2016 CYBERTHREAT DEFENSE REPORT

NORTH AMERICA
EUROPE
ASIA PACIFIC
LATIN AMERICA

Research Sponsors

PLATINUM

BLUE COAT | CITRIX | CODE42 | IMPERVA

GOLD

FIDELIS CYBERSECURITY | invincea | LogRhythm | MICRO FOCUS | NetIQ | WEBROOT

SILVER

CloudLock | GURUCUL PREDICTIVE SECURITY ANALYTICS | IKANOW | SentinelOne | THREATQ

Table of Contents

Introduction

The first two installments of the Cyberthreat Defense Report began the process of looking beyond major breaches and the never-ending evolution of cyberthreats to better understand what IT security teams are doing to defend against them. Highlights of what we learned from those reports include:

- One in four security professionals doubts their organization has invested adequately in cyberthreat defenses (2014).
- Mobile devices and social media applications are IT security's "weakest links" (2015).
- More than two-thirds of organizations are looking to replace or augment their endpoint security tools (2015).

The third-annual Cyberthreat Defense Report pursues this same objective: to inform the IT security community not so much about what the bad guys are up to, but rather about how their peers globally are currently defending against threats and the changes they expect to make going forward. Based on a rigorous survey of IT security decision makers and practitioners – across not only North America and Europe, but for the first time, in Asia Pacific and Latin America as well – the Cyberthreat Defense Report examines the current and planned deployment of countermeasures against the backdrop of numerous perceptions, such as:

- The adequacy of existing cybersecurity investments, both overall and within specific domains of IT
- The likelihood of being compromised by a successful cyberattack
- The types of cyberthreats that pose the greatest risk to the organization
- The organizational factors that present the most significant barriers to establishing effective cyberthreat defenses
- The operational, tactical, and strategic value that individual security technologies provide

By revealing these details, we hope to give IT security decision makers a better understanding of how their perceptions, concerns, priorities, and – most important – current defensive postures stack up against those of other IT security professionals and their organizations. Applied in a constructive manner, the data, analyses, and findings covered here can be used by diligent IT security teams to shape answers to many practical (if not pressing) questions, such as:

- Where do we have gaps in our cyberthreat defenses relative to other organizations?
- Have we fallen behind in our defensive strategy to the point where our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative defensive weaknesses)?
- Are we on track with both our approach and progress in continuing to address traditional areas of concern, such as strengthening endpoint security and reducing our attack surface? And what about our investments in other/newer areas that are becoming increasingly important, such as providing adequate protection for mobile users, providing data protection for cloud applications, and leveraging threat intelligence services?
- How does our level of spending on IT security compare to that of other organizations?
- How are other IT security practitioners thinking differently about cyberthreats and their defenses, and should we adjust our perspective and plans to account for these differences?

SURVEY DEMOGRAPHICS:

- **1,000 qualified IT security decision makers and practitioners**
- **All from organizations with more than 500 employees**
- **Representing 10 countries across North America, Europe, Asia Pacific, and Latin America**
- **Representing 19 industries**

Introduction

Another important objective is to provide developers of IT security technologies with some of the answers they need to better align their solutions with the concerns and requirements of potential customers. The net result should be better market traction and success for solution providers that are paying attention, along with better cyberthreat protection technologies for all of the intrepid defenders out there.

The findings of this report are divided into four sections, as follows:

Section 1: Current Security Posture

The security foundation an organization has in place and the perception of how well it is working invariably shape future decisions about cyberthreat defenses, such as:

- Whether, to what extent, and how urgently changes are needed; and
- Specific types of countermeasures that should be added to supplement existing defenses.

Our journey into the depths of cyberthreat defenses begins, therefore, with an assessment of respondents' perception of the effectiveness of their organization's investments and strategies relative to the prevailing threat landscape. We also provide insight into the high-level definition of these strategies based on the types of technological countermeasures they incorporate.

Section 2: Perceptions and Concerns

Our exploration of cyberthreat defenses then shifts from establishing baseline security postures to determining the types and sources of cyberthreats that concern today's organizations the most. Like the perceived weaknesses identified in the previous section, these concerns serve as an important indicator of where and how it best makes sense for organizations to improve their cyberthreat defenses going forward.

This section of the report also investigates the reasons for obtaining third-party threat intelligence, operating SIEM solutions, and investing in cloud access security brokers (CASB) – along with the factors that most often inhibit today's organizations from establishing adequate cyberthreat defenses.

Section 3: Attack Surface Reduction

Establishing effective cybersecurity defenses requires more than simply implementing next-generation technologies designed to detect the latest wave of elusive cyberthreats. In fact, given that most breaches today result from threat actors' exploiting known vulnerabilities and/or configuration-related weaknesses, it's completely reasonable to suggest that a more sensible strategy is to reduce one's attack surface first, and then use an overlapping set of detection-focused countermeasures to mitigate the residual risk.

Tactics that help organizations with the first part of this strategy – reducing their attack surface – include:

- Reducing the number of open ports and services on Internet-facing systems
- Using next-generation firewalls and CASBs to granularly control access to network and cloud-based computing resources
- Eliminating all unnecessary protocols and services running on endpoints, servers, and other internal systems
- Leveraging identity and access management solutions to implement a least-privileges policy

This section of the report examines a few other relevant tools and tactics that can also be applied in this regard, including network access control (NAC) and file integrity monitoring (FIM) technologies, full-network scans for vulnerable systems, and strategies for remediating malware-infected devices.

Section 4: Future Plans

Organizations can ill afford to stand still when it comes to maintaining effective cyberthreat defenses. IT security teams must keep pace with the changes around them by making changes of their own. Some of their intentions will be revealed in Section 2, where we cover the network, endpoint, mobile, and application security technologies planned for acquisition in 2016. This section further explores their plans for the future.

Research Highlights

Section 1: Current Security Posture

- **Security takes a bigger bite.** 85% of respondents are spending more than 5% of their IT budgets on security. Nearly a third are spending more than 16% (page 6).
- **Rising attacks, dwindling optimism.** 76% were affected by a successful cyberattack in 2015, while only 62% expect to fall victim again in 2016 (page 7).
- **Mobile devices are the weakest link.** For the third consecutive year, mobile devices are perceived as IT security's weakest link, closely followed by social media applications (page 9).
- **Must-have network security investments.** Next-generation firewalls are the top-ranked network security technology planned for acquisition in 2016, followed by threat intelligence services and user behavior analytics (page 10).
- **Massive exposure to SSL blind spots.** Only a third of respondents have the tools necessary to inspect SSL-encrypted traffic for cyberthreats (page 12).
- **Critical laptop backup negligence.** Only one in five regularly backs up more than 80% of mobile users' laptops (page 13).
- **Shielding endpoints from cyberthreats.** Containerization/micro-virtualization tops the rankings for both endpoint security and mobile security technologies that respondents plan to acquire in 2016 (page 14).
- **Failure to monitor privileged users.** Only 30% of respondents are confident that their organization has made adequate investments to monitor the activities of privileged users (page 18).

Section 2: Perceptions and Concerns

- **Threats keeping us up at night.** Malware, phishing, and SSL-encrypted threats give IT security the most headaches (page 19).
- **Mobile threats on the rise.** 65% of respondents experienced an increase in mobile threats over the past year (page 20).
- **Leveraging CASBs to protect sensitive data.** Preventing disclosure of sensitive data is the leading reason why organizations are deploying CASBs (page 23).
- **Employees are still to blame.** Low security awareness among employees continues to be the greatest inhibitor to defending against cyberthreats, followed closely by too much data for IT security teams to analyze (page 24).

Section 3: Attack Surface Reduction

- **NAC extends its reign.** NAC remains the top technology for reducing a network's attack surface (page 26).
- **Ignorance is bliss.** Less than 45% of organizations conduct full-network active vulnerability scans more than once per quarter (page 27).
- **Working harder – not smarter.** Nearly a third continue to rely on manual efforts to remediate malware-infected hosts (page 28).

Section 4: Future Plans

- **Security budgets still rising.** Nearly three-quarters of IT security budgets are expected to rise in 2016 (page 29).
- **BYOD backpedaling.** The percentage of organizations with BYOD policies has dropped for the third consecutive year. IT organizations are not keeping their promises to roll out new BYOD implementations (page 30).
- **Fed up with inadequate endpoint defenses.** 86% are looking to replace or augment current endpoint protection tools (page 31).

Section 1: Current Security Posture

IT Security Budget Allocation

What percentage of your employer's IT budget is allocated to information security (e.g., products, services, personnel)? (n=977)

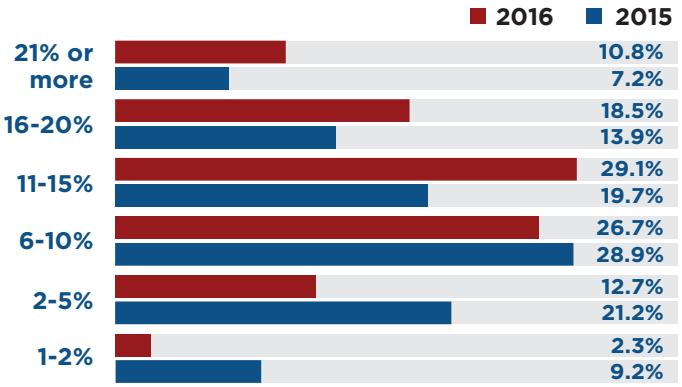


Figure 1: Percentage of IT budget allocated to security.

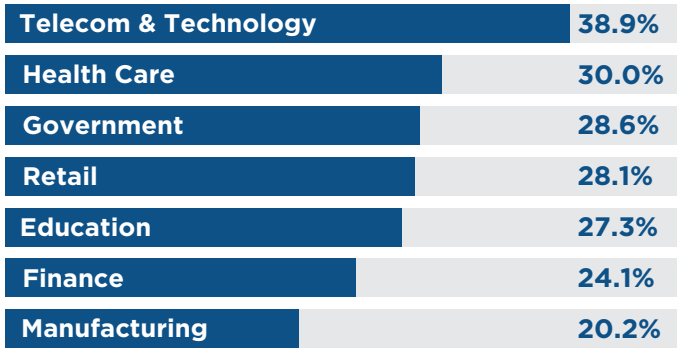


Figure 2: Percentage spending 16% or more on security.

Budgets for information security products, services, and personnel are not only healthy in an absolute sense, but also are trending in a positive direction. Up from 70% a year ago, a remarkable 85% of respondents indicated their organization is now committing in excess of 5% of the IT budget to security (see Figure 1). Even more noteworthy, nearly a third (30%) claimed their organization is now spending north of 16% on security. At the same time, the group investing less than 2% of the IT budget on security shrank markedly, from just over 9% a year ago, to a scant 2.3% this time around.

Overall, we see these results as reinforcing anecdotal evidence that IT security is now receiving board-level attention at more organizations than ever before. As the importance of strong cyberthreat defenses to the success of the modern business gains wider recognition at the highest levels within today's organizations, security funding is, quite naturally, starting to increase. IT security teams must not squander this windfall, or the accompanying opportunity to transition their security apparatus from a cost of doing business to an enabler of the business.

Other notable findings:

- Geographically, Mexico (61.9%) and Brazil (49.1%) have the greatest percentage of organizations spending in excess of 16% of their IT budgets on security. This result may reflect their attempt to catch up after historically under-investing in security, as opposed to getting ahead of organizations in other countries.
- The finance vertical (24.1%) ranks among the lowest of the "big 7 industries" (education, finance, government, health care, manufacturing, retail, and technology) whose organizations are spending more than 16% of IT budget on security. This finding may reflect the approaching "steady state" of spending, given that segment's historically high relative level of security investment (see Figure 2).
- The very largest organizations (>25,000 employees) are spending proportionally more on security than their smaller counterparts (<5,000 employees), with 47.1% of the former investing more than 16% of their IT budget compared to less than half that many for the latter.

"Overall, we see these results as reinforcing anecdotal evidence that IT security is now receiving board-level attention at more organizations than ever before."

Section 1: Current Security Posture

Past Frequency of Successful Cyberattacks

How many times do you estimate that your organization's global network has been compromised by a successful cyberattack within the past 12 months? (n=943)

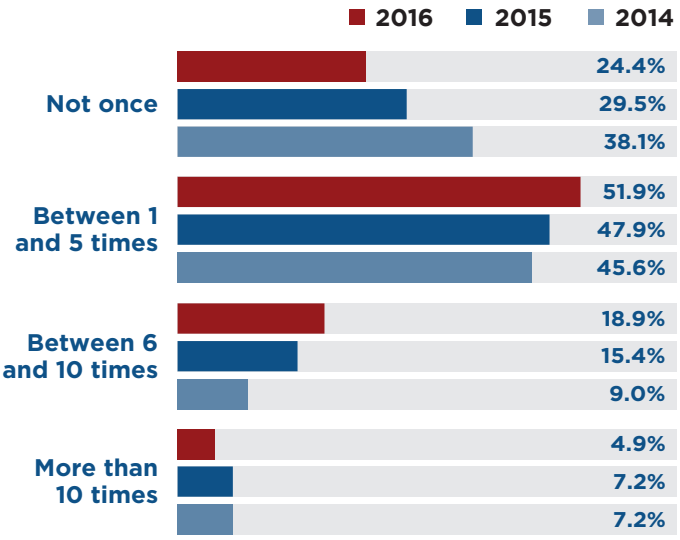


Figure 3: Frequency of successful attacks in the past 12 months.

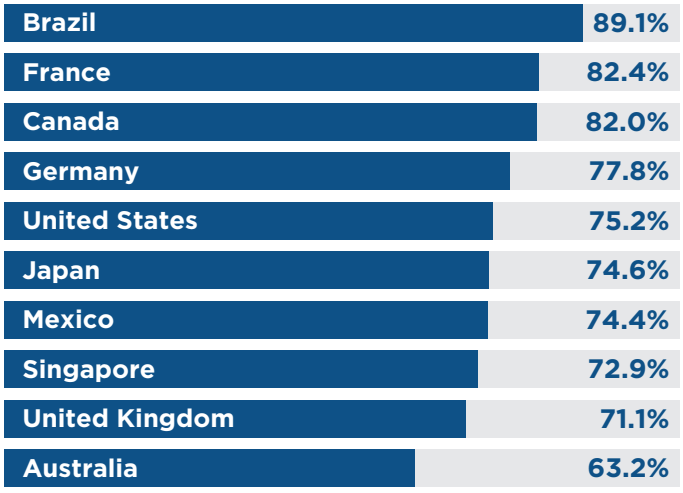


Figure 4: Percentage compromised by at least one successful attack in the past 12 months.

There's arguably no greater motivating factor for continued investments in cyberthreat defenses than a successful cyberattack.

The good news from our respondents is that the frequency at which they're getting hit is, for the most part, holding steady (see Figure 3). Sure, the statistics for organizations that suffered at least one successful attack in the past 12 months edged up a bit, to 75.6% (from 70.5% a year earlier). And for the first time, more than half (51.9%) of responding organizations fall into the unenviable category of having been breached between once and five times in the prior 12 months. But those being victimized "more than 10 times" actually dropped year over year, from 7.2% to 4.9%. Go team!

Digging a bit deeper into the data, we can also report that Australian organizations are faring the best in two areas: they were most likely to avoid falling victim to a cyberattack even once (36.8%; see Figure 4)

"And for the first time, more than half (51.9%) of responding organizations fall into the unenviable category of having been breached between once and five times in the prior 12 months."

and were next to last in likelihood (1.2%) of being hit more than 10 times. A related side note: not a single French respondent reported their organization was successfully attacked more than 10 times in the past 12 months!

In addition, larger organizations (>10,000 employees) are being hit "6 times or more" at roughly twice the rate of their smaller counterparts. This is not particularly surprising when you consider that larger organizations are likely to have a substantially greater attack surface to defend.

Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2016? (n=978)

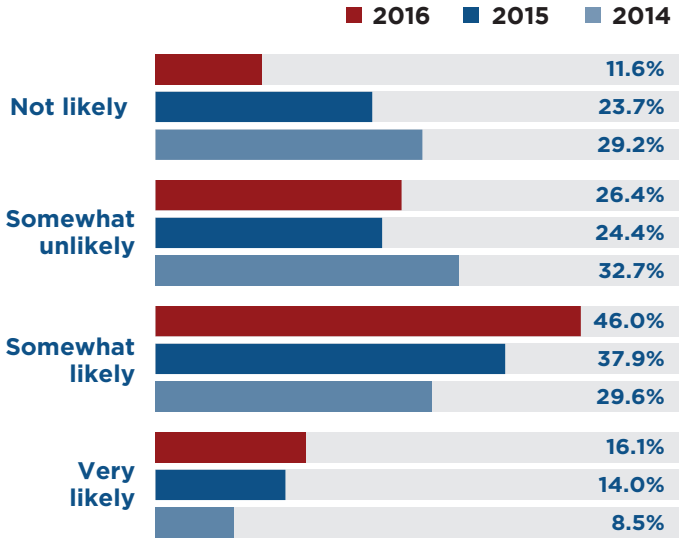


Figure 5: Likelihood of being successfully attacked in the next 12 months.

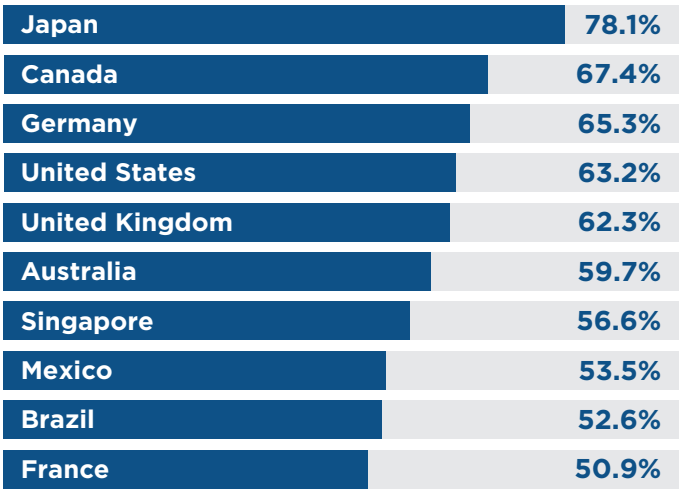


Figure 6: Percentage indicating compromise is "more likely to occur than not" in the next 12 months.

When asked about the likelihood that their organization's network would be compromised in the coming year, respondents were, for the third year in a row, more optimistic than would seem warranted. Despite more than three-quarters' indicating their organization's computing environment had been compromised within the past year (see Figure 3), only 62% considered it "somewhat likely" or "very likely" that it would happen again over the next 12 months (see Figure 5).

That said, there are signs that pessimism – or perhaps it's realism – is increasing among respondents, at least in relative terms. To begin with, the differential in the two statistics from above – reflecting the prior year's actual occurrence of breaches compared to the next year's expected occurrence of breaches – has steadily decreased in each of the past three years, from a high of 23.0% to the current low of 13.5%. In other words, the degree of optimism is shrinking.

"...there are signs that pessimism – or perhaps it's realism – is increasing among respondents..."

Further reinforcing this point is the finding that only 11.6% of respondents consider it "not likely" that their organizations will be breached in 2016, compared to nearly one quarter who expressed that same expectation for 2015.

Not surprisingly, the breakdown by country of respondents who consider it more likely than not that their organizations will be compromised in the coming year (see Figure 6) tracks closely with the data on successful breaches experienced over the past 12 months (see Figure 4). Japan, Canada, Germany, and the United States remain near the top of each chart, while France claims the coveted last (and most secure) spot in both cases.

Security Posture by IT Domain

On a scale of 1 to 5, with 5 being highest, rate your organization's overall security posture (ability to defend cyberthreats) in each of the following areas: (n=990)

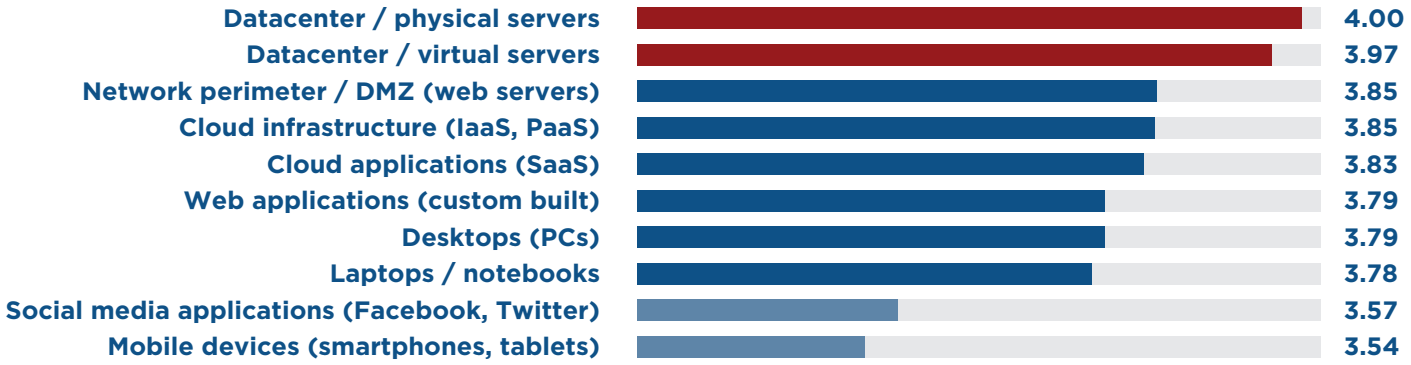


Figure 7: Perceived security posture by IT domain.

Data on the perceived ability to defend against cyberthreats in different IT domains (see Figure 7) helps inform priorities for future spending on security technology and services.

While respondents expressed relatively high confidence in their defenses for both physical and virtual servers, our results found client devices of all types – but especially mobile devices – present the greatest security challenge to today's organizations. This result makes perfectly good sense to us: IT can be expected to be better at securing resources over which it has greater control (e.g., servers) than those it does not (e.g., mobile devices).

Other findings of interest:

- Establishing adequate protection for/from social media applications such as Facebook and Twitter remains a relative weak spot in organizations' defenses.
- There is no significant difference in the perceived security posture for homegrown web applications compared to cloud-sourced applications (SaaS).
- Similarly, there is negligible perceived difference in the ability of respondents' organizations to protect different flavors of cloud services (i.e., IaaS/PaaS vs. SaaS).

"...our results found client devices of all types – but especially mobile devices – present the greatest security challenge to today's organizations."

In addition, it would be remiss of us not to mention that the findings from this year were nearly identical to those from last year – well, sort of. To clarify, while the order in which the different IT domains are ranked is virtually unchanged from last year – with only the entries for web and cloud applications flip-flopping – the weighted scores received by each domain are, in fact, significantly different. Indeed, scores jumped across the board, from a low (but still substantial) 0.40 increase for "network perimeter" to a whopping 0.85 increase for "laptops/notebooks." Even "mobile devices" had a healthy bump, up 0.79 to 3.54.

What can we say? Apparently, our respondents are starting to feel pretty good about the investments they've made in each of these areas over the past few years. As for whether this becomes a trend – or, more importantly, translates into an appreciable decline in successful cyberattacks in the coming years – we'll just have to wait and see.

Section 1: Current Security Posture

Network Security Technology Deployment Status

Which of the following network security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard all network assets against cyberthreats? (n=982)

2016

	Currently in use	Planned for acquisition	No plans
Network-based antivirus	69.9%	22.7%	7.4%
Advanced malware analysis / sandboxing	63.7%	26.6%	9.7%
Secure email gateway (SEG)	62.2%	27.4%	10.4%
Secure web gateway (SWG)	61.5%	26.5%	12.0%
Web application firewall (WAF)	61.4%	29.6%	9.0%
Data loss/leak prevention (DLP)	61.1%	29.1%	9.9%
Denial of service (DoS) / distributed denial of service (DDoS) prevention	60.7%	27.0%	12.3%
Intrusion detection / prevention system (IDS/IPS)	59.8%	29.9%	10.4%
Security information and event management (SIEM)	53.3%	34.2%	12.6%
Security analytics / full-packet capture and analysis	52.2%	35.5%	12.3%
Network behavior analysis (NBA) / NetFlow analysis	49.6%	33.5%	16.9%
User behavior analytics / activity monitoring	48.4%	35.9%	15.7%
Next-generation firewall (NGFW)	47.9%	41.2%	10.9%
Threat intelligence service	45.0%	38.1%	16.9%

Table 1: Network security technologies in use and planned for acquisition.

Participants were requested to designate a deployment status – currently in use, planned for acquisition within 12 months, or no plans – for a specified list of network security technologies. (Endpoint and mobile security technologies are addressed in a subsequent section.)

Table 1 provides a visual and numerical representation of the responses. Percentages in darker shades correspond to higher frequency of adoption and/or acquisition plans. Percentages in lighter shades correspond to lower adoption and/or acquisition plans.

In last year's report we expressed our surprise that both web application firewalls and advanced malware analysis had relatively low adoption rates – just over 50% for each at the time. Well, it now appears that at least a few IT security decision makers agreed with our point that these seem like particularly worthwhile technologies to have, especially to counteract the increasing prevalence of targeted application-layer attacks and rising volume of advanced persistent threats (APTs).

Section 1: Current Security Posture

Network Security Technology Deployment Status

The technology with the biggest year-over-year increase in adoption rate: advanced malware analysis, up over 11 points to 63.7%. This increase comes at the expense of network-based antivirus (down more than 6%) and intrusion detection/prevention systems (down nearly 10%). Shining almost as brightly, web application firewalls enjoyed a 7-point increase in adoption rate (rising to 61.4%).

"The technology with the biggest year-over-year increase in adoption rate: advanced malware analysis, up over 11 points to 63.7%."

Other notable findings:

- Despite its declining rate of use, network antivirus remains atop the heap as the most frequently deployed network security technology in our list (at least for now).
- A healthy 10-point increase in its deployment frequency vaulted data loss prevention (DLP) to be among the leading technologies, from its former position near the bottom of the list.
- Next-generation firewall (NGFW) is the top-rated network security technology planned for acquisition in 2016.
- Threat intelligence services continue to exhibit a promising trajectory, with 38% of respondents signaling intent to acquire such a solution in 2016.
- With multiple flavors of analysis/analytics technologies (i.e., security, network, and user behavior) and SIEM rounding out the leader board for adoption in the coming year, it's clear that bolstering capabilities for monitoring and analyzing network traffic for the presence of cyberthreats remains a high priority for many organizations.

Our closing observation for this table is a favorable one for most security solution providers: for all but IDS/IPS, there was a decrease in the percentage of companies that indicated "no plans" to acquire each of the listed technologies within the next 12 months.

Inspection Capabilities for SSL-encrypted Traffic

Describe your agreement with the following statement: "My organization has the necessary tools to inspect SSL-encrypted traffic for cyberthreats." (n=994)

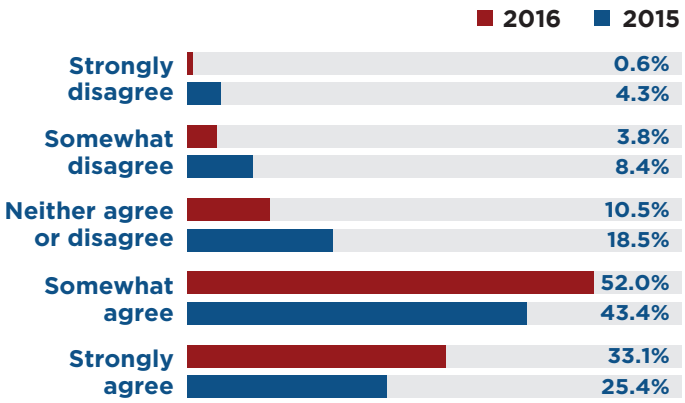


Figure 8: Availability of tools for inspecting SSL-encrypted network traffic.

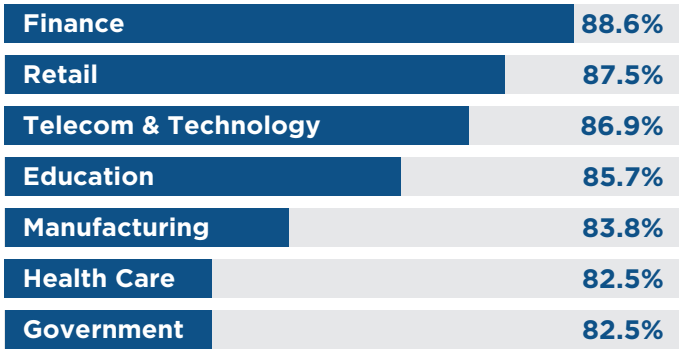


Figure 9: Percentage agreeing somewhat or strongly.

At first glance, the glass appears to be considerably more than half full when it comes to organizations' having the tools they need to inspect SSL-encrypted traffic for cyberthreats (see Figure 8). After all, an astonishing 85.1% responded with either "strongly agree" or "somewhat agree," suggesting that their organizations have this issue fairly well covered. In addition, this number represents a healthy bump from the year prior, when the combined tally for the same responses was just over two-thirds. So it would seem that today's organizations get it: SSL/TLS encryption is pervasive and inspecting this traffic for threats is important.

But hold the phone a second. If that's truly the case, then why, when we take a sneak peek ahead to Figure 13, do we see "SSL-encrypted threats" shown as one of the types of threats that most concern responding organizations? A logical conclusion is that there's still plenty of room for improvement in this area. For starters, let's not overlook the fact that over half of the respondents to this question

"...over half of respondents (52%) only 'somewhat agree' that their organizations have the necessary tools to inspect SSL-encrypted traffic."

(52%) only "somewhat agree" that their organizations have the necessary tools to inspect SSL-encrypted traffic. Tied into this, too, is the matter of coverage. It's very likely the case that most organizations use such tools primarily at the most obvious and critical junctions, such as web and cloud gateways. Are they truly being used everywhere they're needed at this point? Probably not.

A final observation on this topic is that the data also shows health care and government organizations lagging behind those from the other "big 7" vertical industries (see Figure 9). Why are we not surprised?

Section 1: Current Security Posture

Backup Practices for Mobile Users' Laptops

What percentage of laptops used by your mobile workforce are backed up regularly (daily or continuously) to guard against data loss due to cyberthreats? (n=983)

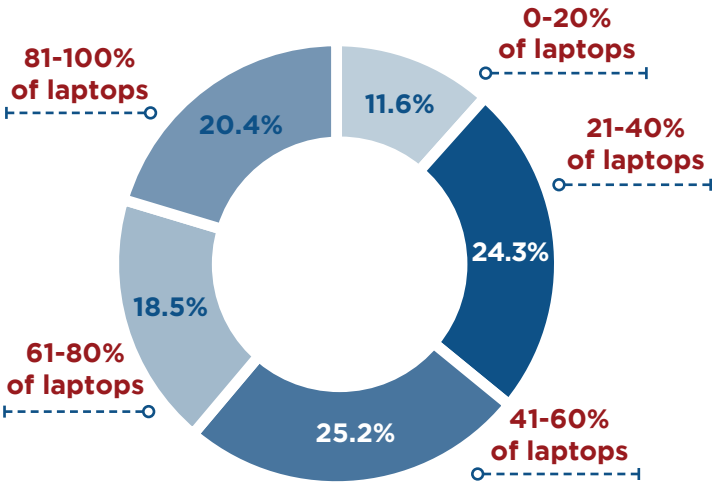


Figure 10: Percentage of mobile users' laptops backed up regularly.

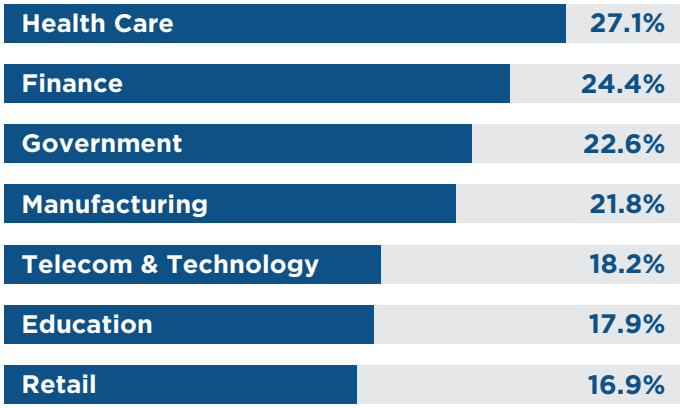


Figure 11: Percentage backing up 80% or more of mobile users' laptops.

"On a global basis, only one in five respondents reported their organization regularly backs up more than 80% of mobile users' laptops."

One of our new areas of investigation for this year's study was to gain some insight into the extent that organizations are backing up the laptops of their mobile users to help guard against data loss stemming from cyberthreats. The answer: not so much (see Figure 10).

On a global basis, only one in five respondents reported their organization regularly backs up more than 80% of mobile users' laptops. More than a third back up less than 40% of these highly exposed devices.

Other notable findings:

- French organizations trail those in other countries, with just under one in 10 conducting regular backups for more than 80% of their mobile users' laptops.
- Health care organizations lead other verticals, with more than a quarter regularly backing up more than 80% of mobile users' laptops (see Figure 11).
- Size of organization has little impact on the decision to back up laptops.

Given the number of easy-to-use, feature-rich, and relatively affordable solutions available in the market, it is somewhat inexplicable to us that laptop backup practices are currently so lackluster – and we hope to see this change when we ask again next year!

Endpoint and Mobile Security Deployment Status

Which of the following endpoint security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard desktops, laptops, and servers against cyberthreats? (n=988)

2016

	Currently in use	Planned for acquisition	No plans
Antivirus / anti-malware (signature based)	70.5%	24.8%	4.8%
Advanced malware analysis / sandboxing	64.1%	27.9%	8.0%
Disk encryption	62.8%	27.7%	9.5%
Antivirus / anti-malware (machine learning)	60.6%	28.9%	10.5%
Data loss/leak prevention (DLP)	54.9%	32.8%	12.3%
Application control (whitelist/blacklist)	54.8%	32.8%	12.4%
Self-remediation for infected endpoints	47.8%	35.9%	16.2%
Digital forensics / incident resolution	46.2%	34.9%	18.9%
Containerization / micro-virtualization	40.6%	37.9%	21.5%

Table 2: Endpoint security technologies in use and planned for acquisition.

The same approach used to assess network security technologies was repeated to gain insight into deployment status and acquisition plans for both endpoint and mobile security technologies. Once again, percentages in darker shades correspond to higher frequency of adoption and/or acquisition plans, while percentages in lighter shades correspond to lower frequency of adoption and/or acquisition plans. Let's begin with traditional endpoints (see Table 2).

Just as we saw for network security technologies (see Table 1), the biggest year-over-year increase in adoption rate was for advanced malware analysis technology, which leapt from the middle of the pack in last year's report (53.3%) to second place this year (64.1%). Advanced malware analysis technology trailed only signature-based antivirus/anti-malware technology (70.5%).

Although signature-based antivirus/anti-malware still tops the currently-in-use technologies list, its hold on this position is clearly tenuous, as it also took the biggest hit in year-over-year results, shedding just over 11 points. Next in the "heading in reverse" category was application control, which slipped from to 63.2% to 54.8% in a year's time.

"Although signature based antivirus/ anti-malware still tops the currently-in-use technologies list, its hold on this position is clearly tenuous, as it also took the biggest hit in year-over-year results, stumbling just over 11 points."

In recognition of the rapid evolution of endpoint security technologies (see The Road Ahead from the 2015 Cyberthreat Defense Report), we also added a new entry to the list this year: antivirus/anti-malware

Endpoint and Mobile Security Deployment Status

Which of the following mobile security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard mobile devices (smartphones and tablets), and corporate data accessed by mobile devices, against cyberthreats? (n=981)

2016

	Currently in use	Planned for acquisition	No plans
Mobile device antivirus / anti-malware	62.5%	27.3%	10.2%
Mobile device / application management (MDM/MAM)	58.4%	31.5%	10.1%
VPN to on-premises security gateway	57.1%	30.4%	12.5%
Network access control (NAC)	56.4%	31.5%	12.1%
Mobile device file / data encryption	55.2%	31.4%	13.4%
VPN to cloud-based security gateway	52.3%	35.3%	12.4%
Virtual desktop infrastructure (VDI)	49.8%	34.9%	15.3%
Containerization / micro-virtualization	40.2%	39.5%	20.3%

Table 3: Mobile security technologies in use and planned for acquisition.

technology that uses machine learning as its primary mechanism for threat detection, instead of relying on signatures. The new kid on the block had a very strong showing, with slightly more than six in 10 respondents indicating their organizations have already deployed this technology.

As for which endpoint security technologies organizations plan to acquire in the coming year, the data shows containerization/micro-virtualization (37.9%) leading the way, followed closely by endpoint self-remediation solutions (35.9%). None of the listed technologies could be classified as doing poorly in this regard, suggesting heavy activity overall when it comes to improving endpoint defenses.

Now let's take a look at the mobile security landscape. Even though the deployment rate for all of the technologies listed has increased year over year, none is currently in use by a heavy majority of organizations. To us, this result points to: (a) a market segment that is still shaking itself out and, therefore, is fertile ground for further innovation; and (b) an area where organizations are likely to be leveraging multiple, overlapping solutions to get the job done.

"Not only are deployment rates for mobile security technologies up across the board year over year, but so too are planned investments for the coming year..."

Other notable findings from Table 3:

- The debate about if and when antivirus/anti-malware technology would make its way onto mobile devices in a big way has apparently been settled. In just two years, that technology went from the bottom of the barrel (in use at only 36% of respondent organizations) to leader of the pack (with 62.5% now using it).

Section 1: Current Security Posture

Endpoint and Mobile Security Deployment Status

- Not only are deployment rates for mobile security technologies up across the board year over year, but so too are planned investments for the coming year (with the exception of mobile device management and mobile application management (MDM/MAM), which are pretty much holding steady).
- With 39.5% of responding organizations signaling their intent to acquire it in the coming year, containerization/micro-virtualization consolidates the title of most sought-after endpoint/mobile security technology for 2016 (see Table 2).

Application and Data Security Technology Deployment Status

Which of the following application and data-centric security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard enterprise applications and associated data repositories against cyberthreats? (n=978)

2016	Currently in use	Planned for acquisition	No plans
Database firewall	64.9%	24.2%	10.8%
Web application firewall	64.4%	25.9%	9.7%
Database activity monitoring (DAM)	53.4%	33.2%	13.5%
Application delivery controller (ADC)	52.4%	31.6%	16.0%
File integrity / activity monitoring (FIM/FAM)	50.9%	35.5%	13.6%
Runtime application self-protection (RASP)	49.8%	32.4%	17.8%
Application vulnerability scanner	48.6%	35.9%	15.5%
Cloud access security broker (CASB)	47.1%	33.1%	19.8%
Static/dynamic/interactive application security testing	46.1%	37.2%	16.7%

Table 4: Application and data security technologies in use and planned for acquisition.

Anecdotal evidence suggests enterprises are steadily placing greater emphasis on protecting that which arguably matters most at the end of the day: sensitive data and the applications on which their business depends. To better understand what this trend actually means for current priorities and future plans, this year we took the same approach used for network, endpoint, and mobile security technologies to delve into the all-important areas of application- and data-centric defenses (see Table 4).

Key findings from this inaugural survey question:

- Database firewalls (64.9%) and web application firewalls (64.4%) claim the top spots as the most widely deployed app/data security technologies.
- With a respectable 52.4% deployment rate, application delivery controllers (ADCs) are clearly recognized as having evolved beyond their load balancing and performance optimization roots to be worthwhile app/data security platforms.

"These results point to [application and data security being] a hot market segment in 2016."

- Relatively high ratings across the board when it comes to future acquisition plans confirm that enterprises are indeed focusing heavily in these areas. These results point to a hot market segment in 2016.

Our closing thought on this topic is that although static, dynamic, and interactive application testing (37.2%) were the top-rated technologies planned for acquisition in 2016, we wouldn't be at all surprised to see cloud access security brokers (33.1%) outstrip them in the end, especially as enterprise use of cloud application and infrastructure services (SaaS/IaaS) continues to accelerate.

Monitoring Capabilities for Privileged Users

Describe your agreement with the following statement: "My organization has invested adequately in technology to monitor activities of users with elevated or privileged access rights." (n=996)

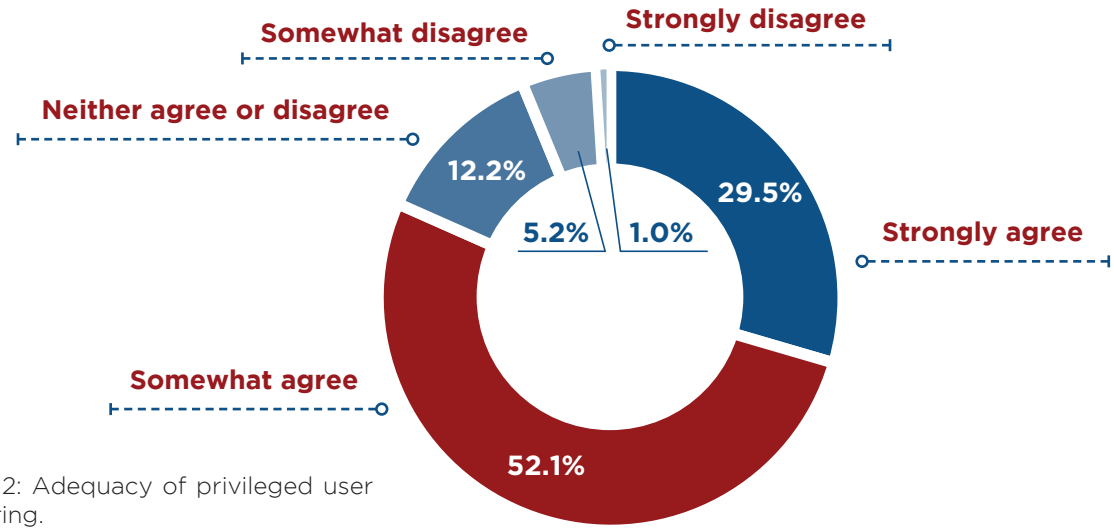


Figure 12: Adequacy of privileged user monitoring.

Participants were asked to indicate whether they believe their organization has invested adequately in technology to monitor activities of users with elevated or privileged access rights (i.e., privileged users). At the same time that only three out of 10 respondents are confident regarding their organization's ability to monitor privileged users, it's encouraging to see that only 6.2% feel their organization is negligent in this critically important area (see Figure 12). But therein lies the rub, too. This is a critical area, period.

With privileged accounts, we're quite literally talking about having access to the keys to the kingdom: the ability to take down application servers and networks, gain access to reams of sensitive data, or surreptitiously plant malcode on any device in the computing environment. And it's not just a rogue privileged user from within your ranks whom you need to worry about, but also any threat actor who manages to obtain credentials to one or more privileged accounts. So is it really a good thing that over half of our respondents (52.1%) only "somewhat agree" their organization has made adequate investments for monitoring privileged users? Suffice it to say, in our opinion, there's still plenty of room for improvement.

"...only three out of 10 respondents are confident regarding their organization's ability to monitor privileged users."

And let's be clear, too, about another elephant in the room. Privileged users/accounts are not the only ones that represent a significant risk to today's organizations. According to the 2015 Verizon Data Breach Investigations Report, more than half (50.7%) of the web application attacks in 2014 involved the use of stolen credentials (i.e., compromised user accounts). And although the result is typically some sort of fraudulent activity (such as unauthorized purchase of goods) as opposed to the catastrophic takedown of one's network, the losses incurred are still very real. As a result, it's not just protection and monitoring of privileged users/accounts that IT security teams need to be concerned with, but ultimately all users/accounts.

Section 2: Perceptions and Concerns

Types of Cyberthreats

On a scale of 1 to 5, with 5 being highest, rate your overall concern for each of the following types of cyberthreats targeting your organization. (n=986)

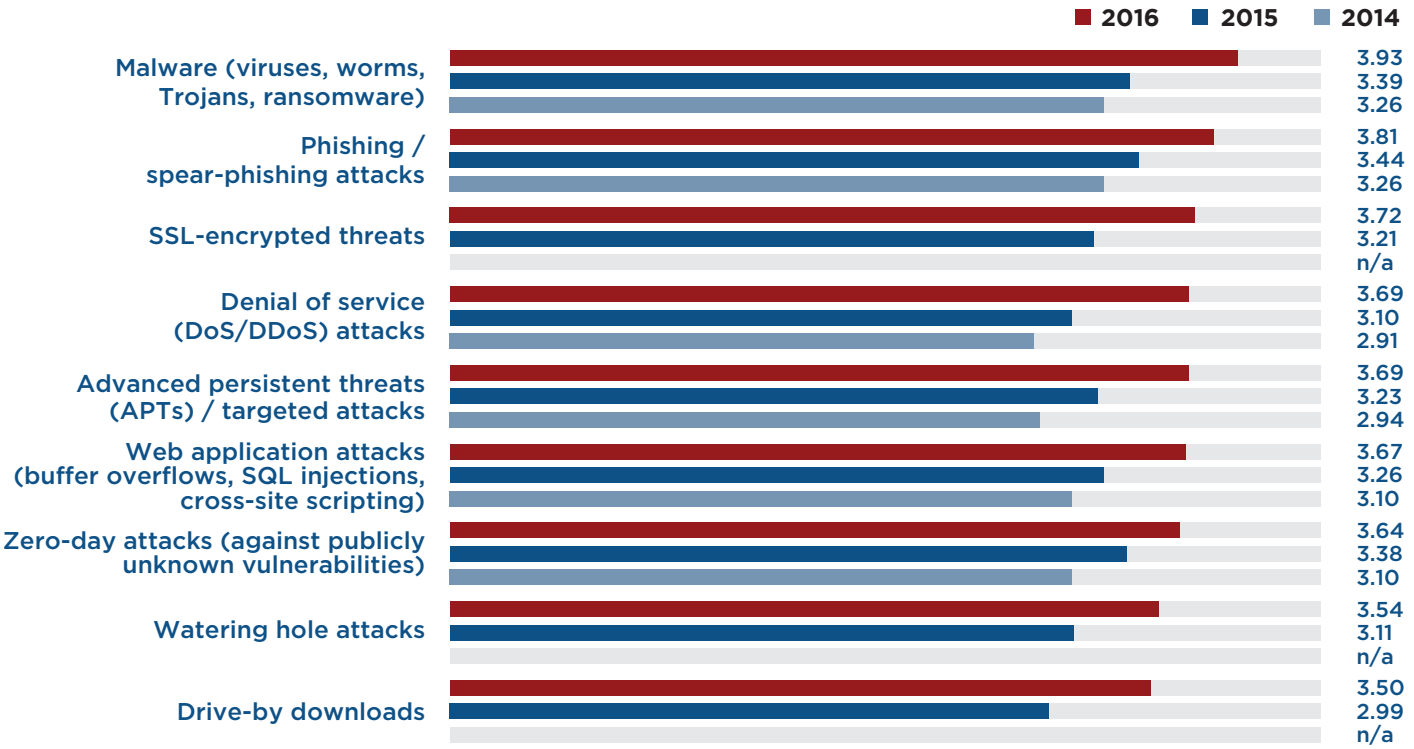


Figure 13: Relative concern by class/type of cyberthreat.

"The level of concern grew across the board, with the weighted scores for all types of cyberthreats increasing year-over-year…"

After being edged by phishing/spear phishing in last year's report, malware regained its title as the type of cyberthreat that concerns our respondents the most (see Figure 13). Not to be outdone, phishing/spear phishing trails by only a small margin to continue its three-year run near the top of the chart. Bringing up the rear for another year are drive-by downloads and watering hole attacks. All of that said, however, it is important to acknowledge that:

- The level of concern grew across the board, with the weighted scores for all types of cyber-threats increasing year-over-year, from 0.26 at the low end (zero-day attacks) to 0.61 at the high end (denial of service/distributed denial of service (DoS/DDoS) attacks); and,
- The total span of the weighted scores remains relatively low (0.43), suggesting that to many respondents, a "threat is a threat" – all types warrant concern and, presumably, attention.

Our final observation on this topic is that DoS/DDoS and APT attacks are the types of cyberthreats for which respondents' concern has increased the most over the three years that we've been collecting data and publishing the Cyberthreat Defense Report.

Mobile Devices (Still) in the Crosshairs

How has the volume of mobile device threats targeting your users' smartphones and tablets changed in the past 12 months? (n=969)

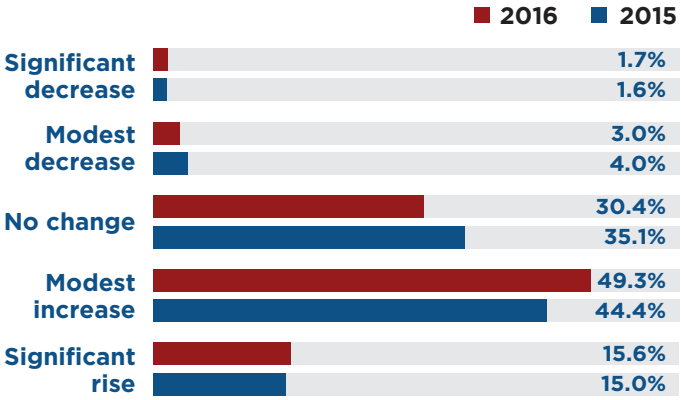


Figure 14: Change in volume of threats to mobile devices.

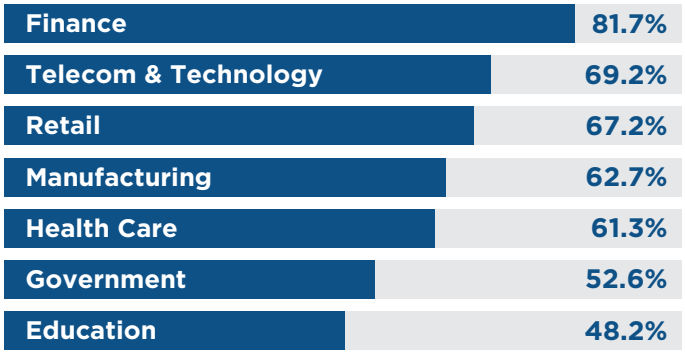


Figure 15: Percentage perceiving an increased volume of mobile threats.

When asked to characterize how the volume of threats targeting their organization's mobile devices (e.g., smartphones and tablets) changed in the previous 12 months, an astounding 64.9% indicated there had been an increase (see Figure 14). Combined with the relatively modest adoption rates for mobile security technologies (see Table 3), this finding helps complete the explanation for why mobile devices have been designated the weakest link in most organizations' defenses – for three straight years now!

Other notable findings:

- Geographically, Brazil (74.6%) and Canada (72.9%) had the highest rates of respondents' observing an increase in the volume of mobile device threats, while Singapore (53.3%) and Australia (54.7%) had the lowest.

"...this finding helps complete the explanation for why mobile devices have been designated the weakest link in most organizations' defenses – for three straight years now!"

- Within the financial services segment, more than four out of five respondents indicated an increase in the volume of mobile device threats. In contrast, less than half of respondents from the education sector reported the same thing (see Figure 15).
- Overall, only 4.7% of respondents reported a decline in the volume of mobile device threats over the past year.

Threat Intelligence Practices

Select the following reasons your organization has integrated commercial and/or open source threat intelligence into your existing security infrastructure. (Select all that apply.) (n=977)

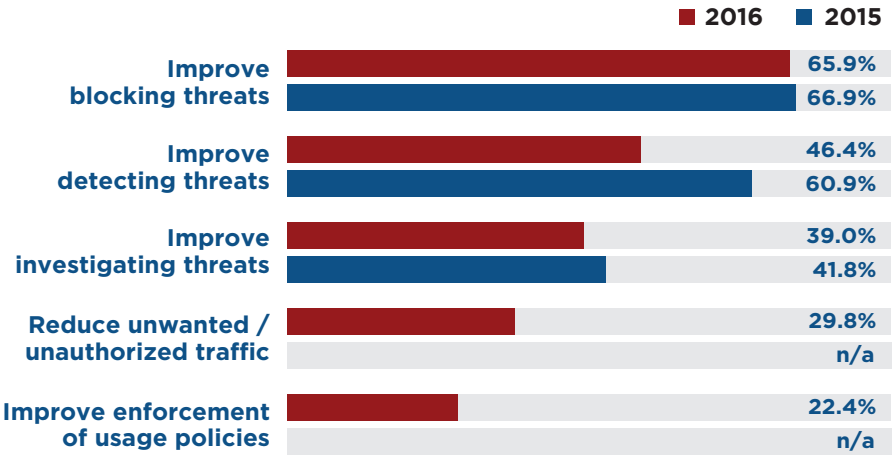


Figure 16: How threat intelligence is being leveraged.

For the second year in a row, supplemental (i.e., third-party) threat intelligence services is one of the hottest areas in which organizations are investing to bolster their cyberthreat defenses (see Table 1). But how are IT security teams actually using this valuable resource – which can include everything from ordinary threat indicators (e.g., file hashes and reputation data) and threat data feeds (e.g., malware analysis and trend data) to strategic intelligence (e.g., detailed information on adversaries and their motivations, intentions, tactics, techniques, and procedures)?

The answer, once again this year, is that the predominant use case for threat intelligence services is to enhance an organization's ability to block threats (65.9%). The next highest-ranking options – improving threat detection capabilities (46.4%) and improving threat investigation capabilities (39.0%) – both trail blocking by a considerable margin. Even further behind are the less-defense-oriented uses of keeping unwanted traffic off the network (29.8%) and better enforcing corporate policies (22.4%) (see Figure 16).

"...threat intelligence services is one of the hottest areas in which organizations are investing to bolster their cyberthreat defenses."

These findings suggest that most organizations are still investing primarily in services that deliver ordinary threat indicators and remain focused on tactical value. As the intelligence-related practices of IT security teams mature, however, we expect to see increasing interest in richer sources of information to support strategic use cases (such as informing an organization's longer-term security strategy and investment plans).

Returning to the data, there were no notable differences in the findings based on geography, vertical industry, or size of company.

Security Information and Event Management Practices

Select the reasons your organization operates security information and event management (SIEM) technology. (Select all that apply.) (n=966)

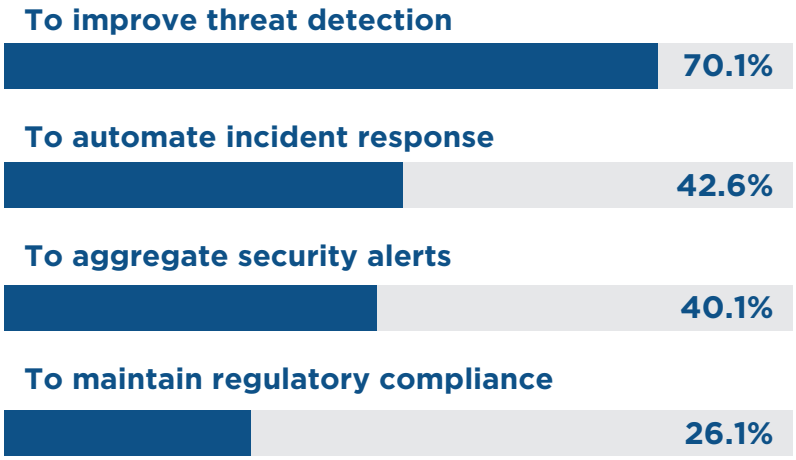


Figure 17: How SIEM technology is being leveraged.

Our next query was intended to ascertain the specific ways that organizations are extracting value from their investments in SIEM solutions. As nearly nine out of 10 responding organizations are leveraging (52.2%), or planning to acquire (35.5%), SIEM solutions (as depicted in Table 1 earlier in this report), it's interesting to note that SIEM technology benefits IT organizations in so many ways.

Improving threat detection (70.1%) was, by far, the predominant use case cited by respondents (see Figure 17). A bit surprising to us was the relatively low rate of use for maintaining regulatory compliance (26.1%). We would have expected this use case to have ranked more highly, given the ability of SIEM solutions to consolidate log/event data and produce countless reports, many of which are tailored to specific compliance regimes.

"Improving threat detection (70.1%) was, by far, the predominant use case cited by respondents."

Less surprising was the lukewarm reception to automating incident response (42.6%). In general, among organizations of all types and sizes, we continue to see an aversion to any sort of security automation that could result in needless disruption of users and essential business practices (e.g., being quarantined/blocked when they shouldn't be).

Just as with our similar question pertaining to threat intelligence services, there were no notable differences in the findings based on geography, vertical industry, or size of company.

Cloud Access Security Broker Practices

Select the reasons your organization operates cloud access security broker (CASB) technology. (Select all that apply.) (n=906)

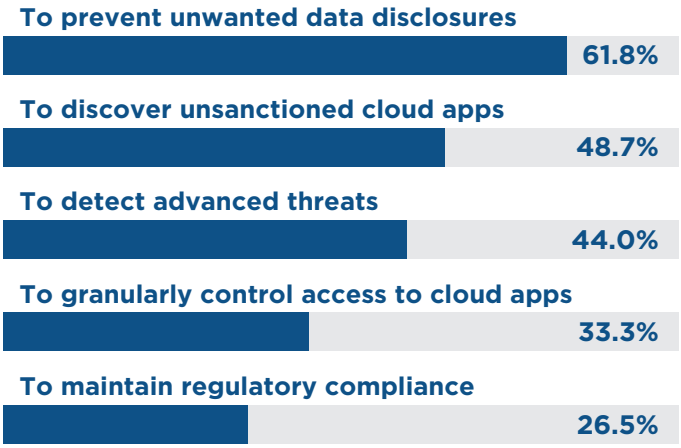


Figure 18: How cloud access security brokers are being leveraged.

In the fast-paced world of cloud applications and SaaS, organizations are regularly facing security challenges such as applications they don't manage, mobile devices they don't control, and users who don't think twice about sharing files among "anyone with the link." If the volume of acquisitions and major partnership deals from this past year is any indication, then the answer to all of these issues (and presumably many more) is CASBs. Analogous in many ways to their more familiar cousin, the secure web gateway, these Swiss Army knives of cloud application and data protection have rapidly become an essential security platform for organizations using cloud services – which means just about everyone.

Again, though, just because a solution can do a dozen or so things to help with an organization's cyberthreat defenses doesn't mean every IT security team is actually using all of the related capabilities. So how are CASBs being used, at least at this early point in their evolution, adoption, and implementation by today's enterprises?

"For just over six out of 10 respondents, the primary objective of a CASB is to prevent the disclosure of sensitive data."

For just over six out of 10 respondents, the primary objective of a CASB is to prevent the disclosure of sensitive data (see Figure 18). Progressively less important are the need to discover use of unsanctioned applications (48.7%), the need to detect advanced threats plaguing one's cloud services (44.0%), and granularly controlling which users have access to which cloud services (33.3%). Bringing up the rear, just as with our similar question pertaining to SIEM solutions, is the scenario of using a CASB to help maintain regulatory compliance (26.5%).

Most intriguing to us among these findings is the relatively low incidence of using CASBs to granularly control user access to cloud services. We see this as signaling a liberalization of security policies as enterprises enter the cloud era – or at least increased recognition that restricting users and being known for always saying "no" are less important than finding/stopping threats and preventing unauthorized migrations of sensitive data.

A final observation is that, unlike responses to the previous two questions, there is a bit more variation for different geographies and vertical industries. For example, in a few instances, discovering unsanctioned applications (France, Germany) or detecting advanced threats (Brazil) were cited as the top use case. Similarly, in a few others (United States, Mexico, education, and organizations with more than 10,000 employees), detecting advanced threats jumped into second position, ahead of discovering usage of unsanctioned applications.

Barriers to Establishing Effective Defenses

On a scale of 1 to 5, with 5 being highest, rate how each of the following inhibits your organization from adequately defending itself against cyberthreats. (n=990)

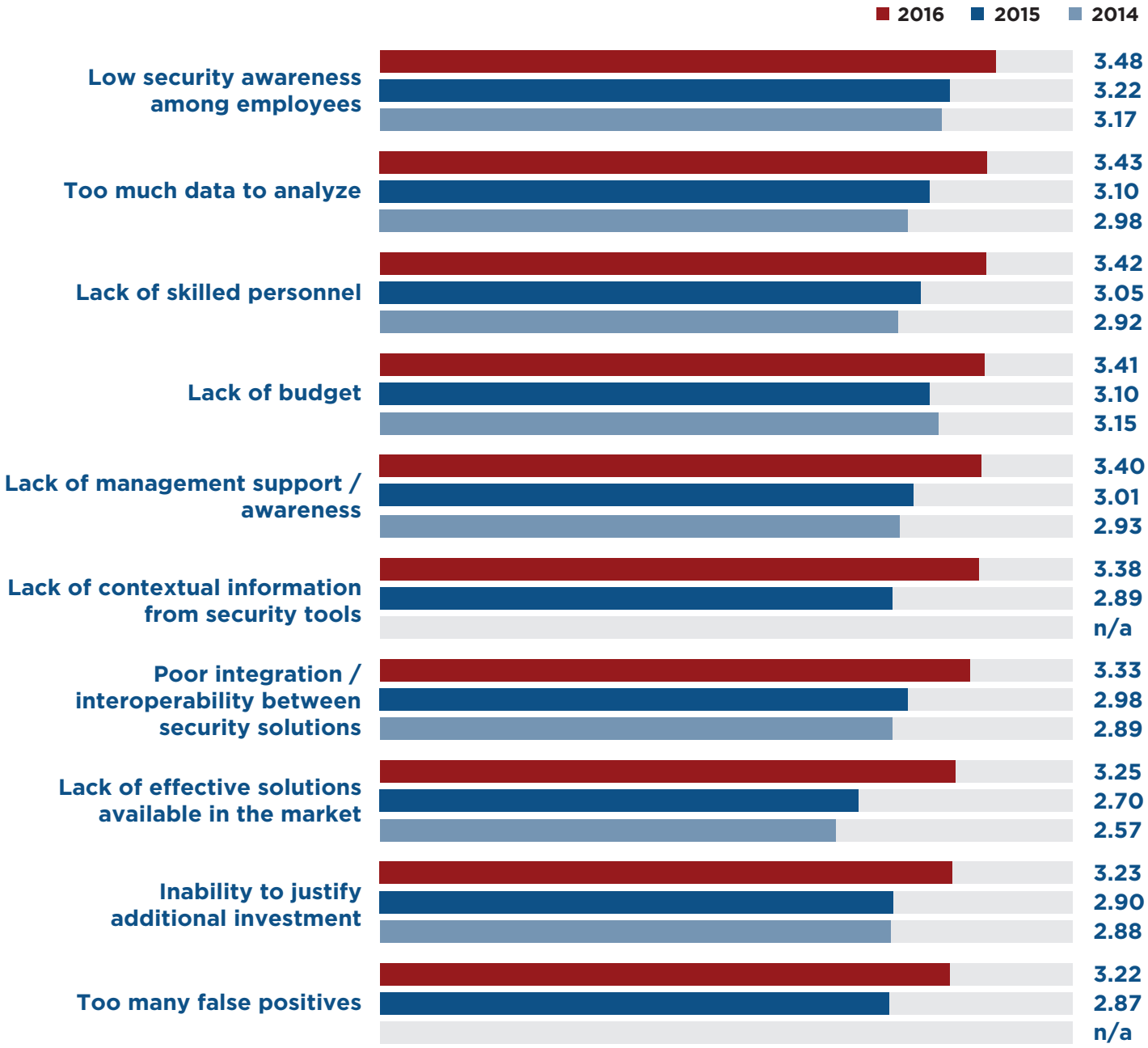


Figure 19: Inhibitors to establishing effective cyberthreat defenses.

Barriers to Establishing Effective Defenses

Establishing effective cyberthreat defenses is not easy. If it were, there would be far fewer successful cyberattacks and greater confidence on the part of IT security practitioners with regard to the likelihood of future breaches (see Figures 3 and 5). Part of the issue is the ever-evolving threat landscape, along with the nature of "playing defense."

Today's threat actors have a seemingly endless capacity to advance their wares and only need to find a single weak spot. As defenders, however, IT security teams can only guess at hackers' next moves and must provide coverage for every single user, endpoint, server, and application within and beyond the physical walls of the datacenter. Then there are all of the other obstacles that must also be overcome to achieve success (see Figure 19).

Once again, users are the Achilles' heel for most security programs, as "low security awareness among employees" tops the chart for the third consecutive year. The next three inhibitors also retain positions in the top four for yet another year, though their order has been shuffled a bit. Consistent with other findings confirming that InfoSec budgets are healthy (see Figures 1, 2, and 23), "lack of budget" has slipped from second to fourth. Replacing it in the runner-up spot is "too much data to analyze" – a familiar refrain that we've actually been hearing from enterprises for at least three or four years now.

"Once again, users are the Achilles' heel for most security programs, as 'low security awareness among employees' tops the chart for the third consecutive year."

As for the biggest mover year-over-year, "lack of effective solutions in the market" holds that dubious honor, jumping more than half a rating point to climb out of its former position as the lowest-rated inhibitor (now held by "too many false positives").

Section 3: Attack Surface Reduction

Technologies for Attack Surface Reduction

Which of the following technologies does your organization regularly use to reduce your network's attack surface? (Select all that apply.) (n=976)

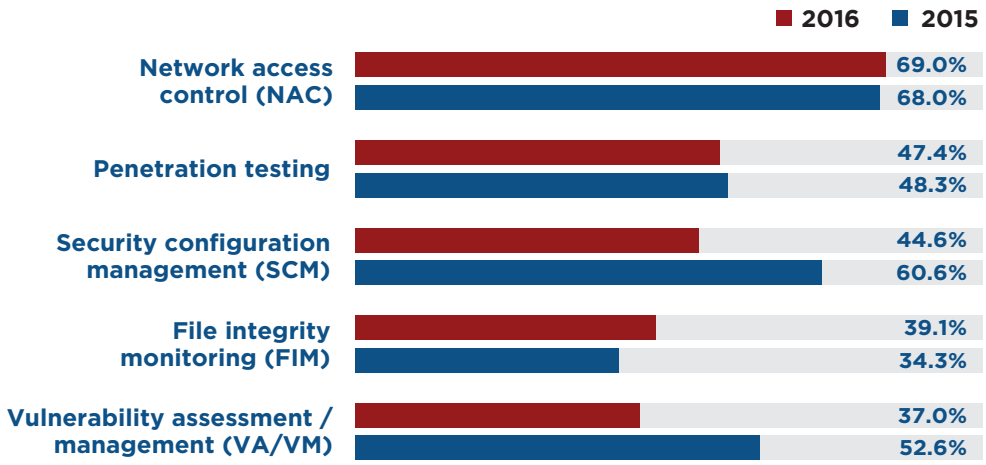


Figure 20: Technology choices for attack surface reduction.

Identified earlier as playing a respectable role in organizations' mobile security strategies (see Table 3), NAC was also selected by respondents as the top technology for reducing their network's attack surface (see Figure 20). Holding relatively steady in year-over-year response rates, too, were security configuration management (47.4%) and file integrity monitoring (39.1%).

In comparison, both vulnerability assessment/management and penetration testing were down substantially, with each having shed more than 15 points from last year's results. We find these declines confusing as both technologies are generally regarded as powerful mechanisms for identifying exploitable weaknesses that can subsequently be buttoned up, thereby significantly improving an organization's overall security posture. One possible explanation is that many respondents applied a literal interpretation to the wording of the survey question, specifically the qualifier that their organization "regularly uses" the given technology. After all, both of these technologies are typically used in an ad hoc (or periodic) manner, as opposed to being always on.

"...NAC was also selected by respondents as the top technology for reducing their network's attack surface."

Other notable findings:

- Like last year, European organizations (29.3%) have a markedly lower usage rate for vulnerability assessment technology than their North American counterparts (40.8%).
- NAC usage was highest among Japanese respondents (81.0%), while government organizations (75.4%) topped the chart from a vertical industry perspective.
- Very large organizations (>25,000 employees) have a higher incidence rate for each of the technologies listed than organizations of other sizes.

Frequency of Network Vulnerability Scans

How frequently does your organization conduct full-network active vulnerability scans? (n=962)

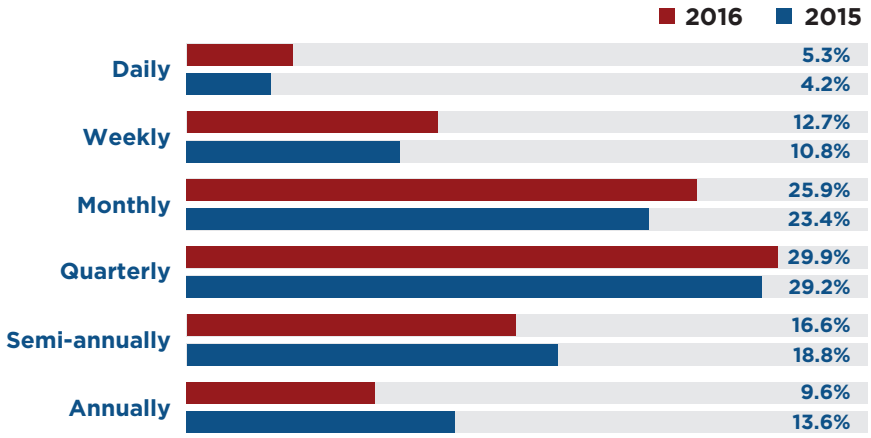


Figure 21: Frequency of full-network active vulnerability scans.

Respondents were asked how frequently their organization conducts full-network, active vulnerability scans (as opposed to scanning individual devices or enclaves, or using passive vulnerability scanning technologies that, by design, are always on). Similar to what we saw last year, the results are somewhat mixed (see Figure 21).

The good news is that usage is trending in a security-positive direction: those scanning monthly or more often inched upward from 38.4% to 43.9%, while those scanning less than quarterly dropped from 32.4% to 26.2%. Overall, this shift represents increased attention to the practice of attack surface reduction, and better recognition of the value it provides.

The bad news: more than a quarter of organizations remain stuck in the Stone Age, as they conduct full-network scans at best semi-annually. We can only hope that they're actually scanning more frequently with a less-expansive scope.

We also recognize that figuring out what to do with the results of these scans is not always easy. Gauging the severity of individual issues and establishing remediation priorities and plans specific to your organization can be challenging and time-consuming – and that doesn't even account for the time and effort

"Overall, this shift represents increased attention to the practice of attack surface reduction, and better recognition of the value it provides."

required to implement associated fixes. Next-generation vulnerability management solutions can definitely help, but it still falls to IT security teams/management to push a stronger agenda in this crucial area. Stepping off our soapbox, we can report that the data about scanning practices shows very little variation by country of origin, vertical industry, and size of organization – except for:

- Brazil (68.5%) and Mexico (26.8%), which are outliers at opposite ends of the spectrum of organizations that conduct full network scans at least monthly
- Education (38.5%), which comes in at the bottom of the verticals list for the same, modestly healthy scanning frequency
- Organizations with more than 25,000 employees (52.0%), which outstrip organizations of other sizes by an average of 8% at this same frequency

Host Remediation Strategies

How does your organization typically remediate malware-infected hosts? (n=972)

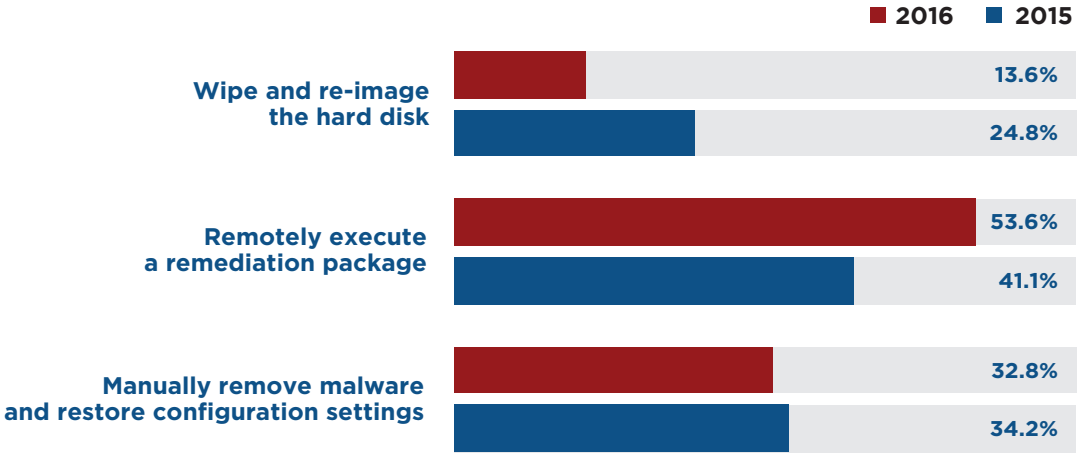


Figure 22: Preferred host remediation strategies.

Dealing with infected hosts is a fact of life for today's IT security teams. But what approaches do they favor for cleaning things up?

With this year's results, we are seeing a distinct preference to "remotely execute a remediation package," which is now favored by more than a 20-point margin over a manual approach to removing malware (see Figure 22). This finding is not particularly surprising as manual efforts are not only less efficient, but also tend to leave organizations exposed for a longer period, during which the potential for data theft and other forms of damage increases.

Also noteworthy is respondents' relatively low affinity for the practice of wiping and re-imaging a host's hard disk to remediate a malware infection. Presumably, IT security teams are not finding this approach effective (perhaps for preventing re-infections). Also, they may not be adequately set up to take advantage of it – for example, due to complicating factors such as not limiting hosts to a handful of standard images, or because they lack a sufficiently robust plan/practice for backing up data for individual hosts.

"This finding is not particularly surprising as manual efforts are not only less efficient, but also tend to leave organizations exposed for a longer period..."

These findings were fairly consistent across different demographic cuts, with one notable exception: adoption of remote remediation practices lags in both the government (39.3%) and education (41.8%) verticals, where manual remediation efforts continue to have a stronger presence.

Section 4: Future Plans

IT Security Budget Change

Do you expect your employer's overall IT security budget to increase or decrease in 2016? (n=982)

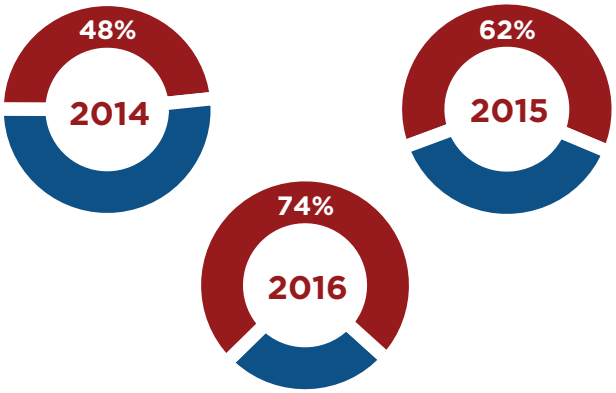


Figure 23: Percentage indicating security budget is growing.

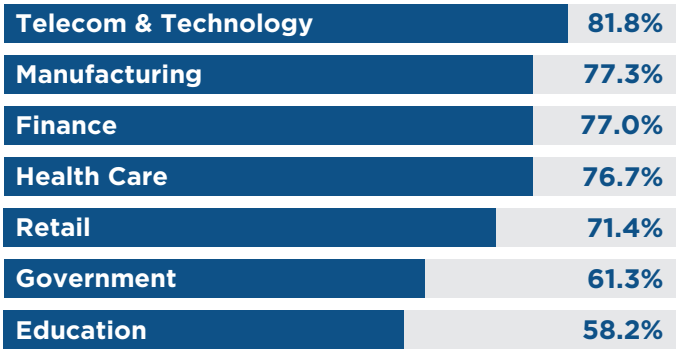


Figure 24: Percentage indicating security budget is growing, by industry.

Without adequate funding, no IT security team stands a chance of keeping pace. Thankfully, for the third consecutive year, our data shows that IT security budgets are in excellent shape. Up from just over 61% a year ago, now nearly three-quarters of respondents indicated that their organization's security budget is expected to grow in the coming year (see Figure 23). Even more encouraging: only a minuscule 3.3% expect their budget to shrink in 2016 – compared to 8.4% who expected that outcome a year ago.

Other notable findings:

- For both Brazil (31.6%) and Mexico (37.2%), approximately one-third of respondents expect their organization's IT security budget will grow by more than 10% in 2016.
- North American respondents (80.6%) flipped the script on their European counterparts (67.9%) from last year, with more of the former than the latter now signaling a budget increase is on the way.
- Education (58.2%) and government (61.3%) trail all other vertical industries, with the lowest (but still respectable) rates of respondents who expect security budget growth (see Figure 24).
- Manufacturing (77.3%) places near the top of the "expecting growth" list – perhaps as a result of attempts to get a handle on growing exposure from increasing volumes of operational technology (i.e., industrial control systems) that are network/Internet connected.

"Thankfully, for the third consecutive year, our data shows that IT security budgets are in excellent shape."

Section 4: Future Plans

Backpedaling on BYOD?

When, if ever, do you expect your organization to implement a bring-your-own-device (BYOD) policy to allow employee-owned devices to access confidential network data and/or applications? (n=977)

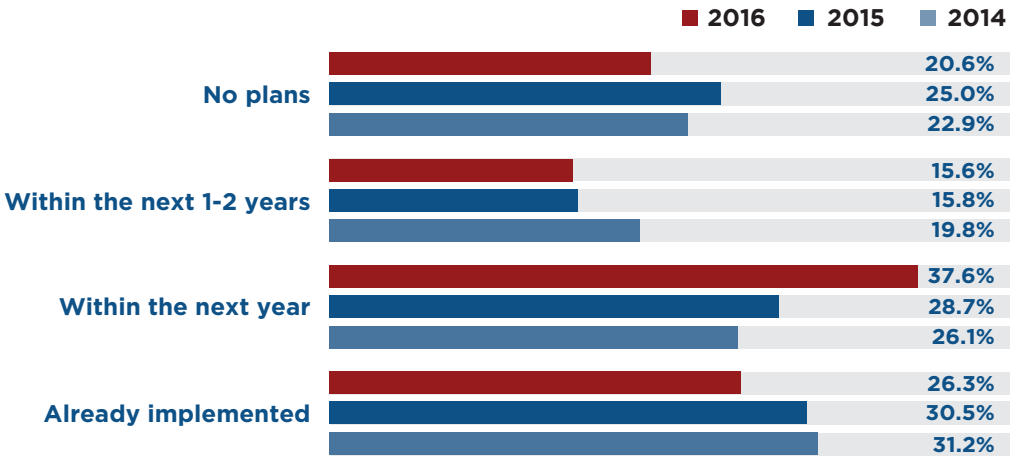


Figure 25: Timeframe for implementing BYOD policy.

Two years ago, when we first asked about implementing BYOD policies, the results were positively bullish. Nearly a third of respondent organizations had already done so and another quarter were planning to formally embrace BYOD in the following year.

Last year yielded almost identical response rates, suggesting that BYOD adoption plans had encountered a hiccup (since the percentage having already implemented BYOD policies hadn't increased).

Now, in our third year of asking this question, the data definitively indicates a retreat in BYOD implementations, down to 26.3% from 30.5% a year ago (see Figure 25). We can only guess at the reason for this backpedaling, but assume it has something to do with discovering that BYOD programs are harder to establish, manage, secure, and sell to users than many organizations first thought. This theory is consistent with accumulating anecdotal evidence, and aligns with our earlier finding that most organizations continue to employ a hodgepodge of technologies for mobile device protection (see Table 3).

"Now, in our third year of asking this question, the data definitively indicates a retreat in BYOD implementations..."

Other notable findings:

- Despite apparent difficulties in getting BYOD programs off the ground in the past, more than half of our respondents (53.2%) expect their organization to do just that within the next two years.
- BYOD is decidedly unpopular among the government crowd, with more than four in 10 respondents indicating their organization has no plans to adopt the practice.
- In comparison, more than three-quarters of telecom/technology respondents expect their organization to have a BYOD policy in place within the next year.
- Larger organizations (>25,000 employees) have, at least thus far, been more aggressive than their typically more nimble, smaller counterparts (<500 employees), with BYOD adoption rates of 37.9% and 25.2%, respectively.

Endpoint Protection Revolution

Which of the following best describes your organization's intent to evaluate new or alternative anti-malware protection for endpoints (desktops and laptops)? (n=963)

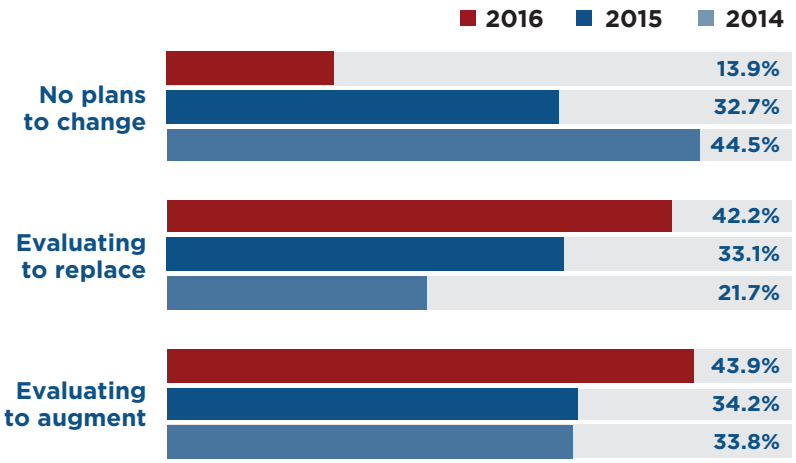


Figure 26: Plans for replacing or augmenting endpoint protection software.

The effectiveness and value of traditional endpoint security solutions, especially those that rely on signature-based detection mechanisms, have been in question for some time. However, with advanced malware now featuring countless tricks – such as polymorphism, active sandbox deception, and the ability to erase all traces of its presence after striking – the answer is clearly in.

Specifically, our data shows that a whopping 86.1% of respondent organizations are not satisfied with their current endpoint protection software (see Figure 26). This figure is up from 67.3% last year, and is most pronounced for respondents from Japan (93.2%) and the telecom/technology (90.8%) and retail sectors (90.3%).

Although respondents from Germany (76.2%) and the government (75.4%) and education verticals (77.4%) expressed the least amount of interest in making a change, it's still pretty clear that they, too, are not exactly satisfied with the status quo.

"Any way you cut it, however, these results point to a segment of the security market on the verge of revolution – one where incumbent providers are far from safe as so-called next-generation endpoint security solutions are poised to grab a significant piece of the pie."

Finally, among organizations reported to be looking for something new, there is roughly a 50:50 split between those intending to replace their incumbent endpoint protection solution and those merely looking to augment it. Any way you cut it, however, these results point to a segment of the security market on the verge of revolution – one where incumbent providers are far from safe as so-called next-generation endpoint security solutions are poised to grab a significant piece of the pie.

The Road Ahead

Let's face it, the decreasing optimism expressed by our survey respondents – with 62.1% now expecting their organization will fall victim to a successful cyberattack in the coming year, compared to only 51.9% two years ago – is not particularly surprising.

To begin with, this finding tracks with the related trend shown by the increasing number of organizations that experienced at least one successful cyberattack in the preceding 12 months (75.6% in 2015, up from 61.9% two years earlier). Then there's the harsh reality that the industrialization of hacking makes it substantially easier for attackers to succeed, while an ever-growing attack surface makes it considerably harder for IT security teams to counteract them.

As this year's survey results indicate, there's also the issue that many organizations still have plenty of room to improve – even in areas that would typically be considered core defenses. For example:

- Along with social media applications, endpoint computing devices of all types – but especially mobile ones such as smartphones and tablets – are recognized as relative weak spots in most organizations' defenses (see Figure 7).
- Although they are among the leading solutions planned for acquisition in the coming year, many next-generation technologies most likely to be effective against advanced malware and targeted attacks – such as security and user behavior analytics, network behavior analysis, and cyberthreat intelligence services – show fairly modest adoption rates (see Table 1).
- More than half of today's security teams only "somewhat agree" that their organization has the tools needed to inspect SSL-encrypted traffic for cyberthreats and exfiltration of sensitive data (see Figure 8).
- Only one in five organizations regularly backs up at least 80% of their mobile users' laptops (see Figure 10).
- Only a third of IT security professionals are confident that their organization is doing enough to monitor privileged user accounts for signs of misuse and/or compromise (see Figure 12).
- Adoption rates for key practices and technologies aimed at reducing a network's attack surface – such as penetration testing, file integrity monitoring, and conducting full-network vulnerability scans more often than quarterly – remain fairly modest (see Figures 20 and 21).
- Nearly nine out of 10 respondents recognize that the anti-malware solution they are currently using to defend their endpoints is not providing adequate protection (see Figure 26).

All is not lost, though. On the positive side of the ledger, anecdotal evidence indicates that cybersecurity is now a board-level topic/concern for more organizations than at any time in the past. The fact that security budgets are both healthy and growing is also an encouraging sign (see Figures 1 and 23). Having additional funding at their disposal should enable enterprise security teams not only to fill known gaps in their organization's defenses, but also to start getting ahead in the game.

Looking beyond the scope of this year's survey, here are some key areas where we believe additional/proactive attention and investments have the potential to significantly enhance an organization's ability to defend against current and future generations of cyberthreats.

Cloud access security brokers. With nearly a dozen significant acquisitions and partnerships in 2015 alone – including Blue Coat Systems (acquired Elastica and Perspecsys), Microsoft (acquired Adallom), Palo Alto Networks (acquired CirroSecure), Check Point (partnered with FireLayers), Cisco (partnered with Elastica), HP (partnered with Adallom) and Forcepoint (formerly Raytheon/Websense; partnered with Imperva) – CASBs are undeniably one of the hottest segments of the InfoSec market. And with good reason. To begin with, just about every organization on the planet needs one (or soon will). Adoption of cloud applications and infrastructure (i.e., SaaS and IaaS solutions) – both sanctioned and not – continues to accelerate, trailing behind it the need to secure these services in a scalable way that transcends the highly inconsistent native features and functions of the cloud services themselves. Then there's the fact that leading solutions can do it all – providing everything from visibility into Shadow IT

The Road Ahead

and cloud service usage to comprehensive access control, data security, threat protection, and even compliance support. The net result is a win-win scenario that we expect will lead CASBs to achieve enterprise adoption rates on par with antivirus and firewall technologies within the next two to three years. And, if you want to get ahead of the curve, we also see a similar scenario playing out for "social media application security brokers" … or whatever (hopefully better) name the market eventually settles on.

Advanced web application protection. There's a new wrinkle – or at least sub-classification – in the landscape of threats targeting web applications. Defined in detail by the Open Web Application Security Project (OWASP) in its recent handbook[1] on the topic, automated threats have now been formally recognized as the latest/greatest scourge plaguing the web applications upon which today's businesses have come to rely. Characterized by the ease with which they can be replicated/reused and their focus on abuse of application functionality (rather than ordinary vulnerabilities), these threats – which include account aggregation, ad fraud, credential stuffing, card cracking, and site scraping (just to name a few) – are not only pervasive but also inherently difficult for traditional countermeasures to detect. As a result, defending against them will require a corresponding wrinkle in organizations' security strategies. Specifically, just as it has become best practice to bolster the effectiveness of ordinary firewalls and IDS/IPSs with integrated threat intelligence services, so too is it now making good sense to do the same thing for web application firewalls. One difference with this latter case, however, is the need for the provisioned services to extend beyond ordinary reputation and indicator of compromise (IOC) data to deliver extensive bot-, device-, and credential-focused intelligence.

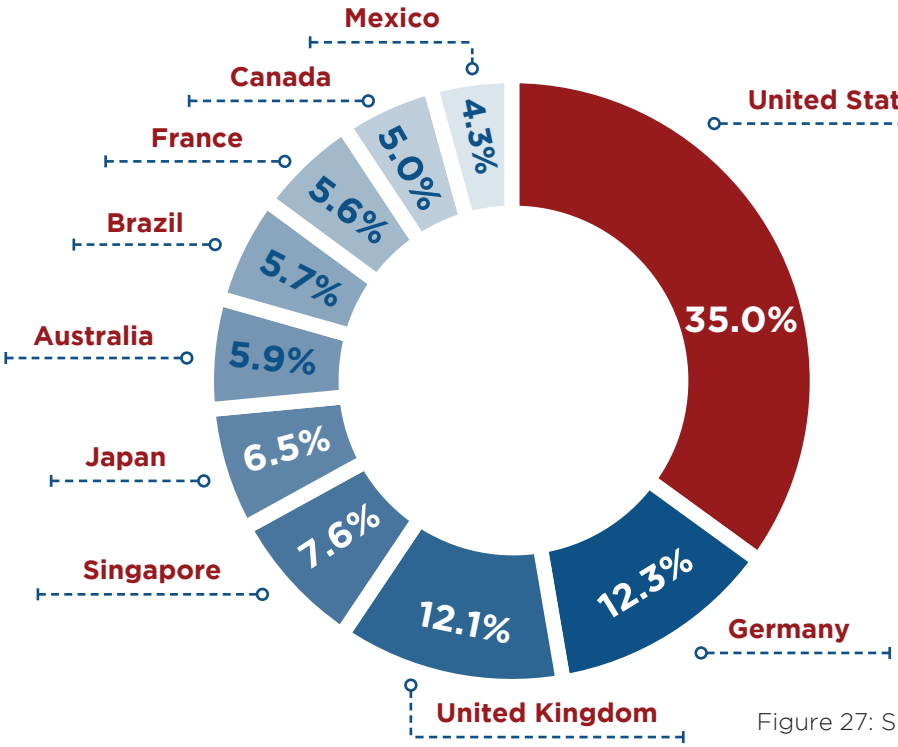
User-centric security. For several years now, protecting the ultimate target with data-centric security or the immediate conduit to data with application-centric security has been a particular emphasis of the security industry at large. It's not that we want to deter anyone too much from those entirely appropriate objectives, but we can't help make the observation that greater attention is also warranted for what we're labeling user-centric security. Keep in mind that employees (or more generally, users) have been identified as the weakest link in organizations' ability to establish effective cyberthreat defenses for three consecutive years now (see Figure 19). So isn't it about time to do something more to mitigate against users as threats? Robust identity and access management policies, practices, and controls (e.g., to really and truly implement a least-privileges security model) should be a big part of the plan. But we're thinking beyond that. After all, more data breaches result from credential theft and threat actors' masquerading as authorized users than from any other cause. In particular, we see user behavior analytics emerging as another technology that modern organizations can use to get a better handle on the user side of the security equation. Greater effort and investment in user awareness training also wouldn't hurt. But we're not holding our breath on that one.

Cyberthreat hunting. The 2015 Cyberthreat Defense Report explained that cyberthreat intelligence services were evolving from delivering basic indicators (e.g., file hashes and reputation data) and threat feeds to richer data about threat actors in general, as well as a given organization's most likely set of adversaries. But so what? Richer data is completely worthless if no one's actually doing anything with it. That is pretty much what appears to be happening, at least at this point, as most organizations indicate they are using cyberthreat intelligence services primarily to enhance the effectiveness of their threat blocking infrastructure (see Figure 16). To take greater advantage of the richer data available from leading cyberthreat intelligence services, IT security teams should establish a formal cyberthreat hunting program and explicitly task some subset of their security architects with next-generation defense planning. The former is all about having a well-defined process for leveraging intelligence to better detect and isolate advanced threats, while the latter is about applying projected threat scenarios to help ensure the organization's defenses will be effective two, three, and even five years down the road.

For further insights on these and other emerging areas pertinent to IT security, be sure to tune in for the fourth annual Cyberthreat Defense Report, currently scheduled for release in the first quarter of 2017.

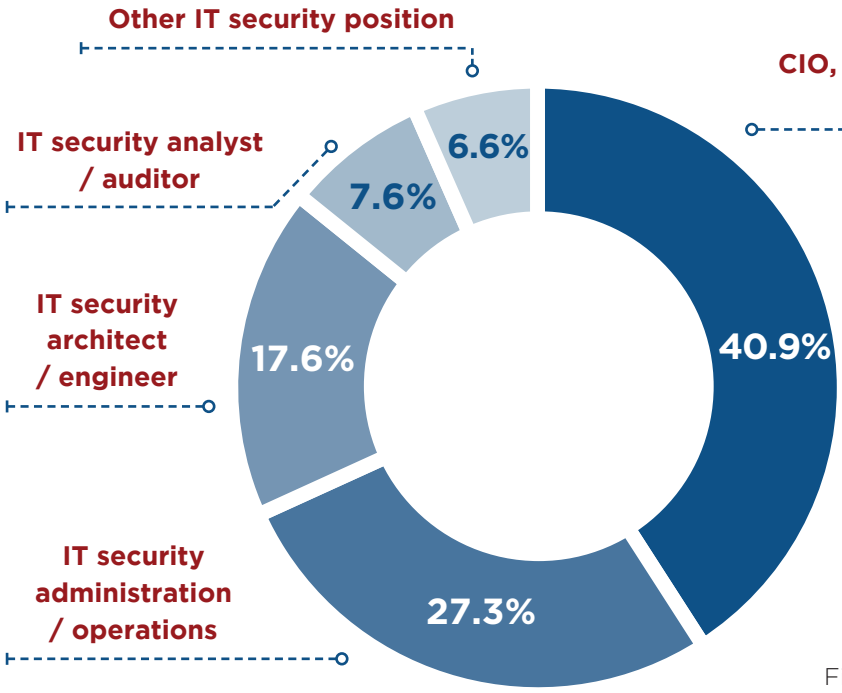
1. https://www.owasp.org/images/3/33/Automated-threat-handbook.pdf

Appendix 1: Survey Demographics



Of our 1,000 qualified survey participants, 40% specified United States of America or Canada as their country of residence, while 30% hailed from Europe (United Kingdom, Germany, and France), 20% from Asia Pacific (Singapore, Japan, and Australia), and 10% from Latin America (Brazil and Mexico).

Figure 27: Survey participation by geographic region.



As for the roles of our survey participants, four out of 10 held senior positions (CIO, CISO, or IT security executive) with IT security responsibilities. Just over a quarter identified as IT security administrators/operations staff, while nearly a fifth were security architects. The balance split almost evenly between analysts/auditors and personnel identifying their position within IT security as "other."

Figure 28: Survey participation by IT security role.

Appendix 1: Survey Demographics

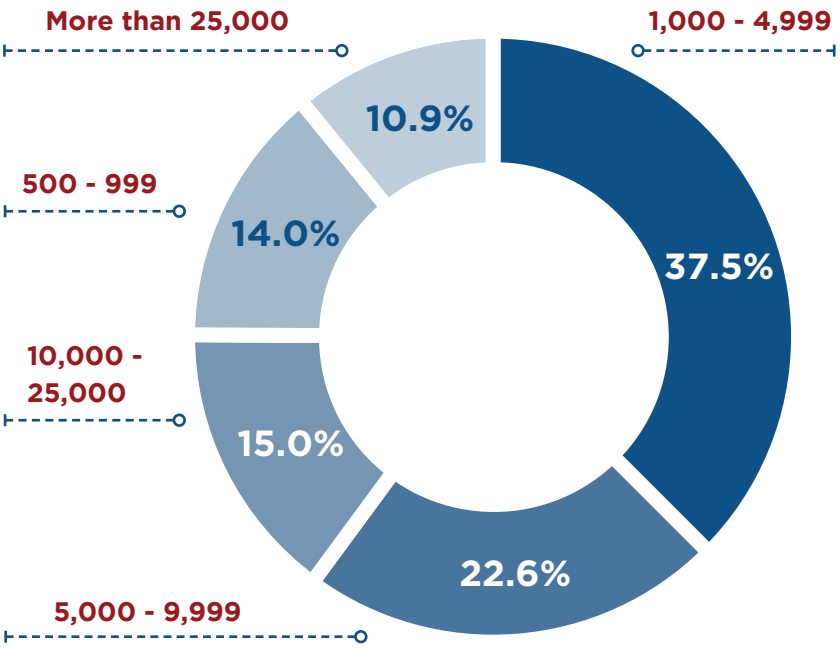


Figure 29: Survey participation by organization employee count.

Just over a quarter of the survey respondents were from enterprises with more than 10,000 employees. The largest segment of the survey population (60.1%) was from organizations with between 1,000 and 10,000 employees. Only 14% of participants were from smaller organizations with between 500 and 1,000 employees.

Distribution of survey participants by vertical industry was fairly broad, with representation across 19 industry segments, and a twentieth category designated as "other." The "big 7 Industries" – education, finance, government, health care, manufacturing, retail, and technology – accounted for just shy of two-thirds of all respondents. No single industry accounted for more than 18% of participants.

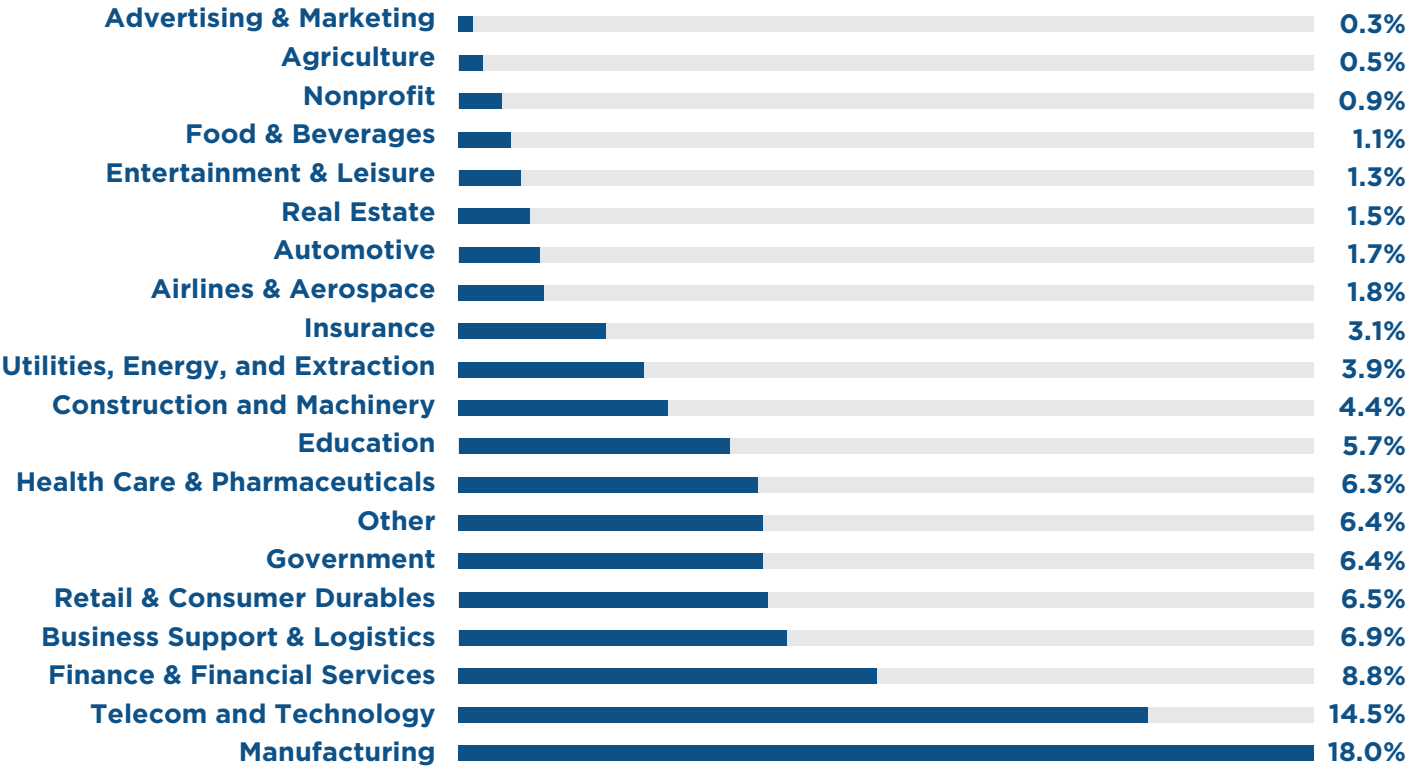


Figure 30: Survey participation by industry.

Appendix 2: Research Methodology

CyberEdge Group developed a 26-question (10- to 15-minute) web-based survey instrument in partnership with its sponsoring vendors. (No vendor names were referenced in the survey.) The survey was promoted to information security professionals across North America, Europe, Asia Pacific, and Latin America in November 2015.

Non-qualified survey responses from non-IT security professionals and from participants employed by an organization with fewer than 500 global employees were discarded. Most survey questions (aside from demographic questions) included a "don't know" choice to minimize the potential for respondents to answer questions outside of their respective domains of expertise, which altered the sample size ("n") for each set of survey question responses.

All qualified survey responses were inspected for potential survey "cheaters," meaning survey takers who responded to questions in a consistent pattern (e.g., all A responses, A-B-C-A-B-C responses) in an attempt to complete the survey quickly in hopes of receiving the incentive. Suspected cheater survey responses were deleted from the pool of responses.

Appendix 3: About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our highly experienced consultants have in-depth technical expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Cloud Security
- DoS/DDoS Protection
- Endpoint Security
- Intrusion Prevention Systems (IPS)
- Managed Security Services Providers (MSSPs)
- Mobile Device Management (MDM)
- Network Behavior Analysis (NBA)
- Network Forensics
- Next-generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Identity Management (PIM)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Virtualization Security
- Vulnerability Management (VM)

For more information on CyberEdge Group and our services, call us at 800-327-8711, email us at info@cyber-edge.com, or connect to our website at www.cyber-edge.com