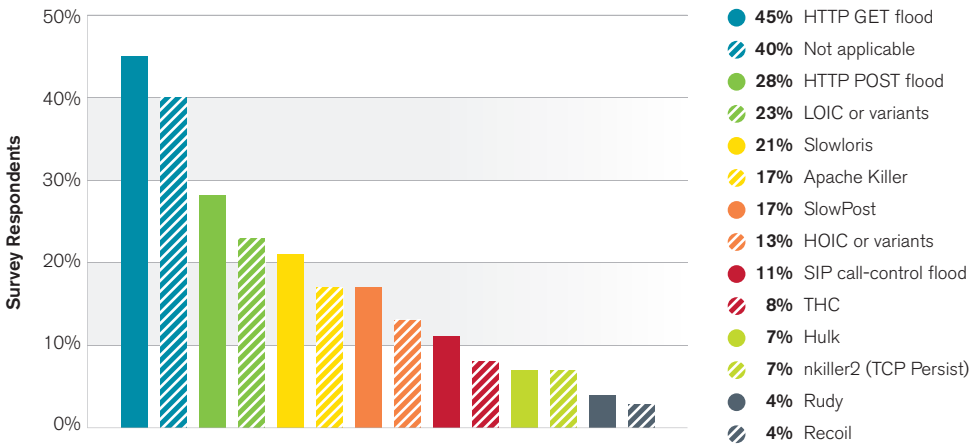


Figure 23 *Source: Arbor Networks, Inc.*

Looking at attack types, we asked whether or not respondents had noted an attack targeting IPv6 services. As in previous iterations of the survey, the proportion of respondents who have witnessed attacks on IPv6 this year is very low—only 2 percent. The size of the largest reported attack on IPv6 is 6 Gbps—just a small fraction of the largest attacks seen targeting IPv4 services.

Moving on to look at attack frequency, the number of attacks experienced per month by our respondents has increased again (Figure 24). Last year just over 25 percent of respondents indicated they have seen more than 21 attacks per month. This year the proportion has risen dramatically to 38 percent. This substantial increase backs up anecdotal feedback from Arbor customers indicating they have seen more attacks during this survey period.

Attack durations are trending shorter. Over half of respondents indicated that the longest duration attack they have monitored over the last year was less than six hours. This proportion has increased from last year, and again ties in with ATLAS data indicating that individual attack durations are decreasing (Figure 25). Please see the "ATLAS Attack Durations" section of this report for more details.

Attack Frequency

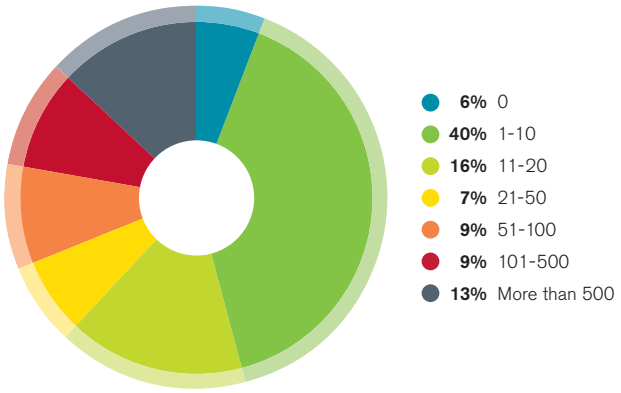


Figure 24 Source: Arbor Networks, Inc.

Longest Attack Duration

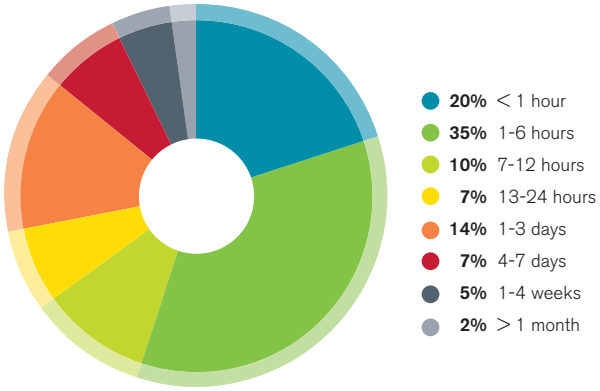


Figure 25 Source: Arbor Networks, Inc.

We also examined perceived attack motivations. We asked respondents what motivations they felt were either commonly or very commonly behind the DDoS attacks they have monitored on their networks (Figure 26). This year the top three motivations are nihilism/vandalism, online gaming and ideological hacktivism—all of which have been in the top three for the past few years. The order and proportions have changed slightly, with nihilism/vandalism and online gaming moving up and ideological hacktivism moving down. It is no surprise that online gaming has moved up as a motivation, as throughout the survey period a significant number of attacks have targeted gaming operators. Please see the "ATLAS: A Time for Reflection" section of this report for further details.

What is interesting is the continued growth in the proportion of respondents who have seen criminal extortion, financial market manipulation or diversion to cover comprise/data exfiltration as common or very common motivations behind DDoS attacks. Last year 15 to 18 percent of respondents selected these motivations, compared to 19 to 20 percent this year. This corresponds with anecdotal information and media coverage about Internet start-up businesses suffering extortion-based DDoS attacks, and with security studies citing DDoS as a method that attackers are increasingly using to distract from other criminal activity.

Attack Motivations

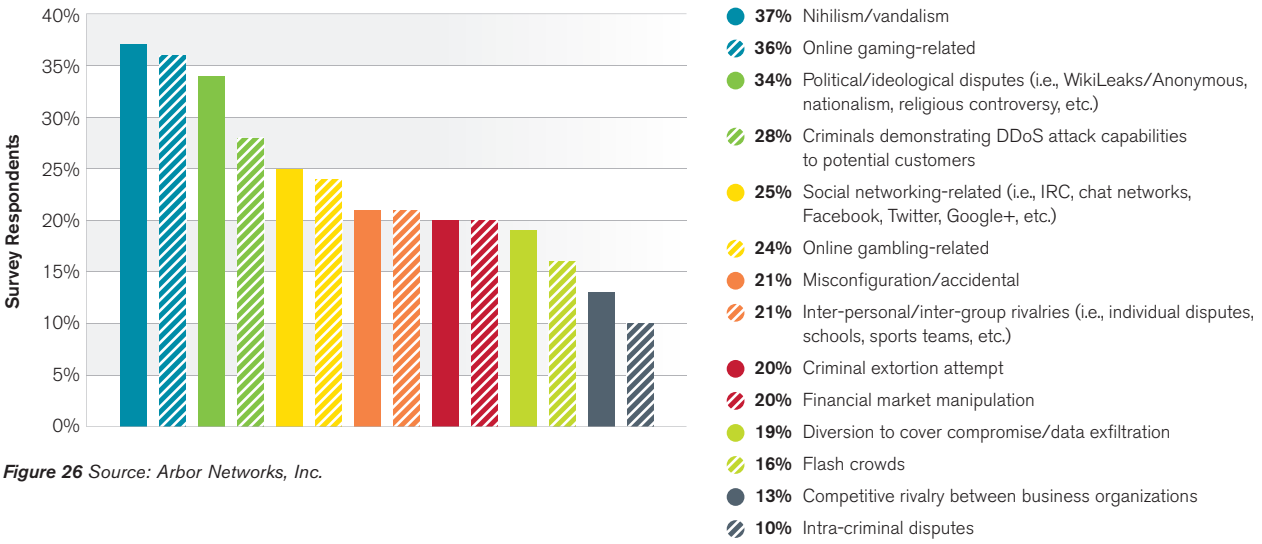


Figure 26 Source: Arbor Networks, Inc.

5 Network, Customer and Service Threat Detection

NetFlow analyzers are the most commonly used threat detection tools, followed by firewall logs. Thirty-five percent of respondents indicated they are already using Layer 7 flow, up from 26 percent last year. NetFlow analyzers are viewed as the most effective way of detecting threats. However, firewall logs—the second most commonly used detection mechanism—rank sixth in terms of effectiveness.

We asked participants which tools they use to detect threats targeting their networks, customers and services (Figure 27). Consistent with last year, NetFlow analyzers are the most commonly used tools, followed by firewall logs. The two had virtually identical percentages to last year. However, there have been some changes. The proportion of respondents using SNMP tools has dropped from 65 percent to 53 percent. IDS/IPS is now the third most commonly used tool—although this increase may be due to improved clarity of answers in the survey options. Interestingly the proportion of respondents using SIEMs has not changed compared to last year, despite ongoing discussion around these solutions within the security industry.

Threat Detection Tools

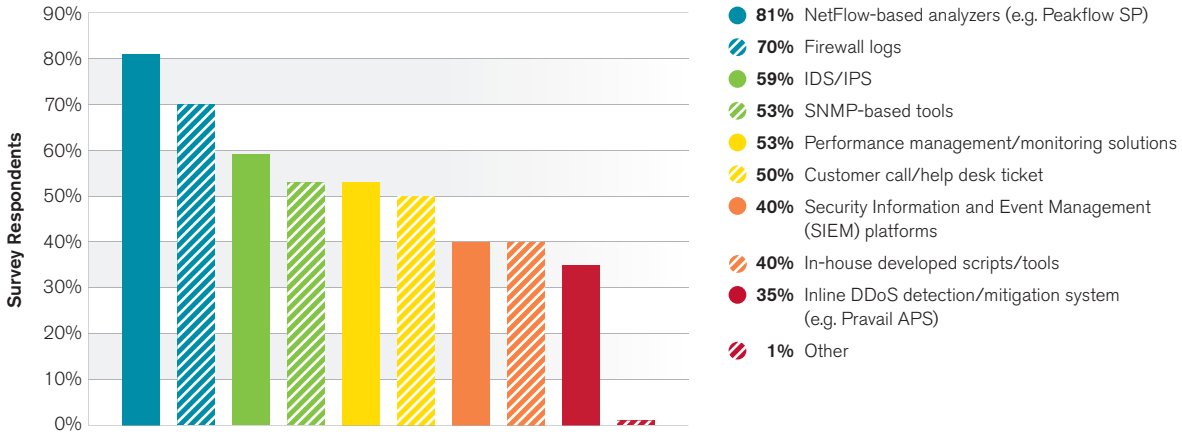


Figure 27 *Source: Arbor Networks, Inc.*

Traditionally, technologies such as NetFlow provide visibility at Layers 3 and 4. However, some router vendors are now starting to provide Layer 7 visibility through proprietary flow extensions and IPFix. These capabilities can extend the broad, cost-effective visibility provided by flow technologies into the application domain. This year 35 percent of respondents indicated they are already using Layer 7 flow, up from 26 percent last year (Figure 28), with a further 37 percent indicating that they would use this capability if their infrastructure supported it. Unfortunately, it is unlikely that core Internet routing infrastructure will support this capability soon.

Layer 7 Flow

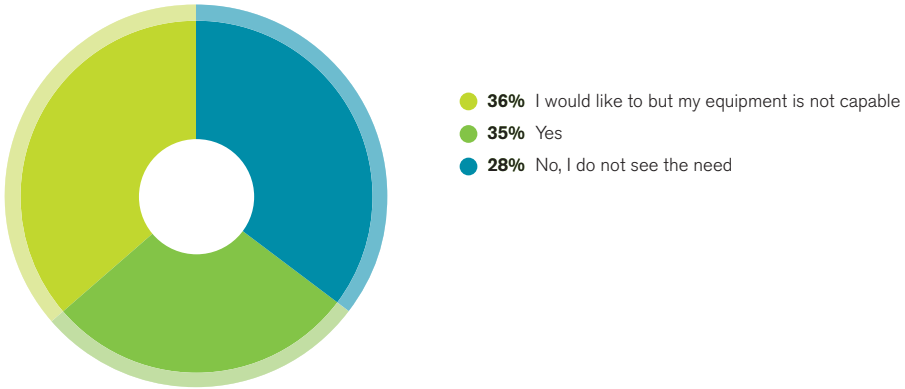


Figure 28 *Source: Arbor Networks, Inc.*

Looking at the effectiveness of deployed threat detection mechanisms (Figure 29), we can clearly see that NetFlow analyzers are viewed as the most effective way of detecting threats, as well as being the most commonly deployed. However, firewall logs—the second most commonly used detection mechanism—rank sixth in terms of effectiveness, down from fourth last year. Also interesting, SIEM solutions are in second to last place in terms of effectiveness, despite their broad industry acceptance.

According to survey results, NetFlow analyzers are clearly viewed as the most effective way of detecting threats, as well as being the most commonly deployed.

Effectiveness of Threat Detection Tools

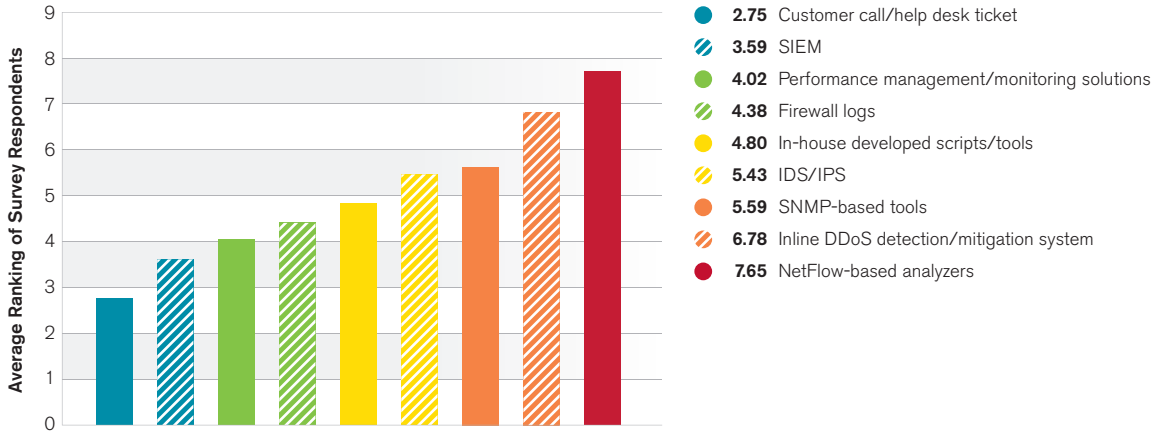


Figure 29 *Source: Arbor Networks, Inc.*

6 Attack Mitigation Techniques

The proportion of respondents using IDMS has moved ahead of those using ACLs for the first time this year, to 70 percent. Also encouraging is the decreasing trend in the use of firewalls to mitigate DDoS events. The proportion of respondents able to mitigate attacks in less than 20 minutes has increased again to 68 percent—up from 60 percent last year. Just under half of respondents indicated that they do NOT detect outbound or cross-bound attacks at all. This is a concern as these attacks can still impact customers or peering and transit capacity. Ideally they should be dealt with in the same way as inbound attacks.

For the first time, more respondents (70 percent) are using IDMS rather than ACLs (Figure 30). The proportion using ACLs has stayed almost the same compared to last year. The increase in IDMS usage represents a very encouraging rise in the application of the surgical mitigation technologies needed to deal with today's DDoS threat.

Attack Mitigation Techniques

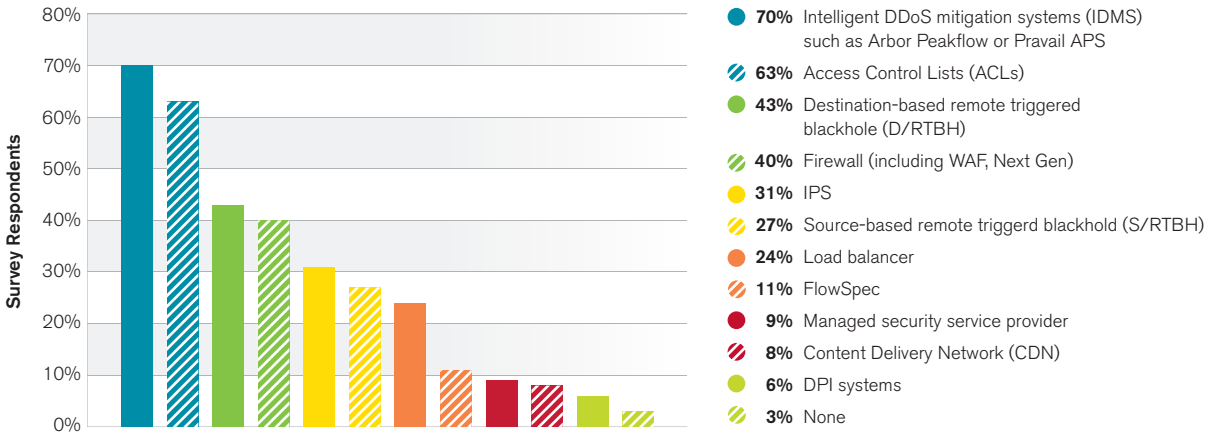


Figure 30 *Source: Arbor Networks, Inc.*

Also encouraging is the decreasing trend in the proportion of respondents using firewalls to mitigate DDoS events. Over the past three years this has dropped from 57 percent to 47 percent and now 40 percent. While firewalls can deal with some DDoS attacks, their capabilities are usually limited and they can be targeted by state-exhaustion attacks—making them a part of the problem. One slightly negative finding is that the use of IPS for DDoS mitigation has increased from 24 percent last year to 31 percent this year. While IPS can deal with some application-layer events via the use of appropriate signatures, these devices suffer from the same state issues as firewalls. As a result, DDoS attacks can target them in the same way.

The proportion of respondents able to mitigate attacks in less than 20 minutes has increased again—to 68 percent this year from 60 percent last year (Figure 31). In last year's report, the increase in this percentage was credited to an increase in the proportion of respondents who mitigated automatically using scripts. This year that percentage has stayed the same—indicating that automation is still working well and that companies have incorporated it into their operational practices. Feedback from many enterprise organizations outside of this survey indicates that they are looking to reduce mitigation delays, given their increased reliance on Internet connectivity. This is a very positive finding.

Time to Mitigate

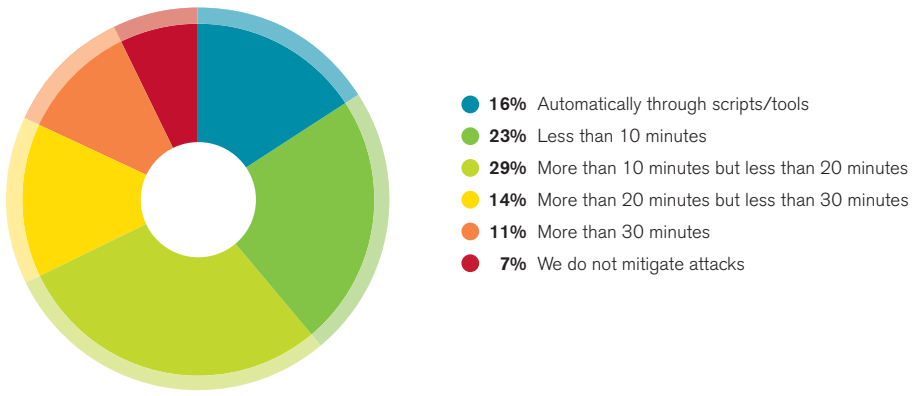


Figure 31 *Source: Arbor Networks, Inc.*

We asked respondents what proportion of the attacks they detected on their networks were outbound or cross-bound. Interestingly, just under half of respondents indicated that they do NOT detect outbound or cross-bound attacks at all, which may indicate a lack of visibility in this area. This is a concern as these attacks can still impact customer aggregation routers, peering and transit capacity. Ideally organizations should detect and deal with outbound and cross-bound attacks in the same way as inbound attacks. For those respondents who do detect outbound or cross-bound attacks, the vast majority report them as less than 10 percent of all events detected on their networks.

Looking at the mitigation of outbound attacks, 40 percent of respondents indicated that they have mitigated an attack—an almost identical result to last year. In terms of mitigating these attacks, ACLs and firewalls are still the most commonly used mechanisms (Figure 32), with almost identical percentages to last year. However, the use of IDMS has increased by five percent to just over one-quarter, which is encouraging.

Outbound Mitigation Mechanisms

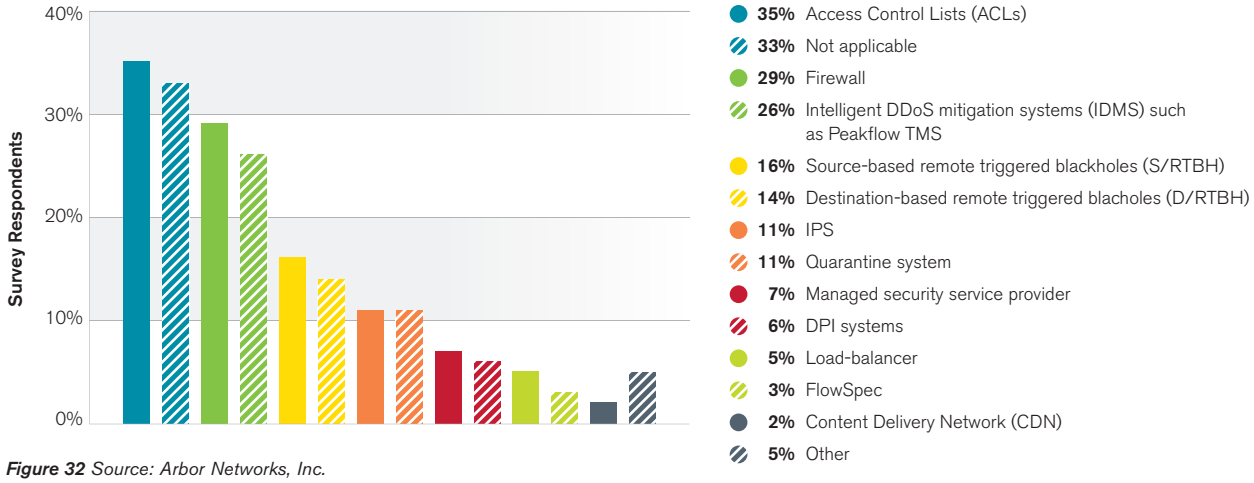


Figure 32 *Source: Arbor Networks, Inc.*

7 Service Provider Corporate Network Threats

By far the most common threat seen in the past year was Internet connectivity congestion due to DDoS attack, with an even greater proportion expressing concern about it in the future. The number of respondents who have experienced advanced persistent threats (APTs) on their corporate network dropped significantly—from 30 percent last year to only 10 percent this year. Over half of respondents saw an increase in incidents on the corporate network, with only 10 percent reporting a decrease. However, just under half say they are at least reasonably prepared with a similar number only somewhat prepared and a further 8 percent completely unprepared. The proportion of respondents allowing employees to use their own devices on internal networks (BYOD) remained relatively static at just under three-quarters. However, 46 percent still do not have any solution deployed to identify these devices—an improvement over last year's 57 percent.

For the first time, this year's survey looked at the incident response capabilities of service provider respondents for events on their corporate networks. The vast majority of respondents do have incident response plans in place, as would be expected, with no respondents reporting that they completely outsource incident response functions to third parties (Figure 33).

Incident Response Posture

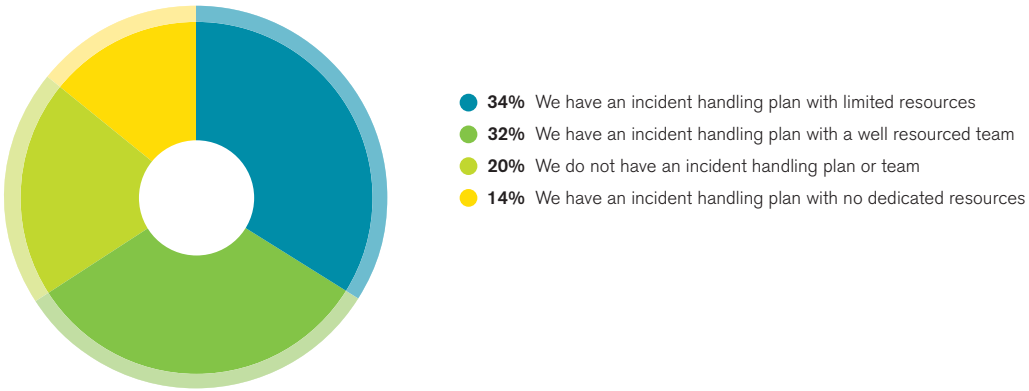


Figure 33 *Source: Arbor Networks, Inc.*

Interestingly only about a third of respondents seem to have contracted with external organizations to assist in incident response (Figure 34). This contradicts other studies done this year, such as the Economist Intelligence Unit (EIU) "Are Business Leaders Ready" report, which Arbor sponsored, where just under three-quarters of research participants reported having external support in place. However, the EIU report did focus on enterprise organizations. The enterprise section of this report (new this year) also shows that a higher percentage of organizations utilize external support than is noted here.

The most common types of organizations contracted by service provider respondents for incident response assistance are IT forensic experts or other specialist IT providers; regulators; and police or other law enforcement.

Incident Response Assistance

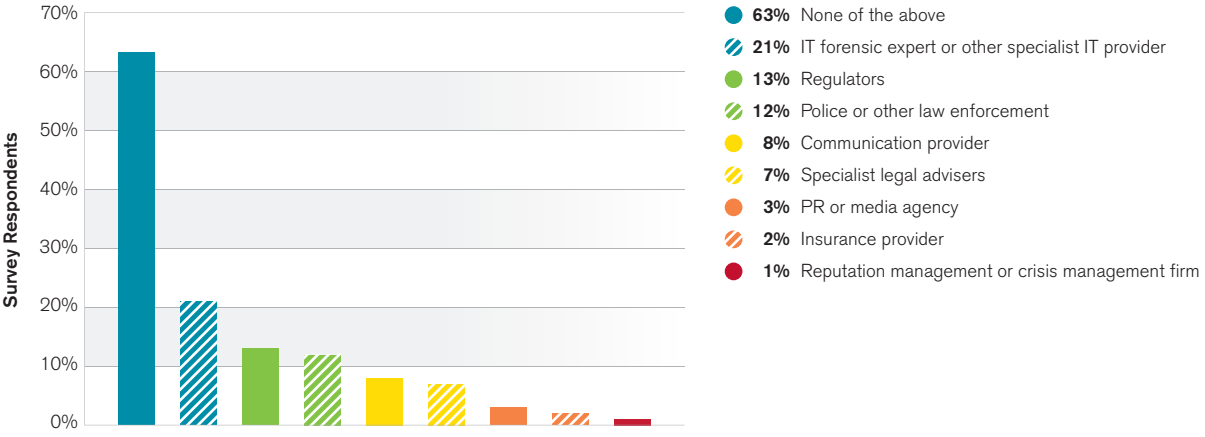


Figure 34 *Source: Arbor Networks, Inc.*

The most commonly observed threat experienced on corporate networks is Internet connectivity congestion due to DDoS attack (Figure 35), reported by over half of respondents. Other widely reported threats include botted or otherwise compromised hosts on the corporate network; Internet connectivity congestion due to genuine traffic growth/spike; and accidental major service outage.

Interestingly, the proportion of respondents who have experienced advanced persistent threats (APTs) on their corporate network dropped significantly, from 30 percent last year to only 10 percent this year. However, regardless of this decline in reported APT infections, just over a third of respondents still expressed concern about APT infection during the coming year. The recent data exfiltration of Sony Entertainment happened after this survey was concluded, so these categories are likely trending as higher concerns now.

Internal Network Security Threats

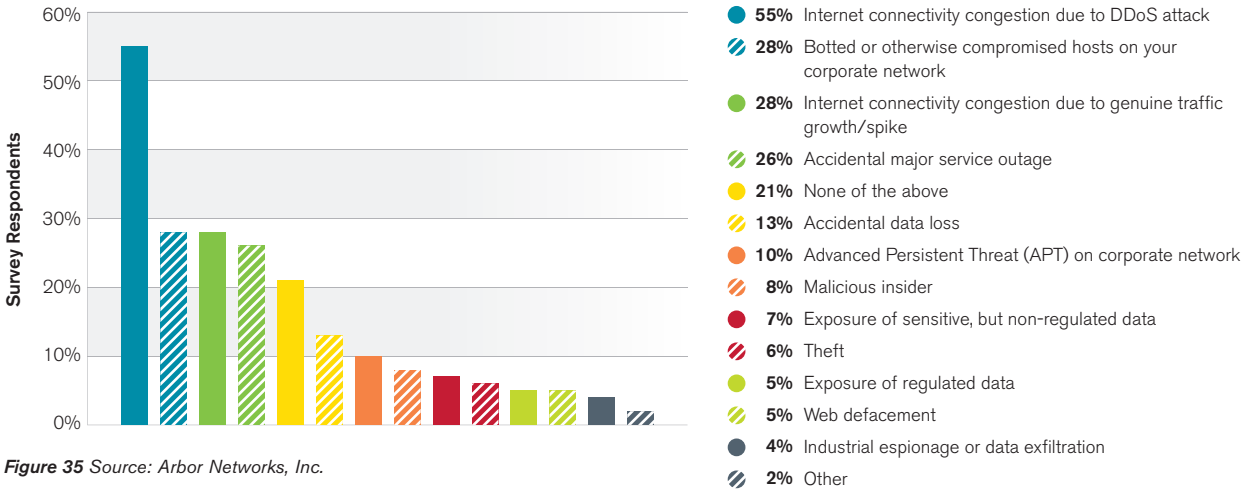


Figure 35 *Source: Arbor Networks, Inc.*

Looking ahead to 2015, the number one concern is overwhelmingly Internet connectivity congestion due to DDoS attack (Figure 36). Additional top concerns include accidental major service outage; botted or otherwise compromised hosts on the corporate network; Internet connectivity congestion due to genuine traffic growth/spike; and exposure of sensitive, but non-regulated data.

Internal Network Security Concerns

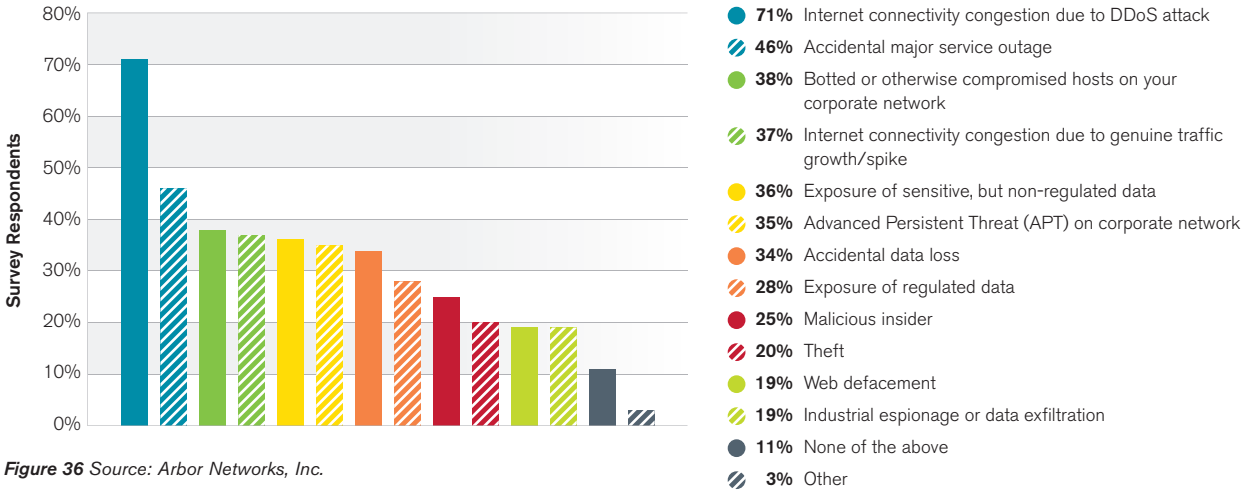


Figure 36 *Source: Arbor Networks, Inc.*

Looking at the threats experienced during the survey period and the concerns for next year, DDoS clearly looms the largest. The increasing frequency, scale and complexity of DDoS attacks are taking their toll, even on service provider corporate networks. While the potential for data loss may represent a bigger risk, it is hard to ignore the ever-increasing threat of DDoS.

We attempted to capture some metrics within the survey around incident response times (Table 1). Overall most organizations reported fairly impressive response times.

Incident Response Time

	Minimum	Maximum	Average
Time from compromise to discovery	1 second	1 month	3 days
Time from discovery to Internal reporting	1 second	1 week	1 hour
Time from reporting to resolution	10 minutes	1 month	1 day
Time from discovery to notification (where applicable)	1 second	1 week	3 hours

Table 1 *Source: Arbor Networks, Inc.*

Looking at the frequency of incidents on internal networks, over 50 percent of respondents indicated an increase over last year (Figure 37). Only 10 percent reported a decrease in incidents. This is a dramatic rise in the rate of internal network incidents and appears even more significant when compared with the results from enterprise, education and government respondents, which show only 34 percent of respondents seeing an increase in incident frequency.

Rate of Internal Network Incidents

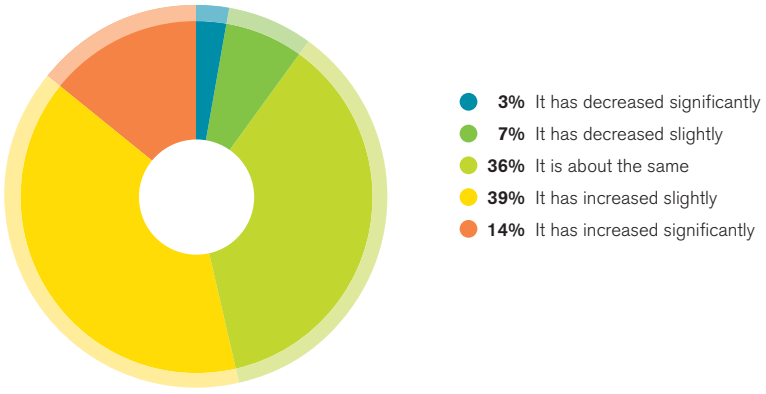


Figure 37 *Source: Arbor Networks, Inc.*

Nearly all organizations indicated at least some level of incident response preparedness (Figure 38). However, 42 percent said they are only "somewhat" prepared and need to improve, while a further 8 percent feel completely unprepared, indicating that it would take a major event to change their posture. This is concerning as a breach in a service provider corporate network could have wide-reaching implications for both service delivery and customer data privacy.

Incident Response Preparedness

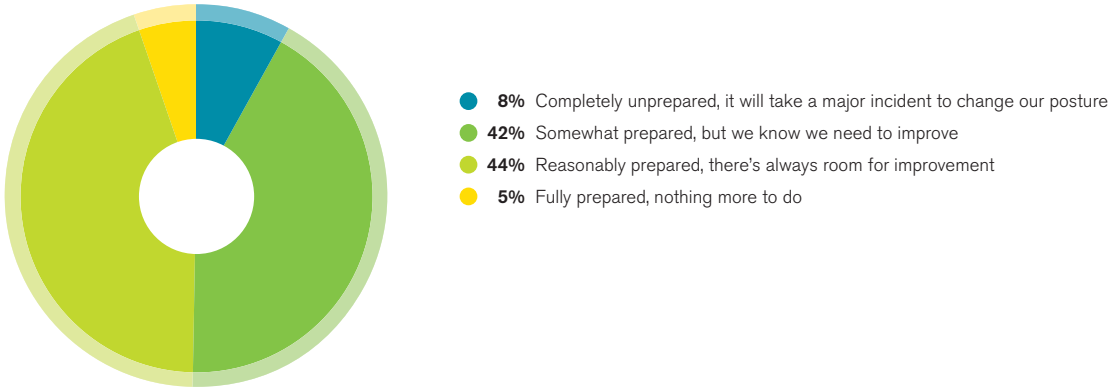


Figure 38 *Source: Arbor Networks, Inc.*

Looking at the various ways in which organizations want to improve incident response, the most popular is deploying more automated threat detection solutions (Figure 39), which was indicated by just under two-thirds of respondents. It is followed closely by reviewing and exercising incident handling plans more frequently; raising awareness of existing plans/preparations across the company; getting regular updates and intelligence on the potential threats to the company; and deploying solutions that speed up the incident response process—all of which garnered more than half of responses. These service provider results are nearly identical to those of their enterprise, government and education counterparts (Figure 84).

Incident Response Improvements

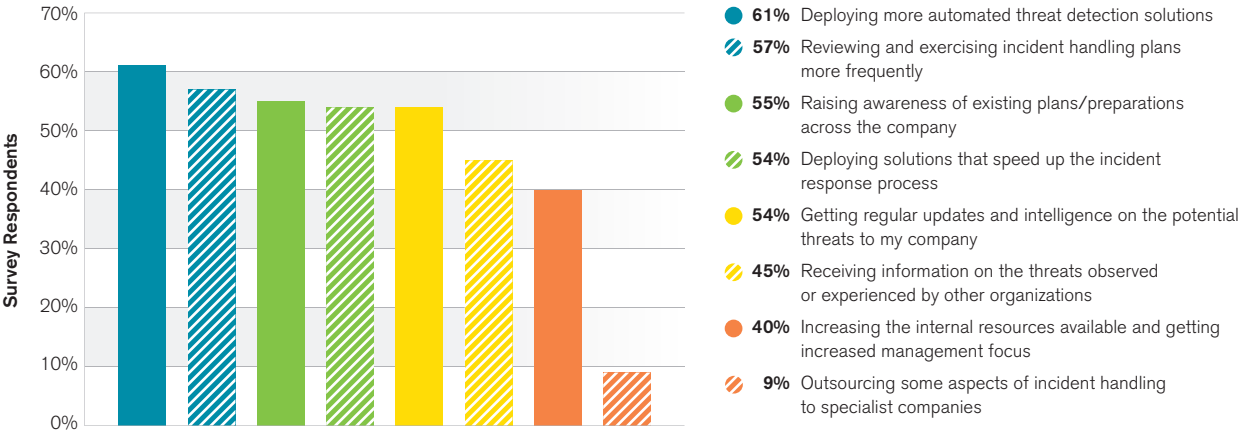


Figure 39 *Source: Arbor Networks, Inc.*

Within corporate networks, NetFlow analyzers and firewalls/IPS/UTP systems continue to represent the most common threat detection mechanisms (Figure 40). While these are the very clear leaders, with over 70 percent adoption rates, several other mechanisms are also widely deployed. In third place at a surprising 44 percent this year are help-desk calls. SIEMs, performance management/monitoring solutions and in-house-developed scripts/tools also came in around the 40 percent mark. This indicates that many organizations have multiple layers of threat detection in place, which is encouraging.

Internal Network Threat Detection Mechanisms

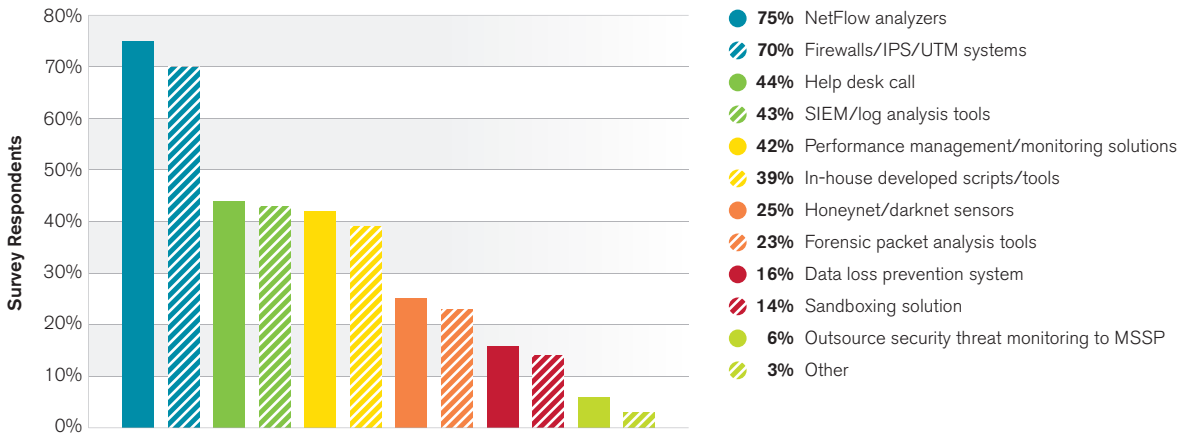


Figure 40 *Source: Arbor Networks, Inc.*

To look at the effectiveness of deployed threat detection tools, we asked our respondents how they have detected events in the past. Surprisingly the top response—reported by 62 percent—is manual detection by employees. However, automated detection using deployed security tools came in a very close second at 60 percent. Other common answers include detection via routine checks and controls, and notification by customer or media. It is telling that the automated tools we have deployed are not catching so many real-world detections. This shows that security vendors still have much room to improve.

Actual Detection Methods and Sources

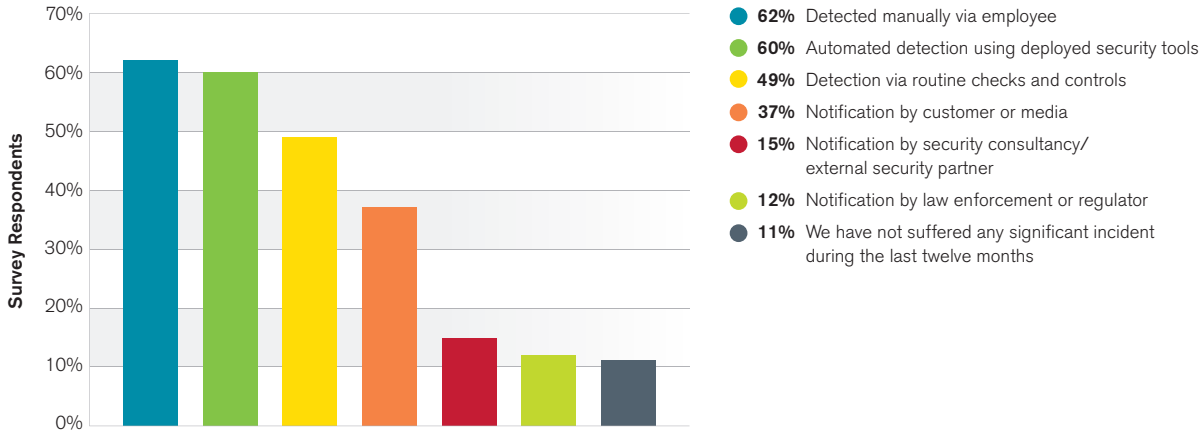


Figure 41 *Source: Arbor Networks, Inc.*

For the first time, this year's survey asked about the nascent practice of employing cyber security insurance. A slim majority of respondents are unaware of their organization's posture (Figure 42), but nearly one-quarter indicated they either already have a policy in place or plan to in the coming year. This is a higher percentage than expected based on data from the EIU report cited earlier in this report, and may indicate increased implementation of these policies across a broader set or regions and organizations.

Incident Response

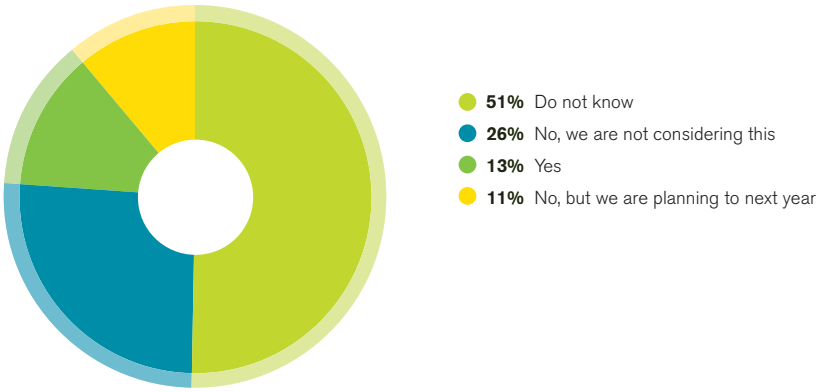


Figure 42 *Source: Arbor Networks, Inc.*

In regards to social media, nearly three-quarters of organizations allow its use on their internal networks (Figure 43), but less than half allow instant messaging. These numbers have fallen modestly when compared with last year's results. Only 10 percent of respondents indicated that they actively block these applications.

Social Media on Internal Networks

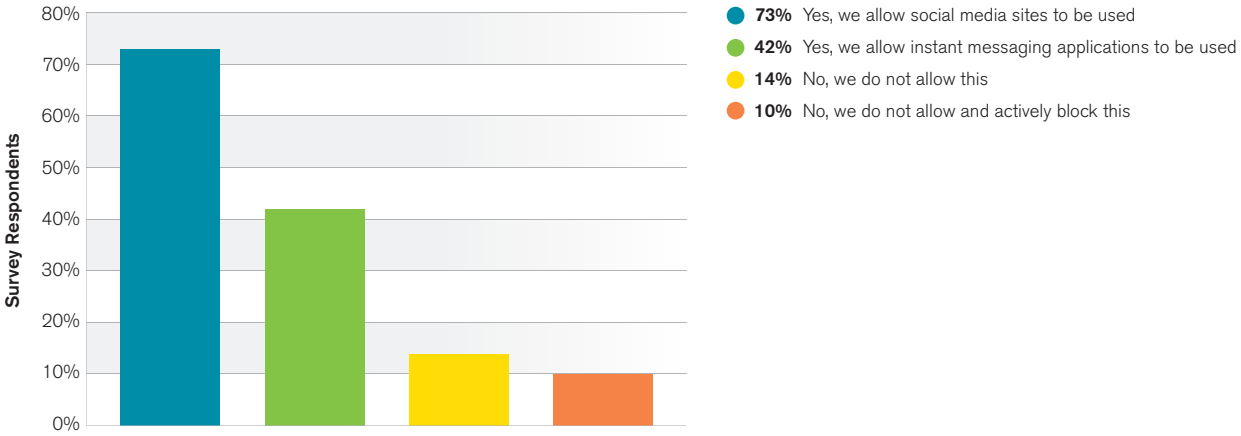


Figure 43 *Source: Arbor Networks, Inc.*

People are often the weakest link in an organization's security posture, and social engineering can be an effective way for attackers to gain a foothold. Organizations should ensure that their staff is educated as to the risks associated with sharing personal or occupational information.

The percentage of organizations allowing the use of personal devices (BYOD) on their internal networks remained virtually unchanged this year at just under three-quarters of respondents, a mere 1 percent increase over last year.

To control the use of employee-owned devices appropriately, organizations should be able to identify these devices on their networks. This year saw modest gains in the visibility of these devices. It should be noted, however, that 46 percent of survey respondents do not have ANY solution deployed to identify these devices (Figure 44). But this is down from 57 percent last year, which is a positive trend. For those who do have mechanisms in place, the two most popular solutions are network access control and identity management systems, consistent with last year. The reported use of network-based posture assessment doubled this year to tie for third place at 22 percent.

Identification of Employee-Owned Devices

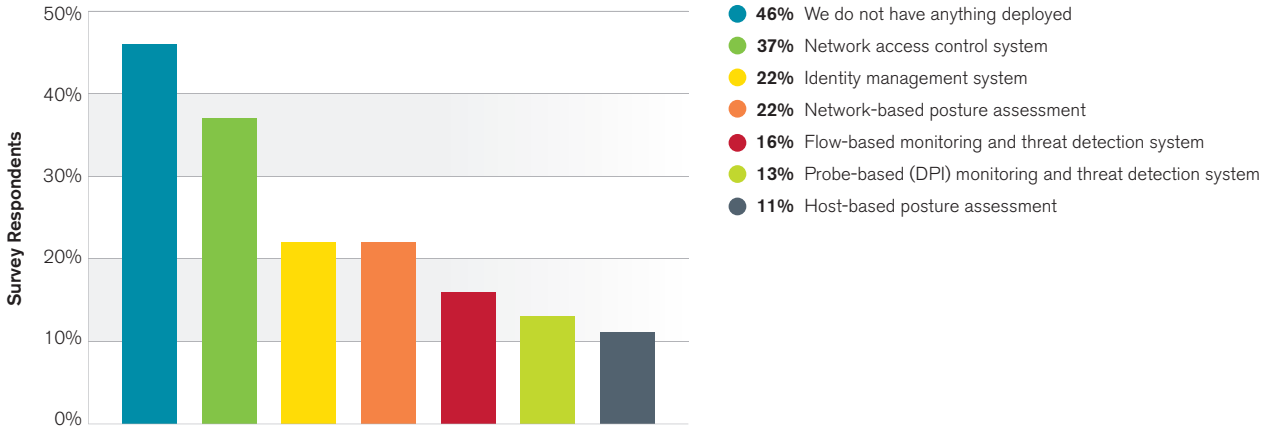


Figure 44 *Source: Arbor Networks, Inc.*

Because employee-owned devices are not managed or controlled by an employee's organization, it is best practice to place some restrictions on their activities and access within the corporate network. This year saw a modest increase in limiting access to internal resources, up 2 percent over last year's 60 percent (Figure 45). The most promising change, however, is the increased use of mobile device management (MDM) to 26 percent of respondents, up from 19 percent last year. The use of security software installed on employee-owned devices also saw a nice boost, up from 16 percent last year to 23 percent this year. The one decline we saw in BYOD restrictions is the use of specific security policies, which dropped to 55 percent of respondents from 66 percent last year. We can only hope the increases in other areas obviated the need for some of those policies.

BYOD Access Restrictions

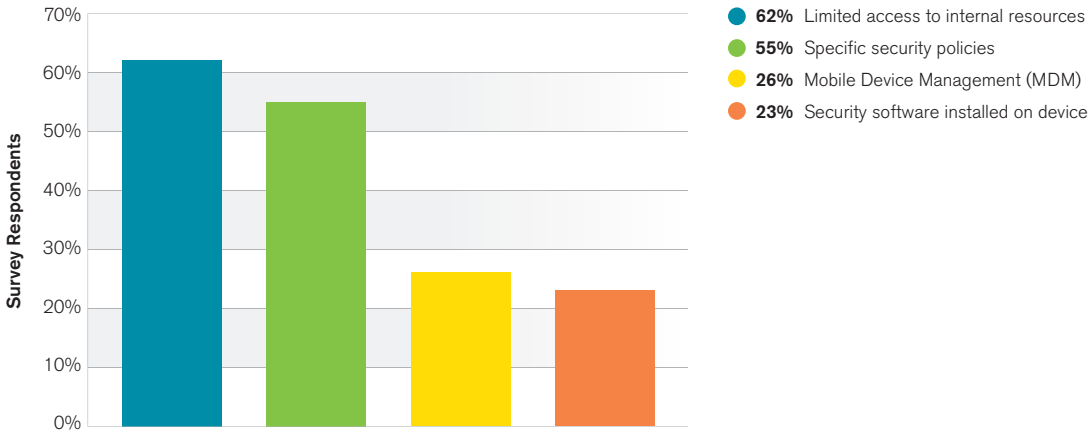


Figure 45 *Source: Arbor Networks, Inc.*

When it comes to using public cloud services to synchronize or back up employee-owned devices, 66 percent of respondents do not allow this—up slightly from last year's 60 percent. This demonstrates the growing concerns that companies have in the use of cloud services as a means of managing information and in the security controls that cloud services have in place.

Certainly there can be risks in allowing BYOD on a corporate network, but fortunately only 5 percent of respondents experienced a security breach that they could attribute to BYOD during the survey period (Figure 46). Interestingly though, in a slight increase over last year, 41 percent of respondents indicated they still do not know if they had a security breach due to BYOD. This is not surprising given the continued lack of visibility of employee-owned devices in some organizations.

BYOD Security Breach

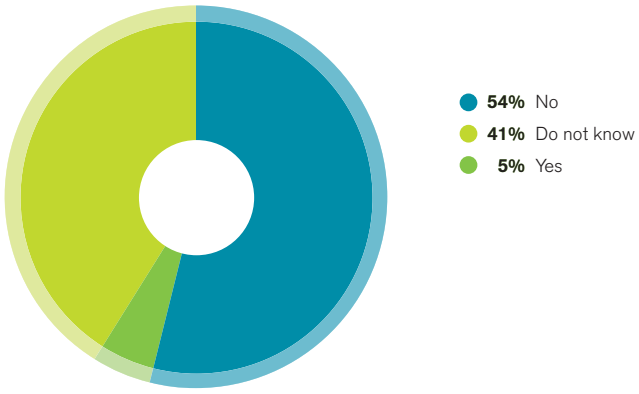
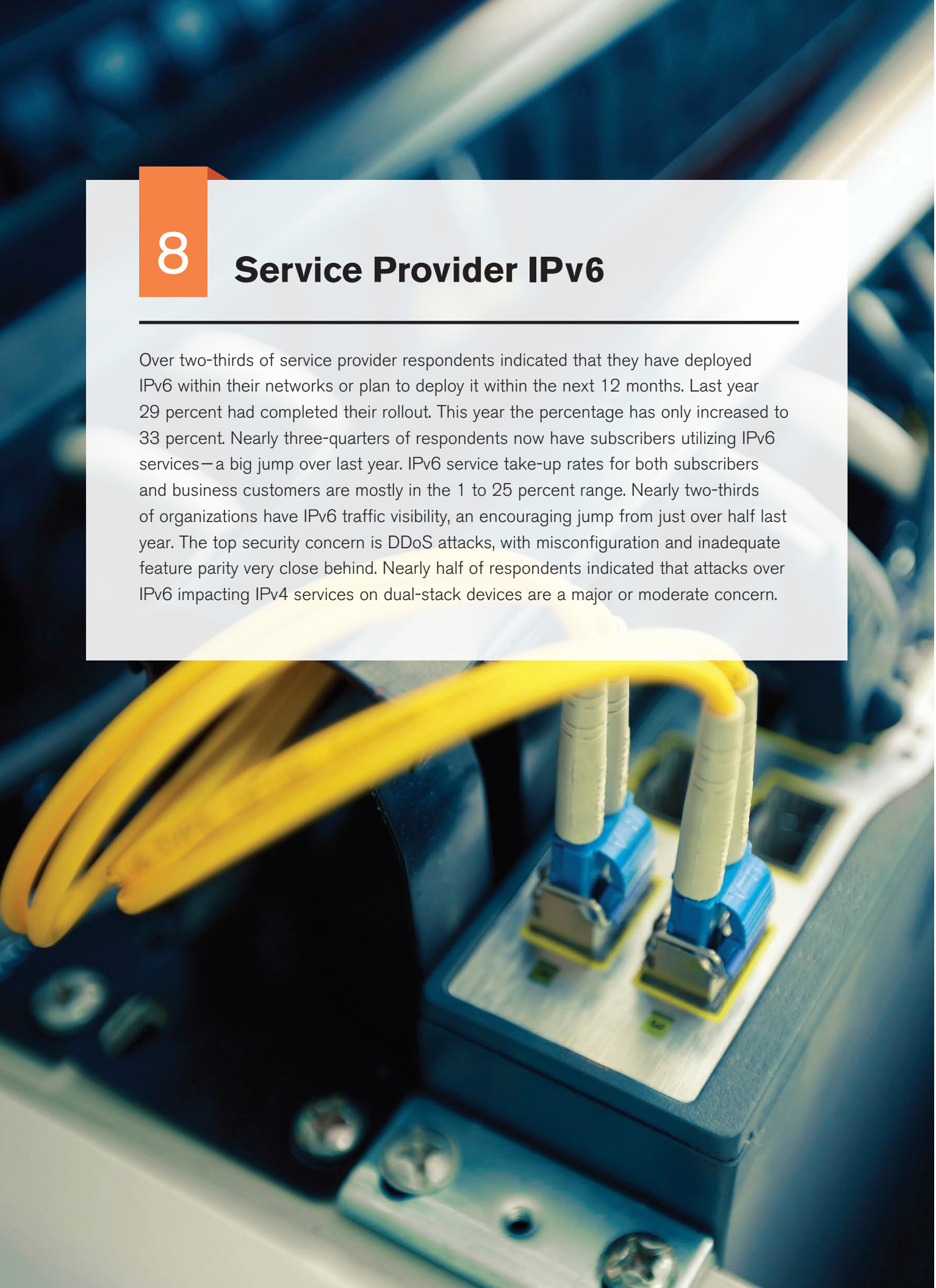


Figure 46 *Source: Arbor Networks, Inc.*



8 Service Provider IPv6

Over two-thirds of service provider respondents indicated that they have deployed IPv6 within their networks or plan to deploy it within the next 12 months. Last year 29 percent had completed their rollout. This year the percentage has only increased to 33 percent. Nearly three-quarters of respondents now have subscribers utilizing IPv6 services—a big jump over last year. IPv6 service take-up rates for both subscribers and business customers are mostly in the 1 to 25 percent range. Nearly two-thirds of organizations have IPv6 traffic visibility, an encouraging jump from just over half last year. The top security concern is DDoS attacks, with misconfiguration and inadequate feature parity very close behind. Nearly half of respondents indicated that attacks over IPv6 impacting IPv4 services on dual-stack devices are a major or moderate concern.

Last year 60 percent of survey respondents reported that they either had IPv6 deployed or had plans to deploy it within the coming year. However, this statistic included responses from both service provider and enterprise organizations. This year's survey included separate sections for service providers and for enterprise, government and education respondents.

This year 68 percent of service providers indicated that they have deployed IPv6 within their networks or plan to deploy it within the next 12 months. In 2012, 80 percent of respondents indicated that they had IPv6 deployed, and the fall to 60 percent in last year's results is likely due to increased enterprise participation. It is interesting to note that in this service provider-only section, we have not returned to the 2012 level. This potentially indicates that the spread of IPv6, given the increased number of service provider participants, is not as broad as it could be. If we combine all the respondents to the IPv6 questionnaire sections (both enterprise and service provider), fewer than 50 percent of the respondents have deployed or plan to deploy IPv6 in the next 12 months.

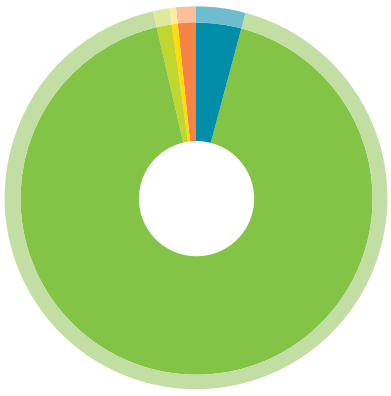
This is confirmed when we look at the proportion of service providers who have their IPv6 deployments completed. Last year 29 percent had completed their rollout. This year the percentage has only increased to 33 percent, with roughly the same percentage indicating that their deployment is still ongoing.

In a similar result to last year, 44 percent of respondents indicated that IPv4 address availability may become an issue for them in the next 12 months. It is interesting to note that this percentage has not changed much this year. Arbor Networks has collaborated with several other organizations—including the University of Michigan, the International Computer Science Institute, Verisign Labs and the University of Illinois—on the subject of IPv6 adoption. For more information, please see the "Measuring IPv6 Adoption" section of this report.

We have seen a big increase in the proportion of respondents who have subscribers utilizing IPv6 services. In 2013 and 2012, 53 and 48 percent respectively had subscribers using these services. This year 68 percent have subscribers using IPv6—an increase of over 20 percent (Figure 47). Where respondents have subscribers using these services, over half indicated that the take-up rate is between 1 and 25 percent, with less than 10 percent seeing take-up rates of between 76 and 100 percent.

The percentage of respondents who have subscribers using IPv6 is now much more comparable to the percentage who cater to business users. This year 88 percent of respondents have business users utilizing IPv6 services—up from just under three-quarters last year (Figure 48). The take-up rates for business customers, however, are actually lower than for subscribers, with 75 percent of respondents indicating that between 1 and 25 percent of their business customers make use of IPv6 services.

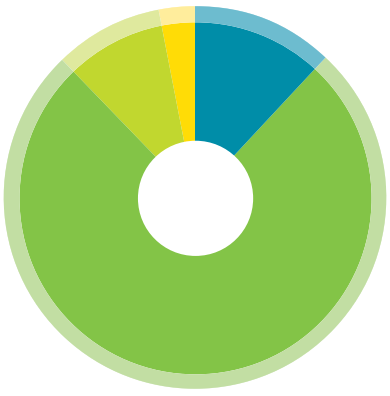
Subscriber IPv6 Usage



- **26%** None, we do not offer IPv6 services to end-users
- **53%** 1-25
- **9%** 26-50
- **3%** 51-75
- **9%** 76-100

Figure 47 *Source: Arbor Networks, Inc.*

Business Customer IPv6 Service Usage



- **12%** None, we do not offer IPv6 service to business customers
- **75%** 1-24
- **9%** 26-50
- **3%** 76-100

Figure 48 *Source: Arbor Networks, Inc.*

Given the higher proportion of respondents seeing their subscribers and business customers utilizing IPv6 services, visibility becomes hugely important. Sixty-four percent of organizations have IPv6 traffic visibility, an encouraging jump from 48 percent last year.

Flow telemetry is a cost-effective technology for gaining broad traffic visibility. Nearly half of respondents have network infrastructure that fully supports IPv6 flow telemetry—up from one-third last year (Figure 49). Interestingly though, the combined percentage that have either full or partial support is identical year over year.

IPv6 Flow Telemetry

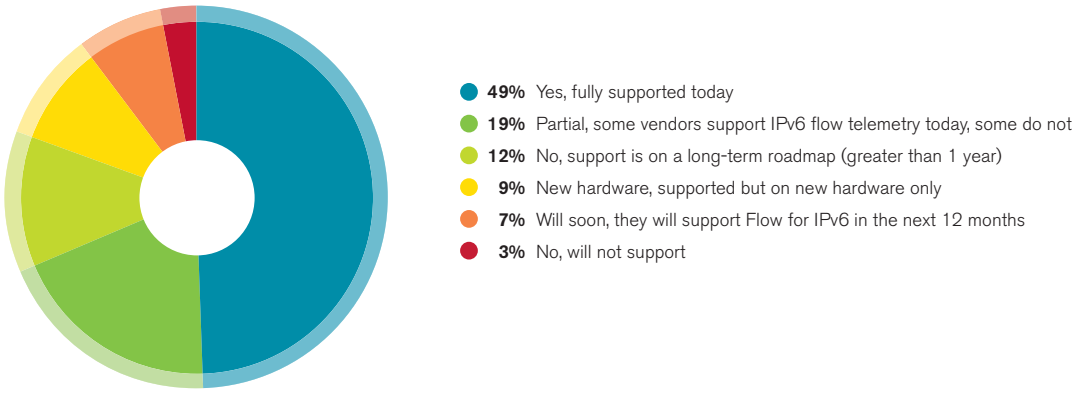


Figure 49 *Source: Arbor Networks, Inc.*

The peak daily rate of IPv6 traffic on respondent networks continues to grow rapidly. Last year the highest reported traffic rate was 20 Gbps—a significant increase over 2012, when 3 Gbps was the highest reported volume. This year the highest reported volume is 80 Gbps, a massive increase over last year, with multiple respondents indicating peak rates above the 30 Gbps level. IPv6 traffic is growing, but how fast? In 2013 ATLAS-monitored IPv6 traffic volumes grew around tenfold. However, the vast majority of respondents only expect IPv6 traffic to grow by less than 60 percent this year. The actual ATLAS-monitored IPv6 traffic levels for 2014 can be seen in the "ATLAS IPv6" section of this report.

Growth predictions are broadly the same as last year, with the vast majority indicating 60 percent or lower growth expectations (Figure 50). It is interesting that expected growth and actual growth rates remain quite distinct.

IPv6 Traffic Growth

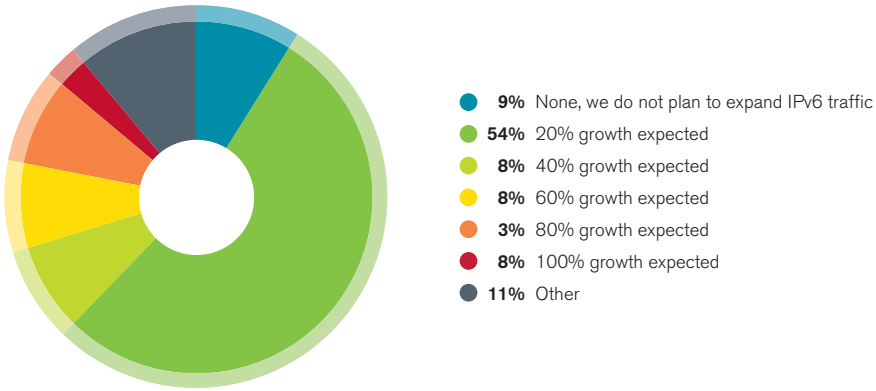


Figure 50 *Source: Arbor Networks, Inc.*

This year, when asked about security concerns related to IPv6, both our service provider and enterprise, government and education respondents have the same top three concerns:

- DDoS
- Inadequate IPv4/IPv6 feature parity
- Misconfiguration

However, the order does differ. For the service providers, the top security concern is DDoS attacks, with misconfiguration and inadequate feature parity very close behind. The order of the latter two has alternated in recent years, and they have again swapped positions this year. Regardless, all these concerns score similarly, which suggests that they are equally critical to respondents.

IPv6 Security Concerns

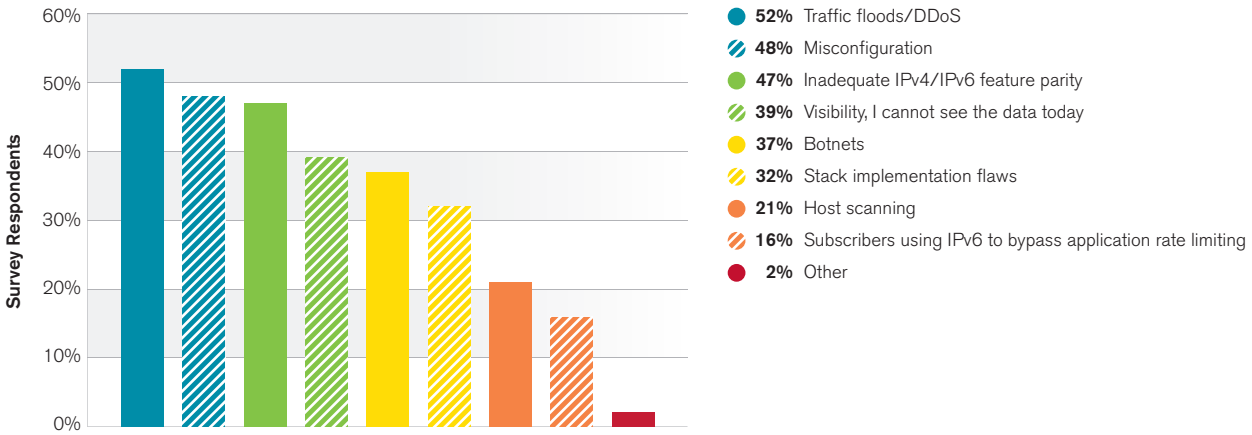


Figure 51 *Source: Arbor Networks, Inc.*

We asked respondents whether they are concerned that attacks targeting dual-stack devices over IPv6 would impact IPv4 services. Nearly half indicated that this is either a major or moderate concern. This backs up anecdotal feedback from outside of the survey and emphasizes why protection of even lightly used IPv6 services is important. In terms of IPv6 mitigation capabilities, the results this year are very similar to last. IDMS systems and ACLs remain the two most important mitigation techniques for dealing with IPv6 attacks, with 71 percent and 69 percent of the respondents relying on these technologies respectively (Figure 52).

IPv6 Mitigation Capabilities

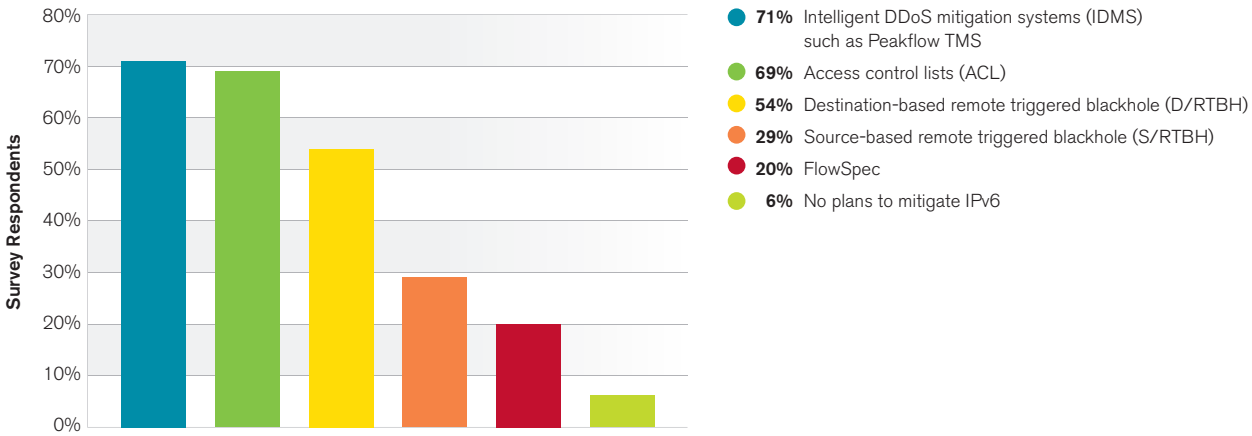


Figure 52 *Source: Arbor Networks, Inc.*

ATLAS IPv6

In addition to tracking DDoS attacks, the ATLAS system gathers traffic statistics from participants. One of the statistics gathered is the amount of native IPv6 traffic crossing the boundaries of participant networks.

The peak, cumulative, native IPv6 traffic volume monitored by ATLAS across approximately 330 participating network operators during this survey period was around 1.24 Tbps—roughly three times the peak monitored last year. As in previous years, the level observed has significantly outstripped the expected growth of survey respondents. However, IPv4 traffic levels have also grown from a peak of around 80 Tbps in 2013 to over 120 Tbps in 2014. Looking at these numbers, IPv6 still only represents around 1 percent of IPv4 traffic volume.

This year approximately one-third of ATLAS participants provided statistics on native IPv6 traffic, a roughly similar percentage to last year. It should be noted that the number of ATLAS participants grew from around 290 to 330 during this period. Figure A14 shows the geographic distribution of the participants providing data on native IPv6 traffic.

Figure A15 shows the levels of IPv6 traffic monitored by ATLAS throughout 2014. Interestingly the traffic levels seem to be relatively flat at the start of the year, with significant growth in the late summer. It is unclear from the data what has caused this specific growth profile. Although the growth this year is significant, it has not kept pace with the growth level seen in 2013 (10x). IPv6 remains at roughly 1 percent of Internet traffic.

ATLAS Participants Providing Native IPv6 Data

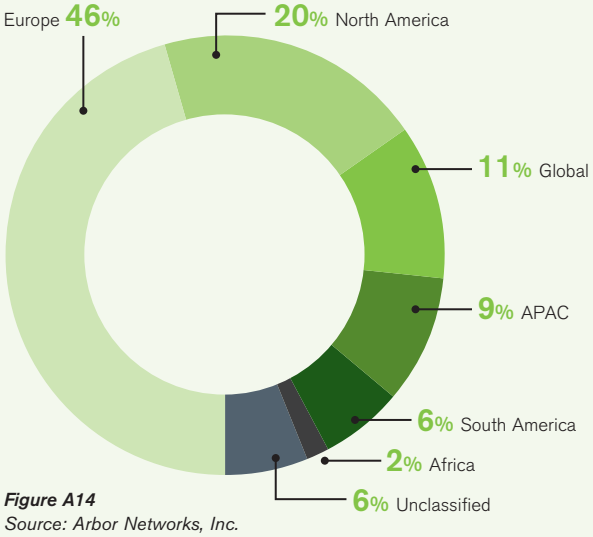


Figure A14
Source: Arbor Networks, Inc.

ATLAS IPv6 Traffic

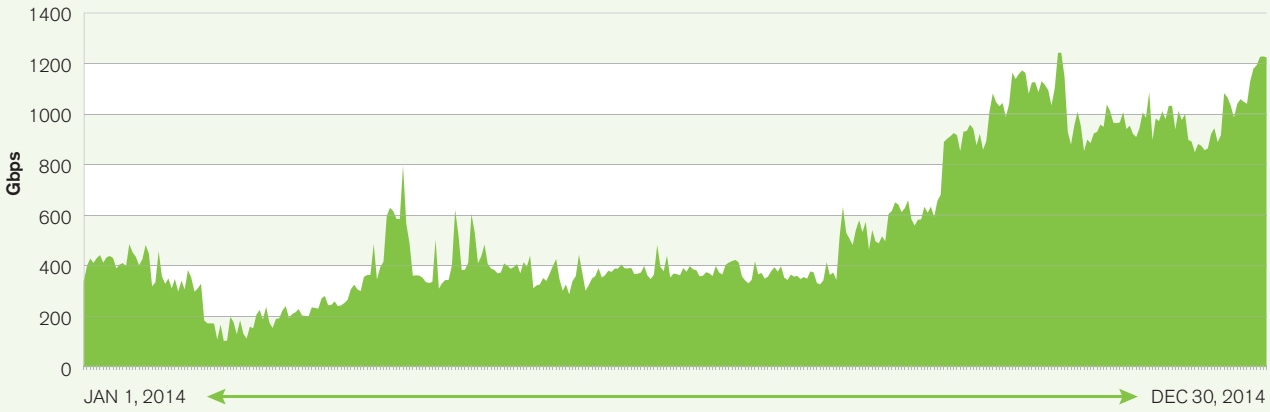


Figure A15 *Source: Arbor Networks, Inc.*

9 Data Center

Sixty-four percent percent of respondents offer data center services. Three-quarters have visibility up to Layer 3/4 traffic, but only 38 percent have visibility at Layer 7. Nearly two-thirds of respondents indicated that they have ingress anti-spoofing filters in place, but 20 percent have no plan to install filters. Firewalls, application firewalls and IPS are still the top three deployed security mechanisms in the data center. Big increases are reported in the use of both IDMS and iACLs. The former is up from 6 percent last year to 48 percent this year, with the latter up from 13 percent last year to 30 percent this year.

Within the data center, the most common reported DDoS attack target is customers, taking over from service infrastructure. Just over a third of respondents saw DDoS attacks that exhausted their Internet bandwidth, indicating that this is still a critical issue. 81 percent cited operational expense as their top cost due to DDoS. There was also a significant increase in those seeing revenue losses, up to 44 percent from 27 percent last year. As in previous years, iACLS and firewalls remain the most popular mechanisms for defending data centers from DDoS attacks. However, 49 percent of respondents indicated that their firewalls experienced or contributed toward an outage due to DDoS, and over one-third of respondents saw their load balancers fail due to DDoS in the last year. A key positive change is the increased use of IDMS to protect the data center, up from just over one-third last year to over half this year.

Cloud computing, data center and hosting providers have seen their traffic grow significantly as more organizations utilize their services. This year 64 percent of respondents offer data center services, a very similar result to the last two years. Three-quarters have visibility up to Layers 3/4 of traffic, but only 38 percent have visibility at Layer 7. Although the Layer 3/4 visibility has decreased slightly from 83 percent last year, Layer 7 visibility has actually risen substantially, up from just 23 percent last year. This may be due to the fact that data center operators, as well as service users, have become more aware of the potential risk of application-layer DDoS attacks. The decrease in Layer 3/4 traffic visibility may also be due to changes in the data center forwarding fabric due to SVN and virtualization.

Data Center Traffic Visibility

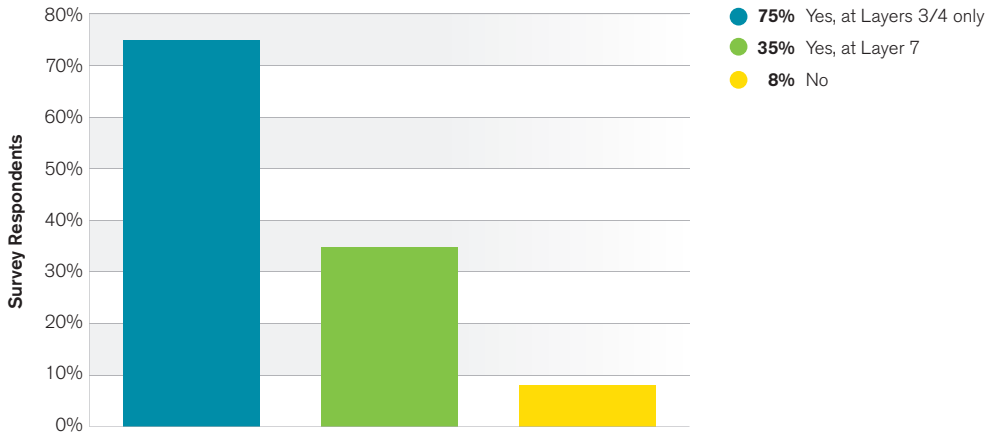


Figure 53 *Source: Arbor Networks, Inc.*

This year has witnessed a storm of large-scale reflection/amplification DDoS attacks using DNS, NTP and SSDP. Understandably there is increased concern around the capabilities within the Internet that allow these attacks to take place. Given that some of the recent attacks have originated utilizing compromised infrastructure within data centers, we asked respondents whether they have implemented anti-spoofing filters within their data center. Encouragingly nearly two-thirds indicated that they have these filters in place, but 20 percent still have NO plan to install filters to guard against source address spoofing (Figure 54). This creates a strong opportunity for attackers to use these data centers to carry out large reflection attacks.

Data Center Anti-Spoofing Filters

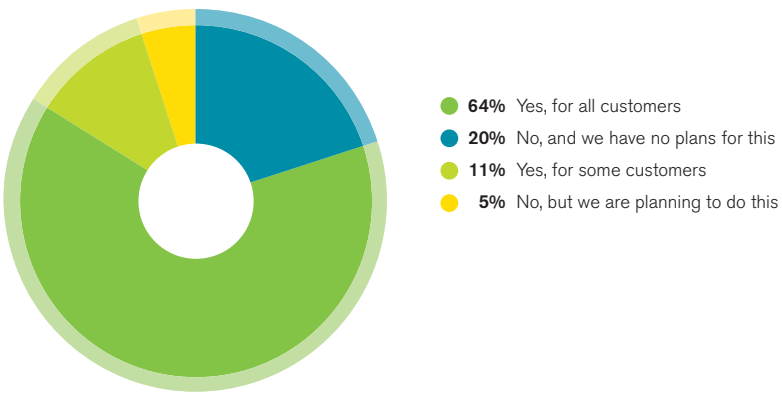


Figure 54 *Source: Arbor Networks, Inc.*

To protect data center infrastructure from threats, most operators have multiple solutions deployed at the data center perimeter. Firewalls, application firewalls and IPS are still the top three deployed security mechanisms in the data center, with levels similar to last year. Respondents report big increases in the use of both IDMS and iACLs. The former is up from 6 percent last year to 48 percent this year, while the latter is up from 13 percent last year to 30 percent this year (Figure 55). These are very encouraging results, indicating that data center operators are increasingly aware of the need for security mechanisms that provide better protection against DDoS by not maintaining significant state.

Data Center Threat Protection

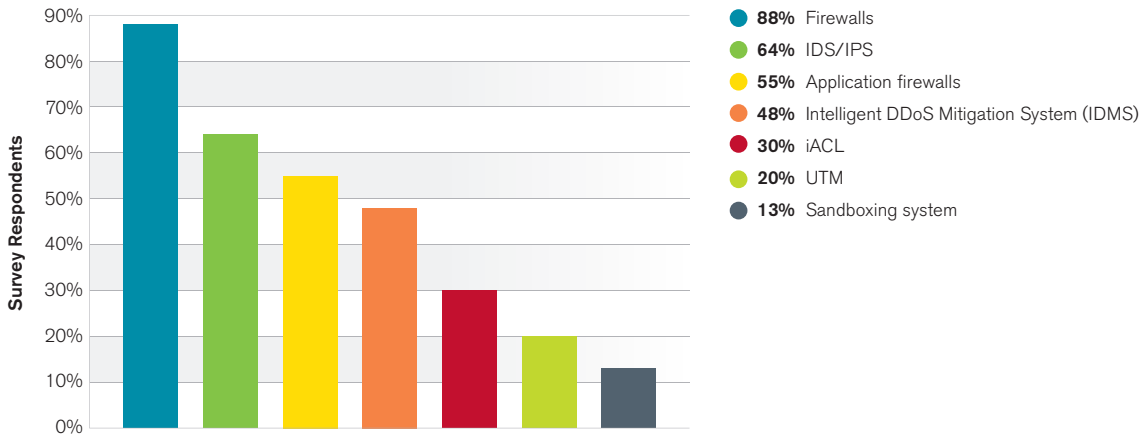


Figure 55 *Source: Arbor Networks, Inc.*

Almost two-thirds of respondents indicated they have seen DDoS attacks in the past year, a slight drop from 71 percent last year. This is still a high proportion (as expected) and shows that DDoS attacks continue to be a major threat for the data center.

Looking at attack frequency, results are broadly similar this year. Two-thirds indicated they see between 1 and 10 attacks per month (Figure 56). The only significant change this year is that no respondents reported seeing more than 50 attacks per month, down from 12 percent last year.

Data Center DDoS Attack Frequency

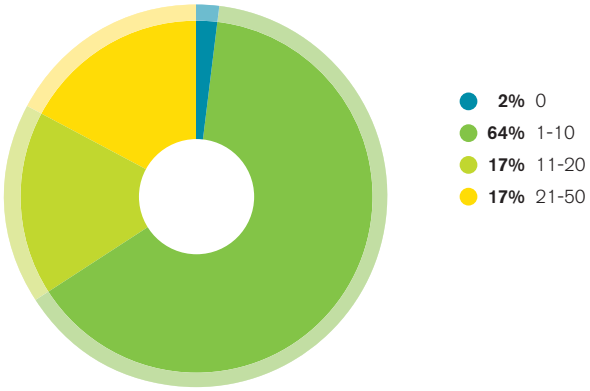


Figure 56 *Source: Arbor Networks, Inc.*

Within the data center, the most common attack target is customers, taking over from service infrastructure. Just over two-thirds experienced attacks targeting customers this year, up from just over half last year (Figure 57). The proportion seeing attacks targeting data center service infrastructure has stayed approximately the same as last year.

Data Center Attack Targets

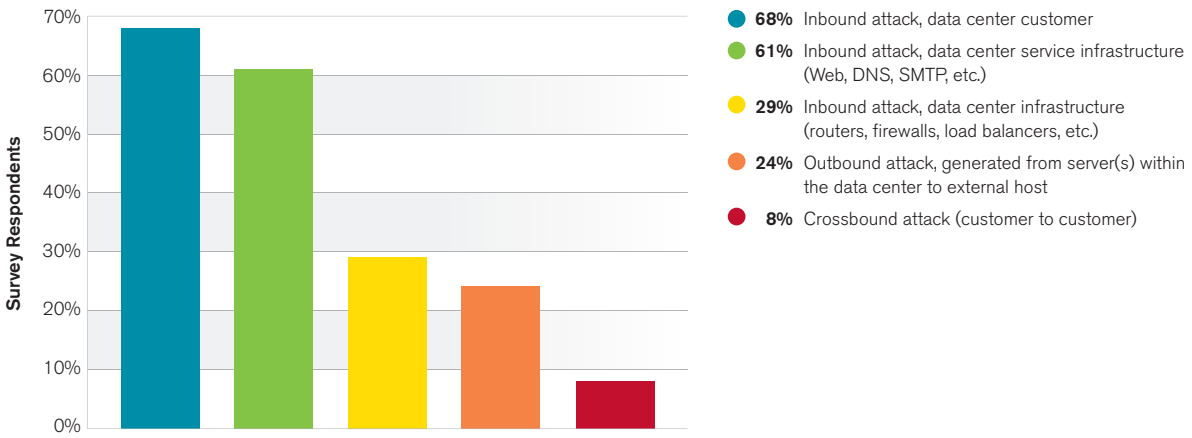


Figure 57 *Source: Arbor Networks, Inc.*

A key area of concern last year was the relatively high proportion of data center operators who had experienced attacks that exceeded their Internet bandwidth. This year the proportion is virtually identical, with just over a third indicating this is still a critical issue. By their very nature, these attacks require an external mitigation mechanism—most commonly a service provider or cloud-based DDoS mitigation service. Without any means of dealing with these attacks, data center operators can see significant service impact across their customer base.

Data Center DDoS Business Impact

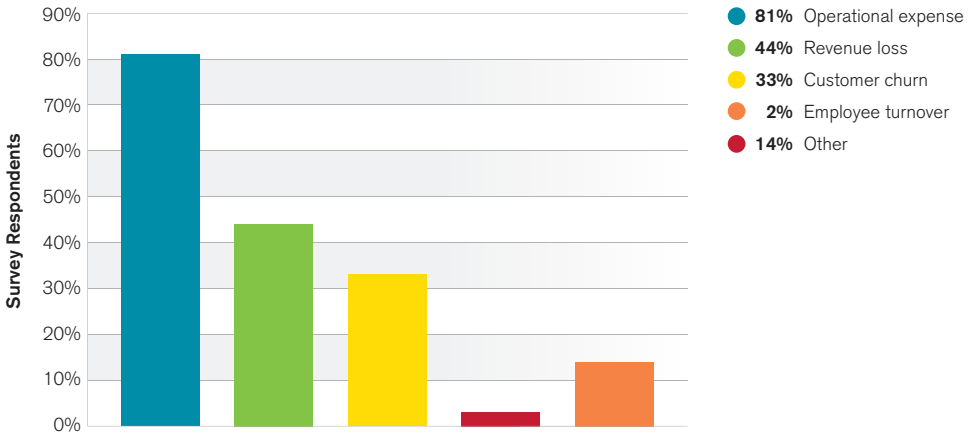


Figure 58 *Source: Arbor Networks, Inc.*

When asked about the business impact of DDoS attacks to the data center, 81 percent of respondents cited operational expense, an identical result to last year. The proportion of respondents who experienced customer churn is also identical to last year. However, there is a significant increase in those seeing revenue losses, up to 44 percent from 27 percent last year.

Data center operators use a wide variety of DDoS prevention and mitigation techniques (Figure 59). We have seen an increase across the board in the various technologies.

Data Center DDoS Defenses

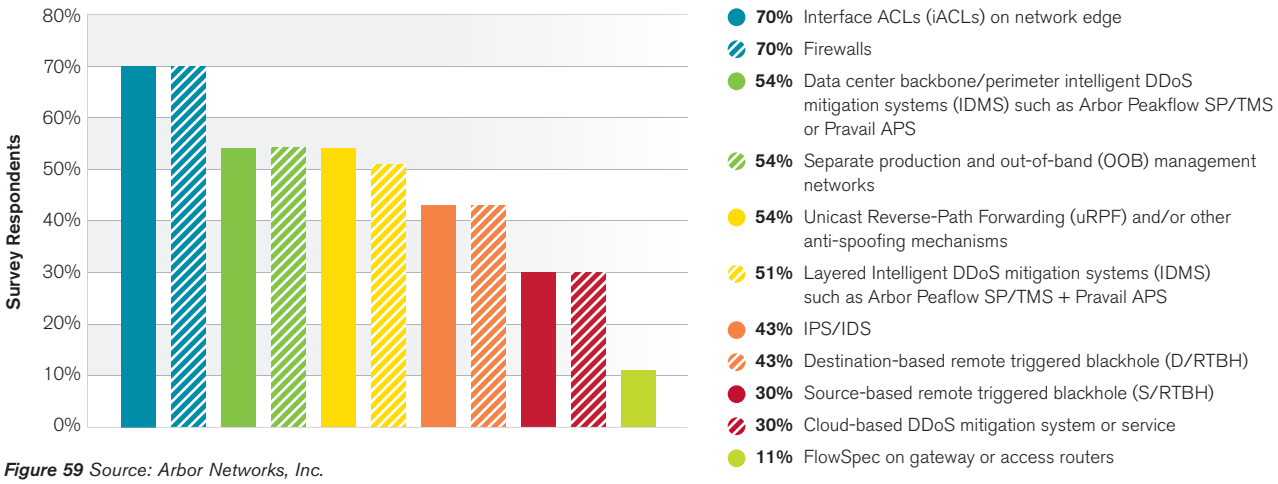


Figure 59 *Source: Arbor Networks, Inc.*

On the negative side, firewalls remain the top defensive mechanism for the data center against DDoS attacks. This is a key issue, as firewalls cannot mitigate a significant proportion of today's DDoS attacks. In fact, they can actually be a target. Just under half of respondents indicated that their firewalls experienced or contributed toward an outage due to DDoS this year—up from 42 percent last year (Figure 60). Load balancers also saw issues, with over one-third of respondents seeing these fail due to DDoS in the last year.

To leverage their investment in these technologies, many data center operators offer their customers managed DDoS detection and mitigation. Similar to last year, 37 percent of respondents provide DDoS services either as part of their base offering or as an additional option. Just over a fifth of respondents offer multiple tiers of DDoS protection service.

Data Center Firewall Failures Due to DDoS

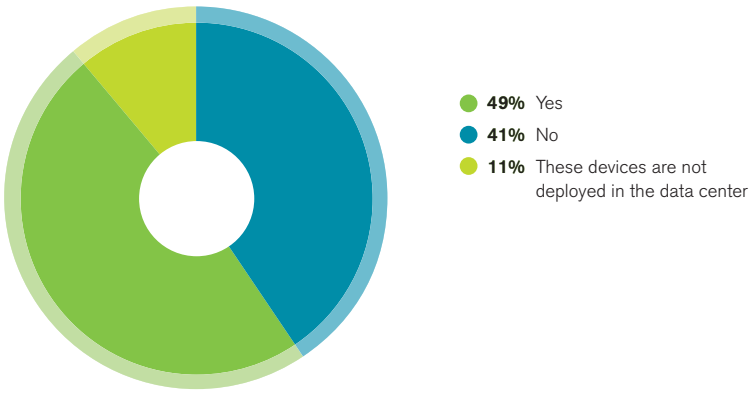


Figure 60 *Source: Arbor Networks, Inc.*

A key positive change is the increased use of IDMS, up from just over a third last year to more than half this year. This is very positive, especially as over half of respondents indicated that they use the best practice of layered IDMS protection.

10 Mobile Network Operators

Mobile devices and applications continue their exponential growth. This growth continues to apply pressure to mobile network operators (MNOs) to meet the common challenges associated with limited spectrum, extending coverage and capital investment. According to this year's survey, 29 percent of respondents offer mobile services, compared to 42 percent last year. This is a significant decrease, but given the increased number of overall respondents, the data gathered provides valuable insights into mobile networks.

Mobile Network Packet Core

With the increased adoption of HSPA+ and LTE, more devices and users are accessing data networks and applications. This increase is forcing MNOs to expand capacity in the packet core and to plan and design for new data-consuming technologies, such as machine-to-machine (M2M) communications, IP multimedia systems (IMS) and the Internet of Things (IoT).

LTE is quickly becoming a pervasively deployed technology. Over three-quarters of respondents indicated that they already have LTE equipment deployed, with a further 16 percent planning to deploy it in 2015. Seventeen percent of respondents indicated that they have experienced a security incident on the packet core that led to a customer-visible outage, down from just over 20 percent last year and 33 percent in 2012. The most common measures that MNOs use to protect their packet core are still iACLs and NAT/PAT. In fact, the use of both these technologies has increased significantly. Eighty percent of organizations do not support the use of IPv6 in either the subscriber devices or mobile infrastructure on their networks. Thirty-six percent of respondents have seen DDoS attacks targeting their mobile users, RAN, backhaul or packet core—an 11 percent increase over last year.

Mobile communication long ago transitioned from being a luxury to being a necessity. This year 68 percent of respondents indicated that they have more than one million subscribers, versus 60 percent last year (Figure 61). Also, 22 percent reported that their networks have more than 25 million subscribers, versus 20 percent last year. The continued growth of subscribers underscores the importance in the availability of the services offered by mobile networks.

Number of Subscribers

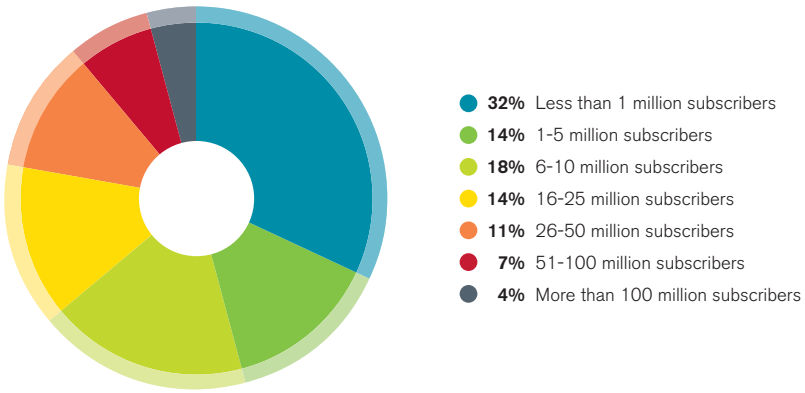


Figure 61 *Source: Arbor Networks, Inc.*

Most organizations continue to operate traditional GSM 2G and 3G networks. However, the number of operators offering LTE services continues to increase, with nearly three-quarters indicating that they are utilizing LTE, versus approximately 63 percent in 2013, 53 percent in 2012 and 29 percent in 2011 (Figure 62).

Seventy-six percent indicated that they already have LTE equipment deployed (Figure 63), with a further 16 percent planning to deploy it in 2015. LTE is quickly becoming a pervasively deployed technology.

Radio Technologies

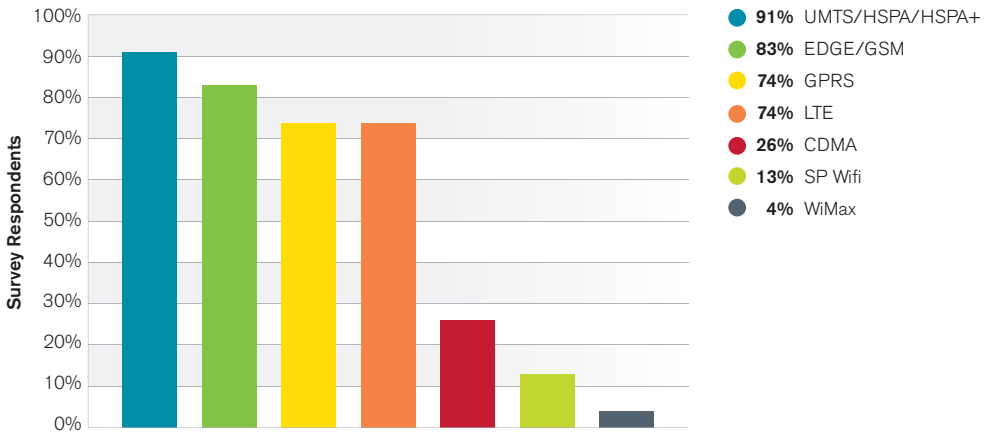


Figure 62 *Source: Arbor Networks, Inc.*

This year 17 percent of respondents indicated that they have experienced a security incident on the packet core that led to a customer-visible outage, down from just over 20 percent last year and 33 percent in 2012. This is an encouraging trend. However, 35 percent still do not know if they have had outages caused by a security incident, up from 25 percent last year (Figure 64). This statistic highlights a continued lack of visibility and detection capabilities on some mobile networks.

LTE Deployment

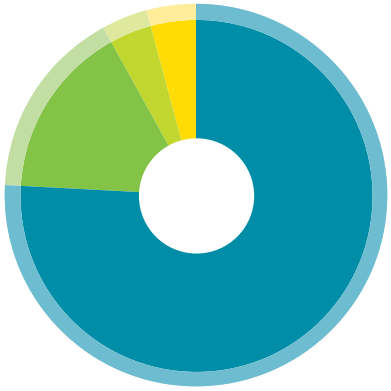


Figure 63 *Source: Arbor Networks, Inc.*

Security Incidents

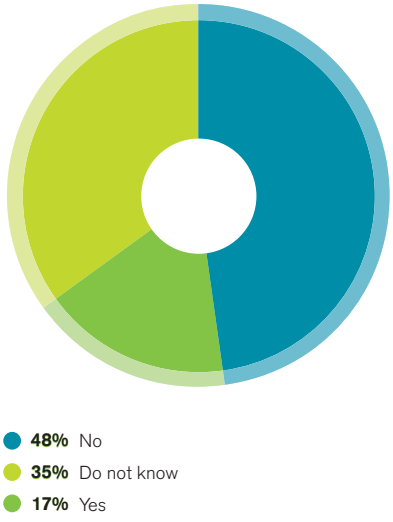


Figure 64 *Source: Arbor Networks, Inc.*

MNOs utilize a wide variety of tools and techniques to protect their infrastructure against availability threats (Figure 65). As in the previous two years, iACLs and NAT/PAT technology are still the most common protective measures. In fact, the use of both has significantly increased this year: NAT/PAT usage rose from 62 percent to 89 percent, and iACL usage jumped from 47 percent to 79 percent. This latter statistic reverses a decrease seen between 2012 and 2013 data.

While the use of GTP firewalls and security gateways (SEGs) remained fairly steady this year, there has been a significant increase in the use of QoE monitoring probes (up from 21 percent to 32 percent), IDMS (up from 38 percent to 47 percent), data signaling gateways (up from 18 percent to 47 percent) and SMS firewalls (up from 12 percent to 47 percent). These increases show that many MNOs may have adopted multiple new solutions to address the threats they face.

Security Measures

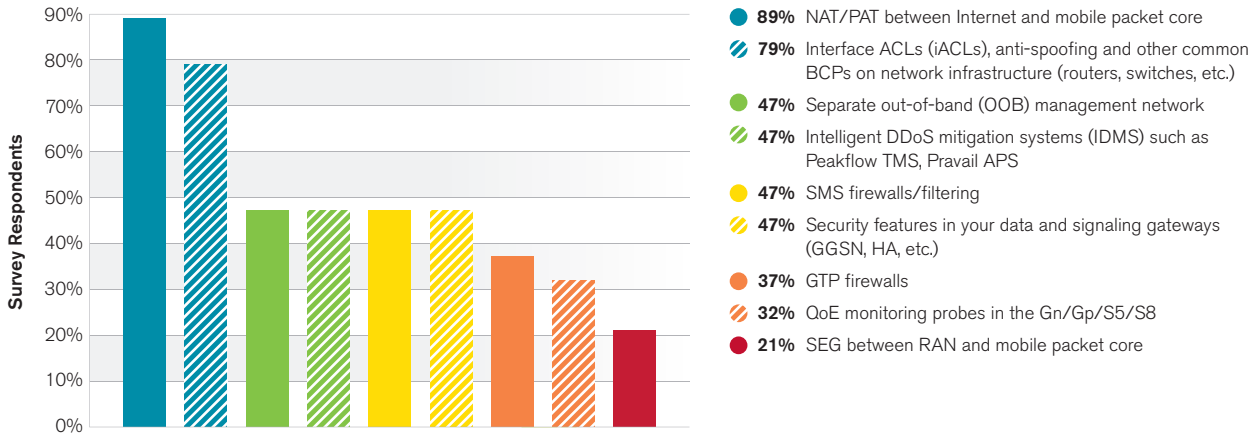


Figure 65 *Source: Arbor Networks, Inc.*

For the first time, this year's survey asked how much visibility MNO respondents have into the many protocols traversing their packet core. One-third of respondents indicated that they have no visibility (Figure 66). This is an almost identical proportion to last year.

The protocols into which MNOs have the most visibility are Diameter and SIP. Forty-two percent of respondents reported good visibility into each. GTP-C came in third place at 33 percent. Interestingly far fewer respondents have visibility into the user plane (GTP-U) and Proxy Mobile IP Version 6. In the case of the latter, this may be explained by the lack of integration between 3GPP technologies and SP Wi-Fi. For GTP-U, it is worrisome that very few operators have visibility into user data and the potential security threats (i.e., malware) that may be affecting both mobile infrastructure and user devices.

Visibility in Packet Core

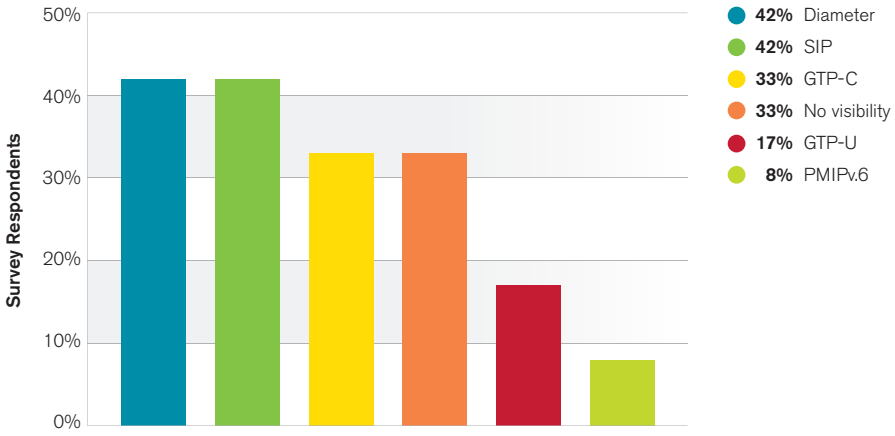


Figure 66 *Source: Arbor Networks, Inc.*

Similar to last year, the majority of respondents who have visibility into traffic on their mobile packet core get it from counters and statistics available directly from the mobile infrastructure itself. Thirty-three percent of operators reported using existing mobile-vendor-supplied, probe-based monitoring solutions. The same proportion reported using third-party probes (Figure 67).

Visibility Mechanism

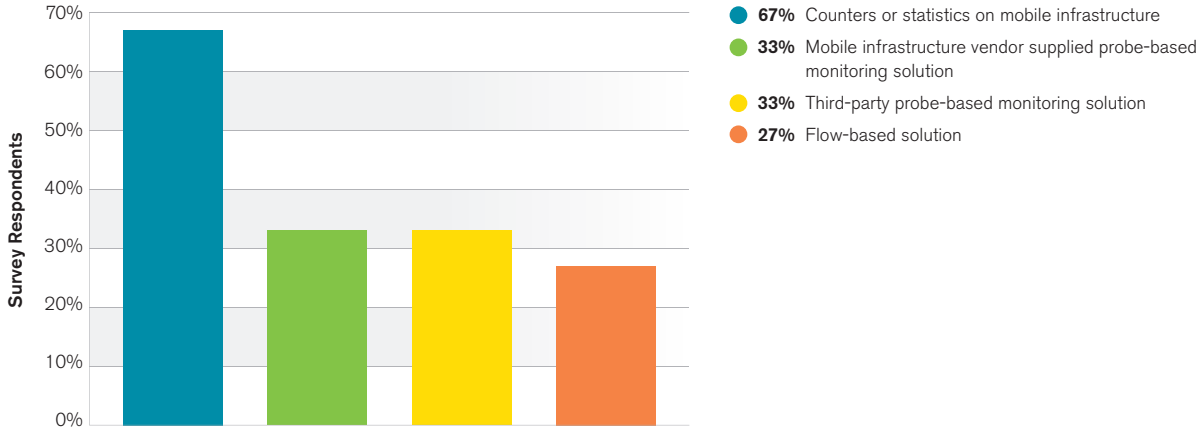


Figure 67 *Source: Arbor Networks, Inc.*

Another new question this year looked at MNO visibility on data-roaming interfaces. With the increasing use of roaming, visiting data traffic continues to grow. It is discouraging to note that only 20 percent of respondents feel that appropriate visibility is in place, while 60 percent are unsure whether they have adequate visibility or not. For those with visibility into roaming data, the counters and statistics available directly from the mobile infrastructure are by far the most commonly used mechanisms (Figure 68). Flow-based solutions and third-party counters are next, with 21 percent using these tools.

Roaming Data Monitoring

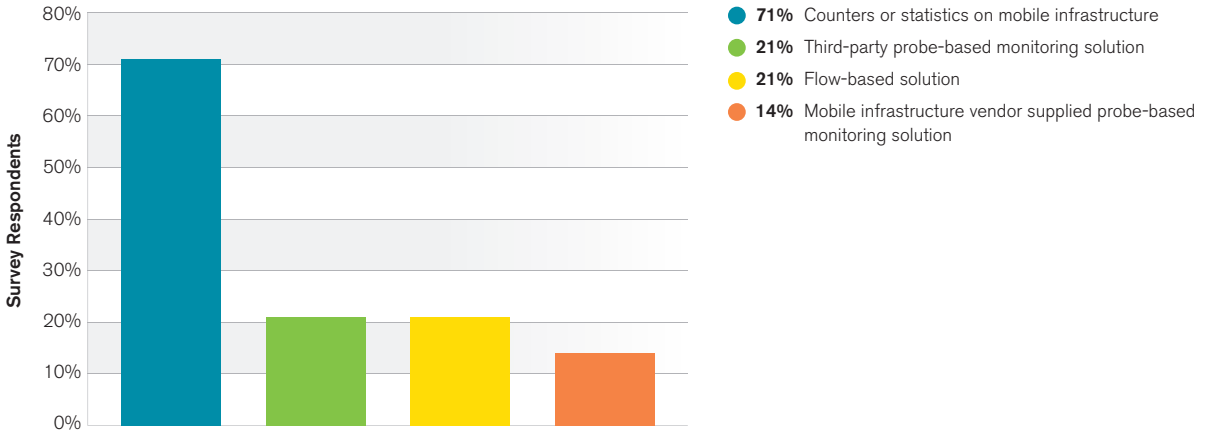


Figure 68 *Source: Arbor Networks, Inc.*

Poorly implemented applications can pose a real problem for mobile operators—causing signaling storms, spikes in DNS traffic and other network-congestion issues (Figure 69). Thirty-six percent of respondents indicated that they have experienced this issue, a similar proportion to last year. Interestingly no one indicated that they have detected this threat using counters or statistics on mobile infrastructure this year, down from nearly 25 percent last year.

Poorly Implemented Application Impact

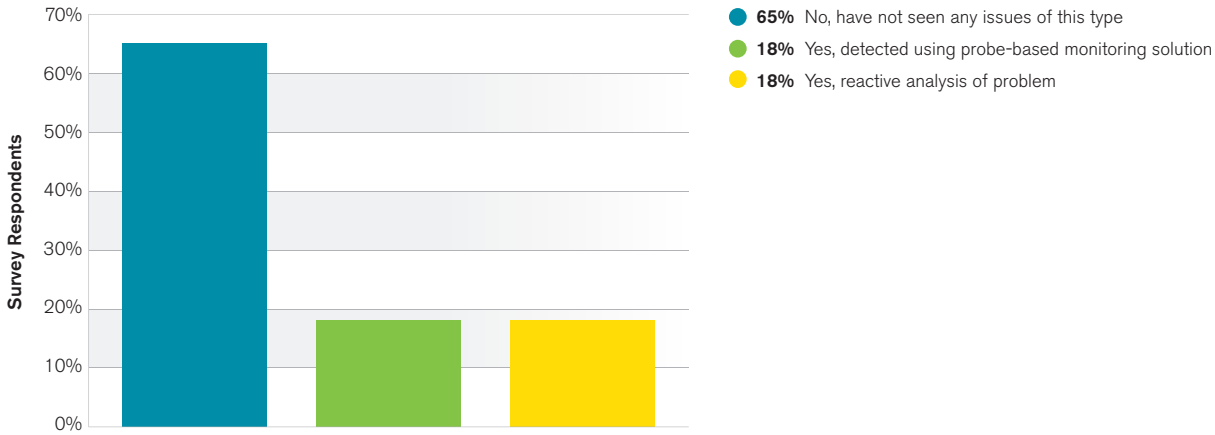


Figure 69 *Source: Arbor Networks, Inc.*

The adoption of IPv6 within mobile networks continues to be relatively low. The vast majority of respondents—80 percent—do not support the use of IPv6 in either the subscriber devices or mobile infrastructure on their networks. In fact, only 10 percent have implemented IPv6 at the subscriber and mobile-infrastructure level. Last year one-quarter of respondents said that they intended to implement IPv6 during the survey period. This has clearly not happened.

Looking at threats from subscriber devices, three-quarters of responding organizations cannot detect a compromised subscriber device on their networks. This backs up the earlier data indicating that mobile operators may have limited visibility into the user-plane traffic that would allow this kind of threat detection. Given the rate of LTE adoption, this remains a frightening statistic, as these subscribers can potentially have a great deal of bandwidth at their disposal.

In this year's survey, we also introduced a more specific question about the DDoS threats originated by mobile devices. Forty-eight percent of respondents have not seen any attacks initiated by mobile users on their networks, with only 13 percent identifying this threat (Figure 70).

DDoS Attacks from Mobile Users

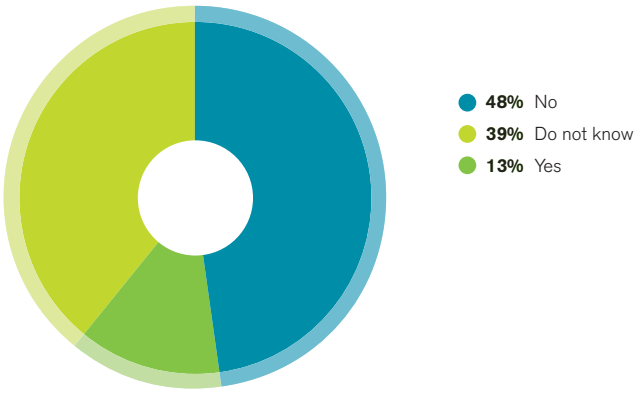


Figure 70 *Source: Arbor Networks, Inc.*

Nearly three-quarters of respondents indicated that they have no plans to mitigate outbound DDoS attacks (Figure 71). This is a concern, especially given the increasing penetration and performance of LTE, in addition to the prevalence of NAT at the boundary of mobile networks. With many subscribers "NAT'ed" to the same source IP address, it is very difficult for upstream providers to successfully mitigate one subscriber generating an attack without affecting other subscribers.

Outbound Attack Mitigation

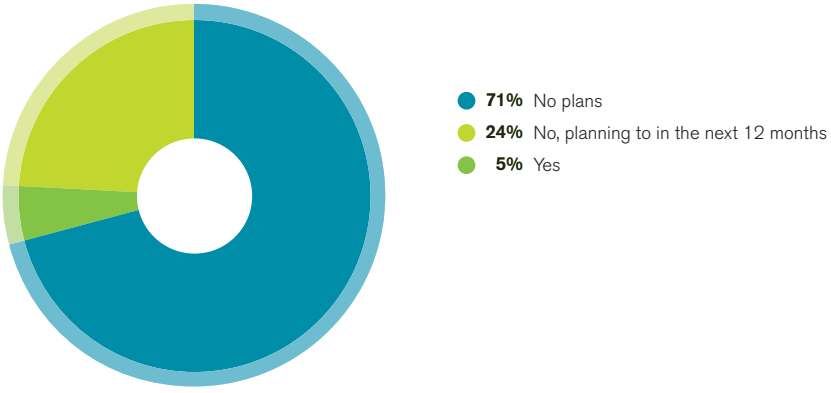


Figure 71 *Source: Arbor Networks, Inc.*

DDoS Attacks Against Mobile Infrastructure

Fifty percent of respondents indicated that they have seen DDoS attacks targeting end-user devices, with 33 percent identifying attacks against the packet core. The number of network operators reporting between 51 and 100 attacks in a single month increased significantly, from last year's 7 percent to 17 percent this year.

Thirty-six percent of organizations have seen DDoS attacks targeting their mobile users, RAN, backhaul or packet core—a significant increase from last year's result of 25 percent (Figure 72). This increase reinforces anecdotal information from mobile operators indicating an increase in DDoS activity.

DDoS Attacks on Mobile Infrastructure or Users

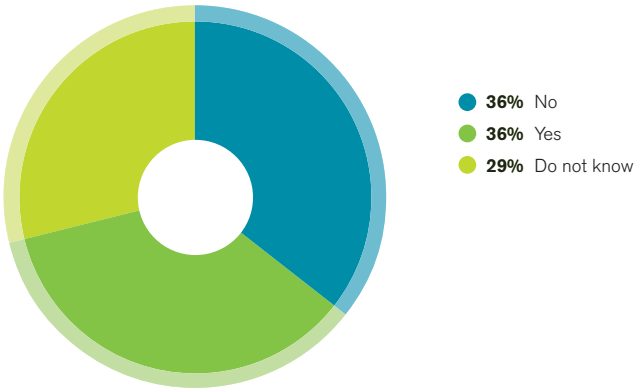


Figure 72 *Source: Arbor Networks, Inc.*

We asked respondents to identify the mobile network elements affected by DDoS attacks. Fifty percent indicated that they have seen such attacks targeting end-user devices (Figure 73), while 33 percent identified packet core and other elements (i.e., Routers). Only 17 percent suffered from DDoS attacks targeting their RAN infrastructure. It will be interesting to see how this trends in the future as MNO respondents increase their visibility within their mobile infrastructure.

Mobile Resources Affected by DDoS Attacks

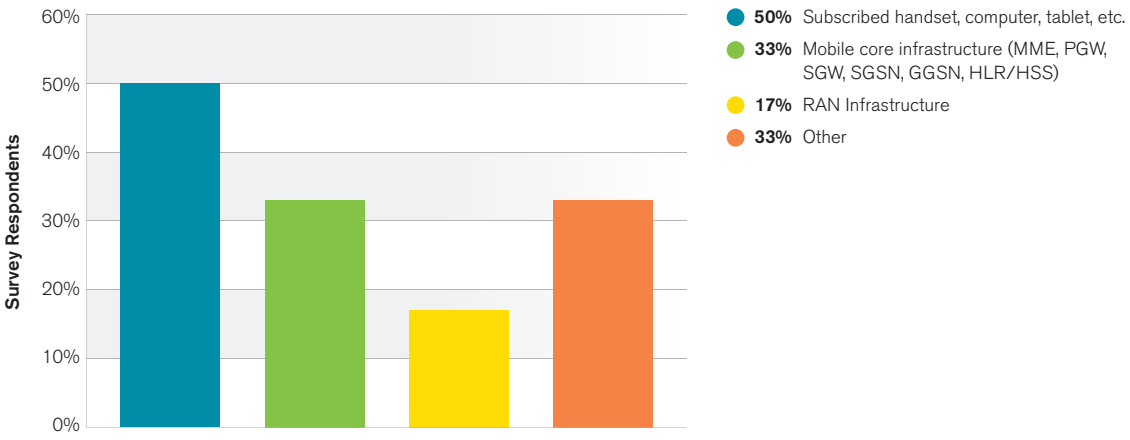


Figure 73 *Source: Arbor Networks, Inc.*

The vast majority of respondents who did see DDoS attacks on their mobile users and mobile infrastructure reported between 1 and 10 events per month. This is in line with last year's results (Figure 74).

Number DDoS Attacks on Mobile Infrastructure

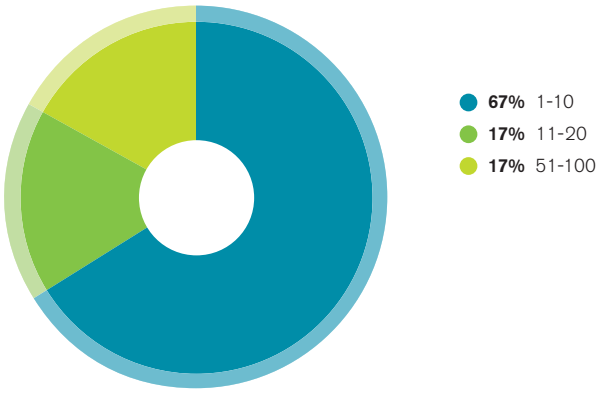


Figure 74 *Source: Arbor Networks, Inc.*

Mobile IP Infrastructure (Gi/SGi)

Less visibility into Mobile Internet (Gi/SGi) infrastructure relative to the last two iterations of this report. Thirty percent of respondents indicated that they had NO visibility at all this year, a significant increase from 20 percent last year.

The proportion of organizations with visibility into the traffic on their mobile Internet (Gi/SGi) infrastructure went down compared to the last two years. This year 57 percent have visibility at Layers 3 and 4, compared to 77 percent last year. Further, only 17 percent have Layer 7 visibility, compared to 23 percent last year. What is most concerning is that 30 percent indicated they have NO visibility at all—a significant increase from 20 percent last year (Figure 75).

Visibility at (Gi/SGi) IP Backbone

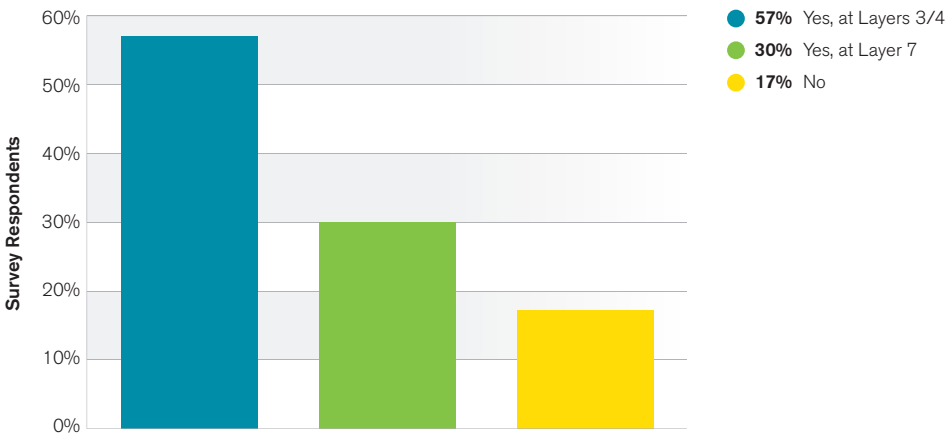


Figure 75 *Source: Arbor Networks, Inc.*

Similar to last year, those with visibility are using a variety of solutions, with infrastructure counters and statistics being the most common mechanism (Figure 76). Flow-based solutions are the second most common mechanism, as solutions developed to operate in generic ISP environments are more applicable at the Gi/SGi interface.

Visibility Mechanism

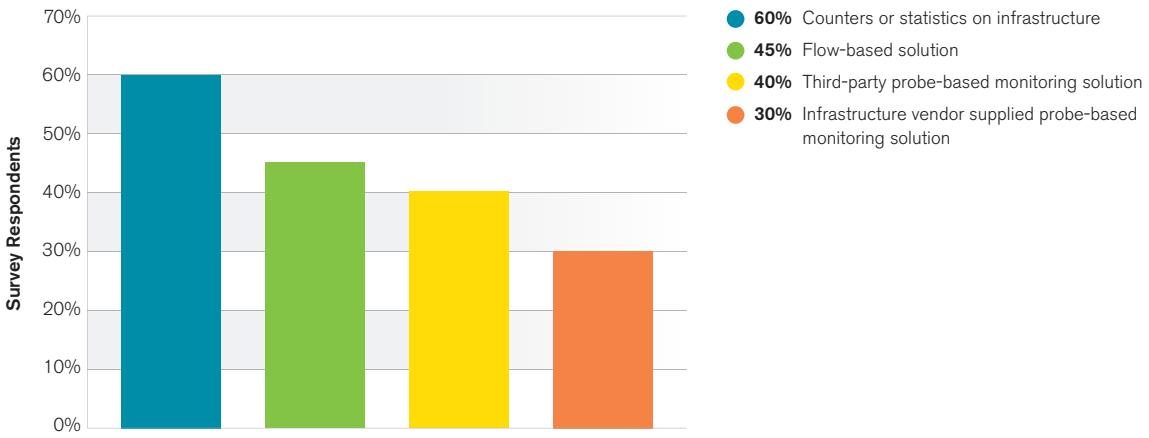


Figure 76 *Source: Arbor Networks, Inc.*

DDoS Attacks Against Mobile IP (Gi/SGi) Infrastructure

Only 7 percent of respondents indicated that they have seen DDoS attacks impacting their mobile Internet (Gi/SGi) infrastructure (Figure 77). This represents a sharp decrease from last year's results, and may indicate a reduction in the number of attacks. However, this could also be due to the reported reduction in visibility. External firewalls are the top targets of attacks seen by organizations this year, followed by routers and switches (link saturation), DNS servers and carrier-grade NAT.

DDoS Impact on IP Infrastructure

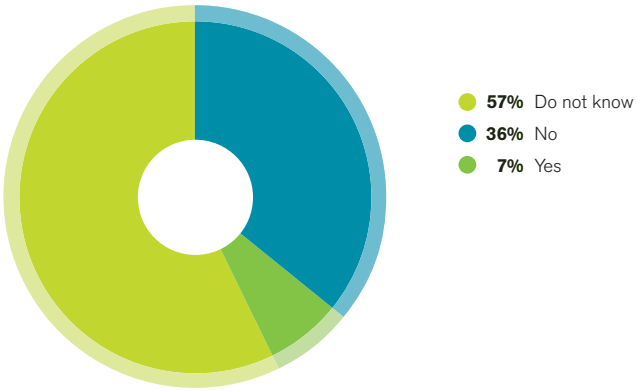


Figure 77 *Source: Arbor Networks, Inc.*

11 Enterprise, Government and Education Network Security

The most frequently observed threats on enterprise networks are DDoS attacks, accidental data loss and botted or otherwise compromised hosts. Each of these categories garnered around 33 percent of respondents. Nearly a fifth of respondents indicated that APTs have targeted their organizations during the survey period. Looking at the frequency of security incidents, just over 33 percent indicated an increase this year, with about 50 percent indicating similar levels to last year. Fewer than 50 percent of respondents feel reasonably or well-prepared for a security incident, with 15 percent indicating that they have no plans or resources in place.

For the first time, this year's WISR survey included a separate set of questions aimed at enterprise, government and education respondents. These sections, accessed via logic embedded within the survey, were tailored to garner more relevant information from these markets.

The most frequently observed threats targeting enterprise, government and education respondents are DDoS attacks, accidental data loss and botted or otherwise compromised hosts. Each of these categories garnered around a third of respondents (Figure 78). This data clearly indicates that DDoS attacks are now seen as one of the top threats to enterprise, government and educational organizations. This backs up anecdotal information, outside of this survey, indicating that a growing proportion of these organizations are looking for DDoS defenses.

Most Significant Operational Threats

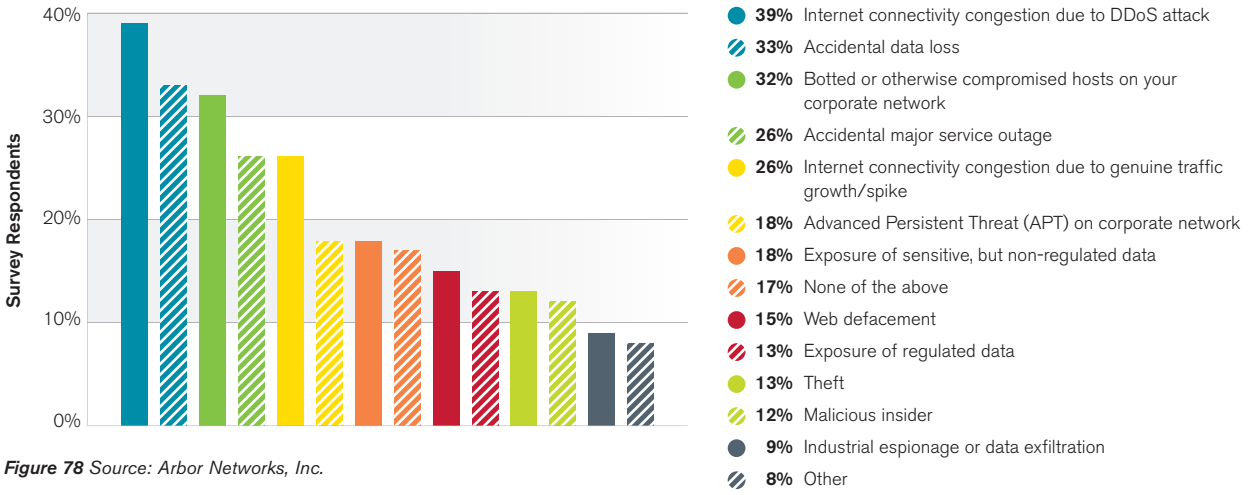


Figure 78 *Source: Arbor Networks, Inc.*

Another hot topic for the past few years is advanced persistent threats (APT). Nearly a fifth of respondents indicated that APTs have targeted their organizations during this survey period. One-fifth also experienced the exposure of sensitive but non-regulated data. Clearly organizations are facing more threats than ever before.

When asked to look at their concerns for the coming year, just over half of all respondents rank DDoS as number one (Figure 79). Other top concerns, also cited by about half of respondents, include advanced persistent threats, exposure of sensitive but non-regulated data and accidental data loss. It is interesting to note that in nearly every category, more respondents expressed concern about threats than have actually experienced them in the past year. While this trend is consistent with last year, where data for service provider and enterprise/government/education respondents was mixed together, the difference is more pronounced this time around.

Operational Security Concerns

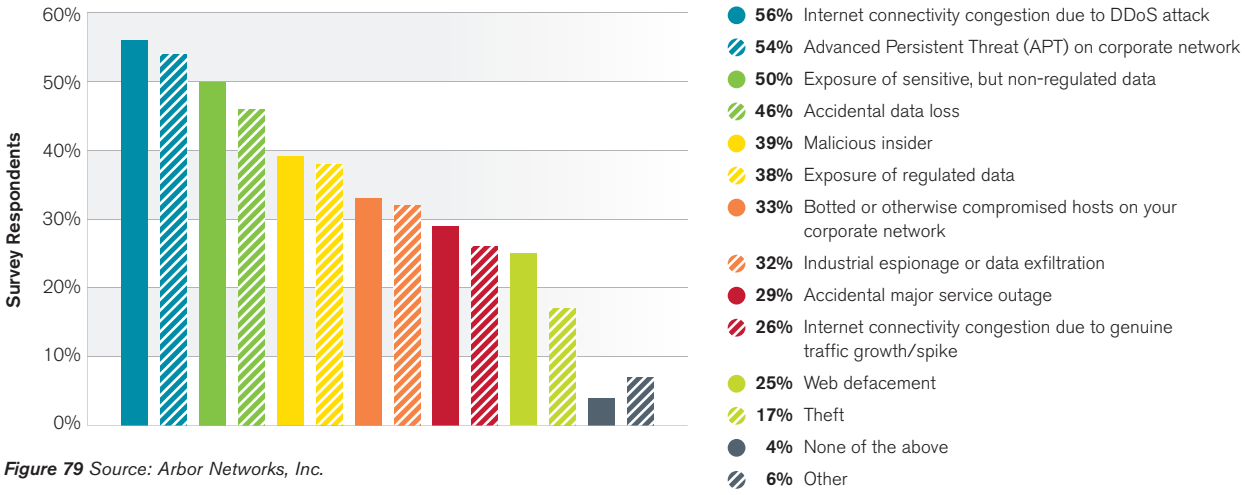


Figure 79 *Source: Arbor Networks, Inc.*

How quickly organizations respond to detected threats is hugely important, and has been highlighted as an issue in other studies. This year's survey asked organizations to estimate their average response times to security incidents. Enterprise, government and educational organizations reported impressive response times (Table 2), although they are generally a bit slower than those of service provider organizations (Table 1).

Incident Response Time

	Minimum	Maximum	Average
Time from compromise to discovery	10 minutes	6 months	1 week
Time from discovery to Internal reporting	1 second	1 month	1 day
Time from reporting to resolution	30 minutes	6 months	1 week
Time from discovery to notification (where applicable)	1 second	1 week	½ day

Table 2 *Source: Arbor Networks, Inc.*

About two-thirds of organizations reported having both an incident response plan and at least some dedicated resources (Figure 80). Fifteen percent of respondents indicated having no plans or resources, while another 18 percent have plans but no resources. These results show less overall preparedness when contrasted with the service provider results earlier in this report. Clearly there is much room for improvement here.

Incident Response Posture

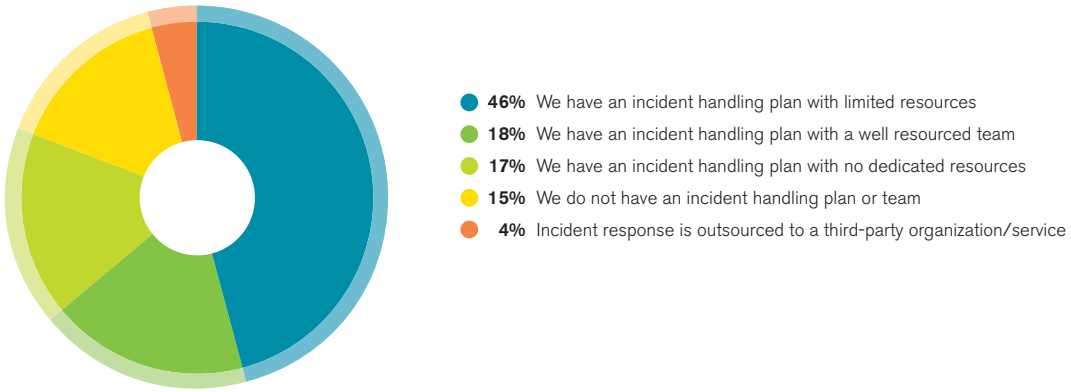


Figure 80 *Source: Arbor Networks, Inc.*

When asked about the use of external organizations to assist during incident response, over half of respondents indicated they have some contract(s) in place—a significantly higher percentage than service providers. This is possibly due to the deeper and broader skill sets available in-house for service providers. Around 40 percent of respondents indicated the use of an IT forensic expert or other specialist IT provider (Figure 81). However, only 25 percent have a relationship with the police or other law enforcement agency; it should be noted that this is double the percentage seen from the service providers.

Use of External Organizations for Incident Response

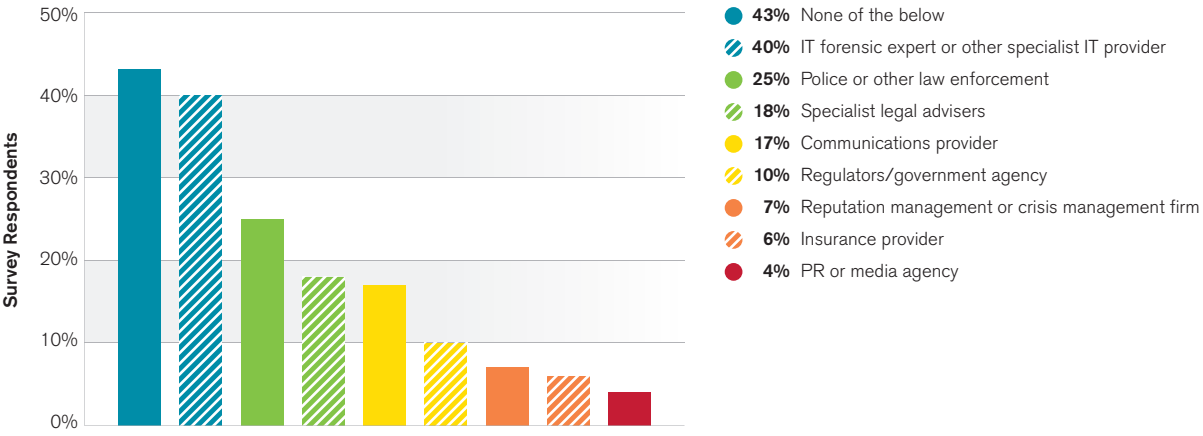


Figure 81 *Source: Arbor Networks, Inc.*

Looking at incident frequency over last year, 35 percent of respondents indicated an increase, and 52 percent indicated similar levels to last year (Figure 82). Only 14 percent reported a decrease in incidents. While still significant, this shows a more modest increase in incident frequency than seen from service provider organizations (Figure 38).

Incident Response Rate

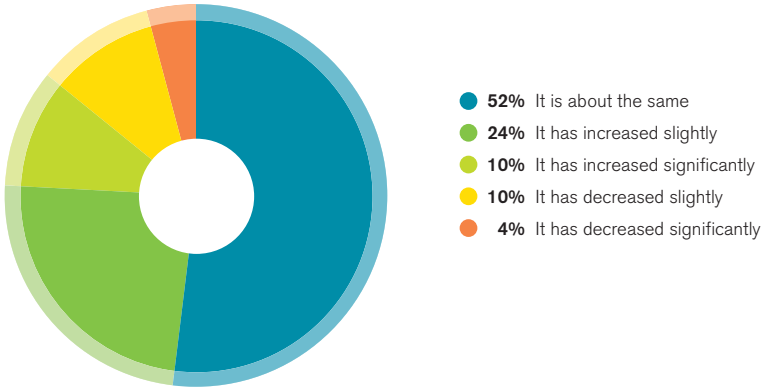


Figure 82 *Source: Arbor Networks, Inc.*

Similar to their service provider peers (Figure 6), nearly all enterprise, government and educational organizations indicated at least some level of incident response preparedness (Figure 83). Just under 50 percent feel reasonably or well-prepared, while 10 percent said they feel completely unprepared. It is disappointing to see over half of respondents feel underprepared, especially in light of the high-profile incidents that have taken place over the past year, including the recent breach of Sony Entertainment.

Incident Response Preparedness

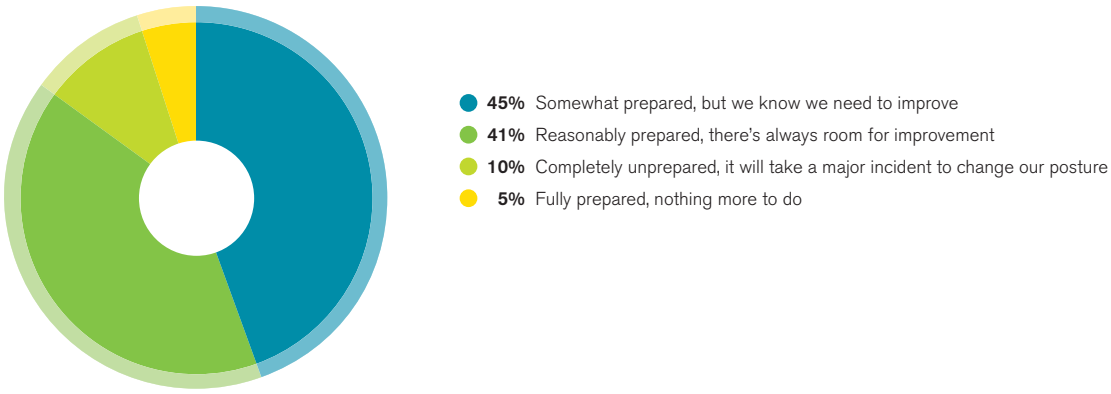


Figure 83 *Source: Arbor Networks, Inc.*

Looking at various ways to improve incident response, the most popular solution is to deploy more automated threat detection solutions (Figure 84), which was indicated by nearly 60 percent of respondents. This was followed closely by: reviewing and exercising incident handling plans more frequently; raising awareness of existing plans/preparations across the company; getting regular updates and intelligence on the potential threats to the company; and deploying solutions that speed up the incident response process—all of which were indicated by around half of the surveyed organizations. These results are nearly identical to those from the "Service Provider" section presented earlier in this report (Figure 39).

Incident Response Improvements

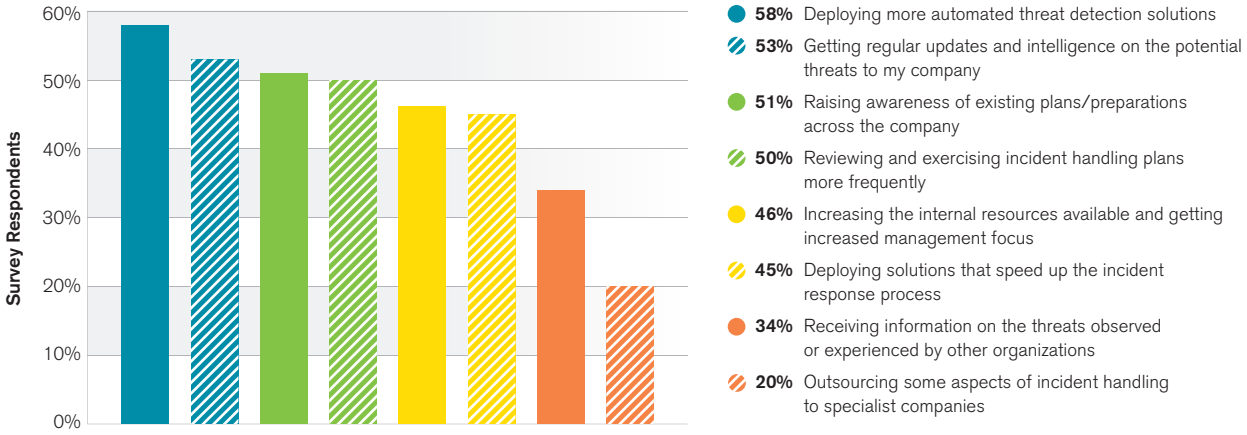


Figure 84 *Source: Arbor Networks, Inc.*

Firewalls/IPS/UTM systems and NetFlow analyzers are the most common threat detection mechanisms used by enterprise, government and educational organizations, which is also consistent with their service provider counterparts (Figure 40). In these verticals, a whopping 85 percent of respondents use these tools (Figure 85), compared to 70 percent of the service providers. It should also be noted that NetFlow analyzers—the number one choice for service providers on their corporate networks—are in second place among enterprise, government and educational organizations, with 20 percent fewer respondents using them. This may be due to the increased familiarity with NetFlow within service providers, who often use it to monitor their service-providing networks.

Internal Network Threat Detection Mechanisms

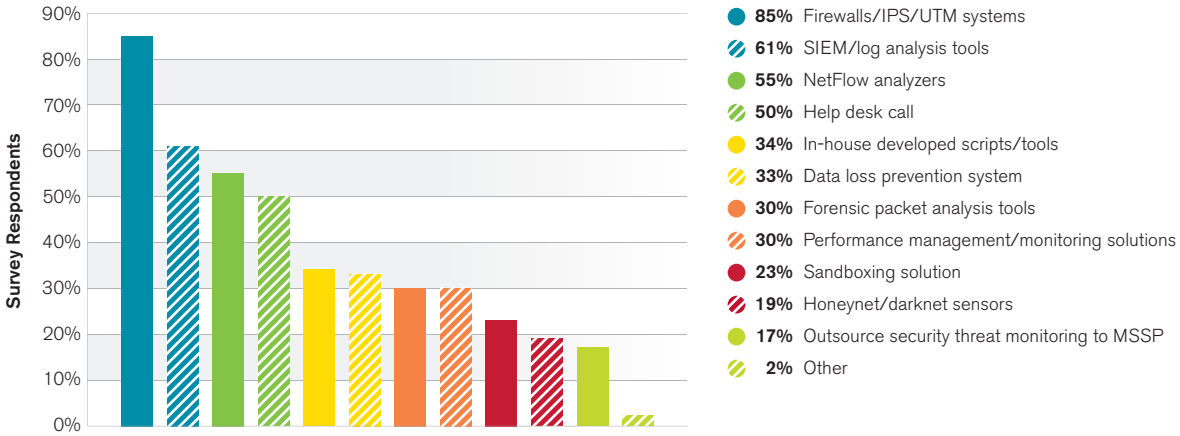


Figure 85 *Source: Arbor Networks, Inc.*

In addition to asking enterprise, government and educational organizations about the tools they have deployed for detecting incidents, we also asked how they have actually detected incidents historically. Automated detection using deployed security tools topped the list at 60 percent (Figure 86). Surprisingly, detection via routine checks/controls and manual detection via employees tied for second place, representing about half of respondents. Similar to the results in the service provider section, we find there are still many real world detections that are not initiated by the automated mechanisms deployed for that purpose.

Actual Detection Methods and Sources

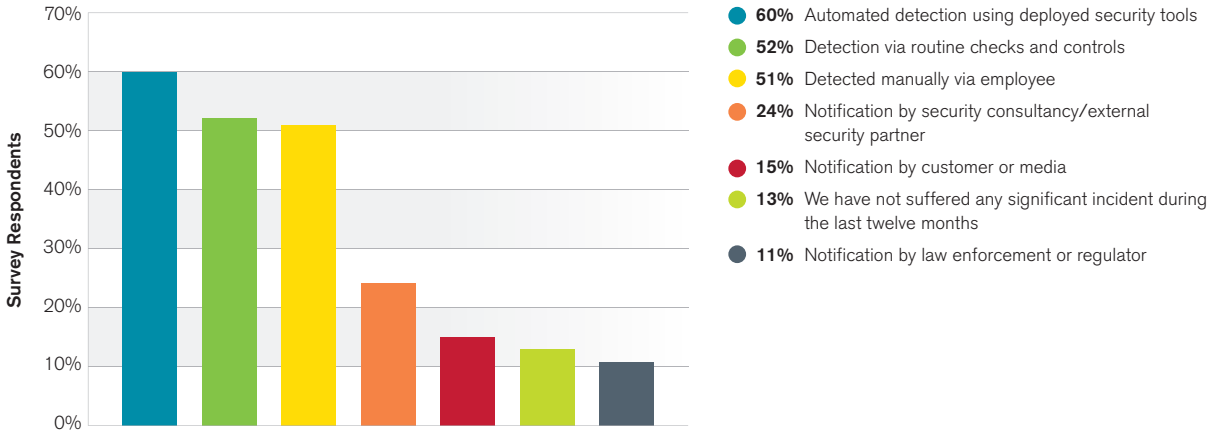


Figure 86 *Source: Arbor Networks, Inc.*

Regarding social media (Figure 87), 75 percent of organizations allow its use on their internal networks, but only 44 percent allow instant messaging. These numbers reflect a very similar posture to service providers' internal networks (Figure 43). Thirteen percent of respondents indicated that they actively block these applications. It is likely that concerns over social engineering exploits and data leakage have motivated this action.

Social Media on Internal Networks

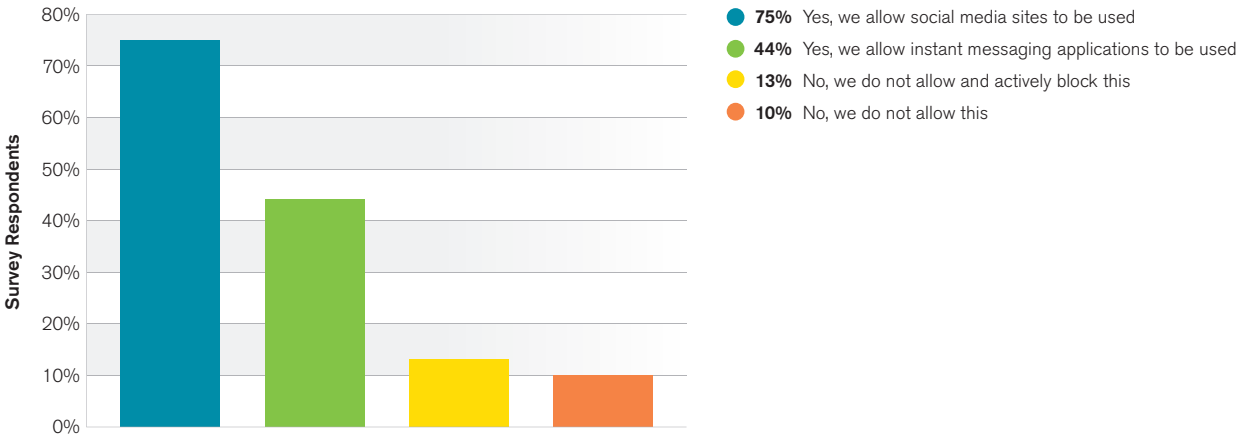


Figure 87 *Source: Arbor Networks, Inc.*

The percentage of enterprise, government and educational organizations allowing the use of personal devices (BYOD) on their internal networks is slightly lower at 62 percent, compared with 72 percent on service providers' internal networks (Figure 44). This is not surprising, as traditional enterprises and government tend to be more conservative on their internal IT practices.

Organizations must be able to identify employee-owned devices on their networks to control BYOD usage appropriately. However, 46 percent of the responding organizations still do not have ANY solution deployed to identify them (Figure 88). This is slightly higher than the service provider responses (Figure 45) documented earlier in this report. For organizations that do have visibility into employee-owned devices on their networks, the two most popular monitoring solutions are network access control and identity management systems, consistent with last year. The reported use of network-based posture assessment doubled this year to tie for third place at 22 percent, just as it did with service providers.

Identification of Employee-Owned Devices

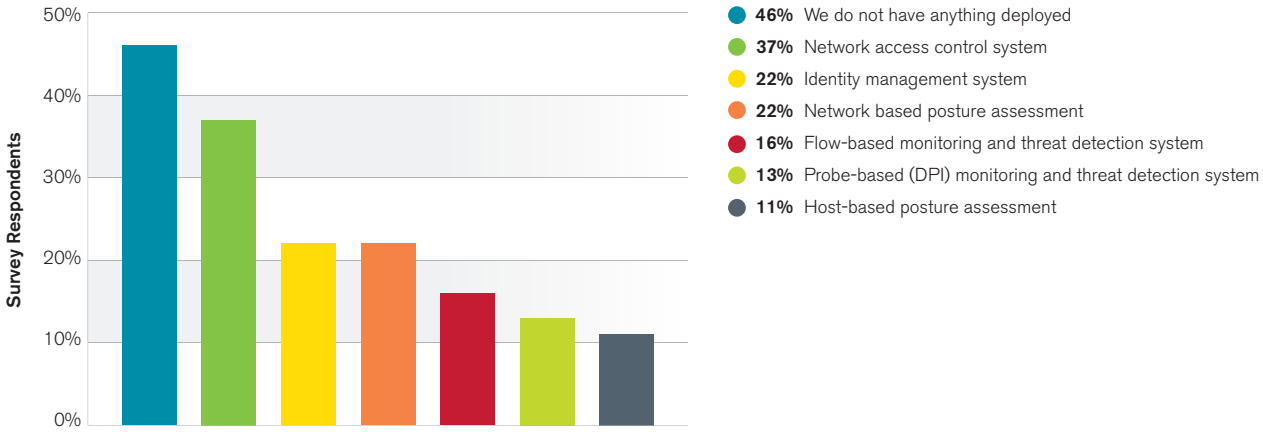


Figure 88 *Source: Arbor Networks, Inc.*

By their very nature, employee-owned devices are not always subject to the same levels of control as employer-provided equipment. It is encouraging that nearly two-thirds of organizations are only allowing these devices to have limited access to internal resources (Figure 89). However, the use of specific security policies and security software installed on devices is slightly lower than on service providers' internal networks (Figure 46). On a more positive note, the use of mobile device management is nearly double that seen in service providers, at 46 percent. These best current practices are trending positive this year with moderate gains.

BYOD Access Restrictions

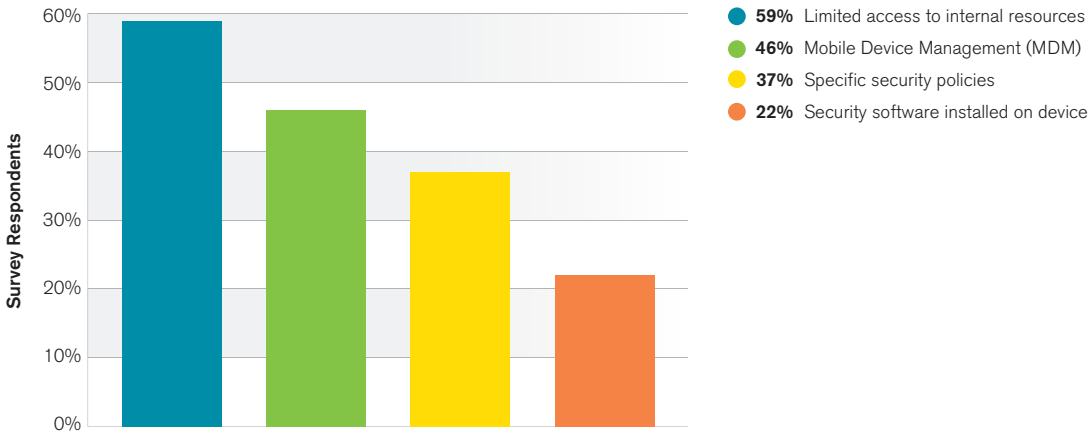


Figure 89 *Source: Arbor Networks, Inc.*

Over 60 percent of organizations do not allow the use of public cloud services to synchronize or back up data on employee-owned devices. This is consistent with last years' combined results, but a bit lower than this year's service provider results.

Certainly there are risks to allowing BYOD on a corporate network. Fortunately only 6 percent of respondents experienced a security breach that could be attributed to BYOD during the survey period (Figure 90). However, 33 percent of organizations indicated they still do not know if they had a security breach due to BYOD. This is not surprising given the continued lack of visibility into employee-owned devices in some organizations.

BYOD Security Breaches

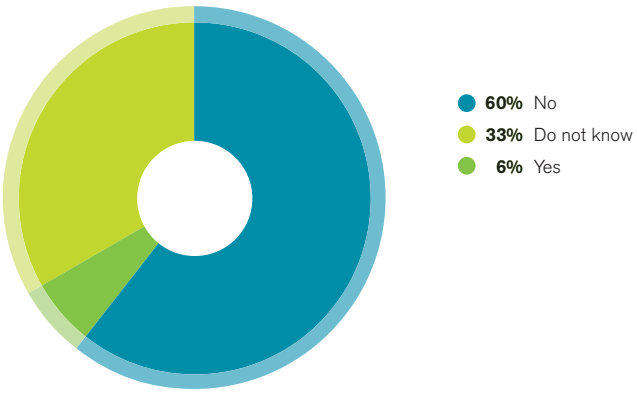
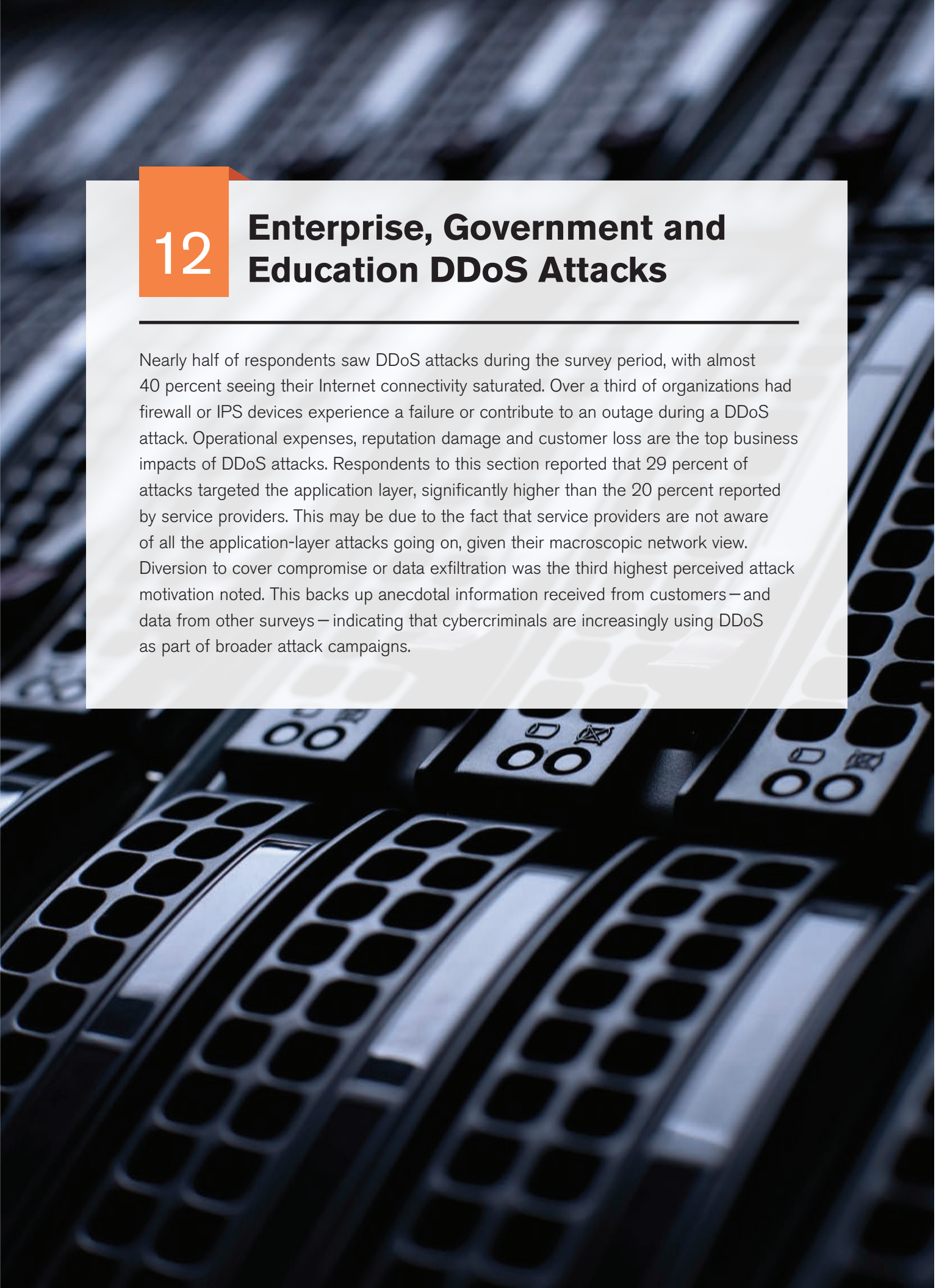


Figure 90 *Source: Arbor Networks, Inc.*



12 Enterprise, Government and Education DDoS Attacks

Nearly half of respondents saw DDoS attacks during the survey period, with almost 40 percent seeing their Internet connectivity saturated. Over a third of organizations had firewall or IPS devices experience a failure or contribute to an outage during a DDoS attack. Operational expenses, reputation damage and customer loss are the top business impacts of DDoS attacks. Respondents to this section reported that 29 percent of attacks targeted the application layer, significantly higher than the 20 percent reported by service providers. This may be due to the fact that service providers are not aware of all the application-layer attacks going on, given their macroscopic network view. Diversion to cover compromise or data exfiltration was the third highest perceived attack motivation noted. This backs up anecdotal information received from customers—and data from other surveys—indicating that cybercriminals are increasingly using DDoS as part of broader attack campaigns.

Forty-seven percent of the enterprise, government and educational organizations we surveyed reported experiencing DDoS attacks over the past year. Among those that did, 38 percent said the attacks exceeded their total Internet capacity.

Looking at the targets of the DDoS attacks (Figure 91), the majority are aimed at customer-facing services and applications. However, nearly half of respondents also indicated that they saw attacks targeting infrastructure such as routers, load balancers, firewalls and overall network bandwidth. This again reinforces the fact that attackers are more frequently targeting infrastructure if they note that services are well-defended.

Targets of DDoS Attacks

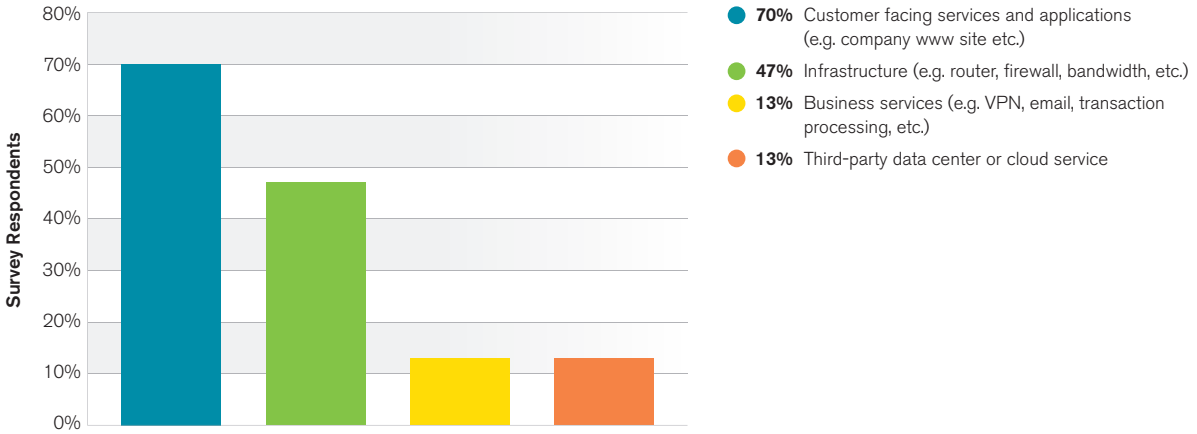


Figure 91 *Source: Arbor Networks, Inc.*

Thirty-five percent of organizations had firewall or IPS devices experience a failure or contribute to an outage during an attack (Figure 92). Firewalls offer a valuable layer in our defensive strategies, but they can become targets of DDoS attacks due to their stateful nature and need to be protected.

Firewalls and IPS Affected by DDoS Attacks

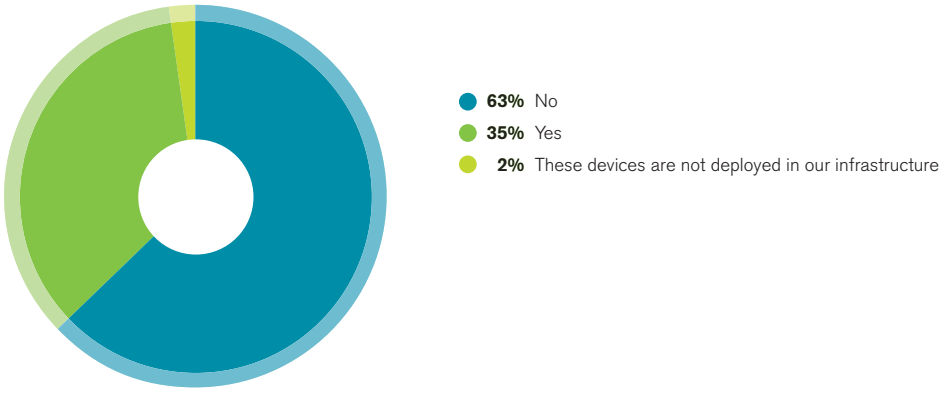


Figure 92 *Source: Arbor Networks, Inc.*

Concerning the duration of the longest DDoS attacks, the vast majority of organizations reported attacks lasting less than one day (Figure 93). This is almost identical to the results from our service provider respondents in terms of attack durations, as would be expected. Nearly 60 percent of organizations reported seeing attacks end in six hours or less. However, nearly a quarter reported attacks lasting longer than one day, while a few saw attacks continue for over a week.

DDoS Attack Duration

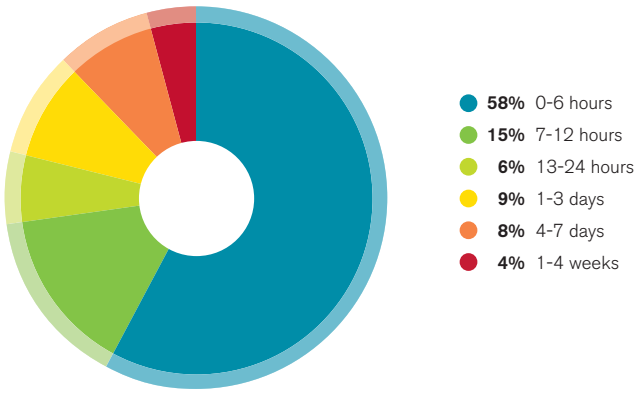


Figure 93 *Source: Arbor Networks, Inc.*

Organizations observed a number of different business impacts as a direct result of DDoS attacks. About half cited operational expenses (Figure 94) and nearly 40 percent indicated reputation damage or customer loss due to DDoS attacks. One-fifth indicated direct revenue loss, with other impacts including employee turnover and stock price fluctuation. The costs associated to DDoS attacks are multi-faceted, and organizations should factor all of these into their calculations when looking at their investment strategies for defensive solutions.

Business Impact of DDoS Attacks

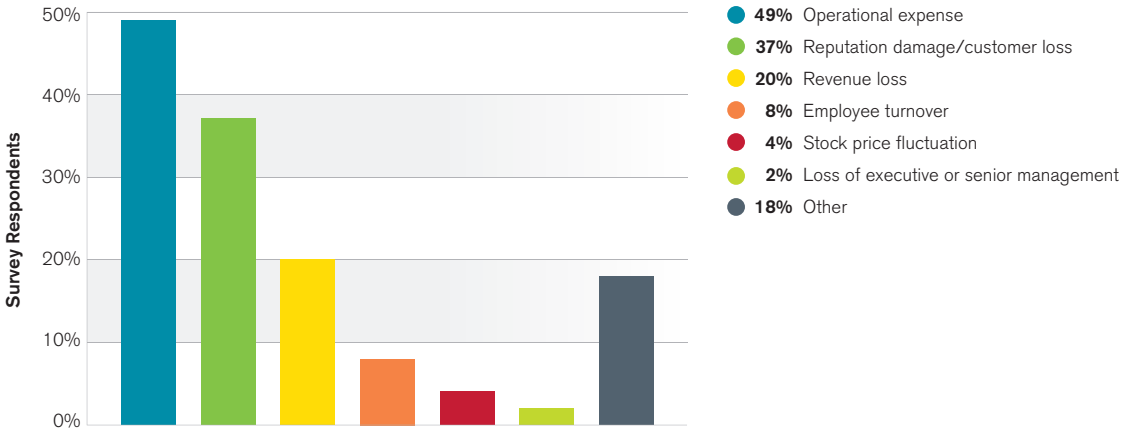


Figure 94 *Source: Arbor Networks, Inc.*

Looking at the types of attacks reported by organizations, half were volumetric in nature (Figure 95)—significantly less than the 65 percent reported by service providers. Meanwhile 29 percent of attacks targeted the application layer, significantly higher than the 20 percent reported by service providers. This may be due to the fact that service providers are not aware of all the application-layer attacks going on, given their macroscopic network view. This reinforces the need for a layered DDoS defense for enterprise, government and educational organizations.

Attack Category Breakout

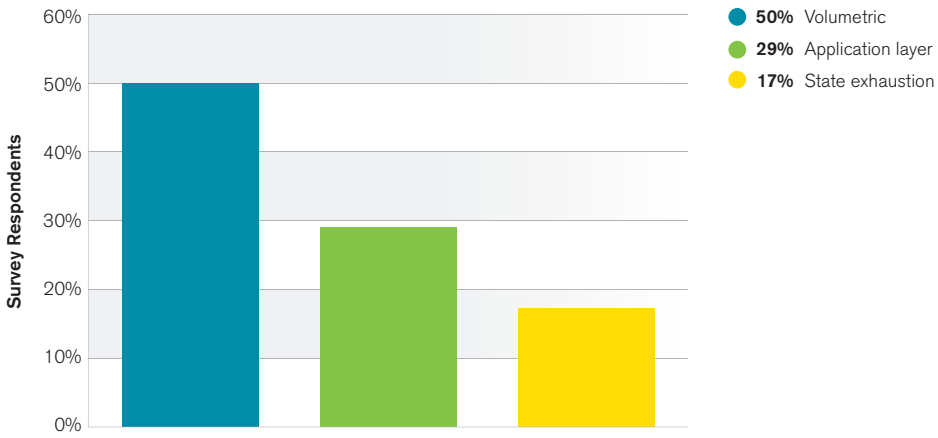


Figure 95 *Source: Arbor Networks, Inc.*

Application-layer attacks continue to primarily target web services and DNS. Over 80 percent of respondents saw attacks targeting HTTP (Figure 96), and nearly 60 percent saw attacks against HTTPS and DNS. As expected, these organizations are seeing an even higher proportion of attacks targeting web services (HTTP and HTTPS) than ISPs, given their more focused visibility. The "Other" category includes attacks against NTP and gaming ports such as 3074 (Xbox Live).

Targets of Application-Layer Attacks

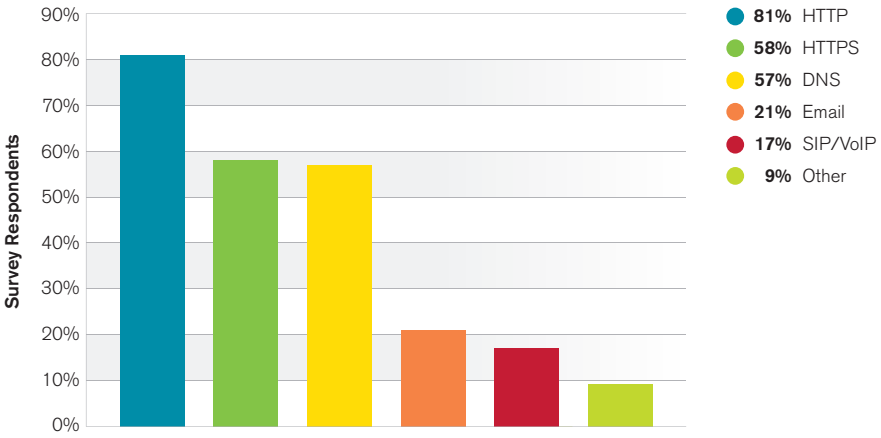


Figure 96 *Source: Arbor Networks, Inc.*

DDoS attacks targeting encrypted web services have become increasingly common in recent years. Nearly half of respondents observed volumetric attacks targeting UDP/TCP port 443 (Figure 97). Forty-two percent saw attacks targeting the encrypted service at the application layer—a much higher level than seen in our service provider responses. A higher proportion of respondents also saw attacks targeting the SSL/TLS protocol. The variation in results between end user and service provider respondents is, as noted above, likely due to the higher granularity of visibility available when the monitoring solution is closer to the services being attacked (and potentially has the ability to look inside encrypted traffic).

Encrypted Application-Layer Attacks

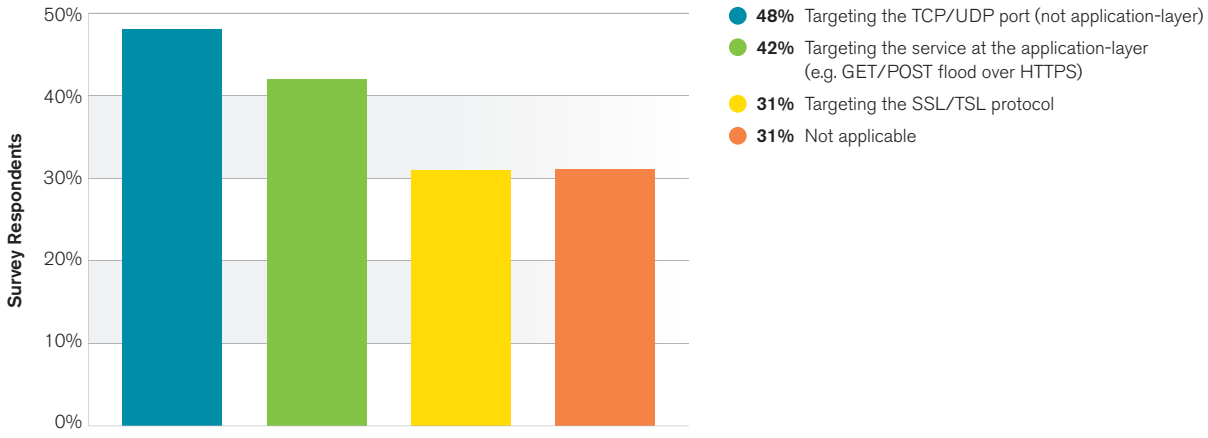


Figure 97 *Source: Arbor Networks, Inc.*

Multi-vector DDoS attacks combine multiple attack techniques concurrently, aimed at the same target, to increase both the attacker's chance of success and the mitigation complexity. Forty-two percent of respondents reported seeing multi-vector DDoS attacks in the past year (Figure 98)—an identical result to our service provider respondents.

Multi-Vector Attacks

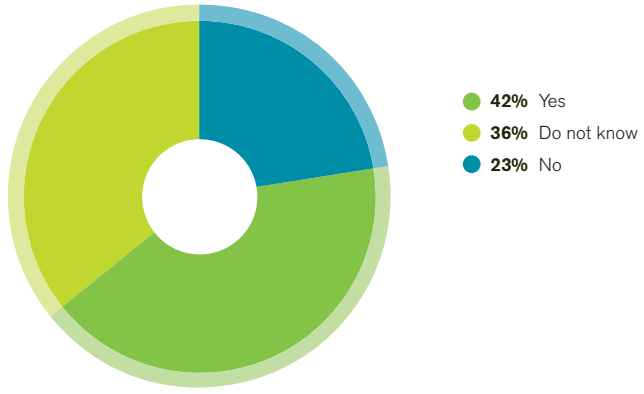


Figure 98 *Source: Arbor Networks, Inc.*

The motivations behind DDoS attacks continue to cover a wide and varied spectrum. As in past years, political and ideological concerns top the list (Figure 99), while vandalism or nihilism comes in a close second. Not far behind, in third place for enterprise/government/education respondents, is diversion to cover compromise or data exfiltration. This backs up anecdotal information received from customers—along with data from other surveys—indicating that attackers are increasingly using DDoS as a smoke screen for other criminal activity. Additionally, respondents reported the continued growth in criminal extortion, financial market manipulation and diversion to cover compromise or data exfiltration seen by our service provider respondents.

DDoS Attack Motivations

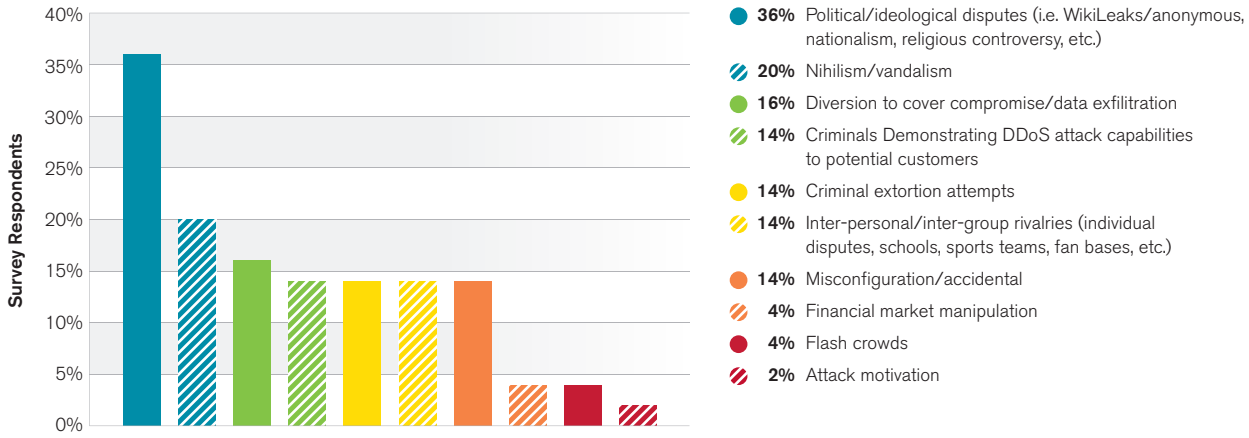


Figure 99 *Source: Arbor Networks, Inc.*

We asked enterprise, government and educational participants whether they have seen DDoS attacks against the cloud services they use. Twenty-five percent indicated that they have seen attacks, a similar level to that indicated by service providers (29 percent).

Regarding DDoS mitigation techniques deployed in enterprise, government and educational networks, firewalls are by far the most common mechanism (Figure 100), with 72 percent citing their use. Load balancers and access control lists are a close second and third, with just under half of organizations using them. This is unfortunate because firewalls and load balancers are known to be susceptible to state-exhaustion DDoS attacks, as evidenced by the 35 percent of respondents who saw their firewalls fail due to DDoS during the survey period. On a more encouraging note, about one-third indicated they are using either intelligent DDoS mitigation systems (IDMS) or cloud-based mitigation services to protect themselves. Only 26 percent reported having a layered DDoS mitigation strategy, which is the current best practice.

DDoS Mitigation Techniques

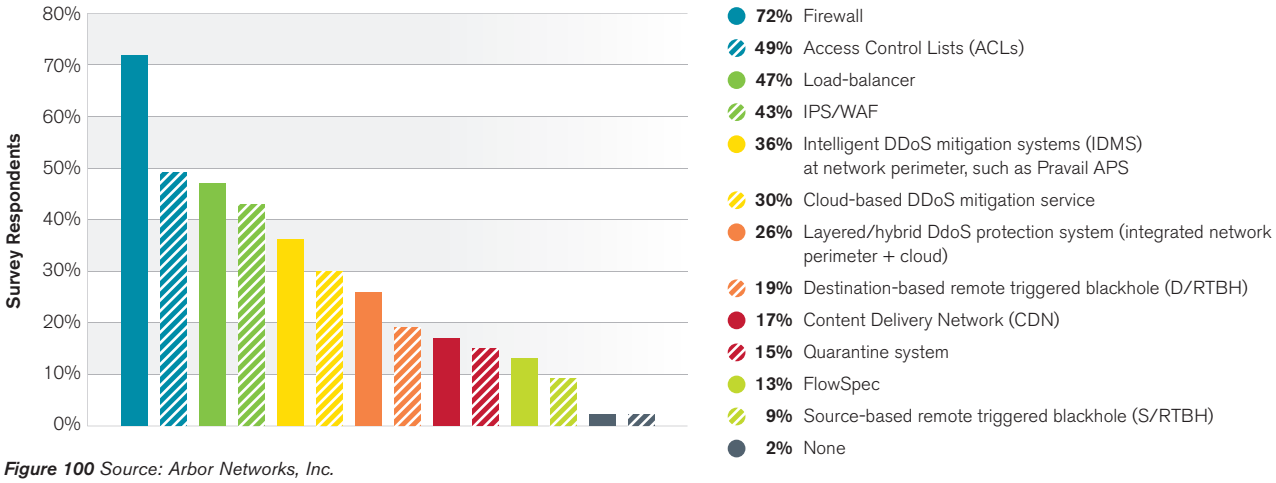


Figure 100 *Source: Arbor Networks, Inc.*

The time required to mitigate DDoS attacks is crucial, as this can be a key factor in the cost of an attack to an organization. Twenty-five percent of respondents indicated it takes more than 30 minutes to mitigate an attack (Figure 101). Only about 20 percent indicated they can stop the attack in less than 10 minutes. Interestingly 6 percent reported that they do not mitigate attacks. As more organizations become dependent on the Internet for business continuity, downtime becomes more costly. Reducing mitigation times and deploying proactive defenses are becoming increasingly important.

We asked enterprise, government and educational organizations if they can detect outbound or cross-bound attacks originating from their own networks. It was a pleasant surprise to learn that 57 percent of respondents now have this capability.

DDoS Attack Mitigation Time

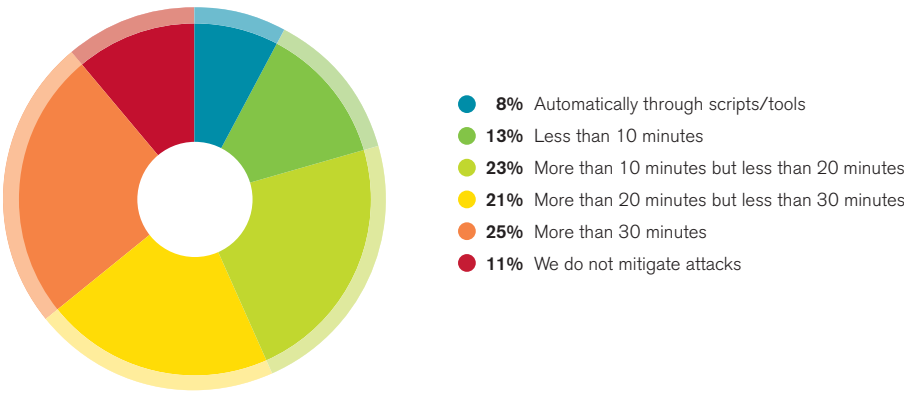
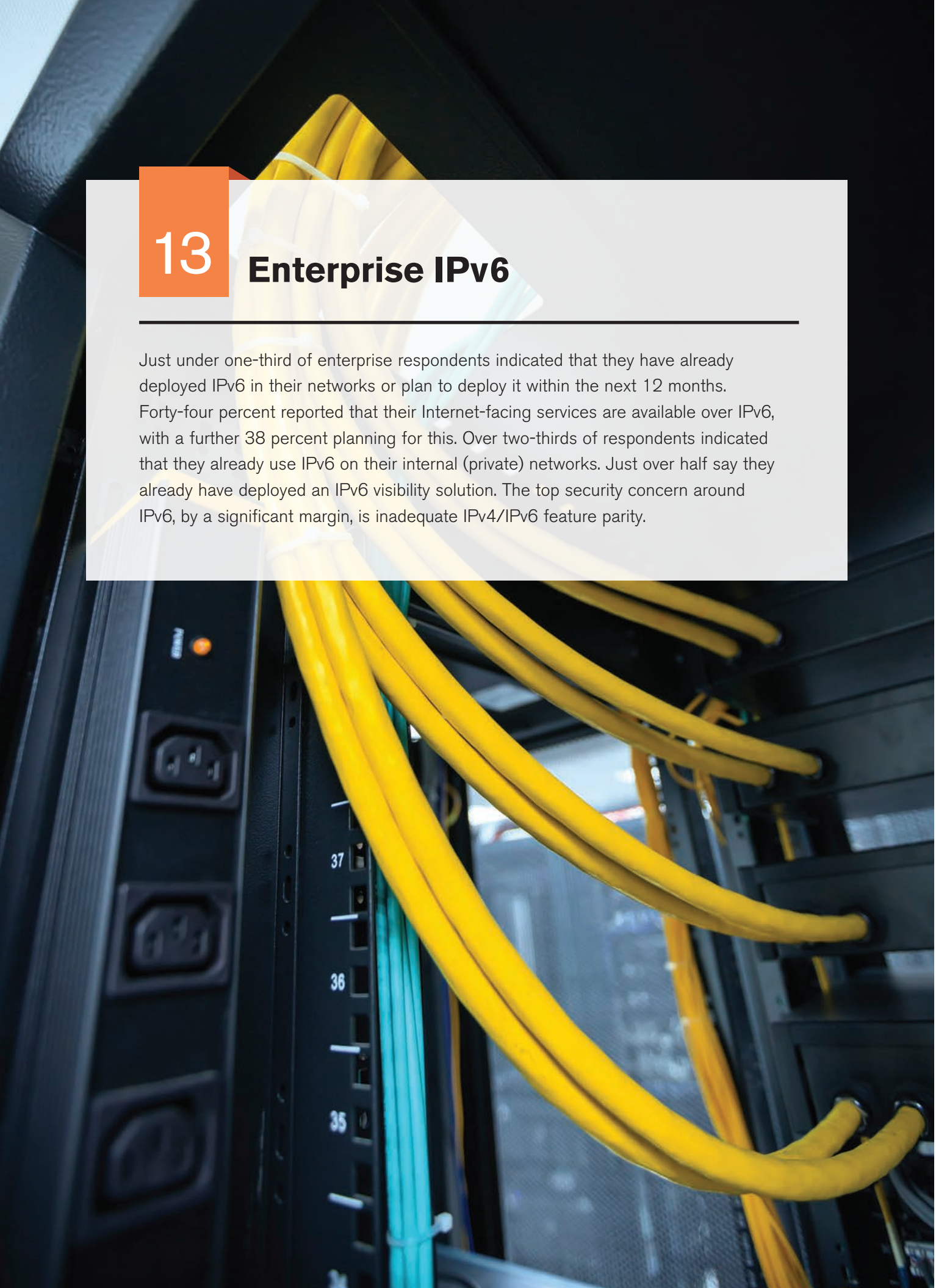


Figure 101 *Source: Arbor Networks, Inc.*



13 Enterprise IPv6

Just under one-third of enterprise respondents indicated that they have already deployed IPv6 in their networks or plan to deploy it within the next 12 months. Forty-four percent reported that their Internet-facing services are available over IPv6, with a further 38 percent planning for this. Over two-thirds of respondents indicated that they already use IPv6 on their internal (private) networks. Just over half say they already have deployed an IPv6 visibility solution. The top security concern around IPv6, by a significant margin, is inadequate IPv4/IPv6 feature parity.

Just under a third of enterprise respondents indicated that they have IPv6 deployed in their networks or plan to deploy it within the next 12 months. This is a much lower proportion than our service provider respondents. However, it does match the proportion of business customers who our service provider respondents see utilizing IPv6 services.

Looking at deployment progress, just over a quarter of enterprise respondents indicated that they have completed their IPv6 rollout, approximately the same level as seen in the service provider space. A further third have deployments in progress. Only 3 percent of respondents have no plans for IPv6. It will be interesting to see how deployments progress in next year's results.

This year 44 percent of enterprise respondents indicated that their Internet-facing services are available over IPv6, with a further 38 percent planning for this (Figure 102). This indicates that some organizations that have not yet completed their IPv6 deployments are already offering services on their infrastructure.

IPv6 Service Availability

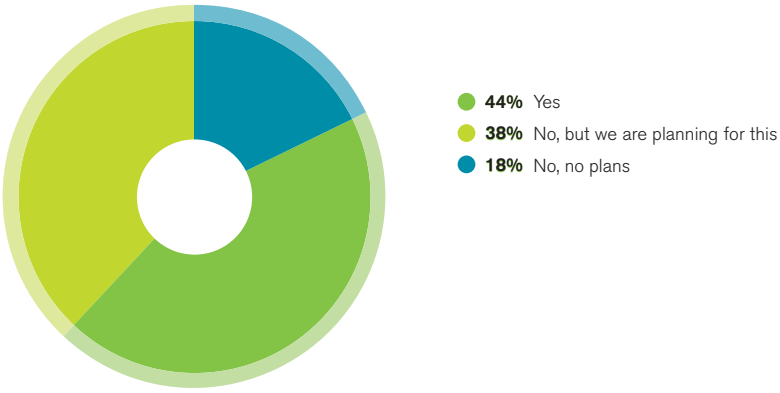


Figure 102 *Source: Arbor Networks, Inc.*

Over two-thirds of enterprise respondents indicated that they already use IPv6 on their internal (private) networks. This is a much higher percentage than we would have expected based on anecdotal information.

In terms of IPv6 traffic visibility, just over half of enterprise respondents have a solution deployed—a similar percentage to our service provider respondents. On the subject of IPv6 flow telemetry, only 30 percent have networking equipment with full support—a much lower result than in the service provider space (Figure 103). However, a quarter of respondents indicated that support is coming soon within their infrastructure. This may indicate that network equipment vendors have been slower to add IPv6 flow telemetry capabilities to enterprise-class products.

IPv6 Flow Telemetry

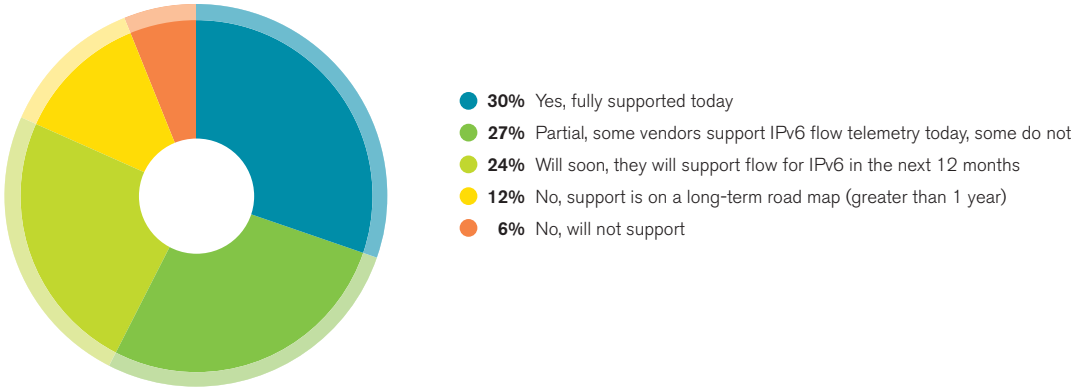


Figure 103 *Source: Arbor Networks, Inc.*

The top security concern around IPv6, by a significant margin, is inadequate IPv4/IPv6 feature parity, with DDoS and misconfiguration tied in second place (Figure 104). The level of concern around feature parity is MUCH higher among enterprise respondents compared to service providers. This may again indicate that network equipment vendors have been slower to add IPv6 features to enterprise-class products.

IPv6 Security Concerns

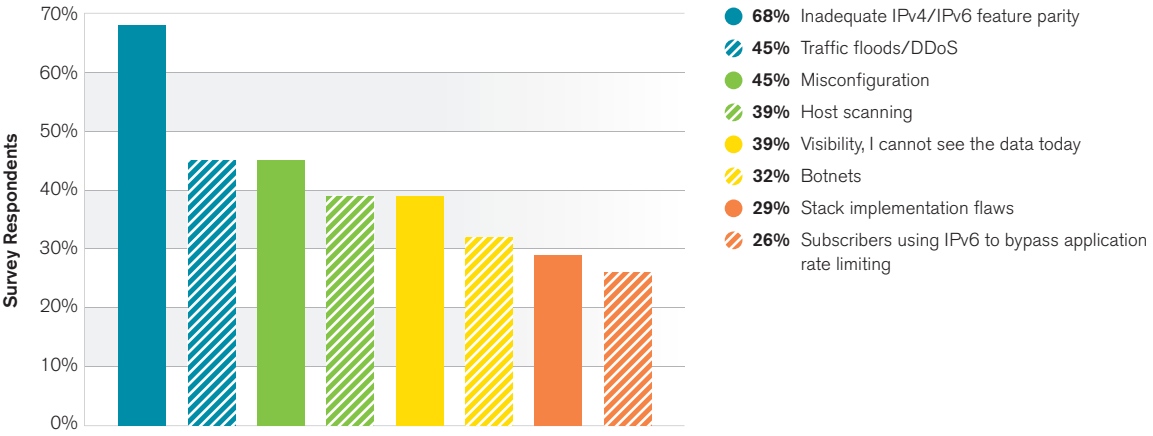


Figure 104 *Source: Arbor Networks, Inc.*

ARBOR + SIGCOMM

Measuring IPv6 Adoption

At the SIGCOMM 2014 research conference on networking, Arbor Networks—together with collaborators including the University of Michigan, the International Computer Science Institute, Verisign Labs and the University of Illinois—presented the results of a study designed to track developments in the ongoing rollout of IPv6.

The study examined a decade of data and reported on 12 measures drawn from different global-scale Internet data sets to compare IPv6 adoption relative to IPv4.

Seven Measures of IPv6 Adoption Over Five Years

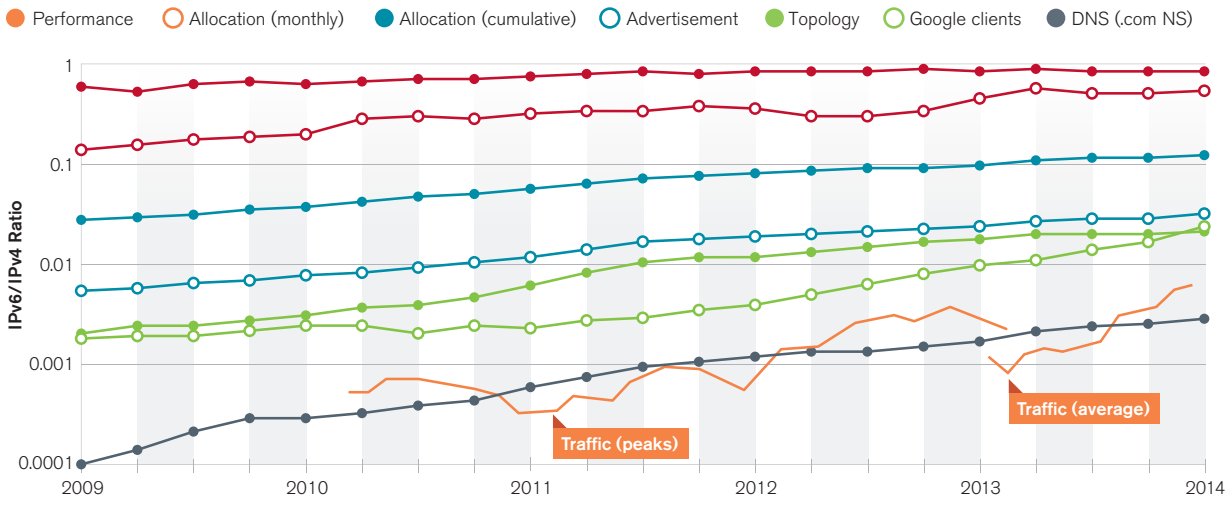


Figure SIG1 *Source: Arbor Networks, Inc.*

Highlights

1. IPv6 adoption relative to IPv4 varies by as much as two orders of magnitude (100x). Because of this, care must be taken when looking at individual measurements of IPv6.

2. The increase in IPv6 traffic relative to IPv4 over 2012 and 2013 has been phenomenal, growing more than 400 percent each year. However, it should be noted that IPv6 traffic levels are still just shy of 1 percent of IPv4 levels.

Traffic per Customer and Ratios for Peak and Average Datasets

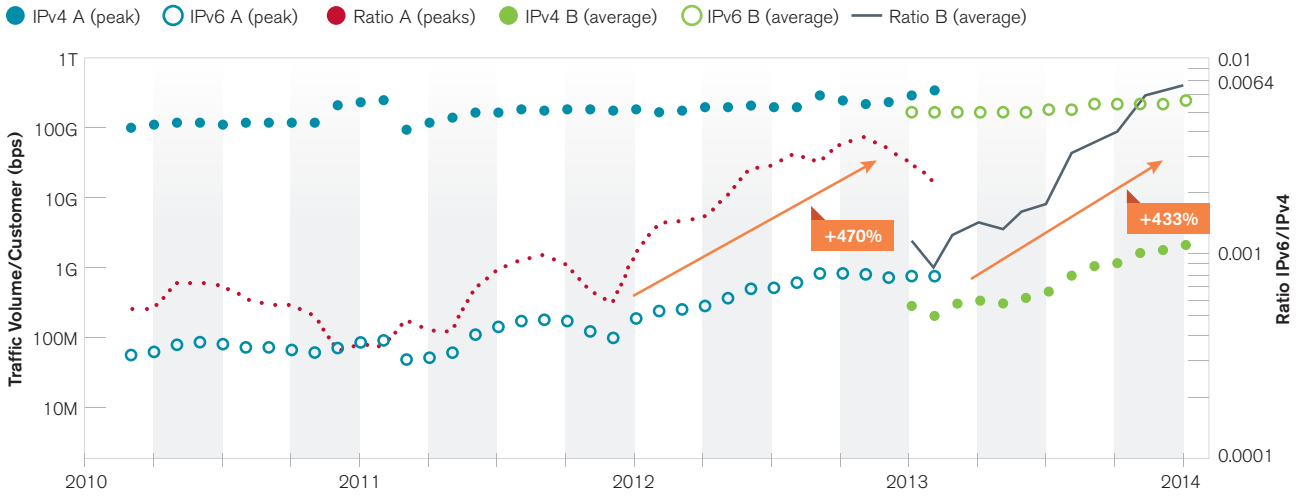


Figure SIG2 *Source: Arbor Networks, Inc.*

IPv6 Growth	IPv6 Status at End of:		
Operational Aspect Measured	**2010**	**2013**	
IPv6 percent of Internet traffic One year growth vs. IPv4 (March 2010-March 2011)	0.03% -12%	0.64% +433%	20x growth
Content's portion of traffic (HTTP + HTTPS)	6%	95%	15x growth
Native IPv6 packets vs. all IPv6 Native IPv6 Google clients	9% 78%	97% 99%	Traffic flipped
Performance: 10-hop RTT^{-1} vs. IPv4	75%	95%	Nearly on-par

Table 3 *Source: Arbor Networks, Inc.*

3 How people are using IPv6 has evolved immensely. IPv6 is now largely used natively and mostly for content, neither of which was the case just three years ago. The significant increase of HTTP and HTTPS traffic in the IPv6 application mix could correlate with a much broader increase of IPv6-connected end users accessing IPv6-enabled web servers.

Comparison of IPv6 Application Breakdown and Convergence at Similar Ratios as IPv4 Signaling Adoption

	2010	2013	
Application	IPv6	IPv6	IPv4
HTTP	5.61%	82.56%	60.61%
HTTPS	0.15%	12.66%	8.59%
DNS	4.75%	0.33%	0.22%
SSH	0.56%	0.27%	0.20%
RSYNC	20.78%	0.13%	<0.01
NNTP	27.65%	<0.01%	0.25%
RTMP	0.00%	<0.01%	2.74%
Other	40.50%	4.05%	27.39%

Table 4 *Source: Arbor Networks, Inc.*

4 The study also exposed differences in IPv6 deployment across global regions. This suggests that both the incentives and obstacles to adopt the new protocol vary in different parts of the world.

Regional IPv6 vs. IPv4 Ratios

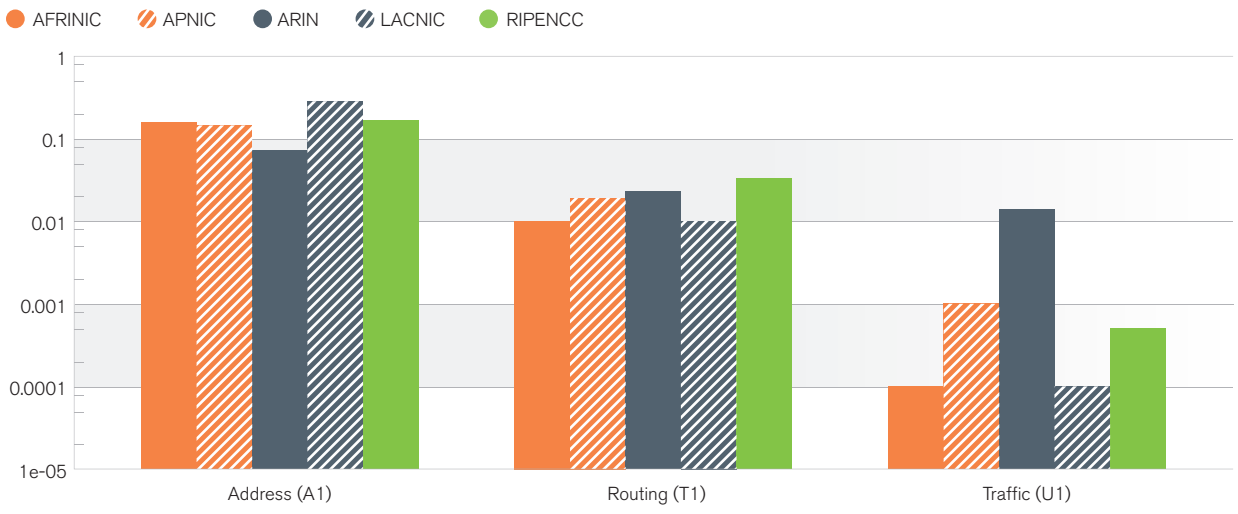
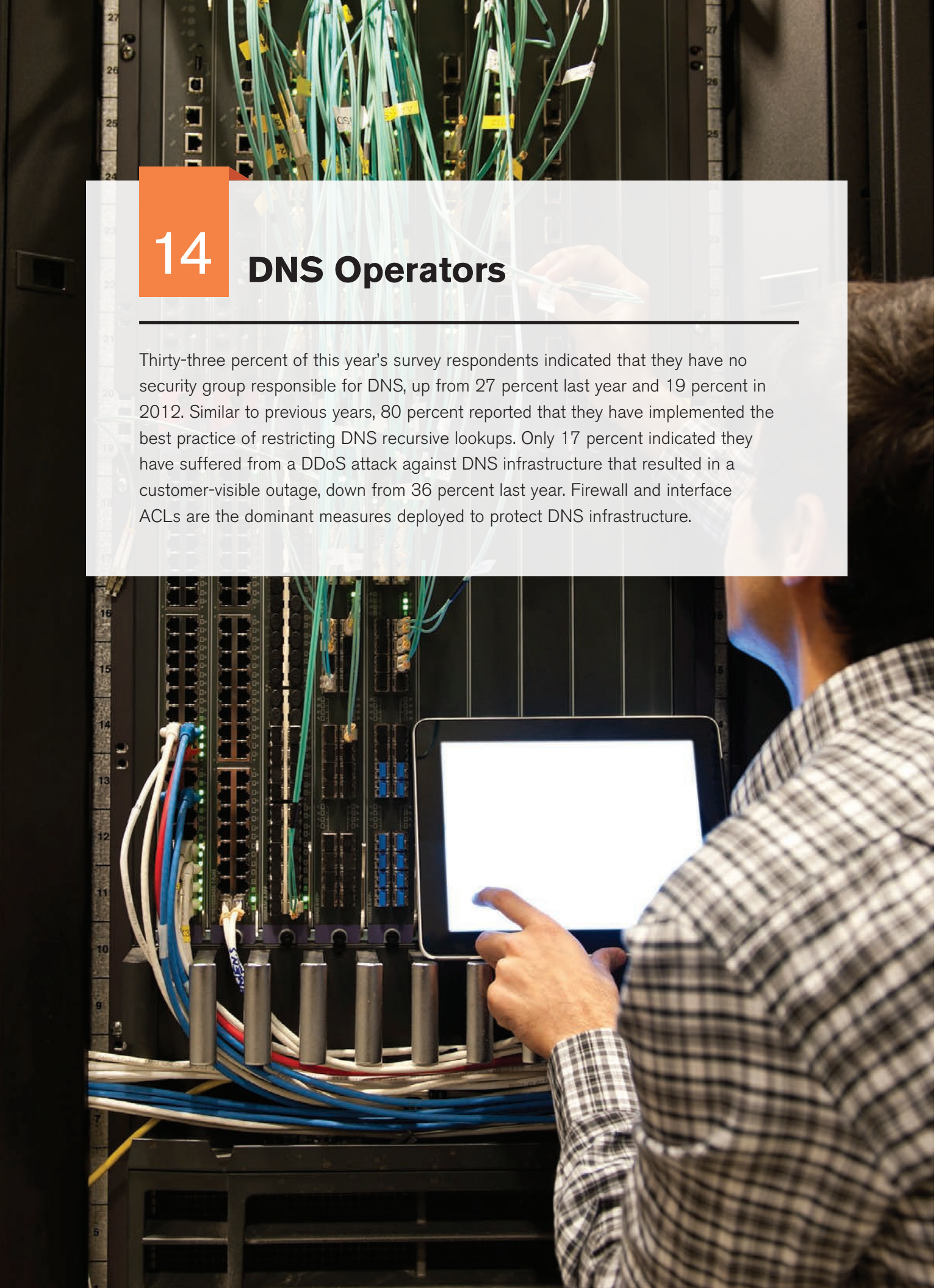


Figure SIG3 *Source: Arbor Networks, Inc.*

www.arbornetworks.com/asert/2014/08/ipv4-is-not-enough



14 DNS Operators

Thirty-three percent of this year's survey respondents indicated that they have no security group responsible for DNS, up from 27 percent last year and 19 percent in 2012. Similar to previous years, 80 percent reported that they have implemented the best practice of restricting DNS recursive lookups. Only 17 percent indicated they have suffered from a DDoS attack against DNS infrastructure that resulted in a customer-visible outage, down from 36 percent last year. Firewall and interface ACLs are the dominant measures deployed to protect DNS infrastructure.

Seventy-eight percent of this year's survey respondents operate DNS services in their networks. Last year we highlighted that the proportion of organizations with NO security group responsible for their DNS infrastructure was growing. This growth has continued, with 33 percent indicating they have no security group responsible for DNS, up from 27 percent last year and 19 percent in 2012 (Figure 105). This is not a good sign, given the fact that DNS is frequently exploited to carry out reflection/amplification attacks.

DNS Security Responsibility

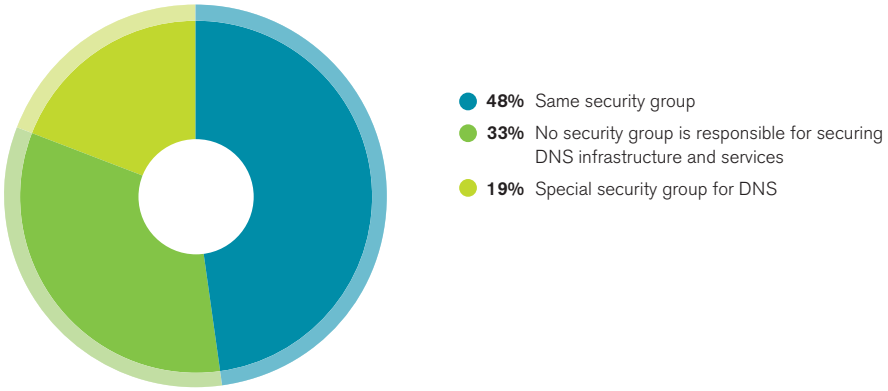


Figure 105 *Source: Arbor Networks, Inc.*

On the subject of DNS reflection attacks, 80 percent of respondents have implemented the best practice of restricting DNS recursive lookups. This looks good at first glance. However, it is an almost identical result to previous surveys, so little progress is being made in reducing the availability of infrastructure that attackers can leverage. The percentage with visibility into DNS traffic at Layers 3/4 dropped to 56 percent, compared with 67 percent last year. On a more positive note, visibility at Layer 7 has improved slightly, from 37 percent last year to 41 percent this year (Figure 106).

DNS Traffic Visibility

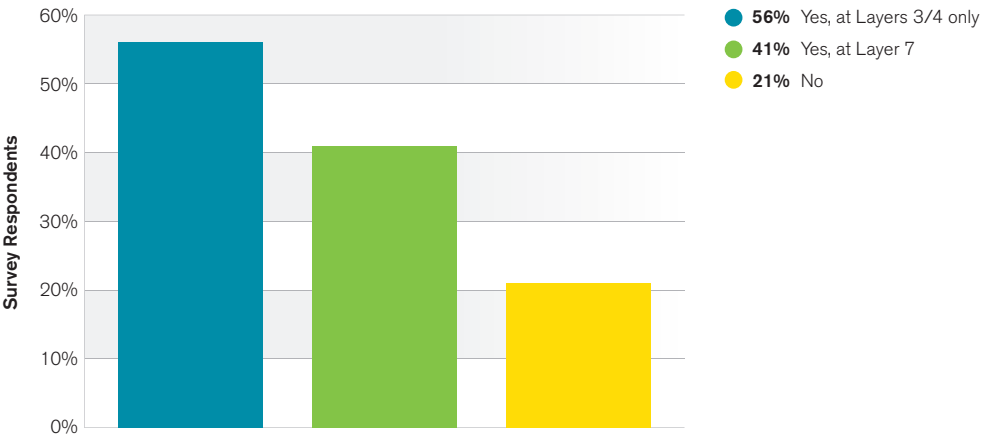


Figure 106 *Source: Arbor Networks, Inc.*

Only 17 percent of respondents indicated that they have suffered a customer-visible outage from a DDoS attack against their DNS infrastructure this year. This is a massive drop from 36 percent of respondents last year. It may be the result of better DNS protection, but could also be due to the shift toward other reflection/amplification protocols this year (e.g., NTP and SSDP).

Consistent with the above, the proportion of respondents seeing attacks toward either authoritative or recursive DNS servers has dropped significantly compared to last year—down to 21 percent and 15 percent respectively, from 35 percent and 23 percent (Figure 107 and 108).

Attacks Targeting Authoritative Servers

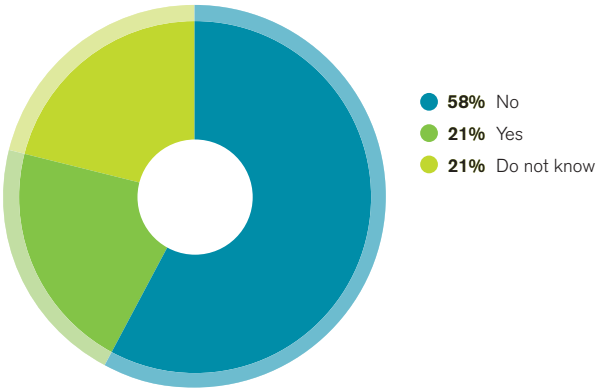


Figure 107 *Source: Arbor Networks, Inc.*

Attacks Targeting Recursive Servers

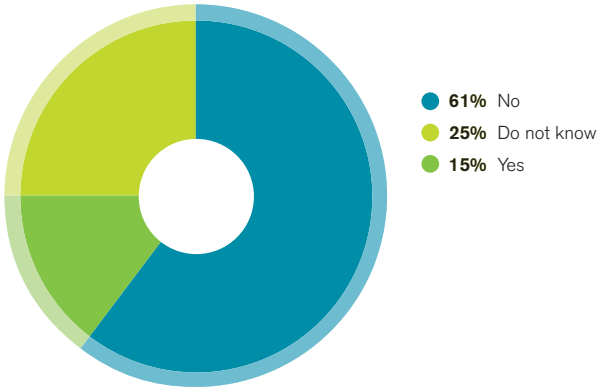


Figure 108 *Source: Arbor Networks, Inc.*

Firewall and interface ACLs are the dominant measures deployed to protect DNS infrastructure (Figure 109). There appears to have been significant growth in the proportion of respondents using firewalls for this purpose, up from 56 percent last year to 70 percent this year. This is a concern, especially when we consider that the use of IDMS to defend DNS infrastructure has dropped from 56 percent to 42 percent during that same period.

DDoS Protection Mechanisms

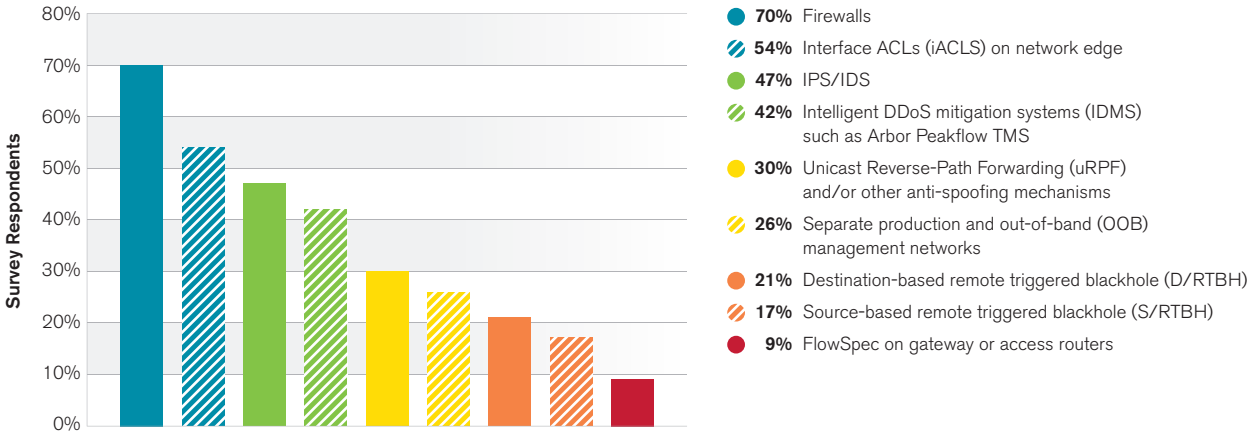


Figure 109 *Source: Arbor Networks, Inc.*

The responses around DNSSEC are very similar to those observed in previous years. Slightly less than half reported they do not observe any issues with DNSSEC functionality due to a lack of EDNS0 and/or TCP/53 DNS support on the Internet. However, as last year, just over a third reported not having enough visibility to determine whether this has caused any issues. Interestingly the percentage of respondents who have experienced greater impact from DNSSEC-related DNS reflection/amplification attacks has fallen from 26 percent last year to 19 percent.

15 Organizational Security Practices

The proportion of respondents implementing BCP 38/84 anti-spoofing has dropped from 51 percent last year to 37 percent this year. The use of anti-spoofing filters at the Internet edge is the primary way to prevent reflection/amplification DDoS attacks, so it was expected that the use of anti-spoofing would have gone up. The number of organizations that practice DDoS attack and defense simulations continued decreasing this year to only 34 percent (Figure 26), a significant reduction from 45 percent last year and 49 percent in 2012. A meaningful improvement was observed in proactively blocking traffic to known botnet command and control (C&C) servers. Participation in closed or vetted global OPSEC groups is broadly similar to last year's result, with a small drop from 39 percent to 36 percent.

The proportion of respondents following the best infrastructure-related security practices seems to have fallen across the board this year. The only exception is the use of Generalized TTL Security Measures (GTSM), which has stayed roughly the same (Figure 110). The drop in the use of best practices is highly concerning.

Implementation of BCP 38/84 anti-spoofing has dropped from 51 percent to 37 percent year over year. Knowing that the lack of anti-spoofing filters at the Internet edge is one of the key reasons why reflection/amplification DDoS attacks are possible, we expected that BCP 38/84 implementation would increase and not decrease. Given the storm of these attacks seen this year, this is bad news.

Also falling again this year is the proportion of respondents with a separate out-of-band management network. Having a separate network to monitor and control key infrastructure is hugely important, so it is troubling that more organizations have not been implementing this.

Infrastructure Best Current Practices

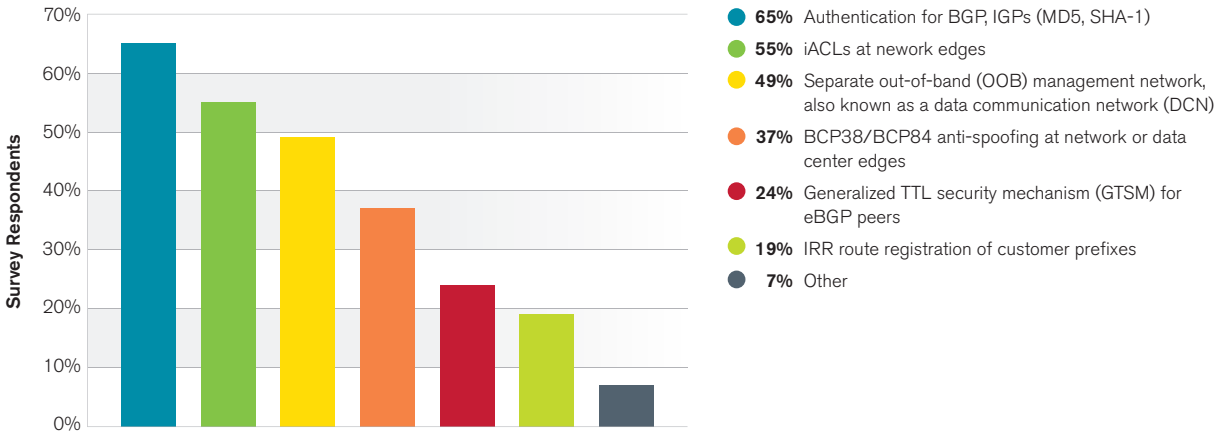


Figure 110 *Source: Arbor Networks, Inc.*

The old adage "practice makes perfect" is still applicable today, especially when we look at incident handling. For organizations to effectively deal with DDoS attacks, they need to have both defined processes and familiarity with those processes. The proportion of respondents who practice DDoS attack and defense simulations continued decreasing this year to only 34 percent (Figure 111), a significant reduction from 45 percent last year and 49 percent in 2012. However, this year saw a significant increase in those who are planning attack and defense simulations, up from 2 percent to 19 percent.

DDoS Attack Simulations

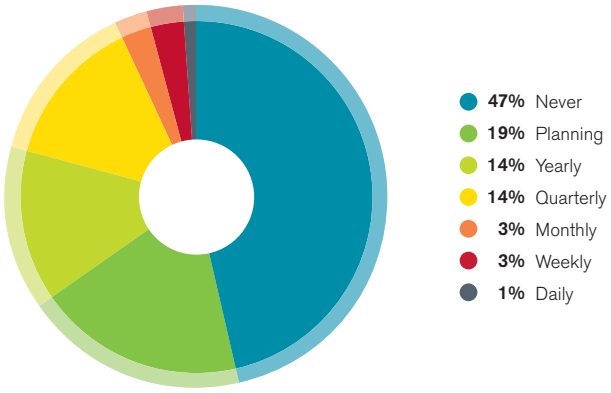


Figure 111 *Source: Arbor Networks, Inc.*

Things are significantly worse this year in the area of routing security precautions. Only 48 percent of organizations explicitly filter their customers' route announcements, a huge drop from 81 percent last year and 76 percent in 2012 (Figure 112). It is unclear why this drop has occurred. Similarly the percentage of respondents who monitor for route hijacking decreased substantially from last year—from 52 percent to 40 percent (Figure 113).

On a more positive note, we observed a meaningful improvement this year in the proportion of respondents who proactively block traffic to known botnet C&C servers, malware drop sites, etc. This year 56 percent block this traffic—a marked rise from the 38 percent seen in each of the last two reports.

Participation in closed or vetted global OPSEC groups is broadly similar to last year's result, with a small drop from 39 percent to 36 percent. Eighty-three percent indicated that they believe these groups are highly effective in handling OPSEC issues on an inter-organizational basis. Given this belief—together with the broadly held view in the OPSEC community that information sharing needs to improve to counter current threats—it is surprising that the participation levels in these groups does not seem to be increasing.

BGP Route Filtering

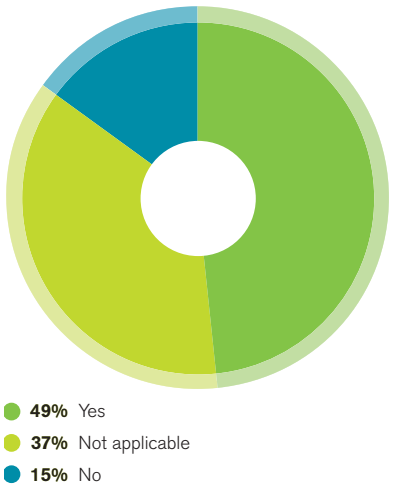


Figure 112 *Source: Arbor Networks, Inc.*

Route Hijack Monitoring

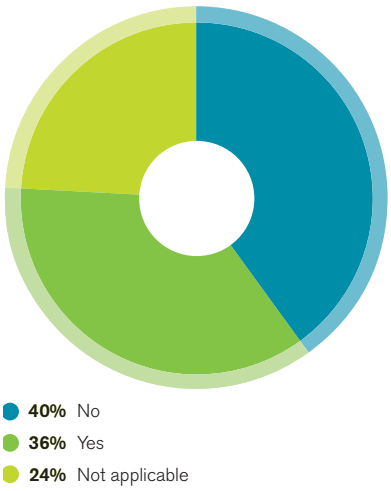


Figure 113 *Source: Arbor Networks, Inc.*

The primary reasons cited for preventing participation in these groups are the lack of time or resources (Figure 114). Unfortunately, this has been consistent over the last few years.

Participation in OPSEC Community

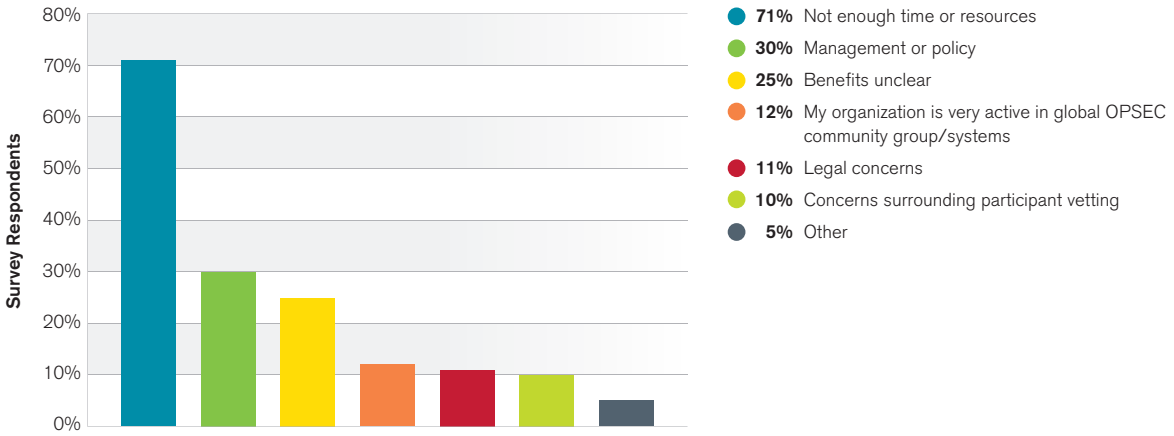


Figure 114 *Source: Arbor Networks, Inc.*

Just under three-quarters of respondents indicated that their OPSEC team maintains current contact information for key OPSEC resources and/or other empowered groups within their peer, transit provider and customer organizations. This is slightly lower than last year, which in turn was lower than the year before. Maintaining up-to-date contact information for OPSEC teams is of paramount importance, especially with DDoS attack sizes growing rapidly, as this makes it more likely that multiple organizations will need to be involved in any mitigation effort.

CONCLUSION

Arbor has conducted the worldwide infrastructure security survey for the last 10 years, and has had the privilege of tracking the evolution of the Internet and its uses from the early adoption of online content to today's hyper-connected society. We've witnessed an explosion in the volume of traffic, variety of applications and number of connected devices—along with significant changes in the threat landscape.

When we conducted our first survey in 2004, the corporate world was on watch for self-propagating worms like Slammer and Blaster that had devastated networks the year before. Back then data breaches were most likely carried out by employees who had direct access to data files. Today's organizations have a much wider and more sophisticated range of threats to worry about—and a much broader attack surface to defend.

Attackers now have access to tool kits that allow them to easily use and customize a variety of mechanisms to achieve their goals. Localized cybercriminals and script kiddies have given way to organized crime, cyber enterprises and nation states. Use of the Internet is now ubiquitous, with cloud services becoming the backbone of many companies. Social media has flourished, and our personal information has become more widely available. The business impact of a successful DDoS attack or breach can be devastating. Clearly the stakes are much higher now.

As the threat landscape has evolved, so has the survey behind this report. Over 280 network operators participated in this year's report, representing a wide spectrum of geographies and business focuses. This diversity gives the report sufficient representation from various areas of interest to produce statistically relevant data. For instance, we are able to compare and contrast results from both service provider and enterprise respondents—pointing out areas where they are similar and where they are different. We can also report from the point of view of datacenter and mobile network operators—pointing out areas of strength and weakness.

With a total of 182 questions, this year's survey is longer than in previous years. This allows us to continue exploring year-over-year trends in some of the existing threat and defense areas, while exploring new technologies and areas of interest. Even though the survey uses logic to limit the questions presented to each participant, we recognize that it is quite a long survey to take. We would like to thank each and every respondent who took the time to fill it out. The quality of the report would not be there without you.

The results of the survey are, as always, quite interesting. In many areas, the results are consistent with those of previous years—or they follow a consistent trend. For instance, the size and frequency of DDoS attacks continue to grow, with the mechanisms used and motivations behind them becoming more diverse. Some respondents continue to use state-dependent tools such as firewalls in their DDoS defenses, despite data spanning years that shows this approach is not effective.

In other areas of the survey, the results are markedly different from previous years. For example, the application of best practices for defense, the proportion of respondents who practice incident response regularly, the use of intelligent DDoS mitigation systems (IDMS) in data centers and the growth of IPv6 show quite different results year over year.

Our goals in conducting the survey and generating this annual report are to educate the broader community on the threats that are out there, and to provide a forum for sharing how today's service providers and end-user organizations are dealing with them. We hope that you have found this report interesting and educational. More importantly we hope that it will drive positive change in the security posture of network operators.

About the Authors

Darren Anstee, Director, Solutions Architects, Arbor Networks

danstee@arbor.net

Darren Anstee has 20 years of experience in pre-sales, consultancy and support for telecom and security solutions. As director of solutions architects at Arbor Networks, Darren works across the research, strategy and pre-sales aspects of Arbor's traffic monitoring, threat detection and mitigation solutions for service providers and enterprises around the world. Prior to joining Arbor, he spent over eight years working in both pre- and post-sales for core routing and switching product vendors.

C.F. Chui, Solutions Architect, APAC, Arbor Networks

cfchui@arbor.net

With more than 20 years of experience in the networking industry, C.F. Chui is a veteran in designing, implementing and supporting highly available network systems and solutions. In his current role with Arbor Networks, C.F. works closely with customers in the Asia Pacific region to develop and optimize approaches for their network security solutions to ensure the most effective deployment and highest customer satisfaction. He is also actively involved in Arbor's global research projects.

Before joining Arbor, C.F. held different regional positions in pre- and post-sales for various large core routing and switching vendors. His expertise lies mainly in the areas of Internet routing technology, network threat detection and network visibility solutions.

Jorge Escobar, Solutions Architect, Americas, Arbor Networks

jescobar@arbor.net

Jorge Escobar is a solutions architect for Arbor Networks, with a main focus on mobile network operators and global strategic alliances. Jorge has over 17 years of experience in the networking and telecom industries, where he has held different positions in network implementation, technical consultancy, business development and senior management. After spending the last seven and half years with Cisco Systems, he joined Arbor last year. Jorge plays a key role in expanding Arbor's network security leadership into the mobile space, as well as leading all technical engagements with Arbor's strategic partners around the world.

Gary Sockrider, Solutions Architect, Americas, Arbor Networks

gsockrider@arbor.net

Gary Sockrider is Arbor Networks' solutions architect for the Americas. He seeks to understand and convey the constantly evolving threat landscape, as well as the techniques and solutions that address them. Gary is an industry veteran with 25 years of broad technology experience, ranging from routing and switching to network security, data center and collaboration. Prior to joining Arbor, he spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless Communications.

Glossary

A

ACL Access Control List
APT Advanced Persistent Threat
ASERT Arbor Security Engineering & Response Team
ATLAS Active Threat Level Analysis System
AV Anti-Virus

B

BCP Best Current Practice
BGP Border Gateway Protocol
BYOD Bring Your Own Device

C

C&C Command-and-Control
CGN Carrier Grade NAT

D

DDoS Distributed Denial of Service
DNS Domain Name System
DNSSEC Domain Name System Security Extensions
D-RTBH Destination-based Remotely Triggered Blackholing
S-RTBH Source-based Remotely Triggered Blackholing

E

EDNS0 Extension Mechanisms for DNS

G

Gbps Gigabits-per-second
Gi Global Internet

H

HOIC High Orbit Ion Cannon
HTTP Hypertext Transfer Protocol
HTTP/S HTTP Secure

I

IAAS Infrastructure As A Service
iACL Infrastructure ACL
ICMP Internet Control Message Protocol
IDMS Intelligent DDoS Mitigation System
IDS Intrusion Detection System
IPS Intrusion Prevention System
IPv4 Internet Protocol version 4
IPv6 Internet Protocol version 6

K

KPI Key Performance Indicator

L

LOIC Low Orbit Ion Canon
LTE Long Term Evolution

M

Mbps Megabits-per-second
MDM Mobile Device Management
MPC Mobile Packet Core

N

NAT Network Address Translation
NMS Network Management System

O

OPSEC Operational Security
OTT Over the Top

P

PAT Port Address Translation

Q

QoE Quality of Experience

R

RAN Radio Access Network

S

SEG Security Gateways
SIEM Security Information Event Management
SLA Service Level Agreement
SMTP Simple Mail Transfer Protocol
SNMP Simple Network Management Protocol
SOC Security Operations Center
SPF Sender Policy Framework
S/RTBH Source-based Remotely Triggered Blackholing
SYN Synchronize

T

TCP Transmission Control Protocol
Tbps Terabits per second

U

UDP User Datagram Protocol
uRPF Unicast Reverse Path Forwarding

V

VoIP Voice over Internet Protocol
VPN Virtual Private Network

W

WAN Wide Area Network
WiMAX Worldwide Interoperability for Microwave Access


ARBOR NETWORKS
WORLDWIDE INFR
10
YEARS
ECUR

Corporate Headquarters

76 Blanchard Road
Burlington, MA 01803 USA

Toll Free USA +1 866 212 7267
T +1 781 362 4300

North America Sales

Toll Free +1 855 773 9200

Europe

T +44 207 127 8147

Asia Pacific

T +65 68096226

www.arbornetworks.com

ARBOR® NETWORKS

SR/WISR2014/EN/0115-LETTER