NETSCOUT
Guardians of the Connected World | Arbor

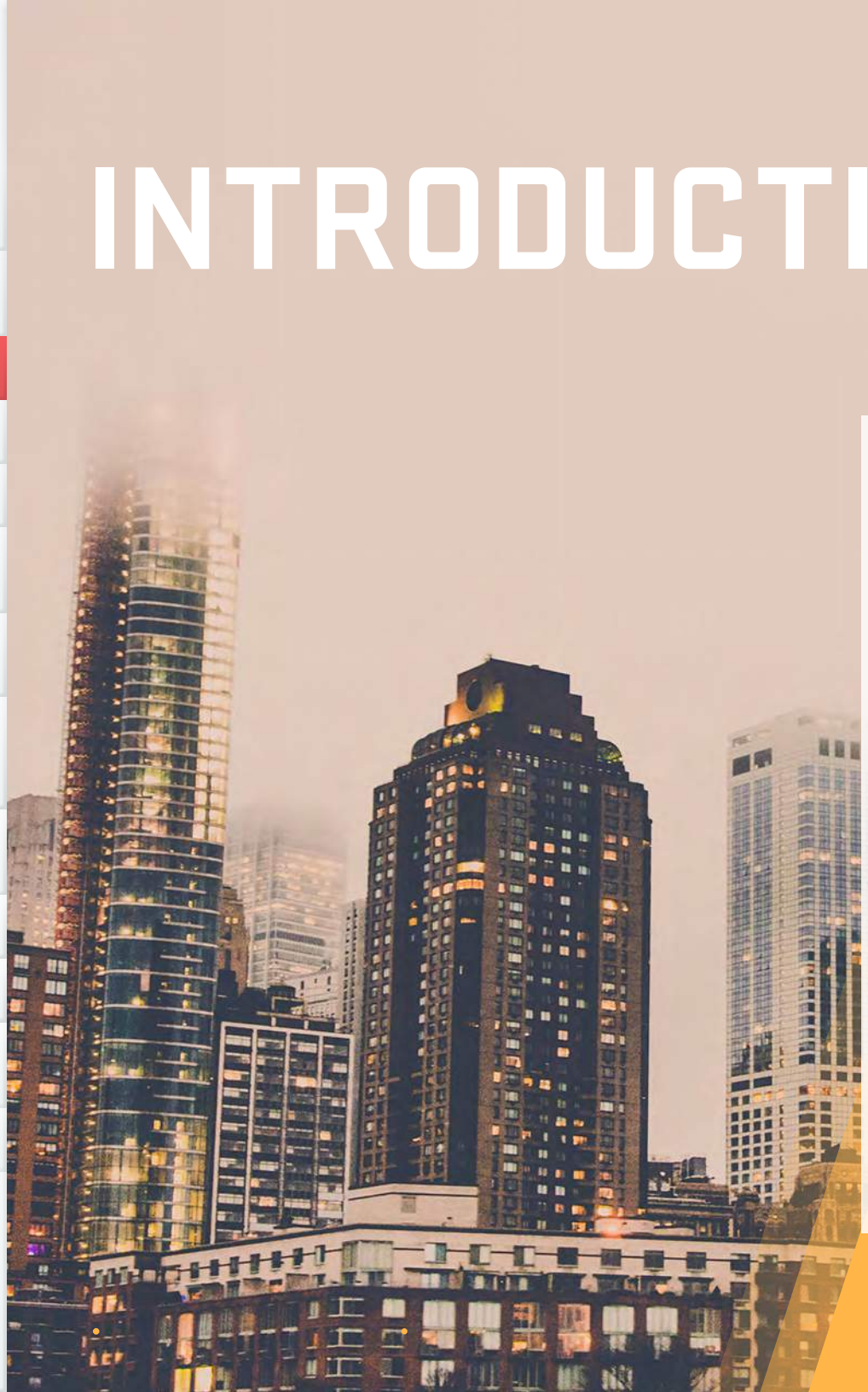
INSIGHT INTO THE

Global Threat Landscape

NETSCOUT Arbor's 13th Annual Worldwide Infrastructure Security Report

CONTENTS

INTRODUCTION



WELCOME TO OUR 13TH 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. NETSCOUT Arbor collected this data through a survey conducted in October 2017.

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 the years, but the core goal is still to provide real insight into infrastructure security from an operational perspective.

This document highlights key industry trends and threats facing network operators, along with the strategies used to mitigate them.

2017

128 FREEFORM + MULTIPLE CHOICE QUESTIONS

390 RESPONSES

2016

135 FREEFORM + MULTIPLE CHOICE QUESTIONS

356 RESPONSES

Survey Methodology

The 13th annual *Worldwide Infrastructure Security Report* (WISR) is based on a survey comprised of 128 free-form and multiple-choice questions. In our ongoing attempt to streamline and improve the survey, this is down from 135 in 2016.

Beyond the reduction in the number of questions, the 2017 survey has more specific logic flows that enable service providers and enterprise, government and education (EGE) respondents to see a different set of questions depending upon their self-classification and earlier answers. The questions we ask diverge depending upon the nature of the respondent.

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

NETSCOUT Arbor distributes the WISR survey by specifically targeting individuals within the operational security community to get the most accurate picture possible. Survey participation continues to grow despite additional efforts to encourage recusal of respondents without direct network or security operational experience.

DEMOGRAPHICS OF SURVEY RESPONDENTS

Service providers represent the majority of respondents at 55 percent (Figure 1), continuing the trend toward a more balanced mix of service providers and enterprise, government and education (EGE) organizations. Breaking down the EGE segment, 67 percent are enterprise respondents, with 19 and 14 percent representing education and government respectively.

SERVICE PROVIDERS

In a change from previous years, we asked service providers to tell us which services they offer, rather than asking them to identify with their primary service offering (Figure 1). Nearly one third considers themselves to be Tier 1 network operators, an increase from a quarter last year. Significant numbers of providers also offer hosting (63 percent), cloud (47 percent) and managed services (45 percent). The rise in hosting, cloud, and managed services reinforces the focus of providers on value-added revenue streams and the further erosion of traditional services.

EGE

Looking more closely at the EGE respondents, a broad array of verticals are represented (Figure 1). The largest proportions are from education and research organizations at 19%, followed by banking and finance.

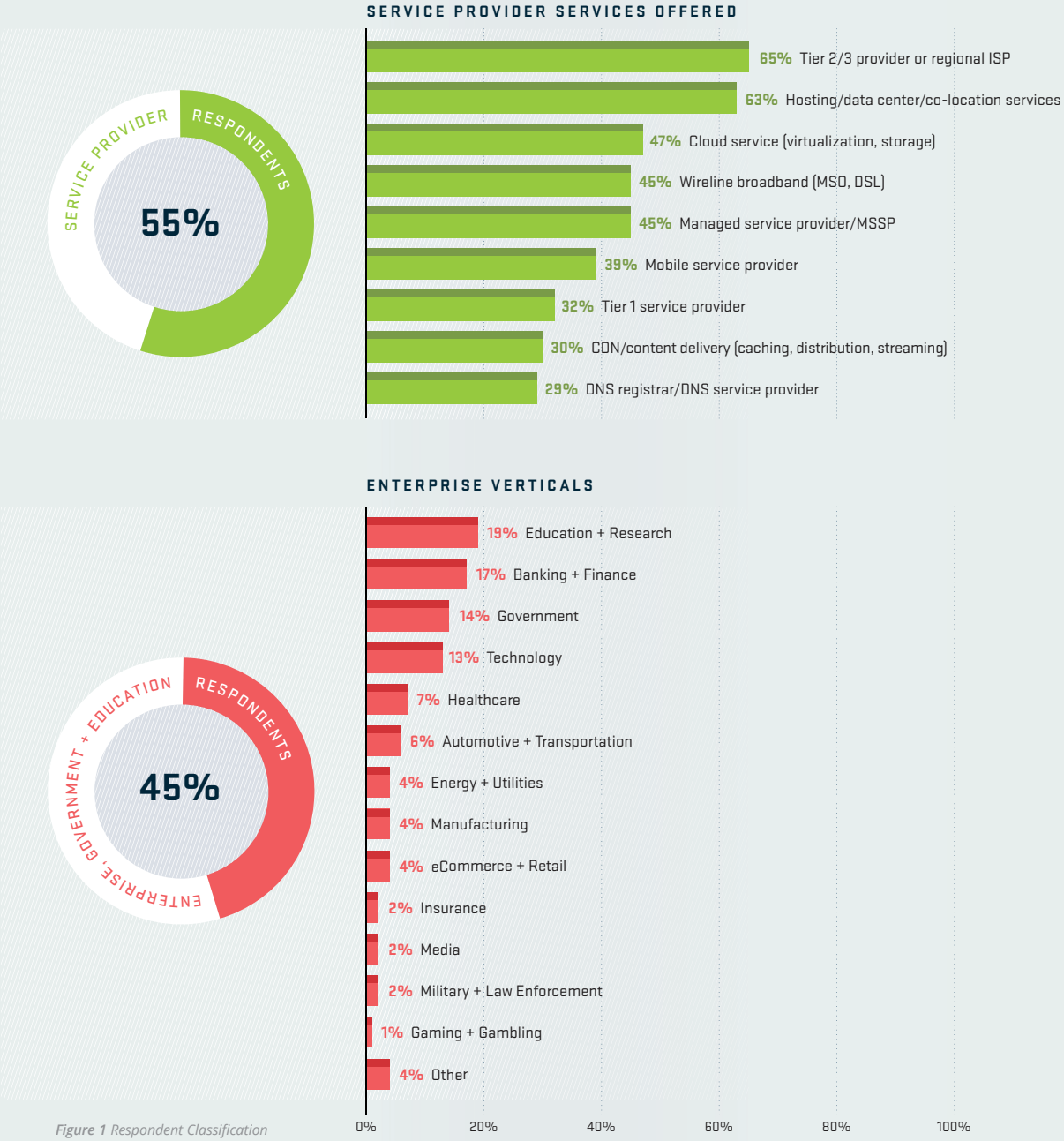


Figure 1 Respondent Classification

Nearly two thirds of all respondents identify as security, network or operations professionals (Figure 2), a similar result to last year. Security professionals have the highest representation with 32 percent.

The survey garnered wide participation from all around the world (Figure 3).

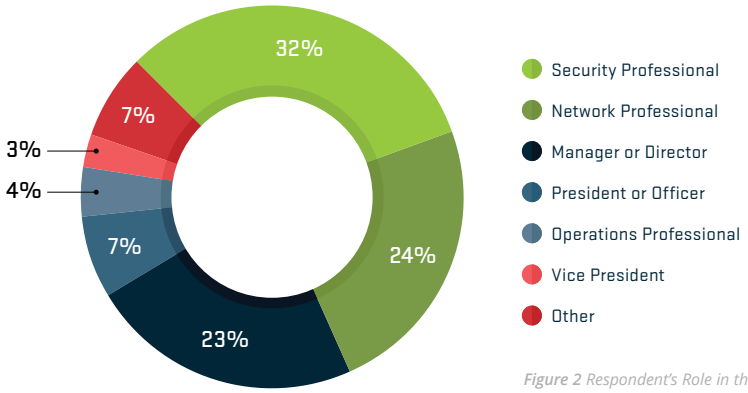


Figure 2 Respondent's Role in the Organization

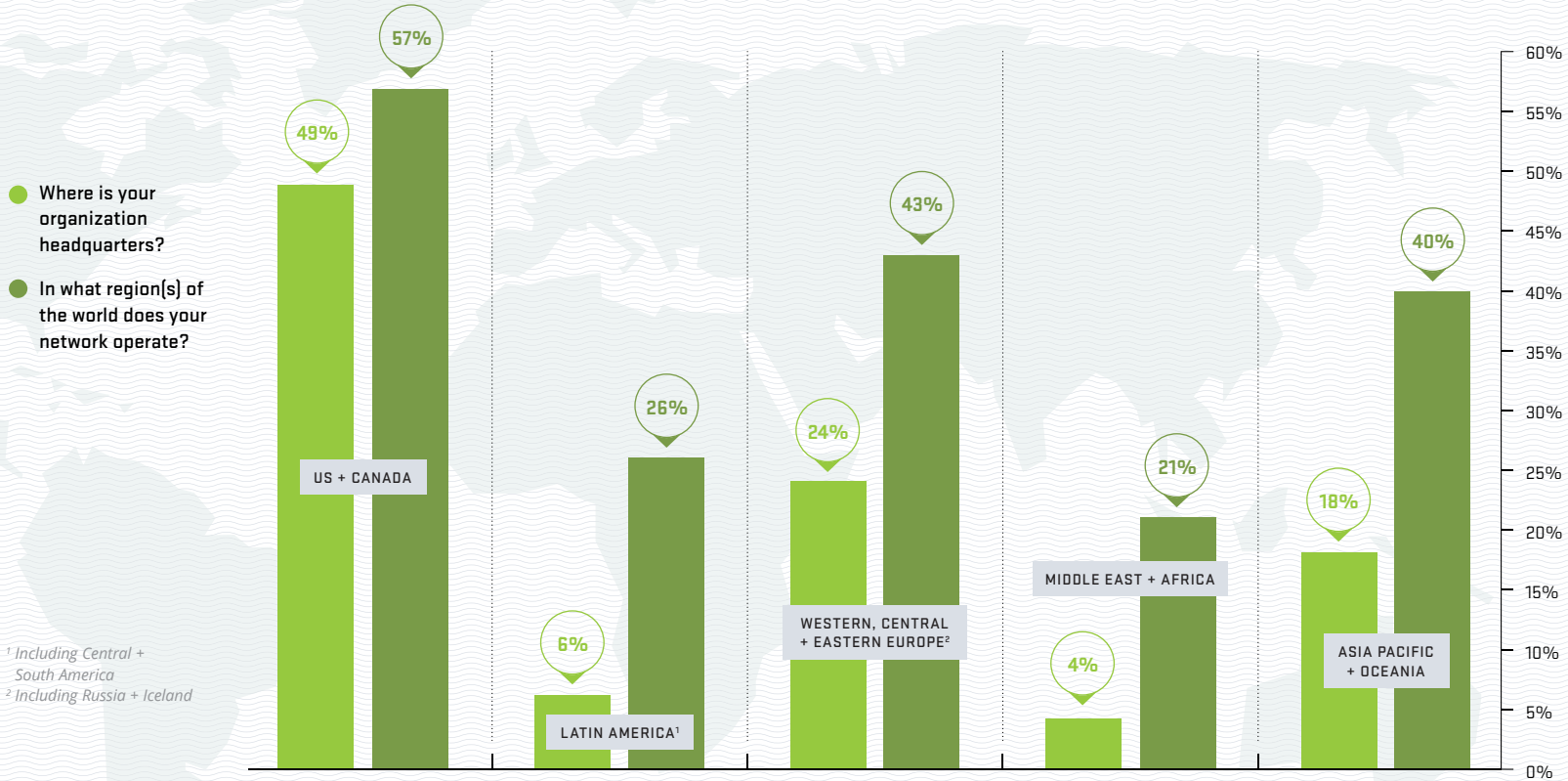


Figure 3 Respondent's Geographic Information

KEY FINDINGS

Service Providers

Attacks targeting cloud-based services rebounded, back up to over one third from only one quarter the previous year.

Online gaming was still viewed as the leading impetus for DDoS attacks. Criminals demonstrating attack capabilities took second place, with extortion rounding out the top three motivations.

OPERATIONAL THREATS

DDoS ATTACKS

DDoS attacks represent the dominant threat observed by the vast majority of service providers. Infrastructure outages also continue to be a threat with over half of operators experiencing this issue.

2018 CONCERNS

As expected, concerns for the coming year roughly mirror threats faced in the past.

PREFERRED THREAT DETECTION

NetFlow-based analysis tools remained the preferred method of threat detection for service providers. The use of SNMP-based tools also grew again this year, overtaking firewall logs, which continue to decline in popularity.

INLINE DDoS DETECTION/ MITIGATION SYSTEMS

Usage grew, an ongoing trend likely driven by the increased use of best-practice hybrid DDoS defense solutions.

EFFECTIVE THREAT DETECTION

NetFlow-based analyzers and inline DDoS detection/mitigation systems are seen as the most effective ways to detect threats.

DDoS

LARGEST ATTACK SIZE

The largest attack reported by a service provider was 600 Gbps, down from 800 Gbps last year.

VOLUMETRIC ATTACKS

While the size of the largest reported attack has decreased, the proportion of volumetric attacks was up. In general, peak attack sizes and the frequency of very large attacks decreased, a trend also observed in 2017 ATLAS data.

DNS + NTP

DNS and NTP remain the most commonly used vectors for reflection/amplification attacks.

TOP TARGETED SERVICE

DNS is the most common service targeted by application-layer attacks.

TOP TARGETED CUSTOMER

As expected, end-user subscribers took the top spot as the most common type of customer targeted. Financial services rose above hosting and government to reclaim the number two spot.

MULTI-VECTOR ATTACKS

Complex, multi-vector attacks are experienced by 59 percent of service providers.

OUTBOUND + CROSS-BOUND ATTACKS

Outbound and cross-bound attacks are not monitored by 46 percent of service providers.

AUTOMATIC DDoS MITIGATION

The use of automatic DDoS mitigation continues to gain traction with over one third of service providers now taking advantage of this technology.

MANAGED DDoS MITIGATION SERVICES

Demand for managed DDoS mitigation services is strong across the board. The top five verticals requesting managed services are financial, government, cloud/hosting, e-commerce and education.

SDN/NFV

SDN/NFV IN PRODUCTION

Compared to last year, the proportion of service providers having SDN or NFV in production has doubled.

OPERATIONAL CONCERNS

Operational concerns are the number one barrier followed by cost. SDN and NFV, even though they are being adopted, did not make a breakthrough in overcoming the concerns of service providers this year.

NETWORK DOMAIN

The data center is the most common network domain for SDN technologies. Quite surprisingly, in second place is IP backbone infrastructure, where service providers usually demonstrate a very conservative approach to technology.

OVERLAY NETWORKS

Overlay networks, including SD-WAN services, are also becoming an attractive spot for SDN.

IPv6

IPv6 GROWTH

It appears the surge in IPv6 growth or adoption is leveling off this year.

IPv6 FLOW TELEMETRY SUPPORT

The majority of service providers now indicate they have full IPv6 flow telemetry support from their vendors.

IPv6 TRAFFIC VISIBILITY

IPv6 traffic visibility, which is the key to detection and protection, has increased again this year.

TOP SECURITY CONCERN

DDoS and botnets are once again top security concerns for operators of IPv6-enabled networks.

DDoS MITIGATION

Overall there is a very welcome trend of increased DDoS mitigation capabilities for IPv6 traffic.

25%

Less than a quarter of service providers participate in global operational security communities or share or distribute observed cyber-security threats and gathered intelligence.

60%

Three fifths of service providers have their own internal security operations center (SOC) team while nearly one fifth either fully or partially outsource SOC capabilities.

This is the second consecutive year the survey shows an overall decline in service providers implementing security infrastructure best practices.

ORGANIZATIONAL SECURITY

SECURITY ANALYST SHORTAGE

The worldwide shortage of security analysts and incident responders is still a key issue. Lack of resources, along with the difficulty of hiring and retaining skilled personnel, are again the two main concerns for building an effective operational security team.

DDoS SIMULATIONS

The proportion that do not practice DDoS simulations and have no plans to do so increased. This is discouraging as dealing effectively with DDoS attacks is not just about technology, but about the people using the technology and the processes supporting it.

INCIDENT RESPONSE

Only 30 percent make time for incident response rehearsals at least quarterly.

ANTI-SPOOFING FILTERS

Surprisingly, given the popularity of reflection attacks over the last five years, the adoption of anti-spoofing filters decreased.

ACCESS CONTROL LISTS

The use of access control lists at the network edge also declined sharply.

Enterprise, Government + Education (EGE)

DDoS

INTERNET BANDWIDTH

Fifty-seven percent of enterprise, government and education (EGE) respondents saw their internet bandwidth saturated due to DDoS attacks, up from 42 percent in the previous year.

ENCRYPTED ATTACKS

Looking at encrypted attacks, 53 percent targeted the encrypted service at the application layer and 42 percent targeted the SSL/TLS protocol.

FIREWALLS

Over half of EGE organizations had firewalls or IPS devices fail or contribute to an outage during a DDoS attack.

EMAIL AND VoIP

Email and VoIP services were more frequently targeted this year, suggesting the focus of DDoS attackers shifted to exploiting more vulnerable services.

MULTI-VECTOR DDoS ATTACKS

There was a clear increase in the proportion of respondents experiencing multi-vector DDoS attacks, up from 40 percent in the previous year to 48 percent.

BRAND DAMAGE

Reputation/brand damage and operational expense are still the top business impacts of DDoS attacks. There was also a big jump in respondents reporting revenue loss.

ATTACK COST

Survey responses broadly indicate that the cost of a major DDoS attack is increasingly significant.

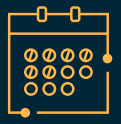
DDoS MITIGATION

DDoS mitigation was a part of business or IT risk assessments for 77 percent of respondents.

For the second consecutive year, there is a decrease in volumetric attacks with a corresponding increase in application-layer attacks.

The most popular targets of application-layer attacks were once again:

1. HTTP 2. DNS 3. HTTPS



x2

The percentage that observed more than 100 DDoS attacks per month more than doubled over the previous year.

NETWORK SECURITY

MOST COMMON ATTACK

Ransomware was the most commonly experienced attacks last year, with DDoS in second place.

KEY THREATS

Ransomware is also top of mind as a key threat for the coming year, while advanced persistent threat (APT) took second and DDoS dropped to third place.

DETECTION TOOLS

For the third consecutive year, firewall logs, IDS and SIEM are were the top three most utilized tools to detect threats.

60%

Sixty percent have deployed visibility solutions for IPv6 traffic, a slight increase from last year.

50%

Nearly half of respondents have an internal security operations center (SOC) team in place but 38 percent rely on third-party and outsourced services.

50%+

More than half are preemptively blocking known botnet Command-and-Control servers and malware drop servers.

IPv6

OPERATING IPv6

This year just over a third of respondents are operating IPv6 in their environments or planning to in the coming year.

INTERNET-FACING SERVICES

Sixty percent provide internet-facing services with IPv6 support.

PRIVATE NETWORKS WITH IPv6

Sixty-five percent have already deployed IPv6 on their private networks.

TOP THREAT

DDoS was cited as the top threat to IPv6 networks by over two thirds of respondents.

ORGANIZATIONAL SECURITY

SECURITY ANALYST SHORTAGE

Looking at the challenges EGE organizations face in building out operational security teams, lack of resources and difficulty of hiring and retaining skilled personnel were again the two main concerns.

DDoS SIMULATIONS

There was a small decrease in those running DDoS defense simulations.

Operational concerns are the top barrier to SDN/NFV deployment. Cost has become less of a concern as operational concerns are coming to the forefront.

SDN/NFV

SDN/NFV DEPLOYMENT PLAN

Only around 40 percent of EGE organizations have plans to deploy SDN/NFV technologies.

COMMON DOMAINS

Data center infrastructure and security were the most common domains where EGE respondents want to utilize SDN.

SDN/NFV DEPLOYMENT PLAN

Both EGE and service providers want to apply SDN to build global overlay networks, including SD-WAN.

DNS Operators

It is a positive sign that more EGE organizations are taking control of their DNS infrastructure and gaining visibility at Layer 7, as effective mitigation of DDoS attacks targeting DNS requires application-layer visibility.

DNS SERVERS

DNS servers are popular both as direct targets of DDoS attacks, but also as unwilling amplification and reflection actors. As a result, it is disappointing again to note that 19 percent of respondents still did not restrict access to their recursive DNS servers.

VISIBILITY

Nearly three quarters of all respondents have visibility at Layers 3 and 4, and 43 percent at Layer 7.

DNS SECURITY TEAM

There was a substantial increase of EGE organizations with a dedicated DNS security team.

IDMS

For service providers, Intelligent DDoS Mitigation Systems (IDMS) were again the most popular defense mechanism.

#1

Firewalls were the most popular choice for DNS defense in EGE networks once again.

25%

Only one quarter of service providers have a special security group for DNS. It is disappointing considering the criticality of DNS to the internet as a whole.

SERVICE PROVIDER

Threats + Concerns

DDoS attacks represented the top threat observed by service providers in 2017, with 87 percent reporting attacks (Figure 4). Infrastructure outages also continued to be a threat with 52 percent of operators experiencing this issue. This is up six percent from the previous year, halting a downward trend seen over the past few years. The percentage of service providers experiencing bandwidth saturation has remained constant from 2016.

Invariably, for 2018, DDoS attacks remain the primary concern for 88 percent of the service providers (Figure 4). This is not surprising, considering the continued concerns around weaponized IoT botnets and the ease with which attackers can gain access to sophisticated attack techniques and capabilities.

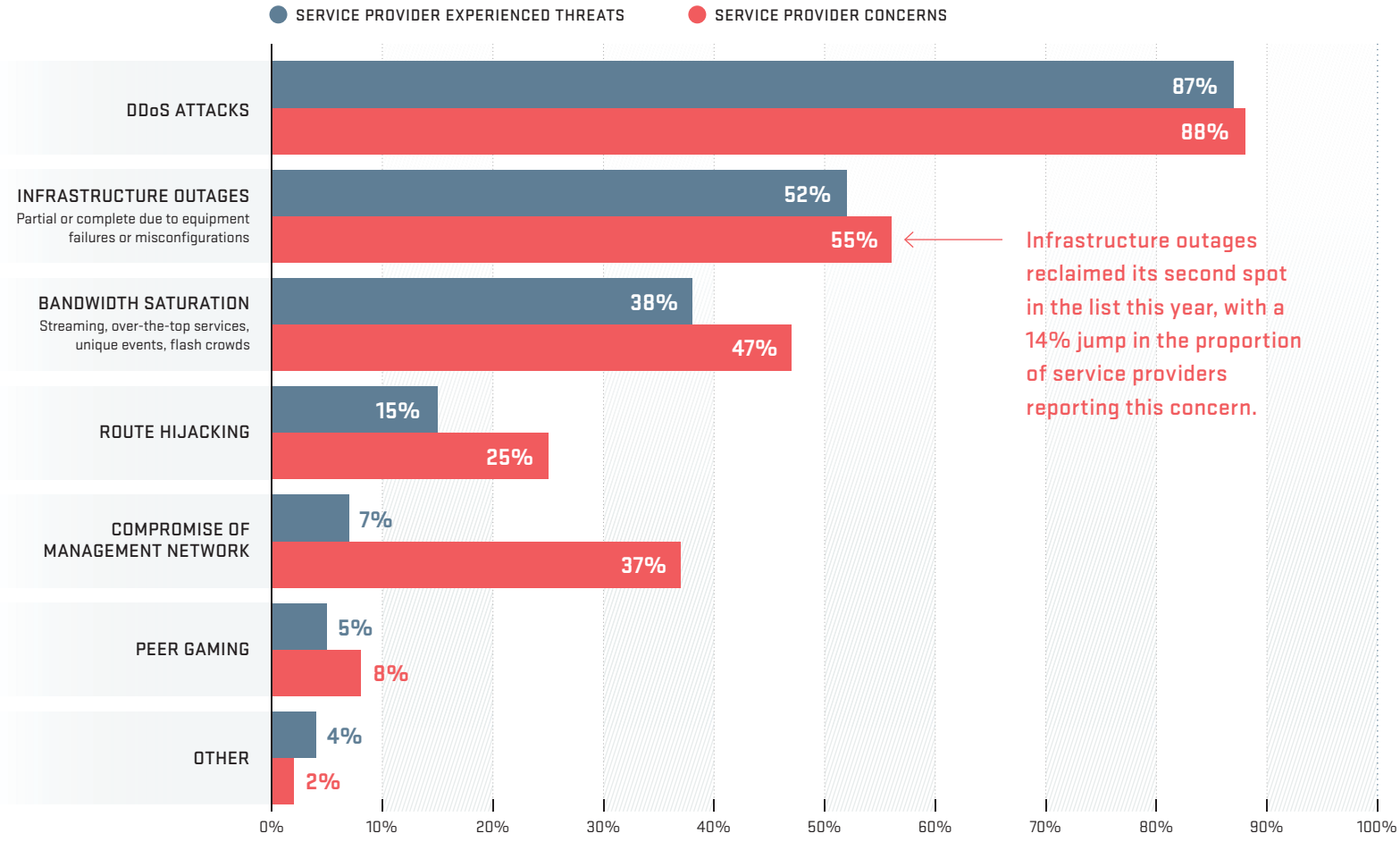


Figure 4 Service Provider Experienced Threats and Concerns

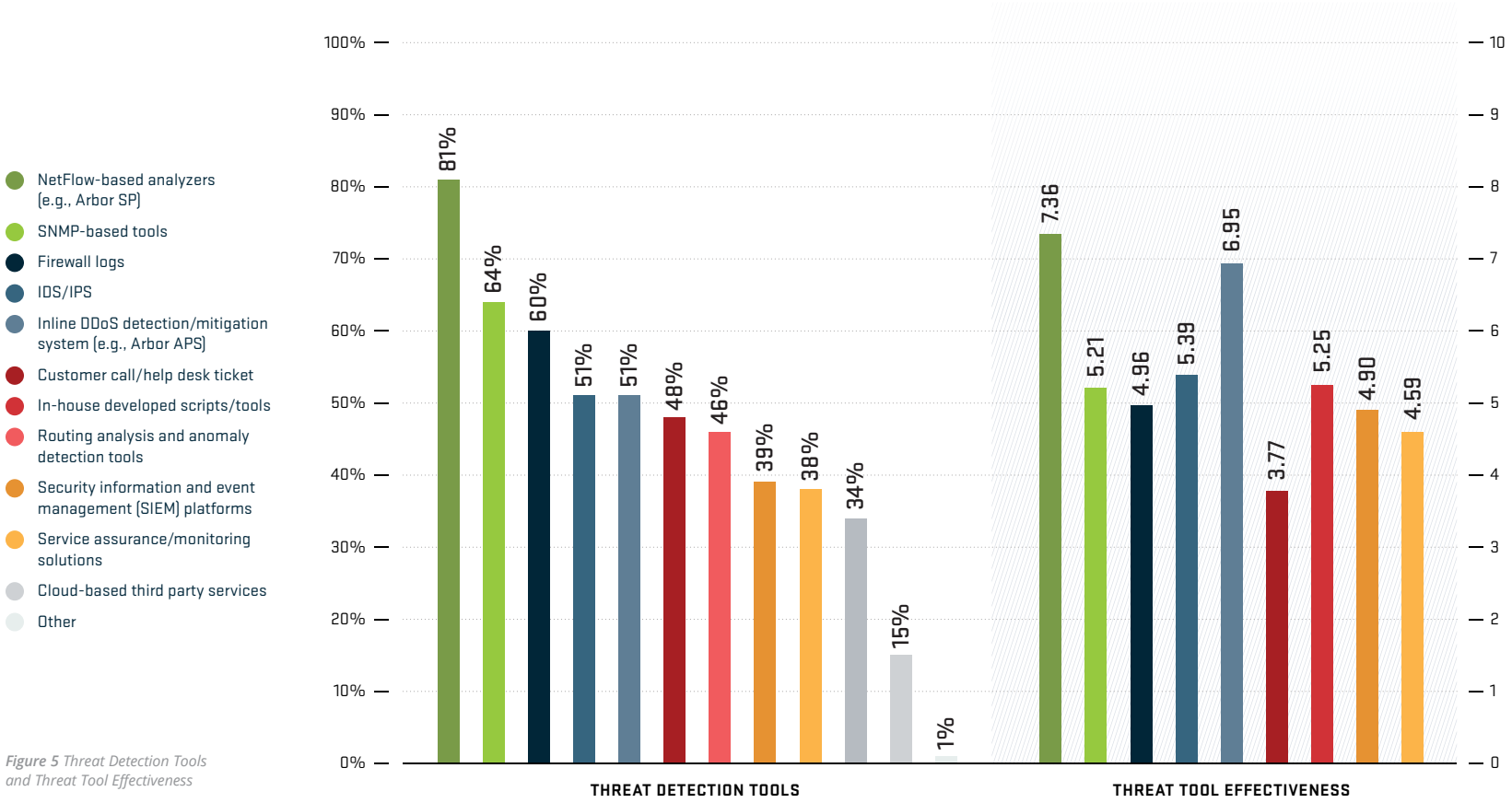


Figure 5 Threat Detection Tools and Threat Tool Effectiveness

As in previous years, respondents still used a wide variety of tools to detect threats against their networks, customers and services (Figure 5). The survey showed that NetFlow-based analysis tools remained the preferred option of service providers, with a slight decrease from 86 to 81 percent in 2017.

The use of SNMP-based tools also grew again to 64 percent, a significant increase over 53 percent in 2016, overtaking firewall logs, which continued to decline in popularity but remain in the top four with IDS/IPS.

Inline DDoS detection/mitigation system usage grew from 42 to 51 percent, an ongoing trend likely driven by the increased use of best-practice hybrid DDoS defense solutions.

Overall, the results of the effectiveness of threat detection tools remained similar to 2016, with NetFlow-based analyzers and inline DDoS detection/mitigation solutions ranked as the most effective ways to detect threats (Figure 5).

Scale + Targeting of DDoS Attacks

In 2017, attackers continued to use reflection/amplification techniques to exploit vulnerabilities in DNS, NTP, SSDP, CLDAP, Chargen and other protocols to maximize the scale of their attacks. In addition, there was a marked increase in the exploitation of IoT devices to generate large packet floods and application-layer attacks. The largest attack reported by a service provider was 600 Gbps, with others reporting attacks of 588 Gbps, 423 Gbps, 338 Gbps and 316 Gbps (Figure 6).

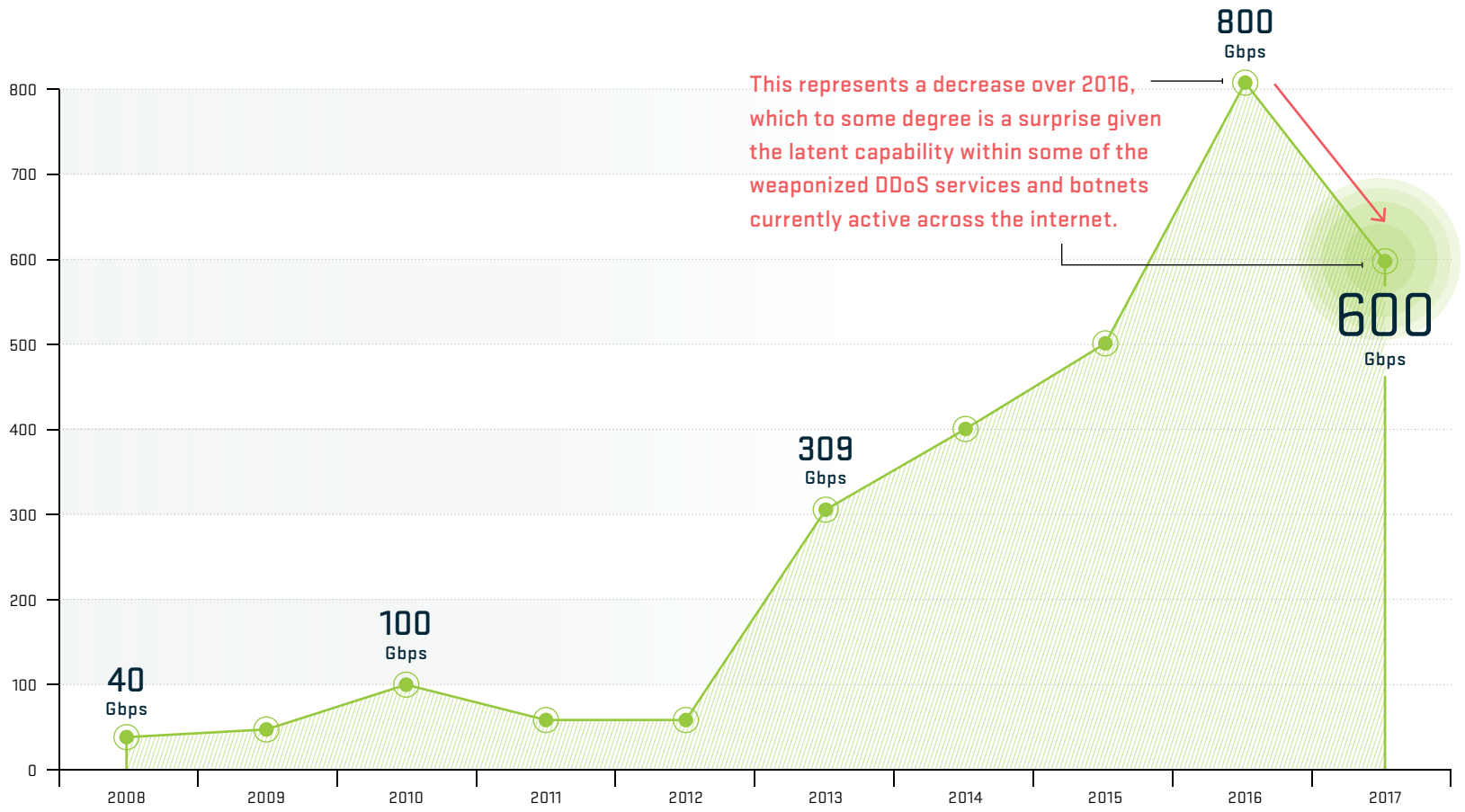


Figure 6 Peak Attack Size (Gbps)

In 2016, nearly one third of respondents reported peak attacks over 100 Gbps, emphasizing the breadth of the DDoS problem in relation to large attacks. In 2017, about one quarter witnessed peak attacks over 100 Gbps, and only seven percent reported attacks over 200 Gbps. In general, peak attack sizes and the frequency of very large attacks decreased, a trend also observed in 2017 ATLAS data (see *ATLAS Attack Sizes*).

While these numbers represent a decline in the very largest attacks, volumetric attacks were still the leading type of attack monitored by service providers. Attackers are using more metered attack volumes to achieve their goals while minimizing collateral damage and unwanted attention.

Looking at the targets of DDoS attacks monitored by service providers, customers remained the number one target at 75 percent, nearly identical to 2016 (Figure 7). Attackers continue to target their victims directly, rather than relying on collateral damage from indirect attacks. The proportion of attacks targeting service infrastructures increased slightly, likely due to continued exploitation of vulnerable services such as DNS.

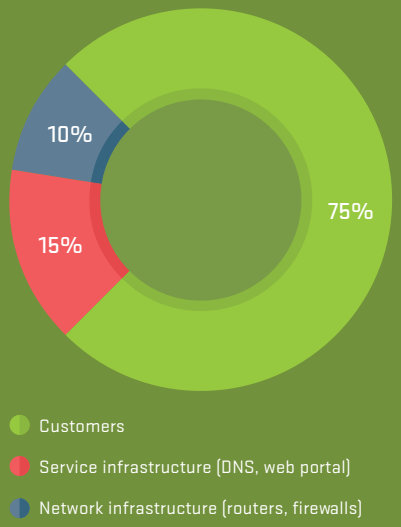


Figure 7 Attack Target Mix

Attack Target Customer Verticals

Figure 8 Attack Target Customer Verticals

As expected, end-user subscribers took the top spot as the most common type of customer targeted (Figure 8). Financial services rose above hosting and government to reclaim the number two spot. Gaming, which garnered sixth place in 2016, rose to fifth place, edging out education.

The growth of cloud services continued as more organizations adopt cloud-based applications and services. These services can offer significant performance, flexibility and cost advantages to business. However, their value is completely dependent on their availability to customers. In 2017, the proportion of respondents seeing attacks targeting cloud-based services rebounded, back up to over one third from only one quarter the previous year (Figure 9).

Cloud services rely heavily on service providers for protection from DDoS threats given their multi-tenant nature. Collateral damage, where attacks targeting one customer impact another unintended victim, represents a significant risk to all customers of a cloud service provider. An attack on one customer can potentially impact many others.

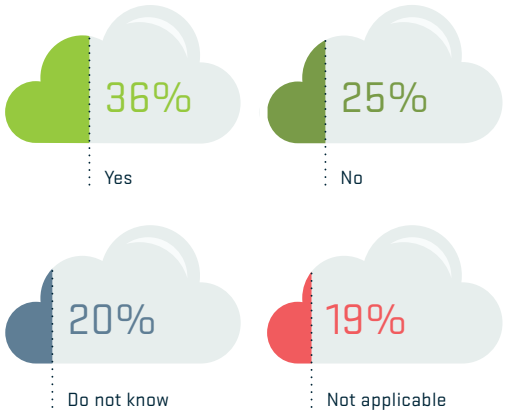


Figure 9 Attacks Targeting Cloud Services

Type, Frequency + Motivation of DDoS Attacks

While DDoS attack vectors vary significantly, cybercriminals are constantly evolving the methodologies they use to evade defenses and achieve their goals. Generally, attack vectors 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.

Looking at the mix of attack types experienced by service providers, volumetric attacks remain the most common, as in all previous iterations of this report (Figure 10). Like the previous two years, 2017 saw a significant increase in the frequency of volumetric attacks around the world. The percentage of attacks that were volumetric in nature increased to approximately 76 percent in 2017, up from 73. This is not surprising, given the widely reported prevalence of reflection/amplification and IoT-based attacks.

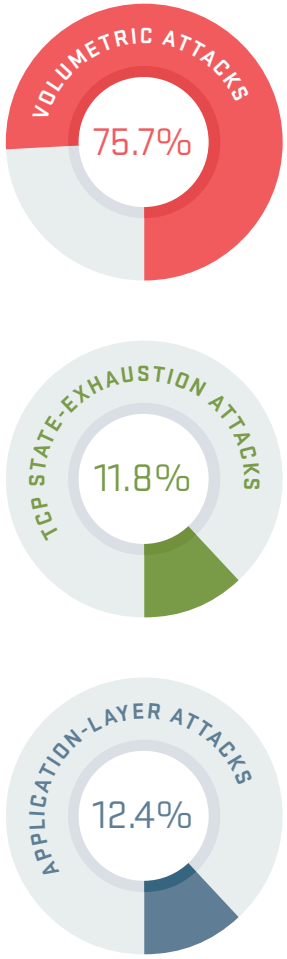


Figure 10 DDoS Attack Types

Unsurprisingly, application-layer attacks continued to exploit many vulnerable services. This year, DNS was the most common service targeted by application-layer attacks, reported by 82 percent of service providers (Figure 11). HTTP remained at 80 percent, identical to 2016. Additionally, the number seeing attacks targeting secure web services (HTTPS) rose significantly from 52 to 61 percent. While decryption is not always necessary for successful mitigation, scalable solutions for decrypting packets are needed more than ever. Fortunately, there are some promising solutions on the horizon.

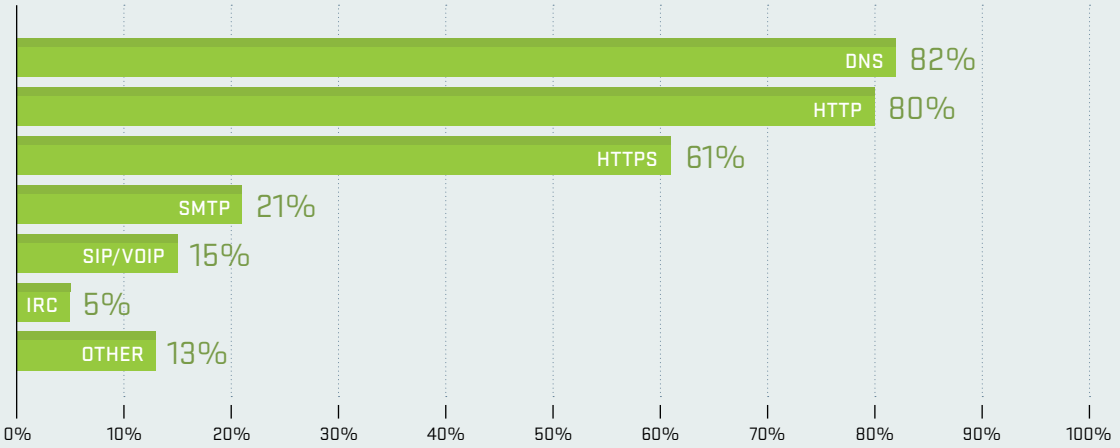


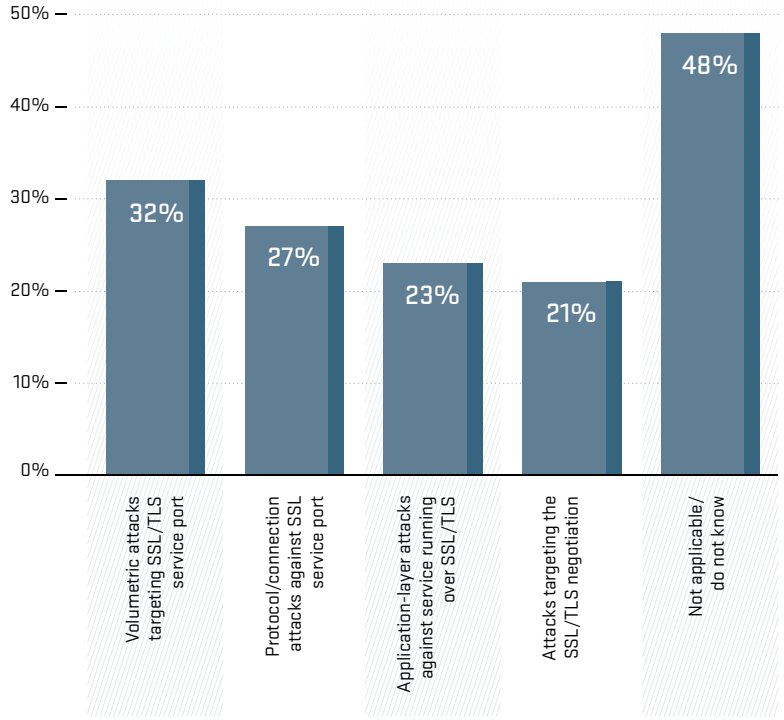
Figure 11 Targets of Application-Layer Attacks

Looking deeper into attacks targeting encrypted services, there are four different categories:

1. Attacks that target the SSL/TLS negotiation
2. Protocol/connection attacks against SSL service port
3. Volumetric attacks targeting SSL/TLS service port
4. Application-layer attacks against underlying service running over SSL/TLS

In 2017, the results were broadly similar to previous year, with over 20 percent experiencing attacks in each category (Figure 12). Given the criticality of many encrypted applications, especially those provided by financial and e-commerce organizations, a successful attack can have significant impact.

Figure 12 Types of Attacks Targeting Encrypted Services



We specifically asked respondents about the protocols used to generate volumetric reflection/amplification attacks (Figure 13). Nearly all protocols showed similar activity to 2016, with DNS and NTP remaining the most commonly used vectors. Attackers continued to leverage poorly configured or protected infrastructures to magnify their capabilities. The *ATLAS Reflections* section of this report drills down into details on reflection/amplification trends.

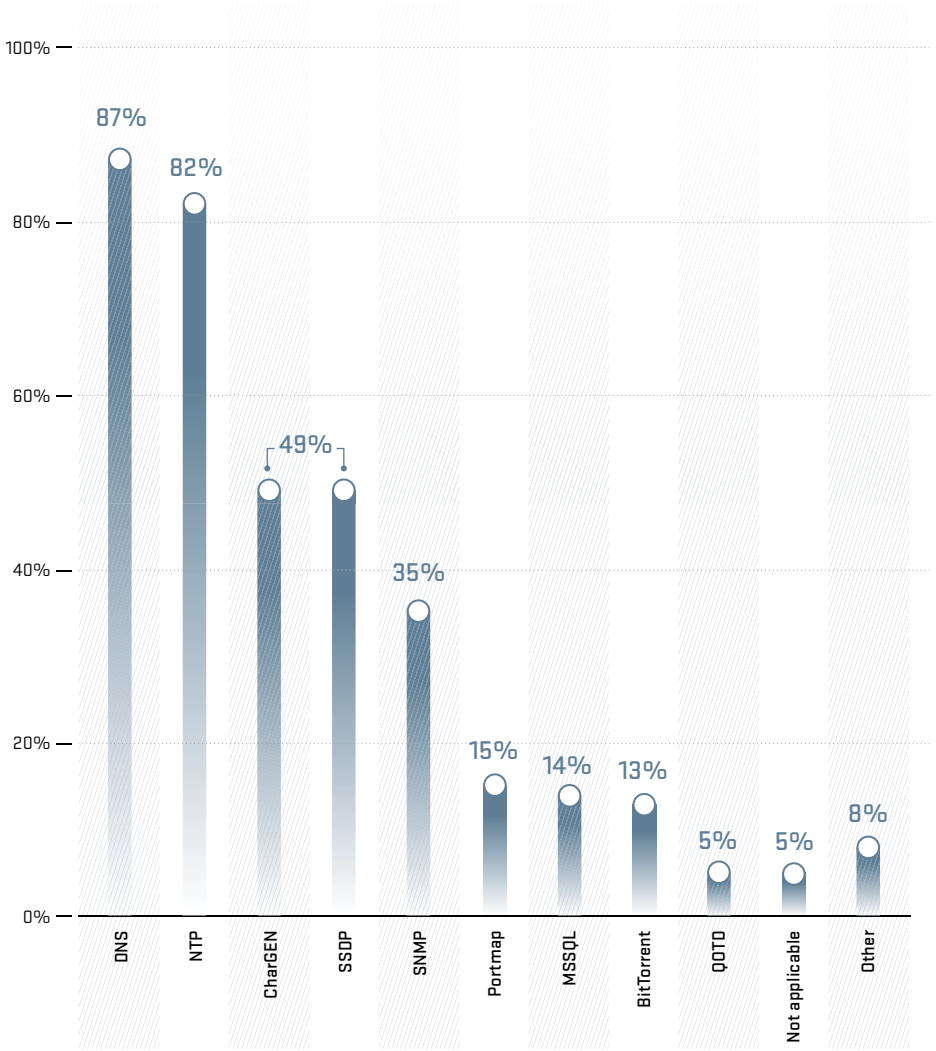


Figure 13 Protocols Used for Reflection/Amplification Attacks

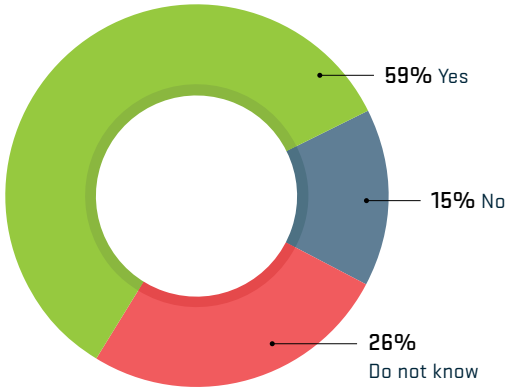


Figure 14 Multi-Vector DDoS Attacks

Multi-vector attacks are nothing new, but their complexity can still make them difficult for defenders to successfully mitigate.

The percentage of service providers seeing multi-vector attacks on their networks decreased, down to 59 percent in 2017 from 67 in 2016, but still above 56 percent in 2015 (Figure 14). Because multi-vector attacks are more difficult to mitigate, a layered defense is the best solution. Layered DDoS defense utilizes a hybrid approach allowing organizations to proactively block stealthy attacks closer to the target, while mitigating larger volumetric attacks upstream where sufficient capacity is available.

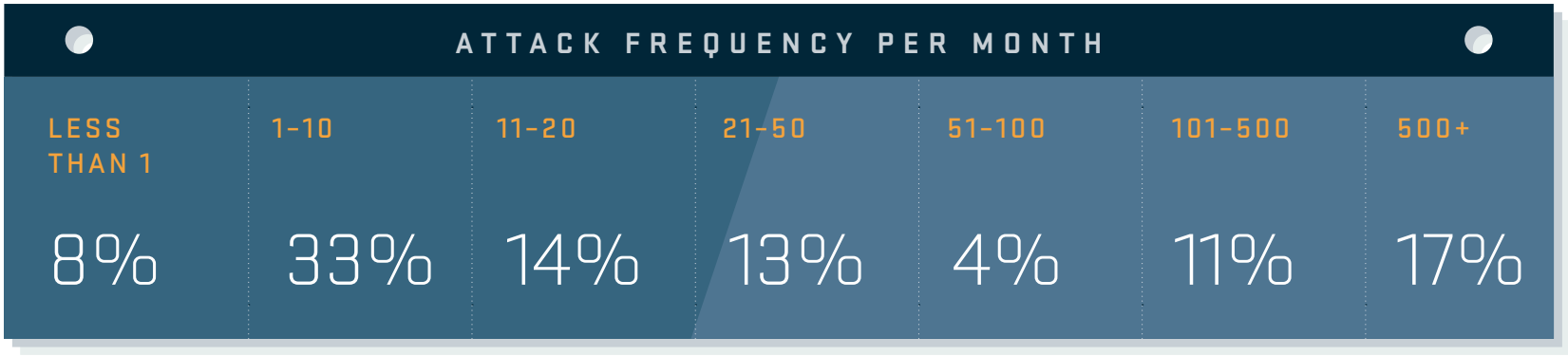


Figure 15 Attack Frequency Per Month

The number of attacks experienced per month by service providers increased somewhat (Figure 15). While 53 percent experienced more than 21 attacks per month in 2016, that dropped slightly to 45 percent in 2017. Conversely, those experiencing over 500 attacks per month increased to 17 percent from 15 percent in 2016.

Attack durations increased in 2017 (Figure 16). Approximately 29 percent of service providers indicated their longest monitored attack was over 12 hours. This is up slightly from 2016, when one quarter reported that their longest attack was over 12 hours but still below the 37 percent reported in 2015. This trend is corroborated by ATLAS data and anecdotal feedback from NETSCOUT Arbor customers indicating longer duration attacks in 2017.

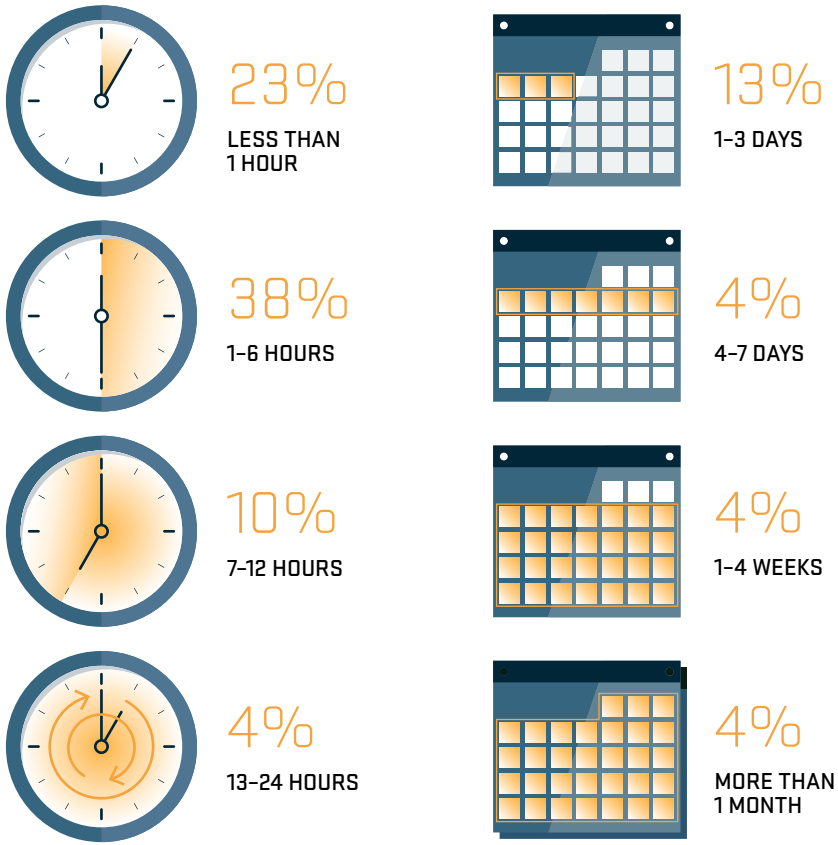


Figure 16 Longest Attack Duration

DDoS Threat Motivations

As in previous years, we asked service providers to indicate the most common motivations behind the DDoS attacks they monitored on their networks. In 2016, the top motivation was online gaming. Ideological hacktivism was in second place, with criminals demonstrating attack capabilities following closely in third.

However, the top motivations shifted in 2017 (Figure 17). Online gaming was still viewed as the leading impetus but only 50 percent saw this as a common motivation, down from 63 percent in 2016. In a near tie with gaming, criminals demonstrating attack capabilities returned to prominence as it took second place, with extortion rounding out the top three motivations.

While nihilism/vandalism made a return to the top five in 2017, ideological hacktivism followed closely, nearly tied for fourth place. The rise of criminals demonstrating their capabilities is indicative of the continuing weaponization of DDoS attacks via easy-to-procure services. The ubiquitous availability of Booter/Stresser services remains a serious problem.

For the first time, we asked survey respondents where IoT-based botnet attacks originated (Figure 18). Nearly half indicated the attacks come from compromised devices outside of their networks, as one might expect. Surprisingly, 22 percent said the traffic originated either fully or partially from inside their own networks.

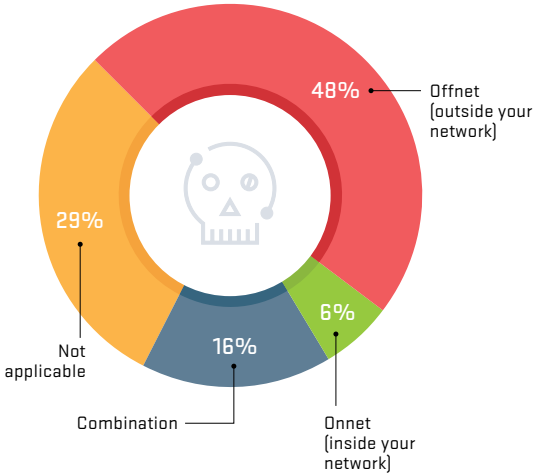


Figure 18 IoT-Botnet Attack Source

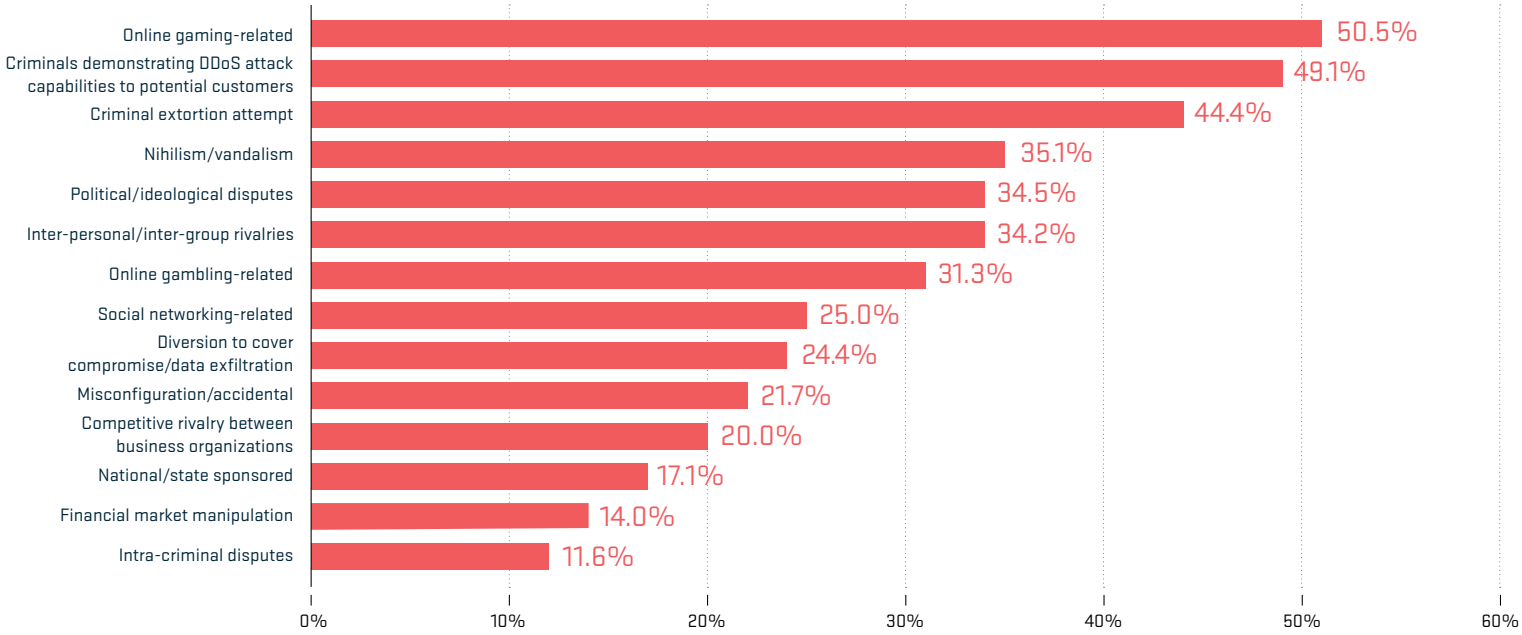


Figure 17 Service Provider DDoS Attack Motivation

Service providers continued to improve their capability to mitigate DDoS attacks, and the 2017 results were very encouraging (Figure 19). IDMS usage increased again to reach a record high of 88 percent, up from 83 percent in 2016. The use of access control lists (ACLs) moved up to second place from third last year. The use of FlowSpec also increased dramatically, nearly doubling from 15 percent in 2016 to 27 percent. Collectively, these statistics indicate a very positive trend in the application of surgical and stateless mitigation technologies.

Once again, the number of service providers that could mitigate attacks in less than 20 minutes increased, reaching 80 percent up from 77 percent in 2016 and 74 percent in 2015 (Figure 20). Furthermore, the use of automatic mitigation rose dramatically to 36 percent, compared with only 27 percent last year. This demonstrates a continued increase in the use of integrated tools and automation within the customer environment. Average attack duration remained relatively short for DDoS attacks, so service providers have a brief time to act when protecting their customers. Overall, mitigation reaction times are continuing to improve.

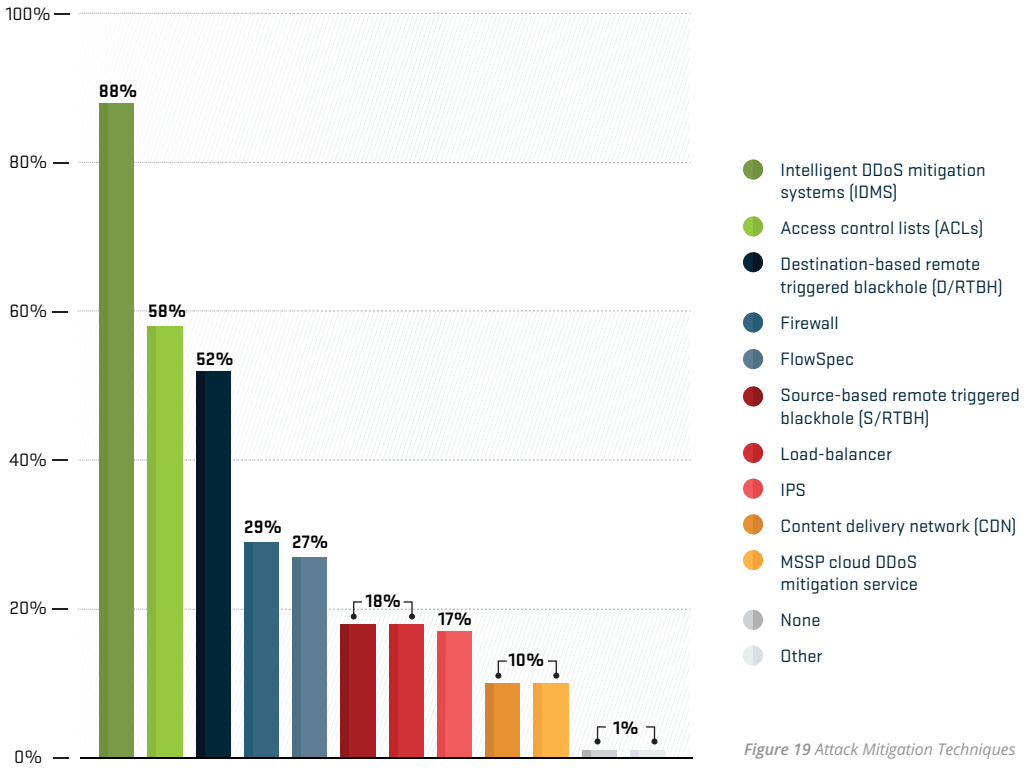


Figure 19 Attack Mitigation Techniques

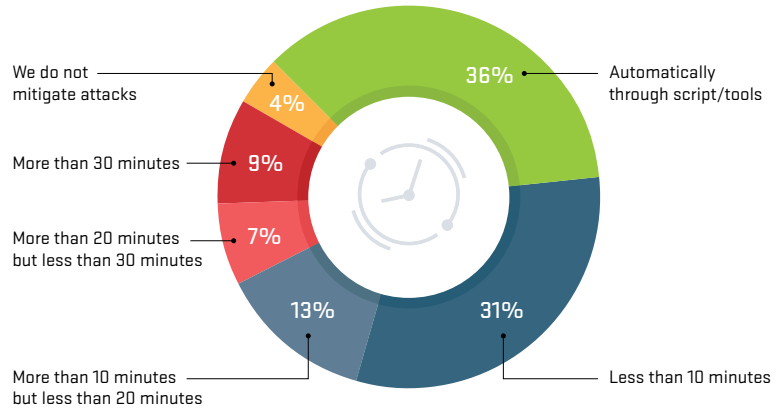


Figure 20 Time to Mitigate

Among organizations that monitored outbound and cross-bound attacks, the majority indicated these attacks were less than 10 percent of all attacks they see (Figure 21). However, some operators identified as much as 50 percent of all attacks as outbound or cross-bound in nature.

Nearly identical to last year, 46 percent did not detect outbound or cross-bound attacks at all. This continues to indicate a general lack of visibility in this area. This is a concern, as these attacks can still impact customer aggregation routers and customer experience. Ideally, organizations should detect and deal with outbound and cross-bound attacks in the same way as inbound attacks.

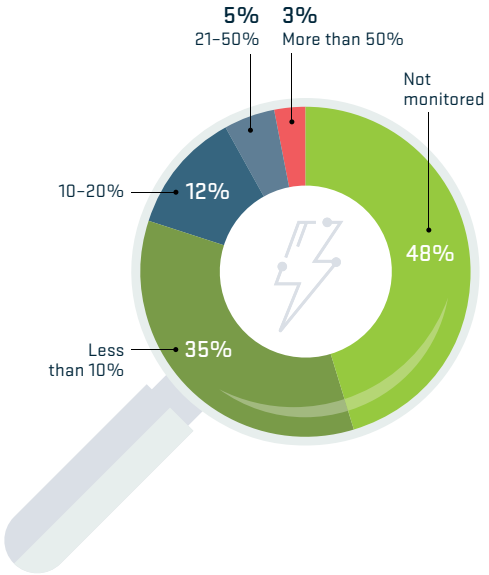


Figure 21 Proportion of Outbound/Cross-Bound Attacks Observed

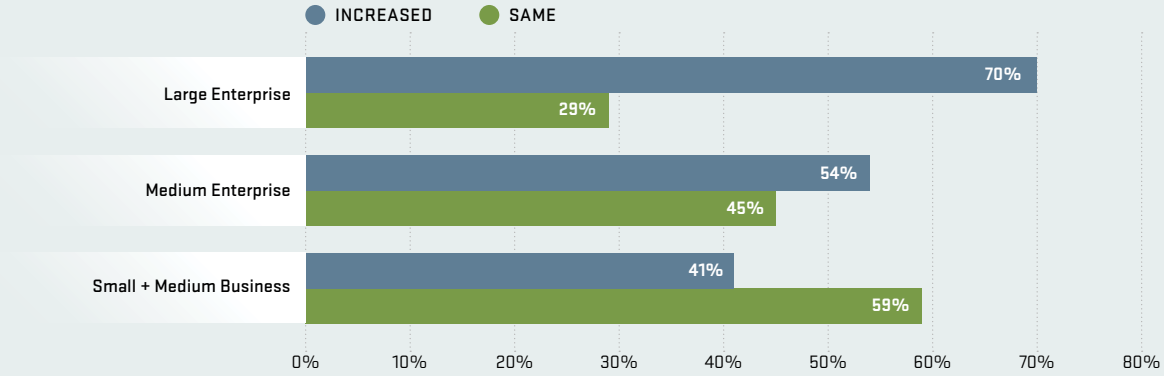


Figure 22 Demand for DDoS Detection/Mitigation Services

Interest in DDoS detection and mitigation services remained strong across all business segments (Figure 22). Virtually no service providers indicated a reduced demand for their DDoS services. Instead, they indicated the strongest growth in demand was by far from large enterprise customers at 70 percent.

The survey drilled into the demand for managed DDoS services in more detail to establish which verticals are driving the increase (Figure 23). Financial services dominated with 60 percent, while government followed closely at 55 percent. Cloud/hosting companies rebounded from 44 percent in 2016 to round out third place at 51 percent. Overall, we saw an increase in demand across virtually all verticals again in 2017. This indicates that organizations, regardless of their business focus, are now very aware of the DDoS threat and are looking to reduce the risk of becoming victims of a successful attack.

Business Verticals for DDoS Services

60% Financial	24% Gaming	17% Retail
55% Government	22% Small Business	16% Gambling
51% Cloud/Hosting	21% Healthcare	15% Law Enforcement
38% eCommerce	19% Utilities	7% Social Networking
31% Education	17% Media	

Figure 23 Business Verticals for DDoS Services

SDN/NFV

NETSCOUT Arbor has been tracking SDN and NFV development in annual reports over last three years. It is helpful to analyze how service provider interest and adoption rates have changed over time.

Compared to last year, the proportion of service providers having SDN or NFV in production has doubled (Figure 24). In 2017, 18 percent of respondents confirmed they had NFV deployed. Twenty-one percent were investigating these technologies or running trials, compared to 27 percent in the previous year. The percentage of those not looking into SDN and NFV was also similar to last year (41 percent versus 38 percent).

We asked service providers to identify the barriers to deploying these technologies (Figure 25). Operational concerns were the number one barrier at 56 percent, followed by cost at 52 percent and interoperability at 46 percent. These results were similar to last year, which leads us to conclude that SDN and NFV, even though they are being adopted, did not make a breakthrough in overcoming the concerns of service providers.

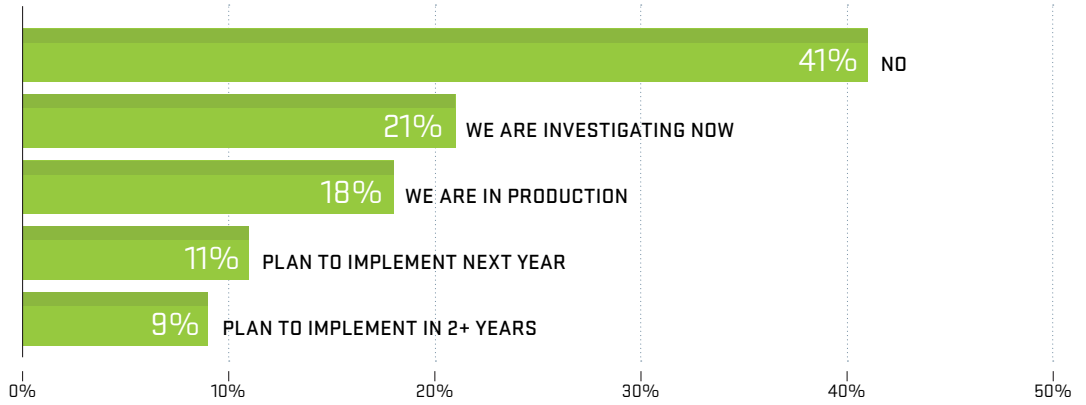


Figure 24 SDN/NFV Deployment

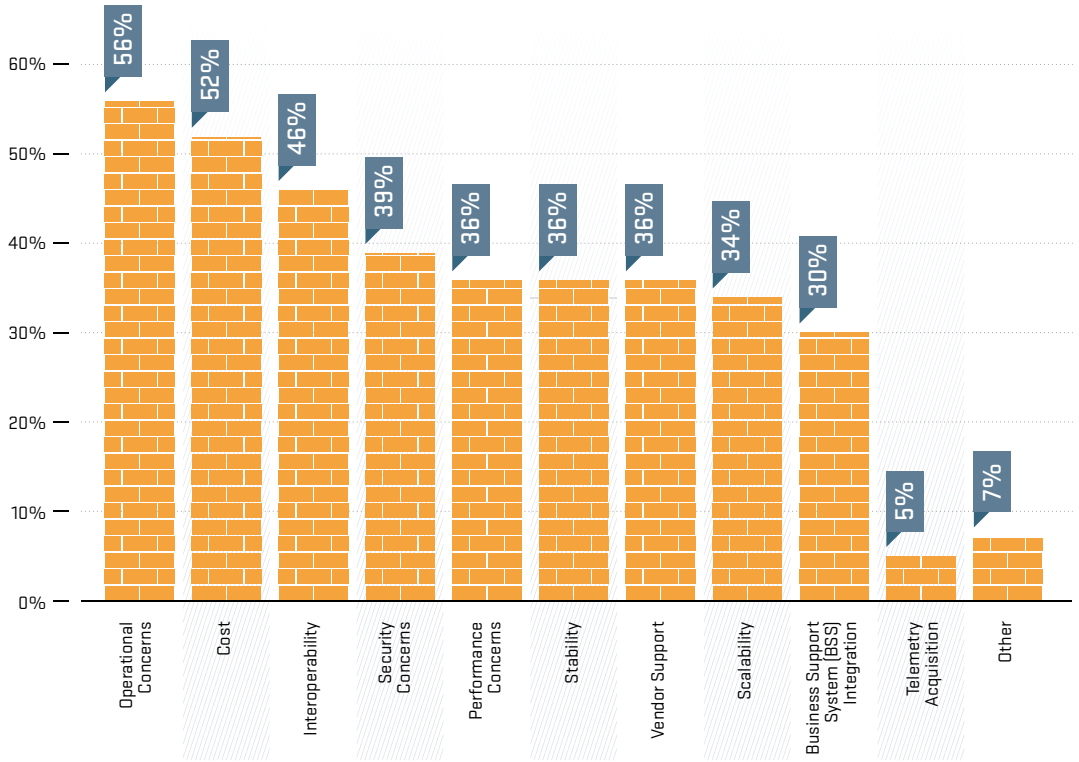


Figure 25 SDN/NFV Key Barriers

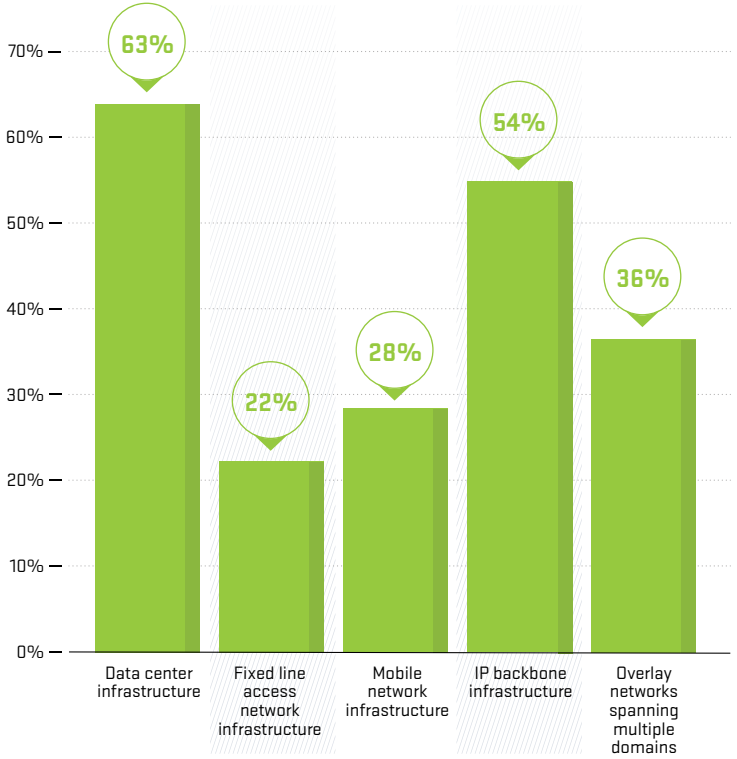


Figure 26 SDN Network Domains

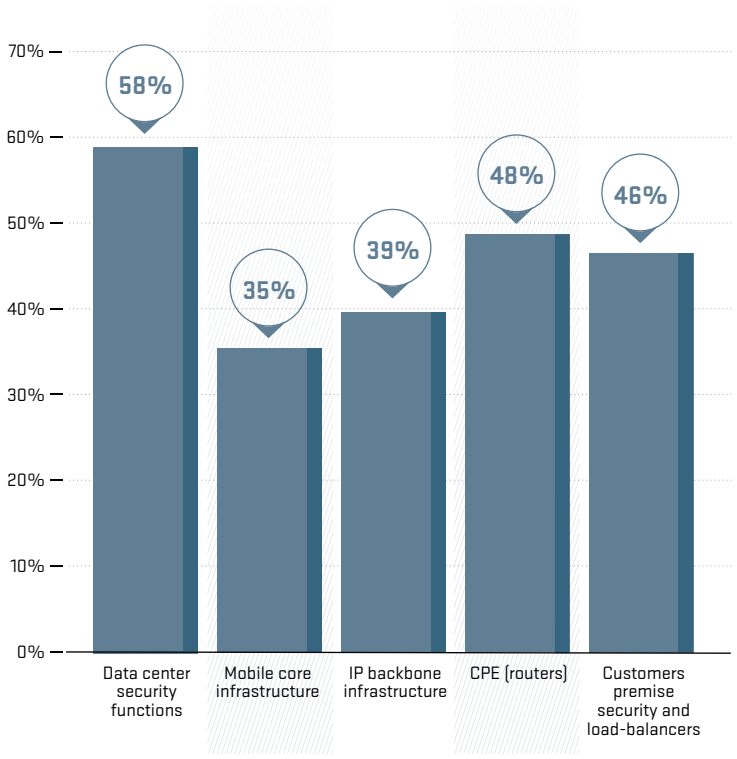


Figure 27 NFV Network Domains

Regarding network locations where SDN technologies are seeing the most interest, the data center was the most common at 63 percent (Figure 26). Quite surprisingly, in second place was IP backbone infrastructure, where service providers usually demonstrate a very conservative approach to technology. However, 54 percent of respondents indicated they planned to implement SDN technologies here. Overlay networks, including SD-WAN services, were also becoming an attractive spot for SDN, according to 36 percent of the providers.

When it comes to a functional domain for NFV, data center security functions were in first place at 58 percent (Figure 27). However, CPE routers and CPE value-added functions were close behind at 48 percent and 46 percent respectively. This clearly indicates that the (virtual) customer premise domain is where the industry wants to apply NFV.

IPv6

Similar to last year, nearly 70 percent of service providers have or will deploy IPv6 within their networks in the coming year (Figure 28). It appears the surge in IPv6 adoption is leveling off this year.

PLANNING TO OPERATE IPv6 WITHIN NETWORK?

Figure 28 IPv6 Operation

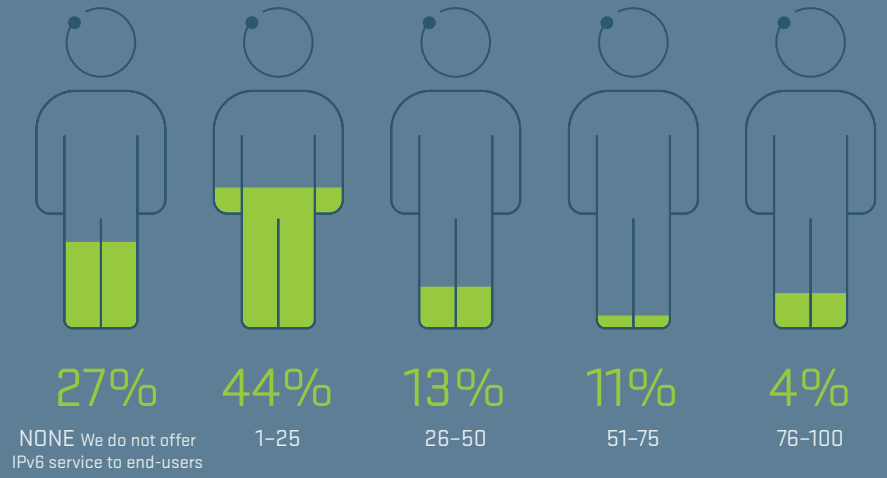


Figure 29 Subscriber IPv6 Usage

Again, in-line with last year, 73 percent of providers indicated they offer IPv6 services to end-users (Figure 29). However, looking more closely at the results we are now seeing higher adoption rates within those organizations that do offer the service. Specifically, 15 percent now indicate more than half of their end-users utilize IPv6 services compared to only eight percent last year.

Nearly identical to last year, 83 percent of service providers offer IPv6 services to business customers (Figure 30). Adoption rates are also broadly similar to last year with one notable exception. Service providers reporting adoption rates above 75 percent doubled to six percent from just three percent the previous year.

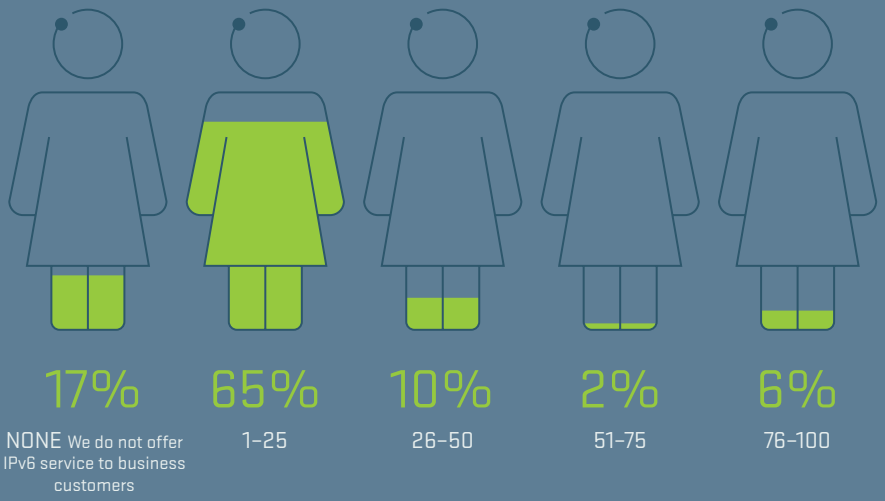


Figure 30 Business Customer IPv6 Service Usage

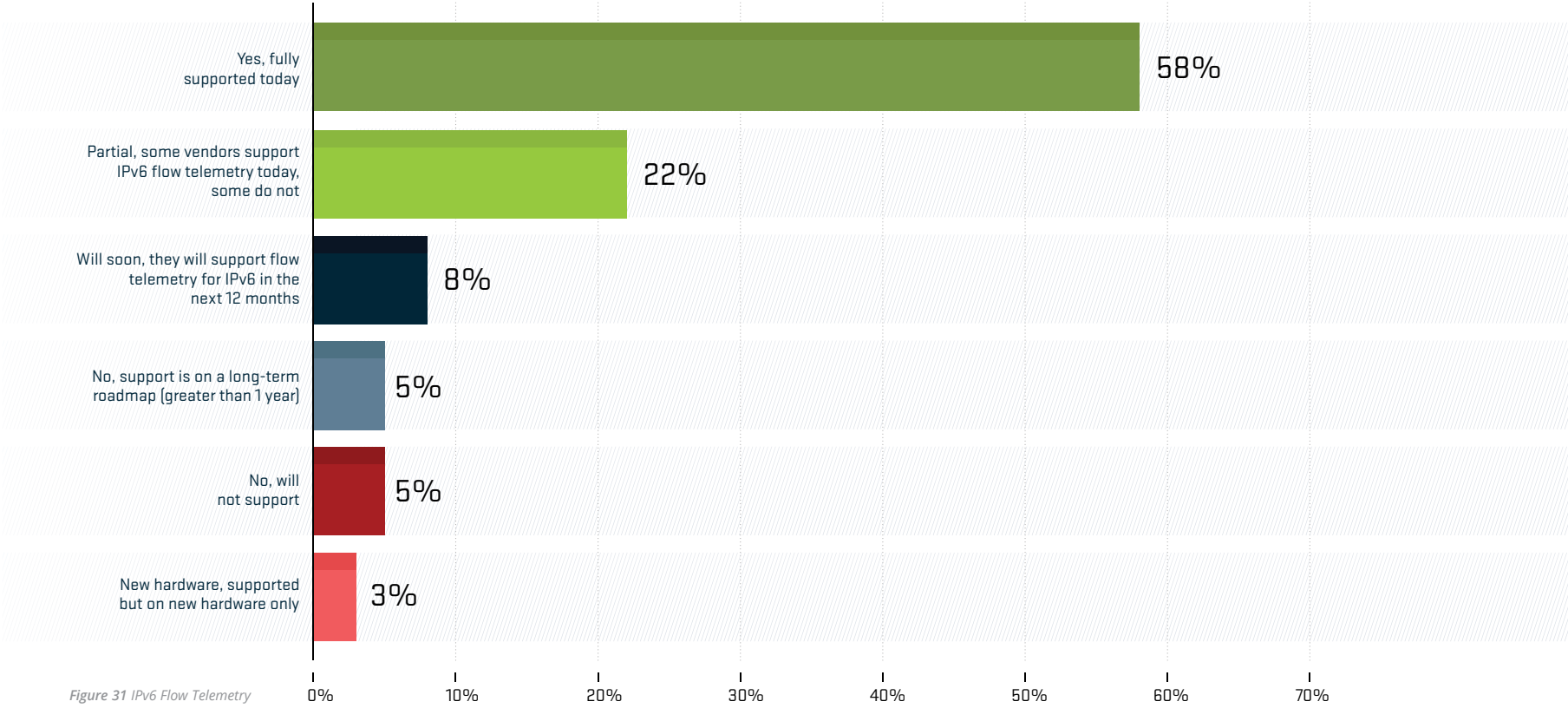


Figure 31 IPv6 Flow Telemetry

Nearly 60 percent of service providers now indicate full IPv6 flow telemetry support from their vendors (Figure 31). An additional 22 percent cite at least partial support for IPv6 flow telemetry showing further improvements in vendor support this year. This is good news for the customers leveraging these networks and shows steady effort on the part of providers to satisfy growth commitments to IPv6.

IPv6 traffic visibility, which is the key to detection and protection, has increased to 70 percent this year from just 60 percent last year (Figure 32). This is a positive indication that service providers are keeping pace with the growth of IPv6 and are focused on telemetry/visibility to help keep the networks healthy and current.

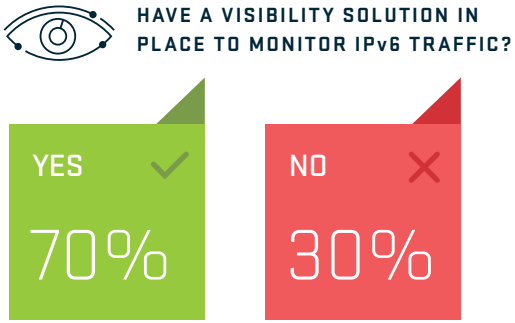


Figure 32 IPv6 Traffic Visibility

Generally, service providers expressed concern over IPv6 attacks against dual-stack devices having an impact on IPv4 services (Figure 33). While 44 percent expressed minor concern, nearly one third indicated moderate concern and 11 percent indicated major concern over this issue.

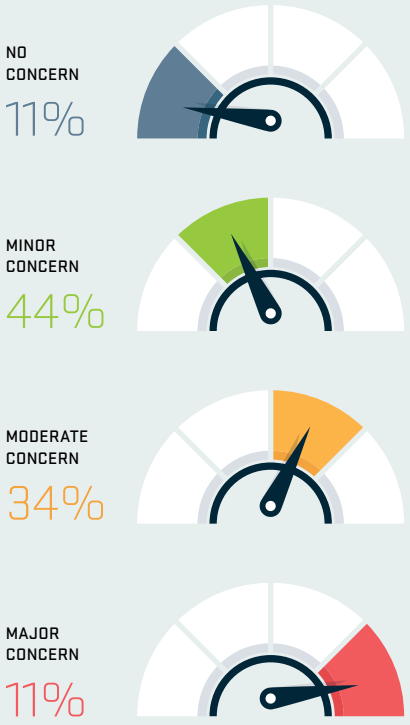


Figure 33 IPv6 Impact on IPv4 Services (Dual-Stack Devices)

Overall, 57 percent of service providers projected some level of IPv6 traffic growth in the coming year (Figure 34). Further, only six percent project no IPv6 traffic growth compared to 14 percent last year.

However, 37 percent were unable to predict future growth this year compared to only 18 percent last year.

Figure 34 Anticipated IPv6 Traffic Growth

When asked about the security concerns of operating IPv6-enabled networks, DDoS and botnets are once again top of mind among respondents (Figure 35). Seventy-five percent are concerned with IPv6 DDoS attacks and 44 percent are concerned about botnets, both up slightly from last year.

At 81 percent, Intelligent DDoS Mitigation Systems (IDMS) remain the first choice in DDoS mitigation solutions deployed by service providers against IPv6 attacks (Figure 36). This percentage has increased from 76 percent last year and 67 percent the year before. Destination-based remote-triggered blackhole (D/RTBH) has maintained at 56 percent. Access control lists (ACL) are a close third, rising from fifth place last year. In addition, the use of FlowSpec as a mitigation measure has also increased to 44 percent from 37 percent last year.

Overall there is a very welcome trend of increased DDoS mitigation capabilities for IPv6 traffic.

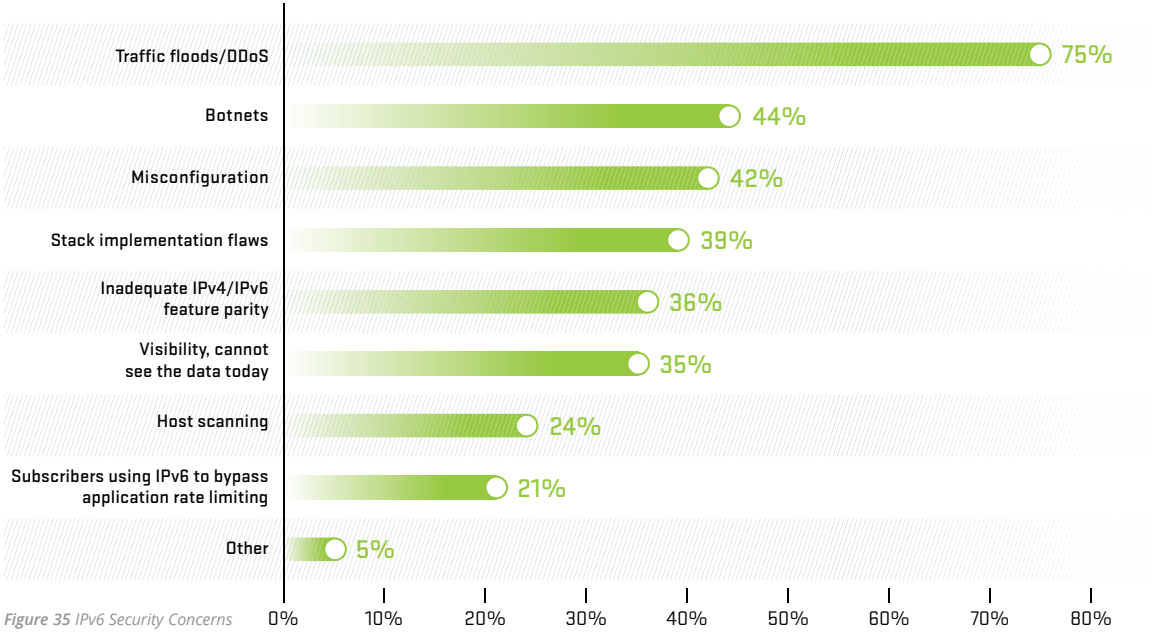


Figure 35 IPv6 Security Concerns

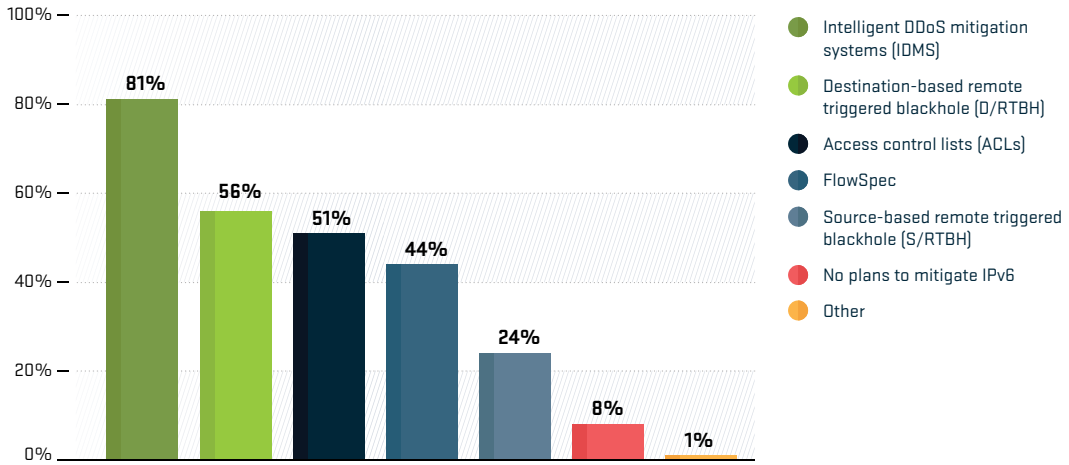


Figure 36 IPv6 Mitigation Capabilities

Organizational Security

Sixty percent of service providers have their own internal security operations center (SOC) team (Figure 37). However, the percentage of service providers without any SOC capabilities fell from 29 to 21 percent. This is positive news, and is likely due to the increased use of third-party and third-party augmented SOC capabilities. Service providers are relying more on outsourcing to enhance their internal security teams. This highlights the global challenges organizations face to build and maintain an internal security team of skilled practitioners.

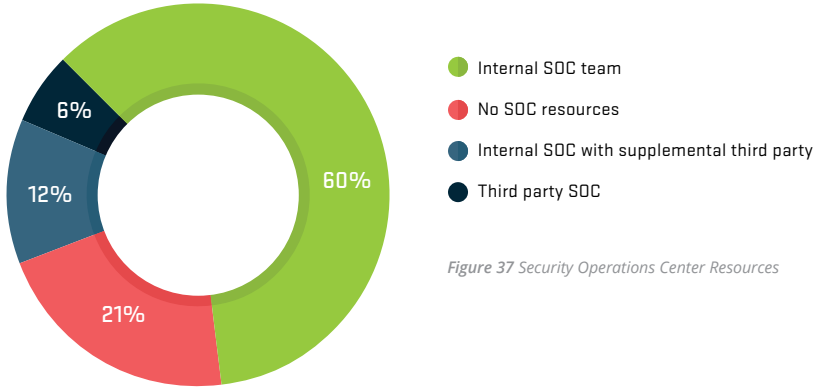


Figure 37 Security Operations Center Resources

Eighty-seven percent of service providers reported that they had some dedicated security personnel (Figure 38), an identical result to the previous year. Also, as in 2016, about a quarter had security teams of 30 or more people, compared to only 14 percent for enterprise, government and education (EGE) respondents.

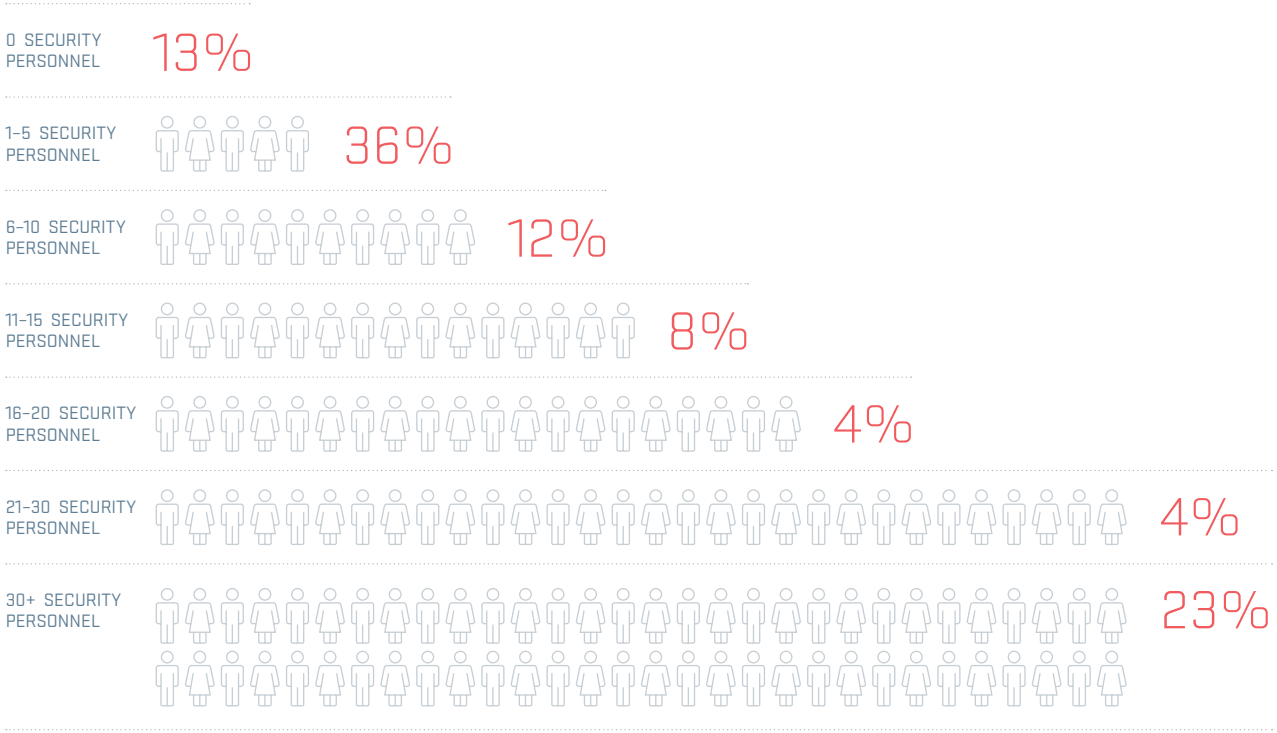


Figure 38 Dedicated Security Personnel

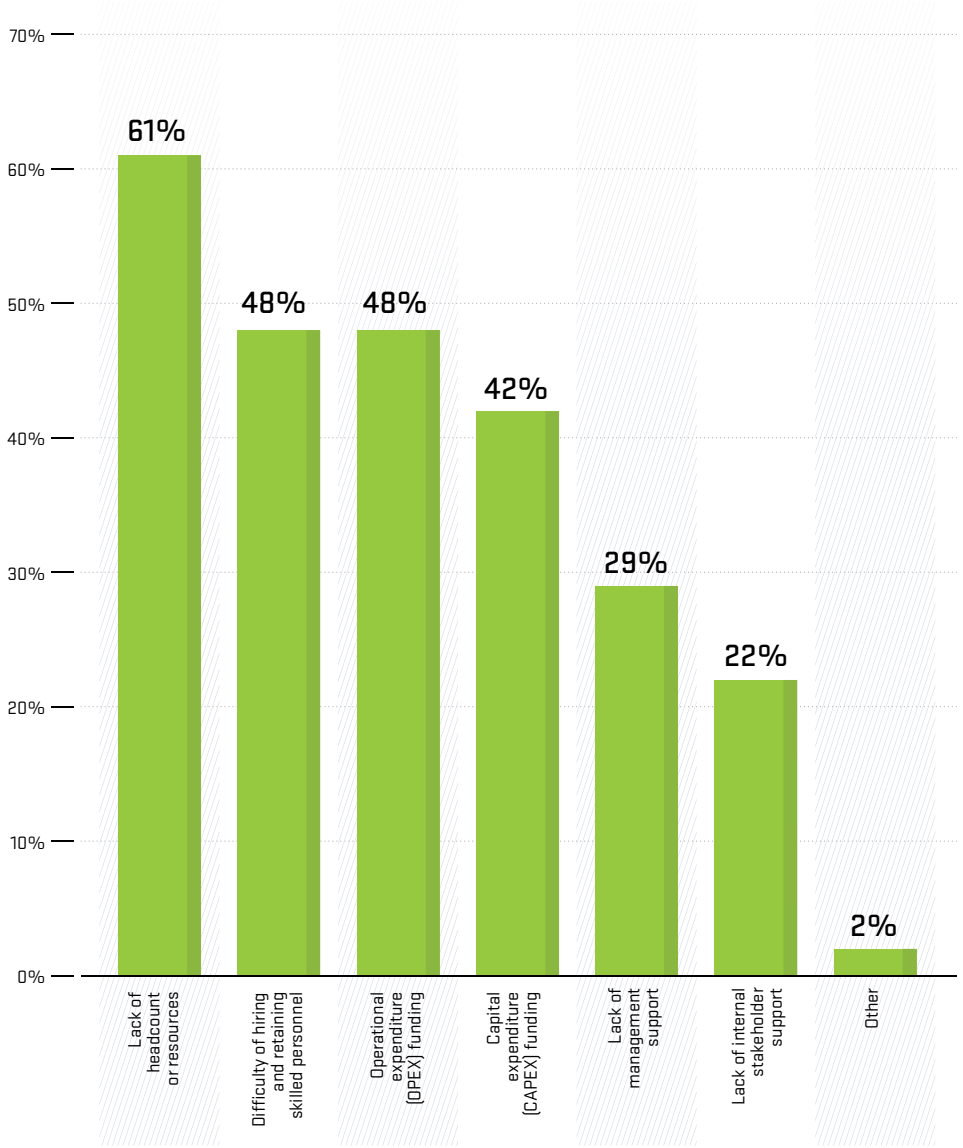


Figure 39 OPSEC Team Challenges

Looking at the challenges of building and maintaining operational security teams, the worldwide shortage of security analysts and incident responders was still a key issue in 2017. Lack of resources, along with the difficulty of hiring and retaining skilled personnel, were again the two main concerns for building an effective operational security (OPSEC) team (Figure 39).

The percentage of service providers carrying out DDoS defense simulations was similar to last year (Figure 40). However, the proportion of service providers that do not practice simulations and have no plans to do so increased from 29 to 34 percent. This is discouraging as dealing effectively with DDoS attacks is not just about technology, but about the people using the technology and the processes supporting it.

Thirty percent made time for incident response rehearsals at least quarterly, a decline from 38 percent in the previous year. However, based on anecdotal information, this reduction could be due to some service providers relying more on automation in their battle against DDoS attacks.

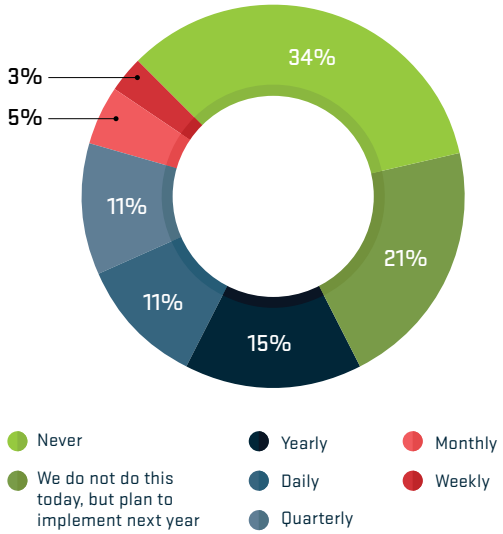


Figure 40 DDoS Simulations

For the second consecutive year the survey showed an overall decline in service providers implementing security infrastructure best practices (Figure 41). However, both of the top two methodologies, authentication for BGP and explicitly filtering routes announced by customers, slightly increased from 62 to 68 percent and from 58 to 59 percent respectively.

Surprisingly, given the popularity of reflection attacks over the last five years, the adoption of anti-spoofing filters decreased from 48 to 43 percent this year. The use of access control lists at the network edge also declined sharply this year from 54 to 47 percent.

On a more positive note, the adoption of the historically lesser-used methodologies increased. There was a greater use of maintaining up-to-date peer contact information, route hijacking monitoring, IRR route registration, blocking of known attack servers and generalized TTL security mechanism than in the previous year.

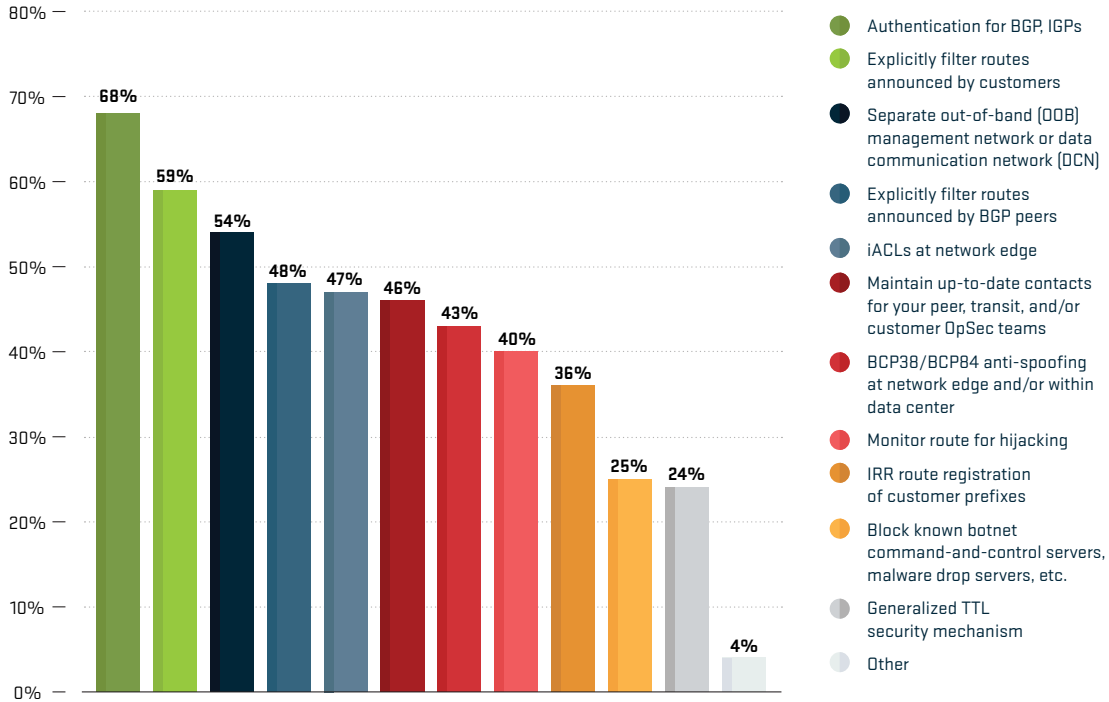


Figure 41 Security Best Practices

Another disappointing result in 2017 was the fact that less than a quarter of service providers participated in global operational security communities (Figure 42), or share or distribute observed cyber-security threats and gathered intelligence. The OPSEC communities have proven themselves very useful during high profile attacks in the last five years. We can only suspect that this downward trend, which started two years ago, is due to the challenges service providers face in building and maintaining an OPSEC team (Figure 42). From 41 percent in 2015, to 26 percent last year, the service providers' participation is down to 24 percent today.

Figure 42 OPSEC Participation

Data Center Operators

To better understand the resources that need protection in data centers, we asked respondents to identify what services their organizations offer (Figure 43). It comes as no surprise that managed hosting was the most common service offered. However, it was surprising to see public or private cloud services ranked second, pushing co-location services into third.

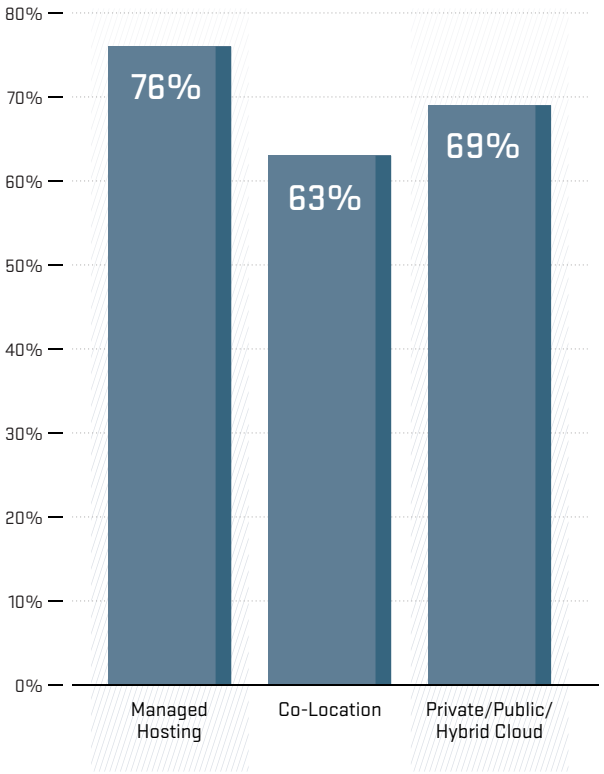


Figure 43 Data Center Services

Unexpectedly, a lower proportion of data center operators saw DDoS attacks targeting their environments (Figure 44), yet the financial impact of attacks grew significantly (Figure 47). Only 40 percent indicated they observed DDoS incidents in 2017, a significant decrease from 60 percent the previous year.

The frequency of attacks also decreased sharply, with only 36 percent seeing more than 10 attacks monthly as compared to 57 percent in 2016 (Figure 45).

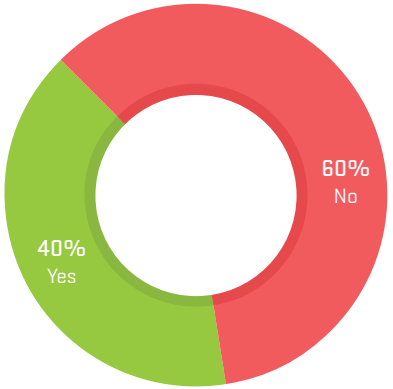


Figure 44 Data Center Experienced DDoS Attacks

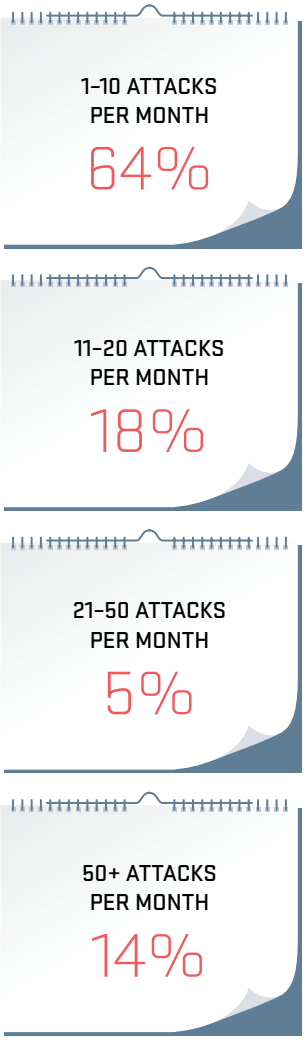


Figure 45 Data Center DDoS Attack Frequency

Despite less frequent DDoS attacks, the survey highlights the growing impact of incidents. Of those who had DDoS attacks, 91 percent observed at least one incident that affected their ability to deliver service. Seventy-eight percent experienced between 1 and 20 service-affecting attacks, a slight increase over 2016 (Figure 46).

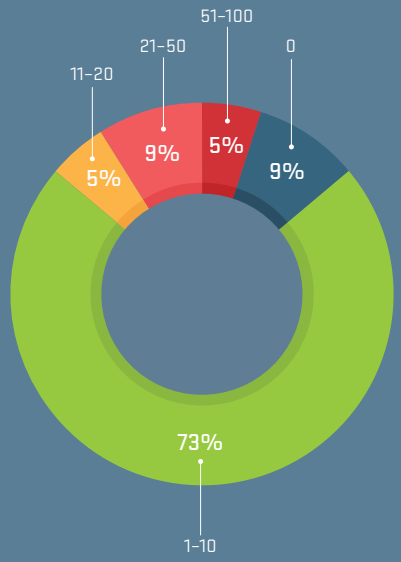


Figure 46 Data Center Service Affecting Attacks

The average cost of a successful DDoS attack to a data center operator significantly changed in 2017. In 2016, 45 percent of the operators reported an attack cost them less than $10,000 on average. In comparison, 45 percent indicated the average total cost of major attacks was between $10,000 and $50,000 per incident in 2017 (Figure 47). In fact, more than half of respondents experienced a financial impact between $10,000 and $100,000, almost twice as many as in 2016.

Looking at the cost break-out, respondents continue to see operational expenses as having the biggest impact on their business as a direct result of a DDoS attack (Figure 48). However, customer churn is now second at 48 percent. This demonstrates how sensitive customers are when it comes to the availability of their services and the DDoS protection provided by a data center operator. Putting this data into perspective, we believe that wide adoption of DDoS mitigation services made it harder for attackers to affect business processes, making them more conscious about the size and complexity of attacks they launched. Consequently, attacks were more advanced and once they passed through defenses, there was a greater impact on data center operations.

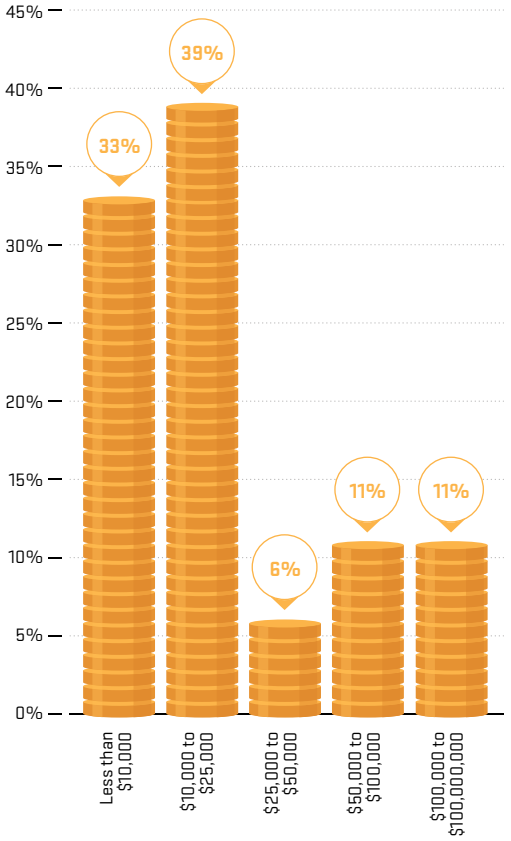


Figure 47 Data Center DDoS Cost

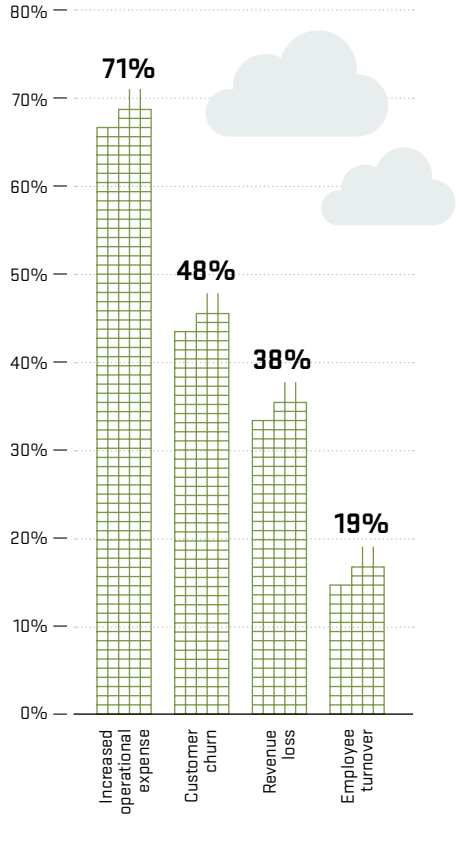


Figure 48 Data Center DDoS Business Impact

WE ASKED DATA CENTER OPERATORS IF THEY EXPERIENCED ATTACKS EXCEEDING THE TOTAL BANDWIDTH AVAILABLE TO THE DATA CENTER.

Historically we observed a growing trend of attacks saturating data centers:

2014	2016
33%	61%
2015	**2017**
50%	45%

This is a positive result which may be due to improved upstream volumetric DDoS protection.

The targets of DDoS attacks within data centers are similar to those in the previous year, with customers the most likely target (Figure 49). However, the percentage of data centers reporting outbound attacks generated by servers grew from 28 to 36 percent. Anecdotally, we have been aware for many years that compromised or rented data center servers are used as 'packet cannons.' It seems that data center operators are increasingly aware of this problem as well.

As in previous years, we asked data center operators what level and type of visibility they have in place. When it comes to visibility levels, there was mixed news. The percentage with Layer 3 and 4 visibility dropped from 77 percent in 2016 to 65 in 2017. However, there were more data centers with Layer 7 visibility, up to 25 percent from 21. It is also encouraging to see that one third of the respondents now have service assurance monitoring, and the proportion with no visibility has dropped from 12 to 10 percent (Figure 50).

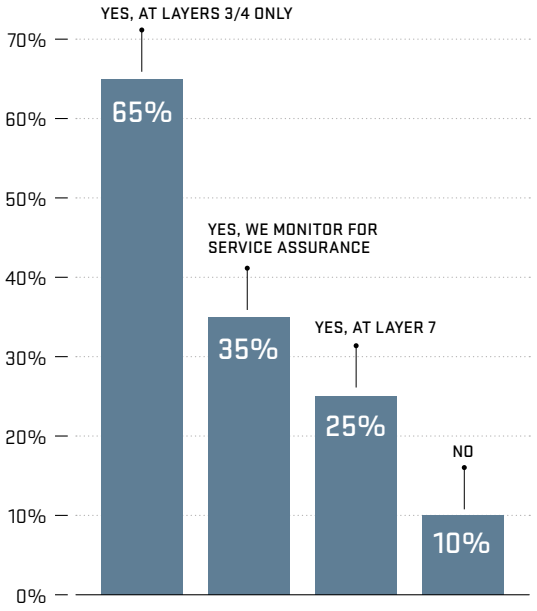


Figure 50 Data Center Internal Visibility

68%
INBOUND ATTACK
Data center management hosting, cloud or co-location customer

50%
INBOUND ATTACK
Data center service infrastructure (portal, management)

36%
INBOUND ATTACK
Data center infrastructure (routers, firewalls, load balancers)

36%
OUTBOUND ATTACK
Generated from server(s) within the data center to external host

9%
CROSS-BOUND ATTACK
Customer to customer

Figure 49 Data Center DDoS Targets

On a more positive note, approximately two thirds of data centers perform baselining of normal operations for intra data center traffic and the percentage of those actively looking for compromised devices grew from seven to 39 percent (Figure 51). Also, those with no visibility decreased from 20 to 14 percent.

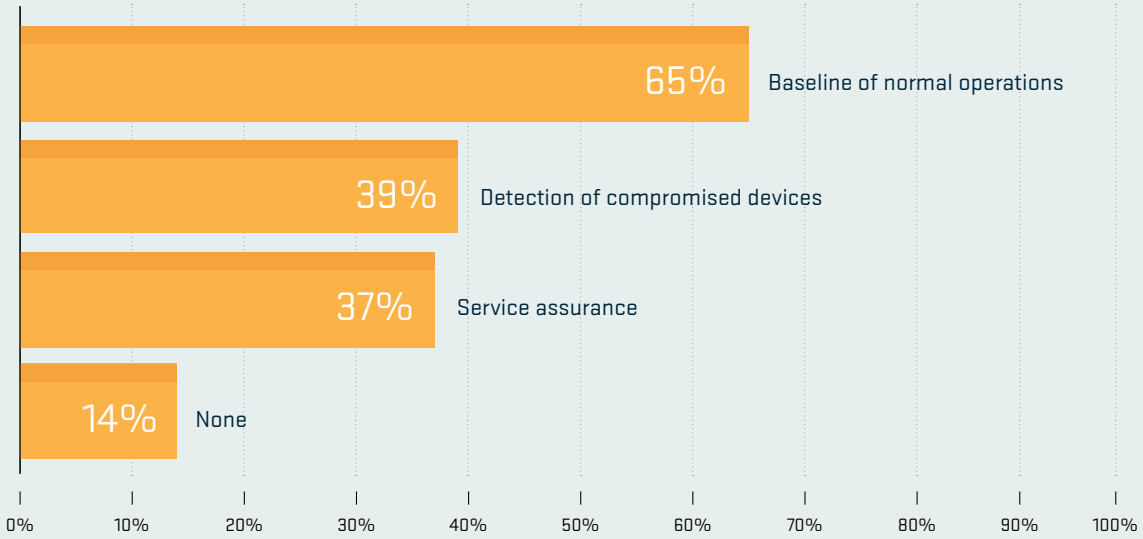


Figure 51 Data Center Outbound and Cross-Bound Visibility

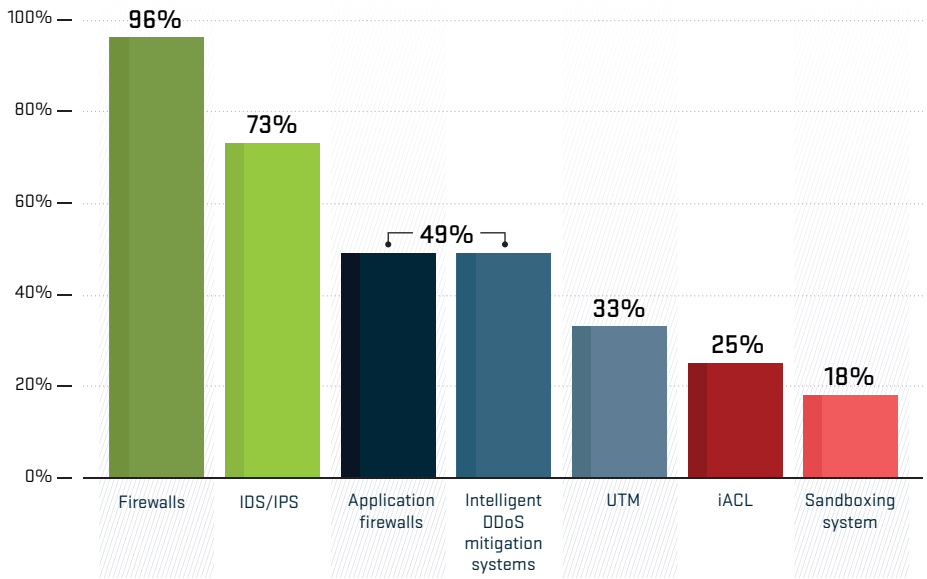


Figure 52 Data Center Perimeter Security Technologies

When it comes to the technologies used to protect data centers at their perimeter, the increased frequency of DDoS attacks seen in 2016 resulted in a wider adoption of Intelligent DDoS Mitigation Systems (IDMS) in 2017. About half of respondents indicated that an IDMS was now a part of perimeter protection, a sharp increase from the previous year's 29 percent. While IDMS shared third place with application firewalls, the most popular technologies remained firewalls and IDS/IPS (Figure 52).

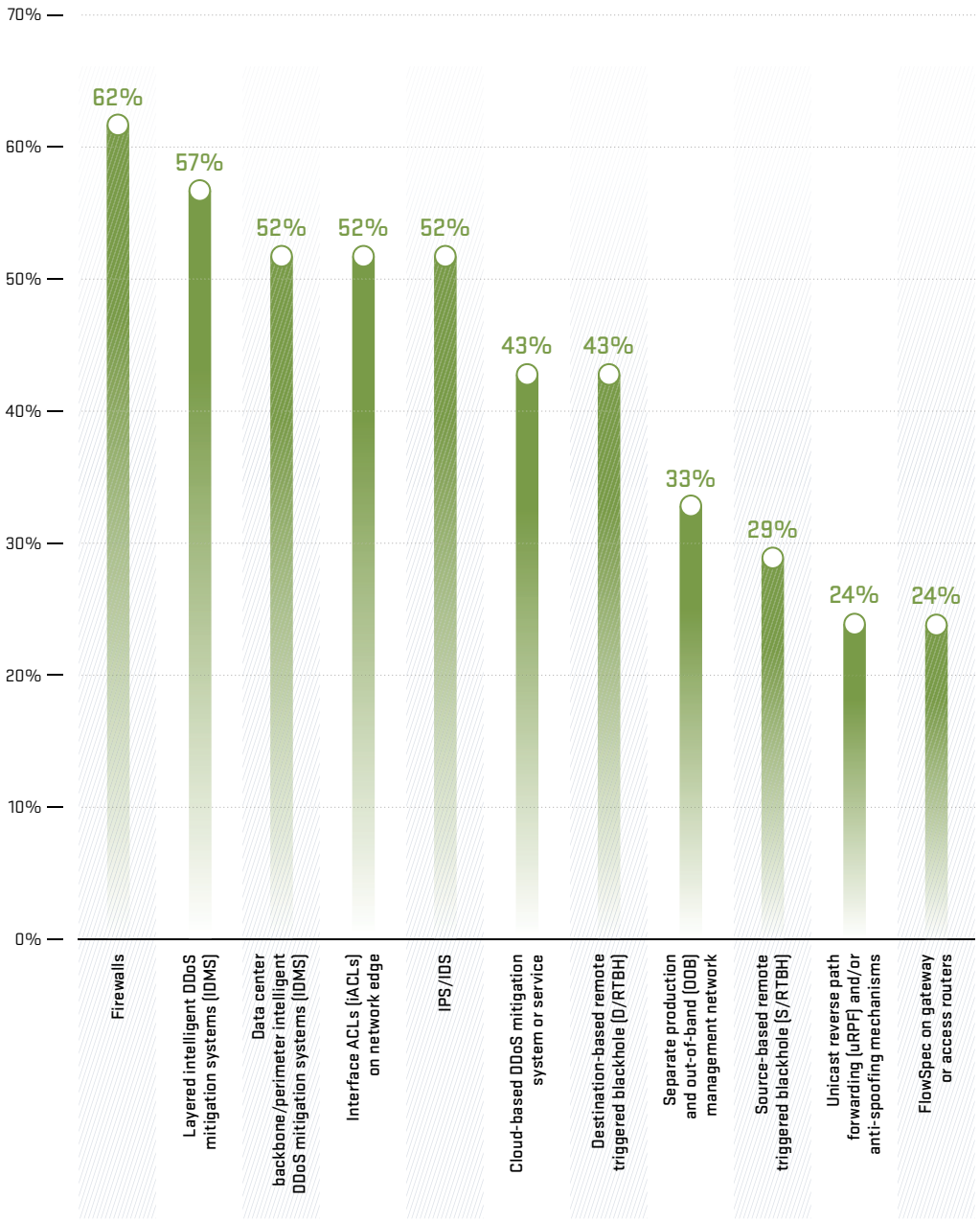


Figure 53 Data Center DDoS Protection Technologies

Looking at perimeter security, it is also worth noting what technologies were utilized for DDoS protection in 2017 (Figure 53). It is good to see that infrastructure ACLs (iACLs), perimeter IDMS and layered IDMS were in the top five of technology choices. The less positive news is that IDS/IPS was still considered a key element of a DDoS protection strategy by more than half of the respondents. Finally, a significant data point is that firewalls made a jump from last to first place, with 62 percent using them for DDoS defense.

This is especially disappointing if we take another data point into account. Forty-eight percent of data center respondents experienced firewalls, IDS/IPS devices and load-balancers contributing to an outage during a DDoS attack — an increase from 43 percent in 2016. We encourage organizations to review their DDoS mitigation architecture and move away, as much as possible, from stateful inspection methods to predominantly stateless architectures optimized for high packet load.

As to the types of DDoS protection offered by data center operators, it is encouraging that one quarter now include some capability within their base offering and 40 percent offer it as an add-on service. Further, an additional 15 percent plan to offer DDoS protection in the coming year. As data center customers demand availability and look for tighter service-level agreements (SLAs), a DDoS mitigation strategy becomes one of the most important factors in choosing a data center service.

Mobile Network Operators

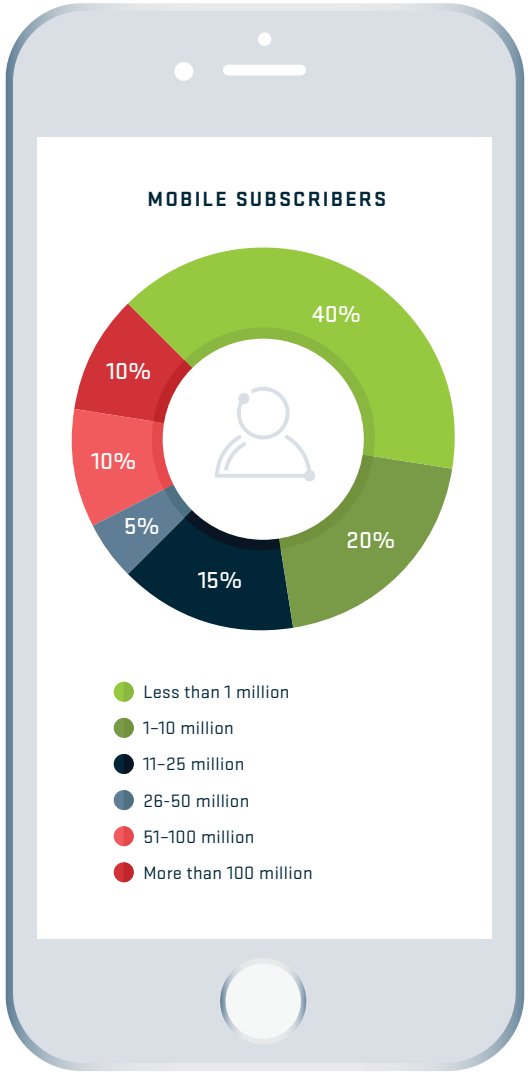


Figure 54 Mobile Subscribers

In 2017, 60 percent of mobile operator respondents had more than one million subscribers, down from 70 percent the previous year (Figure 54).

We asked mobile operators if they had experienced any security incidents on their networks that led to a customer-visible outage, and only a fifth reported such an incident, down from a third in 2016, a very positive trend (Figure 55).

SECURITY INCIDENTS THAT LED TO A CUSTOMER VISIBLE OUTAGE?

No
65%

Yes
20%

Do not know
15%

Figure 55 Customer-Visible Outage

In 2017, only 25 percent of mobile operators had the capability to detect compromised devices from their subscriber networks, down from 37 percent the previous year (Figure 56).

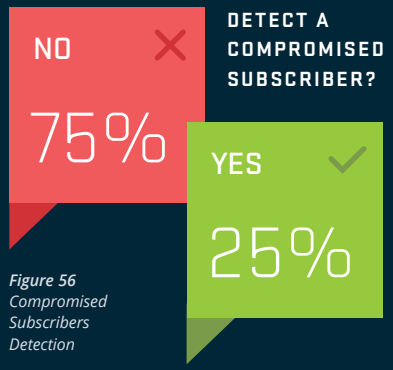


Figure 56 Compromised Subscribers Detection

This significant decrease in the ability to detect compromised devices is worrisome, as gaining better visibility of user devices is key for proactive and effective security incident handling.

Over half of mobile network operator respondents don't have visibility into their subscribers' botnet participation, which is not surprising considering they reported being less capable of detecting compromised devices (Figure 57).

Among those having visibility, 42 percent reported that five percent or less of their subscribers were compromised. Similar to last year, 16 percent reported that none of their subscribers have been compromised, which considering IoT botnet trends, is more likely due to a lack of visibility.

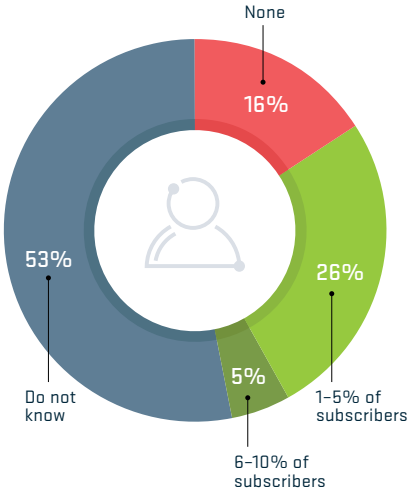


Figure 57 Compromised Subscribers

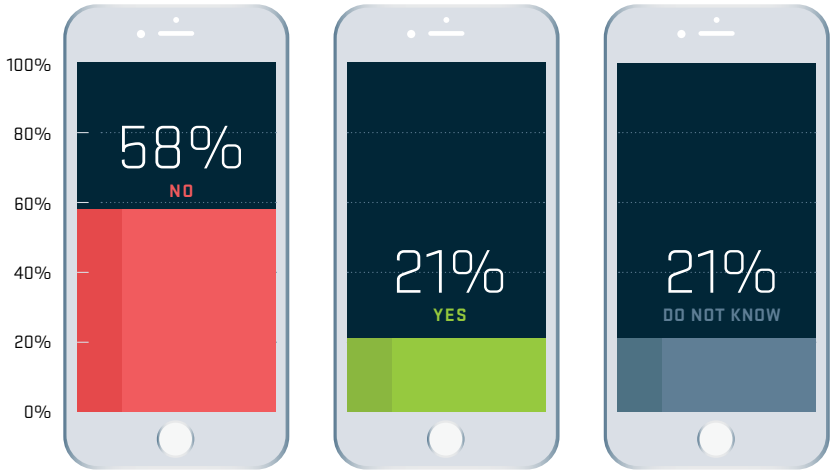


Figure 58 DDoS Attacks from Mobile Users

Fifty-eight percent of operators once again did not see DDoS attacks originating from their mobile user base (Figure 58). Of the remaining, one half noticed DDoS attacks from their subscriber network, while the other didn't know if attacks were generated by their mobile users.

The percentage of mobile network operators mitigating outbound attacks again increased substantially, from over one quarter in 2016 to 37 percent in 2017 (Figure 59). With over a quarter planning to mitigate outbound DDoS attacks in 2018, this is very positive news.

No plans
37%

Yes
37%

No, planning to in the next 12 months
26%

Figure 59 DDoS Attacks Mitigation from Mobile Users

It is very positive news that over a quarter are planning to start mitigating outbound DDoS attacks in 2018.

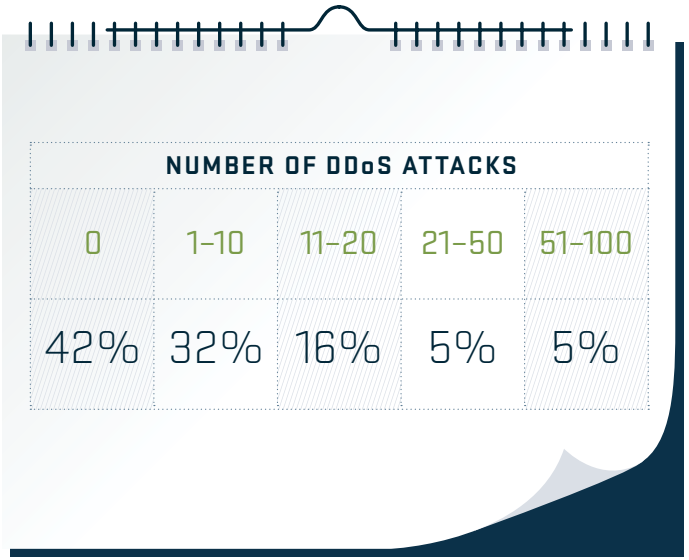


Figure 60 DDoS Attacks Per Month

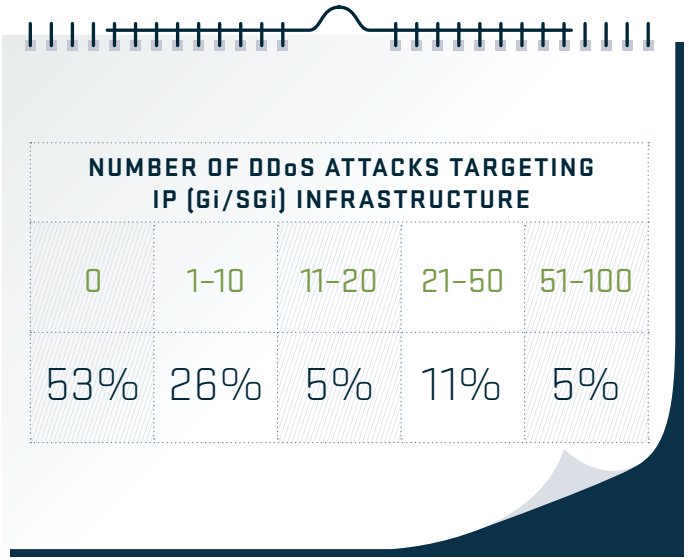


Figure 61 DDoS Attacks Per Month Targeting IP (Gi/SGi) Infrastructure

This year a much lower proportion of network operators observed DDoS attacks targeting their mobile infrastructure/users, from 74 percent in 2016 to 58 in 2017 (Figure 60). However, for those seeing attacks, there was an increase in those noticing between one and 10 attacks per month, at 32 percent up from 21 percent the previous year. The percentage of mobile network operators experiencing over 10 attacks per month fell to 26 percent from 55 percent last year.

The proportion of mobile network operators reporting DDoS attacks targeting their Gi/SGi interface decreased sharply this year, from 72 percent previously to only 47 percent (Figure 61). Overall, there was also a noticeable reduction in the number of attacks seen per month. Only the number of respondents noticing between one and 10 attacks per month increased slightly, from 22 percent to 26 percent.

We have stressed in the previous surveys how the Gi/SGi interface is a critical part of any mobile operator's network, and we were pleased to see a large increase in operators with visibility at Layers 3 and 4, up from 47 percent in 2016 to an impressive 68 percent in 2017 (Figure 62). Even though visibility at Layer 7 decreased from 35 to 26 percent, the overall improvement in visibility is a very positive sign.

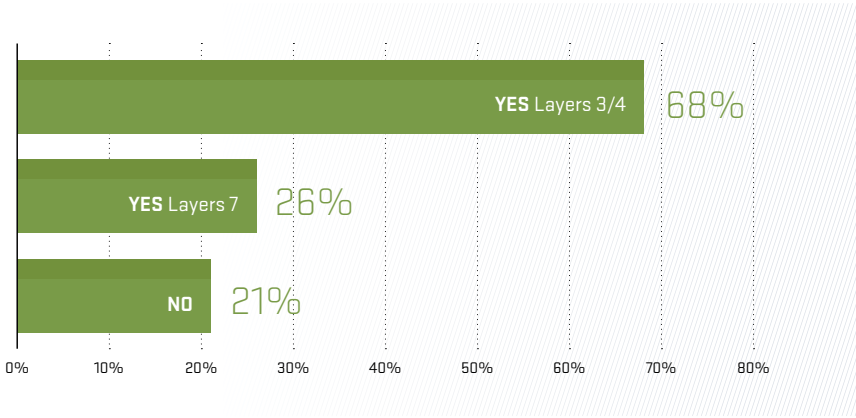


Figure 62 Visibility at IP (Gi/SGi) Backbone

Special Report

ATLAS

NETSCOUT Arbor's Active Threat Level Analysis System (ATLAS®) gathers statistics from NETSCOUT Arbor SP deployments around the world.

ATLAS delivers insight into approximately one third of global internet traffic. There are currently more than 400 networks participating in the ATLAS initiative. Statistics are shared hourly which include DDoS attack details, along with other traffic information. NETSCOUT Arbor's team collates and analyzes this unique data set to determine key trends in DDoS attack activity.

EDITOR'S NOTE

In early 2017, the NETSCOUT Arbor ATLAS team introduced a new data processing engine for the ATLAS system; this new approach has improved Arbor's ability to more accurately identify DDoS events. As a result, some of the ATLAS DDoS attacks figures for 2016 are different from the values used in last year's report. For the sake of consistency, we have run the data collected in 2016 through the new engine and that resulted in new figures.

Attack Size

Without question, 2016 was a dramatic year for DDoS attacks, with the emergence of IoT botnets driving the peak attack size to 841 Gbps. In 2017, the largest attack observed by ATLAS was a 641 Gbps attack (Figure AT1) directed at a target in Brazil. The 641 Gbps number from ATLAS aligns closely with the largest attack reported by the WISR survey respondents this year.

One significant difference between 2017 and 2016 (Figure AT2) was a significant decrease in the number of massive attacks over 100 Gbps (444 versus 1087) and 200 Gbps (40 versus. 125).

This year-over-year decline was due primarily to a major sporting event in Brazil over the summer of 2016 that experienced a high level of targeting.

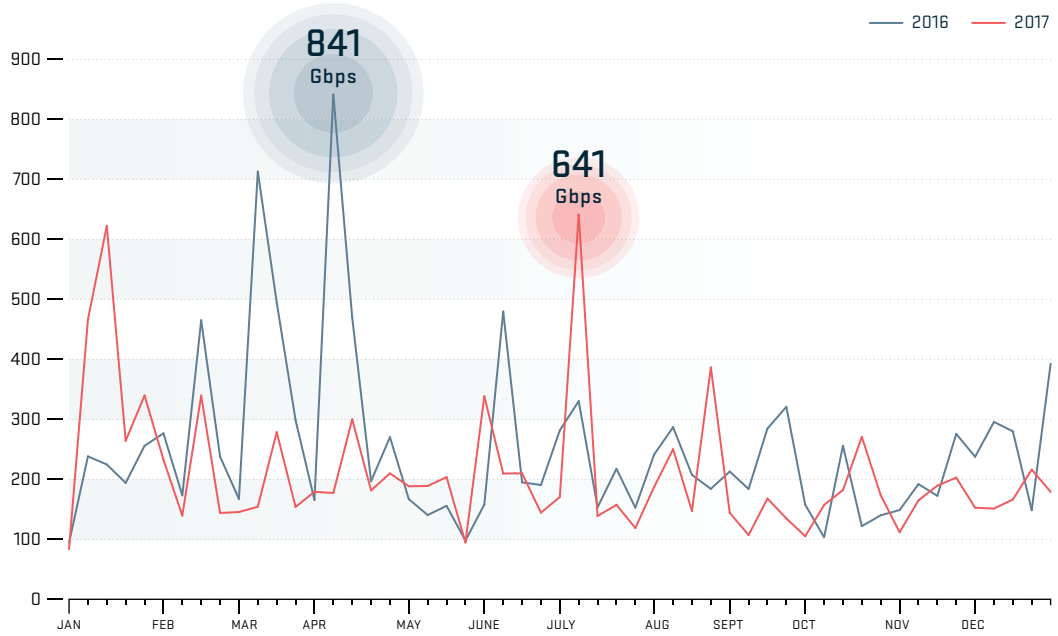


Figure AT1 ATLAS Peak Monitored Attack Size (Gbps), 2016 vs. 2017

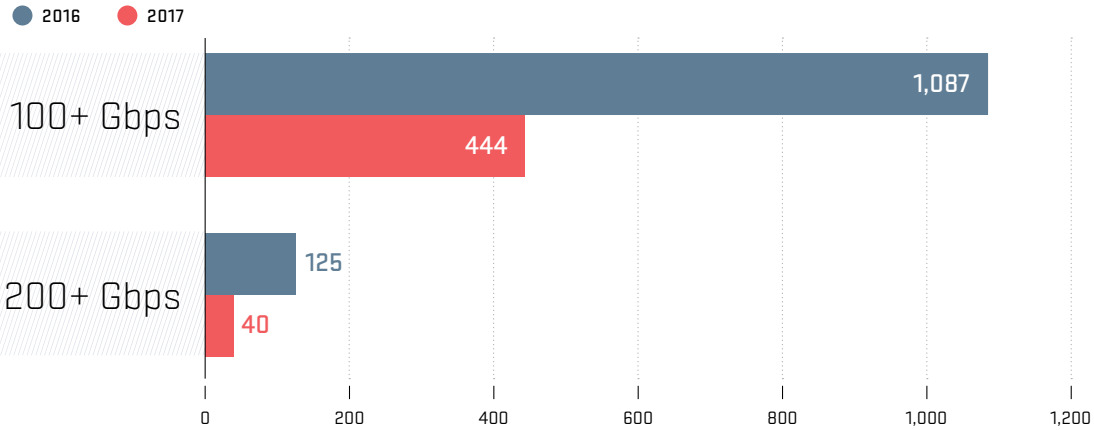


Figure AT2 Growth in Large Attacks 2016 vs. 2017

Although the number of attacks over 100 Gbps in 2017 is down from last year, the overall mix of attack sizes is still shifting up. This year, the percentage of attacks over 1 Gbps has increased to 22 percent, growing three years in a row. The vast majority of attacks, 87 percent, are still smaller than 2 Gbps (Figure AT3).

Attack Size Breakout

Less than 500 Mbps	67.09040%
500 Mbps–1 Gbps	10.81670%
1 Gbps–2 Gbps	8.98951%
2 Gbps–5 Gbps	8.97777%
5 Gbps–10 Gbps	3.02474%
10 Gbps–20 Gbps	0.80118%
20 Gbps–50 Gbps	0.26095%
50 Gbps–100 Gbps	0.03330%
100 Gbps–200 Gbps	0.00497%
200 Gbps–500 Gbps	0.00046%
500 Gbps–1 Tbps	0.00004%

Figure AT3 Attack Size Breakout

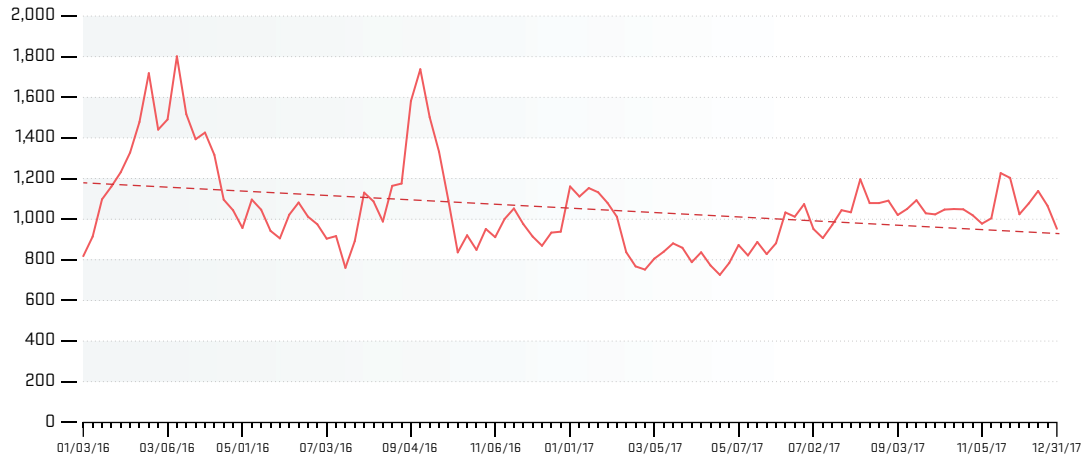


Figure AT4 ATLAS Average Attack Size (Mbps) 2016–2017

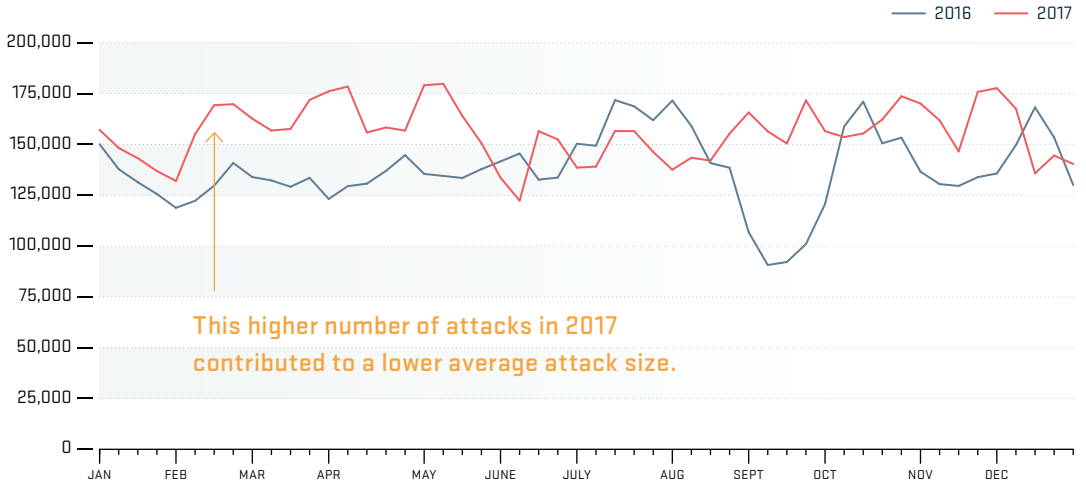


Figure AT5 Number of DDoS Attacks 2016 vs. 2017

Average attack size in 2017 was 990 Mbps, a slight decrease from last year's 1,133 Mbps. Looking at the monthly trend over 2017, we see that the average attack size was over 1 Gbps in the second half of the year (Figure AT4). On the surface, this appears to be a simple linear reduction in average attack size. However, in terms of attack frequency, we see an increase in the number of attacks in 2017 versus 2016 (Figure AT5).

While the number of very large attacks decreased in 2017, the number of attacks between 2 Gbps to 5 Gbps is growing steadily (Figure AT6).

Again, this may be due to the fact that there were major International events in 2016 which led to a spike in large volume attacks compared to 2017.

We believe this is also an indication of attacker innovation as they develop new attack vectors and utilize new tools such as the Mirai botnet's ability to launch application-layer as well as volumetric attacks.

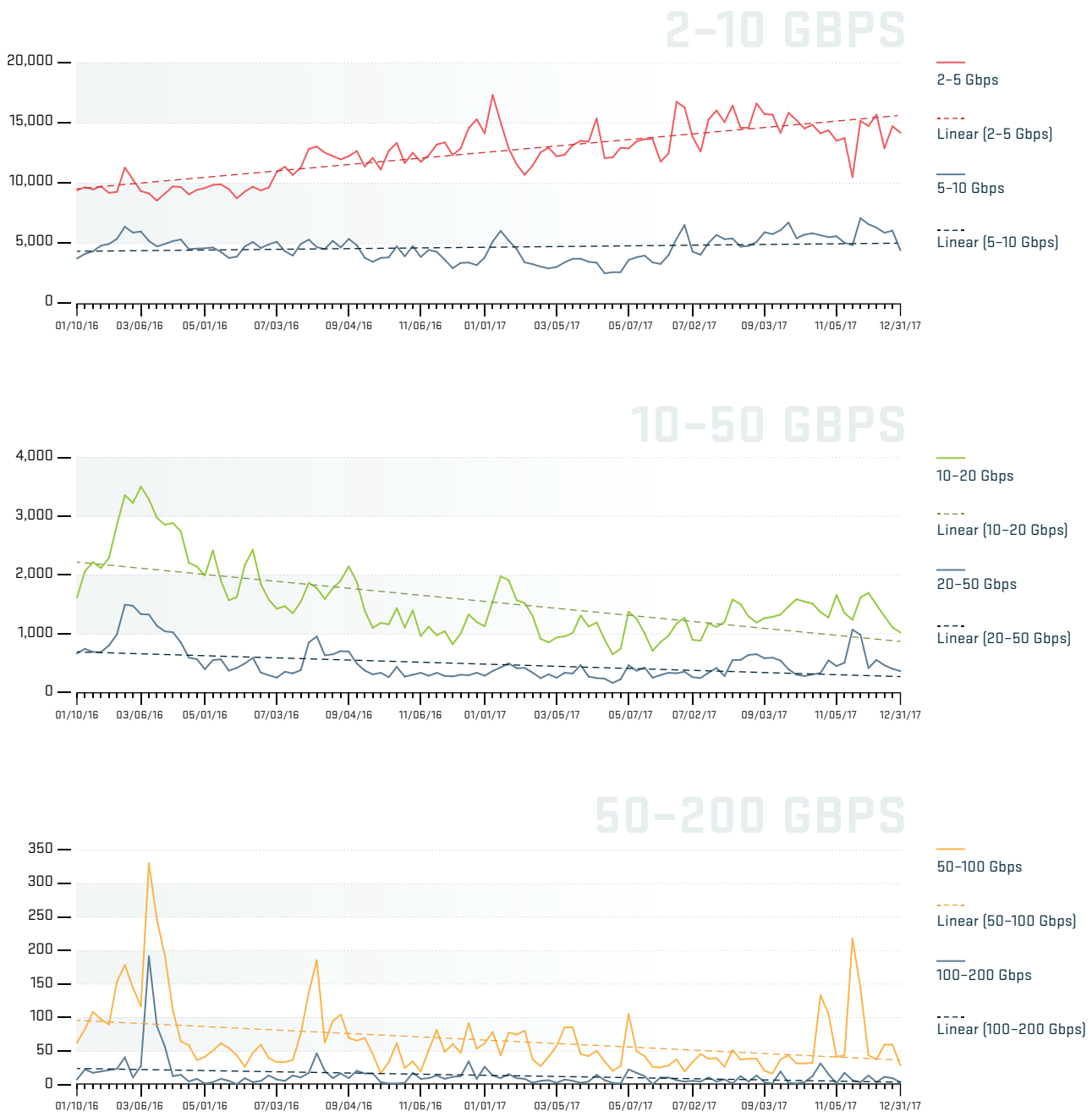


Figure AT6 Average Attack Frequency 2016–2017

THIS YEAR, WE HAVE EXTENDED OUR ANALYSIS TO INCLUDE DIFFERENT GEOGRAPHICAL REGIONS:

- North America
- Latin America
- Europe
- Middle East
- Africa
- Asia-Pacific

Using the same metrics — number of DDoS attacks, peak attack sizes and average attack sizes — the regions were compared.

Looking at the number of DDoS events observed in the different regions (Figure AT7), Latin America has a lower number of attacks compared to the other regions.

We also noticed that starting in August 2017, there is a trend of more attacks seen in Europe than North America and Asia-Pacific.

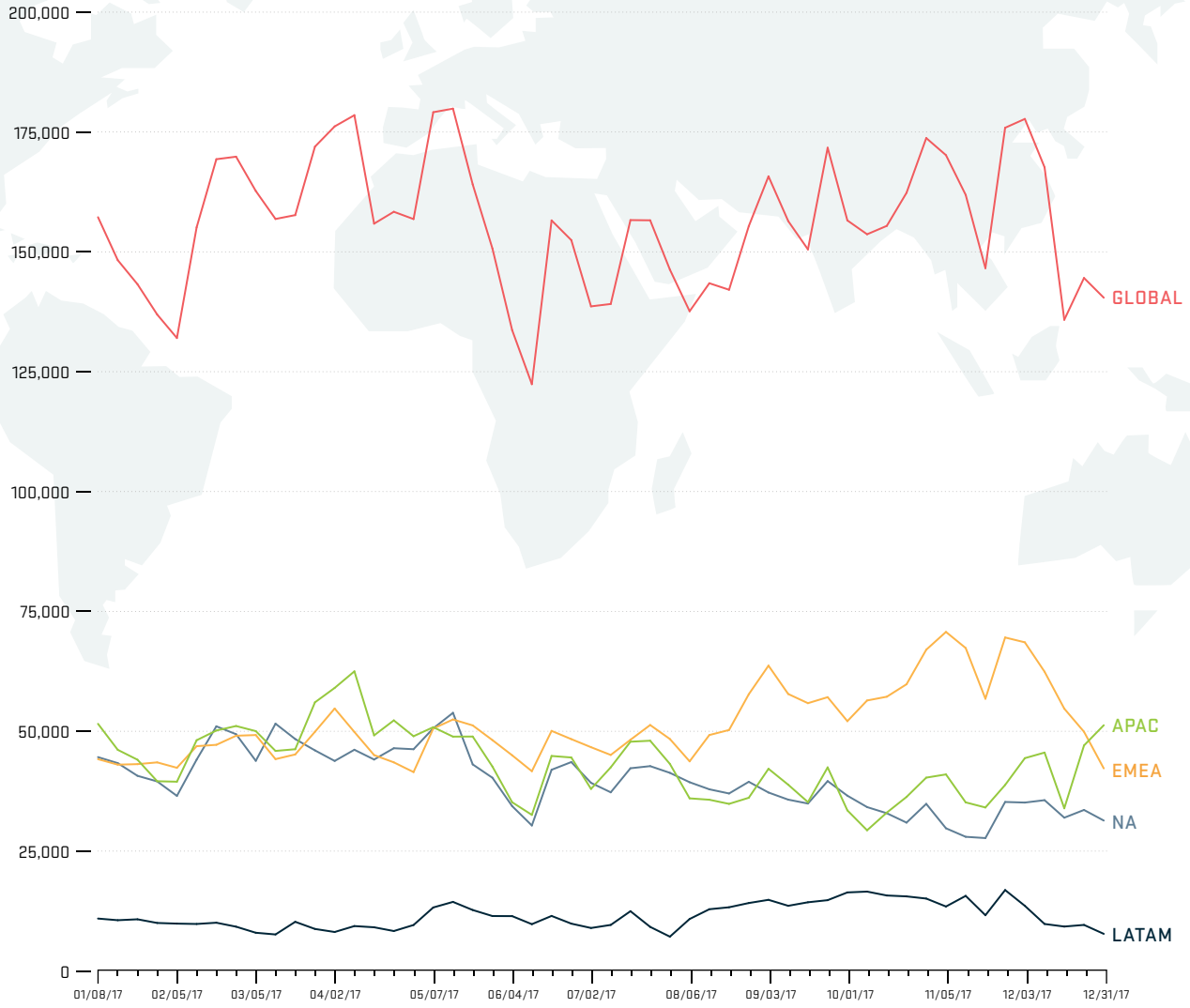


Figure AT7 Number of Attacks by Regions

Although the number of attacks is lower in the Latin America region, the largest attack monitored in 2017 targeted Brazil. Overall, the difference in terms of peak attack size is not that significant between the four regions. (Figure AT8).

Comparison of average attack size between the regions reveals an interesting fact — the average in North America and Europe are actually higher than worldwide average (Figure AT9). In contrast, the Latin America and Asia-Pacific regions both show slightly lower attack sizes than the global number, this indicates a higher proportion of smaller attacks in Asia-Pacific and Latin America regions compared to the others.

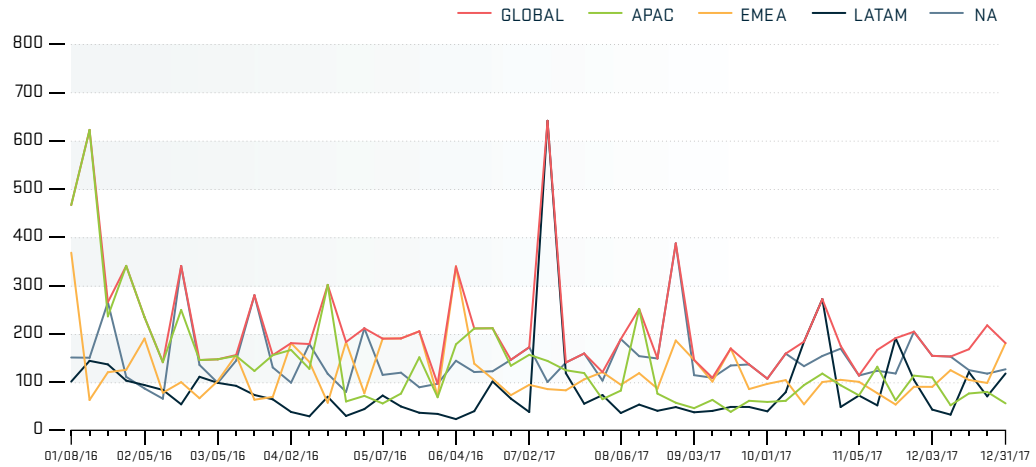


Figure AT8 Peak Attack Sizes by Regions (Gbps)

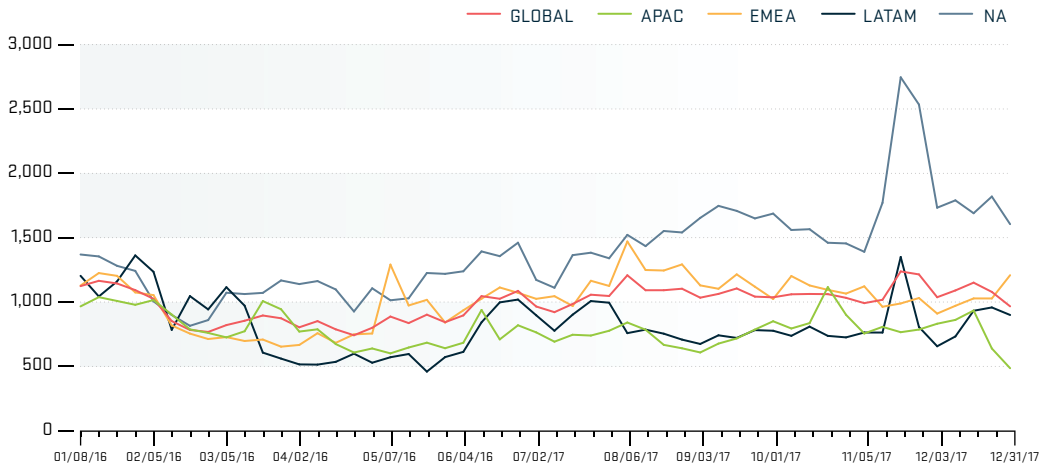


Figure AT9 Average Attack Sizes by Regions (Mbps)

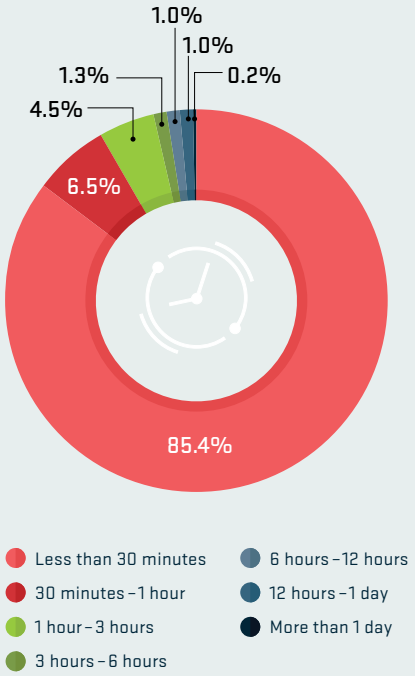


Figure AT10 Attack Duration

Similar to the previous two years, 92 percent of attacks last less than one hour (Figure AT10). The average duration of an attack in 2017 was around 46 minutes, down from 55 minutes last year.

As we stated last year, attackers usually start/stop an attack sporadically over an extended period of time. As a result, the average duration of an attack is less than an hour but a typical attack campaign lasts much longer than that.

Target Countries

Looking at the top 10 countries attacked in 2017, it is very interesting that the top four spots are exactly the same as last year, with similar percentage as well (Figure AT11). The top targets for attacks greater than 10 Gbps were the United States and Hong Kong. While the other countries in the top ten are nearly identical to last year, the positions vary quite a bit (Figure AT12).

It should be noted that mapping DDoS source/destination IP addresses to geographical locations is challenging due to various reasons including source address spoofing by attackers, widely deployed CGNAT and CDN technologies.

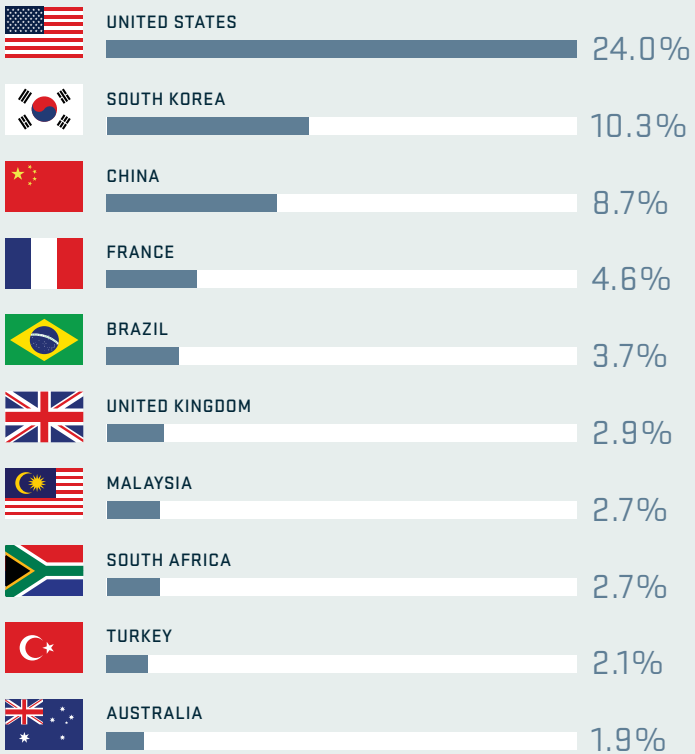


Figure AT11 Top Targeted Countries for DDoS Attacks by Percentage

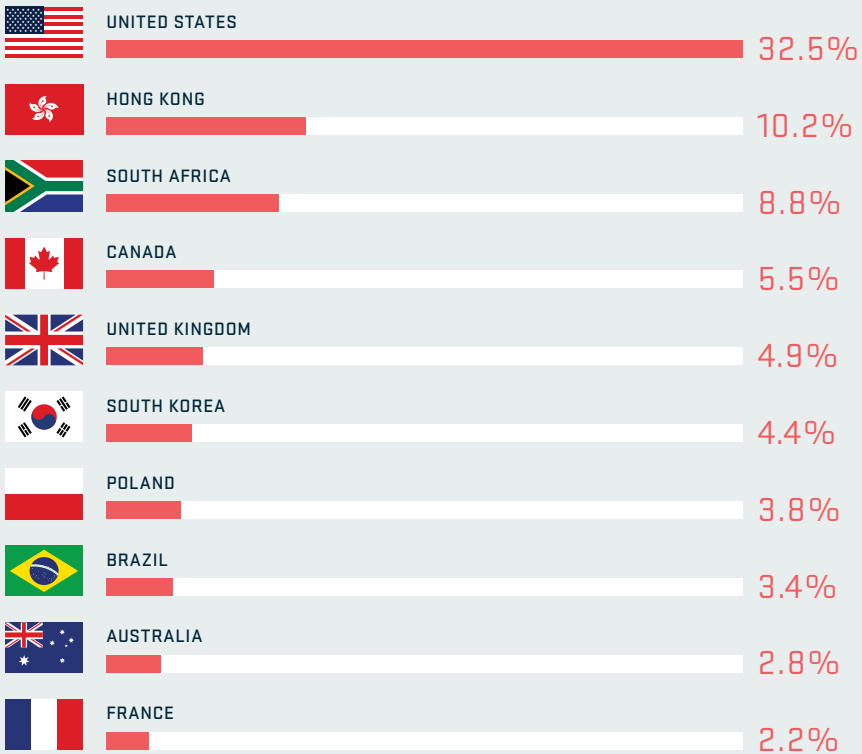


Figure AT12 Top Targeted Countries for DDoS Attacks Greater Than 10 Gbps by Percentage

Reflections

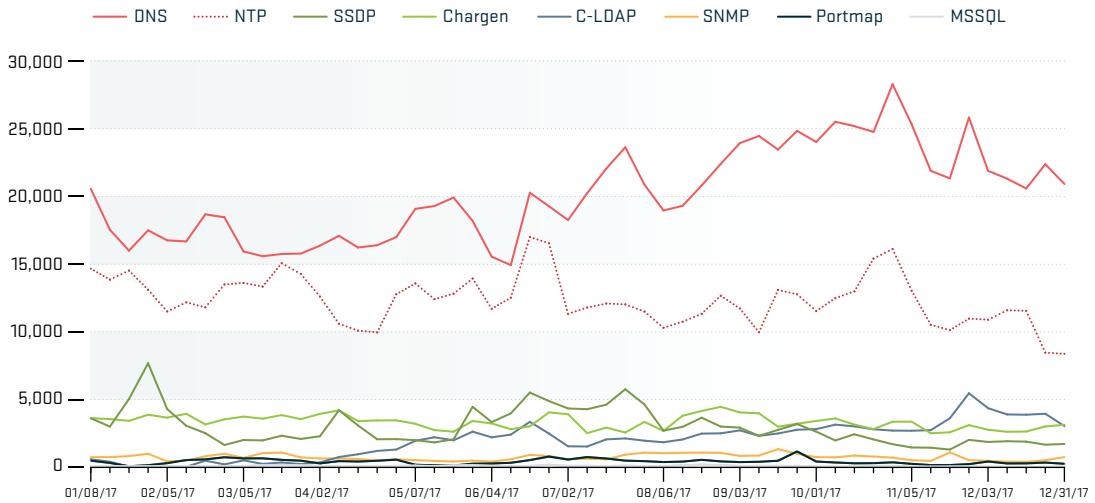
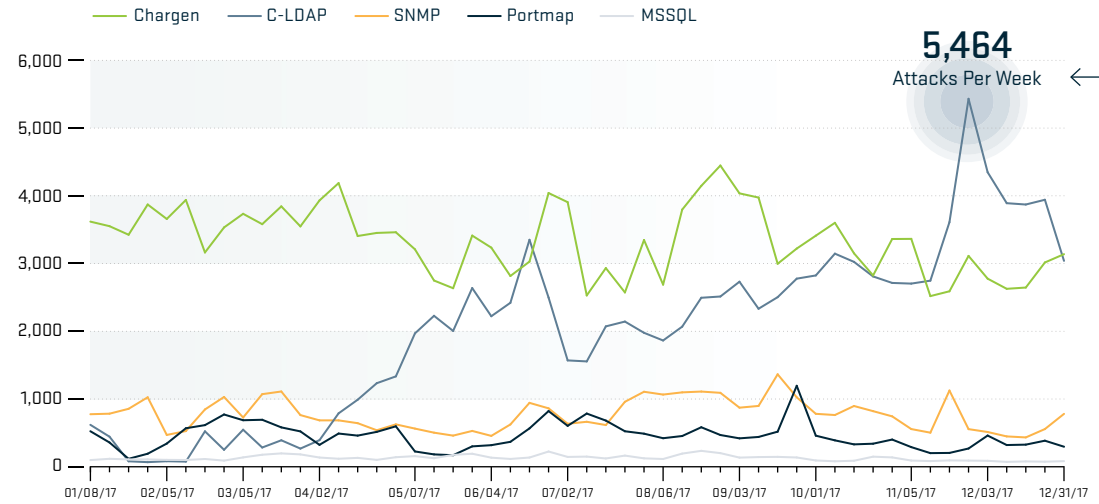


Figure AT13 Reflection/Amplification Attacks, Count Per Week

In 2016, we observed a resurgence of DNS as the dominant protocol used for reflection/amplification attacks. This year, DNS continued to be the most common reflection/amplification attack vector. In fact, the number of DNS reflection/amplification attacks is greater than all the other attack vectors combined. The number of DNS attacks is nearly double the number of NTP reflection/amplification attacks, which came in second (Figure AT13).

Attackers always look for new exploits and this year we observed massive growth in the use of C-LDAP for reflection/amplification attacks during the second half of the year (Figure AT14).



C-LDAP reflection/amplification attacks doubled in the last six months to a peak of 5,464 attacks per week.

Figure AT14 Number of Reflection/Amplication Attacks

Looking at the whole of 2017, once again DNS, NTP, Chargen and SSDP represent the top reflection/amplification attack vectors (Figure AT15). While the percentage of DNS and NTP attacks remain almost the same as last year, the number of attacks from Chargen and SSDP reflection/amplification attack has dropped from a combined total of more than 400,000 attacks in 2016 to around 330,000 attacks in 2017. On the other hand, C-LDAP reflection/amplification is definitely on the rise.

It also worth mentioning that a lot of the attacks observed are multi-vectors attacks, which are attacks where more than one type of vector is deployed simultaneously. For example, in 2017, 10 percent of all reflection/amplification attacks included more than one attack vector (Figure AT16).

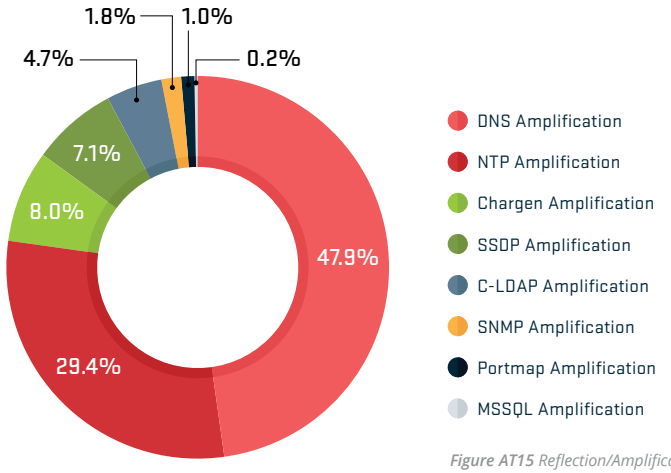


Figure AT15 Reflection/Amplification Attacks by Percentage

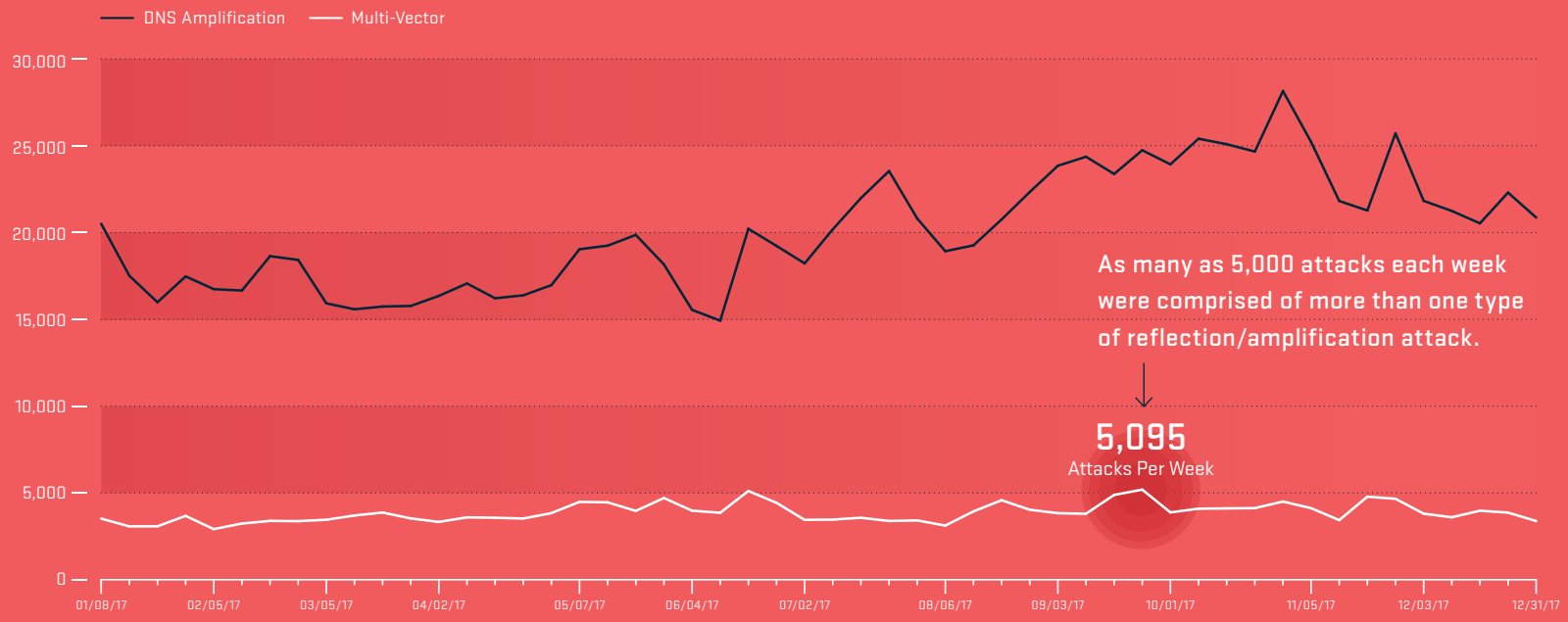


Figure AT16 Multi-Vector Reflection/Amplification Attacks

The average attack size for reflection/amplification is typically higher, as these attacks are designed to be volumetric in nature with the goal of saturating internet bandwidth. Compared to last year, the average attack sizes of reflection/amplification attack vectors decreased slightly (Figure AT17).

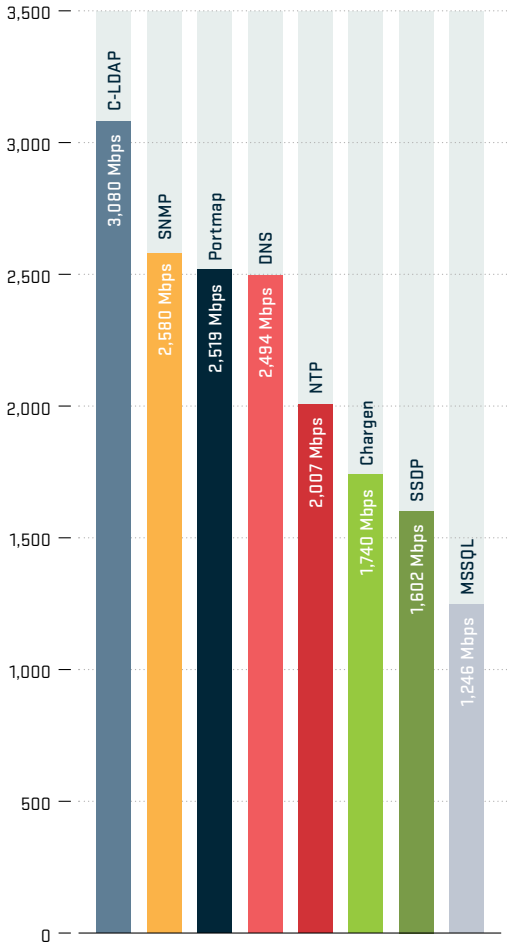


Figure AT17 Reflection/Amplification Attacks, Average Attack Sizes (Mbps)

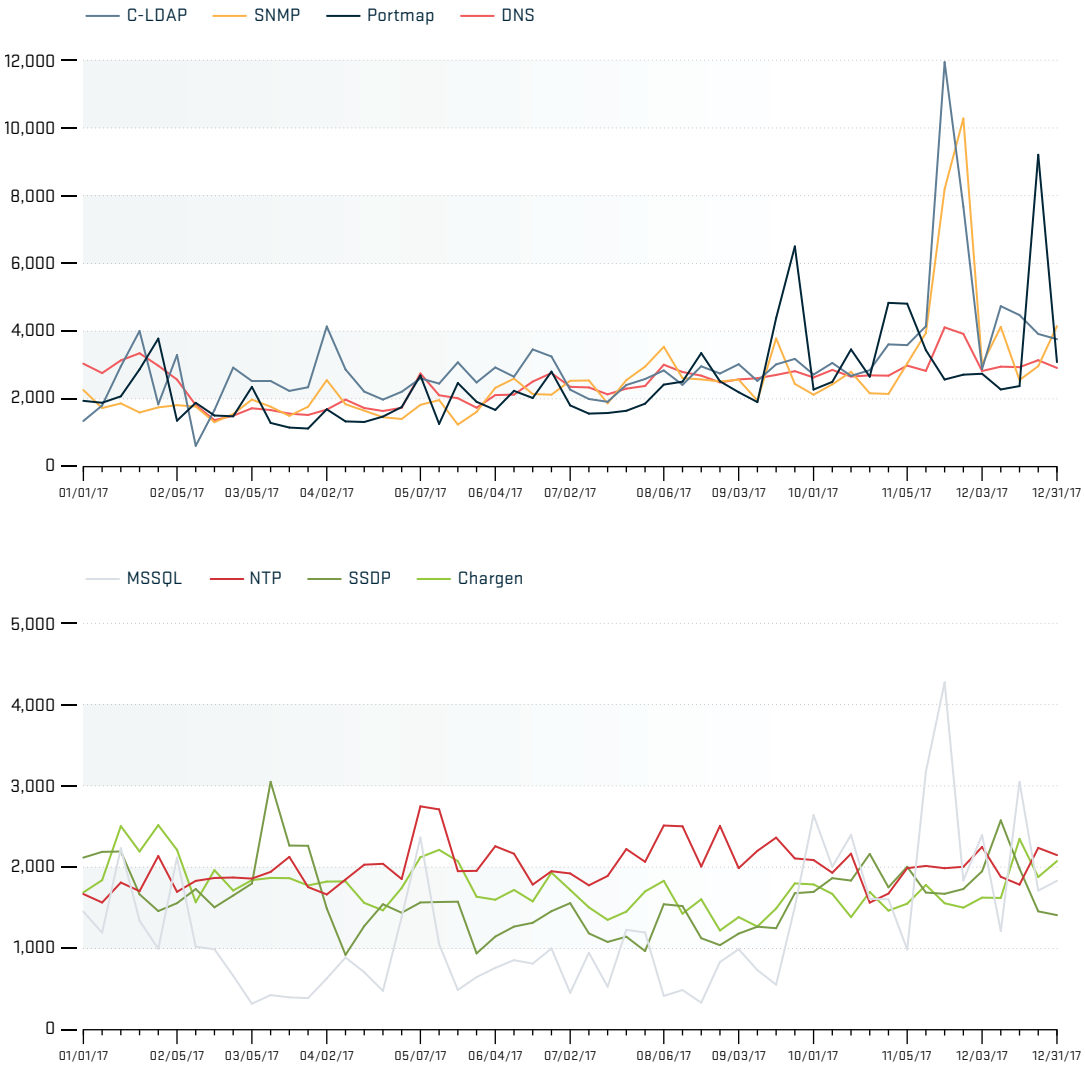


Figure AT18 Reflection/Amplification Attacks, Average Size Trend

The average attack sizes of the reflection/amplification attacks are slightly lower than 2016. Looking at the 2017 timeline graph (Figure AT18), the average attack sizes of most reflection/amplification attacks increased slightly throughout the year, except for Chargen and SSDP attacks.

The largest reflection/amplification attack monitored this year was a 641 Gbps DNS reflection/amplification attack. In the second place was a 622 Gbps NTP attack, a 30 percent increase from last year. In general, peak attack sizes of all reflection/amplification attacks have decreased from last year, except for NTP, CLDAP and SNMP (Figure AT19).

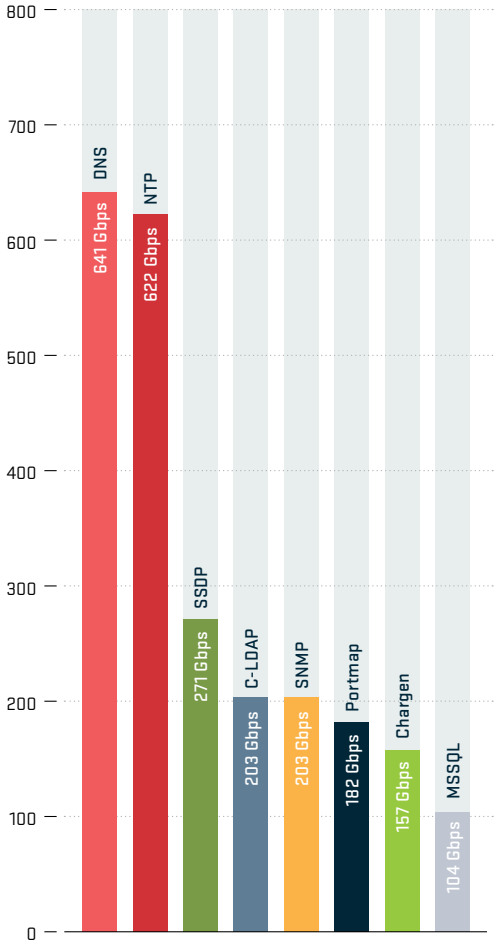


Figure AT19 Reflection/Amplification Attacks, Peak Attack Sizes (Gbps)

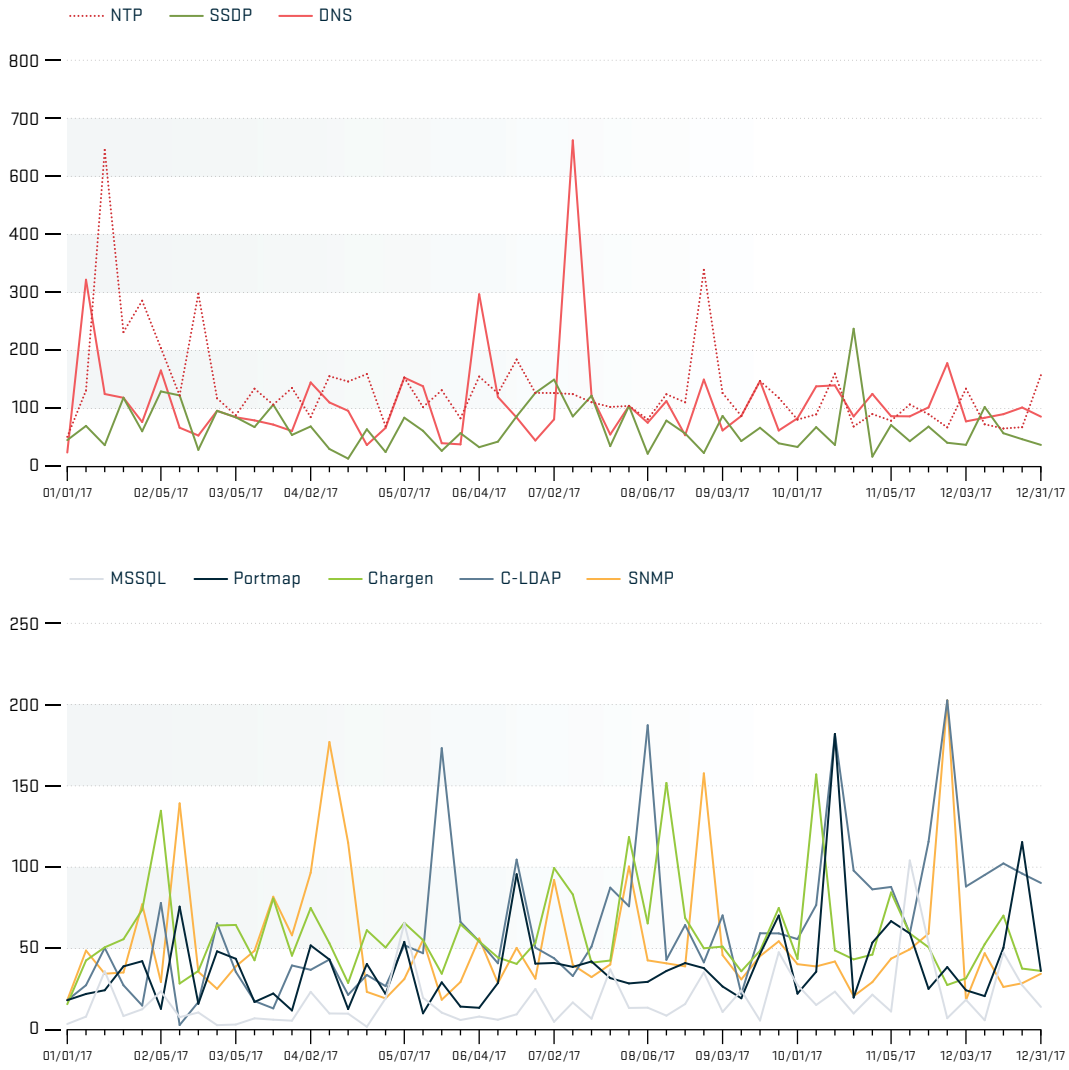
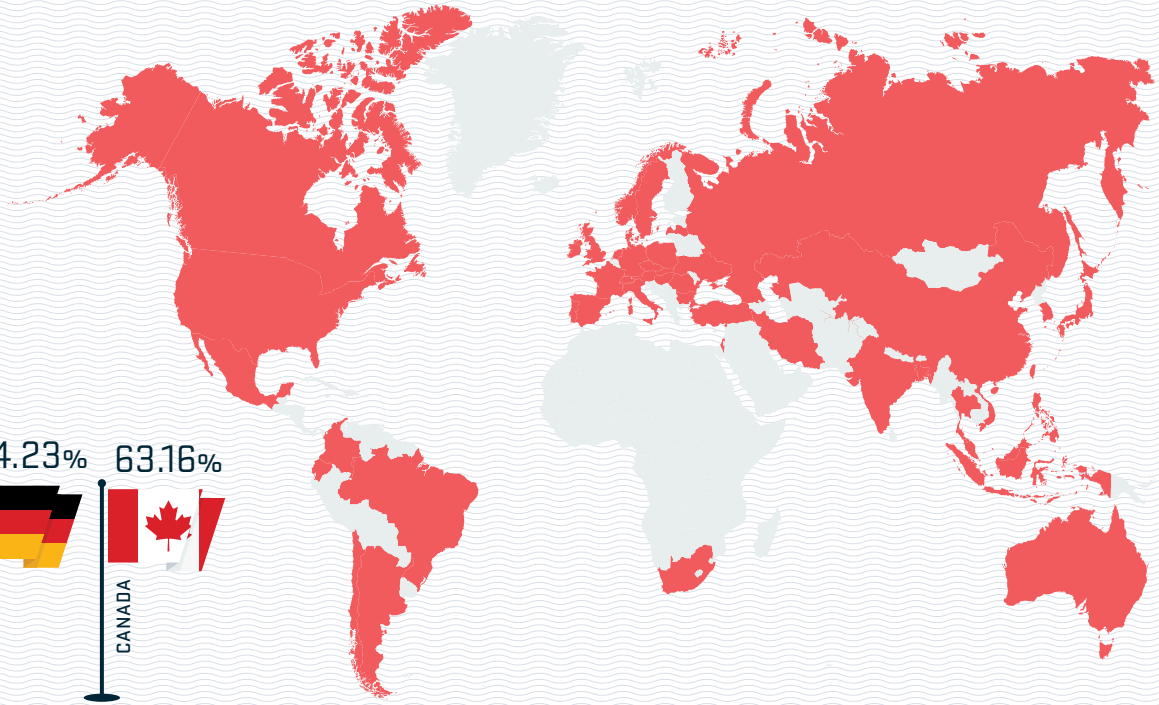


Figure AT20 Reflection/Amplification Attacks, Peak Size Trend (Gbps)

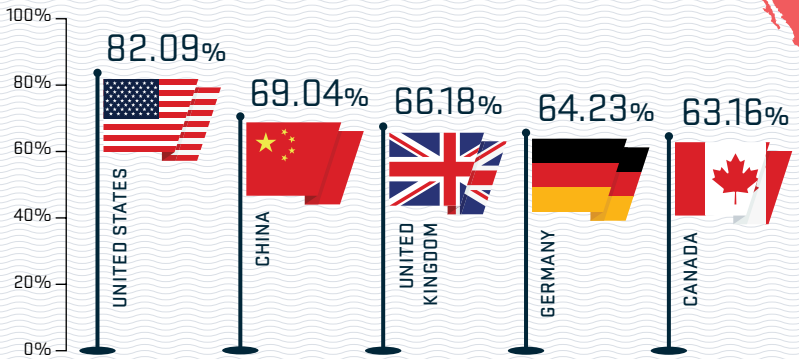
As mentioned before, DNS and NTP reflection/amplification attacks are the dominant attack vectors. In fact, both DNS and NTP have seen peak attack sizes greater than 600 Gbps. Looking at the peak attack size timeline graph (Figure AT20), attackers are varying the attack vectors, with different protocols being chosen to be the 'weapon' used. C-LDAP reflection/amplification became a popular choice during the second half of 2017, growing in size as well as frequency.

Reflection/Amplification Attacks Source Countries

The following diagram (Figure AT21) shows the source countries where the reflection/amplification attacks originated. This provides us with a rough idea, from the geographical perspective, where DDoS amplifiers such as open DNS resolvers are being exploited by the attackers.



TOP FIVE SOURCE COUNTRIES



REMAINING SOURCE COUNTRIES

Russia	61.68%
Brazil	60.90%
Netherlands	60.80%
France	60.66%
Italy	60.03%
Poland	60.03%
Ukraine	58.86%
Romania	58.82%
Spain	58.69%
Turkey	58.23%
Czech Republic	57.80%
Mexico	57.33%
Hong Kong	57.30%
India	57.20%
Sweden	57.18%

Japan	56.60%
Taiwan	55.88%
Vietnam	55.36%
Colombia	54.64%
Australia	53.53%
Indonesia	53.45%
Argentina	53.21%
South Africa	53.11%
Thailand	52.37%
Hungary	52.37%
Bulgaria	52.35%
Chile	51.69%
Singapore	50.43%
Philippines	48.60%
Iran	48.15%

Malaysia	47.30%
Ireland	46.38%
Austria	45.94%
Switzerland	45.88%
Kazakhstan	45.74%
Latvia	45.20%
South Korea	45.14%
Slovakia	45.03%
Denmark	45.03%
Norway	43.93%
Portugal	43.89%
Ecuador	43.87%
Bangladesh	43.73%
Israel	43.44%

Figure AT21 Reflection/Amplification Attacks Source Countries

ASERT Special Report

APPLICATION-LAYER ATTACKS

A SPECIAL REPORT FROM THE NETSCOUT ARBOR SECURITY ENGINEERING & RESPONSE TEAM (ASERT)

As DDoS defenses become more effective, it is more difficult to take down well-protected targets. Attackers have responded by using large IoT botnets to launch more sophisticated application-layer DDoS attacks.

In 2016, a sustained attack against security journalist Brian Krebs resulted in Akamai Technologies discontinuing its gratis protection of his website. The attacks had consumed a large part of Akamai's DDoS defenses, negatively impacting the company's ability to fulfill its contractual obligations to paying customers. Google's Project Shield promptly took over and managed to mitigate the attacks until the attacking botnet was taken down in a concerted worldwide effort by major service providers and security organizations.

Building a large IoT botnet takes time and effort. When botnets are used to launch large, highly visible DDoS attacks, there is a risk for the attacker that the compromised IoT devices will be identified and blocked by service providers. This reduces the effectiveness of the botnet. To avoid this, attackers have now started to focus more on application-layer attacks because they can achieve successes using smaller botnets that produce lower levels of traffic. Application-layer attacks are also effective because they are small in size and will, in most cases, not be picked up proactively by cloud-based managed DDoS protection services. This leaves the task of defending against the attack to the target itself.

The Anatomy of Application-Layer Attacks

Delivery of internet content typically utilizes a number of services, applications and infrastructure components.

1 DOMAIN NAME SERVICES (DNS)

Convert fully qualified domain names (FQDNs) to IP addresses. The response is often based on the user's location and the state of the services which the user is attempting to reach.

2 LOAD BALANCERS

Use a combination of the URL contents and the state of the application servers to redirect the user to an appropriate destination.

3 APPLICATION SERVERS

Examine the URL and retrieve the content which the user is requesting from other services, including database servers. Modern service oriented architectures (SOAs) use a hierarchy of fine-grained, lightweight microservices, each optimized to deliver its part of the response in the most efficient manner possible.

4 DATABASE SERVERS

Used by the application servers for retrieving and storing content which is then presented to the user.

As IoT devices are now the preferred weapon of choice for launching DDoS attacks, it has become easy to use those devices to launch advanced application-layer attacks. IoT devices are online 24x7 and have enough capabilities to launch complex attacks.

ATTACKS AGAINST

DNS Infrastructures

On October 21, 2016, a series of large DDoS attacks using IoT devices was launched against the managed DNS server provider Dyn, resulting in the outage of major brand name services. In fact, these services were perfectly okay and had no issues. However, Dyn's DNS service was not working, resulting in users being unable to resolve domain names to IP addresses.

The attack used against Dyn was a Pseudo Random DNS Query application-layer DDoS attack which attaches a pseudo random label, such as "4asg7vds6tsct.www.netflix.com," to the DNS name of the victim. These queries are unlikely to be in cache for a recursive DNS service, so they will be forwarded to the Authoritative DNS server for the domain. The Authoritative DNS server will respond with a NXDOMAIN message, which in turn will be returned by the Recursive DNS server back to the original client.

If the client now sends another query with a different random label, the same process will be repeated. If the attacker now instructs thousands of clients to send these random queries as fast as they can, the Recursive server and the Authoritative server will very quickly start to run out of resources and be unable to answer queries from legitimate clients. When using shared DNS services, there is a risk that the attack will cause collateral damage, resulting in the outage of all customers using that service. This is what happened in the Dyn attack.

ATTACKS AGAINST

Application Servers

Application-layer attacks have been around for many years but in 2017 there was a significant increase in attacks focused on application servers.

Traditionally attackers used attacks like Slowloris, which opens multiple HTTP connections and then keeps them open. Attackers also used SSL-based attacks, which start the establishment of SSL sessions but never complete them. The goal of both of these attacks is to fill up connection tables and block legitimate users from connecting. In 2017, a new type of application-layer attack focused on attacking modern service oriented architectures (SOA) was discovered by Netflix.

Microservices are becoming popular and are often implemented using Docker and other lightweight application frameworks that are designed to be modular to develop and deploy. An application based on such an architecture will often consist of hundreds of microservices, all of which are heavily interconnected and use API calls to interact with each other. Some of these microservices will require more CPU resources than others. A clever attacker can map out which microservices are more CPU intensive than others and then focus an attack on those. This can result in high CPU load on the application server.

ATTACKS AGAINST

SQL Servers

SQL injection attacks have existed for many years but they have primarily been used for infiltrating websites and for exfiltration of valuable data.

In 2017, there was a major increase in specially crafted SQL injection attacks which use benchmarking tools within the database to cause the database server to consume as much CPU as possible. This attack forces the SQL server to consume a massive amount of CPU resources for each query. This leaves no resources for the application server and results in the website being unable to respond to legitimate queries. One example of such an attack tool is the #RefRef DDoS tool which uses the MySQL Benchmark command to inject CPU-intensive SQL commands.

Mitigating Application-Layer Attacks

All of the attacks mentioned previously do not require high bandwidth and will, in most cases, not be picked up by volumetric DDoS defenses offered by managed DDoS providers. To detect and mitigate these attacks, it is usually necessary to have an application-centric DDoS mitigation device monitoring traffic destined to these servers. This kind of device can identify and then either mitigate the attack itself or automatically invoke cloud-based DDoS mitigation solutions to filter away the attack traffic.

Summary

As volumetric DDoS defenses become more effective, attackers have increasingly turned to application DDoS attacks which focus on specific implementation of protocol weaknesses. Applications like DNS, HTTP and HTTPS, the latter often used for API access as well as user interaction, must be protected using layered DDoS defenses.

ENTERPRISE, GOVERNMENT + EDUCATION (EGE)

Network Security

With three major attacks in 2017, WannaCry, Petya and Bad Rabbit, it is not surprising to see "ransomware" appearing right at the top of the list of threats experienced by enterprise, government and education (EGE) organizations at 35 percent (Figure 63). DDoS dropped to second place, with a slight decrease in the proportion of respondents experiencing attacks. However, with DDoS and ransomware both being experienced by over 30 percent, a significant number of organizations experienced one or both of these threats within the last 12 months.

Looking to the future, ransomware is top of mind as a key threat, with nearly two thirds concerned about this risk (Figure 63). Advanced persistent threats (APT) are also still an important concern for 57 percent, slightly down from 61 percent last year. It is notable that for the last couple of years, APTs ranked as a high concern, yet only a small segment (15 percent in 2017 and 28 percent in 2016) actually experienced these threats. The percentage of EGE respondents concerned about DDoS has increased slightly to 54 percent.

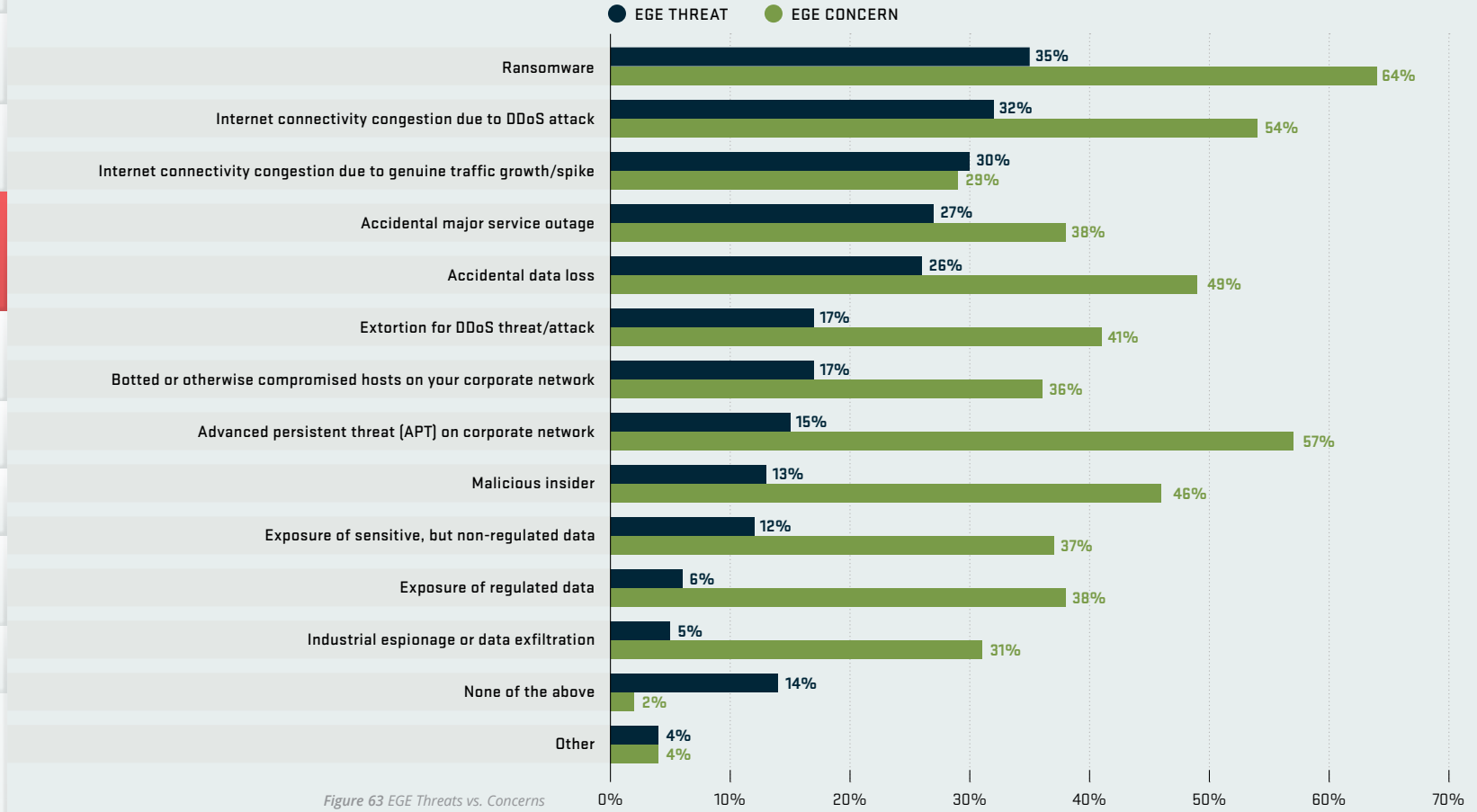


Figure 63 EGE Threats vs. Concerns

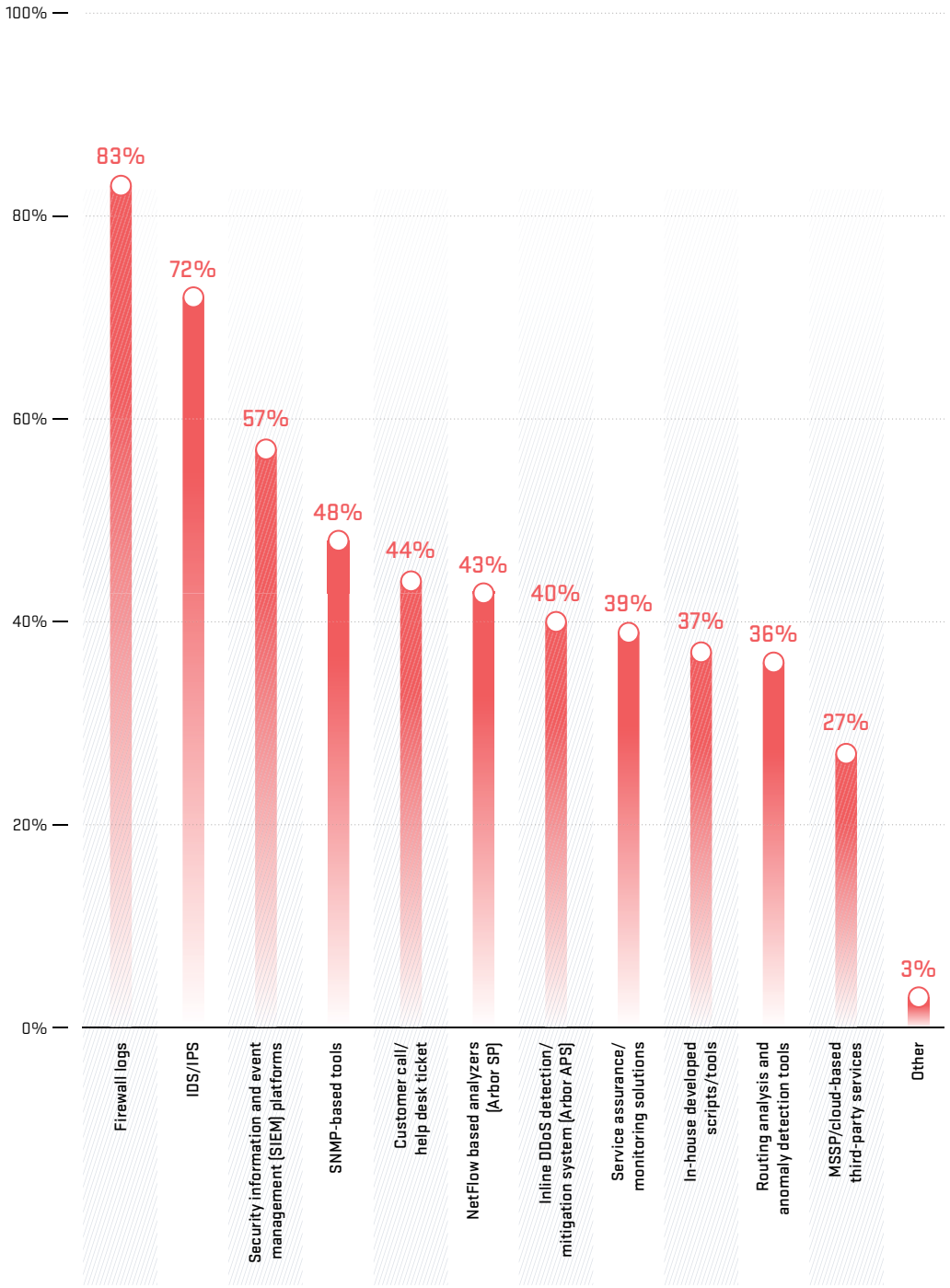


Figure 64 Threat Detection

For the third consecutive year, firewalls, IPS/IDS and SIEM were the top three most utilized tools to detect threats on EGE networks (Figure 64), all of which saw an increase in their use.

The use of inline DDoS detection/mitigation systems dropped by nine percent this year to 40 percent, even though DDoS attacks were still a top threat and hybrid/layered DDoS defense is an established best practice.

This year, respondents chose SNMP-based tools and customer calls/helpdesk tickets more often than NetFlow-based analyzers for threat detection, indicating a concerning reduction in threat visibility.

DDoS Attacks

Forty-one percent of enterprise, government and education (EGE) organizations experienced DDoS attacks in the past year. DDoS continues to be used as a diversion within advanced threat campaigns and other malicious activity. The percentage of respondents that observed more than 100 DDoS attacks during 2017 (Figure 65) more than doubled over the previous year. This sharp increase was expected because of the proliferation of IoT-based DDoS-for-hire services and anecdotal feedback from customers.

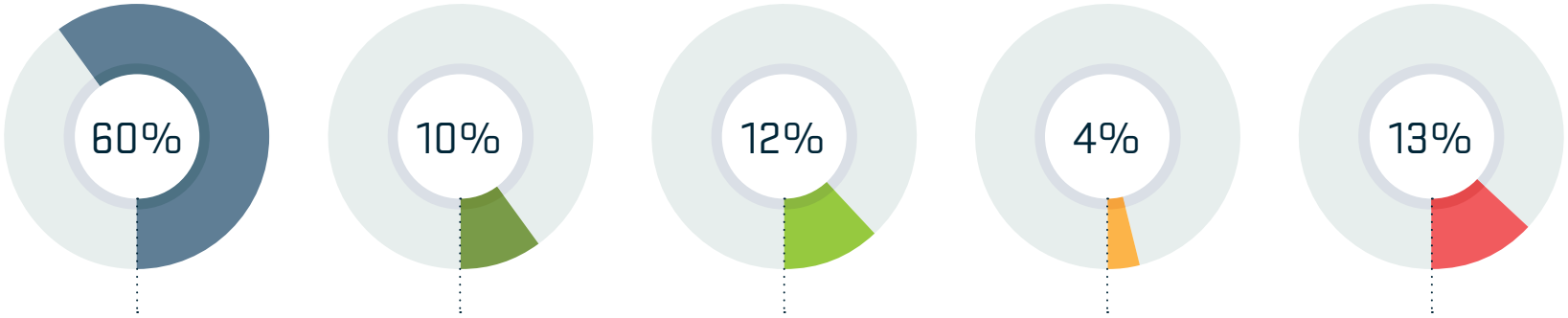


Figure 65 DDoS Attack Frequency

Nearly half of all respondents that were attacked reported seeing 1 to 10 DDoS attacks over the past year: 44 percent in Europe, 50 percent in APAC and 68 percent in North America.

Of those that experienced DDoS attacks, 57 percent saw their internet bandwidth saturated due to an attack, up from 42 percent in the previous year. This is unfortunate but clearly illustrates the need for upstream or cloud-based mitigation services that can handle large volumetric attacks.

Up slightly from last year, 68 percent reported that customer-facing services and applications were the most common targets of DDoS attacks on EGE networks (Figure 66). Networking infrastructure, which was first last year, came in second at 61 percent. DDoS attacks increasingly targeted the application layer, a trend that we have been observing in recent years. This once again highlights the need for a layered-defense strategy.

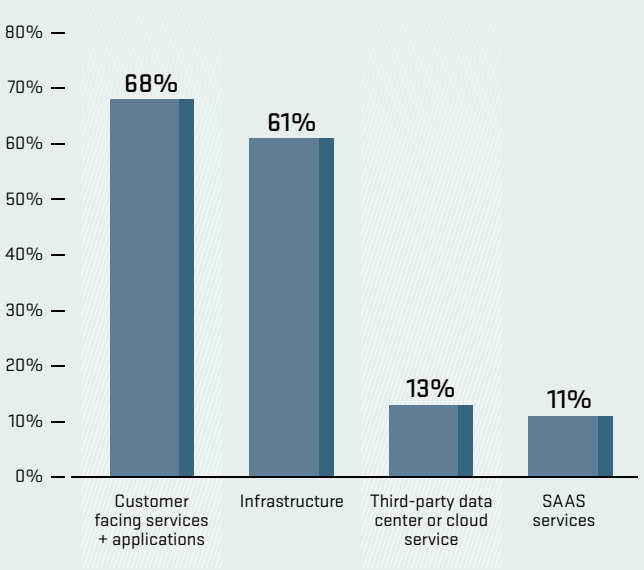


Figure 66 Targets of DDoS Attacks

Over half of EGE respondents had firewalls or IPS devices that experienced a failure or contributed to an outage during a DDoS attack (Figure 67). While stateful security devices can play a useful role, they are especially vulnerable to state-exhaustion attacks. Even the latest firewalls are susceptible to DDoS attacks, so these issues remain consistent year-on-year.

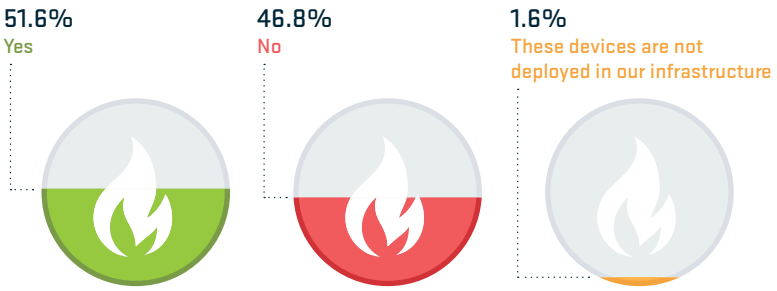


Figure 67 Firewall + IPS Failure

Looking at the longest DDoS attack duration (Figure 68), 84 percent experienced DDoS attacks lasting less than one day, a decrease from 89 percent in the previous year. Further, there was a significant decline in attacks of less than seven hours, falling from 72 percent down to 59. This is surprising given the general trend of shorter duration attacks we've observed in the wild.

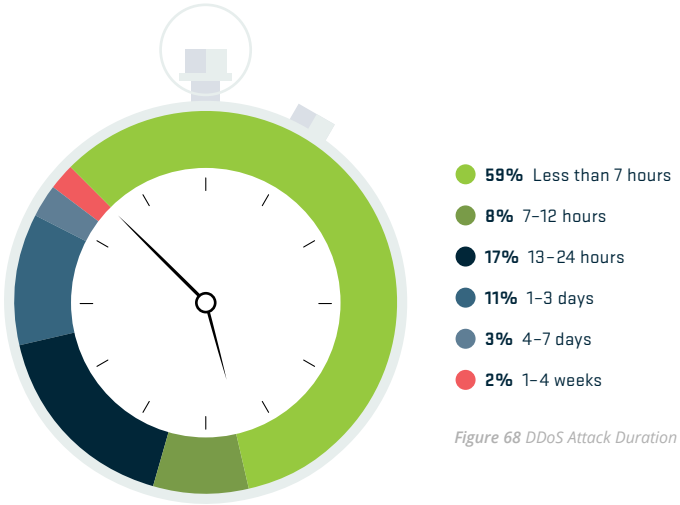


Figure 68 DDoS Attack Duration

DDOS ATTACKS ARE TRADITIONALLY BROKEN DOWN INTO THREE MAIN CATEGORIES:

1. Volumetric
2. State-Exhaustion
3. Application-Layer

For the second consecutive year, there was a decrease in volumetric attacks, from 60 percent last year to 52 percent in 2017 (Figure 69). This was mirrored by an increase in application-layer attacks from 25 percent to 32 percent. This is not surprising as large volumetric attacks are typically mitigated upstream and EGE network operators have better visibility of their own applications than service providers.

These percentages are starkly different than those reported by our service provider respondents, who saw a far lower number of application-layer attacks (12 percent) and more volumetric attacks (76 percent). This further illustrates why a layered-defense strategy is key in the fight against DDoS attacks; a more focused view of traffic at the enterprise or data center level is needed to identify and block stealthy attacks.

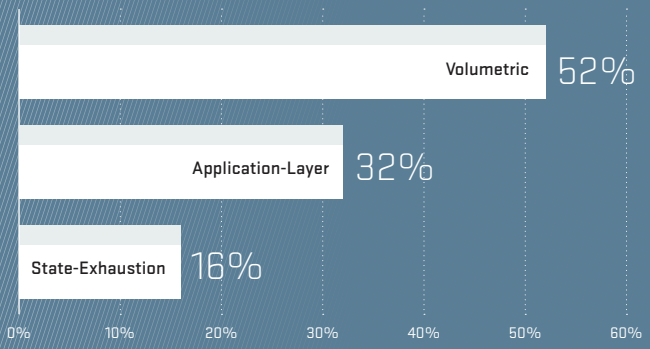


Figure 69 DDoS Attack Types

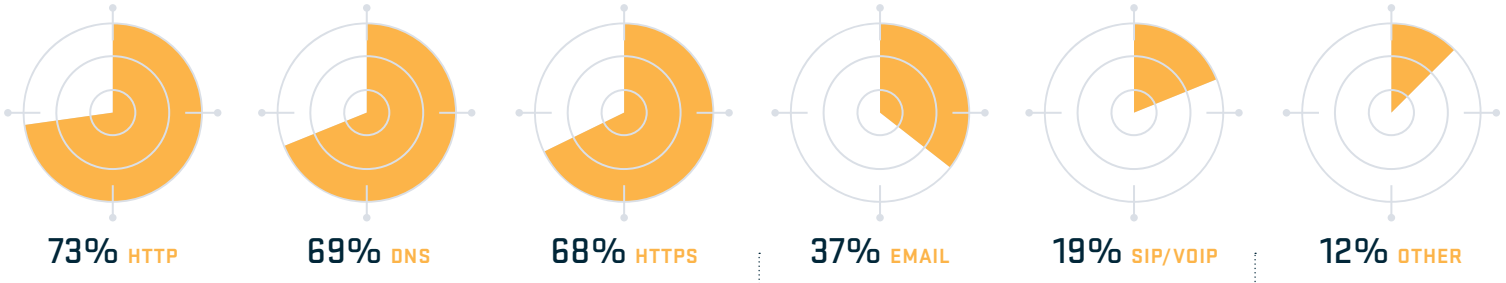


Figure 70 Targets of Application-Layer Attacks

EGE organizations also saw more DDoS attacks targeting their email and VoIP services, suggesting the focus of DDoS attackers has shifted to exploiting more vulnerable services.

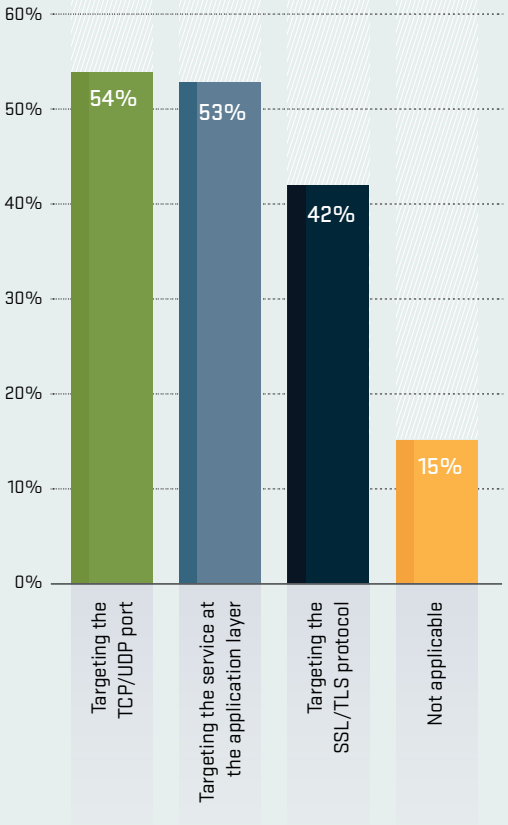


Figure 71 Encrypted Application-Layer Attacks

HTTP remained the most targeted application-layer service for DDoS attacks, but there was a decrease in the percentage of respondents seeing these attacks, from 85 to 73 (Figure 70). In contrast, DNS jumped from the third spot last year to second place, with 69 percent seeing this service targeted, up from 59 percent. HTTPS was also targeted more, at 68 percent up from 63 in the previous year.

The above application services were also the top three targeted as reported by service providers. However, DNS was the top target at 82 percent, followed by HTTP at 80 percent and HTTPS at 61 percent.

DDoS attacks targeting encrypted web services have become increasingly common in recent years (Figure 71). While there was a small decrease in the number of detected attacks targeting the encrypted service at the application layer (from 57 percent last year to 53 currently), the overall results remained mostly unchanged. A higher proportion of EGE respondents witnessed attacks targeting the SSL/TLS protocol than service providers (42 percent compared to 29 percent). The variation in results between EGE 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. The ability to look inside encrypted traffic may also be a factor.

EGE respondents reported a clear increase in multi-vector DDoS attacks, up from 40 percent in the previous year to 48 percent (Figure 72). These incidents utilize multiple, simultaneous vectors to maximize the attackers' ability to disrupt service availability. This was expected given the increased sophistication of weaponized DDoS services seen in our research. The positive news is that EGE respondents now have better visibility to mitigate such threats.

OBSERVED MULTI-VECTOR DDoS ATTACKS?

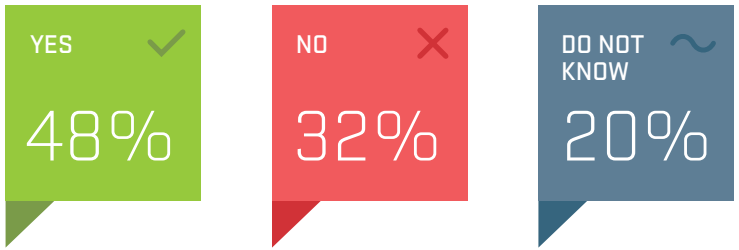


Figure 72 Multi-Vector Attacks

Figure 73 DDoS Attack Motivations

The motives behind the DDoS attacks were extremely varied again in 2017 (Figure 73). There was a substantial increase in criminals showcasing their capabilities to potential victims, with 49 percent seeing this as a common motivation compared to 27 percent the previous year. This, combined with a slight increase in respondents seeing criminal extortion as a motivation, can possibly be attributed to high-profile ransomware campaigns such as WannaCry, Petya, and Bad Rabbit.

One other interesting statistic is the increase in nihilism/vandalism as a common motivation, which was up from 26 to 37 percent. Based on anecdotal evidence, this is likely the result of collateral damage due to the rise of DDoS for hire services and attacks casting a wider, more random net of targets.

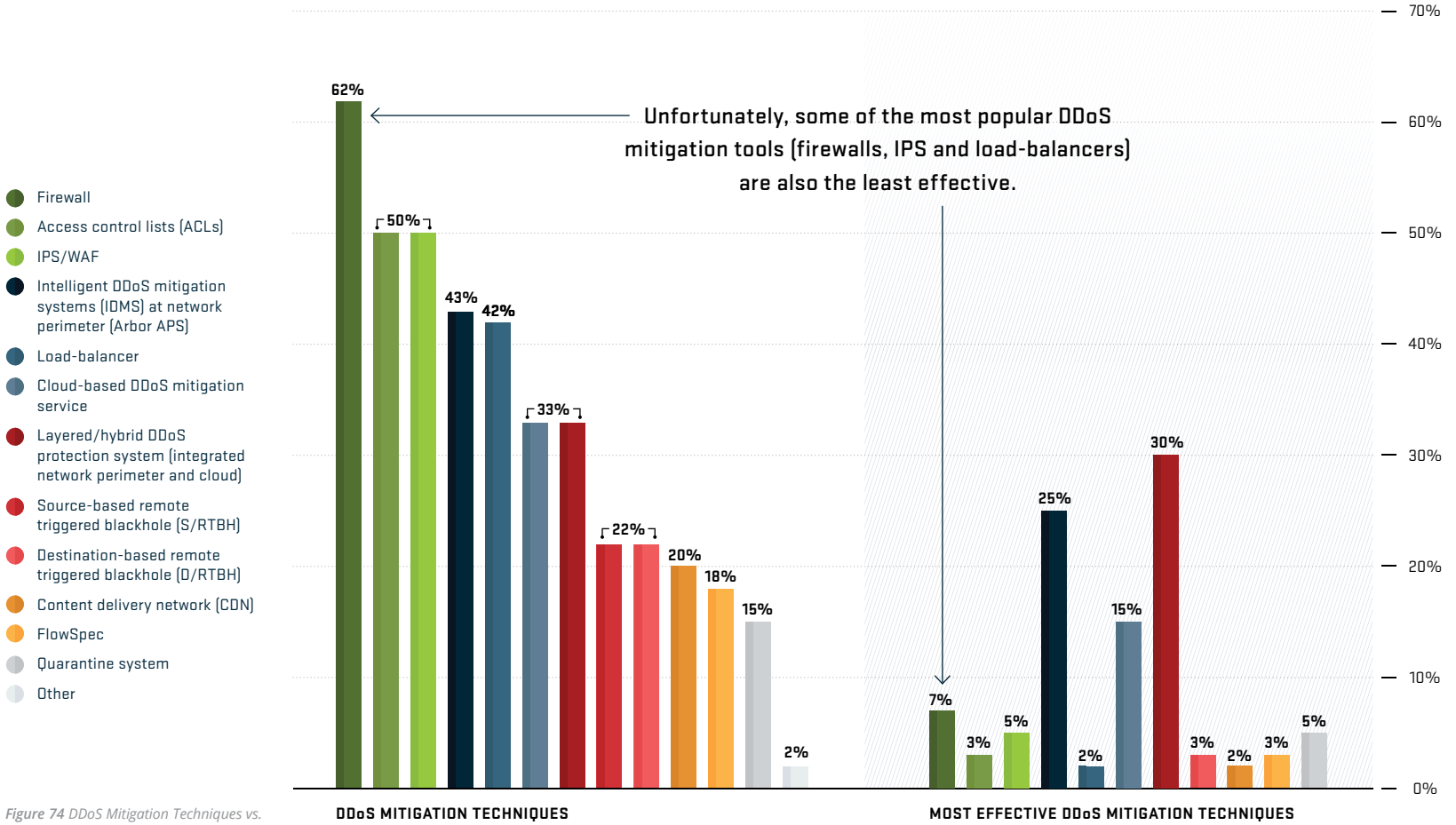


Figure 74 DDoS Mitigation Techniques vs. Most Effective DDoS Mitigation Techniques

As in previous years, firewalls, IPS, WAF and access control lists (ACLS) remained the most common DDoS mitigation mechanisms for more than half of the respondents (Figure 74). The use of firewalls, IPS and WAF remains a concern as those devices are susceptible to state-exhaustion attacks, which were experienced by over a half of respondents.

Of equal concern was the sharp increase in the use of firewalls for mitigating DDoS attacks, at 62 percent up from 49 percent previously. There were only slight changes in the deployment of Intelligent DDoS Mitigation Systems (IDMS) at 43 percent, and the utilization of both hybrid and pure cloud-based DDoS mitigation services, each at 33 percent.

As in previous years, we also asked our EGE respondents to rank the effectiveness of the mitigation techniques they are currently using. Intelligent, cloud-based and layered/hybrid DDoS mitigation systems were reported as the most effective techniques by nearly three quarters of respondents (Figure 74). Layered/hybrid systems took the first spot at 30 percent, followed closely by IDMS at 25 percent. Not surprisingly, while the majority used firewalls, IPS and WAF for DDoS mitigation, very few found them to be the most effective solution.

The faster DDoS attacks are successfully mitigated, the more the operational, financial and customer impact is limited. Seventy-five percent of organizations indicated that they could mitigate a DDoS attack in less than one hour (Figure 75), a very similar and encouraging result to last year.

Approximately a quarter of the respondents reported immediate mitigation capabilities via on-premise devices or "always-on" cloud services last year. In 2017, the number increased to nearly a third, which is also a good sign.

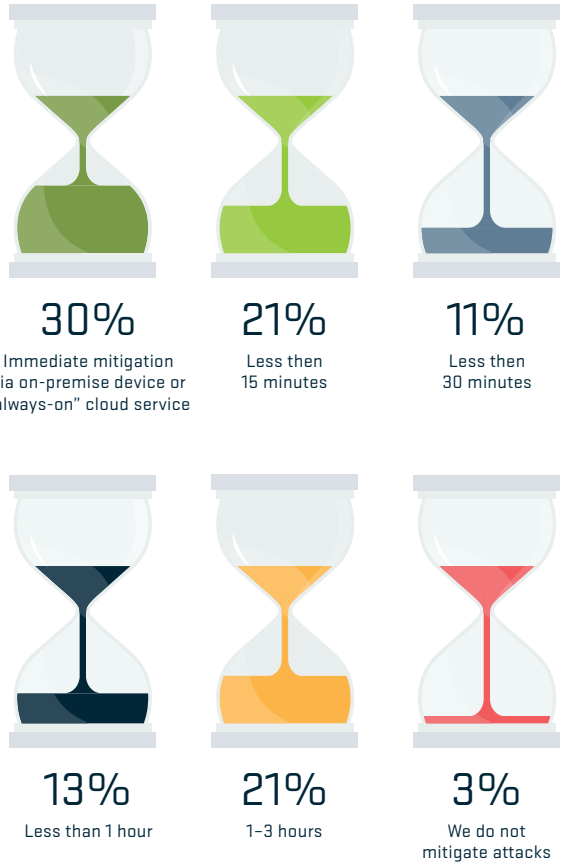


Figure 75 DDoS Attack Mitigation Time

Business impacts due to DDoS attacks continued to vary greatly (Figure 76). Reputation/ brand damage and operational expense were still the two main business impacts, the former cited by 57 percent, an increase from 48 percent last year. There was also a big jump in respondents reporting revenue loss as a business impact, up to 32 percent from just 17 percent previously.

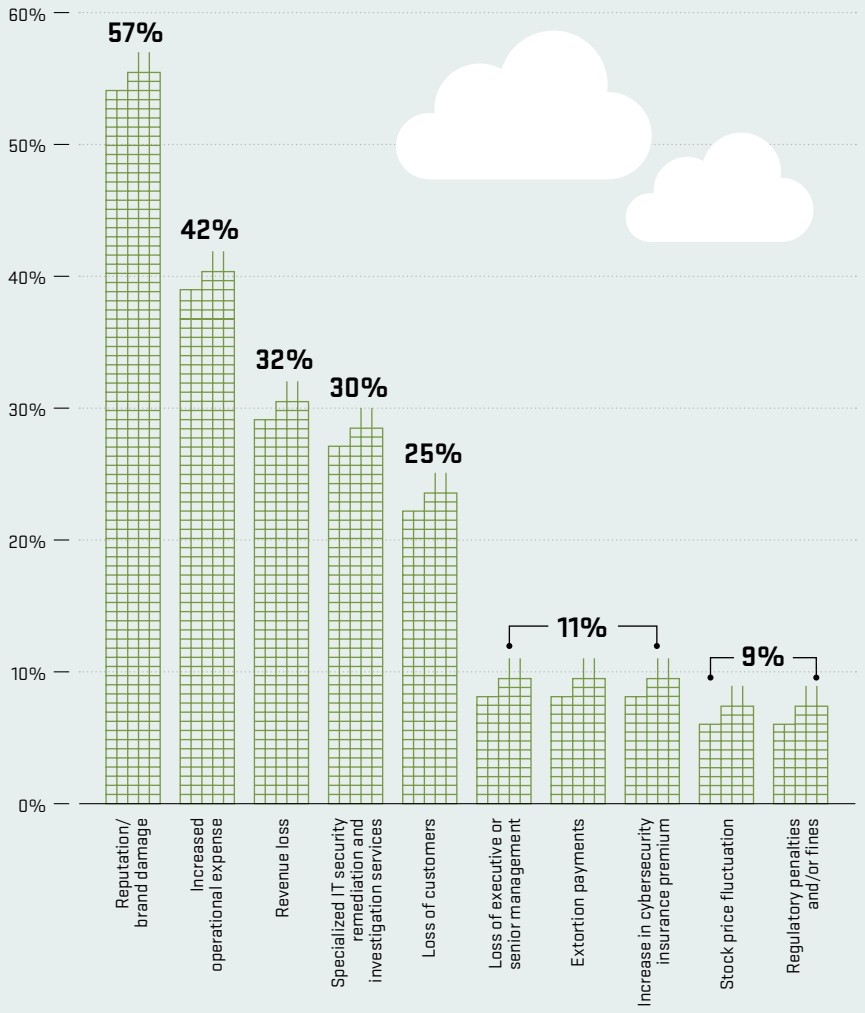


Figure 76 Business Impacts of DDoS Attacks

We asked respondents to estimate the average total cost of a major DDoS attack on their business (Figure 77). Like last year, the vast majority reported a total cost below $10,000. However, over ten percent estimated a cost greater than $100,000, five times greater than previously seen. This indicates either that the cost of a DDoS attack has increased significantly, or that more organizations are now aware of the true impact to their business.

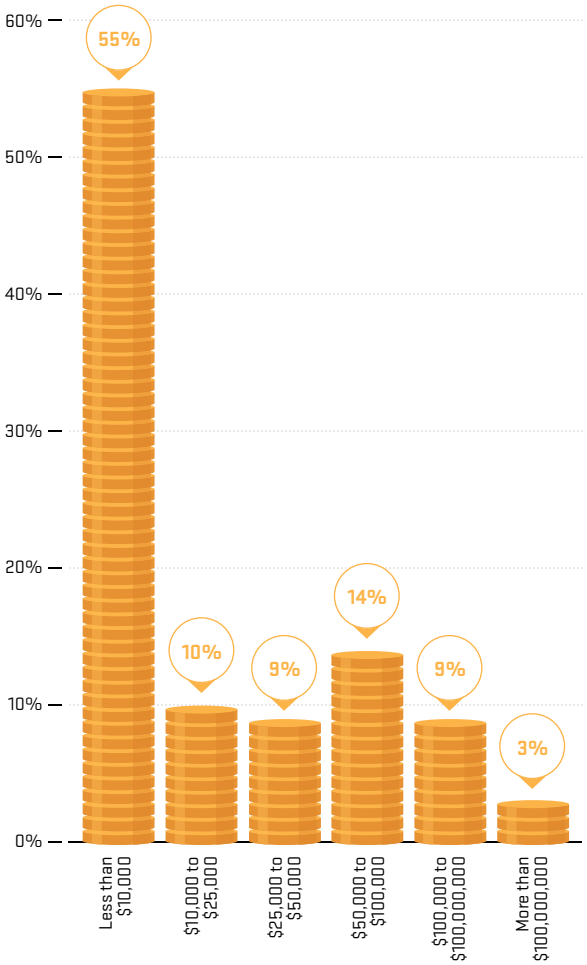


Figure 77 Cost of DDoS Attacks

To provide greater insight into the above, we asked whether DDoS was part of their recurring risk analysis (Figure 78). Seventy-seven percent reported that it was either a part of their business or IT risk assessments, up from 70 percent last year. This is an encouraging trend that we expect to become more prevalent.

As in previous years, we also asked a more general question about the cost of internet downtime. The majority of our respondents could not quantify this, even though more than half of them had experienced a DDoS attack that exceeded the total bandwidth available to their organization, which would have resulted in downtime.

For those that could quantify their downtime, 38 percent reported the cost at $501 to $1,000 per minute, up significantly from 23 percent in the previous year (Figure 79). This again highlights the need for proactive defenses, as organizations become more dependent on the internet for their daily business needs.

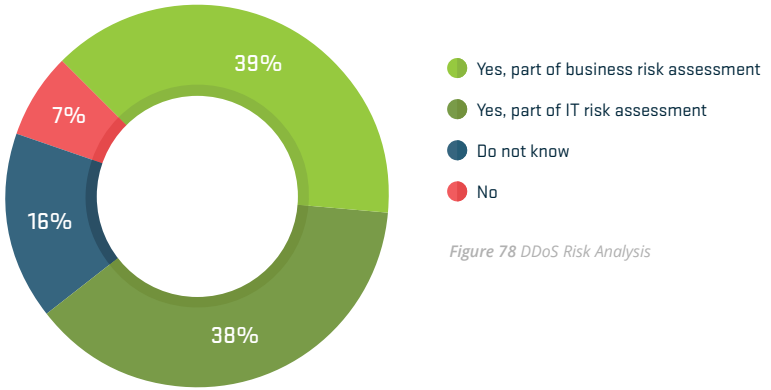


Figure 78 DDoS Risk Analysis

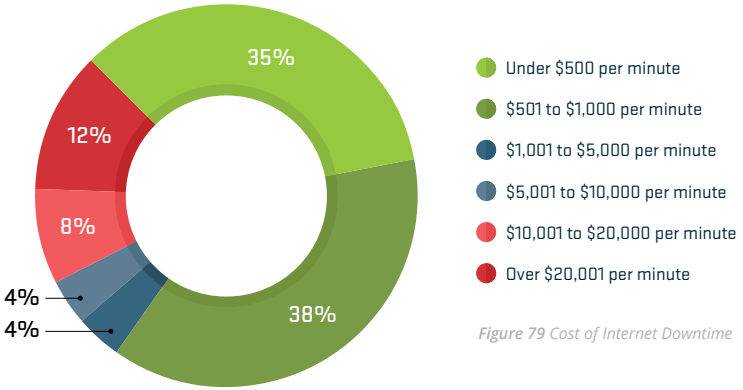


Figure 79 Cost of Internet Downtime

SDN/NFV

Again in 2017, enterprise, government and education (EGE) respondents had fewer plans to utilize SDN/NFV than their service provider counterparts. Nineteen percent had plans to deploy SDN/NFV technologies, while just under a quarter were investigating or testing solutions, a slight increase from last year (Figure 80).

As with service providers, the number one barrier to SDN/NFV deployment within EGE network infrastructures was operational concerns at 56 percent, followed by interoperability and cost (Figure 81). This highlights a shift in the perception, as last year, cost was the main barrier. However, as the industry and market evolves, cost has become less of a concern and operational concerns are coming to the forefront.

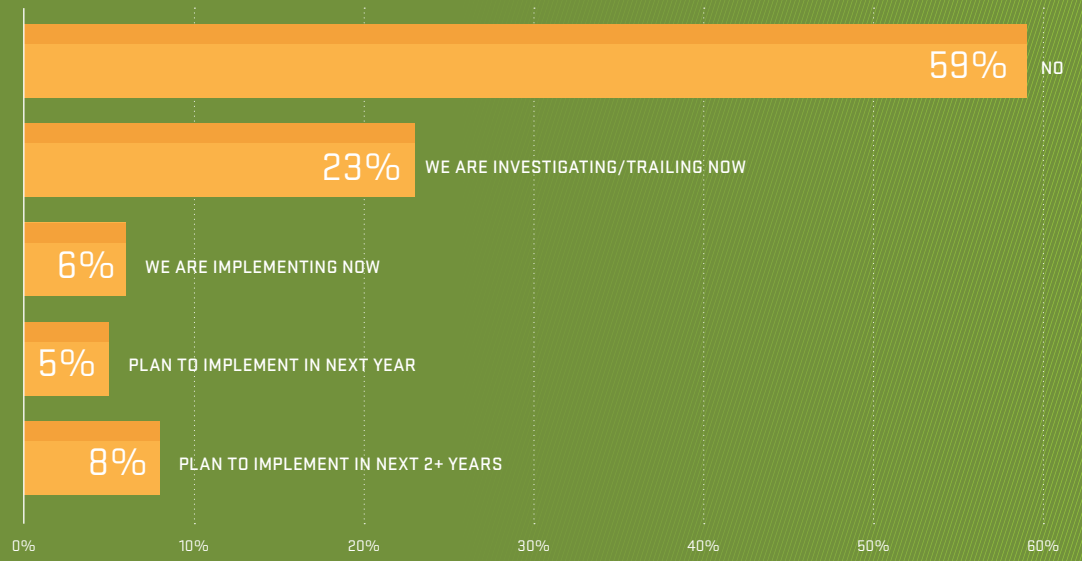


Figure 80 EGE SDN/NFV Deployment

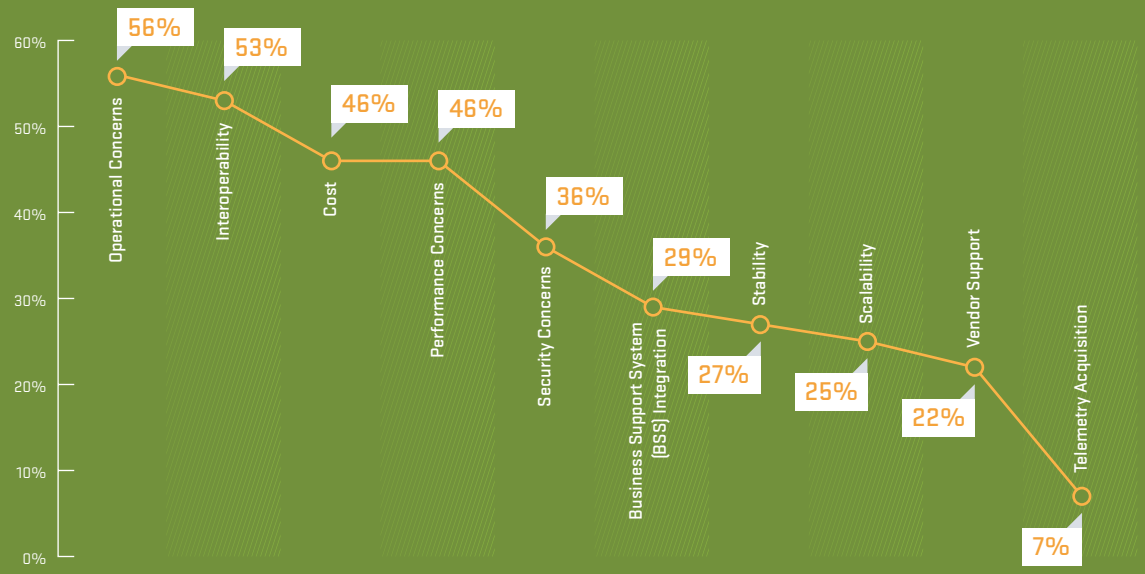


Figure 81 EGE SDN/NFV Key Barriers

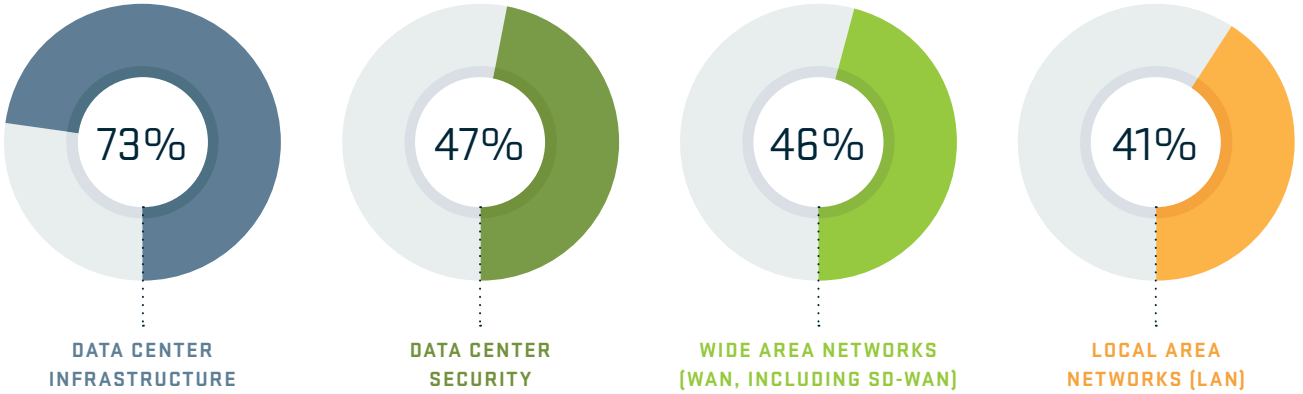


Figure 82 EGE SDN Network Domains

The data center is the domain where most EGE respondents would like to utilize SDN (Figure 82). Here, infrastructure and security were the most common areas with 73 percent and 47 percent respectively. This aligns with service providers, where data center infrastructure was also an area of focus. Both EGE and service provider customers are looking at applying SDN to build global overlay networks, including SD-WAN. As the domain for SDN, WAN was in third place for EGE, with 46 percent looking at this technology area.

NFV use within the EGE infrastructure seems to be moving forward. Firewalls were the most common NFV application, with 25 percent using this virtual functionality (Figure 83). Nineteen percent indicated they were using NFV for router and CPE functions, which correlates with service providers' intent.

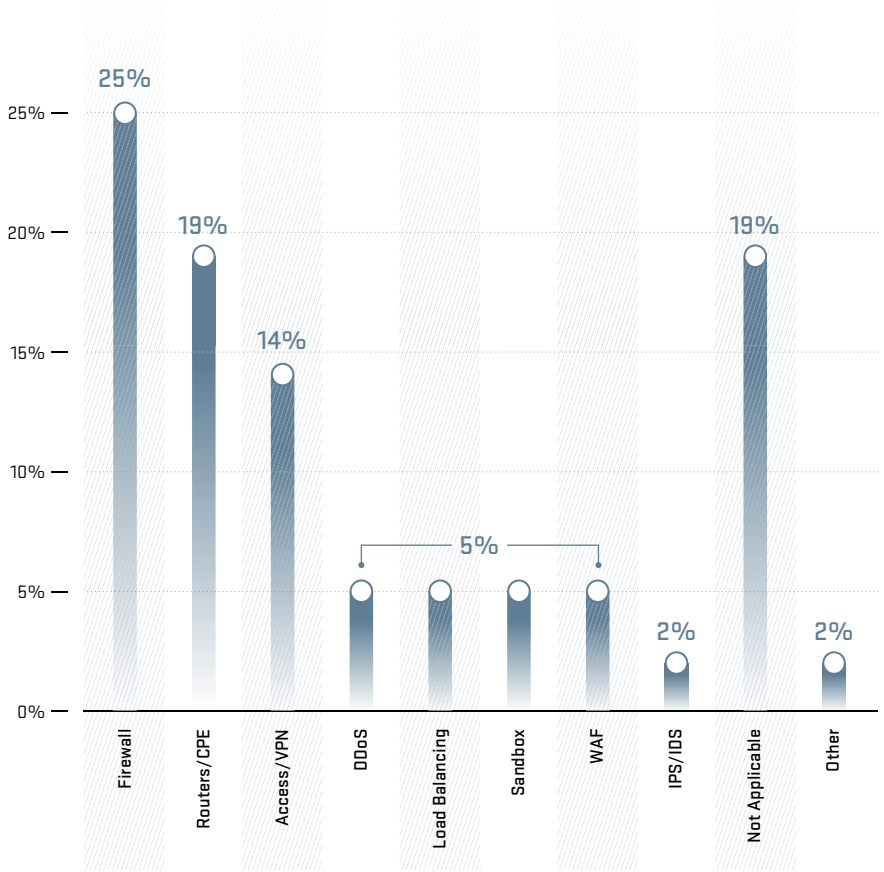


Figure 83 EGE NFV Network Domains

IPv6

In 2017, just over a third of enterprise, government and education (EGE) organizations were operating IPv6 in their environments or planning to in the coming year (Figure 84). This is down a few points from 2016, but a higher percentage than 2015.

OPERATING IPv6 OR PLANNING TO DEPLOY?

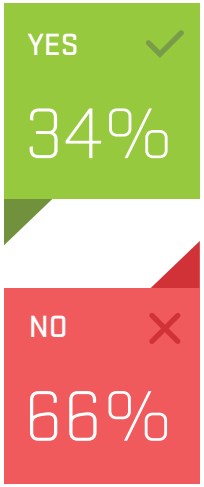


Figure 84 IPv6 Operation

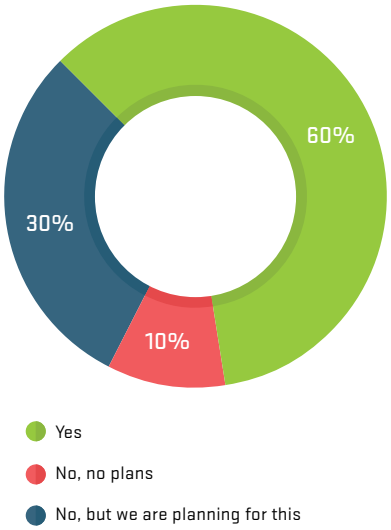


Figure 85 IPv6 Service Availability

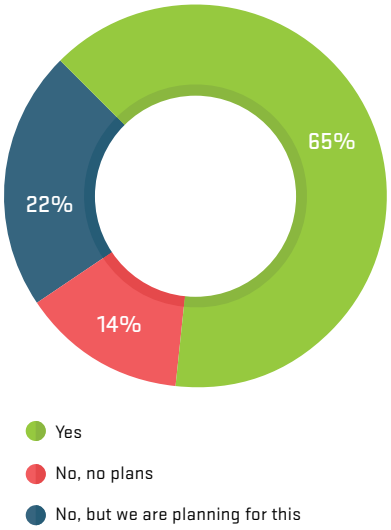


Figure 86 Internal IPv6 Deployment

Sixty percent of the EGE respondents provide internet-facing services with IPv6 support (Figure 85) and 65 percent have deployed IPv6 on their private networks (Figure 86), both down slightly from 2016. The percentage of organizations with no plans to implement IPv6 also appears to have leveled off.

On a positive note, even though the rollout of IPv6 services appears to have stalled within EGE respondents, the already high proportion with IPv6 deployed indicates that any new apps requiring IPv6 will be supported. The tools and telemetry to monitor and protect the apps are mostly in place.

In 2016, 27 percent of EGE networks fully supported IPv6 telemetry and we are happy to report that 45 percent of respondents indicated this was the case in 2017 (Figure 87). This increase is encouraging and shows the need for IPv6 monitoring as it becomes more important to business functions.

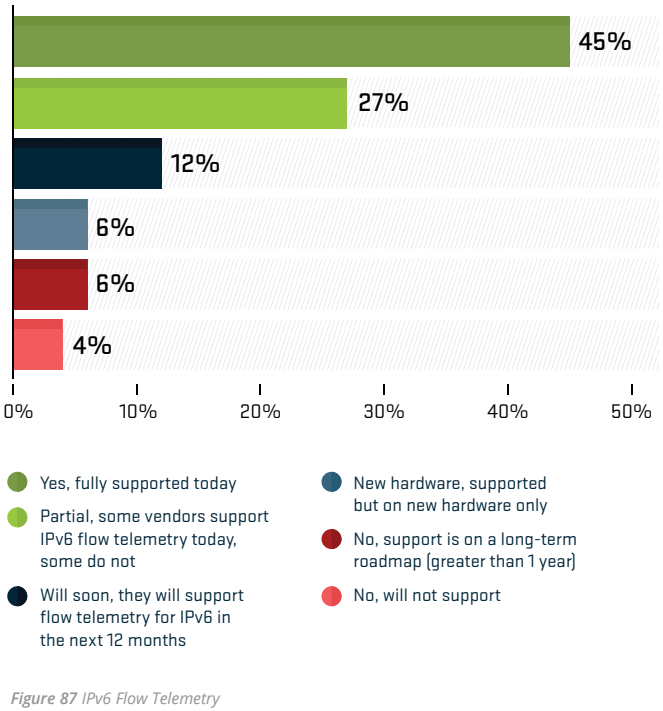


Figure 87 IPv6 Flow Telemetry

More than 60 percent of EGE respondents deployed visibility solutions for IPv6 traffic, up from 57 percent last year (Figure 88). This increase is smaller than anticipated given the growth in the number of respondents who can now gather telemetry from their networks as mentioned previously.

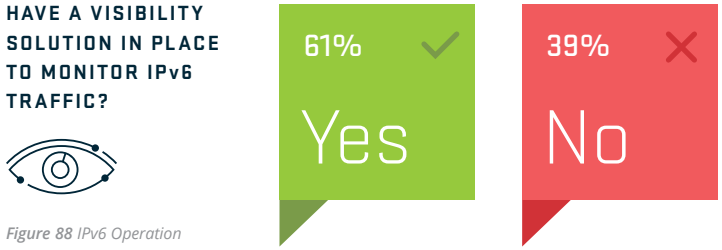


Figure 88 IPv6 Operation

EGE organizations had very similar opinions as those of service providers when it came to the shared risk of IPv4 and IPv6 dual stack services (Figure 89). EGE respondents were more likely to be concerned at some level than their service provider counterparts, but the results were broadly similar.

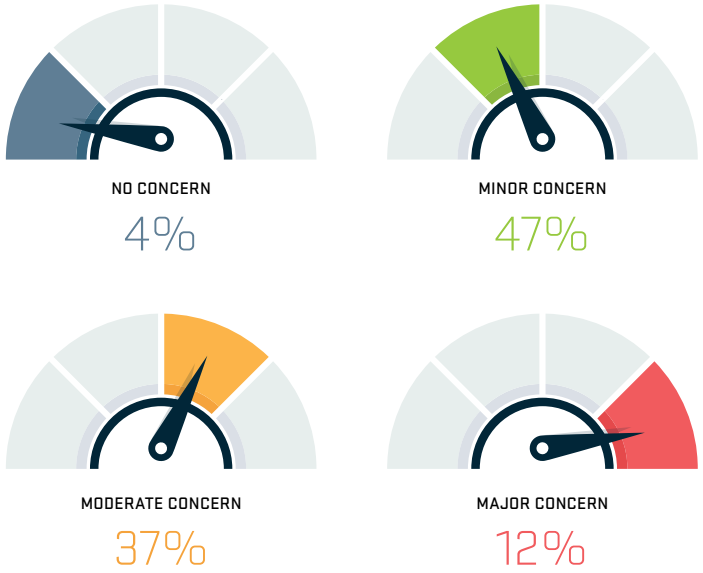


Figure 89 IPv6 Impact on IPv4 Services (Dual-Stack Devices)

In 2017, the biggest security concern for EGE respondents remained DDoS, with an almost identical result to the previous year (Figure 90). Botnets, which were in second position in 2016, were pushed down to fourth place despite a similar proportion reporting that this still was a concern. Misconfiguration and inadequate feature parity each increased by more than 10 percent.

Among all of the EGE respondents, only eight percent observed IPv6 DDoS attacks compared to 25 percent in 2016. We have been waiting for a steady growth trend to emerge in this area for a number of years, but the widespread use of IPv6 for mission critical applications is still not an actuality, as most attacks are still directed toward IPv4 services.

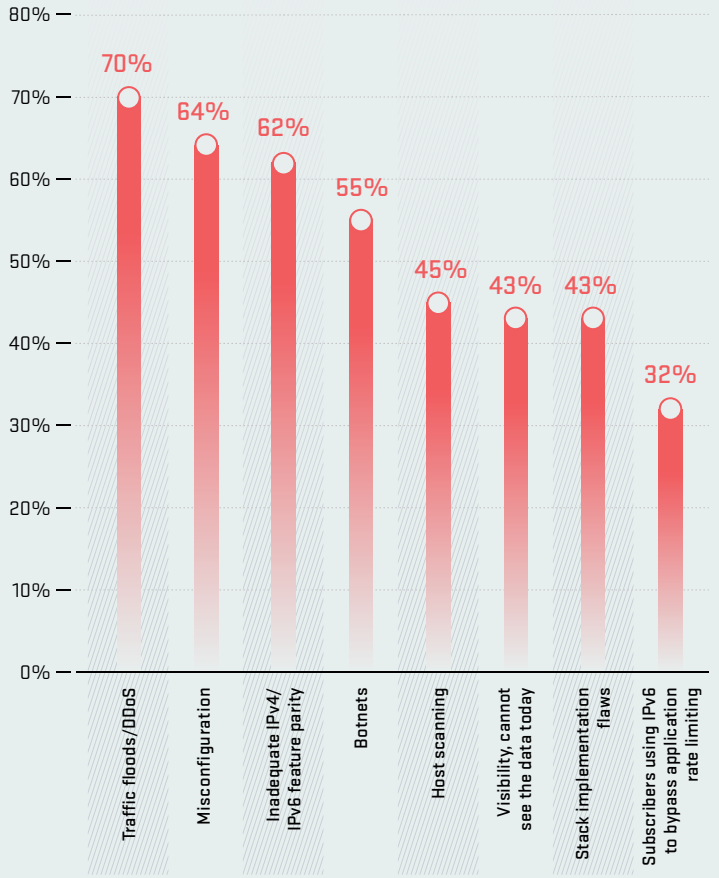


Figure 90 IPv6 Security Concerns

Organizational Security

Forty-eight percent of EGE respondents had an internal security operations center (SOC) team in place in 2017, a slight increase from 46 percent the previous year (Figure 91). In contrast, around 60 percent of the service providers indicated they had internal SOC teams, highlighting the ongoing struggle EGE organizations face in building and maintaining an internal security team of skilled practitioners.

Because of this, 37 percent relied on third-party and outsourced services, a jump from 28 percent the previous year. Fully outsourced SOC teams accounted for 16 percent, a significant increase from nine percent the previous year. This reliance on outsourcing in EGE organizations exceeded service providers by a factor of two, a trend that we expect to continue in the future. The use of external resources reduced the percentage with no SOC capabilities from 26 percent in 2016 to 15 percent, a very positive result.

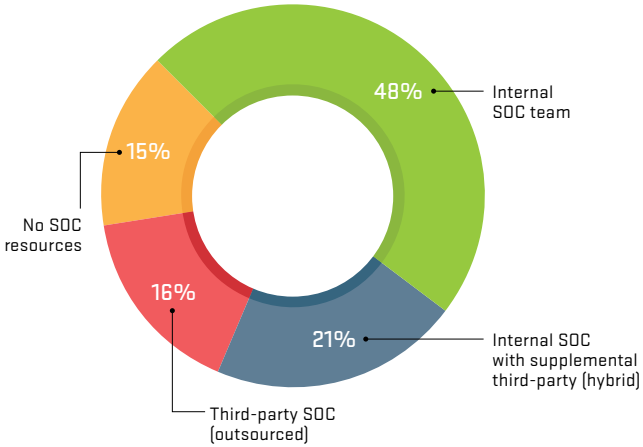


Figure 91 EGE Security Operations Center Resources

Ninety percent of EGE organizations had some dedicated security personnel in 2017 (Figure 92), a slight decrease from 93 percent in 2016, but still a higher percentage than service providers. Only 14 percent of EGE respondents, compared with about a quarter of the service providers, had 30 or more dedicated security staff internally. The smaller security teams may be as a result of the reliance on outsourcing for SOC capabilities.

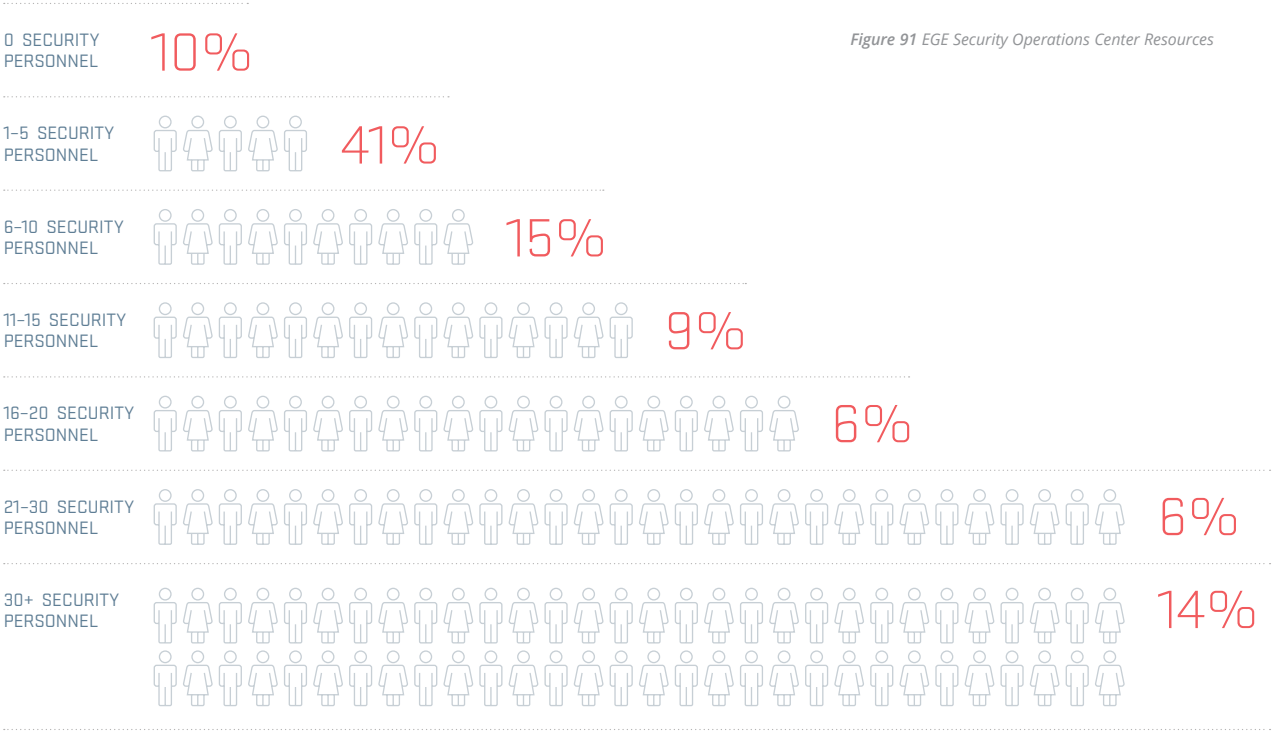


Figure 92 EGE Dedicated Security Personnel

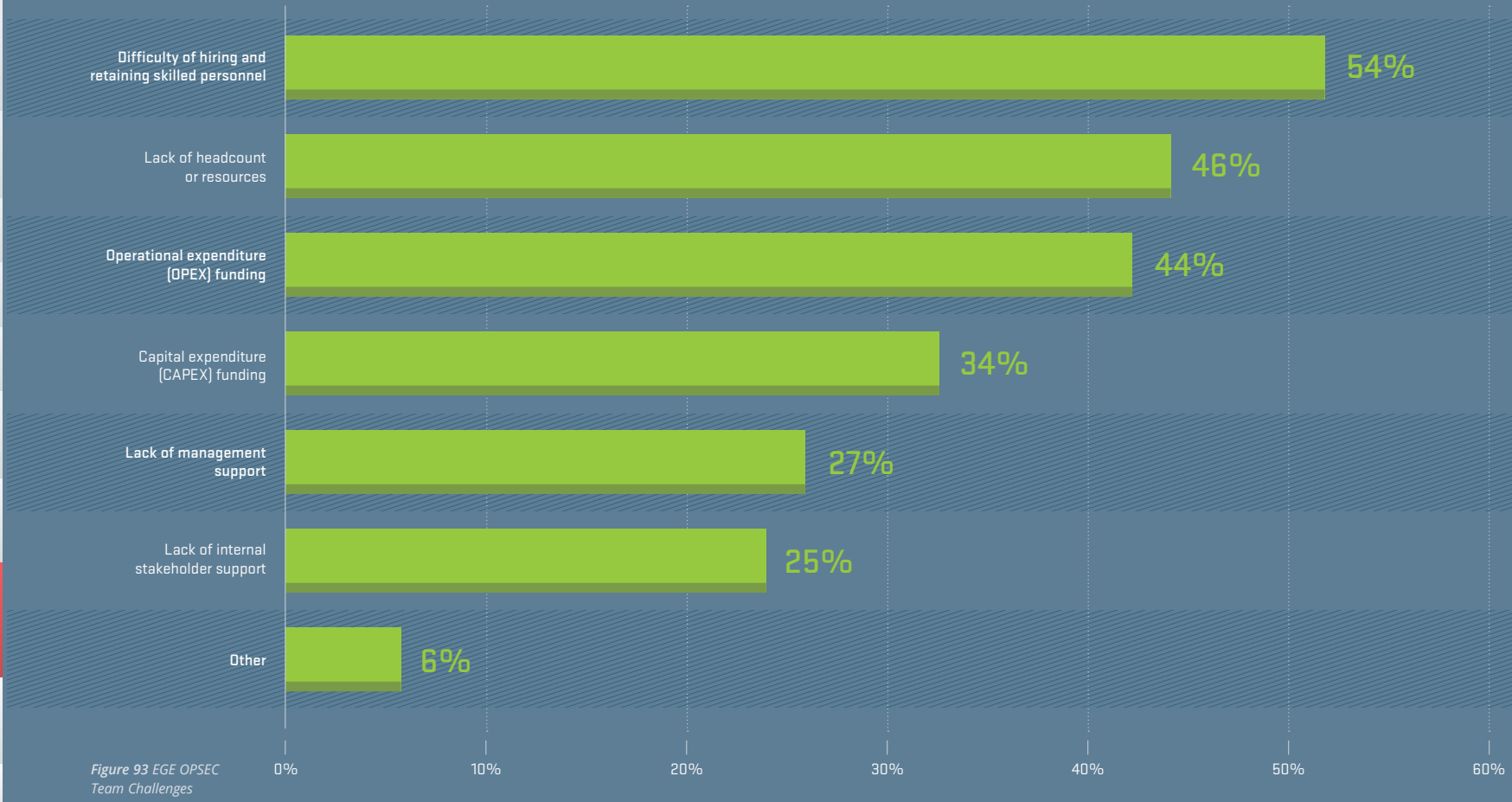


Figure 93 EGE OPSEC Team Challenges

Looking at the challenges faced in building out operational security (OPSEC) teams, the EGE responses aligned with those of the service providers. Lack of resources and difficulty of hiring and retaining skilled personnel were again the two main concerns (Figure 93).

All the other challenges observed showed increases in 2017, a fact that was most likely compounded by the increasing worldwide shortage of security analysts and incident response personnel.

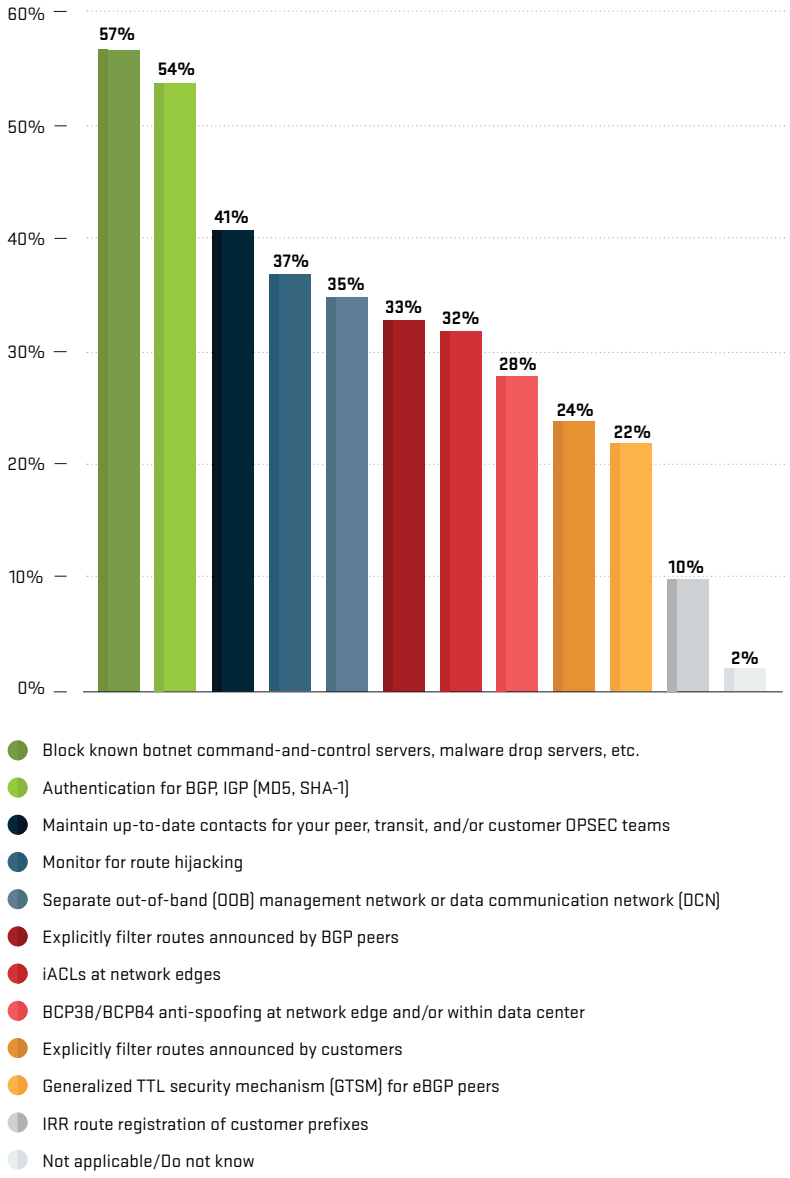


Figure 94 Security Best Practices

The implementation of best-practice security measures was not only lower across the board in 2017 when compared to service providers, but also vastly reduced in comparison to 2016 (Figure 94). Since EGE networks are often smaller and less complex than those of service providers, the security best practices they follow differ, with more than half predictably blocking known botnets Command-and-Control and malware drop servers. Surprisingly, the monitoring of route hijacking claimed the fourth position on the list, an increase to 37 percent from 28 percent the previous year. And, equally surprising, the use of ACLs at network edges was down from 37 to 32 percent.

All EGE respondents indicated that security training and incident response exercises greatly improved the effectiveness of dealing and mitigating DDoS attacks (Figure 95). There was a disappointing decrease from 55 to 50 percent running DDoS defense simulations in 2017. Similarly, the number of respondents carrying out DDoS simulations at least every quarter fell from 40 to 32 percent, which was similar to what we observed with service providers. Though EGE organizations tend to believe they are targeted less frequently, not being prepared to respond to a DDoS attack could result in substantial financial and reputational loss in the event of a successful incident. As in 2016, there is obviously plenty of room for improvement.

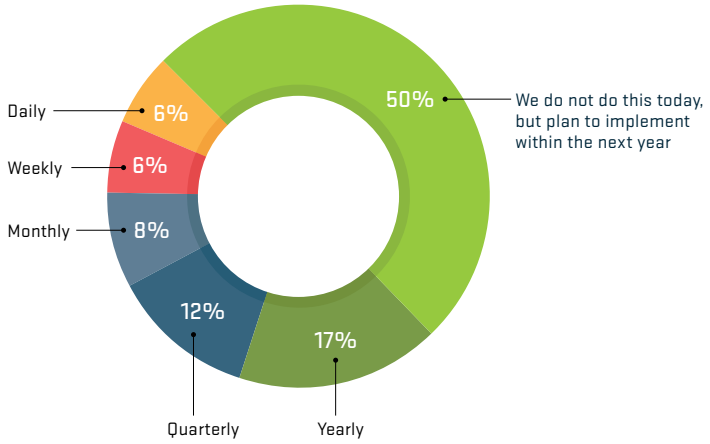


Figure 95 DDoS Simulations

ASERT Special Report

THE RISE OF THE IoT BOTS

A SPECIAL REPORT FROM THE NETSCOUT ARBOR SECURITY ENGINEERING & RESPONSE TEAM (ASERT)

The year 2017 was one in which IoT botnets became the preferred weapon of choice for launching DDoS attacks.

The number of unsecured internet of Things (IoT) devices connected to the internet continues to increase dramatically. As the number of IoT devices increases, so do the security vulnerabilities. Attackers have invented new ways to detect, infect and compromise IoT devices, even those thought to be secure behind corporate firewalls.

IHS MARKIT PREDICTS THE NUMBER OF IoT DEVICES WILL RISE

27 billion CONNECTED DEVICES IN 2017

125 billion CONNECTED DEVICES IN 2030

IHS press release 10/24/17

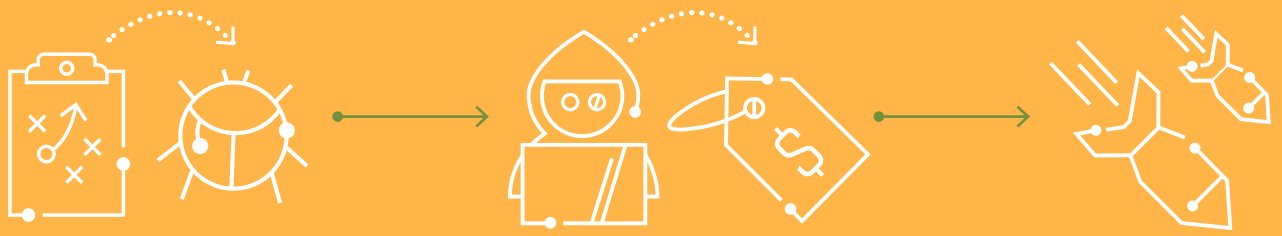
The Attackers Economy + Attack Cycles

The motivations for launching DDoS attacks are many and varied. As DDoS defenses become more effective, it is more difficult for the attackers to take down their targets using standard DDoS attack methods. Modern desktop computers are more secure, both from a technology point of view but also because of automated patching mechanisms. Consequently, attackers are seeing traditional DDoS attack vectors become less effective, and they are finding fewer vulnerable computers to subsume into botnets.

This is forcing attackers to look at new ways of launching DDoS attacks. Taking advantage of the masses of unsecured IoT devices connected to the open internet has proved popular, but using cross-platform infection vectors to gain access to IoT devices behind corporate firewalls is also becoming a reality.

The skills and technical understanding required to do this are in most cases far beyond that of a normal hacker, resulting in the need for the professional malware arms dealer.

The malware arms dealer researches new attack vectors that take advantage of either existing security vulnerabilities or new zero-day vulnerabilities. The arms dealer develops attack tools kits, and as part of a quality assurance cycle (Q&A), often does live field testing. The goal of these dealers is to sell developed attack tools to the Booter/Stresser community, or in some cases, directly to the attackers themselves.



1. **Malware arms dealers are either individuals or organizations which research and develop attack tools that take advantage of security vulnerabilities. As part of their Q&A, often do live field testing.**
2. **The DDoS mercenaries offer DDoS services (Booters/Stressers) for hire to the attackers.**
3. **The attackers mostly use Booter/Stresser services to launch their attacks, though there are some exceptions.**

In 2017, there were two highly visible cases of field testing taking place.

1 THE WINDOWS MIRAI TROJAN

Only active for five days but received multiple new updates in that time period.

2 THE IoT REAPER

Had the potential to infect millions of IoT devices but was deliberately blocked from doing so by its authors. In addition, it was released without any DDoS capabilities but had all necessary hooks in place.

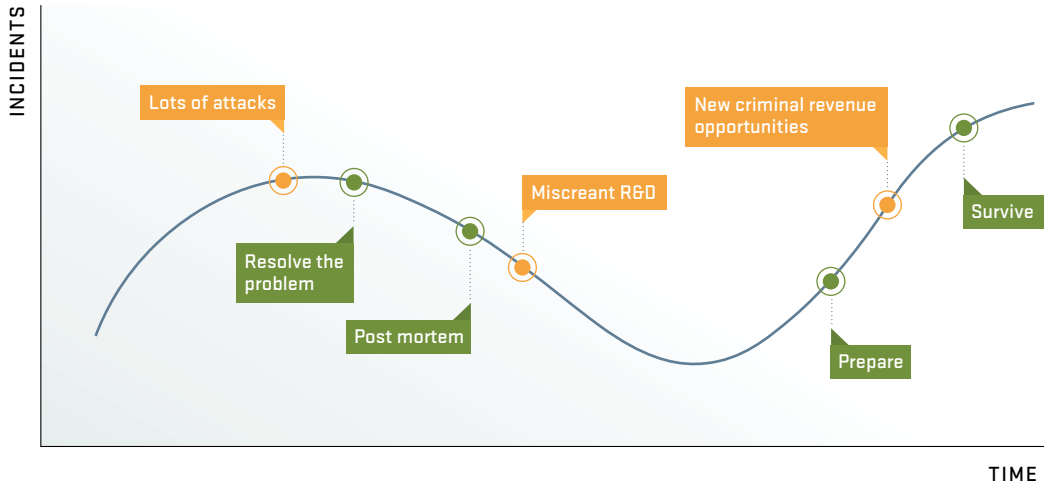
Looking at the number of DDoS incidents, and the appearance of new IoT malware in the 2016–2017 time frame, it becomes apparent that the attacker/incident economy is cyclical in nature.

In 2016, there was a visible spike of attacks concluding with the unprecedented attacks against the websites of Brian Krebs, a journalist and security researcher, and Dyn, a DNS company. These attacks led to a reduction in IoT attack capability due to the alleged BrickerBot and because of service providers blocking IoT devices from infection and remote control. DDoS defenses also became more efficient in blocking some of the new IoT attacks, reducing their potential impact.

After the 2016 incidents, attackers responded by developing new attack tools. First, they created the Windows Mirai Trojan, which allowed them to infect and subsume vulnerable IoT devices behind corporate firewalls into botnets.

Then, attackers started to take advantage of security vulnerabilities in IoT operating systems, with known vulnerabilities like those targeted by IoT Reaper, and zero-day vulnerabilities like on Huawei customer premise equipment (CPE) devices by Zatori Mirai.

Interestingly enough, all of the above mentioned attack tools weren't used in anger, but as mentioned before, they were most probably used for field testing on the internet. The attacks were active for short time periods, with quick multiple new releases and then the Command-and-Control servers were taken offline. Based on the results, they either continued internal development or sold the finalized attack tool to either the Booter/Stresser community or to dedicated attackers with enough funding to pay for such advanced malware.



Malware Innovation

Almost all of the IoT devices targeted in the DDoS attacks in late 2016 were directly connected to the internet, which made it easy for the attackers to detect and subsequently infect the devices with botnet code.

95%

OF ALL IoT DEVICES ARE LOCATED BEHIND SOME KIND OF INTERNET GATEWAY OR FIREWALL

Making them invisible to internet scans and protected from IoT malware.

Attackers realize the DDoS effectiveness of IoT devices.

THEY BEGIN TO LOOK AT HOW TO TAKE ADVANTAGE OF THE REMAINING

5%

In early February 2017, a multi-stage Windows Trojan containing code to scan for vulnerable IoT devices and inject them with the Mirai bot code was detected in the wild.

This weaponization of a Windows Trojan to deliver IoT bot code reveals an evolution in the threat landscape that most organizations are completely unprepared to deal with: DDoS attacks from within.

Windows machines infected by the Mirai Trojan can actively scan for IoT devices whenever they establish a network connection. For example, if a laptop gets compromised by the Windows Mirai Seeder on a public wireless network, it will start scanning for vulnerable IoT devices as soon as it makes a network connection. It could be any network connection — one to an internal corporate network via VPN, a wireless network or a physical one.

Almost all networks, from a small SoHo business to the largest enterprise, have a large number of IoT devices connected to them, from the smart TV in a home to intelligent network-enabled thermostats in a large company. These devices are, in most cases, protected by network firewalls, making them unreachable by scans from malicious devices on the internet.

The Windows Mirai Seeder is a game changer, however, because compromised Windows computers can now scan for vulnerable IoT devices whenever they connect to an internal network via VPN, wireless or physical connections.

Unless proper care is taken to segment internal networks, any device with an IP stack is a potential target for compromise. Currently the Mirai bot infects devices like web cameras and DVR recorders but it can easily be modified to attack other devices like printers, scanners and HVAC controllers. Any device, once compromised, can start scanning for other vulnerable IoT devices and infect them if detected.

The Internally Facing DDoS Extortion Attack

A clever attacker could use the multi-stage Trojan mentioned above to get inside a network, subsuming vulnerable IoT devices into a botnet. The attacker could then scan the internal network to identify vulnerable network devices and critical services.

The attacker could use this information to direct the compromised IoT devices inside the network to launch a devastating attack against the network itself or critical services inside of the network. This kind of attack could be used either to deny service for an extended period, or as a proof-of-capability for an extortion demand.

If the network is not designed to withstand these kinds of internal attacks, it could be a time-consuming, costly and complex task to redesign and secure the network. In the worst case, the network security posture would have to be rethought from scratch, beginning by shutting down all communication on all links, including any internet connections.

A DDoS attack launched using IoT devices located on the inside of an enterprise network can cause very high traffic levels, in terms of both volume and packets-per-second. Even if the attack is destined towards external targets, the attack traffic must first traverse the internal network. This can result in network link congestion on WAN and LAN segments and a high CPU load on network devices, all potentially leading to network outages.

TO MITIGATE THE IMPACT OF SUCH ATTACKS, THE FOLLOWING SHOULD BE IMPLEMENTED:

1

Flow telemetry (such as NetFlow or IPFIX) export, collection, and analysis, along with the collection and analysis of recursive DNS queries and responses.

This provides comprehensive visibility into network traffic and allows for the rapid detection of any abnormalities and internally launched DDoS attacks.

2

Control plane policing on all network devices.

This allows the network devices to withstand both direct attacks against the network elements and traversing traffic attacks.

3

Secure routing protocols against attacks and overload.

Without routing, no traffic can traverse the network.

4

Management plane protection to secure and protect management traffic.

In addition, add reserve bandwidth and capacity on WAN and LAN links for management plane traffic. If unable to communicate with the network elements, the attack cannot be mitigated.

5

Data plane protection to filter and control what traffic should be allowed through the network.

For instance, a DNS server farm should only receive DNS traffic. And client computers should only communicate with specific services on specific ports, not each other. In addition, data plane protection should be implemented using non-stateful controls like iACLs, as stateful controls have to tendency to crash and burn during heavy attacks.

6

A quarantine system to isolate compromised devices.

This allows for the utilization of flow telemetry collection and analysis, recursive DNS collection and analysis, and other forms of detection and classification. These make use of recursive DNS poisoning to implement a universal 'soft' quarantine, as well as VLAN- and WiFi channel-based 'hard' quarantine mechanisms, to isolate botted devices.

7

Do not trust any quality-of-service tags made by clients.

Downgrade those such that management plane traffic has highest priority.

Conclusion

Typical IoT devices are less secure than any desktop computer, making them the attacker's choice for compromise. Attackers are busy inventing new attack methods and vectors, aiming to bypass current countermeasures. They are also looking to take advantage of IoT devices which were previously thought to be secure behind corporate firewalls.

With the introduction of the Windows Mirai Trojan, a new threat scenario has emerged which has the potential to cause a myriad of issues.

As stated earlier, a network designed and secured using best current practices (BCPs) described herein will be highly resistant to such compromise and the ramifications thereof. In addition, the network will be more resistant to new attack vectors.

DNS OPERATORS

DNS Operators

Sixty-eight percent of all respondents indicated that they operate a DNS infrastructure, slightly down from 74 percent in 2016, but in line with 2015 (Figure 96).

OPERATE DNS SERVERS IN THE NETWORK?

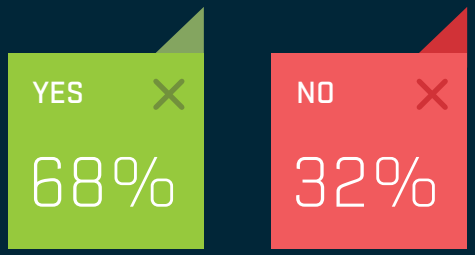


Figure 96 DNS Operators

Most of the DNS operators are in United States, Canada and Europe (Figure 97), although their network operations cover all parts of the globe (Figure 98). This shows that operating a DNS infrastructure is more common in North America and Europe than in Latin America or in the Middle East, Africa and Asia-Pacific regions.

Looking at respondent types, 79 percent of enterprise, government and education (EGE) organizations are running DNS servers, slightly up from 75 percent in 2016. Like in the previous year, we observed that EGE respondents are taking control of critical infrastructures like DNS, rather than outsourcing their management.

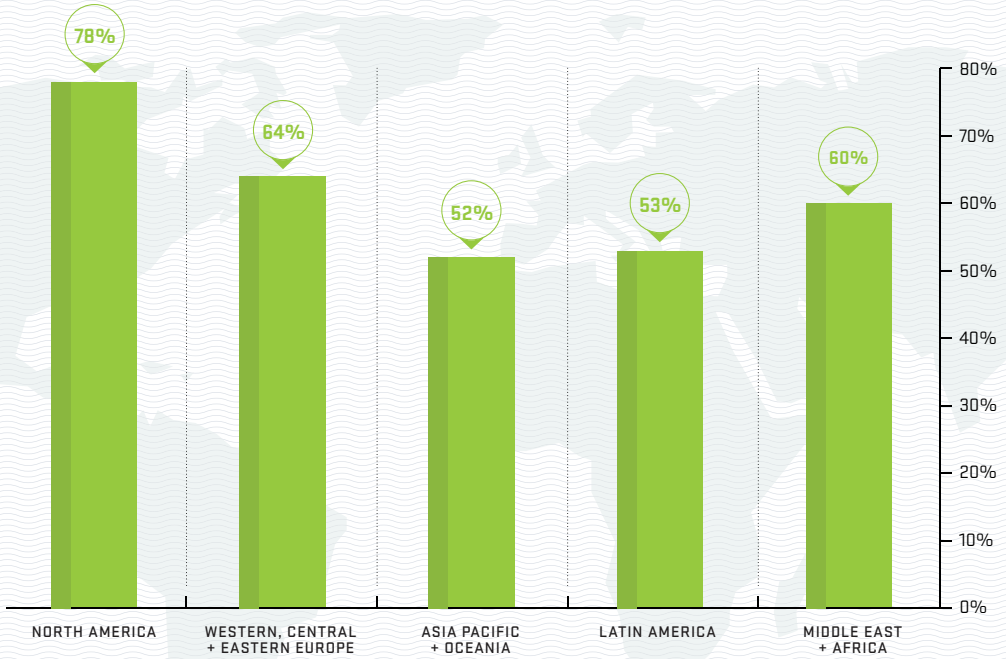


Figure 97 DNS Operators (Per Region HQ)

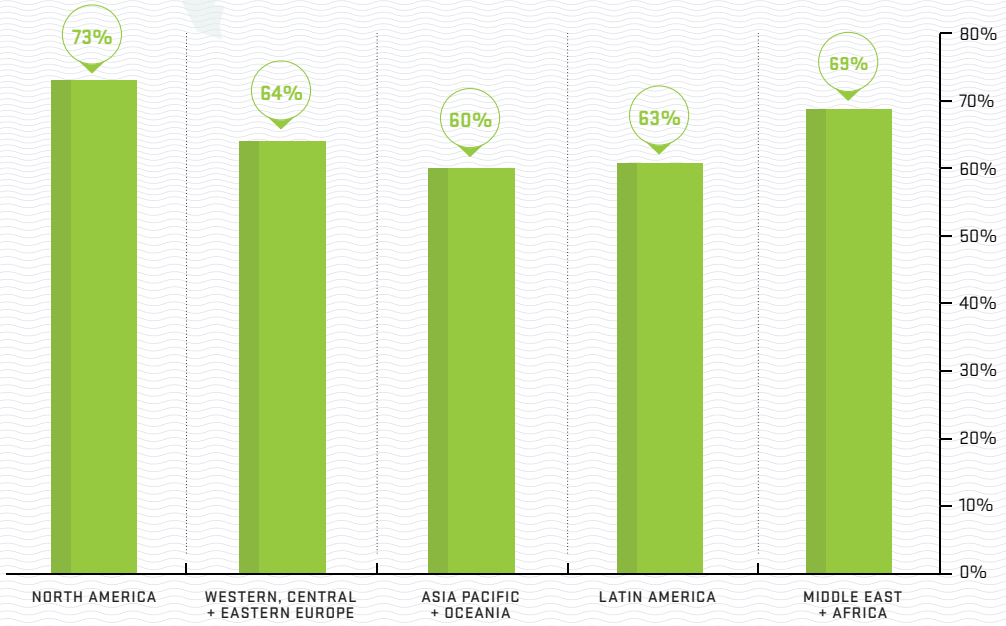


Figure 98 DNS Operators (Per Region Operations)

In 2017, we again asked all respondents if DNS security was managed by a special dedicated group, a primary security team or if there was no assigned responsibility (Figure 99). The results once again showed a small improvement over the previous year, as the percentage with a dedicated DNS security team increased from 22 to 25 percent, and those with no specific responsible group fell from 20 to 16 percent.

Looking at the breakout between EGE organizations and service providers, there was a substantial increase of EGE organizations with a dedicated DNS security team, at 24 percent in 2017 up from 16 in the previous year (Figure 100). As for service providers, it is disappointing to see that those with a special security group for DNS have decreased slightly, from 27 percent to 25, considering the criticality of DNS to these organizations. On a more positive note, in 2017, the percentage of both EGE organizations and service providers with no security group decreased, from 18 percent to 15 for EGEs and from 23 percent to 16 for service providers.

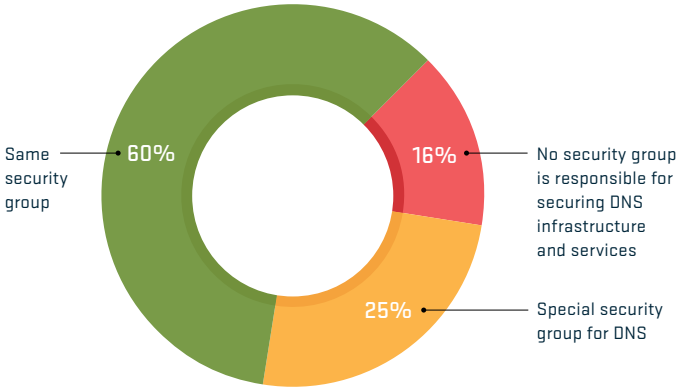


Figure 99 DNS Security Responsibility (All Respondents)

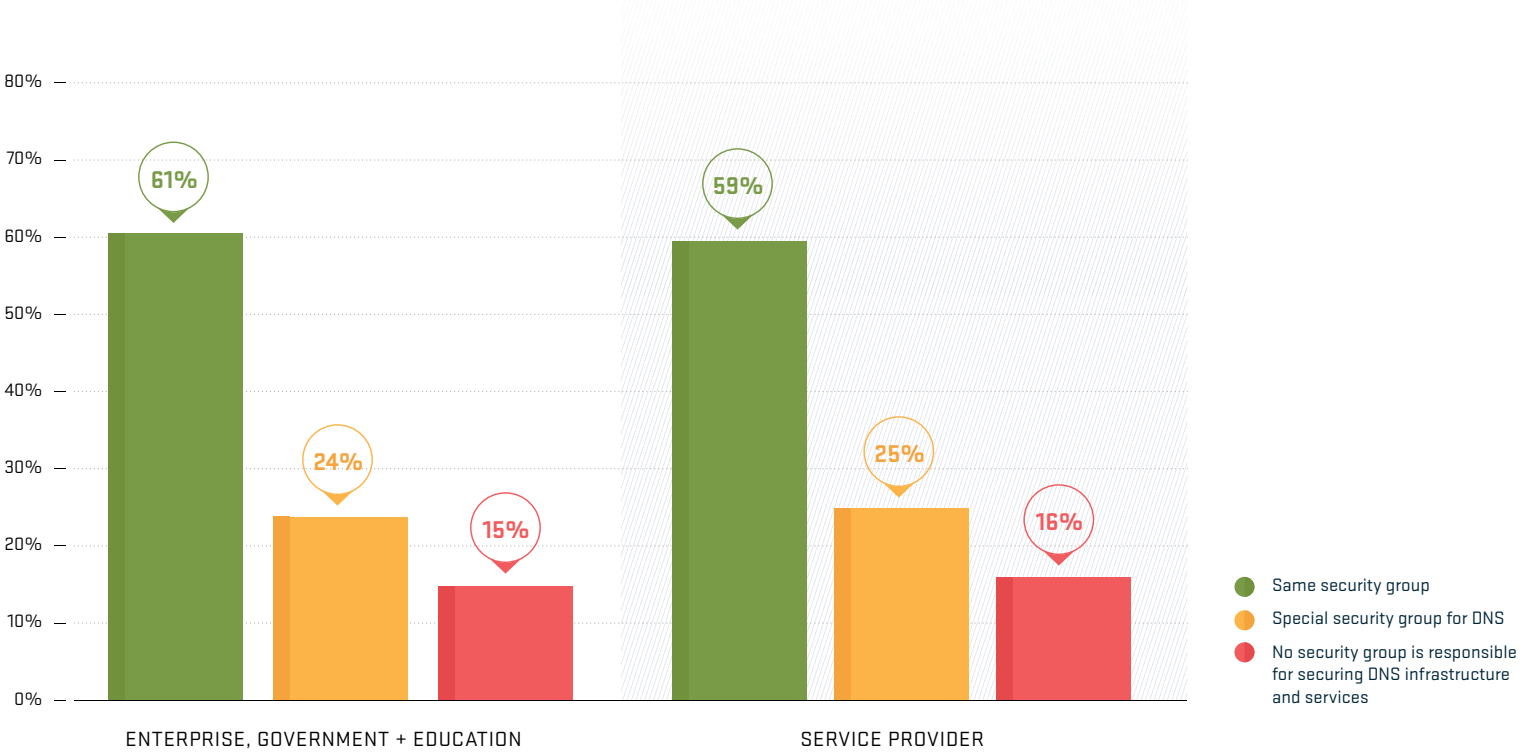


Figure 100 DNS Security Responsibility (Per Operator Type)

Visibility of DNS traffic in 2017 was similar to the previous year, with 73 percent of all respondents having visibility at Layers 3 and 4, and 43 percent at Layer 7 (Figure 101). Only 33 percent of service providers have visibility of their DNS traffic at Layer 7, which is down from 42 percent in 2016 (Figure 102). In contrast, 49 percent of EGE organizations reported having visibility of their DNS traffic at Layer 7, an increase from 35 percent in 2016.

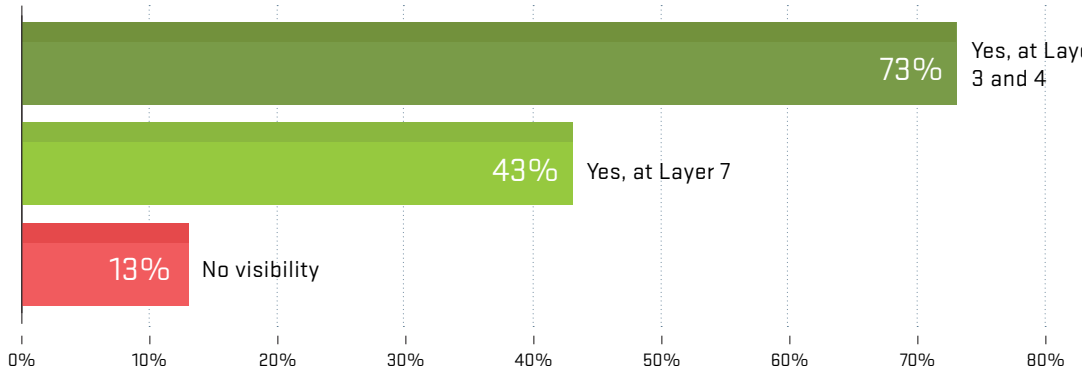


Figure 101 DNS Visibility

It is a positive sign that more EGE organizations are taking control of their DNS infrastructure and visibility at Layer 7, as effective mitigation of DDoS attacks targeting DNS requires application-layer visibility.

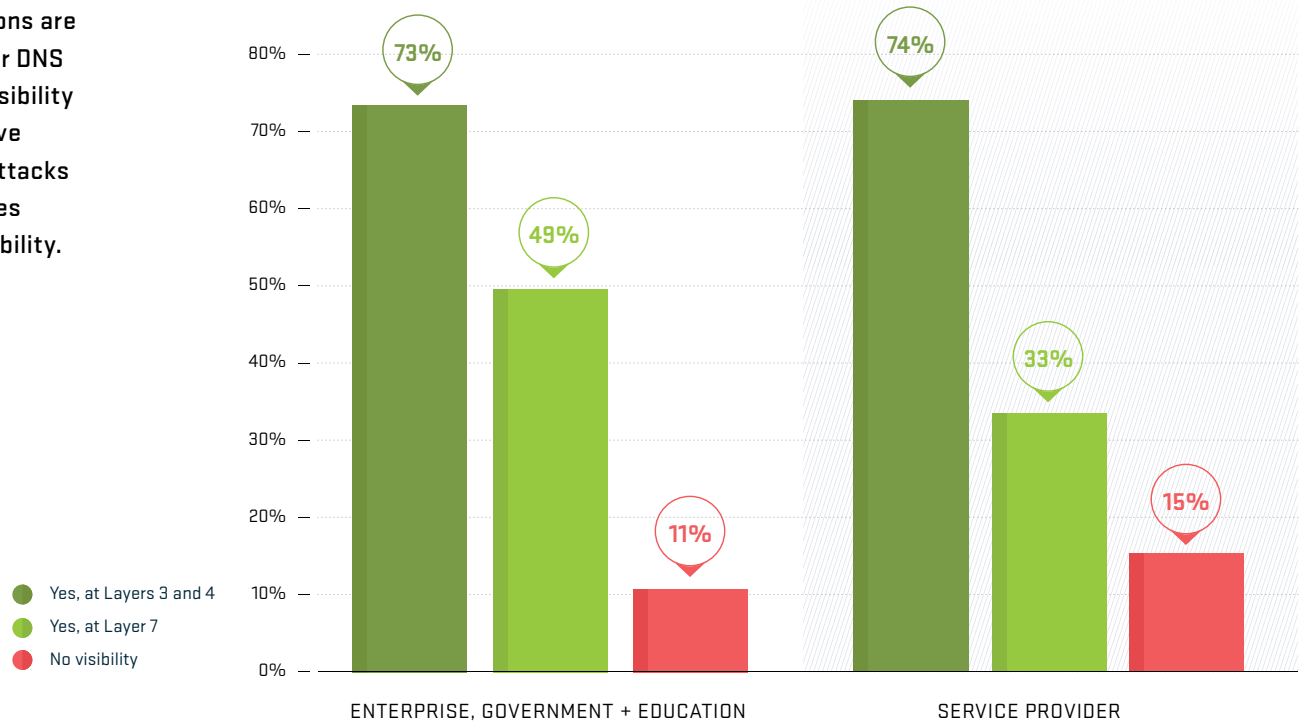


Figure 102 DNS Visibility (Per Operator Type)

As stated in previous reports, DNS is critical to maintaining the availability of services. Unfortunately, DNS servers are popular both as direct targets of DDoS attacks, but also as unwilling amplification and reflection actors. As a result, it is disappointing again to note that 19 percent of respondents still did not restrict access to their recursive DNS servers in 2017 (Figure 103).

RESTRICT RECURSIVE DNS LOOKUPS TO YOUR CUSTOMERS AND NETWORKS?

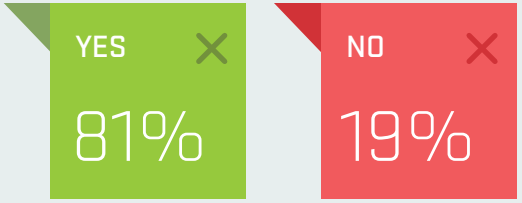


Figure 103 Recursive DNS Restrictions

The percentage of DDoS attacks that target DNS infrastructures and affect service did not change from 2016 for all our respondents (Figure 104). While we can see organizations are making progress in protecting their DNS infrastructure, this shows that DDoS attacks targeting DNS servers remain a constant threat.

Among EGE organizations, the percentage that experienced publicly visible service outages increased to 22 percent in 2017, up from 13 percent in the previous year (Figure 105). Conversely, the proportion of service providers suffering these attacks dropped to 31 percent in 2017 from 39 the previous year.

DDoS ATTACKS AGAINST DNS INFRASTRUCTURE THAT LED TO A VISIBLE OUTAGE?

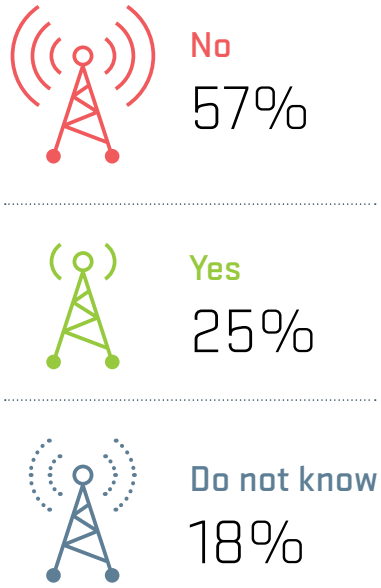


Figure 104 DNS Service Affecting DDoS Attacks

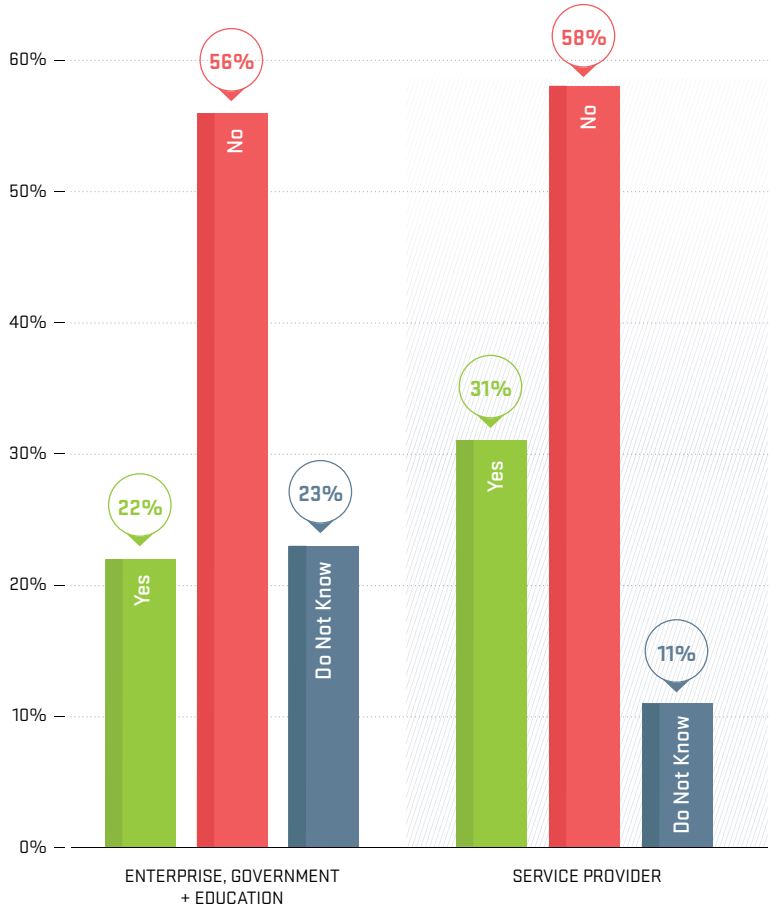


Figure 105 DNS Service Affecting DDoS Attacks (Per Organization Type)

EXPERIENCED DDoS ATTACKS AGAINST AUTHORITATIVE DNS SERVERS?

Figure 106 DDoS Attacks Against Authoritative DNS Servers

EXPERIENCED DDoS ATTACKS AGAINST RECURSIVE DNS SERVERS?

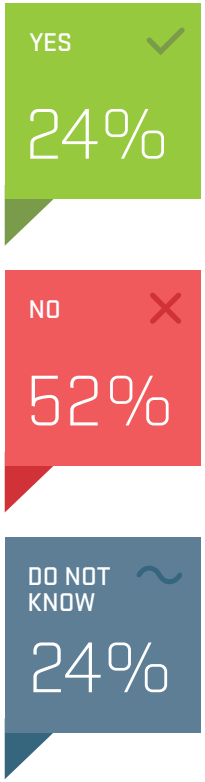


Figure 107 DDoS Attacks Against Recursive DNS Servers

DDoS attacks are still targeting Authoritative DNS servers (Figure 106) more frequently than Recursive servers (Figure 107). However, there was an overall reduction in attacks for both EGE organizations and service providers. The percentage of respondents seeing attacks against Recursive servers went down from 30 percent in 2016 to 24 in 2017, while the proportion of respondents seeing DDoS attacks targeting Authoritative DNS servers decreased slightly to 32 percent.

As expected, service providers saw more attacks against both Recursive and Authoritative DNS servers (Figure 108). Forty-four percent of providers reported attacks against their Authoritative DNS servers compared to 23 percent for EGE organizations, an increase for EGE respondents from 16 percent in 2016. Thirty-four percent of providers saw attacks against their Recursive DNS servers (Figure 109), down from 44 percent in 2016, while 18 percent of EGEs experienced these attacks, down from 24 percent in 2016.

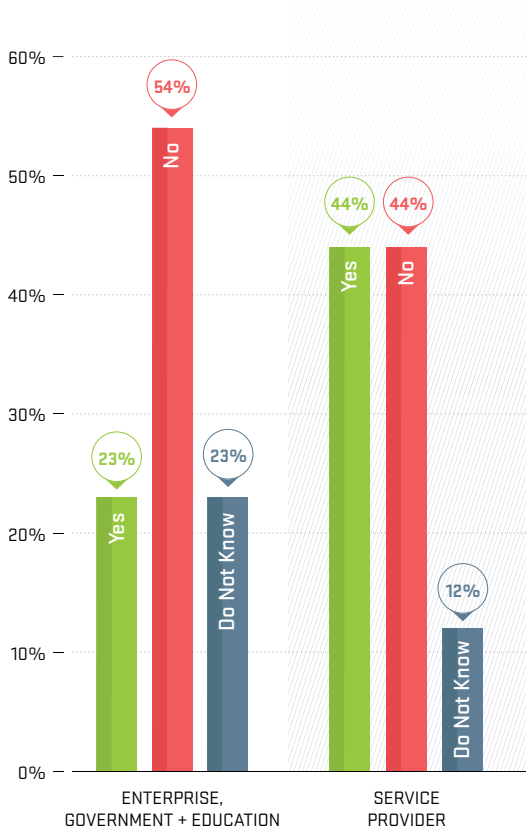


Figure 108 DDoS Attacks Against Authoritative DNS Servers (Per Organization Type)

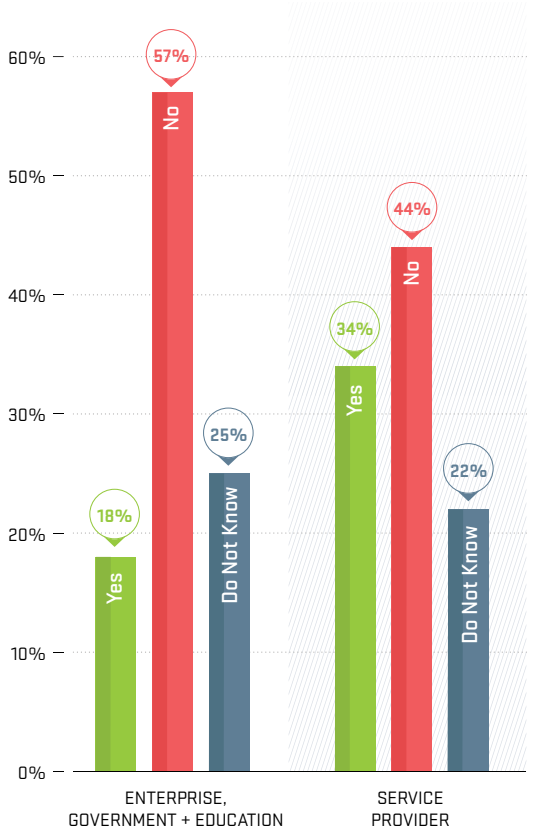


Figure 109 DDoS Attacks Against Recursive DNS Servers (Per Organization Type)

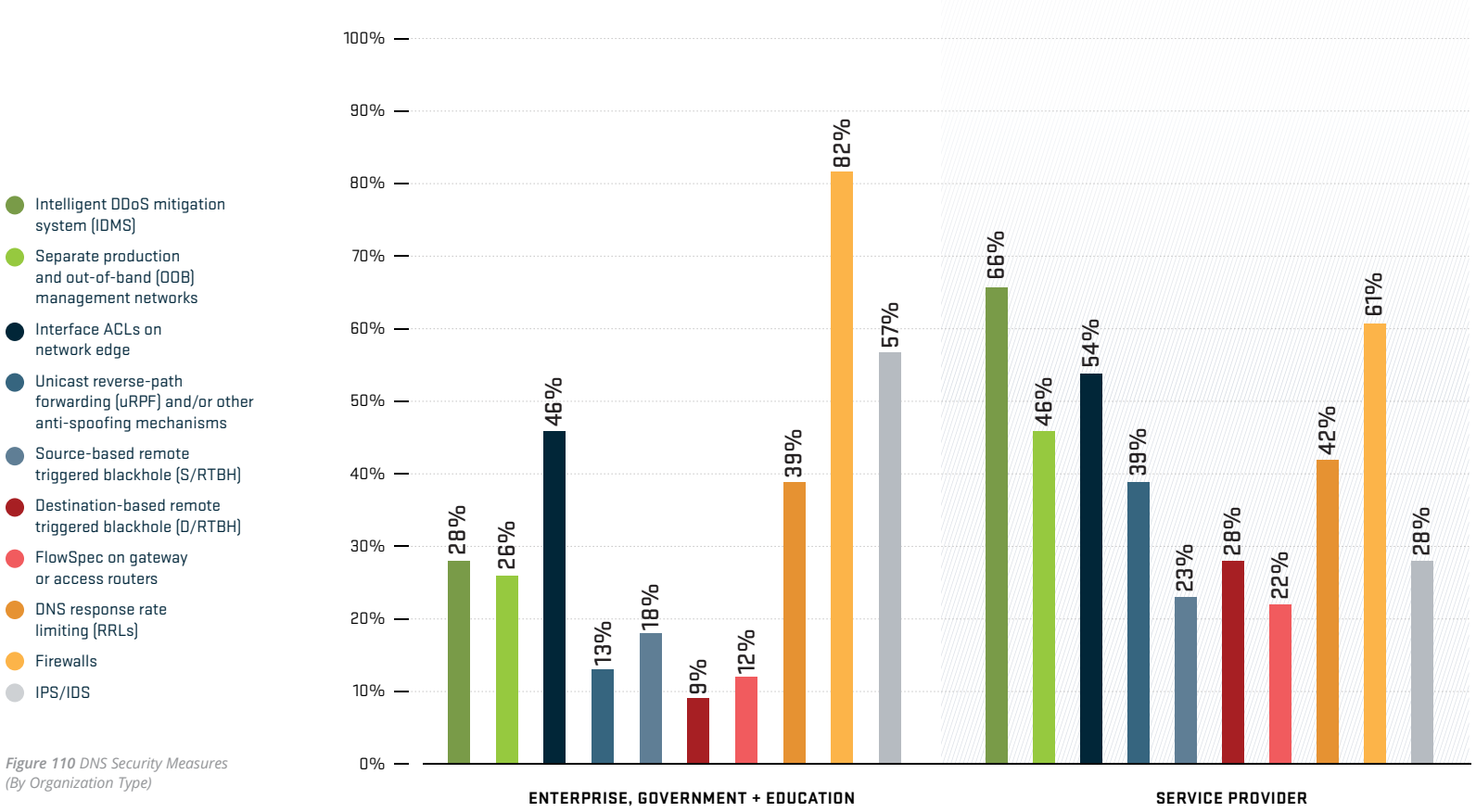
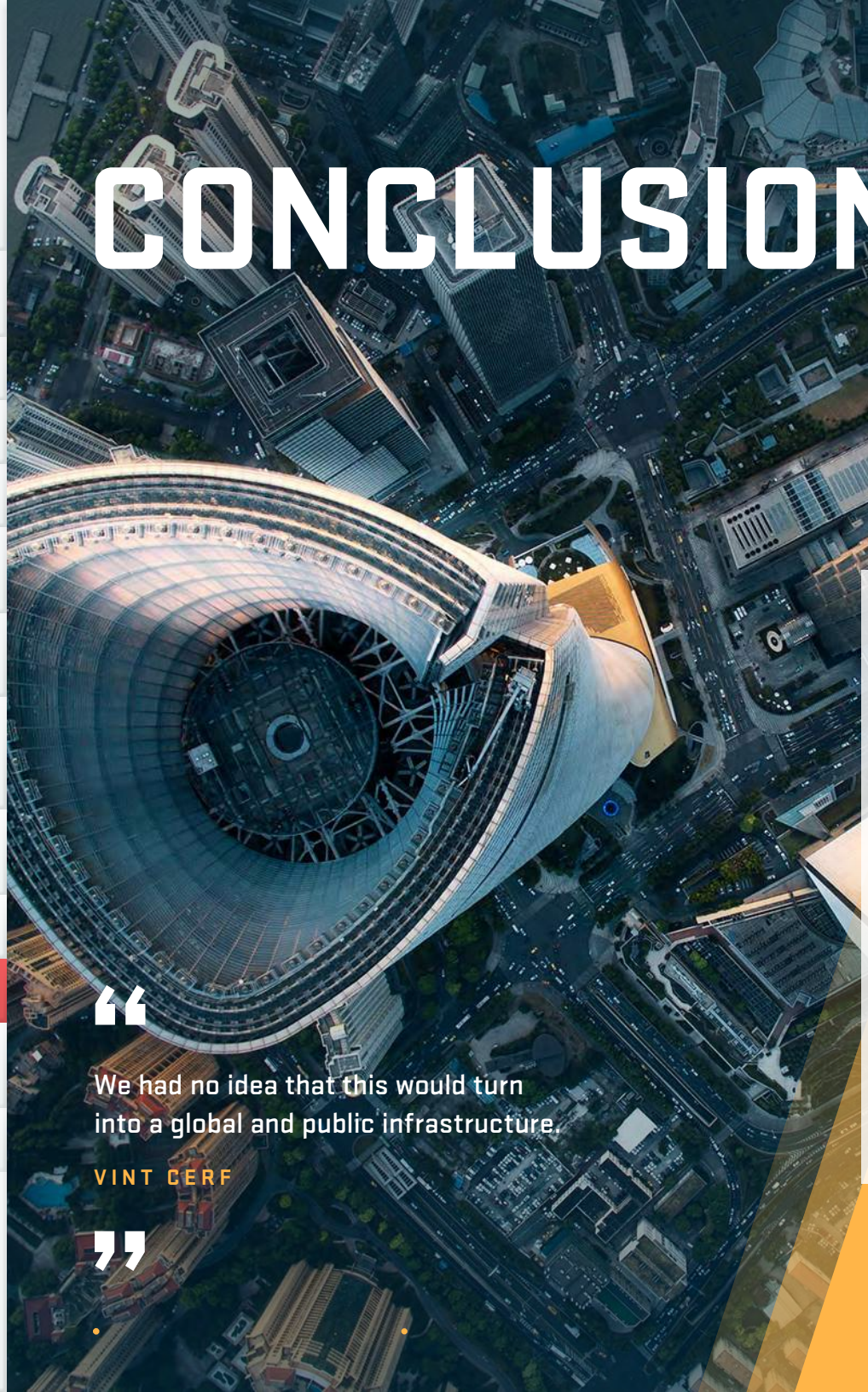


Figure 110 DNS Security Measures (By Organization Type)

The security measures put in place to protect DNS infrastructures vary greatly once again between service providers and EGE organizations. For service providers, Intelligent DDoS Mitigation Systems (IDMS) were again the most popular defense mechanism, with 66 percent of respondents having them deployed, up slightly from 64 in 2016 (Figure 110). Following in second and third place are firewalls and ACLs, respectively at 61 and 54 percent. Seeing firewalls as the second most reported option is disappointing, as these devices do not protect adequately against DDoS attacks due to their nature and the ease with which a state-based attack can overwhelm them.

In EGE organizations, firewalls were the most popular choice, at 82 percent up from 79 percent in 2016, which again is disappointing. In second place were IPS/IDS at 57 percent, another piece of bad news considering that they are similarly vulnerable to DDoS attacks.

CONCLUSION

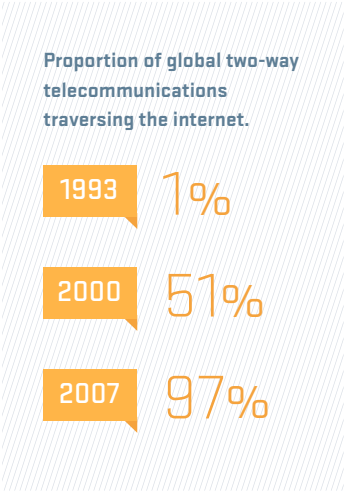


> We had no idea that this would turn into a global and public infrastructure.
>
> VINT CERF

Following the introduction of electronic computers in the 1950s, early concepts of wide area networking originated in the United States, United Kingdom and France. The U.S. Department of Defense awarded contracts in the 1960s, which eventually lead to the ARPANET project. The first message was sent over the ARPANET in 1969.

The concept of transmission control protocol/internet protocol (TCP/IP) suite was presented in a paper in 1974 by authors Vinton Cerf and Robert Kahn, who also came up with the term internet, which was short for "inter-networking of networks." Commercial internet service providers (ISPs) began to emerge in the late 1980s.

Since the mid-1990s, the internet has had a revolutionary impact on culture, commerce and technology, including the rise of near-instant communication.



While it transported only one percent of the information flowing through two-way telecommunications networks in 1993, the internet grew rapidly. It carried 51 percent of two-way traffic by 2000 and more than 97 percent by 2007. The internet continues to grow today, driven by ever greater amounts of information, commerce, entertainment and social networking.

Now, more than ever, business and commerce simply cannot exist without robust internet infrastructure that is continuously available. Even recreation and socialization depend on the internet to deliver information, goods and services. It is this environment that simultaneously enables our modern lifestyle and work routines while also putting them at risk from those who would exploit this ubiquitous availability for nefarious purposes.

As we have seen in this year's report, attackers continue to build and weaponize massive IoT botnets of unprecedented size and capability. Volumetric DDoS attacks have scaled back a bit in sheer size, but continue to increase in frequency. In last year's report, we highlighted the use of reflection/amplification DDoS attacks as equally effective to IoT botnets for generation of very large scale volumetric DDoS attacks.

> "The internet is becoming the town square for the global village of tomorrow."
>
> BILL GATES

This year, we've seen increasing sophistication of IoT-based botnet attack capabilities. These modern botnets are capable of delivering attacks that include application-layer, volumetric and complex multi-vector DDoS attacks. Further, easy-to-use DDoS for hire services have helped make more sophisticated multi-vector DDoS attacks increasingly common.

On a positive note, both service providers and enterprises share an increased appreciation of the impact a successful DDoS attack can have. This is leading to the adoption of more effective defenses. In service provider networks, it is now widely accepted that purpose-built Intelligent DDoS Mitigation Systems serving as part of a layered defense are the only effective option for mitigating DDoS attacks. Enterprise, government and education organizations also indicated that they have an increasing understanding of this reality. While many still deployed traditional security technologies for DDoS defense, there is increased acceptance of the shortcomings of these solutions.

While online gaming is seen as the top motivation behind DDoS attacks this year, criminal activity and especially extortion remain major drivers of malicious activity. The motivations behind attacks are many and varied, but the ease with which anyone can launch attacks is a growing problem. DNS continues to be one of the most targeted internet services. DNS servers are popular both as direct targets of DDoS attacks, but also as unwilling amplification and reflection actors. It is a positive sign that more organizations are taking control of their DNS infrastructure and ensuring visibility of DNS traffic at Layer 7, as effective mitigation of DDoS attacks targeting DNS requires application-layer visibility.

> It is the obvious which is so difficult to see most of the time. People say 'It's as plain as the nose on your face.' But how much of the nose on your face can you see, unless someone holds a mirror up to you?
>
> ISAAC ASIMOV

The global shortage of security professionals, continues to worsen with no end in sight. While many organizations pursue outsourcing, machine learning or automation strategies to help fill the gap, increased efficiency and organic growth of internal teams are still vital strategies. This is the second consecutive year the survey shows an overall decline in service providers implementing security infrastructure best practices. Surprisingly, given the popularity of reflection attacks over the last five years, the adoption of anti-spoofing filters decreased.

Reputation/brand damage and operational expense are still the top business impacts of DDoS attacks. There was also a big jump in revenue loss. Survey responses broadly indicate that the cost of a major DDoS attack is increasingly significant. Over three quarters of enterprise, government and education network operators reported that DDoS mitigation was a part of either their business or IT risk assessments. And, more service providers are now offering DDoS protection services, given the continued increasing interest in these services among customers across a broad range of verticals.

NETSCOUT Arbor is proud to release the 13th annual *Worldwide Infrastructure Security Report*. This report is designed to help network operators understand the breadth of the threats that they face, gain insight into what their peers are doing to address these threats, and comprehend both new and continuing trends. This year's report features responses from service provider, enterprise, government and education organizations.

A good global distribution of respondents rounds out what has been our broadest representation of the internet community ever. We hope that you find the information useful in protecting your business for the coming year.

ABOUT THE AUTHORS

Philippe Alcoy

PRINCIPAL SECURITY TECHNOLOGIST, NETSCOUT ARBOR

palcoy@arbor.net

Philippe has more than 20 years of experience in Cybersecurity Defense & Attack. He started his career with AvantGo in the city of London, securing and mobilizing web applications on early smartphones and PDAs for banks and insurances. After the first IT bubble burst, he joined vulnerability assessment pioneers eEye Digital Security and started a 15-year stint in technical leadership, consulting and management roles in the IT security, risk and compliance management market. Philippe relocated to Asia 10 years ago to manage Qualys APAC operation, looking after large enterprises and managed security service providers. He recently joined the office of the CTO at NETSCOUT Arbor focusing on advanced threat and research.

Steinthor Bjarnason

SENIOR NETWORK SECURITY ANALYST, NETSCOUT ARBOR

sbjarnason@arbor.net

Steinthor Bjarnason is a Senior Network Security Analyst on the NETSCOUT Arbor ASERT team, performing applied research on new technologies and solutions to defend against DDoS attacks. He has more than 18 years of experience working on internet security, IoT security, cloud security, SDN security, core network security and DDoS attack mitigation. Steinthor is an inventor and principal of the Cisco Autonomic Networking Initiative, with a specific focus on security automation where he holds a number of related patents.

Paul Bowen

PRINCIPAL SECURITY TECHNOLOGIST, NETSCOUT ARBOR

pbowen@arbor.net

Paul Bowen brings over 22 years of experience to his role at NETSCOUT Arbor where his primary focus is on advanced threats. Previously he was an architect for advanced threat solutions at Fortinet. He also was the architect for Mandiant cloud-based SIEM, called TAP. Paul spent two years as a security and compliance conference speaker for Hewlett-Packard as a member of Office for Advanced Solutions, seven years as a principal Engineer for Arcsight and 10 years as a manager of global security for Estée Lauder.

C.F. Chui

PRINCIPAL SECURITY TECHNOLOGIST, NETSCOUT ARBOR

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 NETSCOUT Arbor, 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 NETSCOUT Arbor's global research projects. Before joining NETSCOUT 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.

Kirill Kasavchenko

PRINCIPAL SECURITY TECHNOLOGIST, NETSCOUT ARBOR

kkasavchenko@arbor.net

Kirill has more than 14 years of experience in various post- and pre-sales roles dealing with telecom and large enterprises in more than 30 countries in Europe, Middle East, Russia and CIS. His areas of interest are network design and network security at a large scale. On the CTO team at NETSCOUT Arbor, Kirill focuses on emerging technologies and global research projects, applying his expertise in routing and protocol analysis to find new ways to protect customers' networks.

Kirill holds B.S. and M.S. with honors in Computer Sciences from the Saint Petersburg University of IT, Mechanics and Optics as well as a number of industry certifications including Cisco CCIE. Prior to joining Arbor in 2011 he spent seven years on different positions ranging from network technician to chief engineer at systems integrators and network infrastructure vendors.

Gary Sockrider

PRINCIPAL SECURITY TECHNOLOGIST, NETSCOUT ARBOR

gsockrider@arbor.net

Gary Sockrider is an industry veteran bringing over 25 years of broad technology experience including routing and switching, mobility, collaboration and cloud but always with an eye on security. His previous roles include security SME, consultancy, customer support, IT and product management. He seeks to understand and convey the constantly evolving threat landscape, as well as the techniques and solutions that address the challenges they present. Prior to joining NETSCOUT Arbor in 2012, he spent 12 years at Cisco Systems and held previous positions with Avaya and Cable & Wireless.

ABOUT THE EDITOR

Darren Anstee

CHIEF TECHNICAL OFFICER, NETSCOUT ARBOR

danstee@arbor.net

Darren serves as the Chief Technical Officer for NETSCOUT Arbor, developing the technology strategy of NETSCOUT Arbor products and services. His efforts help customers see and understand network traffic in order to tackle their most complex security challenges.

He works closely with NETSCOUT Arbor's Security Engineering & Response Team (ASERT), product management, sales and engineering organizations to drive alignment on the next generation capabilities that will help NETSCOUT Arbor's customers across enterprise and service provider markets. Darren has over twenty years of experience in networking and security, the last 14 years spent with NETSCOUT Arbor.

GLOSSARY

A

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

B

BCP	Best Current Practice
BYOD	Bring Your Own Device

C

CDN	Content Delivery Network
C&C	Command-and-Control

D

DCN	Data Communication Network
DNS	Domain Name System
DDoS	Distributed Denial of Service
D-RTBH	Destination-Based Remotely Triggered Blackholing
S-RTBH	Source-Based Remotely Triggered Blackholing

E

EGE	Enterprise, Government & Education

G

Gbps	Gigabits-per-second
Gi	Global Internet
GTP-C	General Packet Radio Service (GPRS) tunneling protocol (GTP)
GTP-U	GPRS Tunneling Protocol User Plane
GTSM	Generalized TTL Security Mechanism

H

HTTP	Hypertext Transfer Protocol
HTTP/S	HTTP Secure
iACL	Infrastructure ACL

I

ICMP	Internet Control Message Protocol
IDMS	Intelligent DDoS Mitigation System
IDS	Intrusion Detection System
IGP	Interior Gateway Protocol
IoT	Internet of Things
IPS	Intrusion Prevention System
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IR	Incident Response
IRC	Internet Relay Chat
ISP	Internet Service Provider

K

KPI	Key Performance Indicator

L

LTE	Long Term Evolution

M

Mbps	Megabits-per-second
MDM	Mobile Device Management
MITM	Man in the Middle
MNO	Mobile Network Operator
MPC	Mobile Packet Core
MSSP	Managed Security Service Provider

GLOSSARY

N

NAT	Network Address Translation
NFV	Network Functions Virtualization
NGFW	Next Generation Firewall
NMS	Network Management System
NTP	Network Time Protocol

O

OOB	Out of band
OPSEC	Operational Security
OTT	Over the Top

P

PAT	Port Address Translation
PCAP	Packet Capture

Q

QoE	Quality of Experience

R

RAN	Radio Access Network

S

SDN	Software-defined networking
SEG	Security Gateways
SIEM	Security Information Event Management
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
S/RTBH	Source-based Remotely Triggered Blackholing
SSDP	Simple Service Discovery Protocol
SSL	Secure Socket Layer
SYN	Synchronize

T

TLD	Top Level Domain
TLS	Transport Layer Security
Tbps	Terabits per second

U

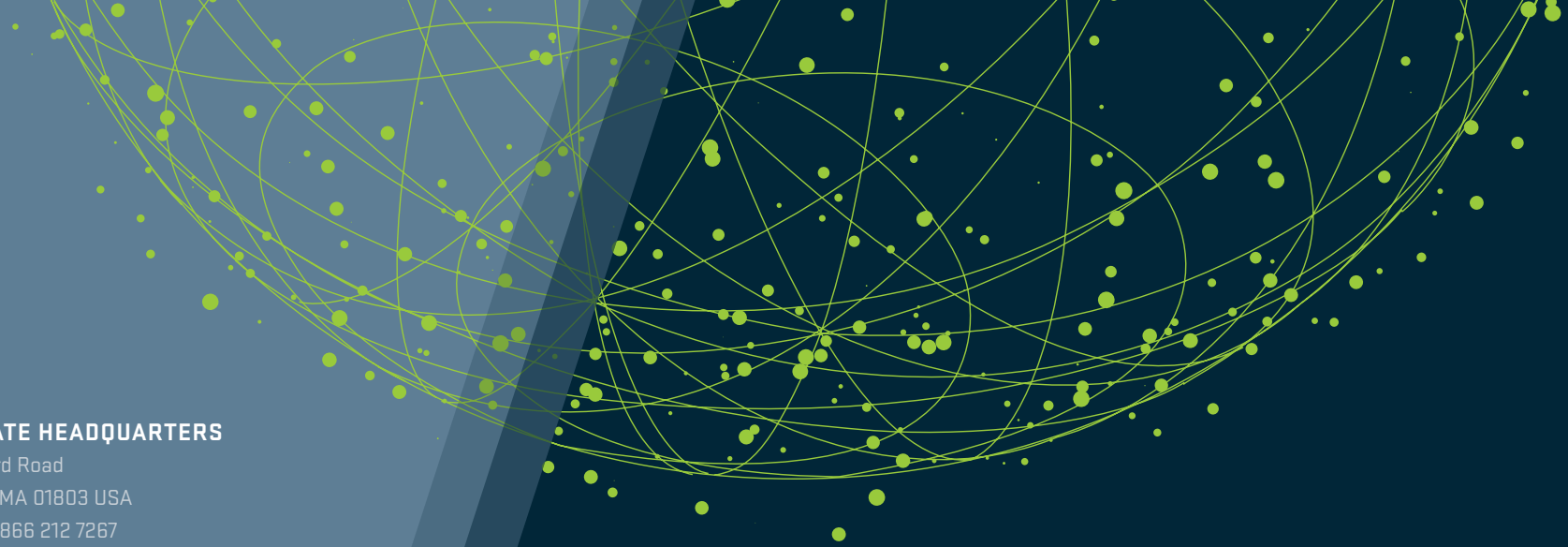
UDP	User Datagram Protocol
uRPF	Unicast Reverse Path Forwarding
UTM	Unified Threat Management

V

VoIP	Voice Over Internet Protocol

W

WAF	Web Application Firewall
WiMAX	Worldwide Interoperability for Microwave Access



CORPORATE HEADQUARTERS
76 Blanchard Road
Burlington, MA 01803 USA
Toll Free +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 6664 3140

LATIN + CENTRAL AMERICA
T +52 55 4624 4842

arbornetworks.com

NETSCOUT
Guardians of the Connected World | Arbor

ABOUT NETSCOUT

NETSCOUT SYSTEMS, INC. (NASDAQ: NTCT) assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility, and insights customers need to accelerate, and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability, and advanced threats that infiltrate networks to steal critical business assets. To learn more about improving service, network, and application performance in physical or virtual data centers, or in the cloud, and how NETSCOUT's performance and security solutions, powered by service intelligence can help you move forward with confidence, visit www.netscout.com or follow @NETSCOUT and @ArborNetworks on Twitter, Facebook, or LinkedIn.