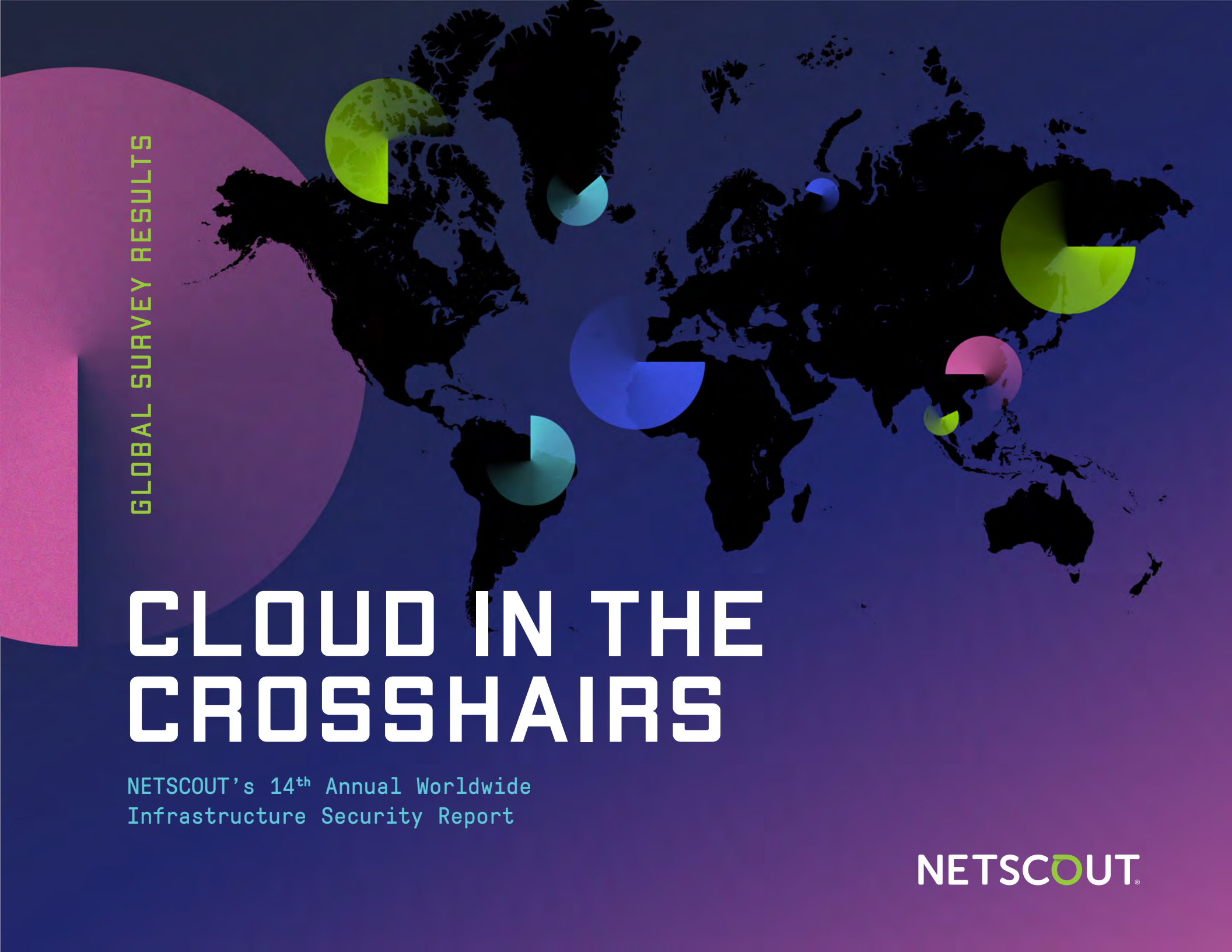


GLOBAL SURVEY RESULTS

CLOUD IN THE CROSSHAIRS

NETSCOUT's 14th Annual Worldwide Infrastructure Security Report

NETSCOUT®

CONTENTS

INTRODUCTION

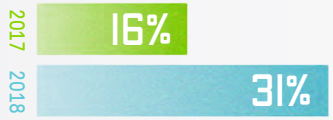
WHEN THE WORLDWIDE INFRASTRUCTURE SECURITY REPORT (WISR) WAS LAUNCHED 14 YEARS AGO, 10 GBPS ATTACKS MADE HEADLINES AND TOOK NETWORKS DOWN. TODAY, ATTACKS FORTY TIMES THAT SIZE ARE ROUTINELY MITIGATED WITH LITTLE TO NO DISRUPTION TO ONLINE SERVICES.

Indeed, that is good news. But think about that for a minute: 400 Gbps attacks are now a matter of routine. The size of DDoS attacks is growing at an alarming pace all around the world, with significant implications for networks operators of all sizes, from global service providers to emerging enterprises.

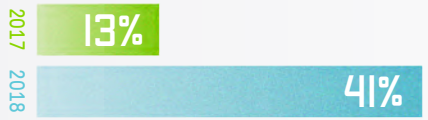
This year, the survey is further enhanced by regional breakdowns of the enterprise respondents. Attack types, targets, techniques, motivations, impacts, and costs are all broken out for US and Canada, Brazil, UK, Germany, France, and Japan. These regional insights from survey respondents are enriched, and frequently validated, by global attack data from NETSCOUT's ATLAS® infrastructure, which delivers visibility into one-third of all internet traffic.

KEY FINDINGS

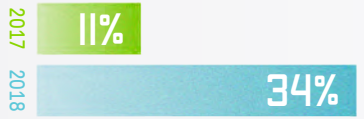
Attacks targeting firewalls and IPS devices



Attacks against SaaS services



Attacks against third-party data centers + cloud services



TERABIT ATTACKS

For the first time ever, a DDoS attack topped 1 Tbps in size. A few days later, a 1.7 Tbps attack was recorded. We've officially entered the Terabit Attack Era. Indeed, we saw a dramatic and persistent increase in DDoS attack size and complexity, as the global max attack size increased 273 percent. This year, 91 percent of enterprises who experienced a DDoS attack indicated that one or more of the attacks completely saturated their internet bandwidth.

CLOUD IN THE CROSSHAIRS

As enterprise organizations invested in cloud-based DDoS mitigation services, attackers shifted to focus on stateful infrastructures. In 2018, attacks targeting firewalls and IPS devices almost doubled, from 16 percent in 2017 to 31 percent.

Important elements of digital transformation strategies are now under attack. In 2018, there was a threefold increase in the number of attacks against SaaS services, from 13 percent in 2017 to 41 percent in 2018. We also saw a significant jump in attacks against third-party data centers and cloud services, from 11 percent to 34 percent.

HIGH COST OF DOWNTIME

For 2018, the cost of downtime associated with internet service outages caused by DDoS attacks was $221,836.80. Germany had the highest downtime costs, at $351,995. Meanwhile, Japan paid the least for downtime, at $123,026.

INSIDE THREATS

Companies again faced risk from inside the firewall—indeed, even from the firewall itself. Forty-three percent reported that their firewall and/or IPS contributed to an outage during a DDoS attack. Malicious insiders also posed a threat, as more than a quarter of respondents indicated their organization experienced an attack by a malicious insider in 2018. France had the highest number at 37.5 percent, while Japan was lowest at 13.8 percent.

ATTACKERS TAKE ON THE PUBLIC SECTOR

Perhaps we should not be surprised given the highly charged political environment in the U.S. and in many places around the world, but 2018 saw a significant change in the customer sectors most often targeted.

In past years, financial services, e-commerce, and gaming customers were at the top of the list. In 2018, it was government customers at 60 percent, up significantly from 37 percent in 2017.

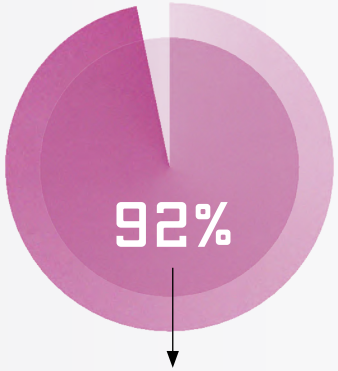
ENTERPRISE

ENTERPRISES REPORTED A HOST OF CHALLENGES THIS YEAR, FROM RANSOMWARE TO EXTORTION TO DDoS ATTACKS, AS WELL AS ONGOING STAFFING AND OPERATIONAL CHALLENGES.

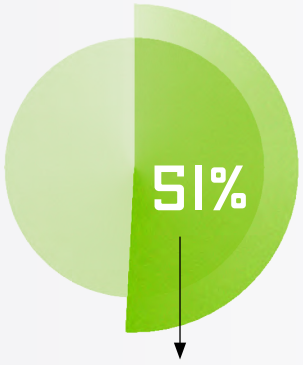
Evident in this year's findings is the continuing game of whack-a-mole between defenders and attackers. For example, as enterprise organizations invested in cloud-based DDoS mitigation services in recent years, attackers shifted their attention to disruptive stateful infrastructure solutions. As a result, attacks targeting firewalls and IPS devices almost doubled, from 16 percent in 2017 to 31 percent in 2018.

The survey provides additional detail with regional breakdowns of the enterprise respondents, including attack types, targets, techniques, motivations, impacts, and costs for US and Canada, Brazil, UK, Germany, France, and Japan.

KEY FINDINGS



Looking to simplify operational security processes



Cited hiring and retaining skilled employees as a major challenge

DIGITAL SERVICES UNDER ATTACK

Important elements of digital transformation strategies are now under attack. In 2018, there was a threefold increase in the number of attacks against SaaS services, as frequency rose from 13 percent in 2017 to 41 percent, as well as against third-party data centers and cloud services (from 11 percent to 34 percent).

TARGETING NEW SERVICES

The increasing use of encrypted traffic was reflected in the growing rate of attacks. In 2018, 94 percent observed such attacks, nearly twice the percentage as the previous year.

SIMPLIFY OPERATIONS, PLEASE

We found a near-universal desire to simplify operational security processes. Ninety-two percent said that they were looking to reduce complexity in some fashion, with the top priority being component and workflow integration.

COST OF DOWNTIME

The cost of downtime in Germany was the highest, at $351,995. Japan had the lowest cost of downtime, at $123,026.

DDoS ATTACK TARGETS AROUND THE WORLD

For infrastructure, the global average was 49 percent. Brazil was highest at 57 percent. Brazil also faced the most attacks on customer-facing services and applications, at 46 percent compared with a global average of 38 percent. Meanwhile, France saw the most attacks on SaaS services, at 53 percent compared with a global average of 41 percent.

HIRING AND RETAINING SKILLED EMPLOYEES

It was cited as a major challenge by 51 percent globally.

ENTERPRISE DEMOGRAPHICS

This year's enterprise report delivers a diverse range of perspectives across regions, industries, and organizations. The global respondent base represents the entire organization, from the C-suite to the end user, providing a multi-disciplinary, multi-industry, and global view.

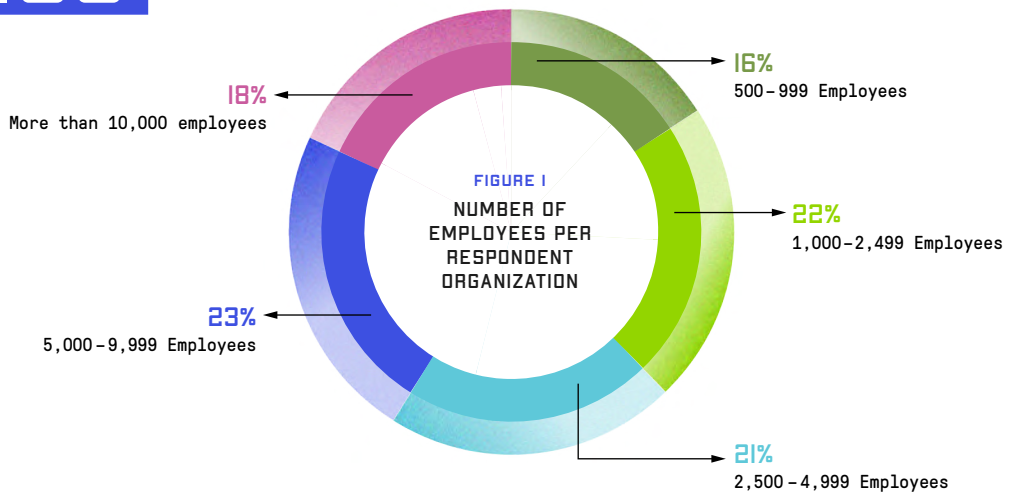


FIGURE 1
NUMBER OF EMPLOYEES PER RESPONDENT ORGANIZATION

FIGURE 2
ORGANIZATIONS' REGIONAL OPERATIONS

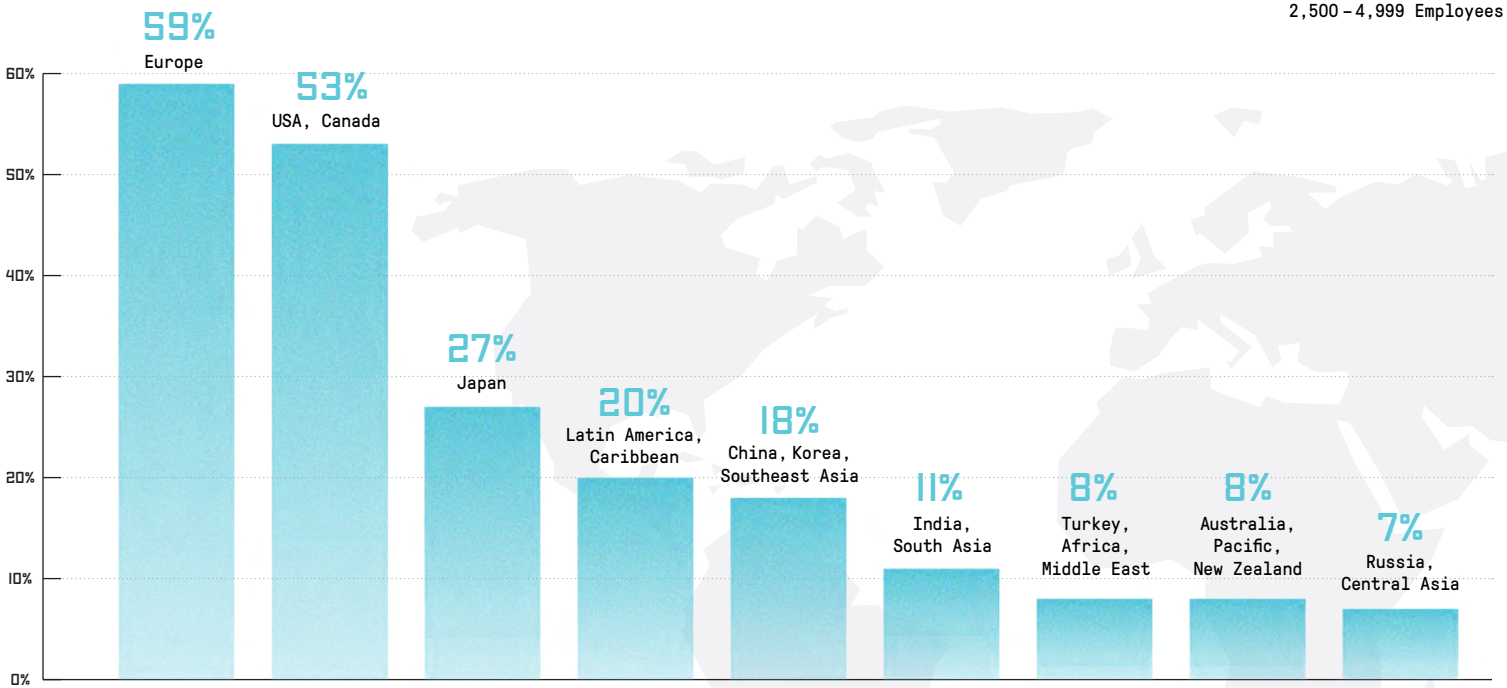


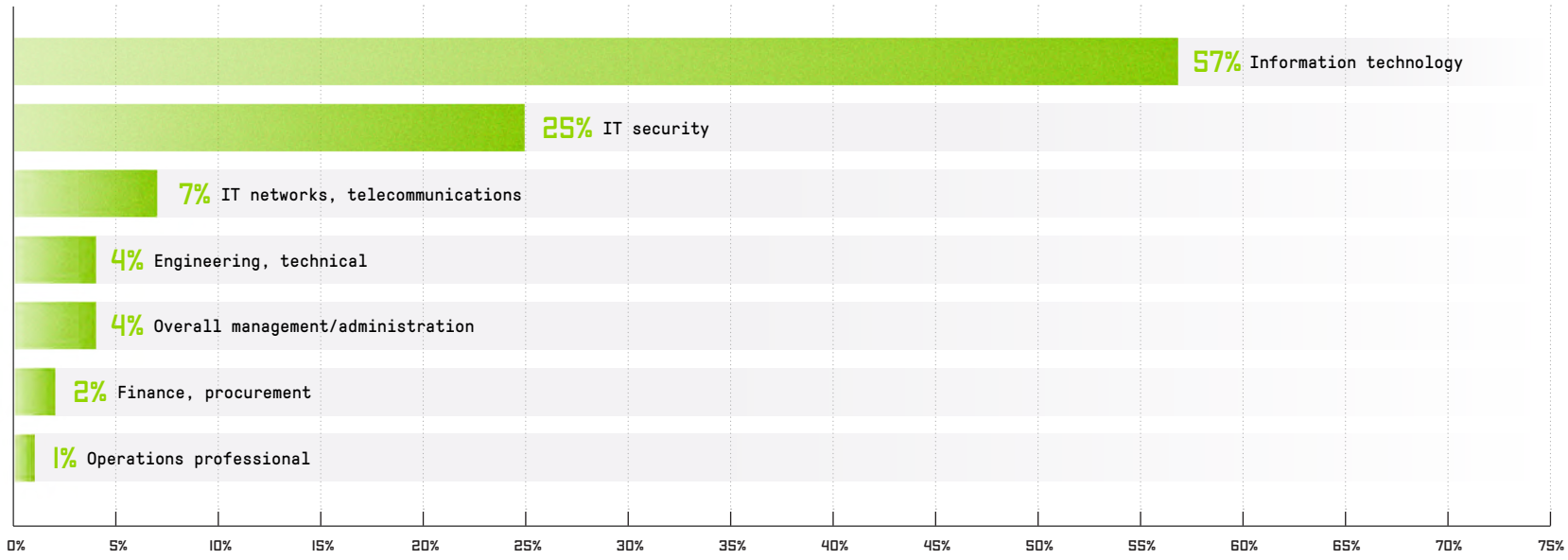
FIGURE 3

VERTICAL SECTORS REPRESENTED

Finance, Insurance, Real Estate 17%	Transportation, Energy, Utilities 12%	Retail, Wholesale 11%	Professional, Other Services 11%	Construction, Natural Resources 10%
Manufacturing 10%	Telecom, ISPs 8%	Government 7%	IT-Related 6%	Education 4%	Healthcare 4%

FIGURE 4

FUNCTIONAL ROLES



ENTERPRISE THREATS

After a series of high-profile ransomware campaigns (WannaCry, Petya, and Bad Rabbit) in 2017, DDoS returned as the top threat experienced by 39 percent of enterprise organizations in 2018 (Figure 5). This number increased to 42 percent for companies with more than 1,000 employees. Meanwhile, more than 30 percent of respondents reported ransomware attacks within the last 12 months, similar to 2017.

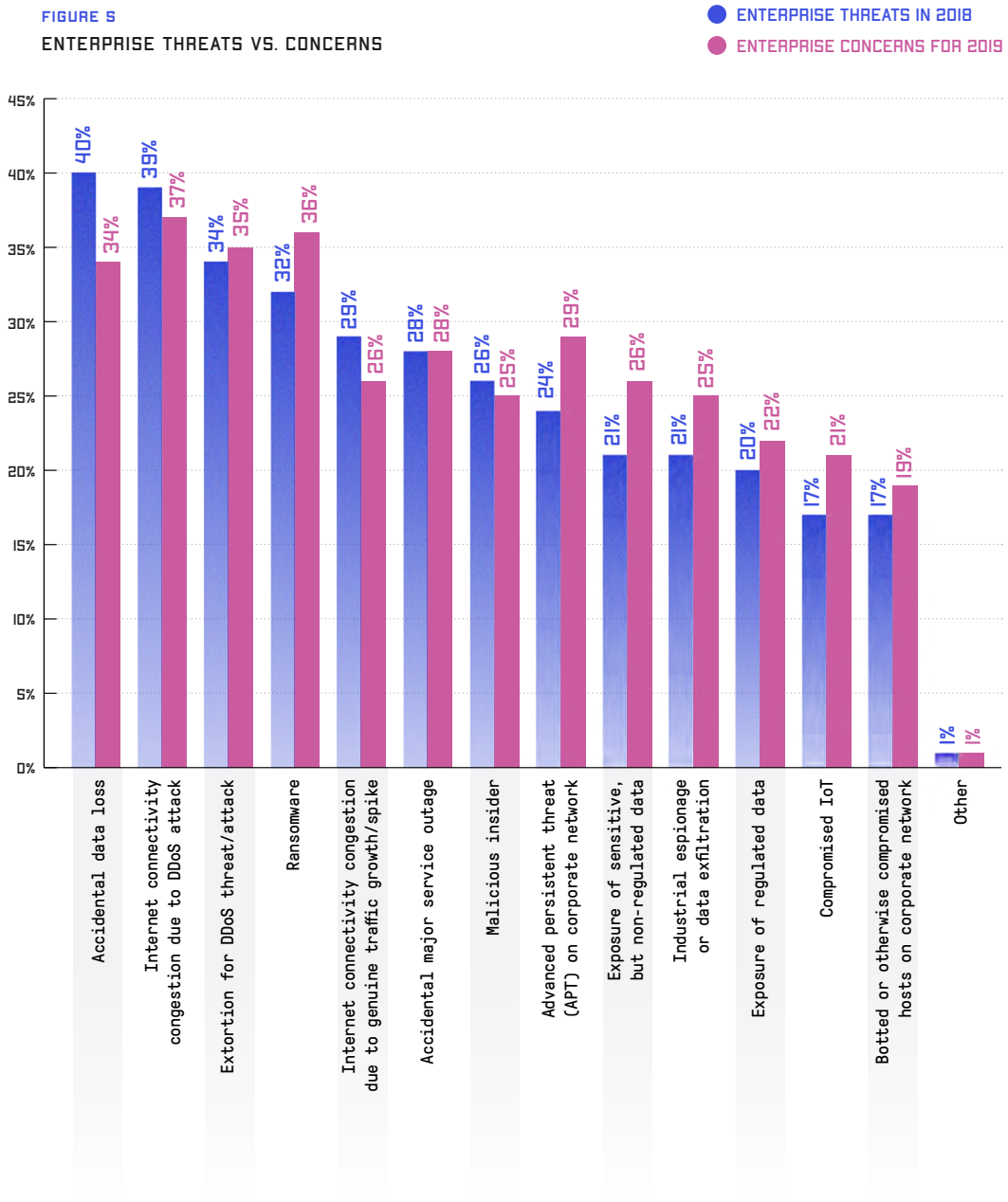
Enterprises also reported a significant increase in extortion for DDoS threat/attacks, which represents a major change in the threat landscape. Reported attacks in this category jumped from sixth place to third, doubling from 17 percent in 2017 to 34 percent in 2018. Today, enterprises suffer from DDoS extortion threats as much as actual DDoS attacks, a trend that we attribute to the maturity and rapid proliferation of DDoS-for-hire services.

DDoS also reclaimed the top spot as the main concern for 2019, followed by ransomware (Figure 5). Both threats are top of mind for more than 36 percent of enterprises, followed by extortion and accidental data loss. Not surprisingly, these concerns precisely mirror the top four threats experienced by more than 30 percent of enterprises in 2018.

Both accidental data loss and ransomware threats scored very high with our European respondents, which could be explained by the wave of ransomware attacks that prominently targeted this region. The implementation of the General Data Protection Regulation (GDPR) may also be a factor, with the emphasis on the protection of personal data and privacy within the European Union.

FIGURE 5

ENTERPRISE THREATS VS. CONCERNS



For the fourth consecutive year, SIEM platforms, firewalls, and IPS/IDS were the top three tools used to detect threats on enterprise networks in 2018 (Figure 6). The use of IDMS increased significantly to 44 percent, reaching parity with firewalls and IPS/IDS. This is a trend that we hope will continue, as stateful security devices are vulnerable to state-exhaustion attacks.

Behavioral analytics and threat intelligence platforms were used by over a third of all enterprises, followed closely by NetFlow-based analyzers. With SNMP-based tools and customer calls/help desk tickets relegated to the bottom of the table, this clearly shows that threat visibility has regained significant traction for enterprise respondents compared to 2017.

LIKE IN 2017, FIREWALLS AND IPS/IDS ARE CONSIDERED TRULY EFFECTIVE AT THREAT DETECTION BY 51 PERCENT IN 2018 (FIGURE 6). IDMS WERE IN SECOND PLACE AT 50 PERCENT, FOLLOWED CLOSELY BY THREAT INTELLIGENCE PLATFORMS.

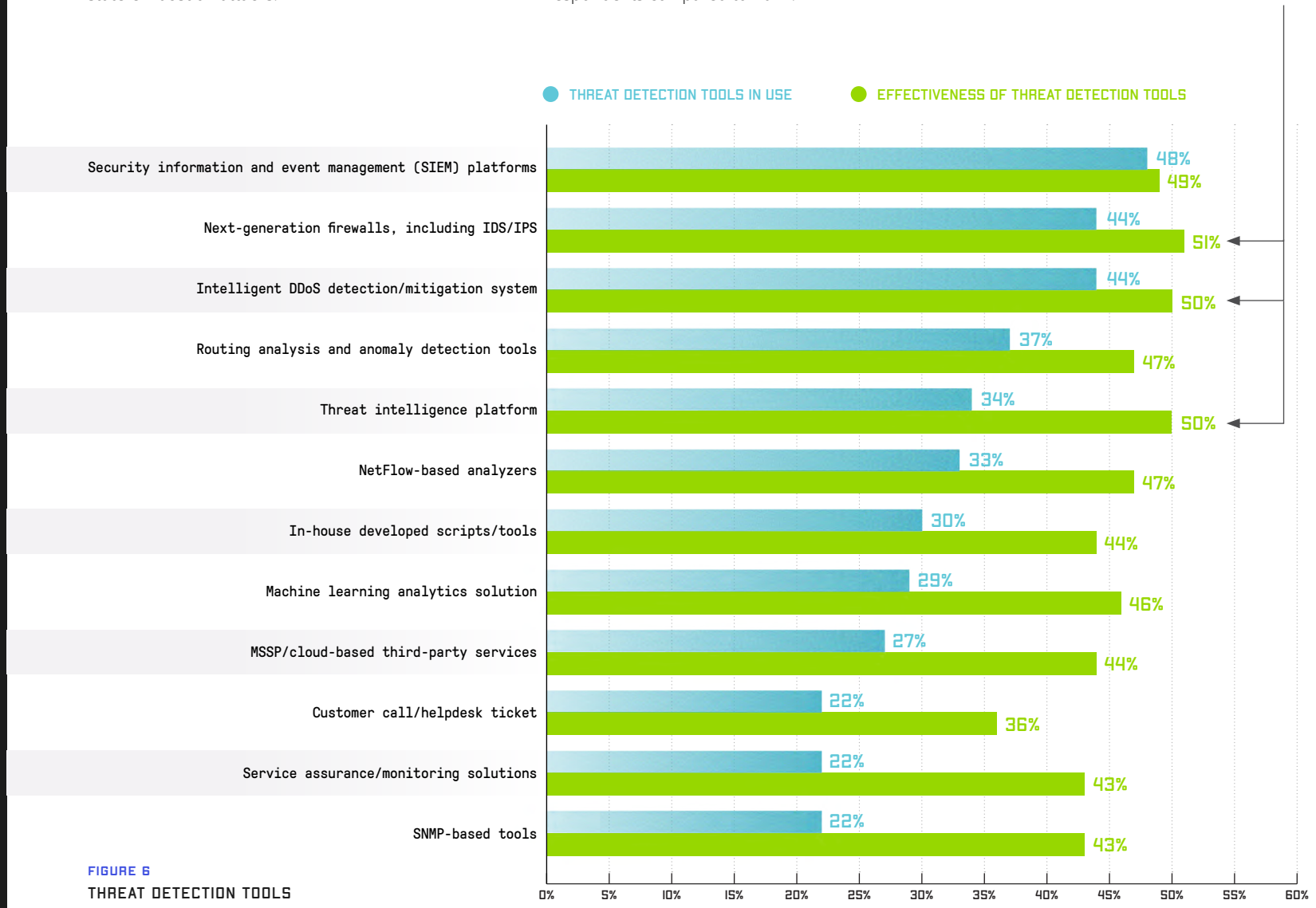


FIGURE 6
THREAT DETECTION TOOLS

More than half of the respondents relied on detecting compromised devices to monitor outbound threats or intra-data center traffic, while 36 percent used baselining (Figure 7). While those percentages were relatively consistent across all geographies, the numbers were reversed in Japan, where half of the enterprises rely on baselining, with compromised devices detection at 39 percent.

We asked our enterprise survey respondents if they used the same tools for outbound traffic monitoring as they use for inbound. They listed the same exact tools in the same order, with the exception of IDMS, which took the second place in front of firewalls and IDS/IPS for outbound traffic monitoring (Figure 8). As enterprises grow more concerned about compromised devices from their own network participating in DDoS campaigns, IDMS are now also being used to monitor traffic for outbound threats, which is a positive trend.

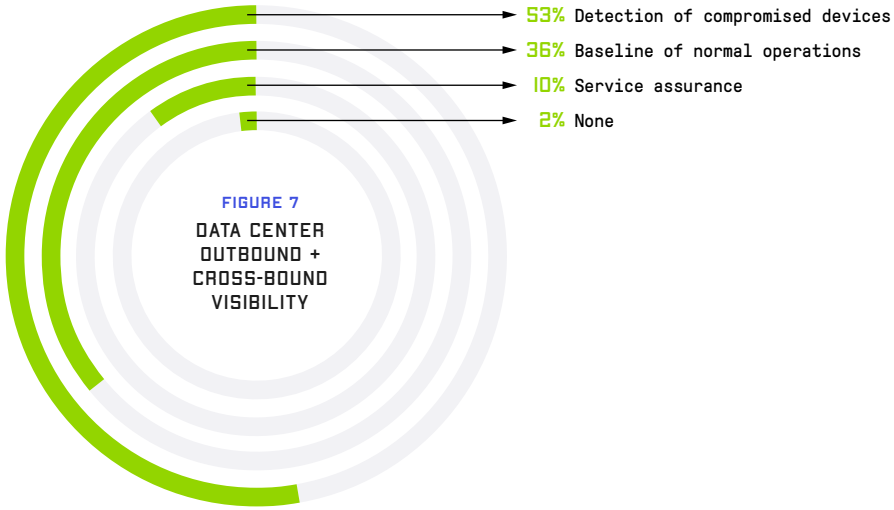


FIGURE 7

DATA CENTER OUTBOUND + CROSS-BOUND VISIBILITY

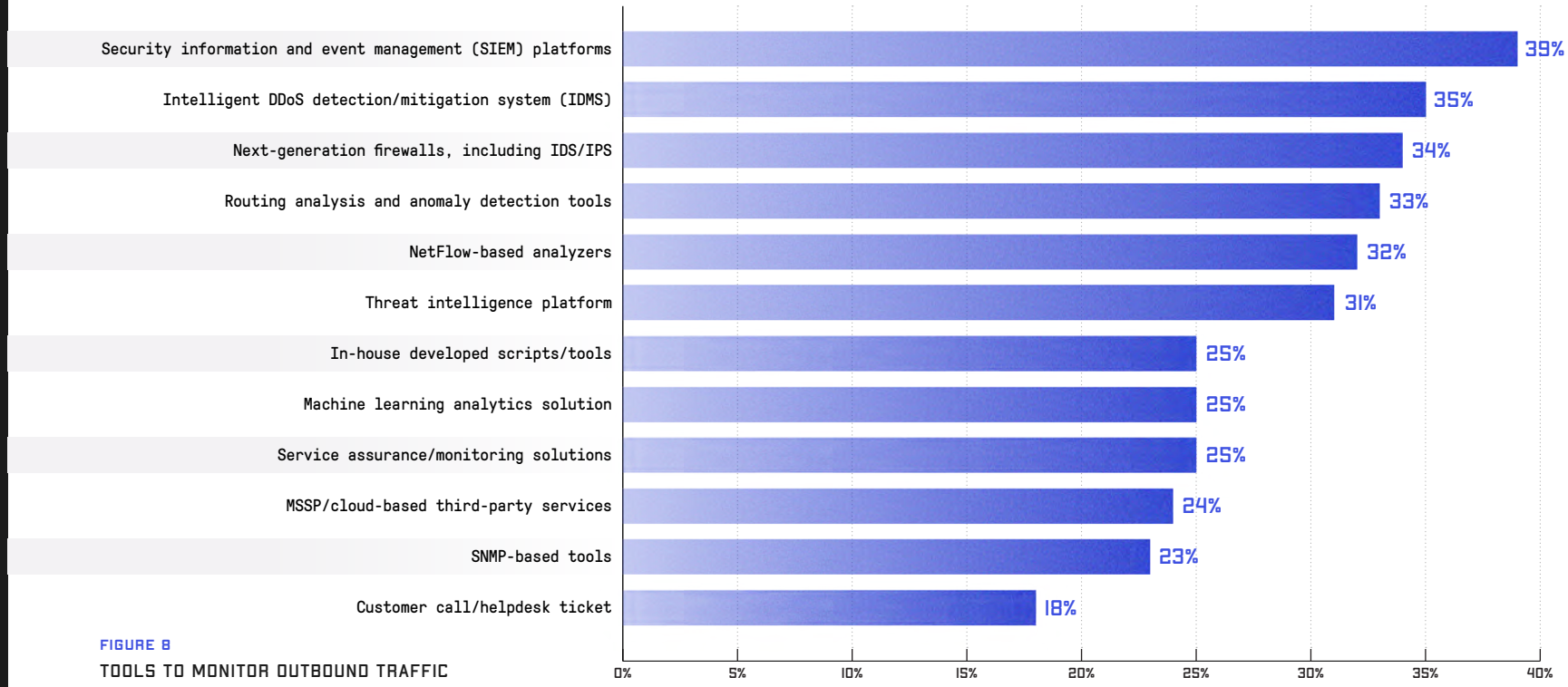


FIGURE 8

TOOLS TO MONITOR OUTBOUND TRAFFIC

Firewalls were still the number one security device deployed by nearly two-thirds of our enterprise respondents, followed by IDMS and IPS/IDS (Figure 9). This was generally the same for all regions, although sandboxing systems and UTM were in the top half for France and Japan.

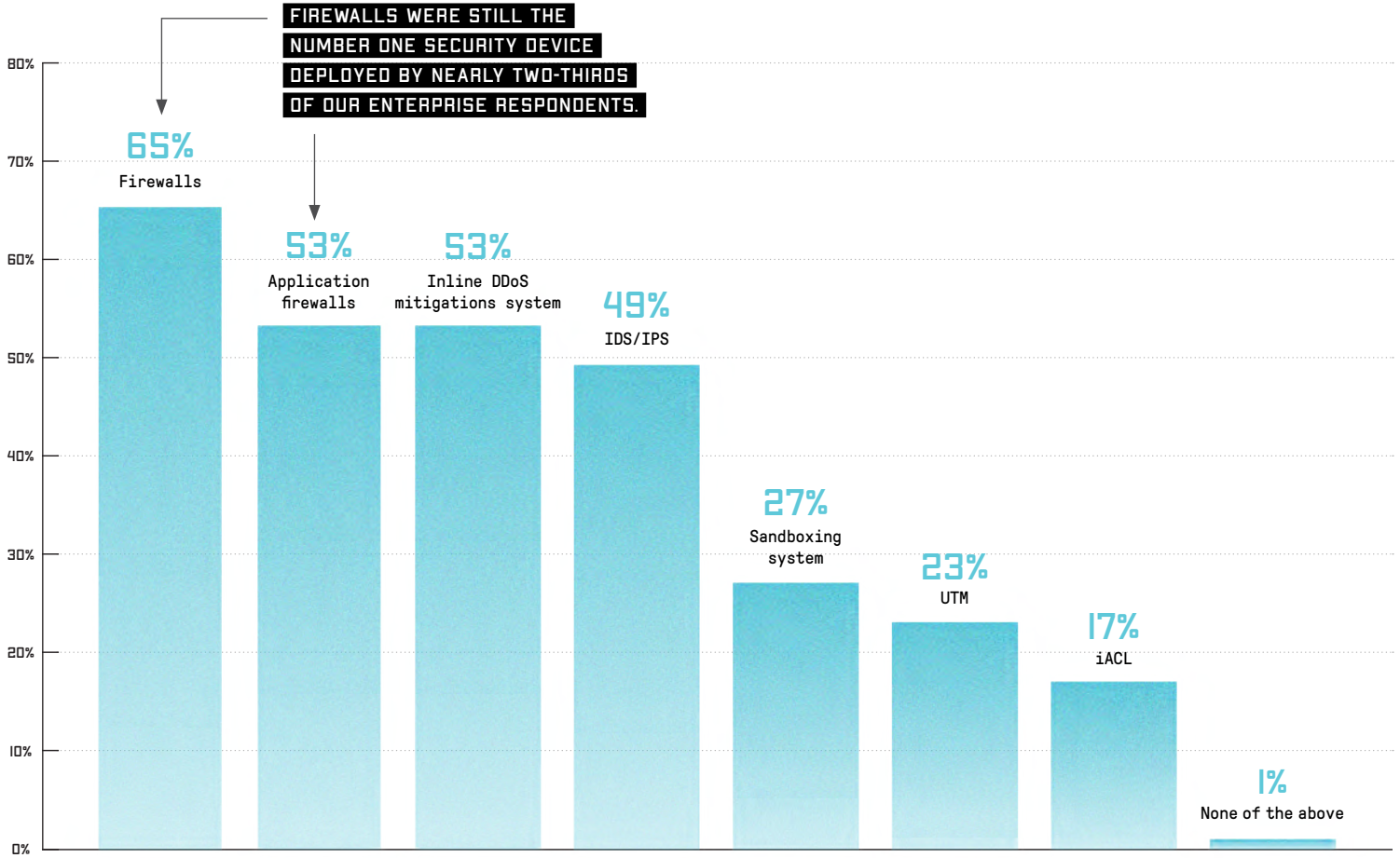


FIGURE 9

SECURITY TECHNIQUES DEPLOYED

ENTERPRISE DDoS ATTACK TRENDS

DDoS attacks are a fact of life for the modern enterprise, as 64 percent of respondents reported between one to ten attacks in 2018, consistent with previous years.

However, defending those attacks remains a moving target. Attackers are smart and efficient, and constantly evolve attack targets and techniques to exploit new vulnerabilities in increasingly complex—and business-critical—IT infrastructures. Attackers are adept at spotting and responding to new IT investments and security deployments.

CONSIDER THE FOLLOWING:

- As enterprise organizations invested in cloud-based DDoS mitigation services, attackers shifted to focus on stateful infrastructures. In 2018, attacks targeting firewalls and IPS devices almost doubled, from 16 percent in 2017 to 31 percent.
- Important elements of digital transformation strategies are now under attack. In 2018, there was a threefold increase in the number of attacks against SaaS services (from 13 percent in 2017 to 41 percent) as well as against third-party data centers and cloud services (from 11 percent to 34 percent).
- The increasing use of encrypted traffic was reflected in the growing rate of attacks. In 2018, 94 percent observed such attacks, nearly twice the percentage as the previous year.

Unfortunately, we observed a growing number of respondents who experienced DDoS attack saturating their internet bandwidth (Figure 10). This year 91 percent of enterprises who experienced a DDoS attack indicated that one or more of them completely saturated their internet bandwidth. In addition, 25 percent reported that more than half of DDoS attacks they experienced exceeded their internet bandwidth. This disappointing statistic indicates volumetric DDoS attacks, especially reflection/amplification, are a continuing challenge. Further, new vectors such as Memcached reflection and SSDP diffraction enhanced the arsenal of attackers in 2018.

DDoS remains the number one threat to the availability of business networks, applications, and services. The consistency of the threat, combined with the diversity of targets and attack types, requires a new approach. Deploying a best practice, multi-layered defense that integrates cloud-based protection from volumetric attacks and on-premises protection against state-exhaustion and application-layer attacks is now an essential component of any security strategy.

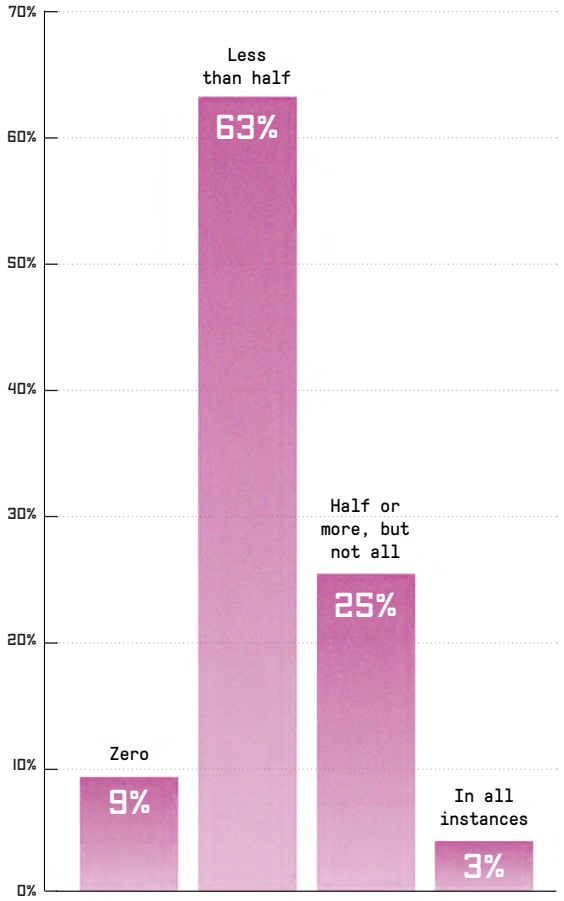


FIGURE 10

DDoS ATTACKS EXCEEDING INTERNET BANDWIDTH

FIGURE 11

DDoS ATTACK TARGETS

49%
Infrastructure

41%
SaaS services

38%
Customer-facing services and applications on your network

34%
Third-party data center or cloud service

Attackers continue to target infrastructure and customer-facing services and applications most frequently (Figure 11). What caught our attention in the 2018 results was the threefold increase in attacks against SaaS services (from 13 in 2017 to 41 percent) and third-party data centers and cloud services (from 11 to 34 percent). This indicates the ever-increasing role of cloud services in modern enterprises and again highlights the need for a cohesive DDoS detection and mitigation strategy.

Once more in 2018, more than half of the respondents reported firewalls and IPS devices that failed or contributed to an outage during a DDoS attack (Figure 12). It is important to remember that while these devices play a useful role, they are especially vulnerable to state-exhaustion attacks.

Looking at the duration of DDoS attacks, around 60 percent of DDoS incidents lasted less than six hours (Figure 13). The most typical cases, in more than half of all incidents, were ones lasting between five minutes and six hours. With this in mind, it is important to have a well-thought out DDoS incident response and mitigation workflow plan in place in order to appropriately and quickly address attacks of this duration. On the other side of the duration spectrum are attacks lasting one week and longer. Consistent with our findings in 2017, these attacks are very rare and accounted for less than two percent of the total number of attacks in 2018.

FIGURE 12

FIREWALL + IPS FAILURE

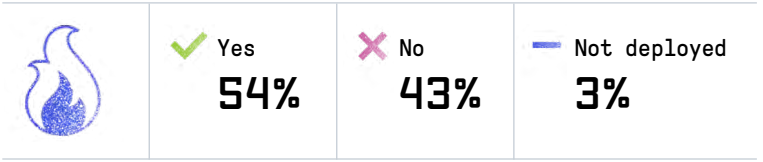


FIGURE 13

DDoS ATTACK DURATION

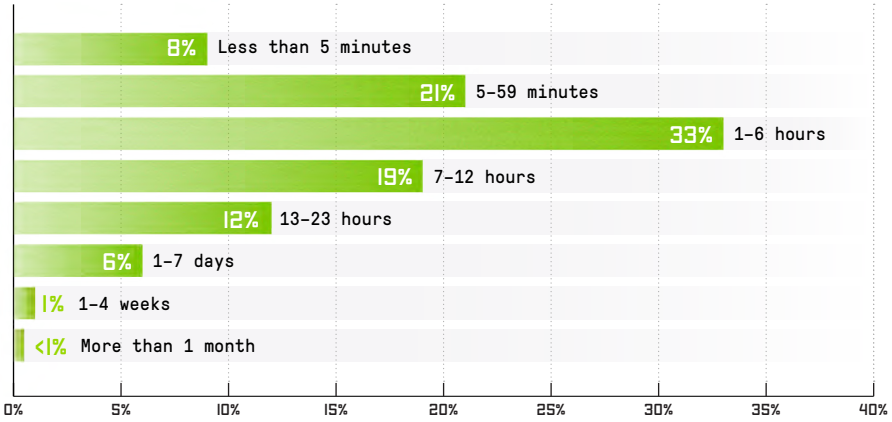
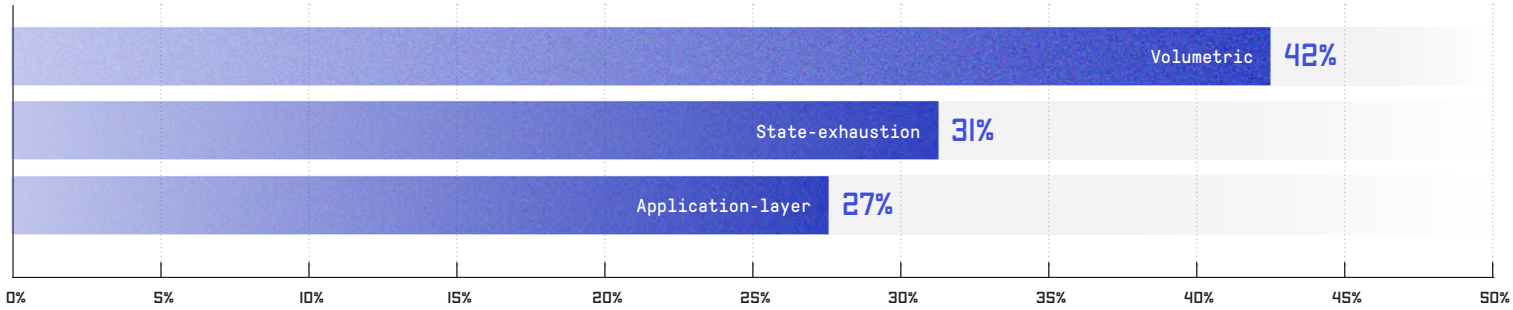


FIGURE 14

DDoS ATTACK TYPES



For the third consecutive year, our enterprise respondents observed a decrease in volumetric attacks, from 60 percent in 2016, to 52 percent in 2017, and to 42 percent in 2018 (Figure 14). In the whack-a-mole world of cybersecurity, we saw a corresponding increase in the number of state-exhaustion attacks, with an increase that almost doubled from 16 percent in 2016 to 31 percent in 2018.

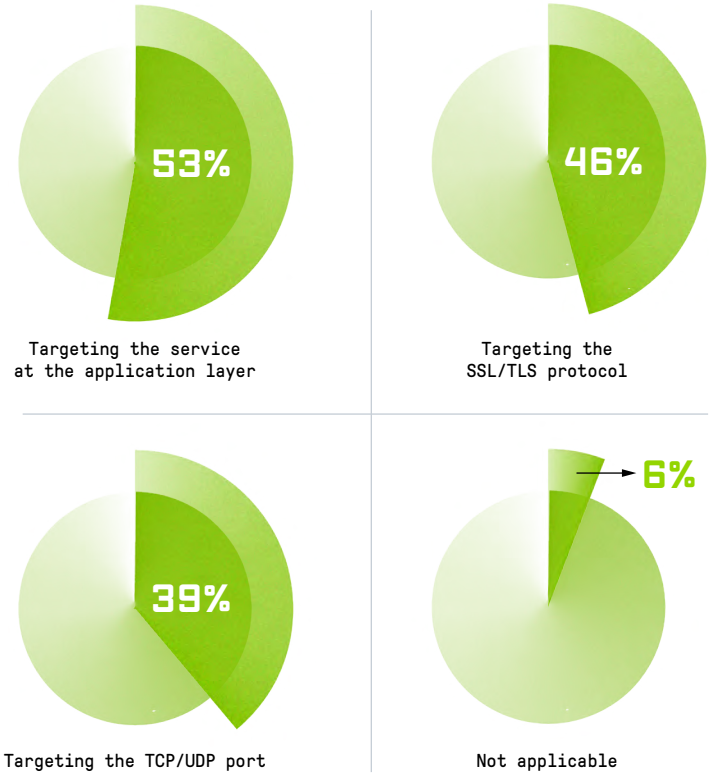
CLEARLY, THERE IS AN ONGOING SHIFT IN THE BEHAVIOR OF ATTACKERS THAT WE HAVE BEEN OBSERVING FOR THE PAST THREE YEARS.

As threat actors realize the increasing difficulty of passing through a volumetric protection layer, they try to reach their goals with stealthier attacks that target either a stateful infrastructure or the applications within the infrastructure.

The increasing global rate of encrypted traffic is reflected in the growing rate of attacks that target encrypted services (Figure 15). In 2018, 94 percent observed such attacks, nearly twice the percentage as the previous year. Attackers often climb the OSI model ladder to try to bring encrypted resources down, targeting either the SSL/TLS protocol or the application layer.

FIGURE 15

DDoS ATTACKS TARGETING ENCRYPTED SERVICES



When it comes to multi-vector DDoS attacks that leverage some combination of volumetric, stateful, and application-layer vectors, the news from 2018 was mixed.

The percentage that observed multi-vector attacks grew significantly, from 48 percent in 2017 to 67 percent, which at first glance seems to be a scary trend (Figure 16). However, at the same time, the proportion that struggled to provide a definitive response dropped from 20 percent in 2017 down to 3 percent in 2018. We believe this is due to improved visibility and detection capabilities, which is positive news.

Despite the observed increase of IPv6 traffic globally, less than a third experienced an IPv6 DDoS attack (Figure 17). Nevertheless, organizations should implement DDoS mitigation capabilities onsite and in the cloud services being used as part of any IPv6 deployment.

Beginning with the rise of Anonymous, DDoS attacks have undergone a transformation in the areas of tools, targets, and techniques. Thanks to old-fashioned software development, the technical barrier to entry for DDoS has been obliterated. Do-it-yourself tools now enable anyone to become an attacker, for any reason—permanently changing the attack landscape as a result.

DDoS ATTACKS ARE USED BY MANY DIFFERENT GROUPS OF THREAT ACTORS, FROM SOCIAL ACTIVISTS TO STATE ACTORS TRYING TO INFLUENCE GEOPOLITICAL PROCESSES. AS A RESULT, ORGANIZATIONS CAN BE TARGETED FOR ANY NUMBER OF REASONS, FROM CORPORATE POLICY TO CELEBRITY ASSOCIATIONS.

FIGURE 16

MULTI-VECTOR DDoS ATTACKS

Yes, in the last 12 months	36%
Yes, not in the last 12 months	31%
No	29%
Do not know	3%

FIGURE 17

IPV6-BASED DDoS ATTACKS IN THE LAST 12 MONTHS

Yes	30%
No	66%
Do not know	4%

By and large, however, most attacks are motivated by profits rather than organic protests. These days, DDoS attacks are often powered by professionally managed DDoS-for-hire services known as booters or stressers, which is reflected in the attack motivation findings. For example, the top motivation cited for attacks in 2018 was criminals showcasing their capabilities to potential customers, followed by criminal extortion attempts (Figure 19).

ONE FINDING THAT WAS PARTICULARLY INTERESTING WAS A TWO-FOLD INCREASE IN ATTACKS BEING USED IN A COMPETITIVE RIVALRY BETWEEN BUSINESSES.

FIGURE 18

DDoS ATTACK MOTIVATIONS

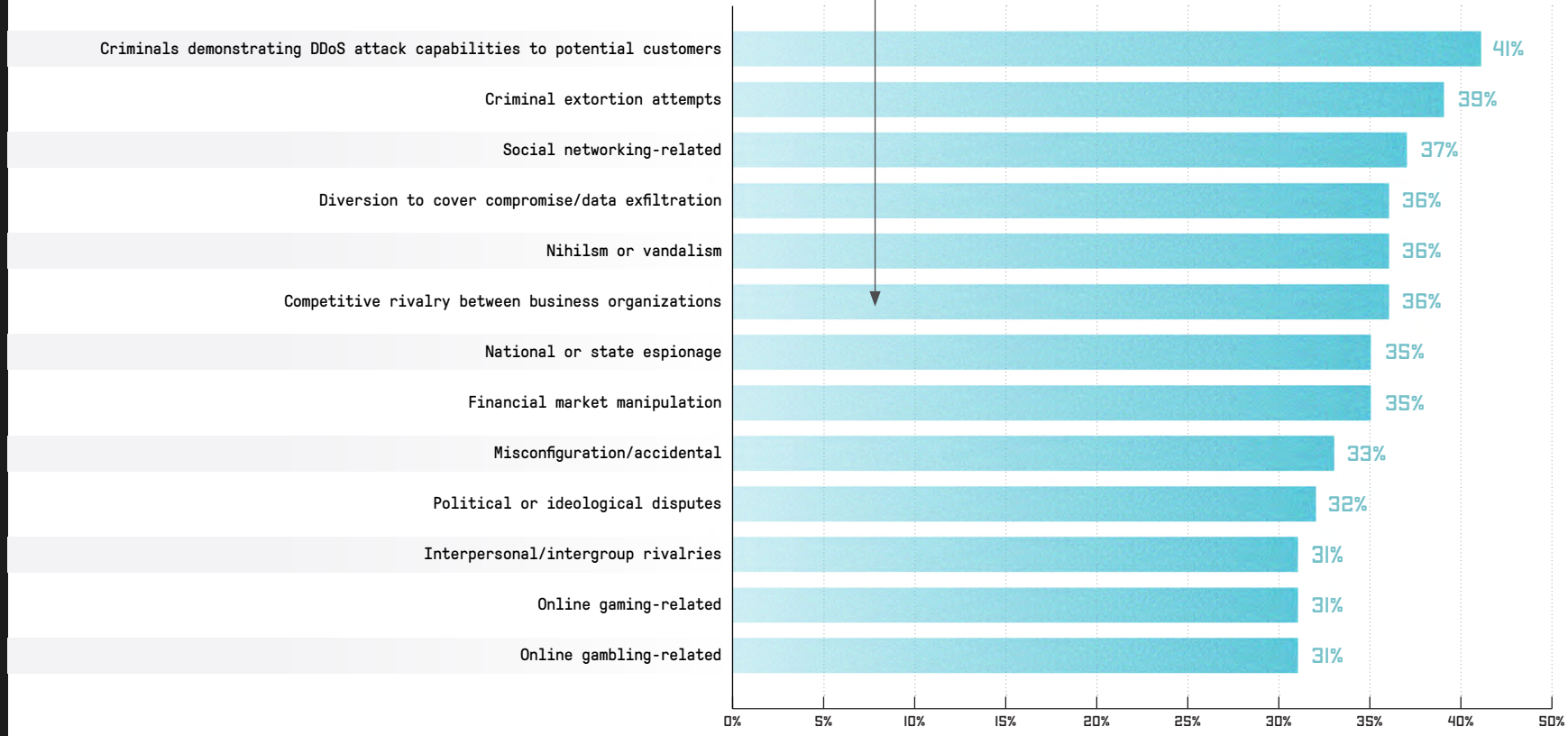
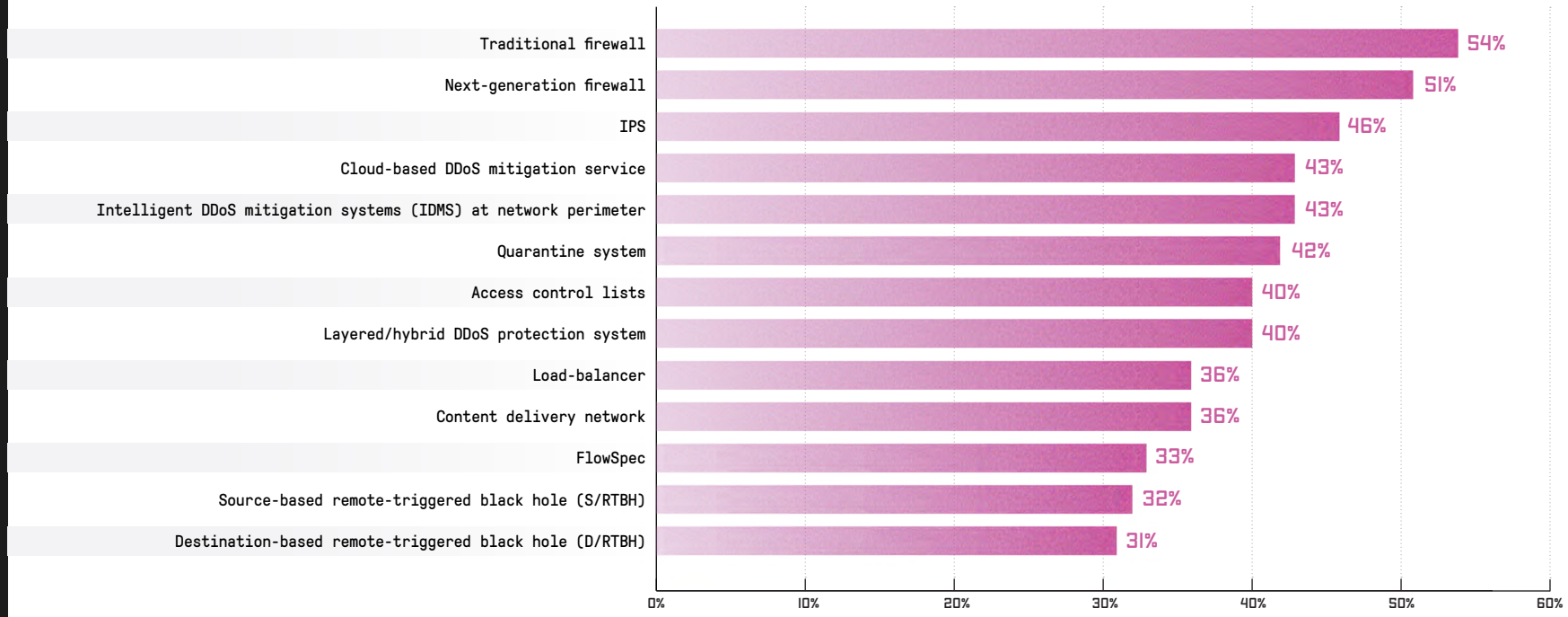


FIGURE 19

DDoS MITIGATION TECHNIQUES



When it comes to DDoS mitigation, there was a double dose of good news. First, we saw the broader adoption of specialized DDoS mitigation strategies, including cloud-based services and multi-layered solutions (Figure 19). More good news comes from the declining use of firewalls, IPS, and load-balancers for DDoS mitigation. This appears to be a lesson learned, as more than half reported that these devices contributed to a DDoS-related outage again in 2018. That correlates with the growing awareness within enterprise organizations regarding the impact DDoS attacks have on business activities.

Speed is a critical component of DDoS mitigation. We asked how quickly organizations detect and mitigate an attack, and more than half said within less than 15 minutes (Figure 20). Of those, approximately one quarter used on-premises devices or "always-on" managed services which result in immediate mitigation. On the other hand, the 16 percent that required more than one hour to mitigate an attack put their organization in a very risky position. By the time mitigation finally starts, the attack is very likely finished, or moved to a different vector.

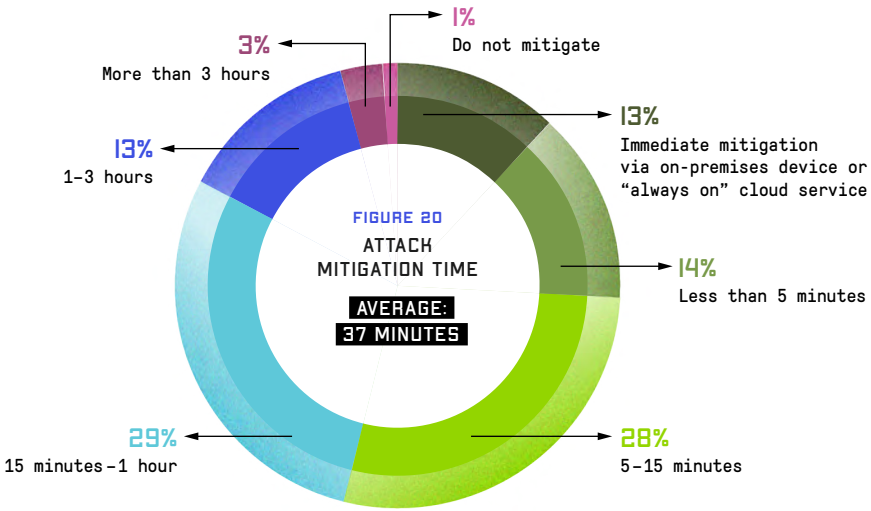


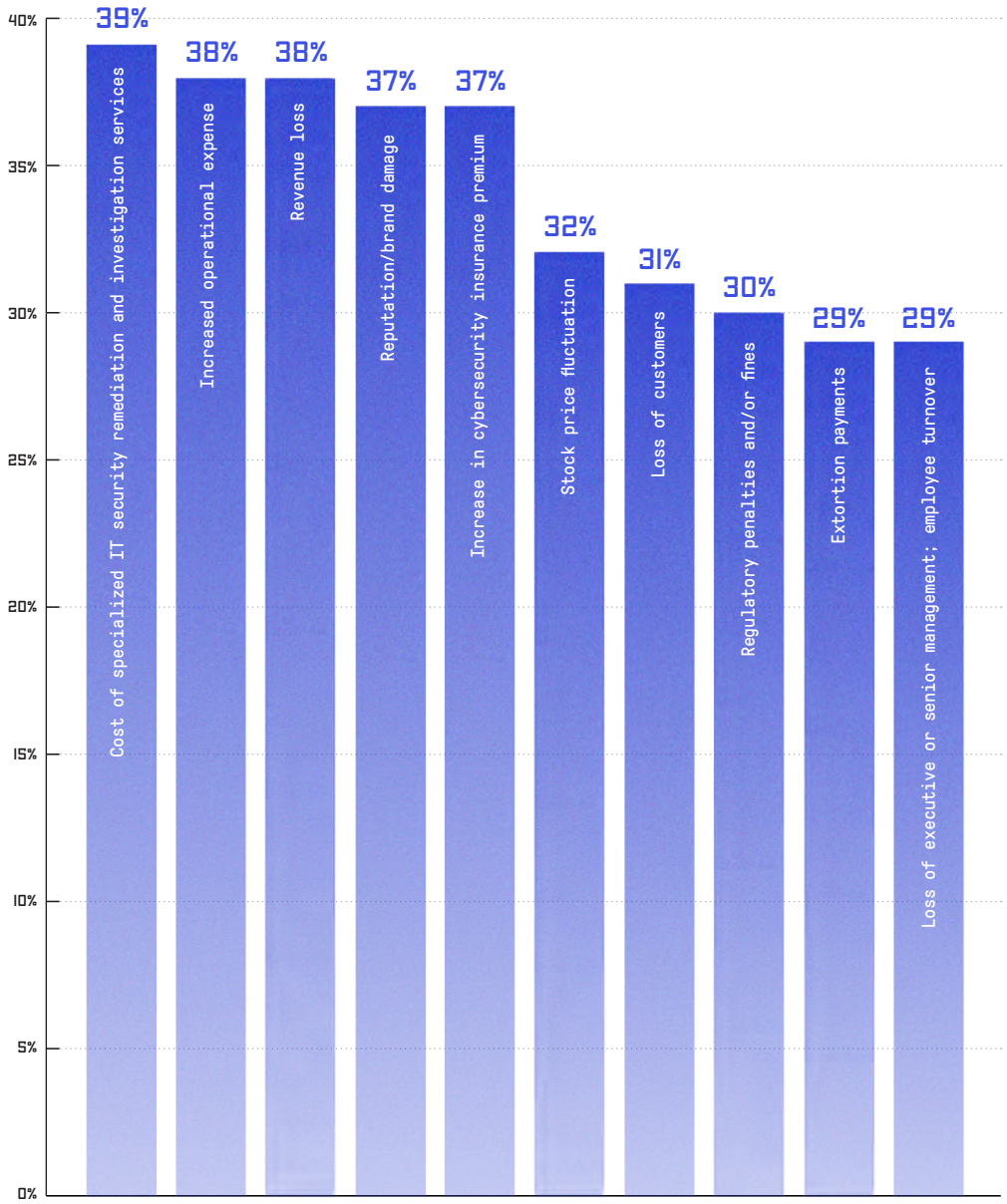
FIGURE 20

ATTACK MITIGATION TIME

AVERAGE: 37 MINUTES

FIGURE 21

BUSINESS IMPACTS OF DDoS ATTACKS



Business impacts due to DDoS attacks varied greatly in 2018. More respondents reported they observed very measurable attack consequences, such as the cost of specialized remediation and investigation services (39 percent), as well as increased OpEx and revenue loss (each at 38 percent) (Figure 21). Damage to reputation/brand and increased insurance premiums were reported by 37 percent.

We are delighted to see that more and more organizations assessed DDoS risks on a recurring basis, either as an IT or business risk. In 2018, only 11 percent mentioned they do not consider DDoS in their recurring risk analysis process, a significant improvement over the 23 percent reported in 2017 (Figure 22).

FIGURE 22

DDoS AS PART OF YOUR ORGANIZATION'S RISK ANALYSIS

Yes, part of IT risk assessment
50%

Yes, part of business risk assessment
39%

No
7%

Do not know
4%

Again in 2018, organizations reported increased per-minute and total costs associated with the outage of internet services. Almost half estimated a per-minute outage cost of between $1,000 and $10,000, instead of $0 to $1,000 as it was in 2017 (Figure 23). When it comes to overall attack cost, the stakes grew higher as well. In 2017, 55 percent estimated the average attack cost to be less than $10,000. In 2018, 53 percent saw the cost impact significantly higher, between $10,000 and $100,000 (Figure 24).

ENTERPRISES HAVE INVESTED IN DDoS DETECTION AND MITIGATION CAPABILITIES BOTH ON-PREMISE AND IN THE CLOUD, WITH A SPECIAL EMPHASIS ON PROTECTING THE AVAILABILITY OF THEIR SERVICES FOR END CUSTOMERS.

FIGURE 23
COST OF DOWNTIME

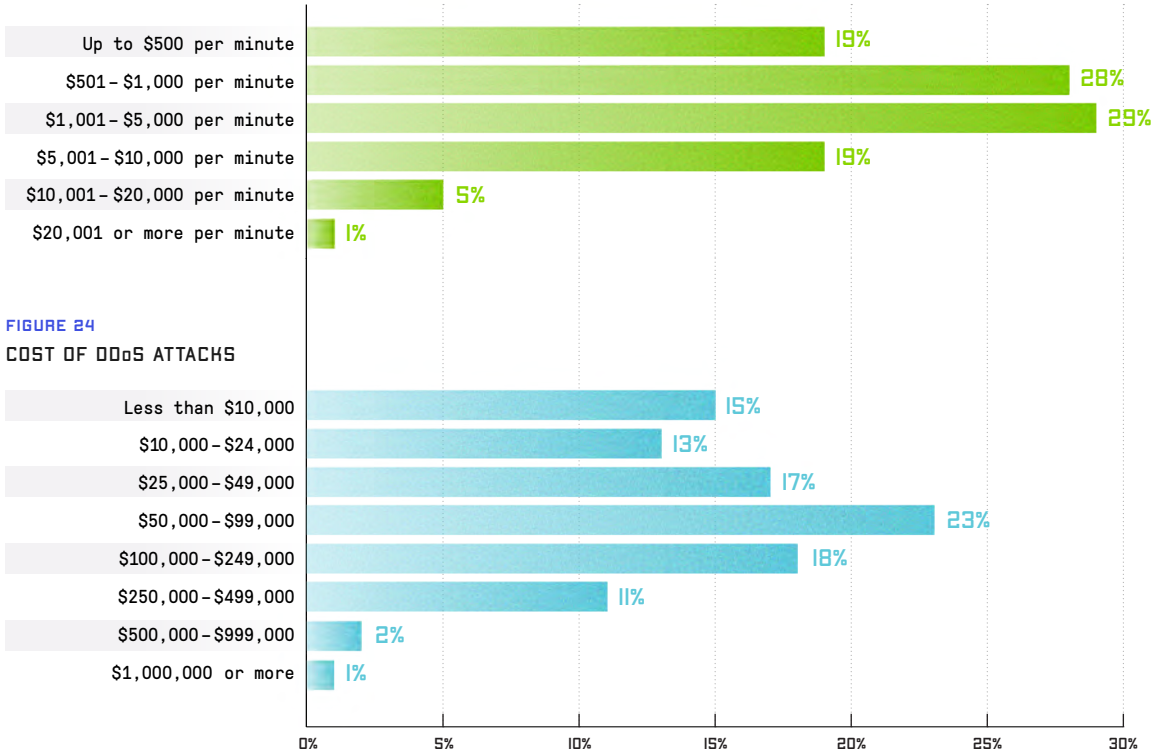
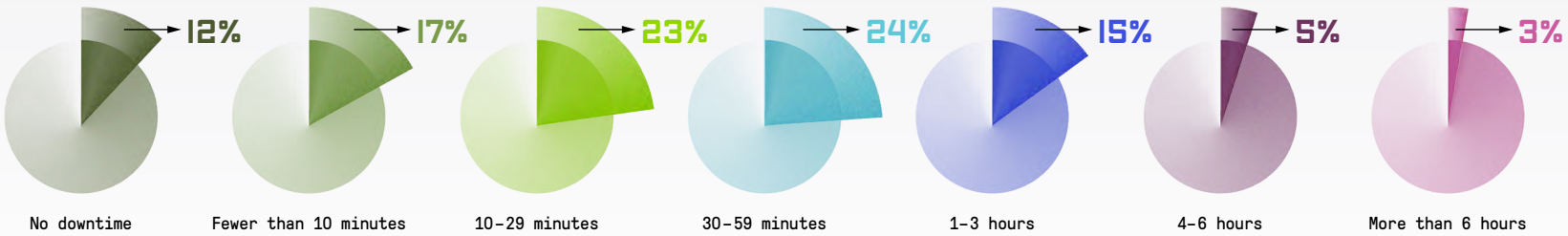


FIGURE 24
COST OF DDoS ATTACKS

FIGURE 25
TOTAL DOWNTIME



ENTERPRISE PUBLIC CLOUD MIGRATION

Enterprise adoption of public cloud offerings represents an ongoing journey, as companies move past early hype and adoption to wrestle with the often-painful challenges involved with major mainstream migration. Issues such as security and availability remain stubborn bottlenecks and are cited as key barriers that are indicative of why most organizations are not close to full adoption. The vast majority of respondents have at least some of their applications in the cloud already, and 11 percent have all their applications in a cloud-based environment. (Figure 26). However, there is still a long road ahead for the migration of in-house applications.

Despite the challenges, organizations remain hungry to move to public cloud environments. Sixty-two percent of the respondents plan to move some applications to public cloud services, while a further 18 percent say that they will move all of their applications to the public cloud (Figure 27).

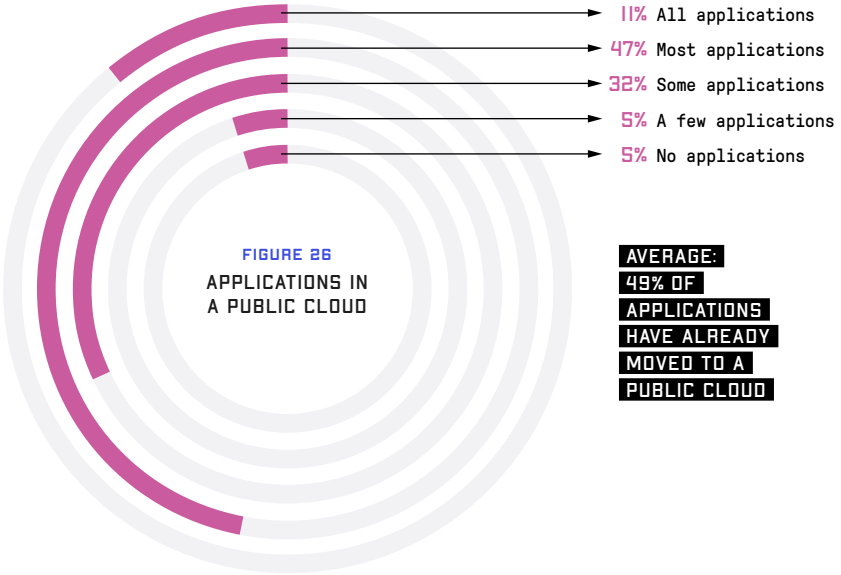
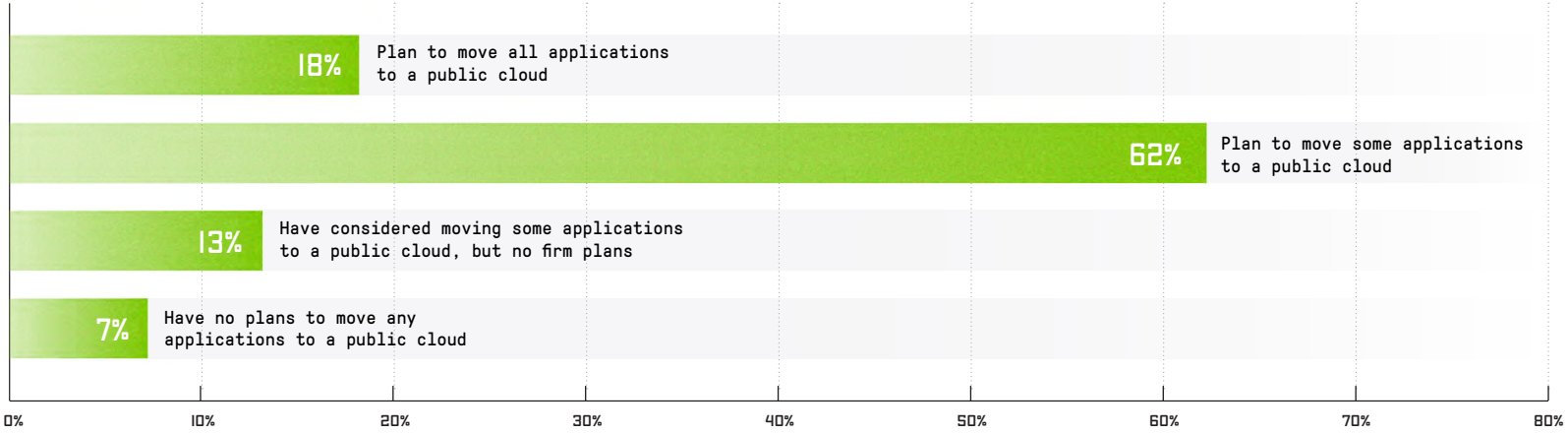


FIGURE 26
APPLICATIONS IN A PUBLIC CLOUD

AVERAGE: 49% OF APPLICATIONS HAVE ALREADY MOVED TO A PUBLIC CLOUD

FIGURE 27
PLANS TO MOVE APPLICATIONS TO A PUBLIC CLOUD

AVERAGE: 17% OF ORGANIZATIONS PLAN TO MOVE APPLICATIONS TO A PUBLIC CLOUD



While cost reduction and the ability to quickly deploy and scale applications continue to be strong drivers of cloud migration, the need for a disaster recovery system topped the list, as nearly 60 percent deemed it extremely or truly important (Figure 28). The ability to expand into new geographical regions and shift CapEx and personnel costs into OpEx round out the top five motivations as significant, but less important, drivers.

One interesting finding was in Europe, where disaster recovery was cited above cost reduction as the primary driver for nearly 60 percent of respondents. This could be related to Article 32 of the GDPR, which calls for "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident."

Security concerns remain a significant impediment to wholesale cloud migration for many, as 61 percent cited it as the top barrier (Figure 29). This tops the list by a margin of roughly 10 points, above stability and availability concerns, compliance or regulatory concerns, and cost. Surprisingly, cost is fourth on the list of concerns for about half of the enterprises, though it is also paradoxically one of the main drivers for moving applications to the cloud.

FIGURE 28

MOTIVATIONS FOR PUBLIC CLOUD MIGRATION

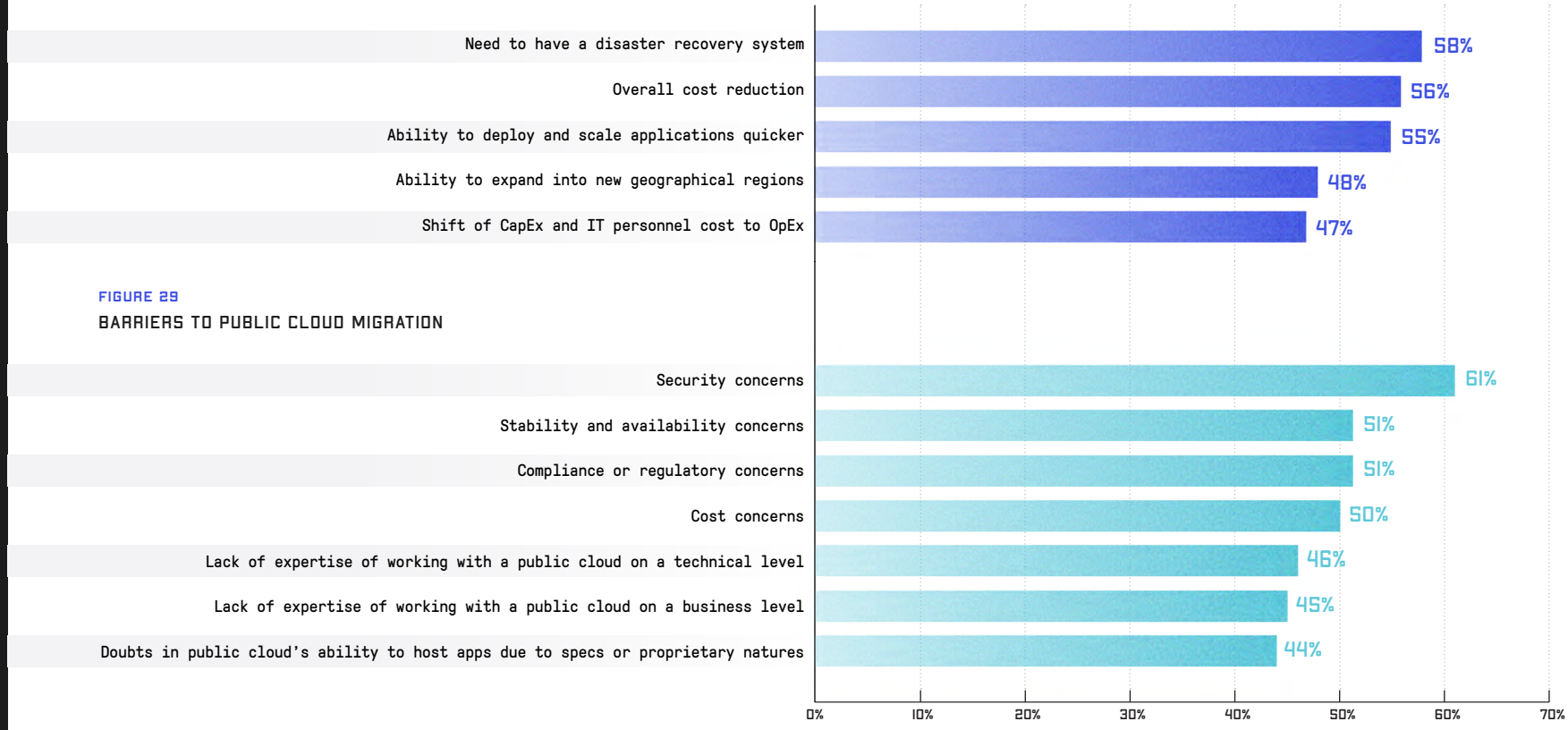


FIGURE 29

BARRIERS TO PUBLIC CLOUD MIGRATION

ENTERPRISE DNS

In 2018, we saw more companies outsourcing DNS operations. Only 37 percent said they operated their own DNS infrastructure, a significant drop from 2017 (Figure 30).

The majority of those that operate internal DNS infrastructures rely on their primary IT security teams to secure the service (Figure 31). Only 14 percent have specialized security for DNS. In 2017, an alarming 16 percent reported having no security team responsible for this critical infrastructure, but thankfully that decreased to only 2 percent in 2018.

Despite the progress cited above, DNS traffic visibility dropped as compared with the previous year, with 68 percent having visibility at Layers 3 and 4, down slightly from 73 percent in 2017 (Figure 32). At Layer 7, the picture is even worse, as only 25 percent reported visibility at that layer, a significant decrease from 49 percent in 2017. On a positive note, those reporting no visibility dropped to 7 percent, down from 11 percent in 2017. While the numbers at first appear grim, it is likely that the trend of outsourcing DNS operations is driving the change in visibility of DNS infrastructure.

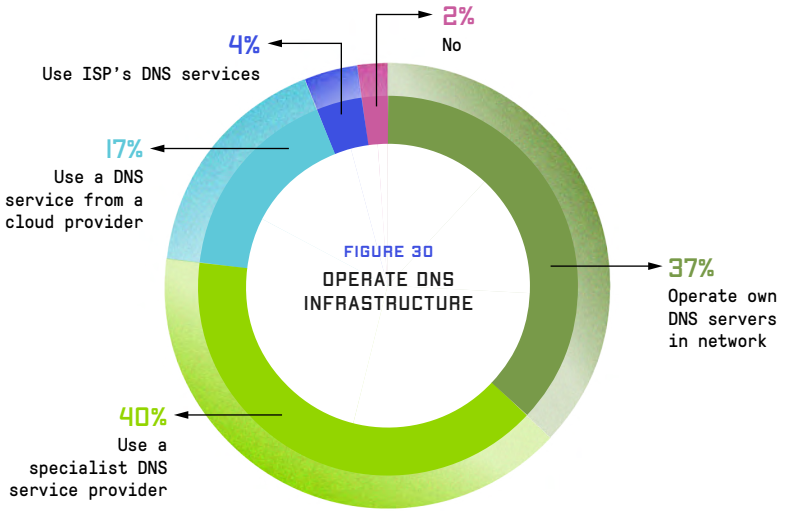


FIGURE 30
OPERATE DNS INFRASTRUCTURE

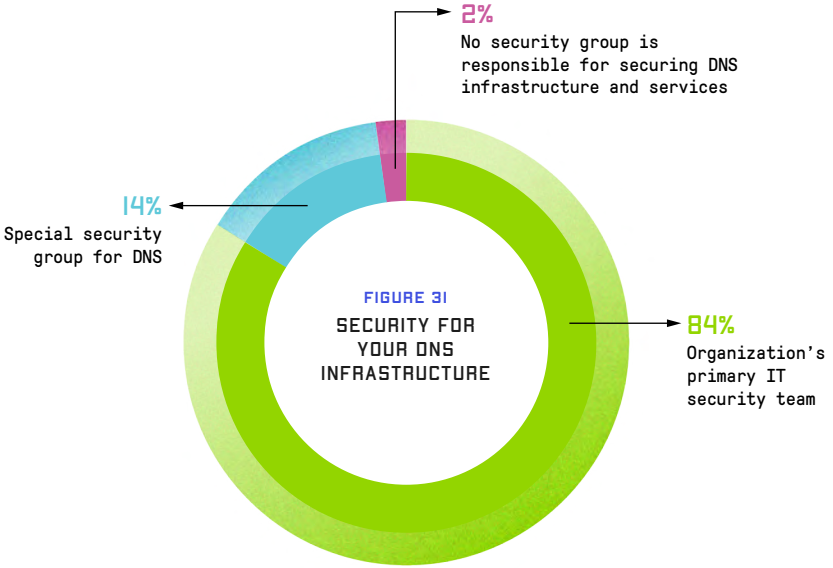


FIGURE 31
SECURITY FOR YOUR DNS INFRASTRUCTURE

FIGURE 32
VISIBILITY OF DNS INFRASTRUCTURE

7%	No visibility
68%	Visibility at Layers 3 + 4
25%	Visibility at Layer 7

When visibility becomes a challenge more successful attacks are expected, and the survey data confirms this expectation. The percentage that experienced publicly visible service outages increased dramatically to 55 percent, compared with 22 percent in 2017 and 13 percent in 2016 (Figure 33).

DDoS attacks are once again targeting authoritative DNS servers more frequently than recursive servers. In fact, those seeing attacks against authoritative servers more than doubled to 52 percent, up from 24 percent in 2017. The proportion seeing DDoS attacks targeting recursive DNS servers decreased again in 2018 to 21 percent, down from 32 percent in 2017.

As one would expect, companies deploy a variety of security measures to protect DNS infrastructures. Once again, firewalls were the most popular choice, but declining to 61 percent from about 80 percent the previous two years (Figure 34). While popular, seeing firewalls as the most reported option is disappointing, as these devices do not protect adequately against DDoS attacks due to the ease with which a state-based attack can overwhelm them.

The use of IDMS increased significantly to 41 percent, up from only 28 percent in 2017. Similarly, the use of FlowSpec increased from 12 percent in 2017 to 28 percent in 2018.

FIGURE 33

DNS INFRASTRUCTURE-RELATED DDoS ATTACKS

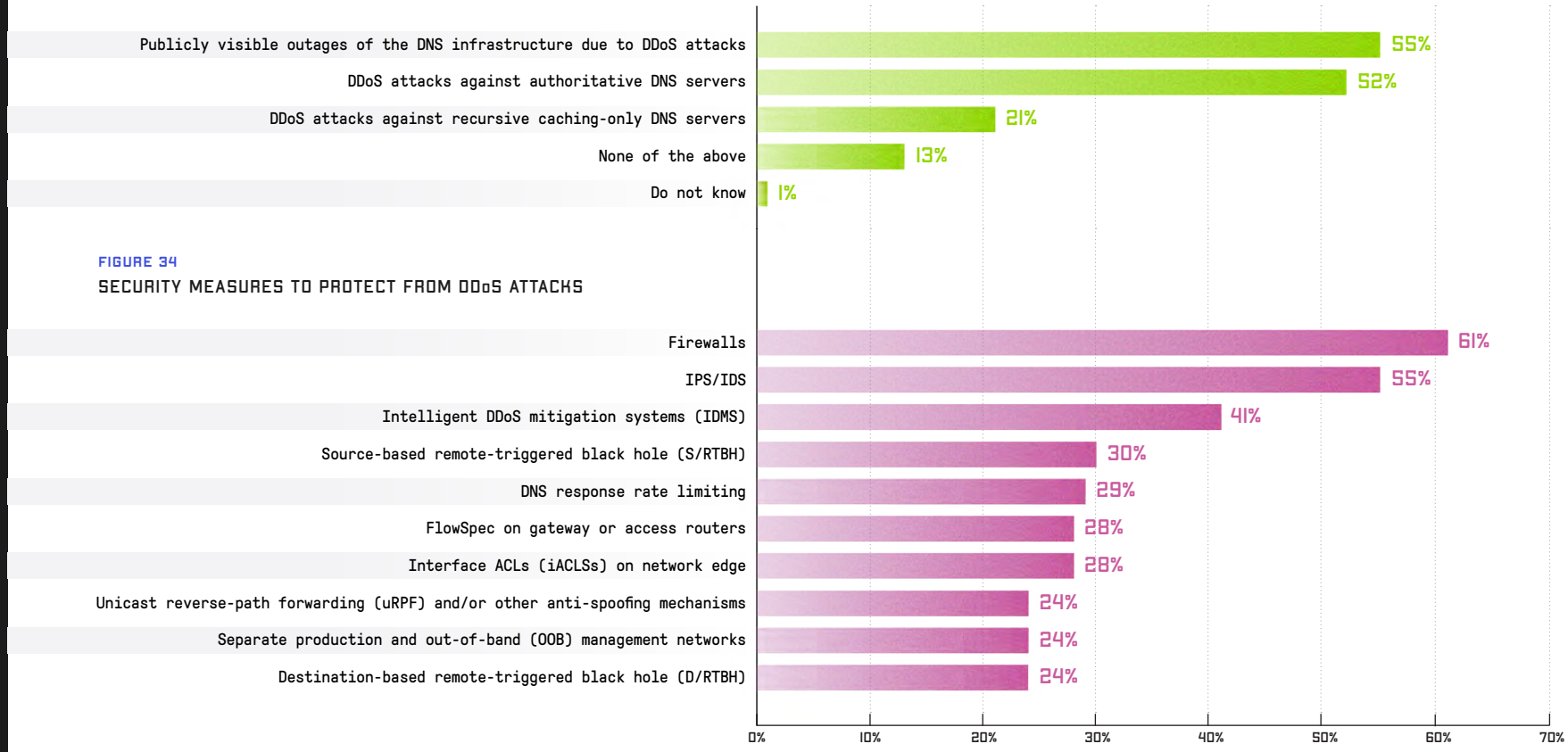


FIGURE 34

SECURITY MEASURES TO PROTECT FROM DDoS ATTACKS

ENTERPRISE ORGANIZATIONAL SECURITY PRACTICES

Similar to DNS infrastructure, we saw an increased reliance on outsourced services, in this case, the use of third-party security operations centers (SOCs). While 47 percent of enterprises have an internal SOC team, nearly one-third supplemented that with external SOCs, a significant increase from 21 percent in 2017 (Figure 35). This trend will likely continue, as 39 percent expect to increase third-party investments into their SOC in the next 12 months.

THIS ILLUSTRATES THAT THE PEOPLE AND SKILLS SHORTAGE IN THE SECURITY INDUSTRY IS AN ADVANCED AND PERSISTENT THREAT IN AND OF ITSELF. IT FURTHER STRESSES THE ONGOING CHALLENGE THAT ENTERPRISES FACE IN BUILDING AND MAINTAINING AN INTERNAL SECURITY TEAM OF SKILLED PRACTITIONERS.

Nearly 60 percent of enterprises say that their security team has 6 to 20 people, with an average of 13 people for about a quarter of the respondents (Figure 36).

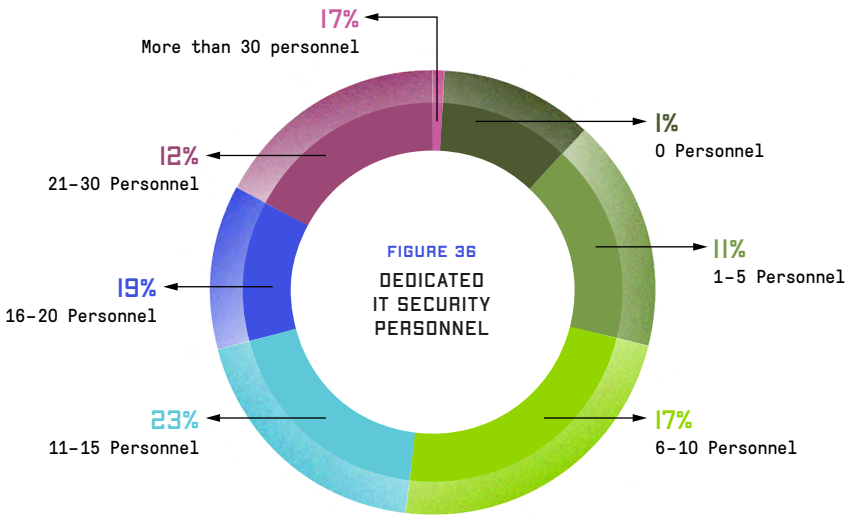


FIGURE 36
DEDICATED IT SECURITY PERSONNEL

FIGURE 35
SOC RESOURCES

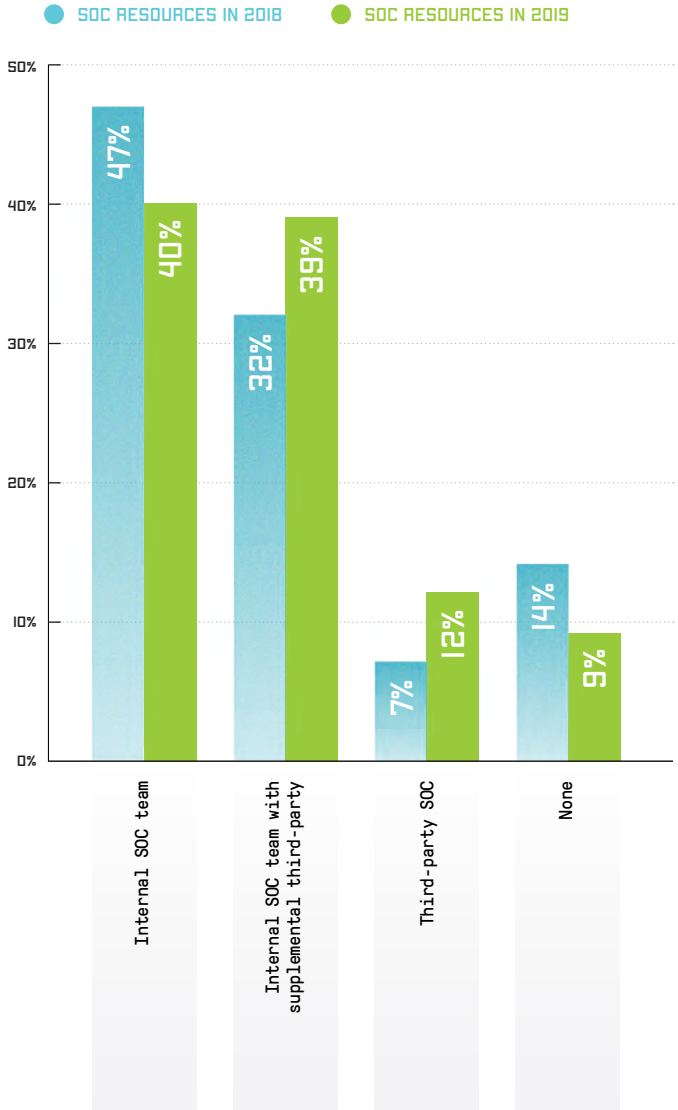
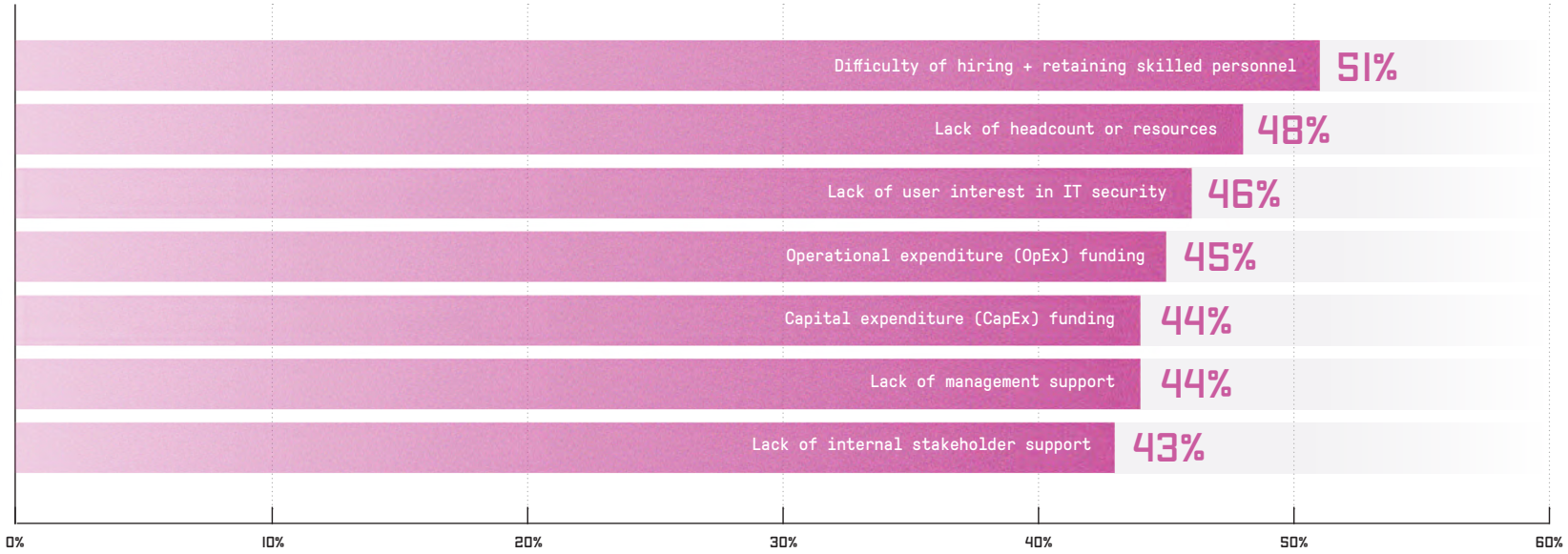


FIGURE 37

OPSEC CHALLENGES



Difficulty in hiring and retaining skilled personnel, along with lack of headcount or resources, were again the top two challenges faced by security leaders (Figure 37). The difficulty of hiring dropped slightly, from 54 percent in 2017 to 51 percent in 2018. However, all other challenges observed by enterprises seemed exacerbated in 2018, as they were reported by at least 43 percent of respondents as compared with 25 percent in 2017.

In 2018, we asked our enterprise responders to quantify the tools they use for their network and cyber security portfolios. Nearly half (46 percent) have at least 20 security solutions in their toolbox, while 11 percent report 40 or more tools. (Figure 38).

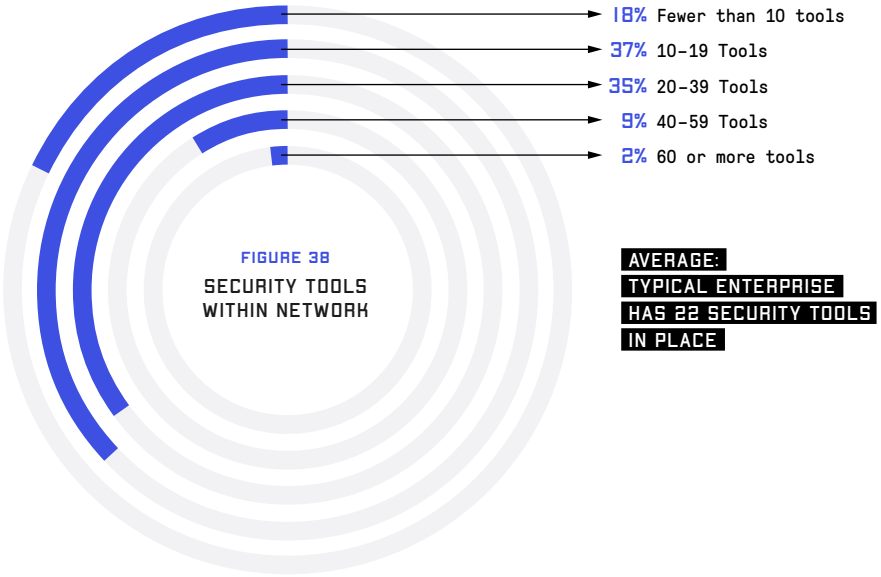


FIGURE 38

SECURITY TOOLS WITHIN NETWORK

AVERAGE: TYPICAL ENTERPRISE HAS 22 SECURITY TOOLS IN PLACE

WE FOUND A NEAR-UNIVERSAL DESIRE TO SIMPLIFY OPERATIONAL SECURITY PROCESSES.

Ninety-two percent said that they were looking to reduce complexity in some fashion, with the top priority being component and workflow integration (Figure 39). Threat Intelligence and security analytics were also important ways to improve decision making, cited by 38 percent and 37 percent, respectively.

Across the board, the proportion of enterprise respondents reporting adherence to best-practice security measures increased to an average of 48 percent, which is a great improvement over 2017 (Figure 40). Not surprisingly, blocking known botnets command-and-control was again on top of the list.

FIGURE 39

SIMPLIFY OPERATIONAL SECURITY PROCESSES

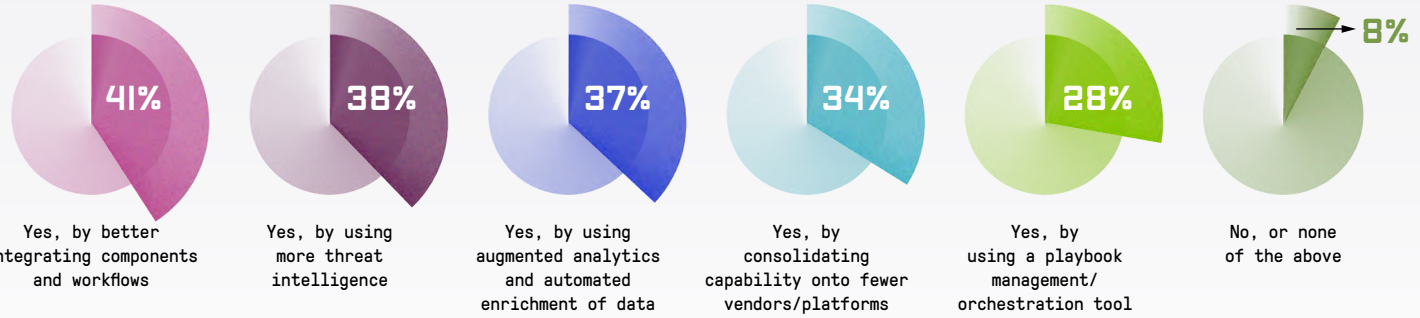
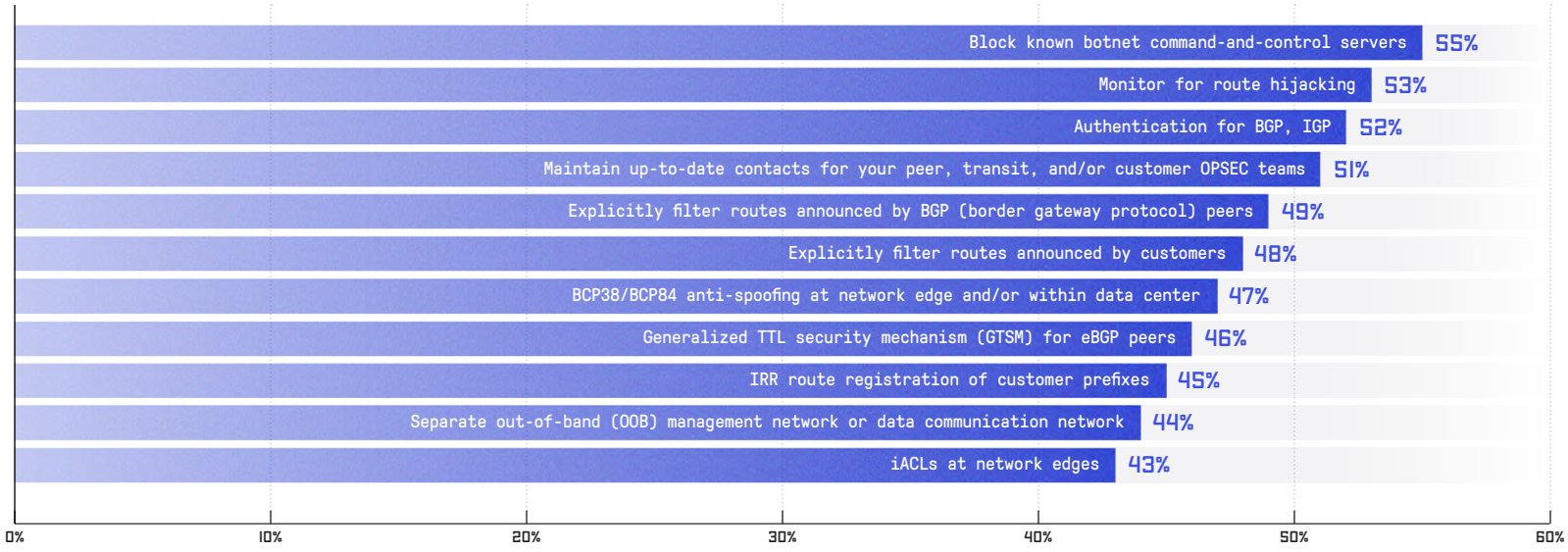


FIGURE 40

NETWORK INFRASTRUCTURE BEST PRACTICES

AVERAGE: 49% OF ORGANIZATIONS FOLLOW BEST PRACTICES



INSIGHTS BY COUNTRY

WE ALSO DUG INTO OUR ENTERPRISE SURVEY DATA FOR HIGHLIGHTS FROM SIX COUNTRIES, LOOKING FOR REGIONAL HIGHLIGHTS AND TRENDS. ATTACK TYPES, TARGETS, TECHNIQUES, MOTIVATIONS, IMPACTS, AND COSTS ARE ALL BROKEN OUT.


United States


Canada


Brazil


United Kingdom


Germany


France


Japan

KEY FINDINGS

We found some interesting variations in DDoS attack targets, techniques, and costs experienced in 2018.

ATTACK TECHNIQUES	GLOBAL AVERAGE	HIGHEST		LOWEST	
Accidental data loss	40%	United Kingdom	46%	US + Canada	36%
DDoS extortion	34%	Japan	40%	Germany	30%
Malicious insider	26%	France	37%	Japan	14%
Industrial espionage or data exfiltration	21%	France	35%	Japan	12%
Compromised IoT	17%	Brazil	25%	France	11%
Bandwidth-saturating DDoS attacks	39%	Japan	46%	France	32%
Firewall and/or IPS contributed to outage during a DDoS attack	54%	Brazil	76%	US + Canada	32%
ATTACK TARGETS					
Infrastructure	49%	Brazil	57%	France	44%
Customer-facing services/applications	38%	Brazil	46%	France	31%
SaaS service	41%	France	53%	Germany	33%
ATTACK TYPES					
Volumetric	42%	Japan	48%	Germany	39%
State exhaustion	31%	France	34%	Japan	28%
Application-layer	27%	Germany	30%	France	22%
Multi-layer	36%	Brazil	49%	Germany	26%

WORKFORCE CHALLENGES	GLOBAL AVERAGE	HIGHEST		LOWEST	
Size of dedicated IT security teams consistent across regions	19 People	Brazil	25	Germany	18
Hiring and retaining skilled employees cited as a major challenge	51%	Japan	57%	France	43%

TOOL PROLIFERATION

Use of security related tools	22 Tools	US + Canada	24	United Kingdom	21

When you hear about finding the signal through the noise, or alert fatigue, here's where it comes from. Globally, teams used an average of 22 security related tools and products within their cyber security portfolio in 2018—remember that was with teams ranging in size from 18–25 people. That number was very consistent with all regions reporting that they use more than 20 tools.

LOOKING FOR HELP

These teams are stretched thin, and at the same time, they're fighting to retain their best people. In 2018, they had as many tools per team as staffers. They're universally in search of a way to simplify operational processes. Only seven percent globally said they were not looking to do that.

COST OF DOWNTIME ASSOCIATED WITH DDoS ATTACKS IN 2018

Germany $351,995	United Kingdom $189,778
Brazil $306,081	France $174,834
US + Canada $218,339	Japan $123,026

US + CANADA

EXPERIENCED IN PAST 12 MONTHS	GLOBAL	US + CANADA
Accidental data loss	40%	▼ 37%
Internet connectivity congestion due to DDoS attack	39%	▼ 37%
Extortion for DDoS threat/attack	34%	► 34%
Ransomware	32%	▲ 34%
Internet connectivity congestion due to genuine traffic growth/spike	29%	▲ 36%
Accidental major service outage	28%	▼ 22%
Malicious insider	26%	▼ 20%
Advanced persistent threat (APT) on corporate network	24%	▲ 32%
Exposure of sensitive, but non-regulated data	21%	▲ 25%
Industrial espionage or data exfiltration	21%	▼ 17%
Exposure of regulated data	20%	▲ 22%
Compromised IoT	17%	▲ 20%
Botted or otherwise compromised hosts on corporate network	17%	▼ 12%

COMPROMISED IoT

Global Average: 17%

US + Canada: 20%

NO SOCS

The trend in the US and Canada is clear: fewer enterprises are operating their own SOCs and more are supplementing their SOC with third-party resources, making hybrid SOC the new direction. This is a reflection of the talent shortage in cyber security. It impacts both enterprise and service provider organizations.

OPERATE OWN SOC

Global Average: 47%

US + Canada: 41%

SUPPLEMENT SOC RESOURCES WITH THIRD-PARTY SUPPORT

Global Average: 32%

US + Canada: 38%

TOO MANY TOOLS

Another factor weighing on network and security teams in 2018 was the sheer number of tools they had to manage.

Global Average: 22 Tools

US + Canada: 24 Tools

SIMPLIFY, PLEASE

Vast majority of respondents are looking to simplify operational security processes in the coming year.

US + Canada: 87%

BRAZIL

EXPERIENCED IN PAST 12 MONTHS	GLOBAL	BRAZIL
Accidental data loss	40%	▲ 42%
Internet connectivity congestion due to DDoS attack	39%	▲ 44%
Extortion for DDoS threat/attack	34%	▲ 37%
Ransomware	32%	▼ 26%
Internet connectivity congestion due to genuine traffic growth/spike	29%	▼ 17%
Accidental major service outage	28%	▲ 29%
Malicious insider	26%	▲ 30%
Advanced persistent threat (APT) on corporate network	24%	► 24%
Exposure of sensitive, but non-regulated data	21%	► 21%
Industrial espionage or data exfiltration	21%	▲ 25%
Exposure of regulated data	20%	▲ 21%
Compromised IoT	17%	▲ 25%
Botted or otherwise compromised hosts on corporate network	17%	▲ 19%

HIGHEST IN OUR SURVEY

DDoS ATTACK TYPE

MULTI-LAYER ATTACKS

Today's sophisticated attackers are blending volumetric, state-exhaustion, and application-layer attacks against infrastructure devices in a single, sustained multi-vector attack. These cyber-attacks are popular because they are difficult to defend against and often highly effective.

Global Average: 36%

Brazil: 49% ▲ Highest in our survey.

DDoS ATTACK TARGETS

INFRASTRUCTURE

Global Average: 49%

Brazil: 57%

CUSTOMER-FACING SERVICES

Global Average: 38%

Brazil: 46%

FIREWALLS

Respondents from Brazil who said that they had a firewall or IPS device contribute to an outage during a DDoS attack.

Global Average: 54%

Brazil: 76% ▲ Highest in our survey.

COST OF DOWNTIME IN 2018

Brazil: $306,081

UNITED KINGDOM

EXPERIENCED IN PAST 12 MONTHS	GLOBAL	UNITED KINGDOM
Accidental data loss	40%	▲ 46%
Internet connectivity congestion due to DDoS attack	39%	▲ 40%
Extortion for DDoS threat/attack	34%	▼ 32%
Ransomware	32%	▲ 41%
Internet connectivity congestion due to genuine traffic growth/spike	29%	▲ 31%
Accidental major service outage	28%	▼ 24%
Malicious insider	26%	▲ 29%
Advanced persistent threat (APT) on corporate network	24%	▼ 12%
Exposure of sensitive, but non-regulated data	21%	▲ 26%
Industrial espionage or data exfiltration	21%	▼ 15%
Exposure of regulated data	20%	▲ 21%
Compromised IoT	17%	▲ 19%
Botted or otherwise compromised hosts on corporate network	17%	▲ 19%

HIGHEST IN OUR SURVEY

ACCIDENTAL DATA LOSS

Global Average: 40%

United Kingdom: 46% ▲ Highest in our survey.

DDoS ATTACK TARGETS

ENCRYPTED SERVICES

Especially at the application-layer.

Global Average: 53%

United Kingdom: 61%

NO SOCS

OPERATE OWN SOC

UK enterprises had the lowest percentage of any country in the report when it came to operating their own SOCs.

Global Average: 47%

United Kingdom: 37% ▼ Lowest in our survey.

SUPPLEMENT SOC RESOURCES WITH THIRD-PARTY SUPPORT

Not surprisingly, these enterprises were also more likely to supplement SOC resources with third-party resources.

Global Average: 32%

United Kingdom: 36%

COST OF DOWNTIME IN 2018

United Kingdom: $189,778

FRANCE

EXPERIENCED IN PAST 12 MONTHS	GLOBAL	FRANCE
Accidental data loss	40%	▼ 32%
Internet connectivity congestion due to DDoS attack	39%	▼ 32%
Extortion for DDoS threat/attack	34%	▼ 32%
Ransomware	32%	▼ 26%
Internet connectivity congestion due to genuine traffic growth/spike	29%	▼ 20%
Accidental major service outage	28%	▲ 32%
Malicious insider	26%	▲ 37%
Advanced persistent threat (APT) on corporate network	24%	▼ 15%
Exposure of sensitive, but non-regulated data	21%	▲ 26%
Industrial espionage or data exfiltration	21%	▲ 35%
Exposure of regulated data	20%	▲ 29%
Compromised IoT	17%	▼ 11%
Botted or otherwise compromised hosts on corporate network	17%	▼ 7%

HIGHEST IN OUR SURVEY

LOWEST IN OUR SURVEY

DDoS ATTACK TYPE

STATE-EXHAUSTION DDoS ATTACKS

Such attacks attempt to consume the connection state tables, which are present in many infrastructure components such as firewalls and IPS.

Global Average: 31%

France: 34% ▲ Highest in our survey.

DDoS ATTACK TARGETS

SAAS SERVICES

France had the highest percentage of attacks targeting SaaS services.

Global Average: 41%

France: 54% ▲ Highest in our survey.

FIREWALLS

Respondents from France said that they had a firewall or IPS device experience or contribute to an outage due to DDoS attack traffic as a result of these state-exhaustion attacks.

Global Average: 54%

France: 54%

COST OF DOWNTIME IN 2018

France: $174,834

GERMANY

EXPERIENCED IN PAST 12 MONTHS	GLOBAL	GERMANY
Accidental data loss	40%	▲ 43%
Internet connectivity congestion due to DDoS attack	39%	▼ 35%
Extortion for DDoS threat/attack	34%	▼ 30%
Ransomware	32%	▲ 33%
Internet connectivity congestion due to genuine traffic growth/spike	29%	▲ 36%
Accidental major service outage	28%	▲ 36%
Malicious insider	26%	► 26%
Advanced persistent threat (APT) on corporate network	24%	▲ 34%
Exposure of sensitive, but non-regulated data	21%	▼ 18%
Industrial espionage or data exfiltration	21%	▲ 24%
Exposure of regulated data	20%	► 20%
Compromised IoT	17%	▼ 16%
Botted or otherwise compromised hosts on corporate network	17%	▲ 19%

DDoS ATTACK TYPE

VOLUMETRIC ATTACKS

German enterprises experienced the fewest volumetric DDoS attacks in the past 12 months.

Global Average: 42%

Germany: 39% ▼ Lowest in our survey.

APPLICATION-LAYER ATTACKS

However, when it comes to the stealthier and more difficult to defend application-layer attacks, German enterprises experienced the most attacks.

Global Average: 27%

Germany: 30% ▲ Highest in our survey.

MULTI-LAYER ATTACKS

Again, today's sophisticated attackers are blending volumetric, state-exhaustion and application-layer attacks against infrastructure devices all in a single, sustained multi-vector attack. These cyber-attacks are popular because they are difficult to defend against and often highly effective. The good news for German enterprises is that they had the lowest percentage of multi-vector attacks in the past 12 months.

Global Average: 36%

Germany: 26% ▼ Lowest in our survey.

COST OF DOWNTIME IN 2018

German enterprises suffered from a double dose of bad news. They had the highest cost per minute of downtime, and the largest amount of downtime associated with DDoS attacks. As a result, the cost of downtime for German business was the highest.

Germany: $351,995 ▲ Highest in our survey.

JAPAN

EXPERIENCED IN PAST 12 MONTHS	GLOBAL	JAPAN
Accidental data loss	40%	▼ 39%
Internet connectivity congestion due to DDoS attack	39%	▲ 46%
Extortion for DDoS threat/attack	34%	▲ 40%
Ransomware	32%	▼ 29%
Internet connectivity congestion due to genuine traffic growth/spike	29%	▲ 34%
Accidental major service outage	28%	▼ 25%
Malicious insider	26%	▼ 14%
Advanced persistent threat (APT) on corporate network	24%	▲ 25%
Exposure of sensitive, but non-regulated data	21%	▼ 10%
Industrial espionage or data exfiltration	21%	▼ 13%
Exposure of regulated data	20%	▼ 8%
Compromised IoT	17%	▼ 11%
Botted or otherwise compromised hosts on corporate network	17%	▲ 25%

HIGHEST IN OUR SURVEY

LOWEST IN OUR SURVEY

DDoS ATTACK TYPE

VOLUMETRIC ATTACKS

Bad news: Japanese enterprises experienced more volumetric attacks than any other region in the survey.

Global Average: 42%

Japan: 48% ▲ Highest in our survey.

MULTI-VECTOR ATTACKS

While Japanese enterprises experienced the lowest percentage of state-exhaustion attacks, they experienced a significantly higher than average amount of multi-vector attacks that leverage some combination of volumetric, state or resource exhaustion, and application-layer vectors.

Global Average: 36%

Japan: 44%

FIREWALLS

Despite the low number of state-exhaustion attacks, respondents said that they had a firewall or IPS device experience or contribute to an outage due to DDoS attack traffic.

Global Average: 54%

Japan: 55%

COST OF DOWNTIME IN 2018

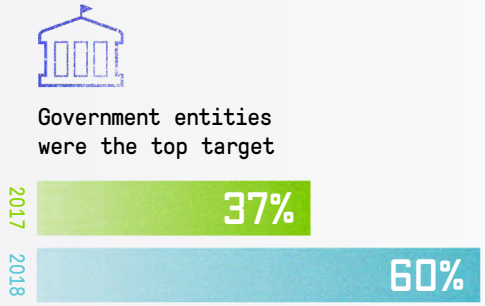
Japan: $123,026

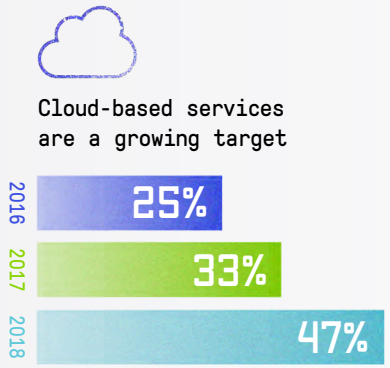
SERVICE PROVIDER

IN THE 14 YEARS WE HAVE BEEN CONDUCTING THE WISR, ONE THING HAS ALWAYS BEEN CLEAR: HAVING BORNE THE BRUNT OF DDoS ATTACKS FROM THE START, SERVICE PROVIDERS HAVE OF NECESSITY TAKEN THE LEAD IN DDoS DEFENSE.

When this report was launched, 10 Gbps attacks made headlines and took networks down. Today, attacks forty times that size are routinely mitigated with little to no disruption to online services.

KEY FINDINGS





PUBLIC SECTOR UNDER FIRE.

DDoS has long been a tool for online protests, thanks to the combination of increasingly sophisticated DDoS for-hire attack services and free attack tools that enable anyone with basic online skills to launch an attack.

In 2018, government entities were the top target at 60 percent, up significantly from 37 percent in 2017. As political instability increases around the world, expect DDoS to continue to be used as a form of protest.

IF IT'S IMPORTANT TO YOU, IT'S IMPORTANT TO THEM.

As service providers place growing importance on the delivery of cloud-based services to enterprises and consumers, it should come as no surprise that attackers are increasingly targeting these services with DDoS attacks. The numbers have jumped significantly over the past three years, from 25 percent in 2016, to 33 percent in 2017, and finally, to 47 percent in 2018.

ONGOING OPERATIONAL CHALLENGES.

For the past three years, we have seen service providers increasingly turn to third-party (outsourced) and third-party augmented (hybrid) SOC capabilities. This highlights once again the global challenges organizations face to build and maintain an internal security team of skilled practitioners, and their reliance on outsourcing to address the issue.

SERVICE PROVIDER DEMOGRAPHICS

The 2018 survey represents a wide range of operators, from global Tier 1 to regional Tier 2 and 3 operators (Figure 41). Most offer multiple cloud services, such as virtualization, storage, cloud applications, and managed security. The second largest group comprises those who deliver hosting, data center, and co-location services.

Nearly two-thirds identified themselves as security, network, or operations professionals, a similar result to 2017 (Figure 42). Security professionals have the highest representation with 35 percent.

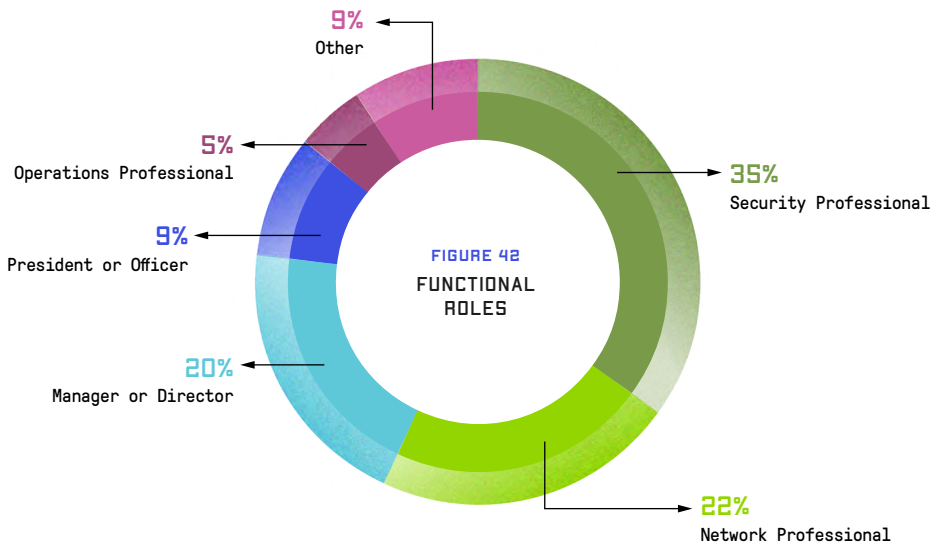
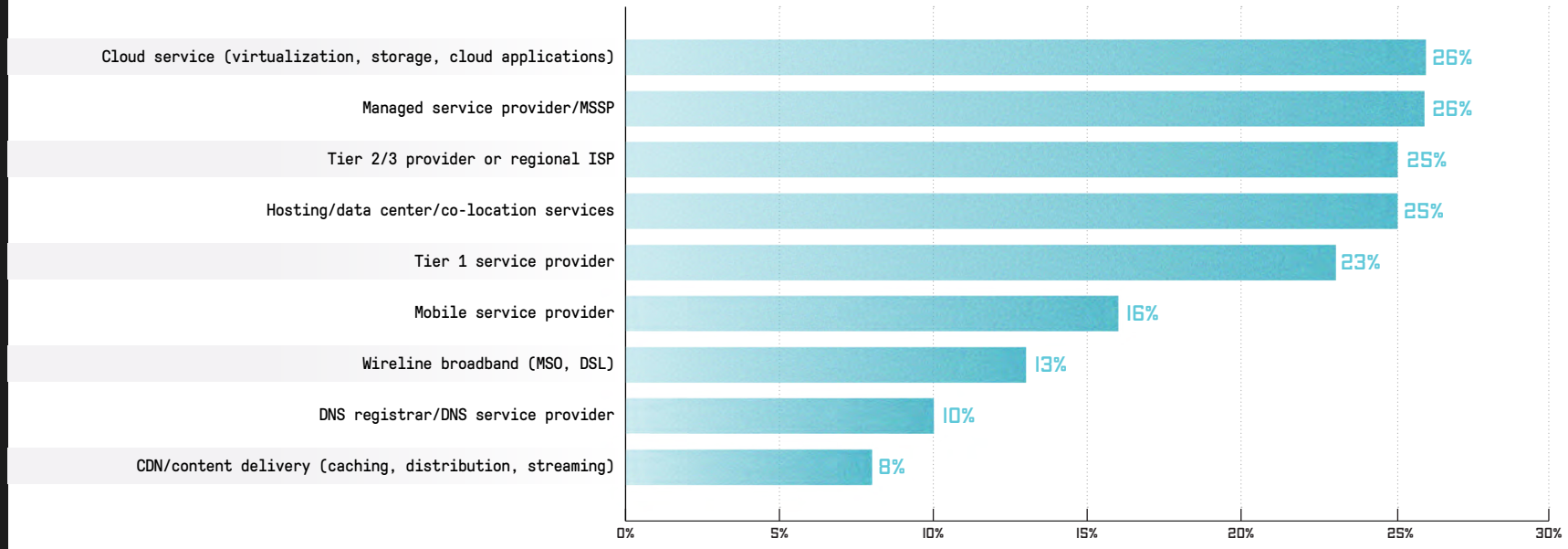


FIGURE 42
FUNCTIONAL ROLES

FIGURE 41
SERVICE PROVIDERS REPRESENTED



SERVICE PROVIDER THREATS + CONCERNS

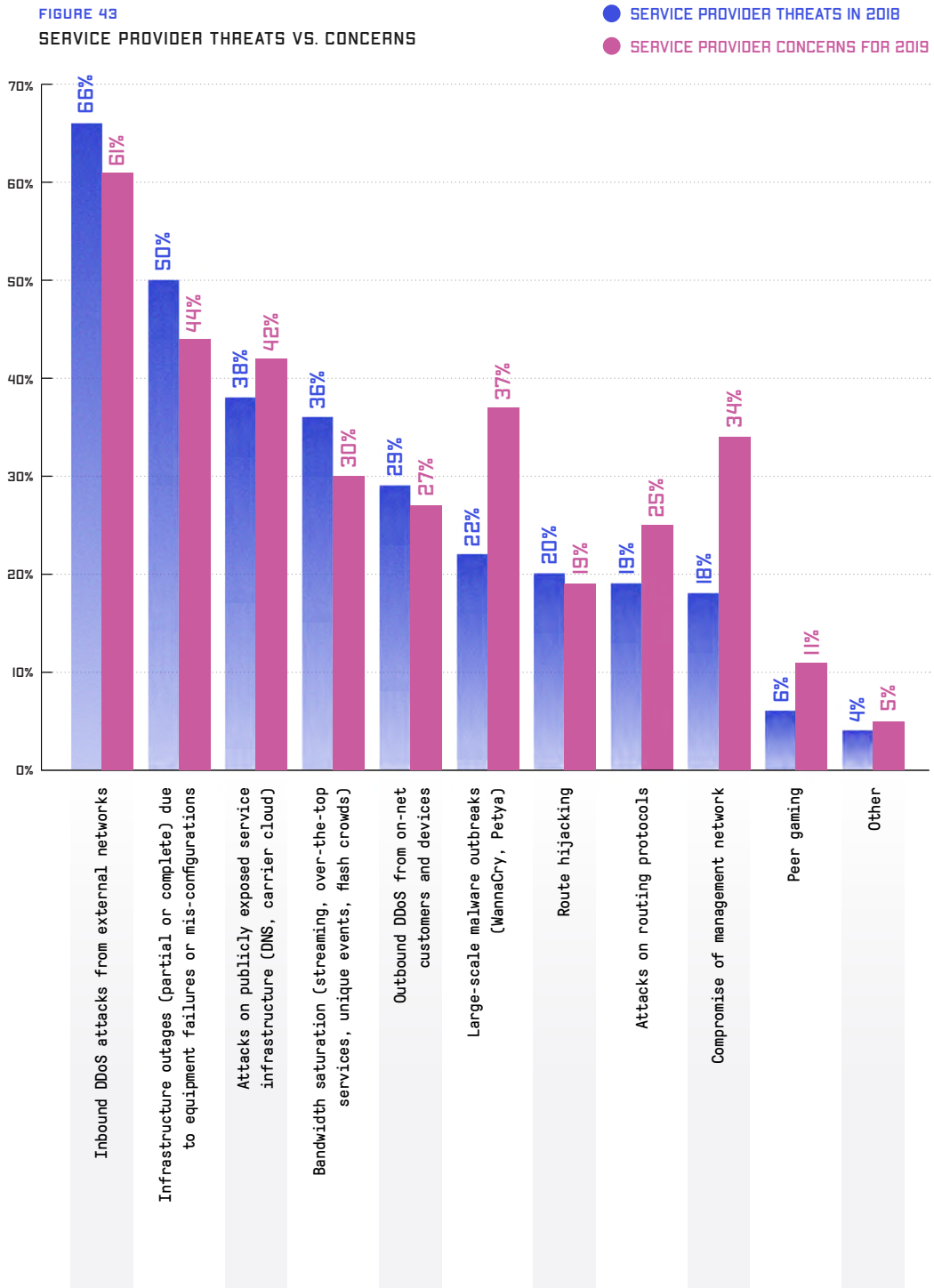
DDoS attacks once again represented the top threat observed by service providers (Figure 43). In 2018, the DDoS attacks category was refined to include both inbound and outbound types, and 95 percent of respondents reported they experienced one or the other of those attacks. That represents a 10 percent increase from 2017, which could speak to an increase in attack frequency, or in service provider visibility and detection capabilities. Inbound DDoS attacks alone were the number one threat, as experienced by 66 percent of the service providers.

Attacks on publicly exposed service infrastructure were reported by 38 percent of service providers, while 22 percent experienced large-scale malware outbreaks.

Looking ahead, DDoS attacks are the primary concern for 2019, according to 88 percent of the service providers (Figure 43). The continued use of reflection/amplification techniques and the continued exploitation of vulnerable IoT devices have many worried about a greater frequency in high volume attacks. Large-scale malware outbreaks were also found to be a significant concern for 37 percent of the service providers in the coming year. This is a trend that we will continue to monitor in future iterations of this report.

FIGURE 43

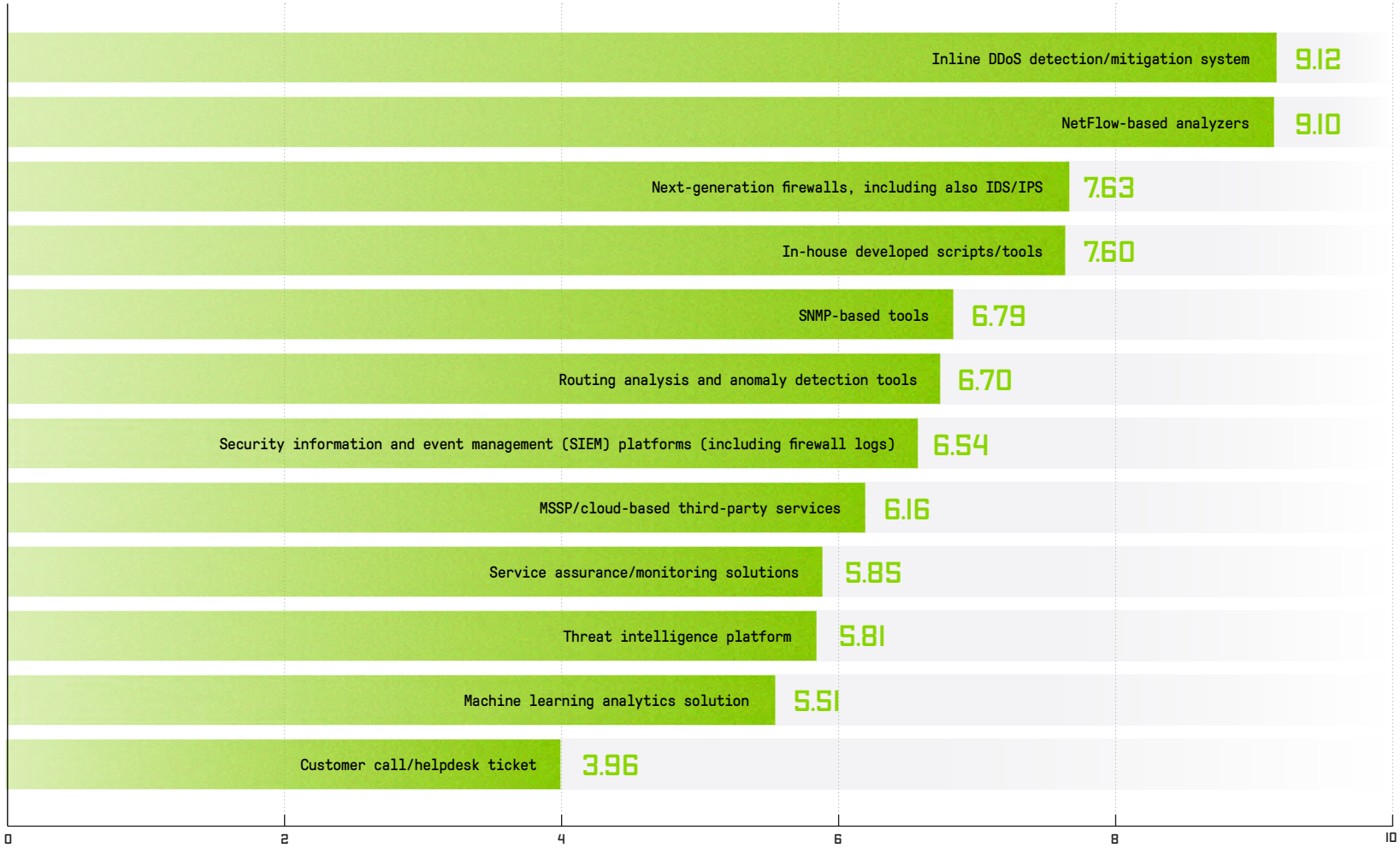
SERVICE PROVIDER THREATS VS. CONCERNS



In terms of the effectiveness of threat detection tools, again in 2018, IDMS and NetFlow-based analyzers dominated the results (Figure 44). Both have gained in popularity, which is a welcome trend. We also saw an increase in the use of IDS/IPS and in-house developed scripts/tools, highlighting the need for DDoS attack detection in service provider environments.

FIGURE 44

THREAT TOOL EFFECTIVENESS



SERVICE PROVIDER DDoS

SCALE, TARGETING, AND MOTIVATION

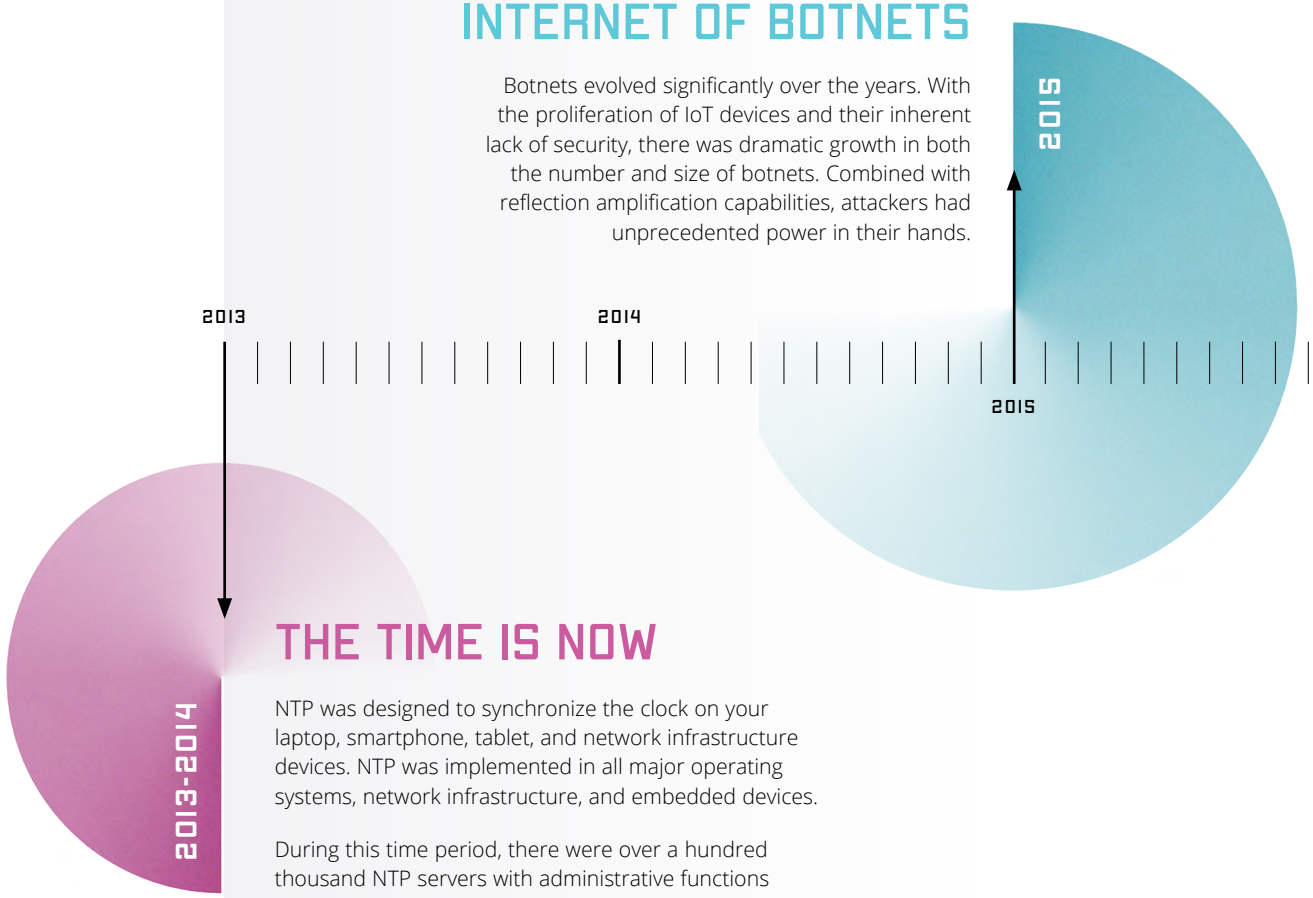
When it comes to the scale of DDoS attacks in 2018, it was a record-breaking year. In May, NETSCOUT published a blog, *The Terabit Attack Era Is Upon Us,* describing a 1.7 Tbps DDoS attack that targeted a North American service provider.

To put a terabyte of traffic in perspective, AT&T estimates that it is equal to watching 400 hours of SD TV plus streaming 200 HD movies.

So how did we get to the Terabit Attack Era? The answer is methodically, thanks to the persistence of attackers in identifying and exploiting every vulnerability to their fullest advantage.

RISE OF IoB, THE INTERNET OF BOTNETS

Botnets evolved significantly over the years. With the proliferation of IoT devices and their inherent lack of security, there was dramatic growth in both the number and size of botnets. Combined with reflection amplification capabilities, attackers had unprecedented power in their hands.



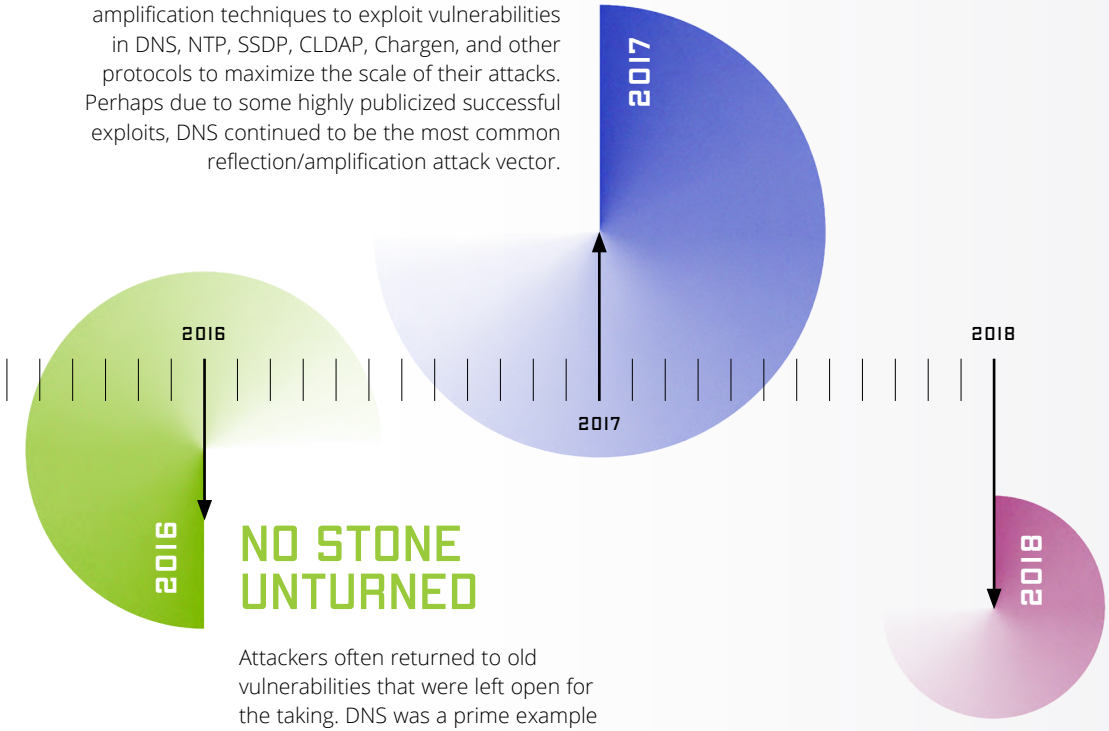
THE TIME IS NOW

NTP was designed to synchronize the clock on your laptop, smartphone, tablet, and network infrastructure devices. NTP was implemented in all major operating systems, network infrastructure, and embedded devices.

During this time period, there were over a hundred thousand NTP servers with administrative functions ill-advisably open to the general internet and vulnerable. In other words, compromising NTP represented a gold mine for attackers looking to amplify the size of their DDoS attack capabilities.

SUCCESS BREEDS IMITATION

If you're not going to fix it, why should we stop? 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. Perhaps due to some highly publicized successful exploits, DNS continued to be the most common reflection/amplification attack vector.



NO STONE UNTURNED

Attackers often returned to old vulnerabilities that were left open for the taking. DNS was a prime example in 2016. There were 28 million open DNS resolvers tailor-made for use in reflection/amplification techniques. Using large botnets such as Mirai or Satori made generating very large attacks all too easy.

HERE WE GO AGAIN

In 2018, another widely used application, Memcached, joined the ranks of high-bandwidth reflection/amplification exploits. Memcached servers were suddenly being used as reflectors/amplifiers to launch extremely high-volume UDP reflection/amplification attacks.

THE ONE IMPORTANT LESSON WE'VE LEARNED IN OUR YEARS OF ANALYZING THE THREAT LANDSCAPE IS THAT ONCE A NEW TYPE OF DDoS ATTACK APPEARS, IT NEVER GOES AWAY.

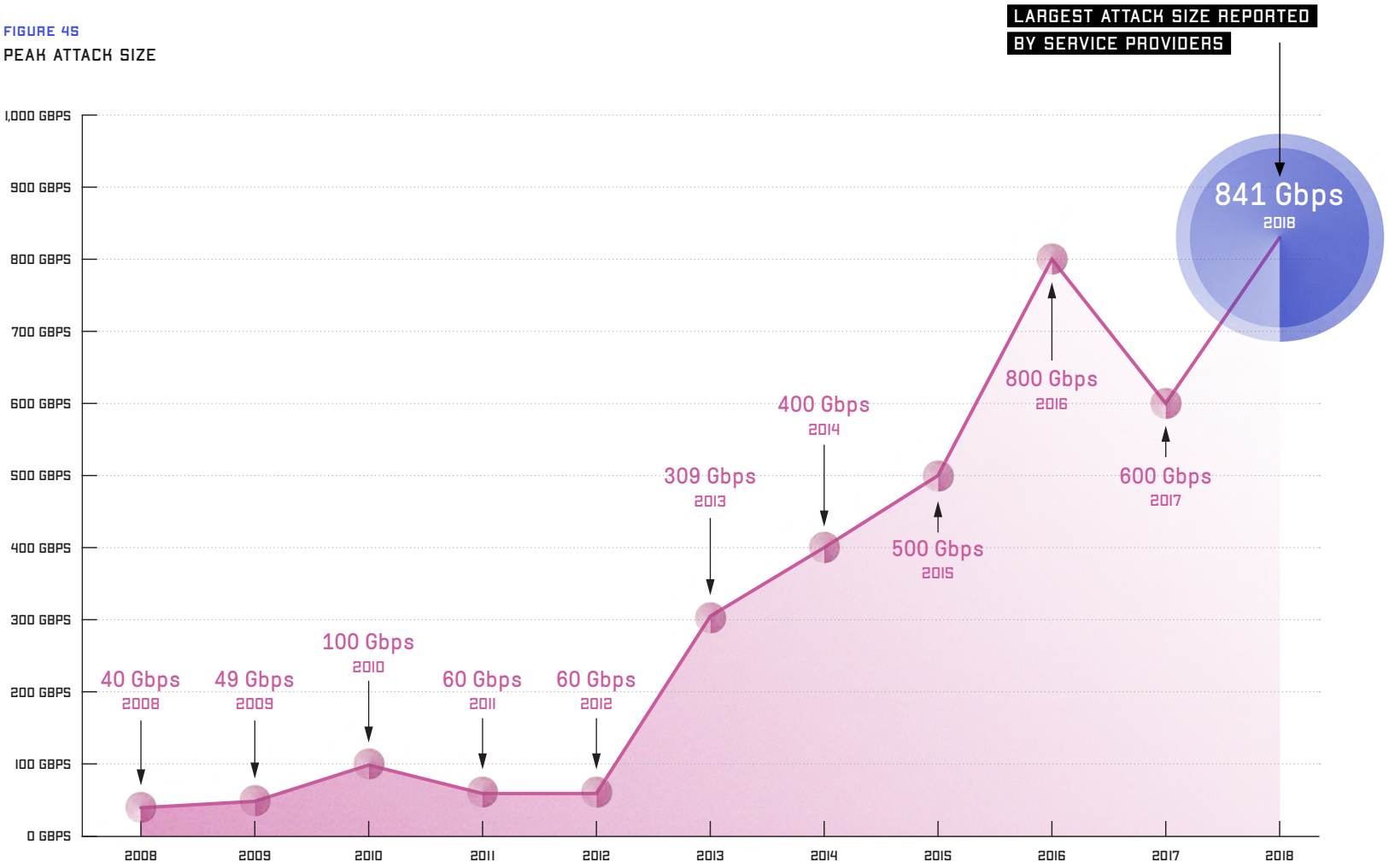
As attack tools grow more sophisticated and new attack vectors emerge, threat actors are finding it easier and more cost-effective to launch larger, more effective attacks.

This in turn demands a hybrid or layered DDoS defense posture that combines on-premises and cloud mitigation capabilities to address the frequency, size, and scale of evolving attacks.

The largest DDoS attack reported by survey respondents was 841 Gbps in 2018, with others reporting attacks of 450 Gbps, 394 Gbps, and 300 Gbps (Figure 45). Not surprisingly, all these resulted from a combination of different reflection/amplification vectors such as DNS, NTP, SSDP, Chargen, SNMP, and Memcached.

FIGURE 45

PEAK ATTACK SIZE



The poor state of IoT security has led to the weaponization of infected devices as "packet cannons" that utilize new reflection/amplification vectors to generate these high-volume DDoS attacks.

In 2018, attack targets were similar to 2017, with end customers in first place (Figure 46). The proportion of attacks targeting service and network infrastructures increased slightly as attackers' ability to impact service provider infrastructures with new tools, such as Memcached amplification, continued.

A significant change in 2018 was in the customer sectors most often targeted. In past years, financial services, e-commerce, and gaming customers were at the top of the list. In 2018, it was government customers at 60 percent, up significantly from 37 percent in 2017 (Figure 47). DDoS has long been a tool for online protests, thanks to the combination of increasingly sophisticated for-hire DDoS attack services and free attack tools that enable anyone with basic online skills to launch an attack.

AS POLITICAL INSTABILITY INCREASES AROUND THE WORLD, EXPECT DDoS TO CONTINUE TO BE USED AS A FORM OF PROTEST.

FIGURE 46
DDoS ATTACK TARGETS

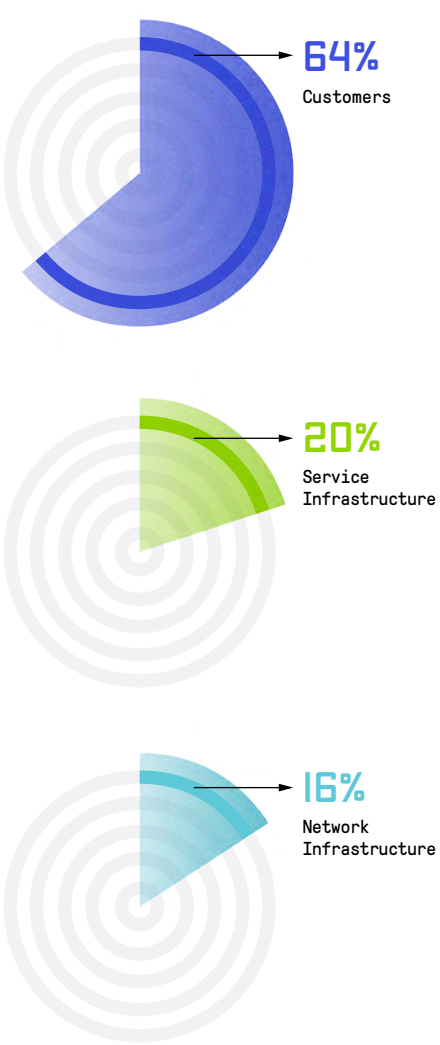


FIGURE 47
TARGETED CUSTOMERS

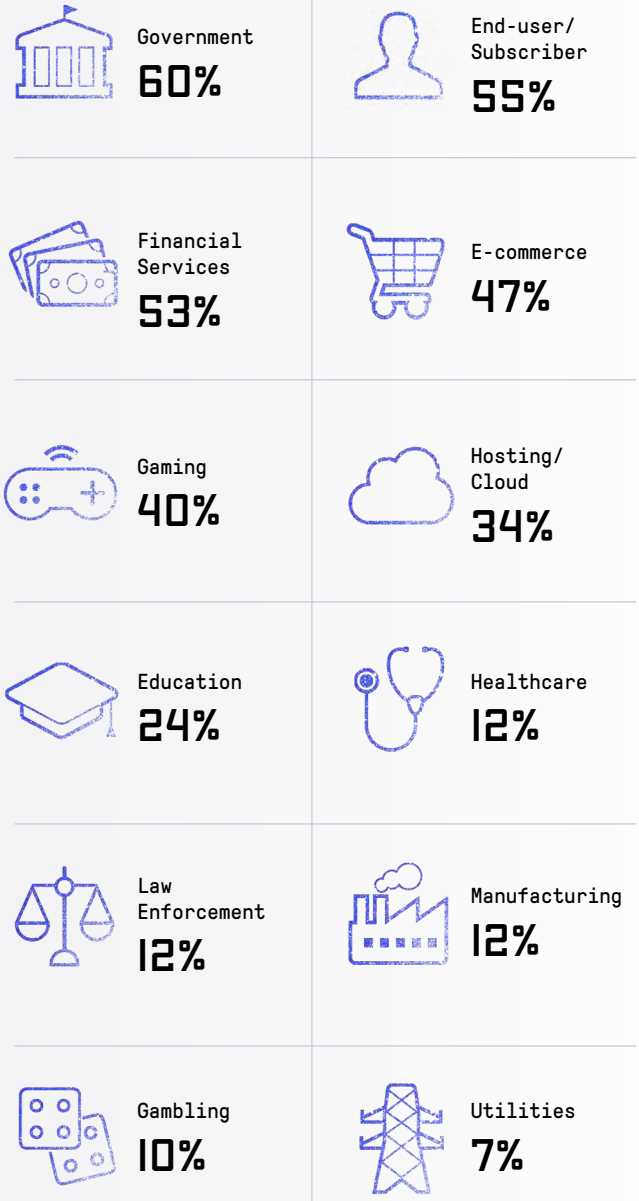
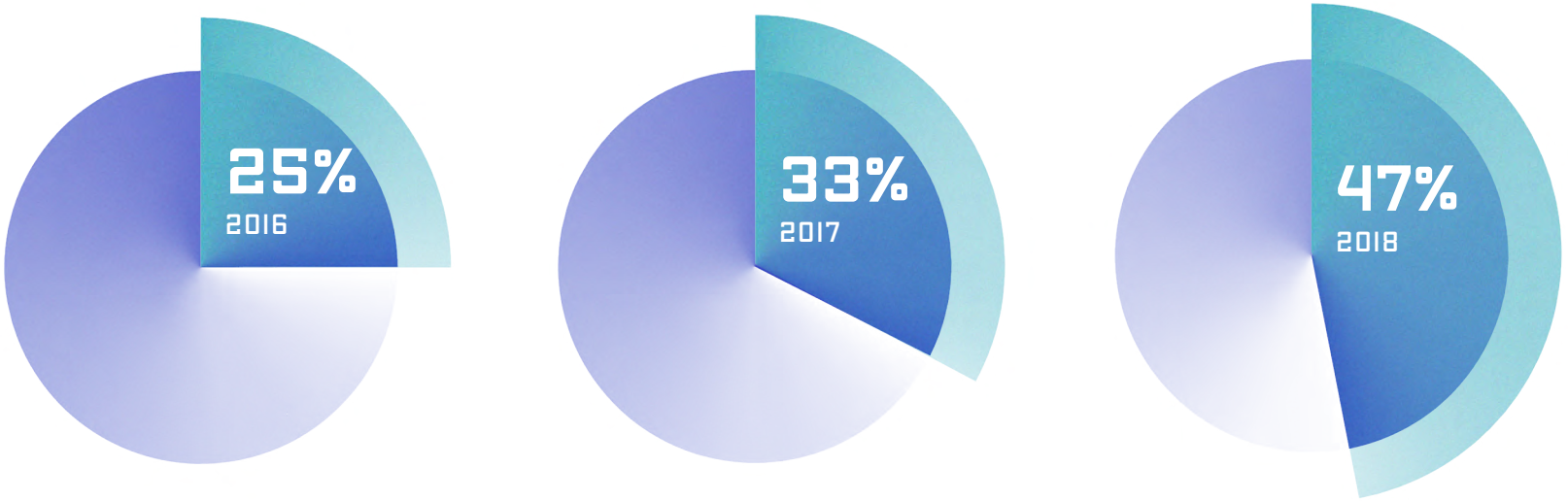


FIGURE 48

REPORTED ATTACKS AGAINST CLOUD SERVICES



As service providers place growing importance on the delivery of cloud-based services to enterprises and consumers, it should come as no surprise that attackers are increasingly targeting these services with DDoS attacks. The percentage of providers who reported attacks against cloud services shows a rising line (Figure 48).

A red flag can be found in the number of those who either are not aware of DDoS attacks against their cloud services or believe this is not applicable to their business (Figure 49). As more organizations adopt cloud-based technologies and rely on services delivered from the cloud, expectations are that anything in the cloud is available 24x7x365, regardless of the scale and complexity of DDoS attacks. DDoS attacks represent the number one external threat to the availability of cloud services, so having no ability to monitor for DDoS attacks, or not being concerned at all, strikes us a lesson waiting to be learned.

FIGURE 49

ATTACKS AGAINST CLOUD SERVICES

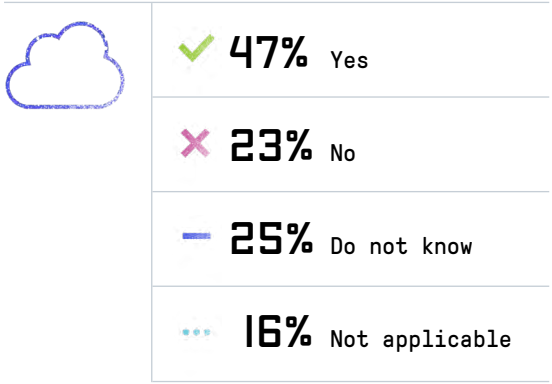
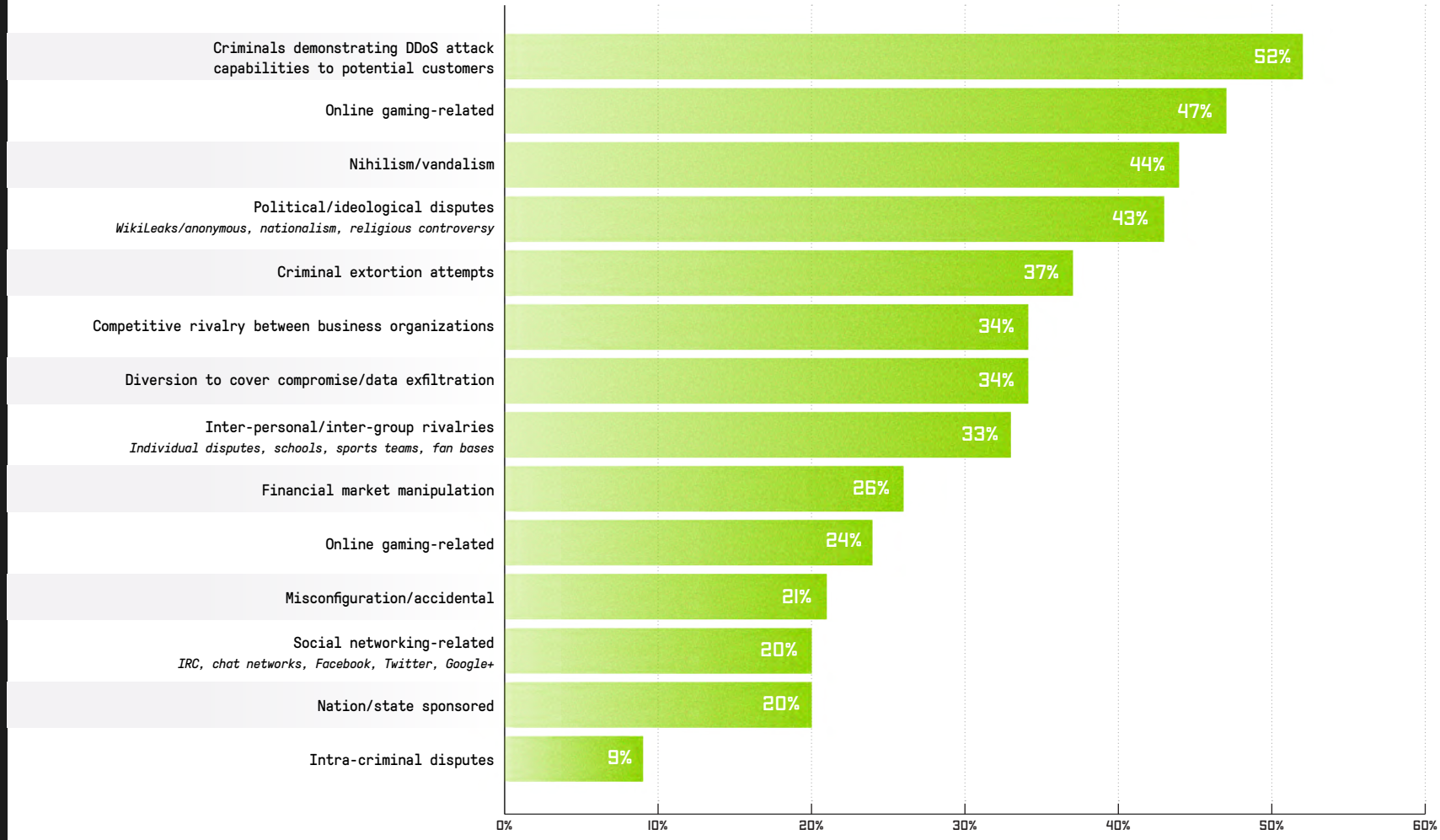


FIGURE 50

DDoS ATTACK MOTIVATIONS



When it comes to the most common DDoS motivations in the service provider environment, respondents cited criminals demonstrating their capabilities (52 percent) and online gaming-related attacks (47 percent) as most common (Figure 50). Looking further, we observed a notable shift from financially motivated extortion attacks to political or ideological disputes and vandalism acts, which rose to fourth and third positions on the list respectively. This change in motivation matches the mix of attack targets in service provider environments and reminds us that political instability and social protests happen simultaneously in the real and digital worlds. We call this Cyber Reflection, where attacks in cyber space stem from political or ideological disputes.

TYPE AND FREQUENCY

Very little changed in 2018 with regard to the mix of attack types experienced by service providers. As in all previous iterations of this report, volumetric attacks were the most common attack types (Figure 51). However, there was a decrease from 78 percent in 2017 to 69 percent, which resulted in more state-exhaustion and application-layer attacks.

With more organizations deploying protection from basic volumetric DDoS threats, attackers turn to more difficult-to-defend state-exhaustion and application-layer techniques.

The top three services targeted by application layer attacks are the same as the previous year: HTTP, HTTPS, and DNS (Figure 52). In each case, nearly three quarters of respondents reported attacks against these services.

FIGURE 51
TYPES OF DDoS ATTACKS

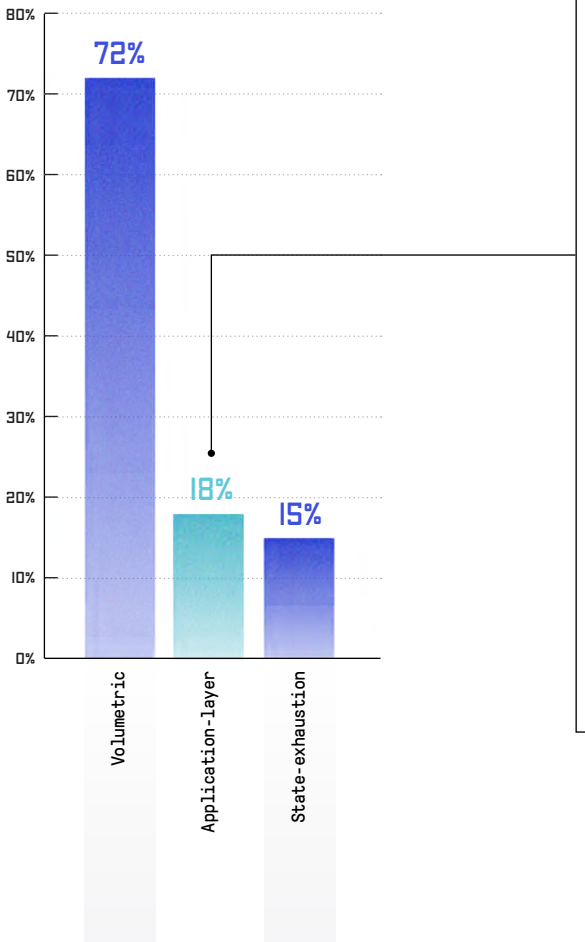


FIGURE 52
TARGETS OF APPLICATION-LAYER ATTACKS

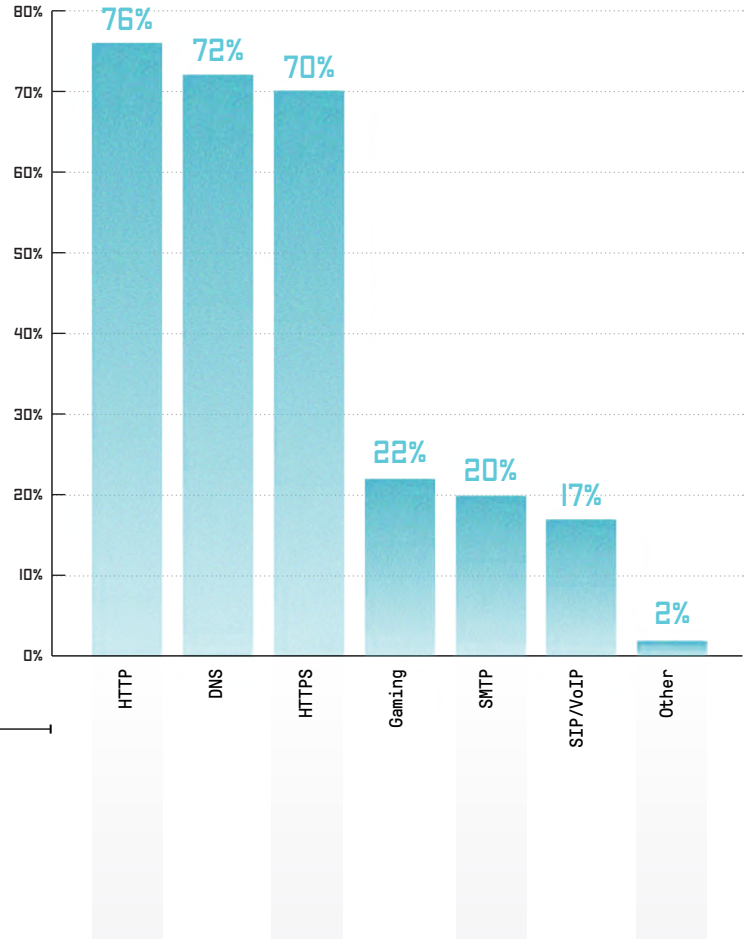
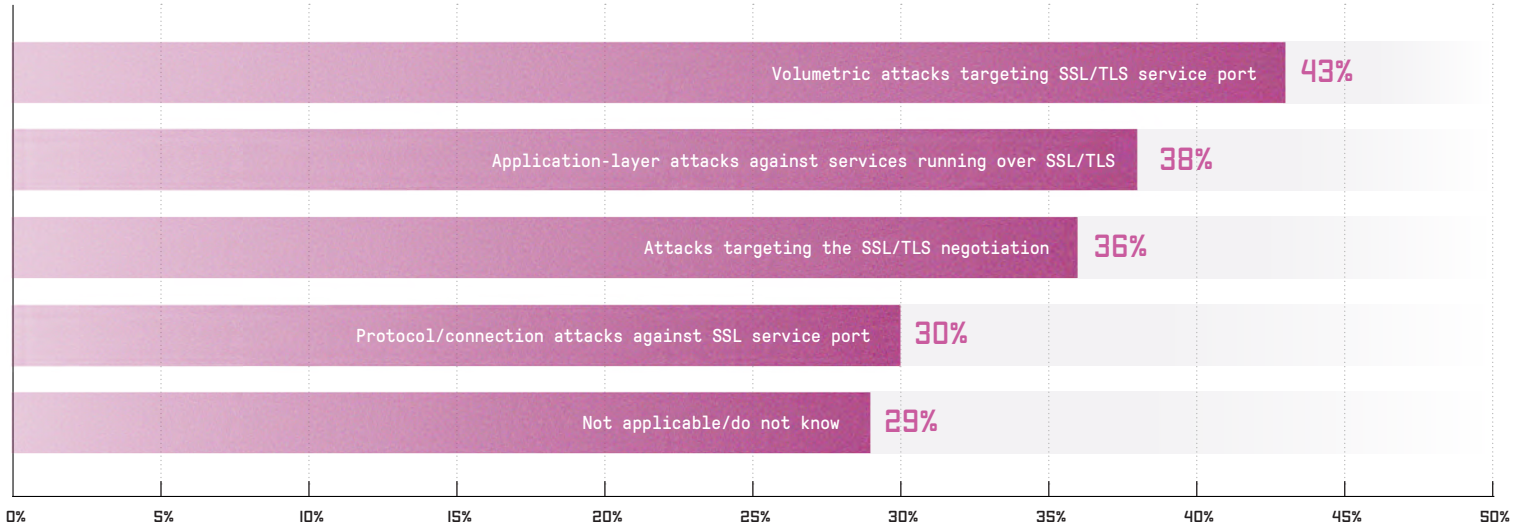


FIGURE 53

TYPES OF ATTACKS TARGETING ENCRYPTED SERVICES



As we saw with cloud services, the more popular they become, the more they are targeted. The same was true with encrypted services. Whereas many cloud service providers had no visibility into, or interest in, DDoS attack traffic, that is not the case with encrypted services. There was a dramatic decrease from 48 percent in 2017 to 29 percent in 2018 for those who either found attacks against encrypted services as "not applicable" or did not know if they happened (Figure 53). This shows that organizations understood these services were being targeted and deployed tools to provide enhanced visibility and protection.

THERE WAS A NOTABLE INCREASE IN THE PROPORTION OF APPLICATION-LAYER ATTACKS AGAINST SERVICES RUNNING OVER SSL/TLS. THIS IS ONE OF THE MOST COMPLEX DDoS ATTACK TYPES TO DETECT AND HAVING THE CAPABILITIES TO MITIGATE THESE ATTACKS SHOULD BE CONSIDERED PART OF ANY DDoS MITIGATION STRATEGY INVOLVING ENCRYPTED SERVICES.

The percentage of service providers seeing multi-vector attacks on their networks in 2018 increased to 65 percent, up from 59 percent the previous year (Figure 54). At the same time, the number of providers who did not observe such attacks dropped down from 15 percent to 10 percent. This indicates that attackers continue to mix attack types and push defenders to improve their detection and mitigation capabilities.

FIGURE 54

MULTI-VECTOR DDoS ATTACKS

As in previous years, there were two major groups of respondents in 2018: those who observe fewer than 10 attacks per month and those who observe more than 100 (Figure 55). This bifurcated effect might be explained by the growing consolidation of the internet, as more and more traffic and resources tend to concentrate in a handful of large network operators.

Analyzing attack durations, more than half said that their longest attacks lasted 6 hours or less, similar to 2017 (Figure 56). Attacks over 12 hours slightly decreased from 29 percent to 25 percent.

The vast majority of service providers have not reported IPv6 DDoS attacks (Figure 57). This speaks less to IPv6 adoption and more to the increased consolidation of internet traffic, especially when it comes to IPv6. Because the majority of IPv6 traffic is still associated with several content providers (CDNs and large service providers), we do not expect IPv6 DDoS attacks to become as popular as IPv4 attacks in the near future.

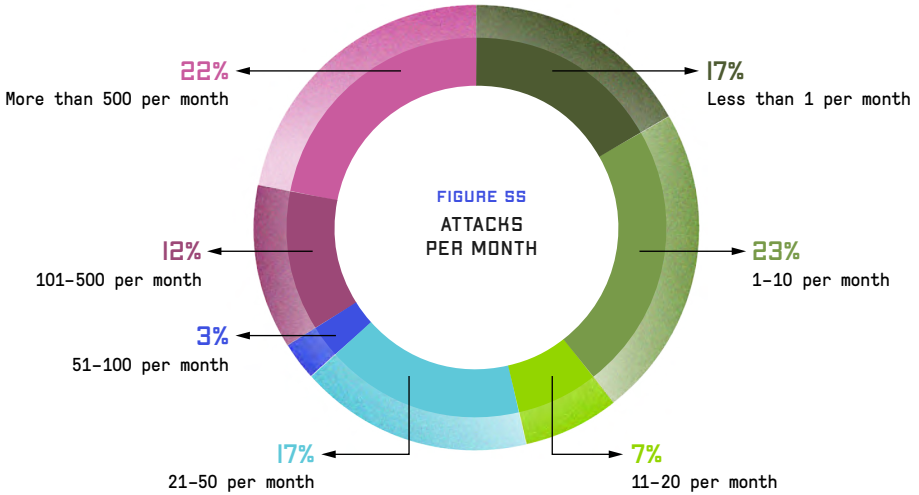


FIGURE 55
ATTACKS PER MONTH

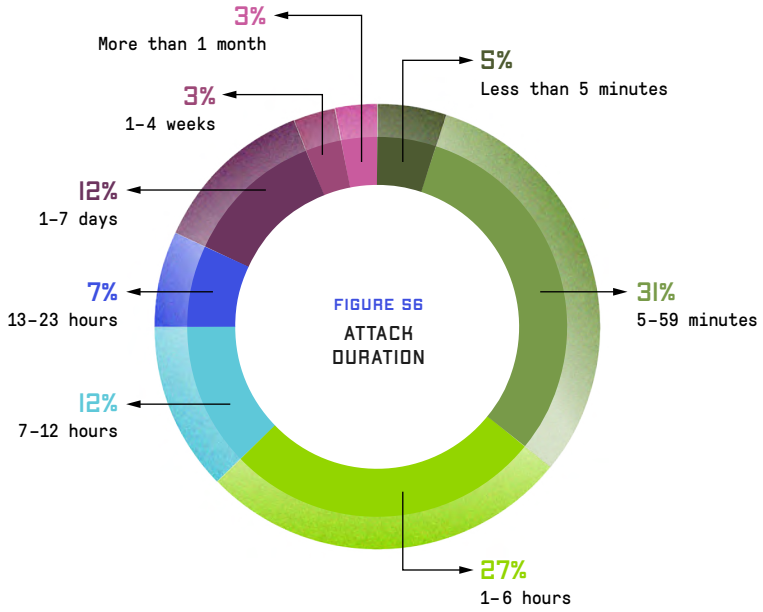


FIGURE 56
ATTACK DURATION

FIGURE 57
IPV6-BASED DDOS ATTACKS IN THE LAST 12 MONTHS

Yes	14%
No	62%
Do not know	24%

We asked service providers about the origin of IoT-based botnet attacks and found that almost half of all attacks originate outside of their networks (Figure 58). As the number of IoT devices grows, the proportion considering the threat of IoT botnets not applicable to their networks decreased from 29 percent in 2017 to 21 percent in 2018.

When asked what DDoS mitigation techniques service providers used in 2018, respondents confirmed that specialized solutions such as IDMS together with ACLs remained the two most popular tools (Figure 59). Most encouraging is the jump made by FlowSpec from the fifth position to the third. As one of the FlowSpec inventors and its early adopters, we strongly believe this technology can be used to mitigate volumetric attacks in the largest and most demanding networks.

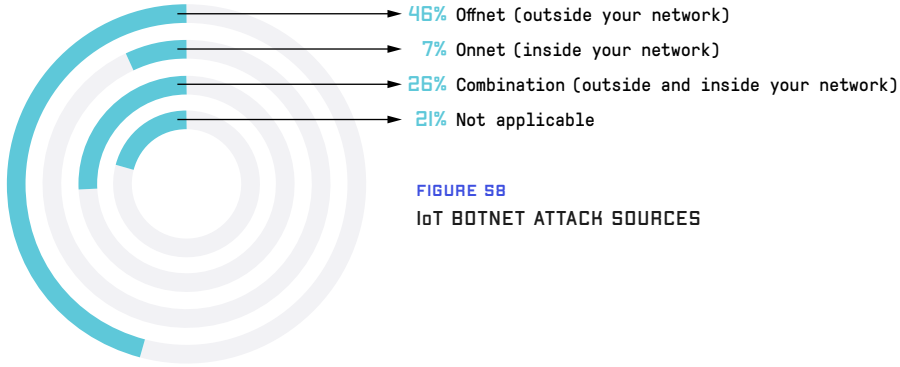


FIGURE 58
IoT BOTNET ATTACK SOURCES

FIGURE 59
ATTACK MITIGATION TECHNIQUES

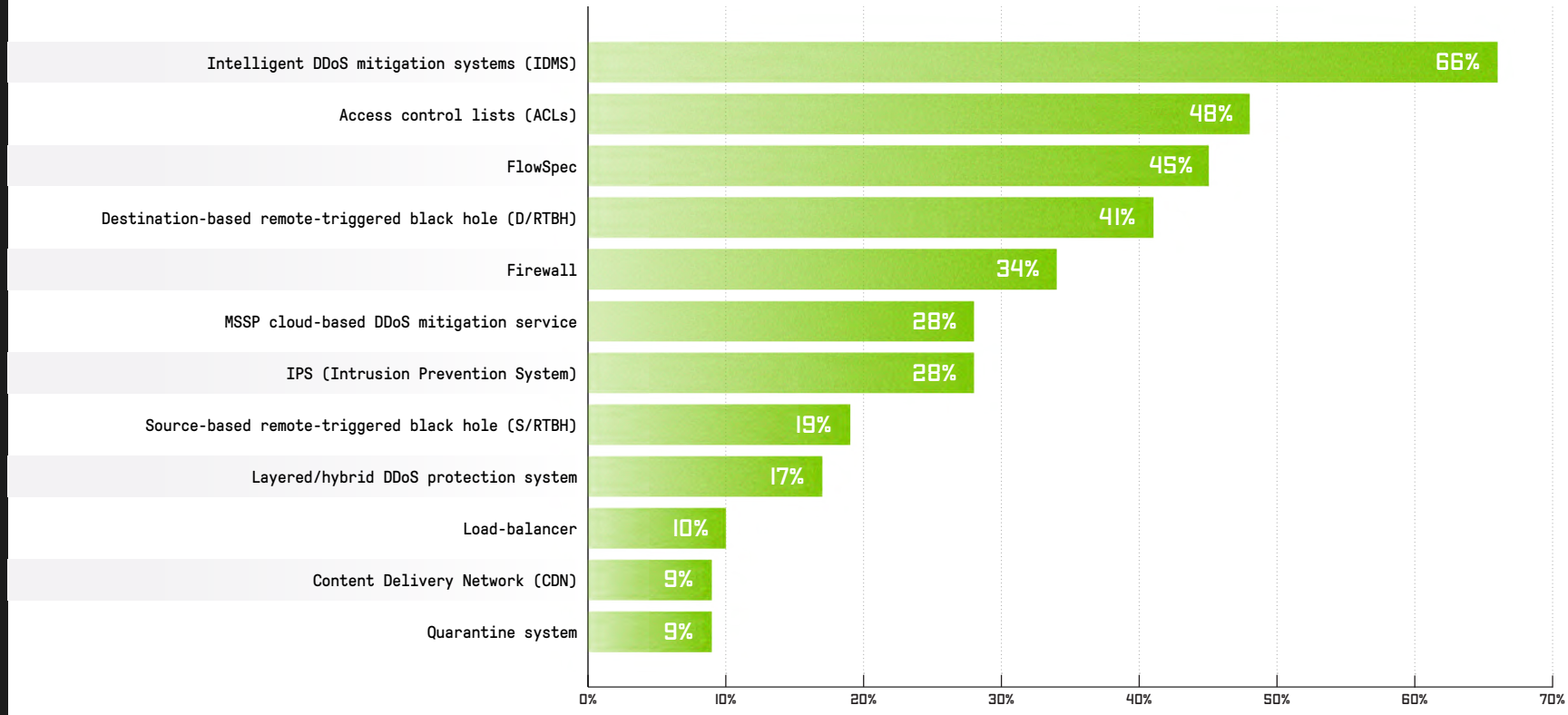
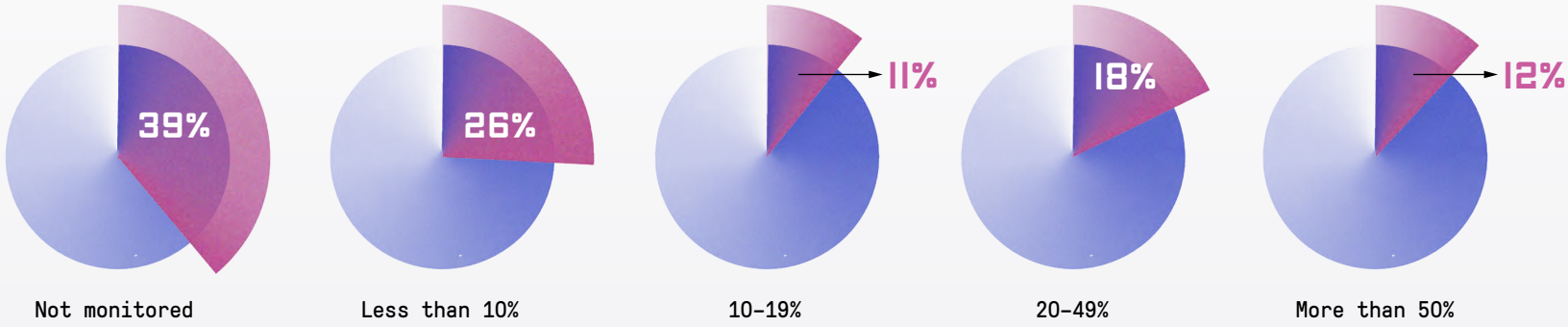


FIGURE 60

PROPORTION OF OUTBOUND/CROSS-BOUND ATTACKS OBSERVED



It is very encouraging to see that more organizations monitor outbound and cross-bound DDoS attacks. In 2018, only 39 percent of service providers said they did not monitor outbound and cross-bound attacks, a marked improvement from the 48 percent reported in 2017 (Figure 60). Improved visibility in this area is good news, since this is the first step in managing the growing threat from internal IoT devices being subsumed into botnets.

Among organizations monitoring these attacks, 30 percent of respondents indicated that 20 percent or more of DDoS incidents were either outbound or cross-bound in nature, a significant increase from 14 percent in 2017. This trend can be explained by improved visibility and the growing rate of attacks that originate internally.

SERVICE PROVIDER ORGANIZATIONAL SECURITY

For the past three years, we have seen service providers increasingly turn to third-party (outsourced) and third-party augmented (hybrid) SOC capabilities (Figure 61).

THIS HIGHLIGHTS ONCE AGAIN THE GLOBAL CHALLENGES ORGANIZATIONS FACE TO BUILD AND MAINTAIN AN INTERNAL SECURITY TEAM OF SKILLED PRACTITIONERS, AND THEIR RELIANCE ON OUTSOURCING TO ADDRESS THE ISSUE.

Sixty-two percent have their own internal SOC team, a slight increase from 60 percent 2017. Another positive sign was the significant decrease of service providers without any SOC capabilities, falling from 21 percent to 11 percent.

Those reporting at least some dedicated security personnel gained 11 percentage points to reach 97 percent in 2018, which is a very positive result (Figure 62). Of this, 29 percent had 30 or more security personnel, up from 23 percent the previous year.

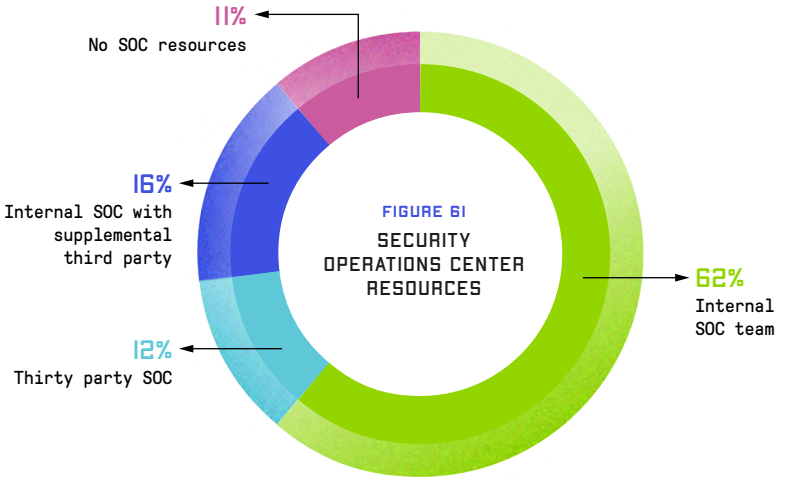


FIGURE 61
SECURITY OPERATIONS CENTER RESOURCES

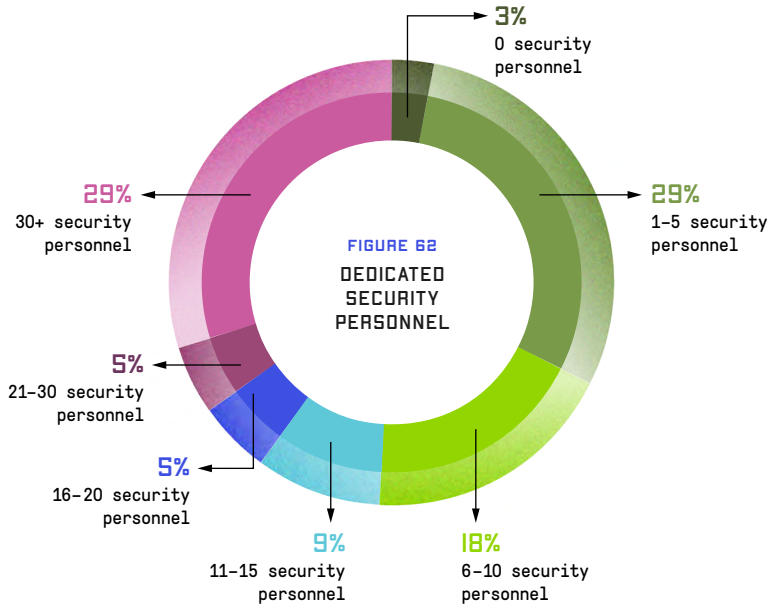


FIGURE 62
DEDICATED SECURITY PERSONNEL

The ongoing worldwide shortage of security analysts and incident responders remains a key issue facing all organizations. Difficulties in hiring and retaining skilled personnel was the number one challenge to building and maintaining operational security teams, increasing from 48 percent in 2017 to 58 percent in 2018 (Figure 63).

Security practitioners are in high demand, and companies are spending to hire them, leading to demand for top talent and churn throughout many organizations. Lack of resources was only cited by 50 percent as an impediment to building a team, down 20 percent from 2017.

FIGURE 63

OPSEC TEAM CHALLENGES

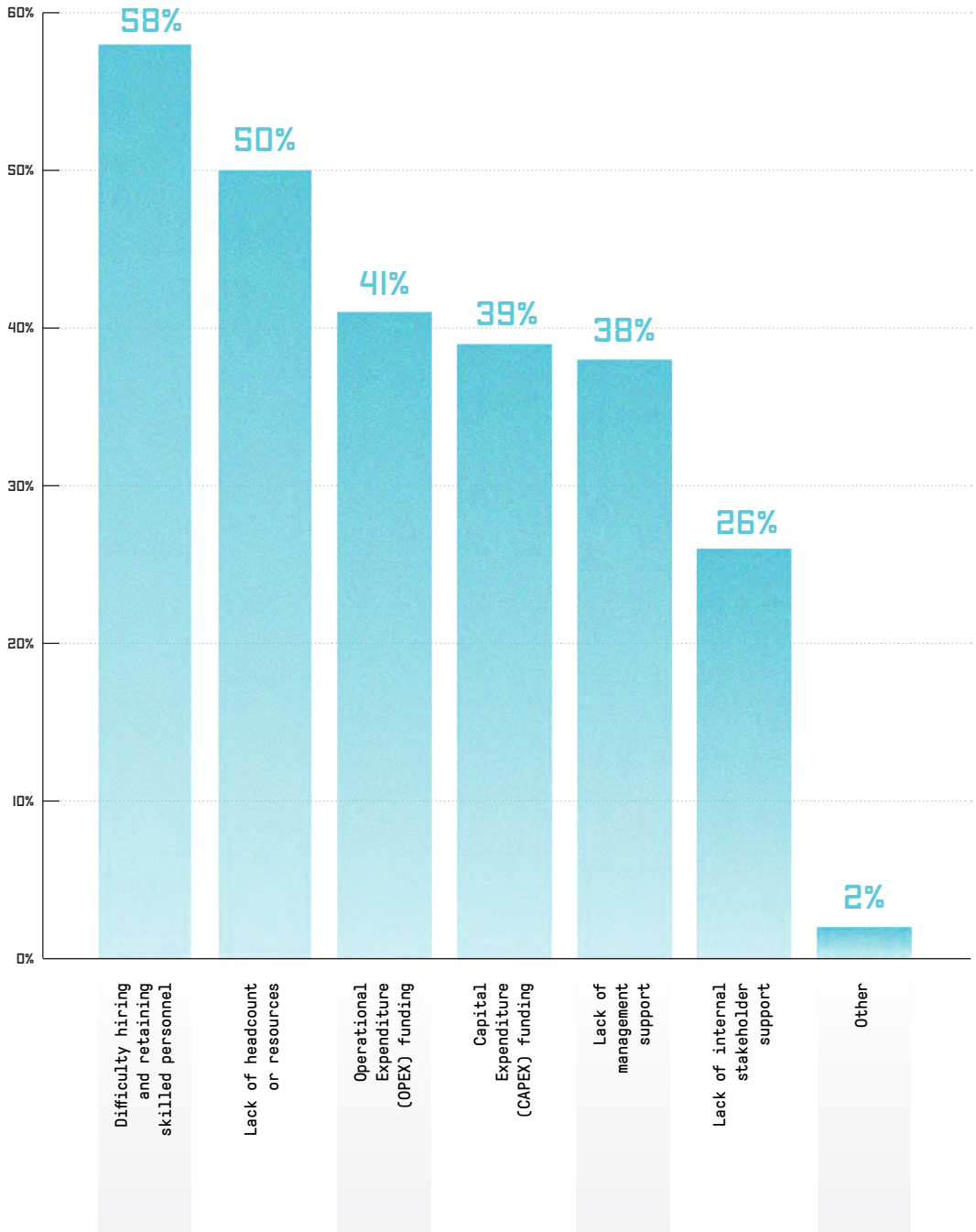
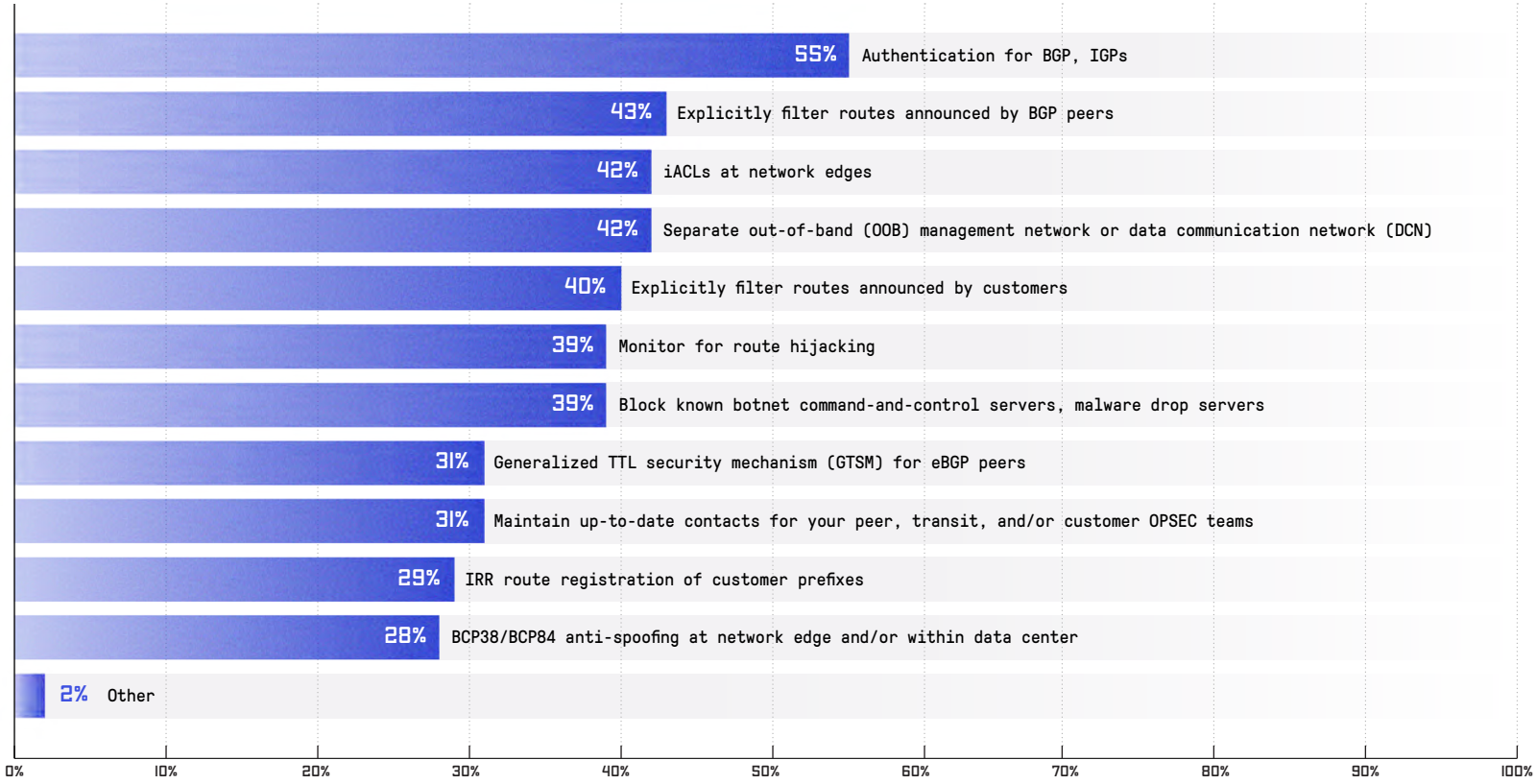


FIGURE 64

SECURITY BEST PRACTICES



For the third consecutive year, we saw a decrease in those implementing security infrastructure best practices, falling by a disappointing 15 percent (Figure 64). The top two methodologies were still authentication for BGP and explicitly filtering routes announced by customers in 2018. Another disappointing finding is the sharp decline of anti-spoofing filters from 43 percent to 28 percent, which goes against the perpetual popularity of reflection attacks in the last 6 years, highlighted once more by the record-breaking Memcached 1.7 Tbps attack.

This is the third consecutive year we saw a decline in service provider participation in global OPSEC community groups. Participation was 41 percent in 2015 and it fell to 20 percent by 2018 (Figure 65). As we note every year, these communities have proven themselves invaluable in time of high-profile attacks. We can once again only assume that this is a consequence of the challenges service providers face in building and maintaining an OPSEC team.

FIGURE 65

OPSEC PARTICIPATION

Yes
20%

No
80%

SERVICE PROVIDER MSSP

In 2018 nearly half of the service providers were involved in managed security services (Figure 66). This shows the growing importance of these revenue-generating services to respondent organizations. We expect this trend will continue as service providers look to solve real challenges for their enterprise customers by delivering more value-added services.

FIGURE 66

MSSP INVOLVEMENT

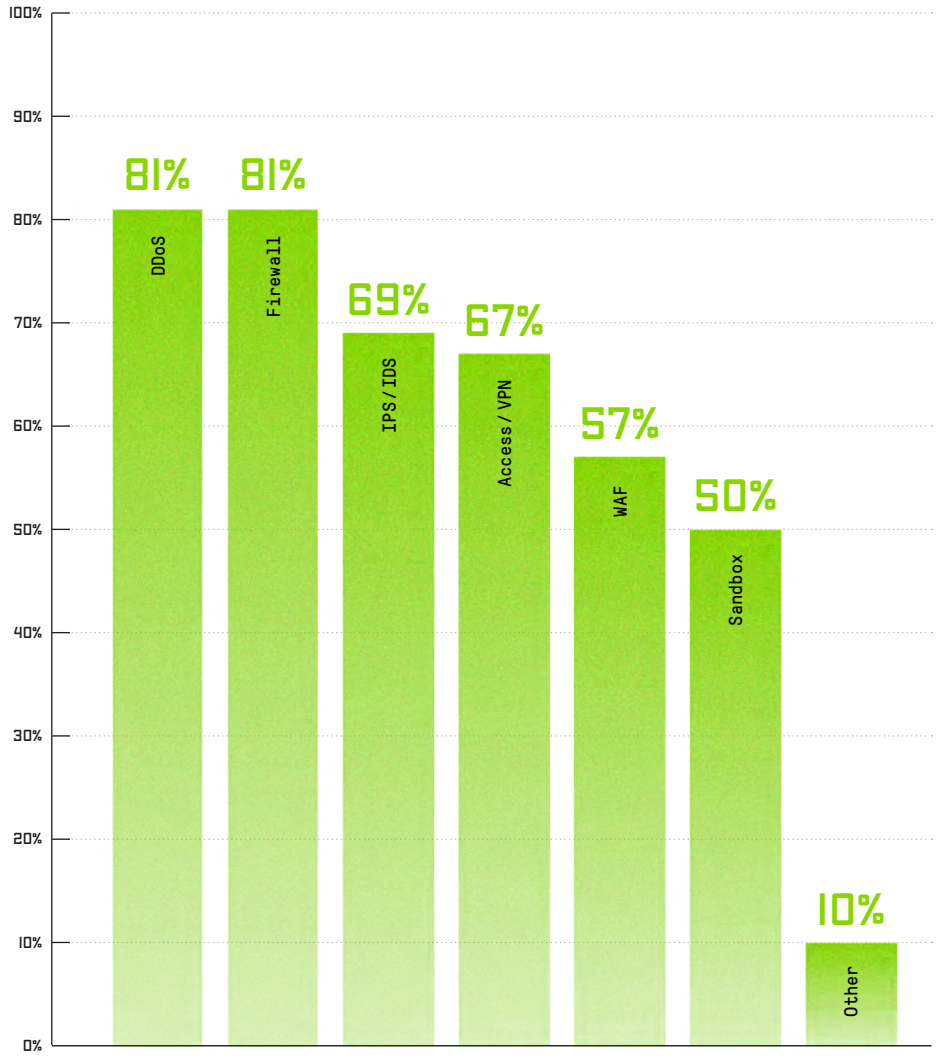
Yes	No
47%	53%

Managed DDoS and firewalls were the top two services provided in 2018, at 81 percent each (Figure 67). Those were followed by IPS/IDS and Access/VPN at 69 percent and 67 percent respectively, along with WAF at 57 percent and sandboxing at 50 percent.

All of these services solve real world challenges for enterprise organizations and are now expected as offerings from service providers to their customers.

FIGURE 67

MANAGED SECURITY SERVICES PROVIDED



Managed DDoS protection is included in a base offering for 37 percent of these service providers, which is below our expectations considering the shared benefits for both the provider and the customers when mitigating a volumetric DDoS attack (Figure 68).

Only 29 percent offer DDoS protection as an additional service, which is also disappointing. While volumetric DDoS attacks can be detected and mitigated upstream by service providers as part of an existing contract, application-layer DDoS attacks are best remediated at the network edge on a per-customer basis. About 75 percent of those offering additional DDoS services provide multiple tiers of protection which is expected and a standard practice.

Not surprisingly, financial services organizations were the number one business expressing interest in managed DDoS offerings, at 72 percent, followed closely by government at 69 percent (Figure 69).

However, while internet service providers and e-commerce businesses came third and fourth at 56 percent and 51 percent respectively, a few of the usual suspects surprisingly didn't make it to the top half of the list. Only 33 percent of healthcare organizations were interested in DDoS managed services, followed by 31 percent of gaming, 18 percent of social networking, and 15 percent of gambling organizations. While those business categories were expected to rank higher since they are popular targets of DDoS attacks, one possible explanation is that those kinds of organizations tend to implement and run DDoS mitigation on their own.

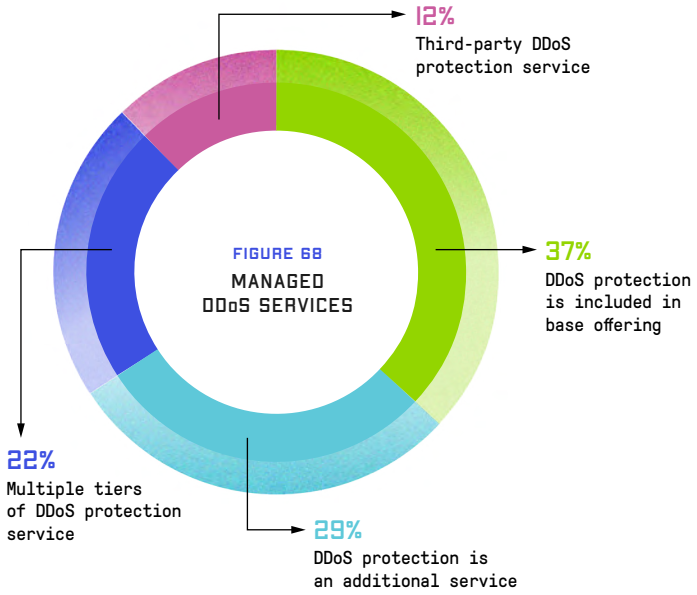


FIGURE 68
MANAGED DDoS SERVICES

FIGURE 69 / MSSP BUSINESS INTEREST

Financial Services 72%	Cloud Provider 44%	Gaming 31%	Social Networking 18%
Government 69%	Media + Entertainment 38%	Education 28%	Transportation 18%
ISPs 56%	Healthcare 33%	Law Enforcement 26%	Gambling 15%
E-commerce 51%	Retail 33%	Manufacturing 26%	Utilities 13%

With the growing scale and complexity of attacks adding pressure to already stressed teams, it was not surprising that business customers expressed growing interest in DDoS detection and mitigation services in 2018 (Figure 70). Consistent with previous years, those with the most mission-critical digital infrastructures led the demand for managed security services. What changed was the level of interest from medium and smaller businesses, with more than half of service providers reporting growing interest in DDoS managed services from these customers.

For 70 percent, SD-WAN security offerings are the biggest technology additions for managed services expansion, with NFV orchestration at 60 percent (Figure 71). As expected, those two technologies dominate, with NFV Telco Cloud (Cloud CPE) being slightly more appealing for 33 percent over NFV Next-Gen CPE (uCPE) at 27 percent.

FIGURE 70

MSSP CUSTOMER DEMAND

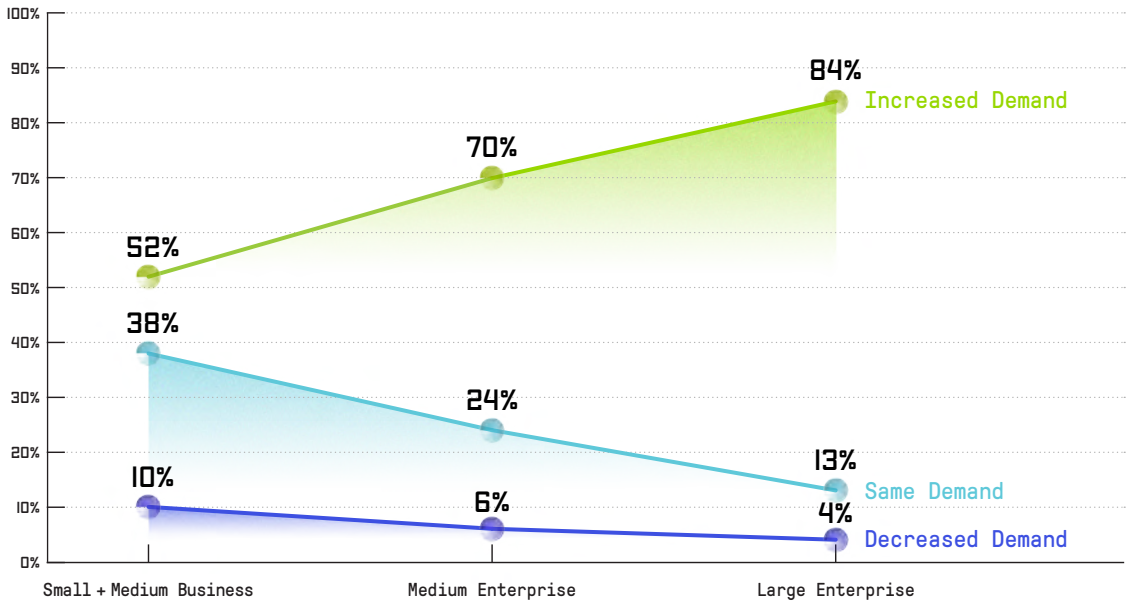
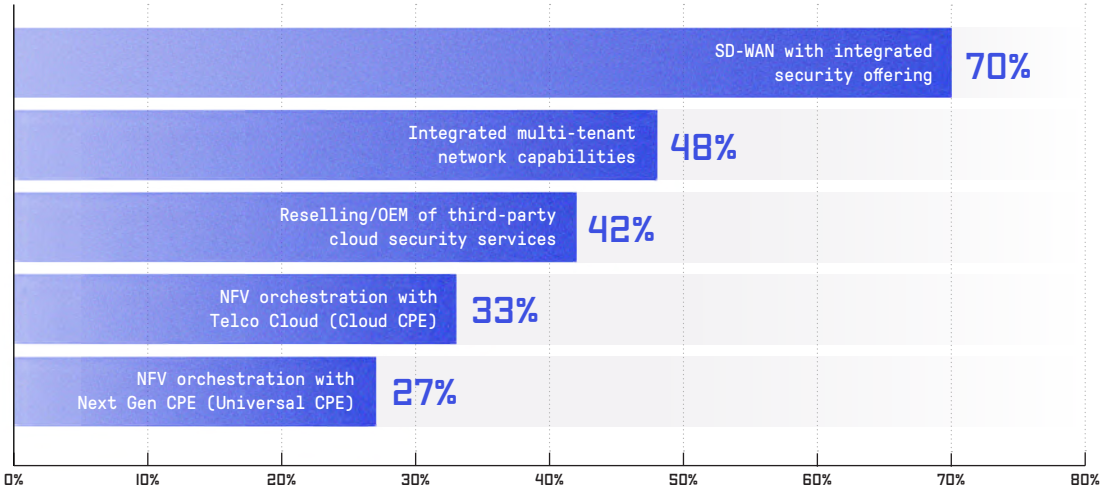


FIGURE 71

MSSP TECHNOLOGY EXPANSION



SERVICE PROVIDER DNS

Among service providers that operate a DNS infrastructure, the majority rely on their primary security teams to secure the service. We are encouraged to see that 29 percent had specialized security for DNS, up from 25 percent in 2017 (Figure 72). Similar to the previous year, 17 percent had no security personnel responsible for this critical infrastructure in 2018. This is unfortunate considering the potential for both service disruption and weaponization.

Visibility of DNS traffic improved overall in 2018. Identical to 2017, 74 percent had visibility at Layers 3 and 4 (Figure 73). At Layer 7, the picture was even better with 38 percent reporting visibility compared with 33 percent in 2017. Another bright spot was the decrease in those reporting no visibility, which was down from 15 percent in 2017 to only 7 percent in 2018.

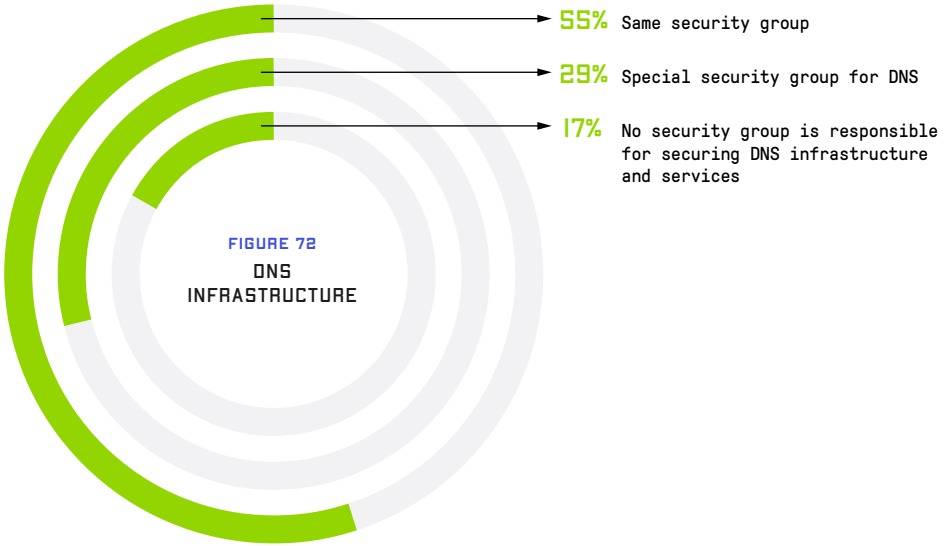
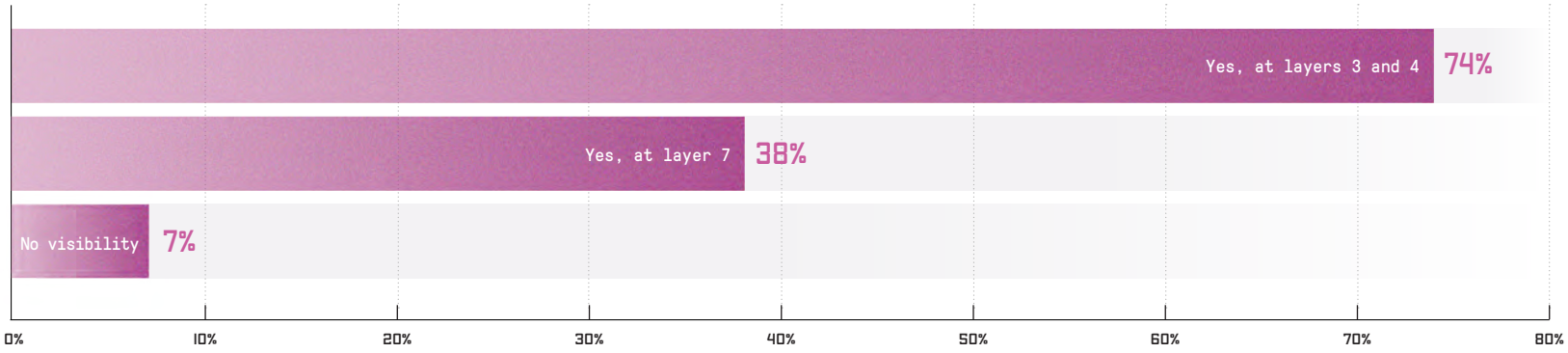


FIGURE 72
DNS INFRASTRUCTURE

FIGURE 73
DNS TRAFFIC VISIBILITY



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 and as unwilling amplification and reflection actors. As a result, it is disappointing to note that 19 percent still did not restrict access to their recursive DNS servers, indicating no progress from 2017 (Figure 74).

FIGURE 74

RECURSIVE DNS LOOKUPS

81%

Yes, we restrict recursive DNS

19%

No, we have open DNS resolvers

In a reversal from 2017, DDoS attacks targeted recursive DNS servers more frequently than authoritative servers in 2018 (Figure 75). Only 26 percent reported attacks against their authoritative DNS servers, compared to 44 percent in 2017. Thirty-six percent saw attacks against their recursive DNS servers, up slightly from 34 percent in 2017. Only about one quarter reported publicly visible outages of the DNS infrastructure due to DDoS attacks, down from 31 percent 2017. While DNS operators made some progress in protecting their infrastructure, DDoS attacks targeting DNS servers remain a constant threat.

FIGURE 75

DNS INFRASTRUCTURE ATTACKS

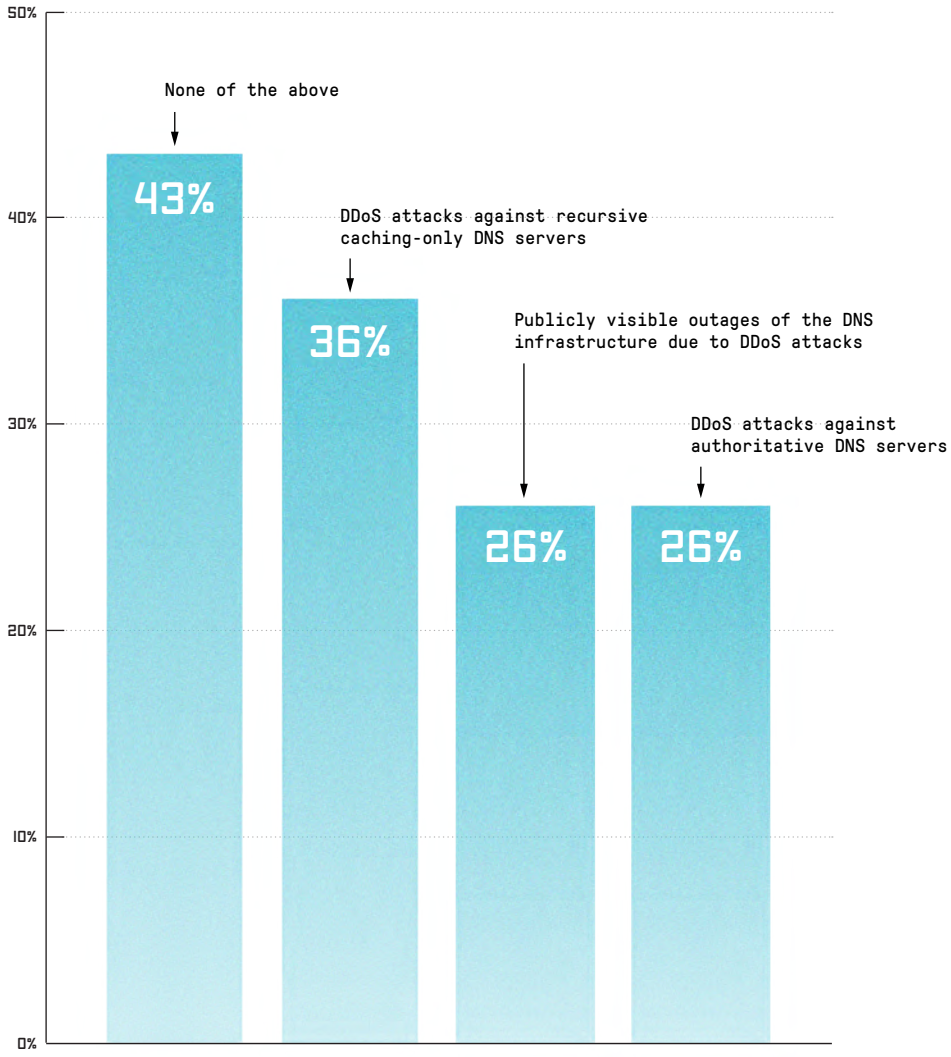
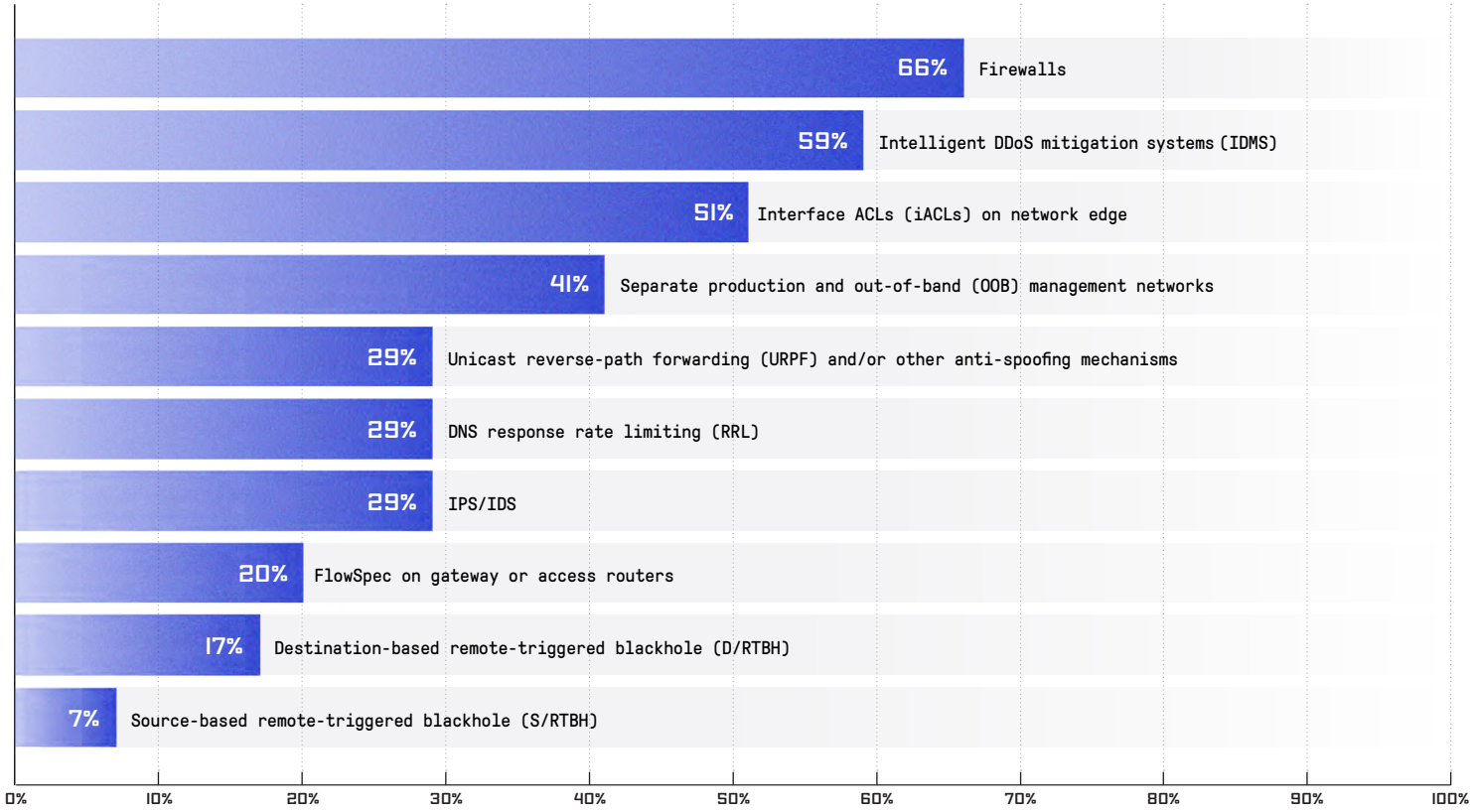


FIGURE 76

SECURITY MEASURES



The security measures put in place to protect DNS infrastructures vary greatly. For the first time in several years, firewalls were the most popular defense mechanism, with 66 percent deploying them, up from 61 percent in 2017 (Figure 76). Falling from first to second place in 2018 was IDMS at 59 percent, down from 66 percent in 2017. Interface ACLs retained third place at 51 percent. Seeing firewalls as the most reported option is concerning, as these devices do not protect adequately against DDoS attacks due to the ease with which a state-based attack can overwhelm them.

ATLAS SPECIAL REPORT

NETSCOUT ACTIVE THREAT LEVEL ANALYSIS SYSTEM (ATLAS®) DELIVERS A TRULY COMPREHENSIVE VIEW INTO INTERNET TRAFFIC, TRENDS, AND THREATS.

With visibility into one-third of all internet traffic, we are ideally positioned to deliver actionable intelligence about botnets, DDoS attacks and malware that threaten internet infrastructure and network availability.

KEY FINDINGS

ATTACK SIZE JUMPS GLOBALLY; ATTACK FREQUENCY VARIES BY REGION

In 2018, we saw the emergence of the Terabit Attack Era with multiple terabit-sized attacks in the first quarter of the year. The size of DDoS attacks is growing at an alarming pace all around the world, with significant implications for networks operators of all sizes, from global service providers to emerging enterprises (Figure 77).

As discussed throughout the report, this increase in attack size is being driven by the use of reflection/amplification techniques that allow cyber attackers to both magnify the amount of malicious traffic they can generate and obfuscate the sources of that attack traffic. This combination has been irresistible to attackers, and for good reason.

2018 DDoS ATTACKS BY REGION

- **ASIA PACIFIC:** 2.3 million
- **EUROPE, MIDDLE EAST + AFRICA:** 1.7 million
- **NORTH AMERICA:** 1.6 million
- **LATIN AMERICA:** 503,000

COLD COMFORT

Globally, the number of DDoS attacks was down 4% year over year, to 6.13 million. Despite that sliver of good news, that equals:

- 16,794 attacks **PER DAY**
- 699 attacks **PER HOUR**
- 11 attacks **PER MINUTE**

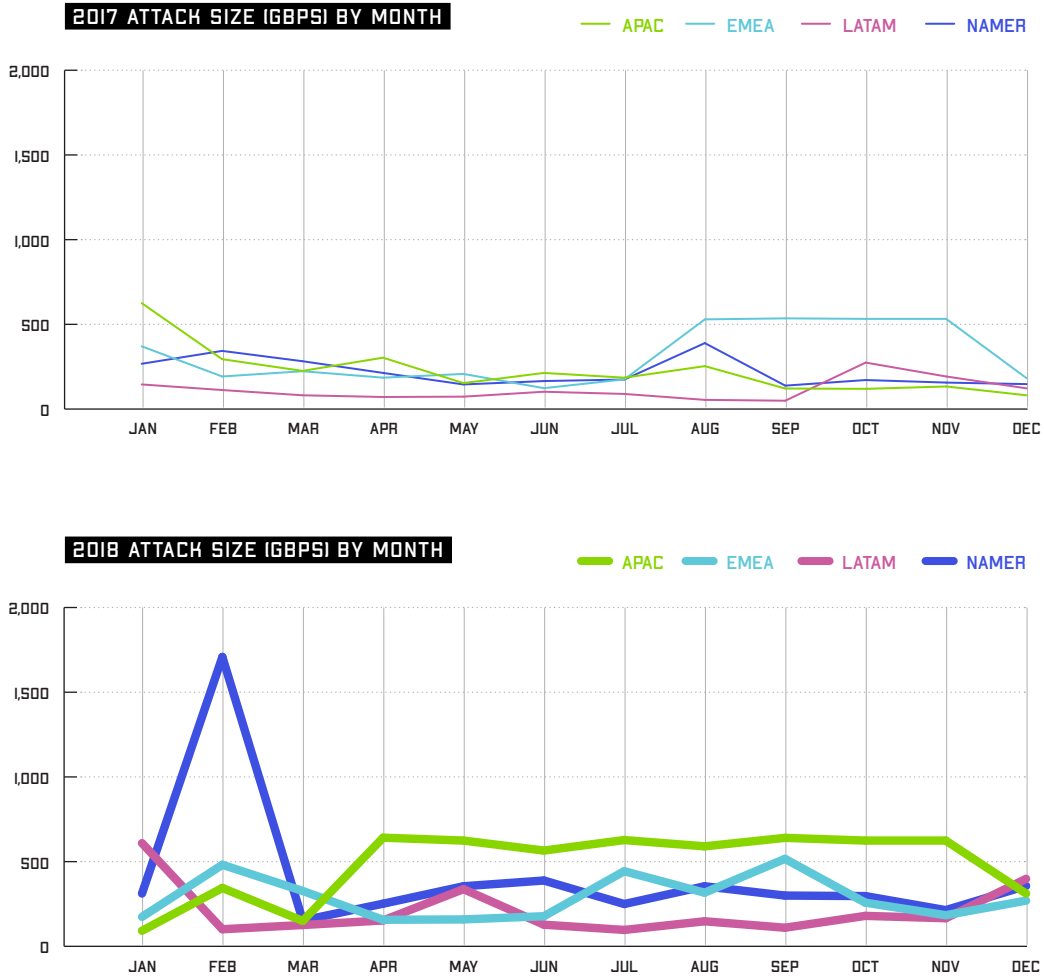


FIGURE 77

GLOBAL ATTACK SIZE (GBPS) BY MONTH 2017 VS. 2018

ASIA PACIFIC

FIGURE 78

APAC ATTACK SIZE (GBPS) BY MONTH 2017 VS. 2018

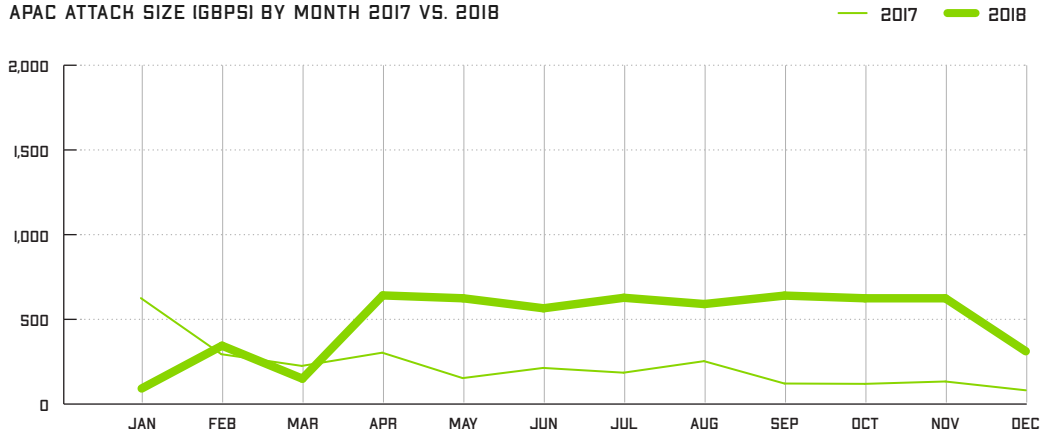
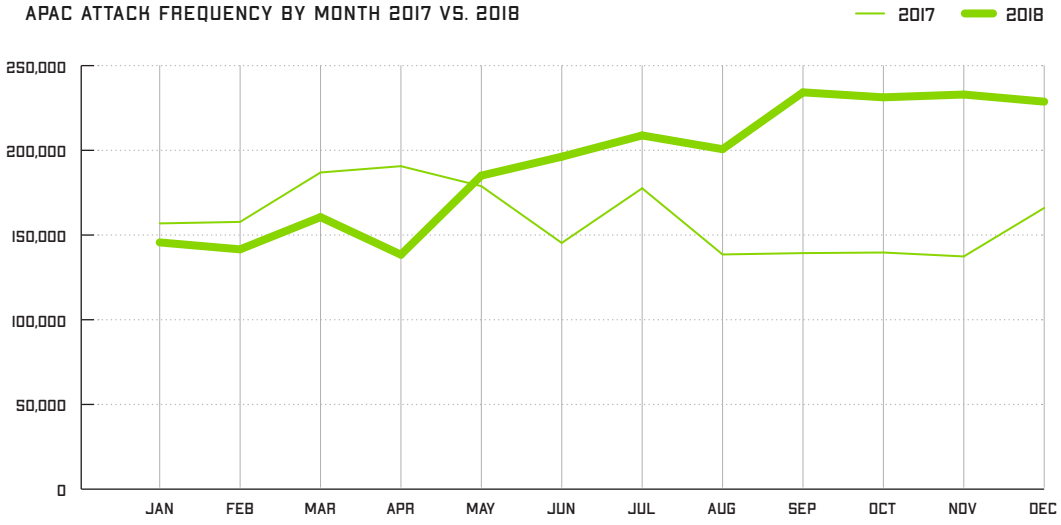


FIGURE 79

APAC ATTACK FREQUENCY BY MONTH 2017 VS. 2018



ASIA PACIFIC BECOMES THE MOST TARGETED REGION

2018

The most targeted region was Asia Pacific with 2.3 million attacks.

2017

The most targeted region was EMEA with an identical 2.3 million attacks.

LARGEST DDoS ATTACK IN 2018

631.9 GBPS

▲ Up 1.52% from 2017

Don't let that fool you. There was in fact a dramatic increase in attack size that was sustained month after month throughout the course of 2018 all across the region.

- Six different months saw attacks greater than 600 Gbps.
- Two more months saw attacks north of 500 Gbps.
- In total, ten months saw attacks greater than 300 Gbps.

To put that in perspective, in 2017, there were only two attacks larger than 300 Gbps.

ATTACK FREQUENCY

▲ Up 16.9% overall

The Asia Pacific region saw the greatest rise in DDoS attack frequency.

EUROPE, MIDDLE EAST + AFRICA

FIGURE 80

EMEA ATTACK SIZE (GBPS) BY MONTH 2017 VS. 2018

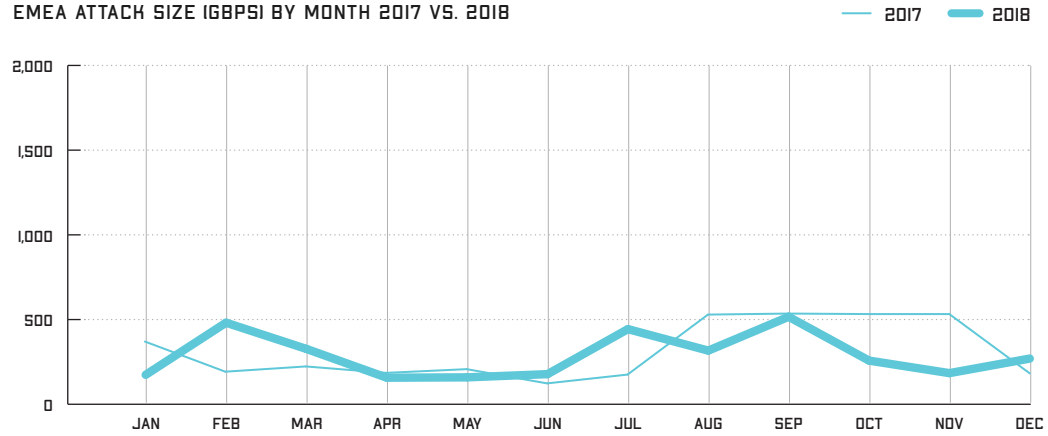
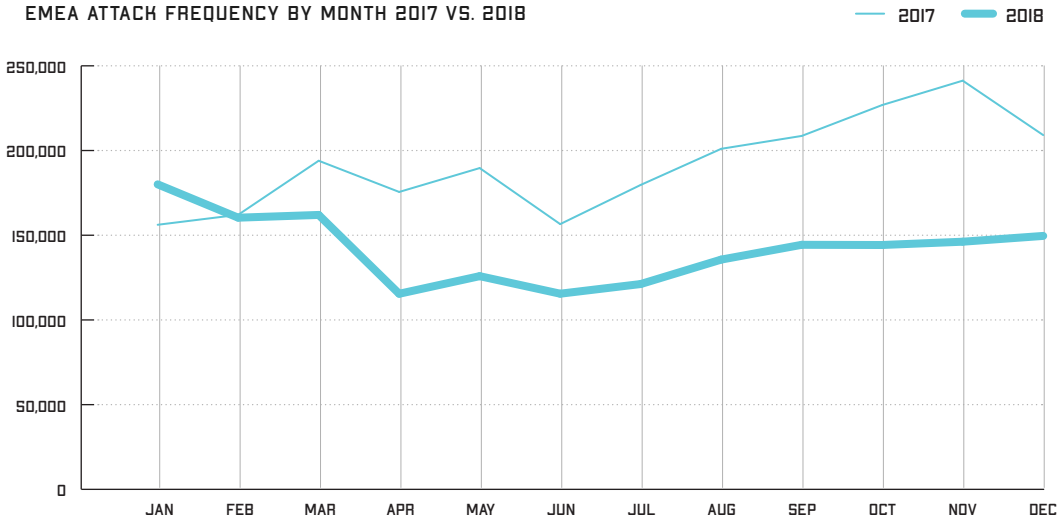


FIGURE 81

EMEA ATTACK FREQUENCY BY MONTH 2017 VS. 2018



LARGEST DDoS ATTACK IN 2018

506.5 GBPS

▼ Down from 531.7 Gbps in 2017

Interestingly, both attacks took place in September.

ATTACK FREQUENCY

▼ Down 26% overall

But it was very consistent throughout the course of the year.

JANUARY: MOST ATTACKS

180,035

APRIL: FEWEST ATTACKS

115,450

AVERAGE PER MONTH

141,692

In 2017, in the 1H of the year, attack frequency was very similar to 2018 numbers, however:

AUGUST–DECEMBER

▲ Number of attacks up 20%

AVERAGE PER MONTH

217,365

LATIN AMERICA

FIGURE 82

LATAM ATTACK SIZE (GBPS) BY MONTH 2017 VS. 2018

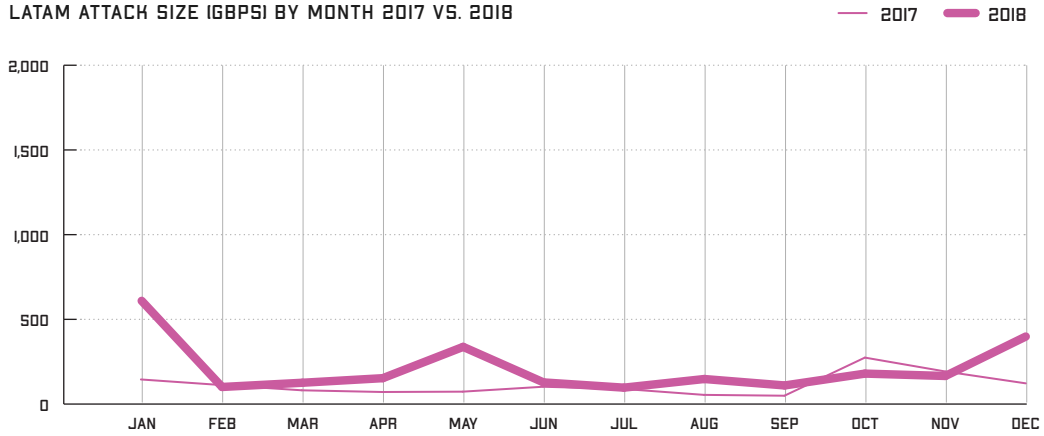
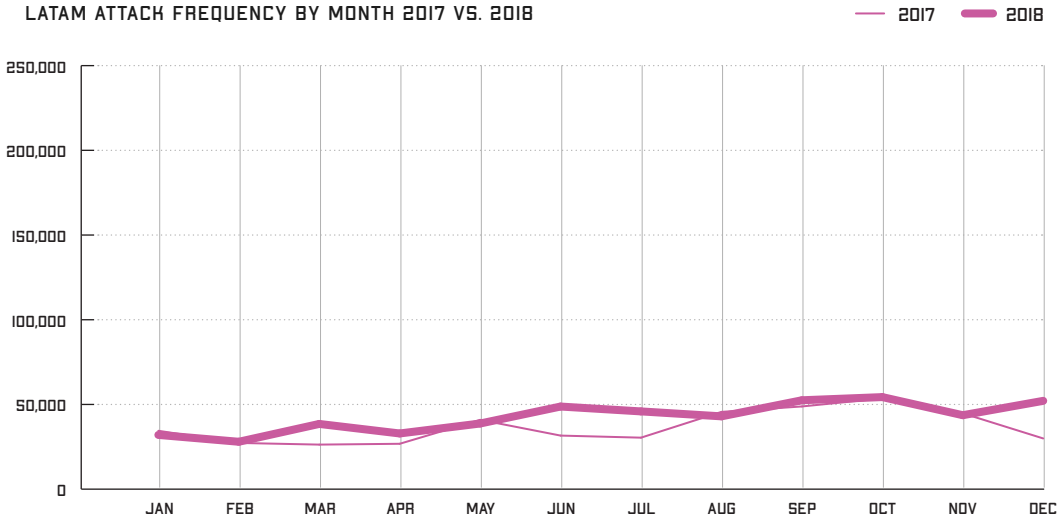


FIGURE 83

LATAM ATTACK FREQUENCY BY MONTH 2017 VS. 2018



LARGEST DDoS ATTACK IN 2018

600.0 GBPS

▲ Up 55% from 270.6 Gbps in 2017

ATTACK SIZE

▲ Up 45% overall

This dramatic increase in DDoS attack size was consistent throughout the year. Looking at the largest DDoS attacks each month and taking their average size, they were larger in 2018 than in 2017.

ATTACK FREQUENCY

▲ Up 13.9% overall

Along with Asia Pacific, Latin America was the only other region to see a rise in DDoS attack frequency.

AVERAGE PER MONTH

41,938

NORTH AMERICA

FIGURE 84

NAMER ATTACK SIZE (GBPS) BY MONTH 2017 VS. 2018

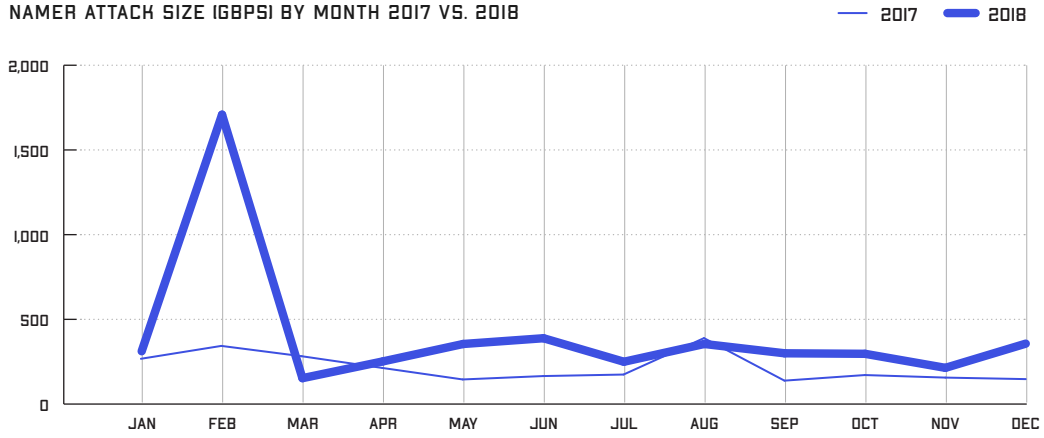
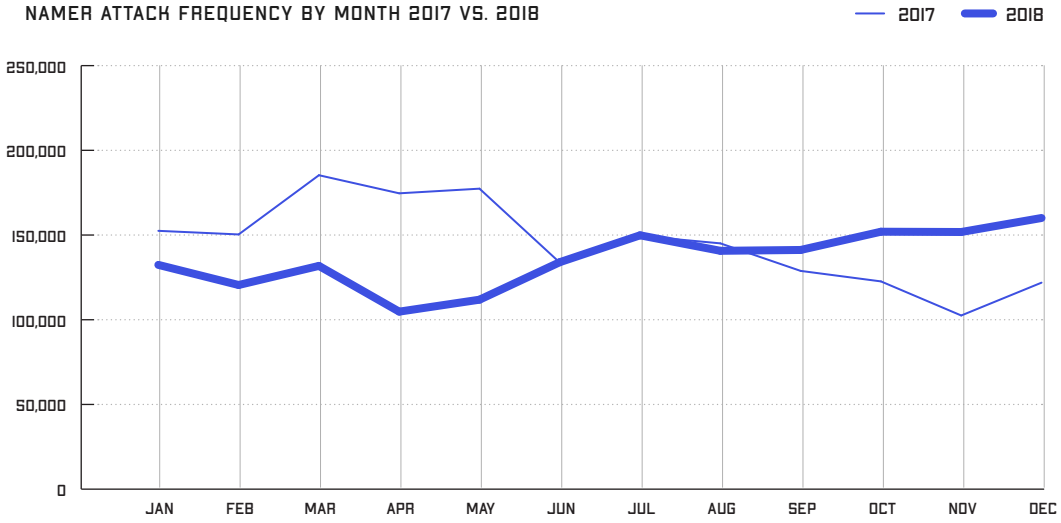


FIGURE 85

NAMER ATTACK FREQUENCY BY MONTH 2017 VS. 2018



LARGEST DDoS ATTACK IN 2018

1.7 TBPS

▲ Largest attack in history was recorded in February 2018

ATTACK SIZE

379 GBPS

Was the next largest attack

Overall, attack size was up consistently throughout the year.

→ Only two months had larger attacks in 2017 than in the corresponding month in 2018.

→ In five different months, the largest attack was more than 2X as big as the same period a year earlier.

ATTACK FREQUENCY

▼ Down 4% overall

TOTAL ATTACKS IN 2018

6.13 MILLION

CONCLUSION

WE'VE PASSED A LANDMARK THIS YEAR, AND IT'S NOT A GOOD ONE.

But entering the Terabit Era of DDoS attacks is just one indicator of the dramatic and persistent increase in DDoS attack size and complexity reported by WISR respondents. With a global max attack size increase of 273 percent in 2018, there are clearly significant implications and new challenges for enterprises and service providers alike.

In 2018, enterprise respondents continued to wrestle with challenges such as ransomware, insider threats, and DDoS attacks, all while struggling to simplify operations. At the same time, attackers increasingly targeted important components of digital transformation initiatives, such as SaaS and cloud services. As companies place growing importance on doing business in a connected world, it's not surprising to see that attackers have followed.

Service providers faced similar issues when it came to protecting cloud-based services, as we saw the number of attacks on these services jump significantly. These companies increasingly turned to external sources for security help, as many face an ongoing challenge in building and maintaining skilled security teams. Finally, we saw an increase in DDoS attacks on the public sector; a clear reflection of ongoing political instability around the world.

As the survey results show, both enterprises and service providers must find a way to minimize risk while still delivering and safeguarding the digital services that drive our connected world. We hope that the insights in this report help network operators understand the breadth of the threats that they face, and gain valuable insight to navigate an increasingly complex threat landscape.

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 on Twitter, Facebook, or LinkedIn.

SECR_005_EN-1901 – WISR

NETSCOUT®