CYBEREDGE GROUP

2014 CYBERTHREAT DEFENSE REPORT

NORTH AMERICA & EUROPE

<< Research Sponsors >>

Platinum sponsor:

paloalto NETWORKS

Gold sponsors:

BLUE COAT ForeScout NetIQ tenable network security TREND MICRO

Silver sponsors:

CYLANCE GENERAL DYNAMICS Fidelis Cybersecurity Solutions WEBROOT

Table of Contents

Introduction

Survey Demographics

- 763 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 11 countries in North America and Europe
- Representing 19 industries

In war, knowing your enemy is imperative to establishing an effective defensive strategy. The same holds true for effective IT security, and several excellent industry reports help inform IT security professionals on this front. The annual Data Breach Investigations Report from Verizon, for example, sheds considerable light on the evolving nature of cyberthreats, the actors behind them, and the techniques being used to perpetrate successful attacks.

The Cyberthreat Defense Report informs the IT security community in another, complementary way. Based on a rigorous survey of IT security decision makers and practitioners across North America and Europe, the Cyberthreat Defense Report examines the current and planned deployment of technological countermeasures against the backdrop of numerous perceptions, such as:

- ☑ The adequacy of existing cybersecurity investments, overall and within specific domains of IT
- ☑ The likelihood of being compromised by a successful cyberattack within the next 12 months
- ☑ The types of cyberthreats and cyberthreat sources that pose the greatest risk to a given organization
- ☑ The effectiveness of both traditional and next-generation/ advanced technologies for thwarting cyberthreats
- ☑ The organizational factors that represent the most significant barriers to establishing effective cyberthreat defenses
- ☑ The most valuable solution capabilities and packaging options

By revealing these details we hope to provide IT security decision makers with a better understanding of how their perceptions, concerns, priorities, and – most importantly – current defensive postures stack up against those of other IT security professionals and organizations. Applied in a constructive manner, the data, analyses, and findings covered herein can be used by diligent IT security teams to gain insights into many practical 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 – as well as tackling newer ones, such as providing security for mobility and defending against advanced persistent threats (APTs)?
- ☑ 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?

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

cy•ber•threat
/ˈsībərˌTHret/

noun

1. the possibility of a malicious attempt to damage or disrupt a computer network or system (source: Oxford Dictionaries)

2. any type of malicious activity or actor that leverages computers and networks to adversely impact other computers and networks, to include everything from well-known forms of malware (e.g., viruses, worms, and Trojans) to malicious insiders and targeted attacks (source: CyberEdge Group)

Research Highlights

Current Security Posture

- ☑ One in four security professionals doubts whether their organization has invested adequately in cyberthreat defenses.
- ☑ Over 60% of respondents were affected by a successful cyberattack in 2013, but less than 40% expect to fall victim again in 2014.
- ☑ Mobile devices (smartphones and tablets) are perceived as IT security's "weakest link," followed by laptops and social media applications.
- ☑ Next-generation firewalls (NGFWs) are most frequently cited for acquisition in 2014, followed by Network Behavioral Analysis (NBA) and Big Data Security Analytics.
- ☑ 77% intend to use network access control (NAC) as part of their mobile security strategy.
- ☑ One in four organizations lacks the tools necessary to properly investigate the root cause and material impact of network security breaches.

Perceptions and Concerns

- ☑ Malware and phishing give IT security professionals the most headaches.
- ☑ Security professionals are more concerned about malicious insiders than cybercriminals.
- ☑ NAC and NGFW solutions are perceived as most effective at mitigating cyberthreats.
- ☑ Low security awareness among employees is the greatest inhibitor to adequately defending against cyberthreats.

Attack Surface Reduction

- ☑ Less than half of organizations conduct full-network active vulnerability scans more than once per quarter.
- ☑ Nearly one-third of organizations are leveraging vulnerability intelligence as "context" for intelligent threat response.
- ☑ NAC is most commonly used to identify vulnerabilities and security misconfigurations on endpoint devices in between full-network vulnerability scans.

Future Plans

- ☑ 89% of IT security budgets are rising or holding steady.
- ☑ Implementation of bring-your-own-device (BYOD) policies will more than double within the next two years—from 31% in 2014 to 77% in 2016.
- ☑ 54% are looking to replace or augment their current endpoint protection software.
- ☑ Third-party validation is least important when evaluating new cyberthreat defenses.
- ☑ Only 7% of IT security professionals prefer a software-as-a-service (SaaS) delivery model for their cyberthreat defenses.

Cut to the Chase

- 25% of survey participants doubt whether their organization has invested adequately in cyberthreat defenses
- Europeans (82%) are somewhat more confident than North Americans (71%) in their cyberthreat defense investments

Section 1: Current Security Posture

The foundation of countermeasures an organization currently has in place and the perception of how well that foundation is working will influence major decisions about cyberthreat defenses, such as:

☑ Whether, to what extent, and with what degree of urgency changes are needed, and

☑ The most likely candidates to enable those changes (i.e., the specific types of countermeasures that should be added to supplement existing defenses).

Accordingly, our journey into the depths of cyberthreat defenses begins with an assessment of the perceived effectiveness of organizations' investments and strategies relative to the prevailing threat landscape. Insight is also provided on the high-level definition of these strategies based on the technological countermeasures that comprise them.

Adequacy of Cyberthreat Defense Investments

When asked how they perceive the adequacy of their employer's investment in cyberthreat defenses, fully one-quarter of respondents expressed doubts, with more than half of this group taking a more definitively negative view (see Figure 1).

This leaves approximately 75% at the opposite end of the spectrum, with a breakdown of 30% "strongly" agreeing and another 44% "somewhat" agreeing with their employer's level of investment. We view this as an extremely encouraging result, particularly given the longstanding impression that IT security professionals are generally frustrated when it comes to obtaining sufficient funding and implementing the solutions they believe are necessary to defend their computing environments.

Interestingly, the data also revealed that European respondents are somewhat more confident than their North American peers in the level of investment in cyberthreat defenses made by their employers. Overall, 82% of the European survey population indicated they agreed (somewhat or strongly) with the adequacy of investments made. This compares to 71% for North American respondents.

This greater degree of confidence expressed by European respondents is at least partially explained and validated, respectively, by:

- ☑ A subsequent finding that fewer European organizations (57%) than North American organizations (64%) were subject to a successful cyberattack over the previous 12 months.
- ☑ A subsequent finding of a similar gap in relative confidence when participants were asked whether they thought their organization had the necessary tools to investigate and determine the root cause and material impact of successful attacks. In that case, 82% of European respondents indicated they had confidence in their organization's capabilities (and corresponding investments), compared to 70% of North American participants.

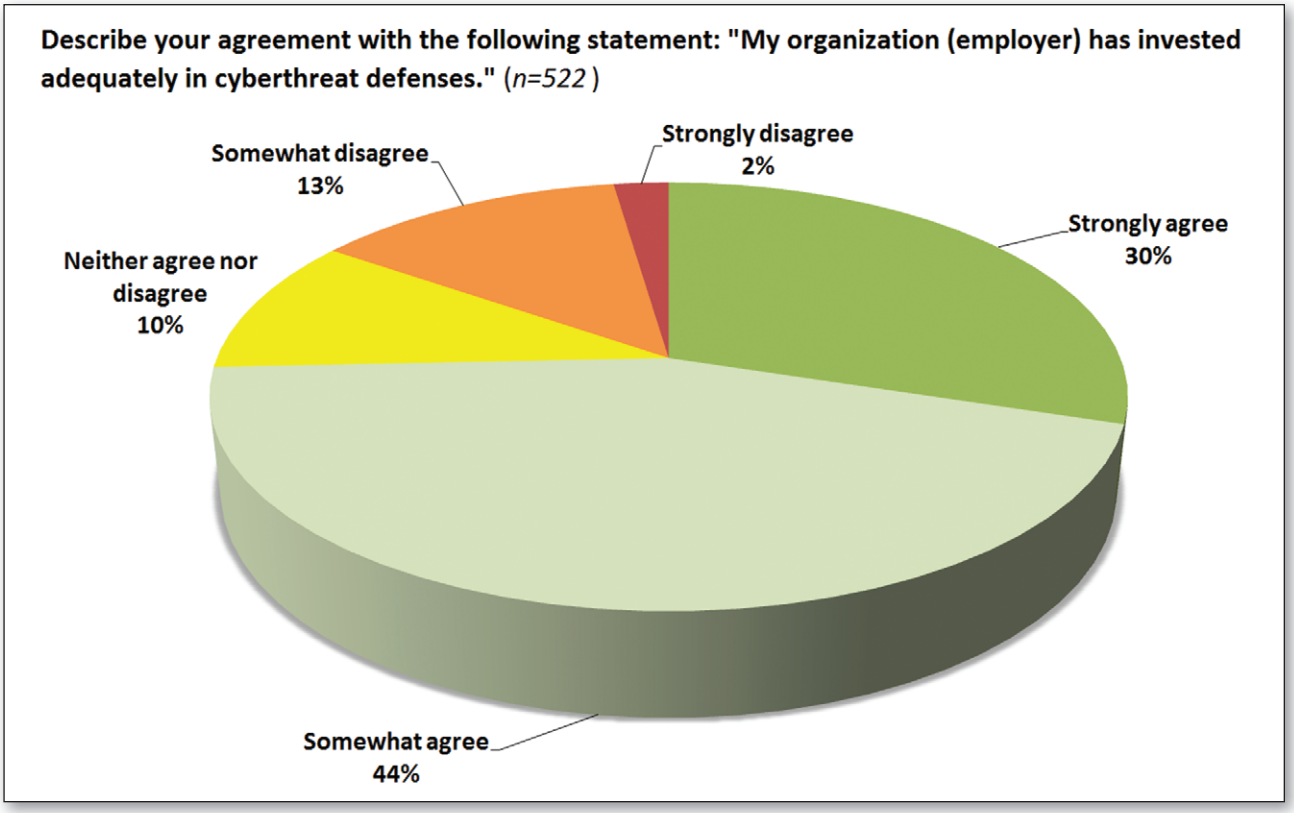

Figure 1: Perceived adequacy of cybersecurity investments

Cut to the Chase

- 84% of represented organizations experienced five or fewer successful cyberattacks in the preceding 12 months
- 38% claim they had not experienced a single successful attack in that same period
- 7% claim they've been successfully breached 10 or more times

Past Frequency of Successful Cyberattacks

For the most part, the relative confidence of respondents in their organization's level of investments in cyberthreat defenses is upheld by this next set of findings.

In particular, over 80% of respondents indicated that their organization's computing environment was compromised five or fewer times in the past year – with nearly half of these claiming there were NO successful attacks over this period (see Figure 2).

Less encouraging, 7% of respondents indicated their organization was subject to 10 or more successful attacks over the past year. Not surprisingly, this finding is generally consistent with the data from the previous question, where a total of 15% of respondents either somewhat or strongly disagreed with the level of security investments made by their organization.

The only significant difference from a regional perspective is that while 43% of European organizations claimed they did not experience a successful cyberattack over the past year, the same was true for only 36% of North American organizations.

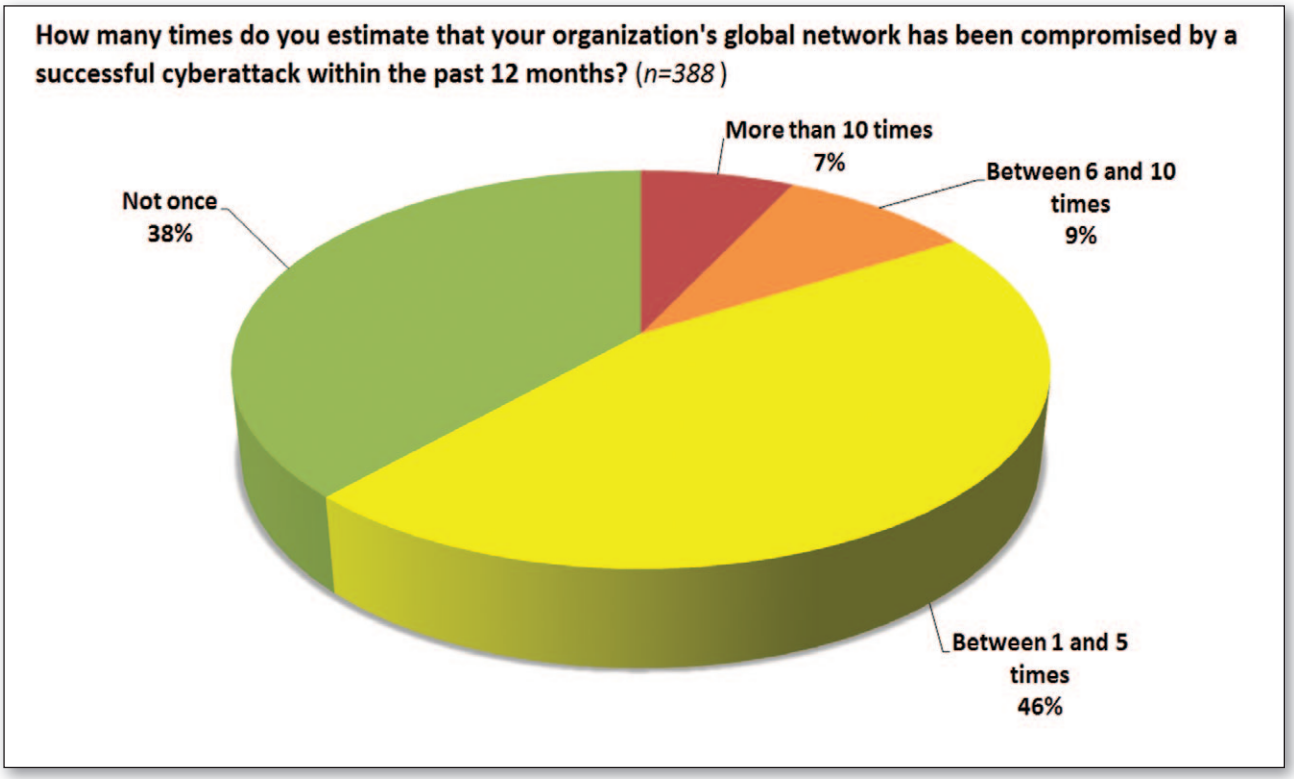

Figure 2: Frequency of successful attacks in the past 12 months

Future Likelihood of Successful Cyberattacks

When asked about the likelihood their organization's network would be compromised in the coming year, respondents were surprisingly optimistic. Despite more than 60% indicating they thought their organization's computing environment had been compromised within the past year (see Figure 2), only 39% considered it "somewhat likely" or "very likely" that it would happen again over the next 12 months (see Figure 3). Whether this optimism stems from changes and investments made as a result of past compromises or just represents wishful thinking is unclear.

No statistically significant differences were observed by region (i.e., North America vs. Europe).

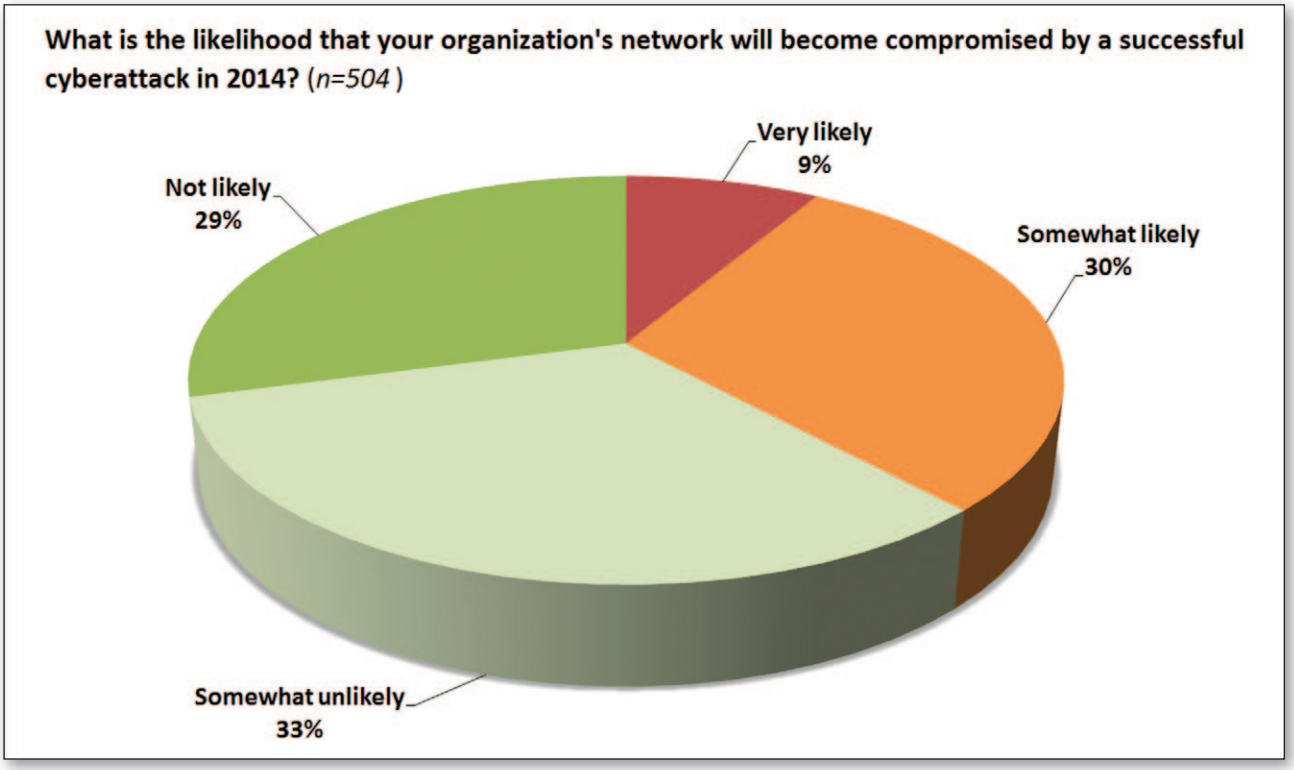

Figure 3: Likelihood of being successfully attacked in the next 12 months

Security Posture by IT Domain

Data on the perceived ability to defend against cyberthreats in different IT domains (see Figure 4) provides additional granularity to the earlier question regarding adequacy of an organization's investments in cyberthreat defenses. Somewhat surprising are the findings pertaining to virtualized server infrastructure

and public cloud services. In particular, our respondents expressed the same high degree of confidence in their defenses for virtual servers as in their physical servers and network perimeters.

One plausible explanation for this seemingly misplaced confidence could be this: although enterprise experience with server virtualization lags that which it has in other areas, and although the security solutions for virtualized infrastructure are somewhat immature on the whole, neither have we seen a significant number of threats/attacks against virtualization software layers or the cloud-specific aspects of public cloud services (as opposed to those aspects they share with traditional datacenter delivery models).

"Client devices of all types – but especially mobile devices – present the greatest security challenge to organizations."

Other notable findings include that:

- ☑ Establishing adequate protection for/from social media applications such as Facebook and Twitter remains a relative weak spot in organizations' defenses, and
- ☑ Client devices of all types – but especially mobile devices – present the greatest security challenge to organizations.

Not surprisingly, the data shows organizations are better able to secure resources over which IT inherently has greater control (e.g., servers) than those it does not (e.g., mobile devices).

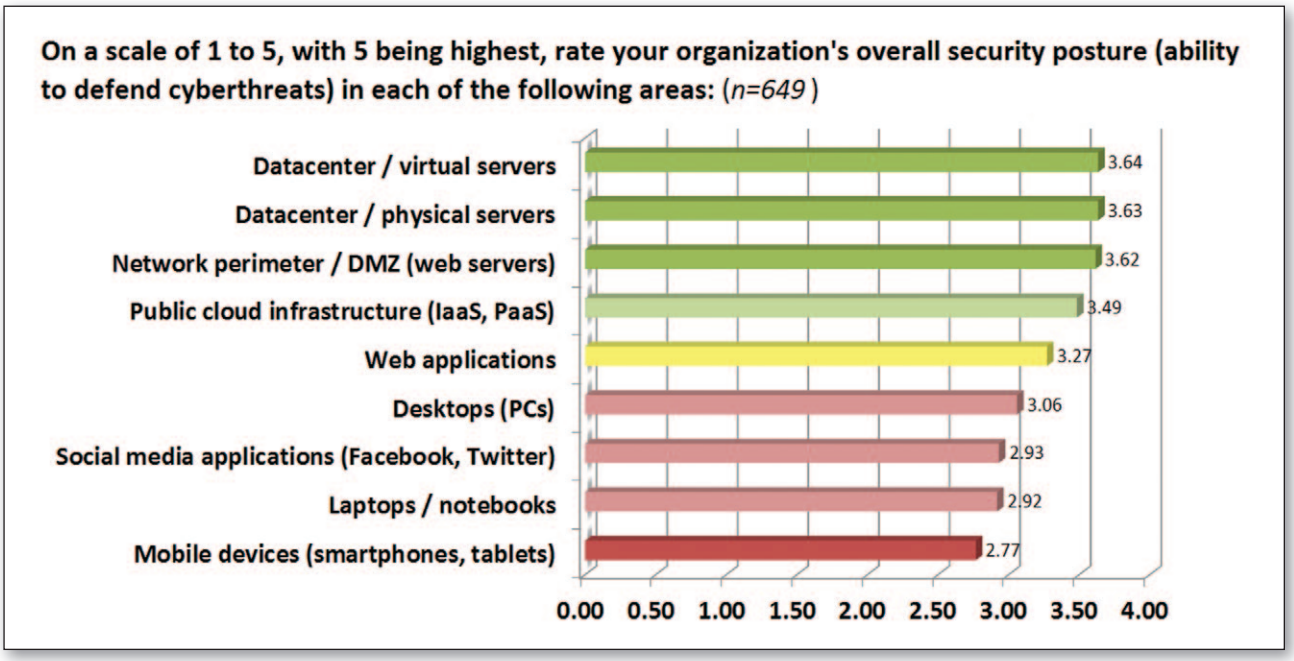

Figure 4: Perceived security posture by IT domain

Network Security Technology Deployment Status

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 the next section.) Table 1 below provides a visual and numerical representation of the responses.

Percentages in green correspond to higher frequency of adoption and/or acquisition plans. Percentages in red correspond to lower adoption and/or acquisition plans.

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=676*)

	Currently in use	Planned for acquisition	No plans
Intrusion detection / prevention system (IDS/IPS)	71%	17%	12%
Secure email gateway (SEG)	68%	15%	18%
Stateful inspection firewall	67%	17%	16%
Network access control (NAC)	64%	20%	17%
User activity monitoring	64%	18%	18%
Privileged user / identity management	62%	19%	19%
Secure web gateway (SWG)	62%	14%	23%
Identity and access management / governance	61%	21%	18%
Penetration testing	61%	20%	19%
Denial of service (DoS) / distributed denial of service (DDoS)	61%	16%	23%
Web application firewall (WAF)	60%	18%	22%
Vulnerability assessment / management (VA/VM)	57%	21%	22%
Full-packet capture and analysis	55%	22%	23%
Advanced malware analysis / sandboxing	54%	21%	25%
Security information and event management (SIEM)	51%	23%	26%
Data loss/leak prevention (DLP)	51%	22%	27%
Next-generation firewall (NGFW)	48%	29%	23%
Network behavior analysis (NBA) / NetFlow analysis	48%	26%	26%
Big data security analytics	40%	24%	36%

<-- Less Frequency ------- More Frequency -->

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

"It seems clear that many organizations are planning to beef up their capabilities for monitoring and analyzing network traffic for the presence of cyberthreats."

Notable findings include:

- ☑ IDS/IPS, secure email gateways, and stateful inspection firewalls are the most frequently deployed defenses.
- ☑ NAC technology also enjoys fairly widespread adoption (likely as result of enterprise mobility initiatives).
- ☑ User activity monitoring, privileged user management, and identity and access management all received "in use" scores of greater than 60% -- indicating that considerable attention is being paid to better understanding and controlling the activities of authorized users.
- ☑ NGFWs were earmarked as the top network security investment over the coming year.
- ☑ With network behavior analysis (NBA), big data security analytics, security information and event management (SIEM), and full-packet capture analysis also near the top of the leader board for the coming year, it seems clear that many organizations are planning to beef up their capabilities for monitoring and analyzing network traffic for the presence of cyberthreats.

Endpoint and Mobile Security Deployment Status

The same approach was used to gain insight into deployment status and acquisition plans for both endpoint and mobile security technologies. Let's begin with the former (see Table 2).

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=676*)

	Currently in use	Planned for acquisition	No plans
Anti-virus / anti-malware (signature-based)	86%	9%	5%
Content filtering (by file type)	69%	13%	18%
Application control (whitelist/blacklist)	67%	17%	16%
Disk encryption	67%	15%	18%
Advanced malware analysis (signatureless)	57%	20%	23%
Data loss prevention (DLP)	55%	19%	26%
Self-remediation for infected endpoints	47%	20%	33%

<-- Less Frequency ------- More Frequency -->

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

"There's still considerable room for improvement – both in developing new endpoint security technologies and better utilizing the ones organizations already have."

Overall, it appears that most organizations are defending their endpoints by combining multiple technologies to establish an effective solution. One noteworthy item, however, is that 14% of these combinations appear to lack any sort of traditional, signature-based anti-malware component. It is unclear whether this speaks to the steadily improving effectiveness of signature-less technologies or some other factor.

We're also compelled to point out that despite fairly high deployment rates for the technologies listed here, endpoints are still cited as the weakest link in most organizations' defense chain (see Security Posture by IT Domain). This suggests there's still considerable room for improvement – both in developing new endpoint security technologies and better utilizing the ones organizations already have.

Shifting to the mobile security landscape, here, too, it seems that multiple technologies are being used to get the job done (see Table 3).

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=676*)

	Currently in use	Planned for acquisition	No plans
VPN to on-premises security gateway	60%	16%	24%
Network access control (NAC)	56%	21%	23%
Mobile device / application management (MDM/MAM)	45%	30%	25%
VPN to cloud-based security gateway	45%	18%	36%
Mobile device file / data encryption	44%	26%	30%
Secure workspace / containerization	43%	22%	35%
Virtual desktop infrastructure (VDI)	42%	27%	31%
Mobile device anti-virus / anti-malware	36%	27%	37%

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

"It's clear that VPN and NAC technologies are the dominant choices for helping to secure remote/mobile devices and their users."

It may also be the case that different combinations of technologies are being employed to meet the unique requirements of varying use cases and constituents. For example, an IT security team might deploy virtual private network (VPN), NAC, and virtual desktop infrastructure (VDI) for its general user population, but then deploy VPN, NAC, mobile device management (MDM), and containerization solutions for its mobile executives.

Regardless, it's clear that VPN and NAC technologies are the dominant choices for helping to secure remote/mobile devices and their users. MDM and MAM (mobile application management) solutions are also continuing to receive considerable attention, as they rank slightly ahead of all other mobile security solutions in terms of expressed acquisition plans reported by respondents for the coming year.

Root-Cause Analysis Capabilities

Participants were asked to indicate whether their organizations have the necessary tools to investigate and determine the root cause and material impact of security breaches (see Figure 5).

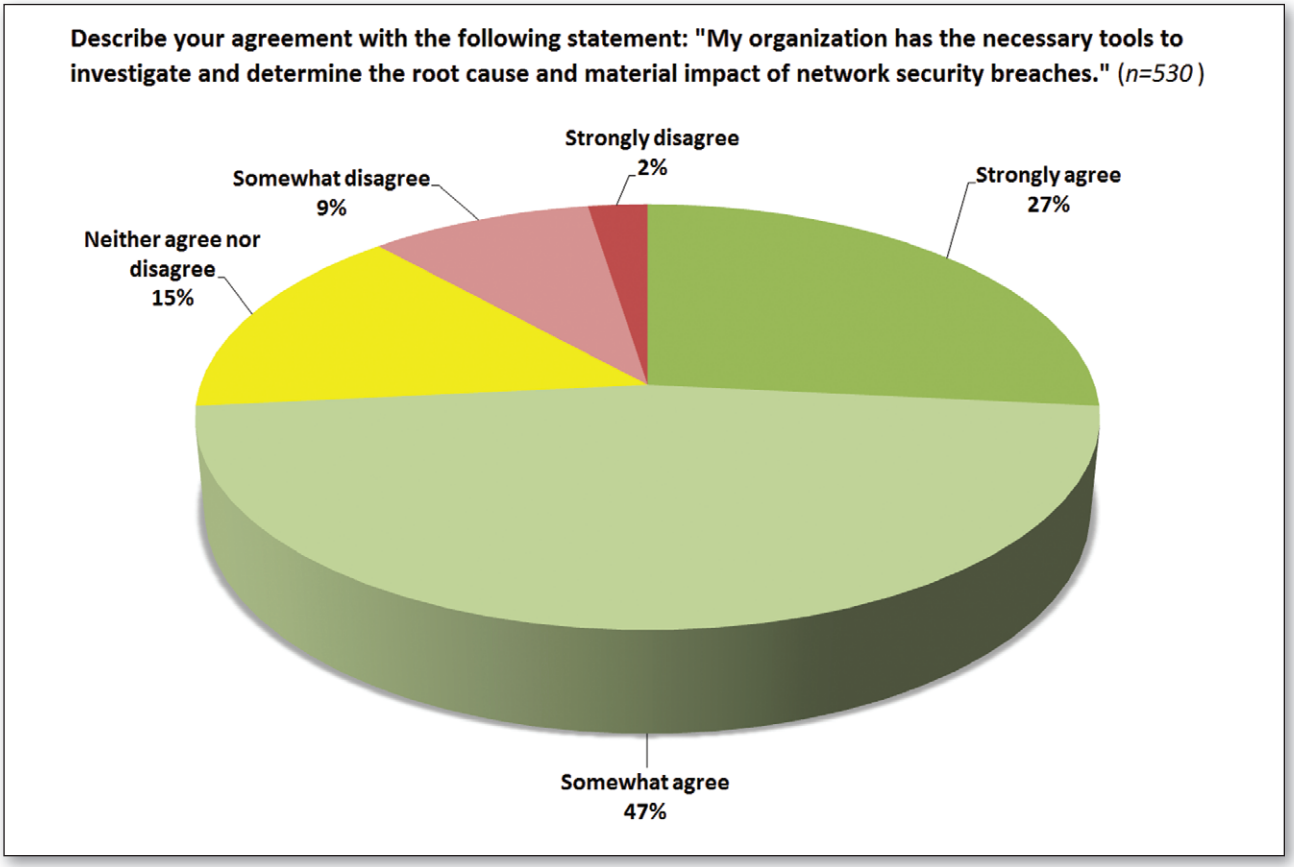

Figure 5: Adequacy of root-cause analysis capabilities

"Approximately one in four respondents were unconvinced that they have the necessary tools at their disposal to adequately investigate security breaches."

Although nearly three-quarters expressed a measure of confidence in this regard, approximately one in four respondents were unconvinced that they have the necessary tools at their disposal to adequately investigate security breaches.

We also observe that European respondents are incrementally more confident in their organizations' root-cause analysis capabilities: while 82% of the Europeans indicated they "somewhat" or "strongly" agreed that their organizations have sufficient capabilities in this area, only 70% of their North American counterparts responded in a like manner.

Section 2: Perceptions and Concerns

The exploration of cyberthreat defenses now 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 that have already been identified, 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 perceived effectiveness of various countermeasures, along with factors that most often inhibit today's organizations from establishing adequate cyberthreat defenses.

Cut to the Chase

- Malware and phishing / spear phishing are of the most concern to respondents
- APTs and DoS/DDoS attacks are of the least concern

Types of Cyberthreats

Malware and phishing/spear phishing are the classes of cyberthreats that concern survey respondents the most (see Figure 6). Trailing by a relatively small margin are web application attacks, zero-day attacks, mobile device malware, and malicious insiders. Least concerning for this audience are advanced persistent threats (APTs) and denial (and distributed denial) of service (DoS/DDoS) attacks, which on a weighted average basis fell below the midpoint on our 5-point scale.

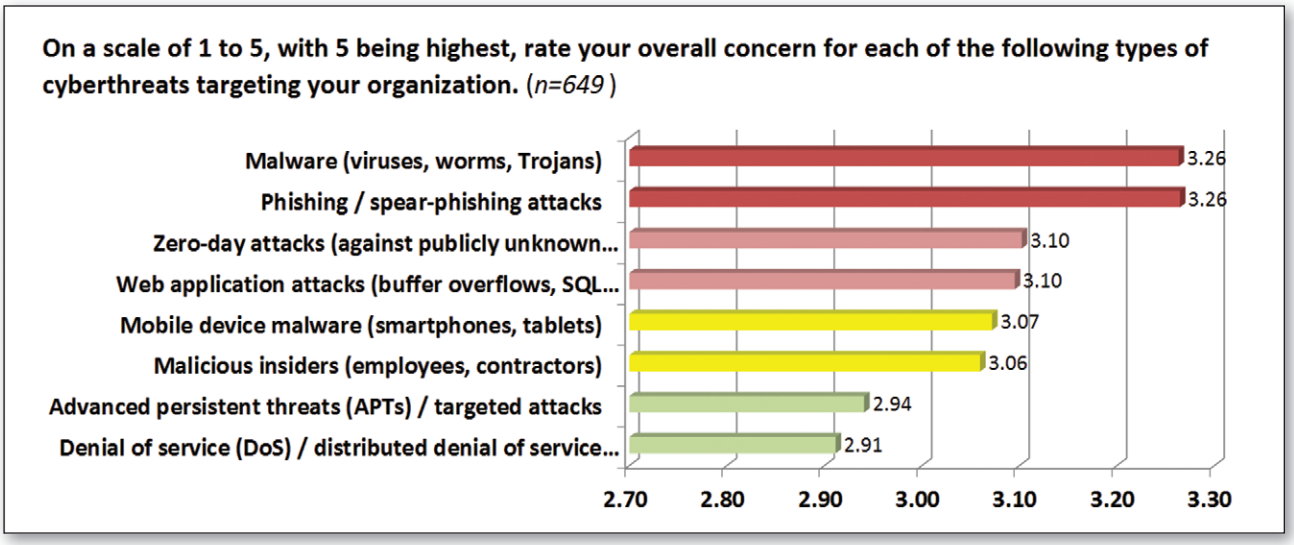

Figure 6: Relative concern by class/type of cyberthreat

"Malware and phishing/ spear phishing are the classes of cyberthreats that concern survey respondents the most."

However, this high-level summary only tells part of the story. Examining the raw data more closely yields a few additional observations:

- ☑ The class of threats most often receiving the designation "extremely concerned" was phishing/ spear phishing attacks (least often was DoS/DDoS attacks).
- ☑ Mobile device malware and DoS/DDoS attacks were tied as the threat classes most often receiving the "not concerned" designation (malware had the fewest instances of this designation).
- ☑ For each class of threats, "not concerned" was chosen by at least 8% of the respondents.
- ☑ Overall, the responses were widely distributed. For most classes of threats, "extremely concerned" and "very concerned" responses were largely offset by an equal distribution of "mildly concerned" and "not concerned" responses. This indicates that the perceived risk of different classes of threats is organization specific and, therefore, relying solely on the weighted averages is not sufficient in this case.

Sources of Cyberthreats

Looking next at the sources of cyberthreats, the data indicates that organizations are generally more concerned about cybercriminals as a group, as opposed to the sub-categories of state-sponsored and politically motivated hackers (see Figure 7). In addition, they are also more concerned with malicious insiders than any individual external source of cyberthreats.

Survey Insight

Respondents were more concerned about potential threats from malicious insiders than any single source of external threat.

Once again, examining the raw data reveals a handful of additional points of interest:

- ☑ Approximately 10% of respondents expressed no concern at all about malicious insiders and cybercriminals
- ☑ Approximately 20% shared the same lack of concern for both state-sponsored and politically motivated hackers
- ☑ At the other end of the spectrum, just under 10% were extremely concerned about all sources of cyberthreats

Comparing the results for this survey question to those for the preceding question also suggests that organizations are generally less concerned about the source of a threat than its type.

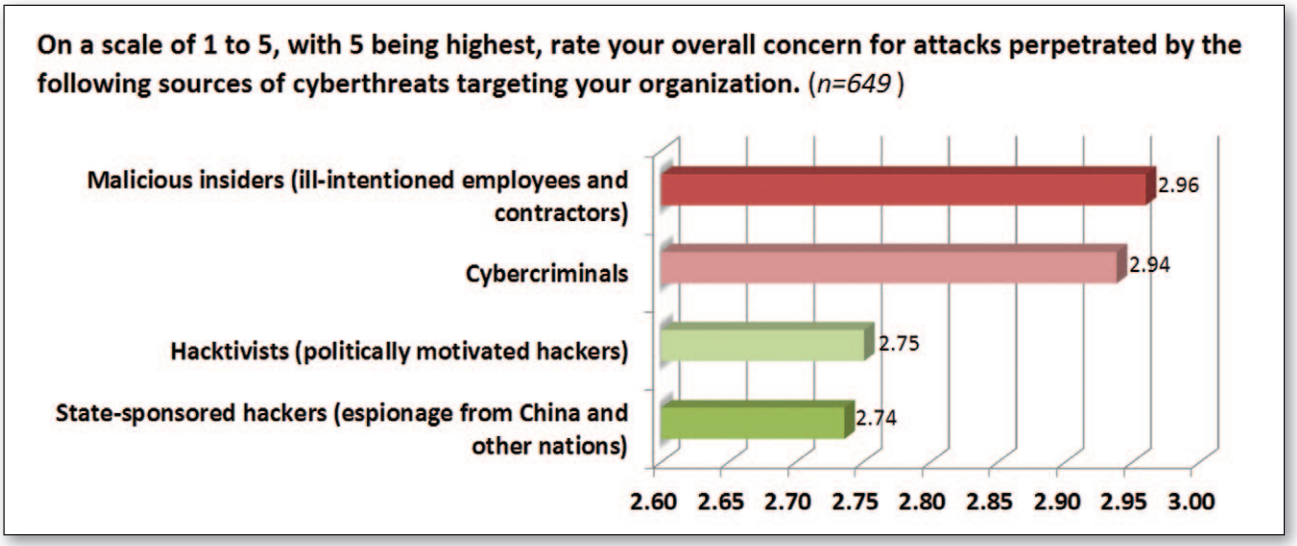

Figure 7: Relative concern by source of cyberthreat

Internal vs. External Cyberthreats

When asked specifically about their relative concern regarding internal threats (from ill-intentioned employees or contractors) compared to external ones (from outside hackers), slightly more than one-quarter of the respondents indicated an equal level of concern about both sources (see Figure 8). (Note: for this survey question all types of external threat sources have been aggregated together; whereas for the previous question, they were evaluated individually.)

"The concern for external threats outweighs that for internal threats by a ratio of approximately 2.5 to 1."

Examining the balance of the responses, we see that the concern for external threats outweighs that for internal threats by a ratio of approximately 2.5 to 1 (52% for "significantly more concerned" and "somewhat more concerned" about external threats compared to 21% for "significantly more concerned" and "somewhat more concerned" about internal threats).

Although this result cannot be ignored, it's important to also consider another perspective supported by the data: a full three-quarters of respondents indicated more than a little concern about internal threats.

The only regional finding of note is that European respondents had a somewhat more balanced perspective overall, with 36% expressing equal concern about internal and external threats. This compares to 24% for North American participants.

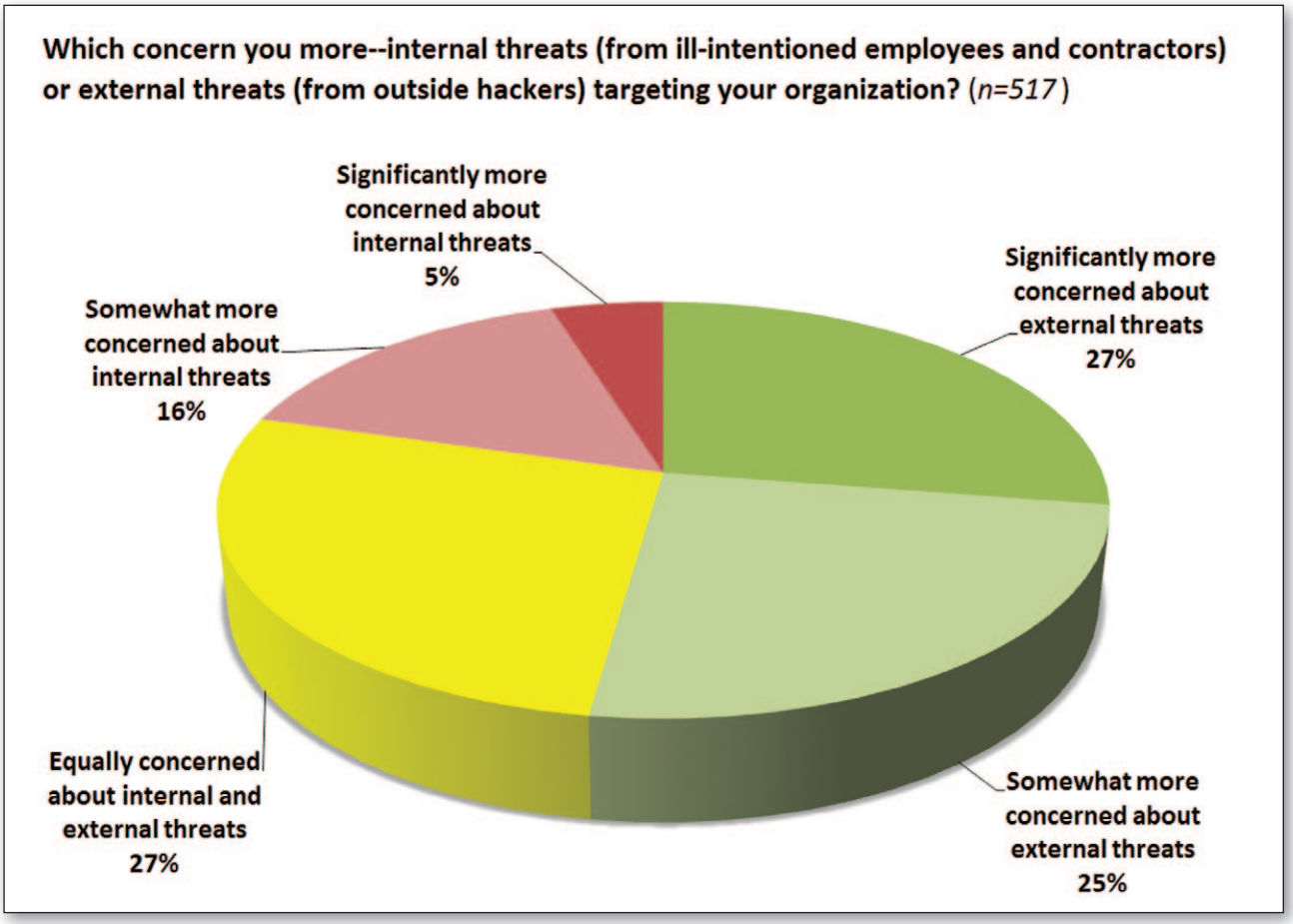

Figure 8: Relative concern for internal vs. external cyberthreats

Survey Insight

NAC and NGFW solutions are perceived by respondents as having the greatest potential to defend today's cyberthreats.

Perceived Effectiveness of Selected Defenses

Respondents were asked to rate their perceived effectiveness of various cyberthreat defense solutions on a scale of 1 to 5, with 5 being the highest. The results, in the form of weighted averages, are depicted in Figure 9.

Although rating effectiveness across different classes of solutions intended to address different problems is not exactly fair, the data still reveals two noteworthy items:

- ☑ On average, all of the solutions are perceived as being between "somewhat effective" and "very effective." Indeed, the variation in ratings both from one solution to the next and from top (NAC) to bottom (MDM) is not that significant.
- ☑ Overall, solutions that reduce an organization's attack surface – either by eliminating vulnerabilities

or shielding them – are generally viewed as more effective at what they do than those that work in a less black-and-white manner and require greater degrees of interpretation or analysis to operate (e.g., big data security analytics, advanced malware analysis, network behavior analysis, and full-packet capture analysis).

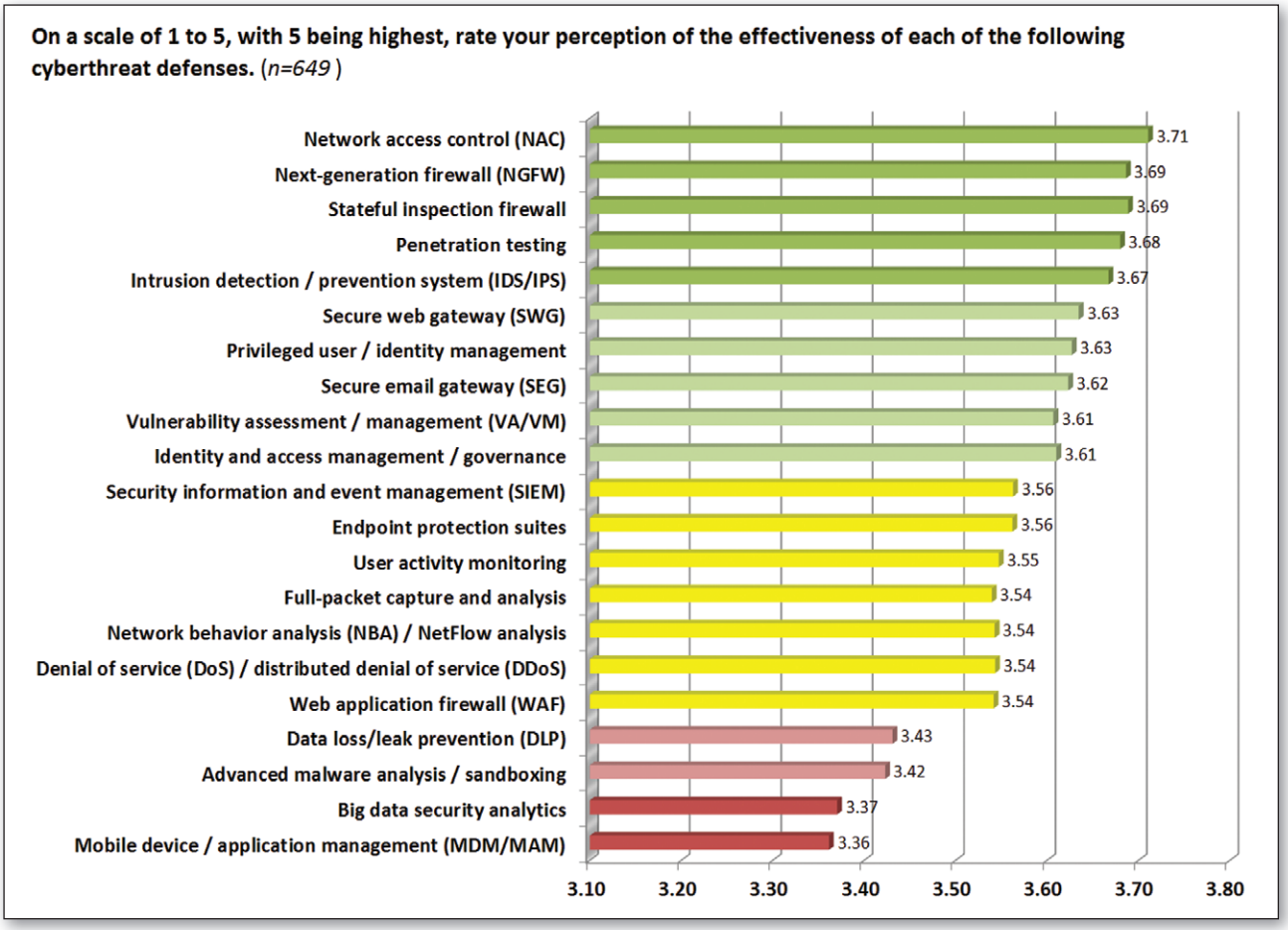

Figure 9: Perceived effectiveness of cyberthreat defenses

Barriers to Establishing Effective Defenses

Establishing effective cyberthreat defenses is by no means easy to do. If it were, one would expect far fewer successful cyberattacks and far higher confidence by IT security practitioners in the level of security investments made by their organizations. Part of the issue is undoubtedly the ever-evolving threat landscape. Hackers have a seemingly endless capacity to advance their wares – not to mention that, as defenders, organizations can only guess at hackers' next moves.

"Turning to the survey data, 'low security awareness among employees' tops the charts, with 'lack of budget' close behind."

But what about other factors? What are the other obstacles that IT security teams must overcome and, more importantly, which of them are most significant?

Turning to the survey data, "low security awareness among employees" tops the charts, with "lack of budget" close behind. Although "too much data to analyze" appears in third position, there really isn't a significant gap between it and the next several items on the list. Not until the last entry – "lack of effective solutions in the market" – is there a discernible difference in the weighted responses. In this case, we view the results as a vote of confidence in the security solutions available to today's IT security practitioners (at least relative to the other obstacles they face).

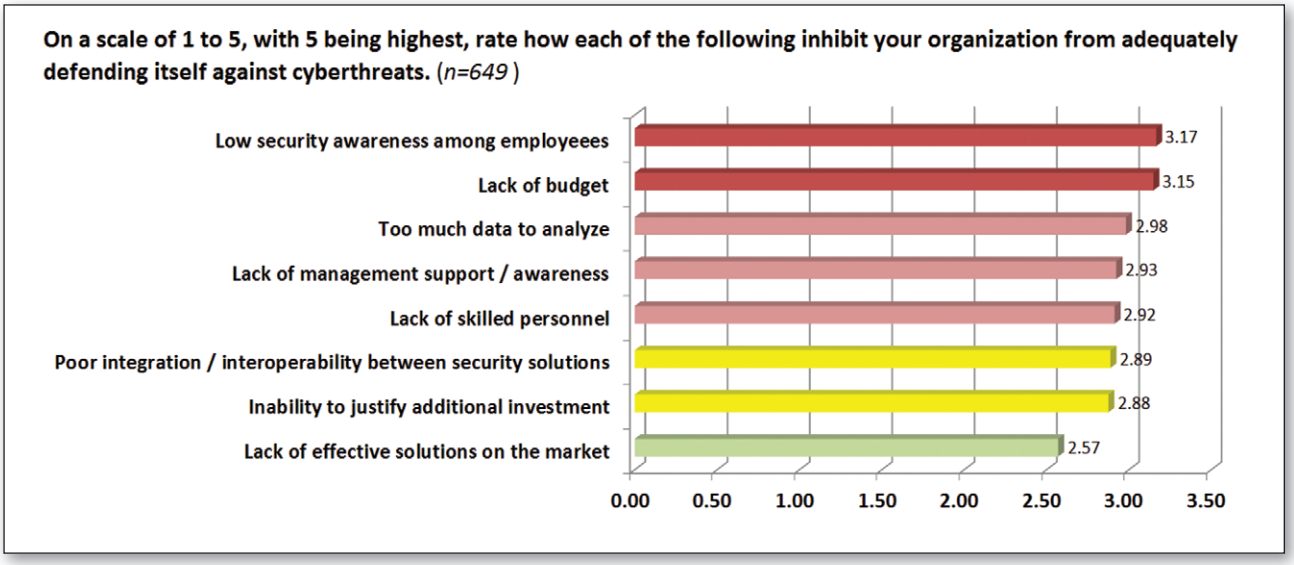

Figure 10: Inhibitors to establishing effective cyberthreat defenses

Section 3: Attack Surface Reduction

"75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching."

Contrary to what the popular press and the buzz at industry tradeshows would have one believe, establishing effective cybersecurity defenses requires more than simply implementing the latest and greatest technologies designed to detect the latest generations of elusive cyberthreats. Indeed, a more practical strategy is to first reduce one's attack surface, and then use a collection of complementary detection-oriented countermeasures to mitigate the residual risk.

Not only is such an approach intuitively appealing, it's also supported by the fact that the majority of cyberattacks still focus on exploiting known vulnerabilities. According to a report[1] published by the Center for Strategic & International Studies, 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.

The options for organizations to reduce their attack surface area are numerous and include tactics such as:

- ☑ reducing the number of open ports and services on Internet-facing systems;
- ☑ using next-generation firewalls to granularly control network and application access;
- ☑ eliminating all unnecessary protocols and services running on endpoints, servers, and other internal systems; and,
- ☑ leveraging identity and access management solutions to implement a least-privileges policy.

This section of the report focuses on another set of options: namely the tools and practices today's organizations are using to manage software vulnerabilities and host security misconfigurations.

Frequency of Network 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). The results are somewhat mixed (see Figure 11).

1. "Raising the Bar for Cybersecurity," James A. Lewis, Center for Strategic & International Studies, February 2013.

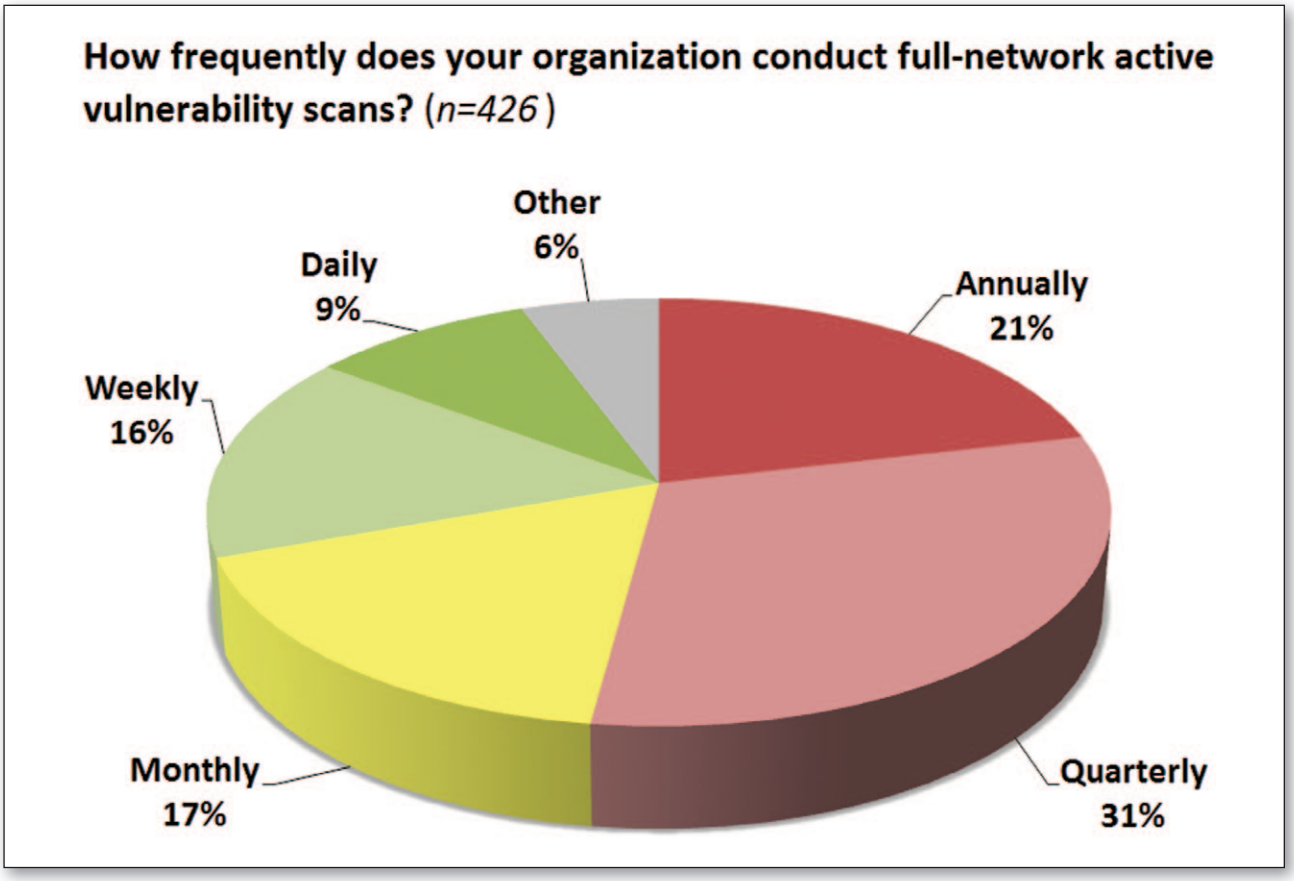

Figure 11: Frequency of full-network active vulnerability scans

Cut to the Chase

- 52% of responding organizations conduct full-network vulnerability scans quarterly or annually
- 25% of responding organizations scan daily or weekly

On one hand, we consider it a positive sign that slightly more than one-quarter of organizations are conducting full network scans weekly or daily. This represents a significant commitment to cybersecurity and likely indicates greater understanding of the tremendous value of continuous monitoring.

On the other hand, it is rather discouraging that approximately one in two organizations only scan their networks quarterly or annually. This finding is not particularly surprising, however, as these rates represent the minimum requirement for compliance with prevailing regulations and standards (e.g., the Payment Card Industry Data Security Standard, or PCI-DSS).

No statistically significant differences were observed by geographic region.

Purpose of Network Vulnerability Scans

Not surprisingly, most organizations use the results of their network vulnerability scans in multiple ways. Purposes range from prioritizing patch management efforts (62% of respondents) and gaining deeper insight into their network's attack surface (62%), to generating regulatory compliance reports (49%). A relatively modest percentage (29%) also use scan information as contextual data to increase the fidelity and meaningfulness of output from cybersecurity management systems – such as their SIEM solutions.

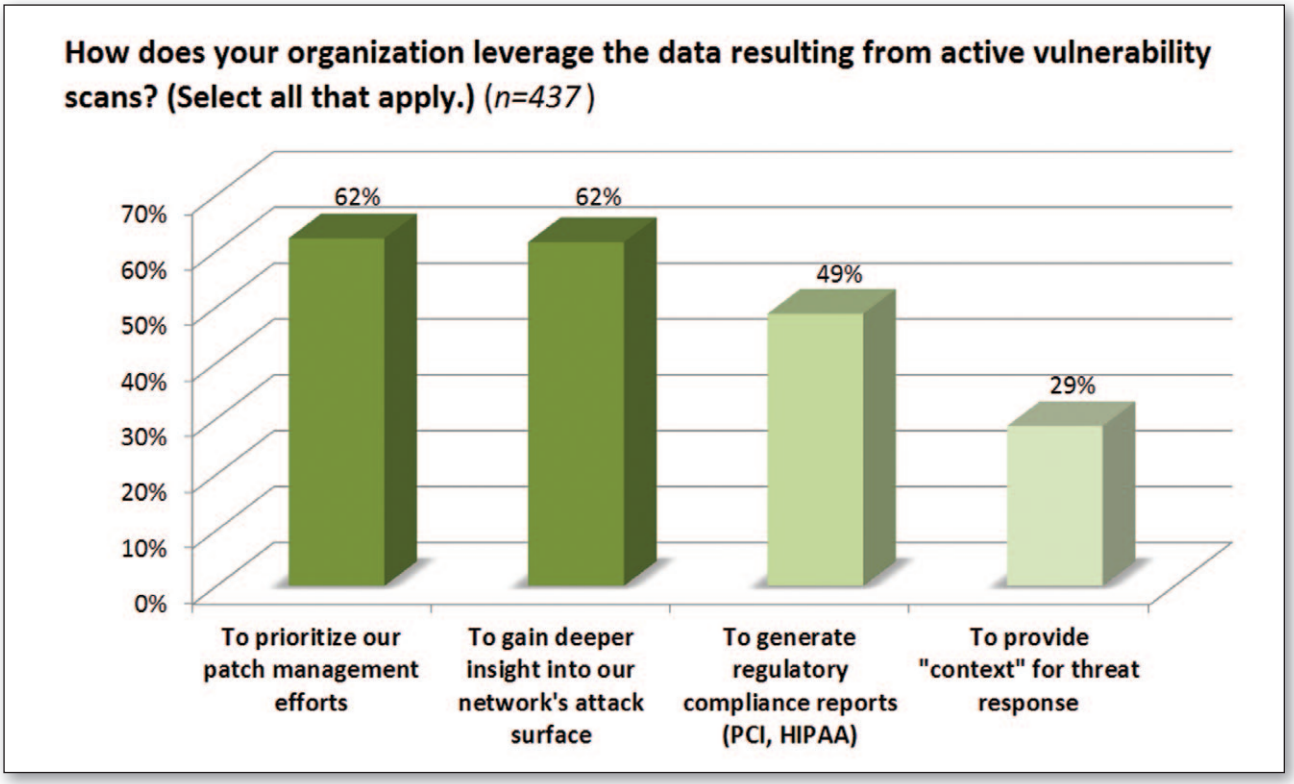

Figure 12: How organizations use vulnerability scan data

Host Security Misconfigurations

Host security misconfigurations – deviations of security settings for servers, client devices, and their software from a desired state – are another class of vulnerability that requires the attention of today's IT security teams. At a minimum, these "departures from normal" leave the door open for cyberthreats to access affected systems, gain a foothold, and then spread to other parts of the computing environment. They might also indicate risky activities being undertaken by ill-intentioned or misguided employees or, worse yet, the presence of malware that has already compromised the affected

system and instigated subtle configuration changes to better facilitate propagation and data exfiltration.

Survey participants were thus asked to indicate which technologies and approaches their organization regularly uses to identify host security misconfigurations (see Figure 13). The most popular response (53%) was NAC – which accounts for both standalone, full-featured NAC, as well as "NAC-lite" offerings, where a subset of associated capabilities is embedded in another security or infrastructure device.

Survey Insight

NAC is our respondents' preferred solution for identifying host security misconfigurations in endpoint devices.

Also well represented were dedicated security configuration management (SCM) tools (45%), followed closely by vulnerability assessment / management solutions (42%) – which often include the ability to scan target systems for considerably more than just the presence of known software vulnerabilities.

Demonstrating there's still considerable room for improvement in this area, nearly one-third of respondents indicated their organization relies solely on manual processes to detect host security misconfigurations, while another 10% appear to be doing absolutely nothing.

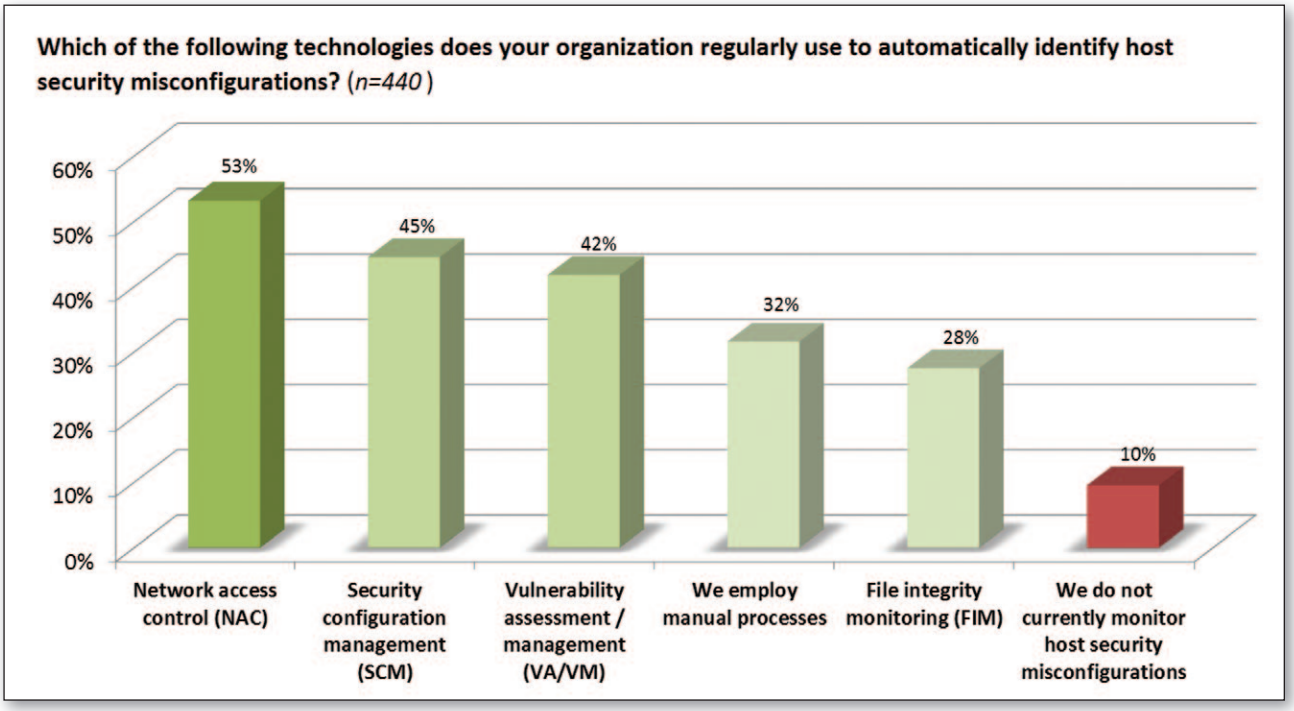

Figure 13: How organizations detect host security misconfigurations

Accounting for Transient Devices

So what about transient devices such as laptops, smartphones, and tablets? How are IT security teams handling vulnerability and security configuration management for devices that don't permanently reside on the corporate network and might not be connected to it when regularly scheduled scans are conducted?

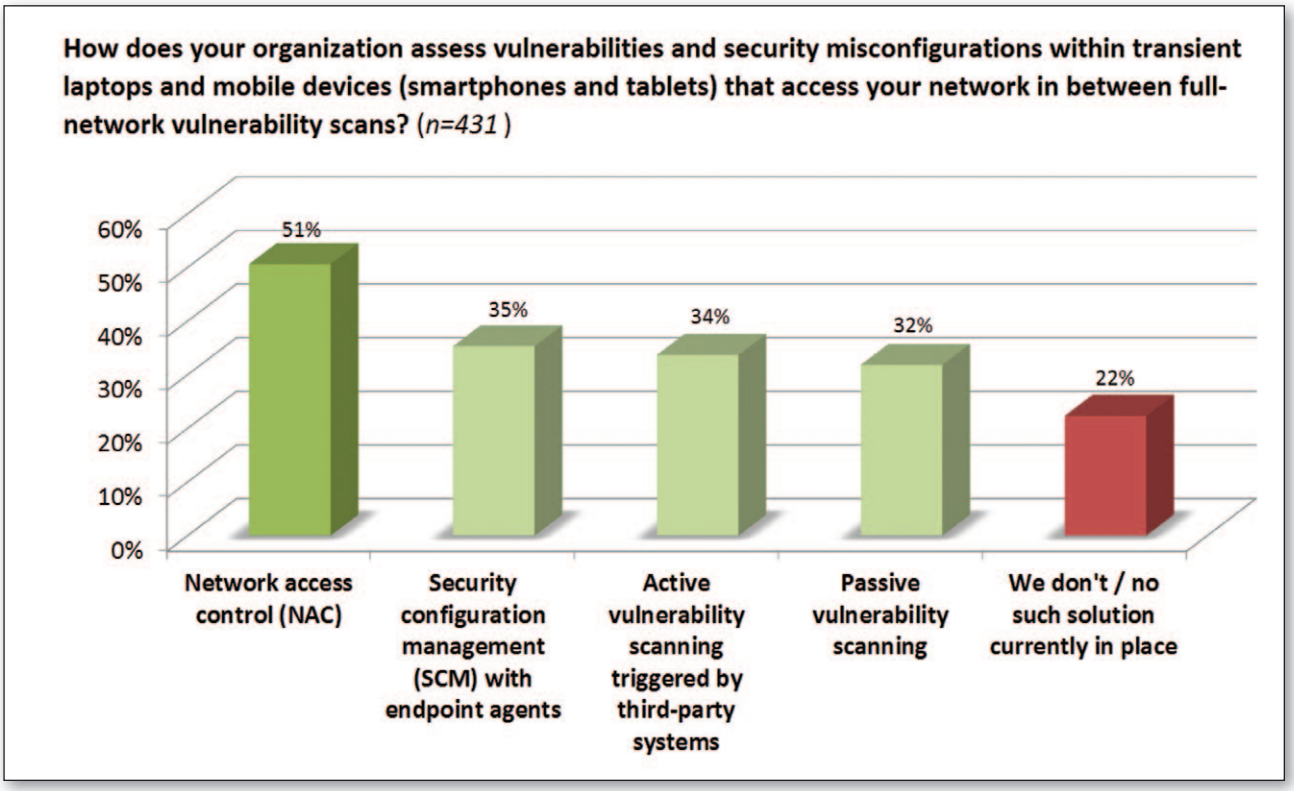

Figure 14: Detecting vulnerabilities and misconfigurations for transient devices

"More than one in five organizations continue to roll the dice by doing nothing to assess the state of their transient devices between regularly scheduled active scans."

Once again, NAC (51%) and SCM tools (35%) emerged as the top solutions (see Figure 14). These were trailed only marginally by passive vulnerability scanning (32%) – which works by detecting systems as soon as they connect to a network and analyzing associated communications traffic to extract vulnerability information – and traditional, active vulnerability scanners triggered by a third-party system (34%), such as a passive vulnerability scanner, SIEM, or NAC solution.

Despite the availability of effective solutions such as these, however, it appears that more than one in five organizations (24% North America, 18% Europe) continue to roll the dice by doing nothing to assess the state of their transient devices between regularly scheduled active scans.

Section 4: Future Plans

"Our data shows 2014 IT security budgets are in excellent shape."

As we well know, 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 in this regard were already revealed in an earlier section of the report, where we covered the network security, endpoint, and mobile security technologies planned for acquisition in 2014. This section further explores their future plans, along with some of the key factors driving their decision-making processes.

IT Security Budget Change

Likely the single biggest factor contributing to an IT security team's ability to affect change is their budget. Thankfully, our data shows 2014 IT security budgets are in excellent shape, with nearly 90% of organizations continuing to invest in cyberthreat defenses at least at the same level they did in 2013 (see Figure 15).

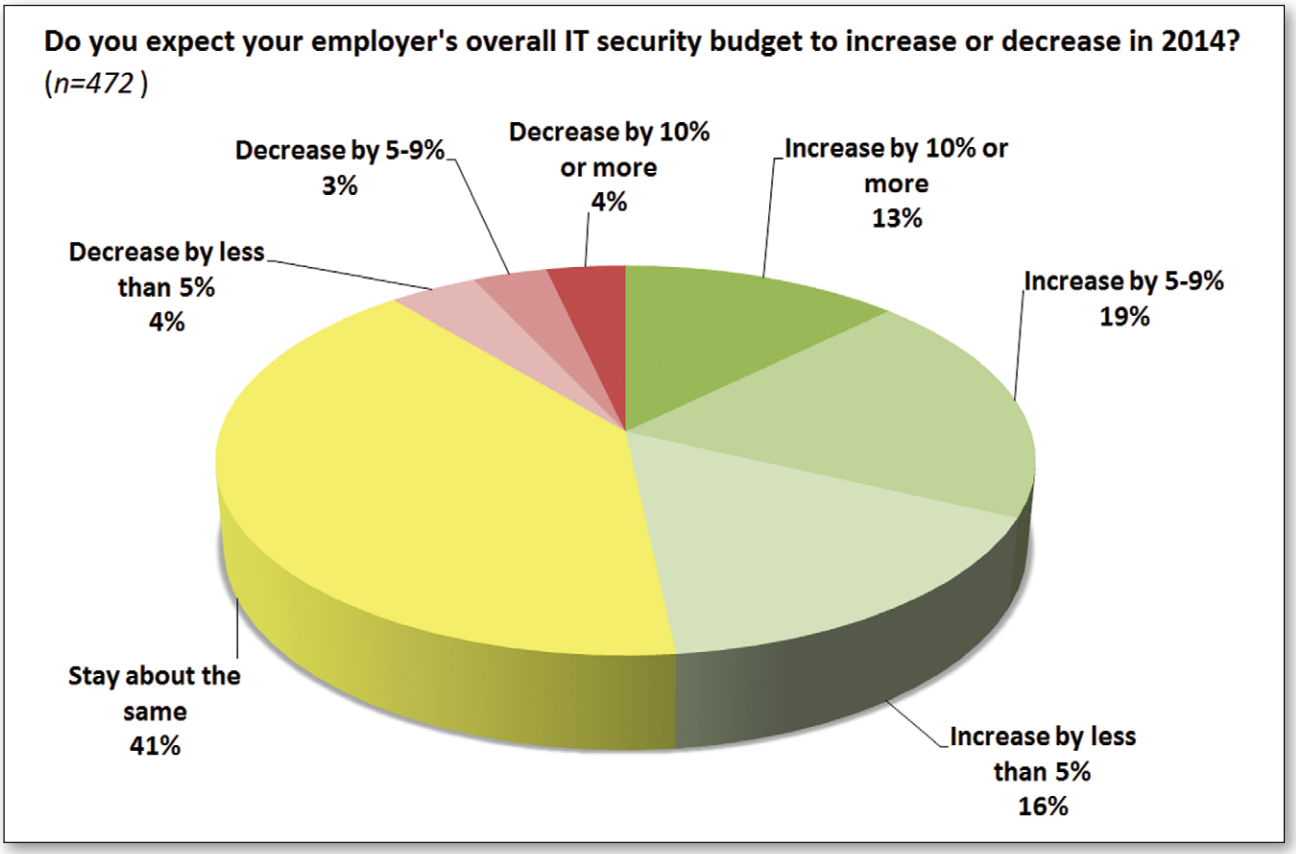

Figure 15: IT security budget changes for 2014

Survey Insight

BYOD has arrived! Within two years, more than three quarters of responding organizations will have BYOD policies in place.

The BYOD Invasion

From a cybersecurity perspective, user mobility and the proliferation of mobile device options is the Web 2.0 of this decade. To be clear, we're not suggesting that all of the security challenges of social media, social networking, and the advanced web technologies operating behind the scenes have been resolved; rather that mobile users and their devices are now the biggest security pain point for most of today's organizations.

A significant portion of this pain stems from the consumerization of IT and it's incorporation in the mobile world in the form of business-driven support for BYOD policies. With BYOD, IT security teams are forced to contend not only with an increasingly diverse population of devices – all with different native security capabilities and widely varying support from third-party security software – but also with the fact that control over these devices must be "shared" with their owners.

So when do organizations expect to have to deal with the challenges of this brave new BYOD world? For nearly one-third of our survey population, that day has already come (see Figure 16). Another 46% will follow within the next two years.

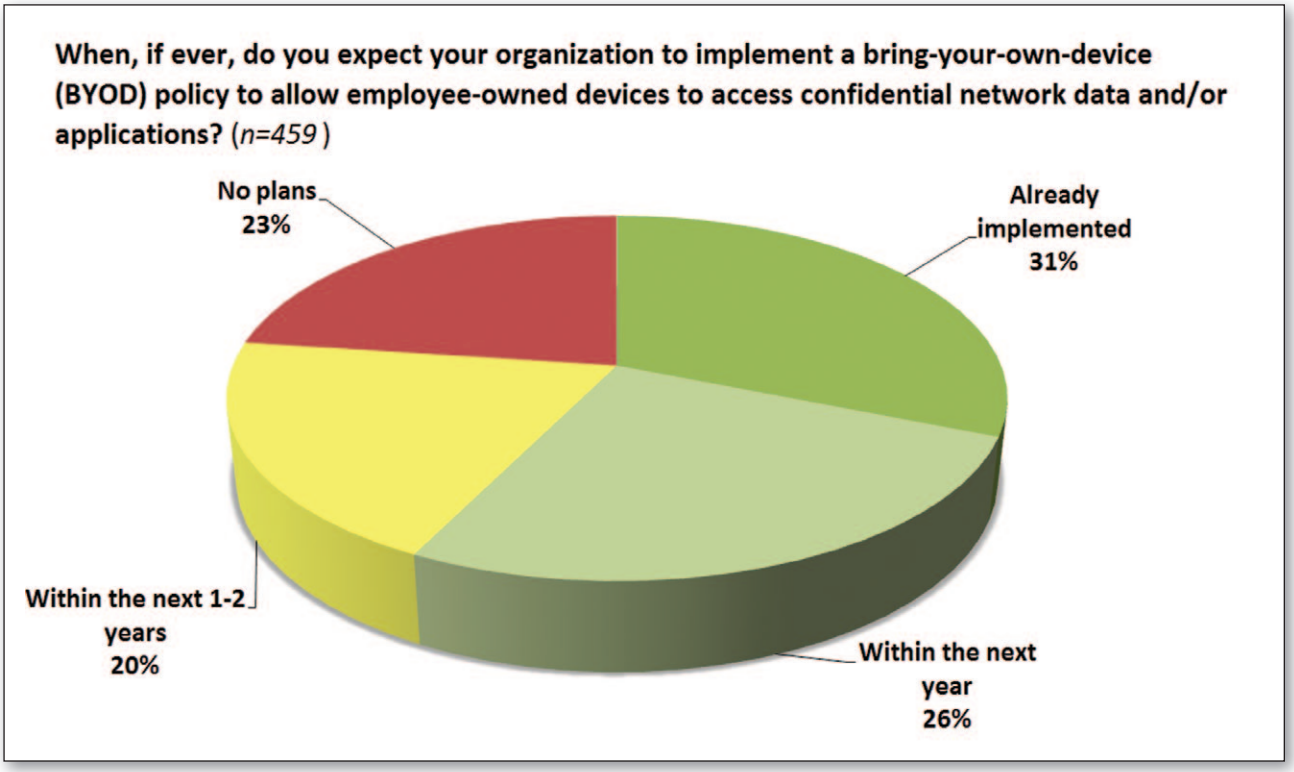

Figure 16: Timeframe for implementing BYOD policy

Digging deeper into the data, we also observe a somewhat less-aggressive adoption of BYOD among European survey participants: only 21% have already implemented a BYOD policy (compared to 35% for North America), while one-third (34%) indicate that they have no plans to do so at any time (compared to 19% for North America).

Endpoint Protection Plans

"More than half signaled they would be evaluating new solutions for endpoint anti-malware protection, either to augment or replace existing countermeasures."

It's not only mobile devices that are problematic for IT security teams, but other types of endpoints (desktops and laptops), too. Part of the issue is, and always will be, the potential for ill-advised user actions – such as opening suspicious email attachments, using USB memory sticks from untrusted sources, and, of course, visiting questionable websites. Compounding matters, however, is the steadily eroding effectiveness of signature-based AV engines in the face of advanced malware – featuring polymorphism and an ever-growing array of evasion techniques.

Given this situation, we asked participants about their organization's intent to evaluate new anti-malware solutions for endpoints. The results reinforce our earlier findings that endpoints remain a problem area for most organizations (see Figure 17). More than half (56%) signaled they would be evaluating new solutions for endpoint anti-malware protection, either to augment (34%) or replace (22%) their existing countermeasures.

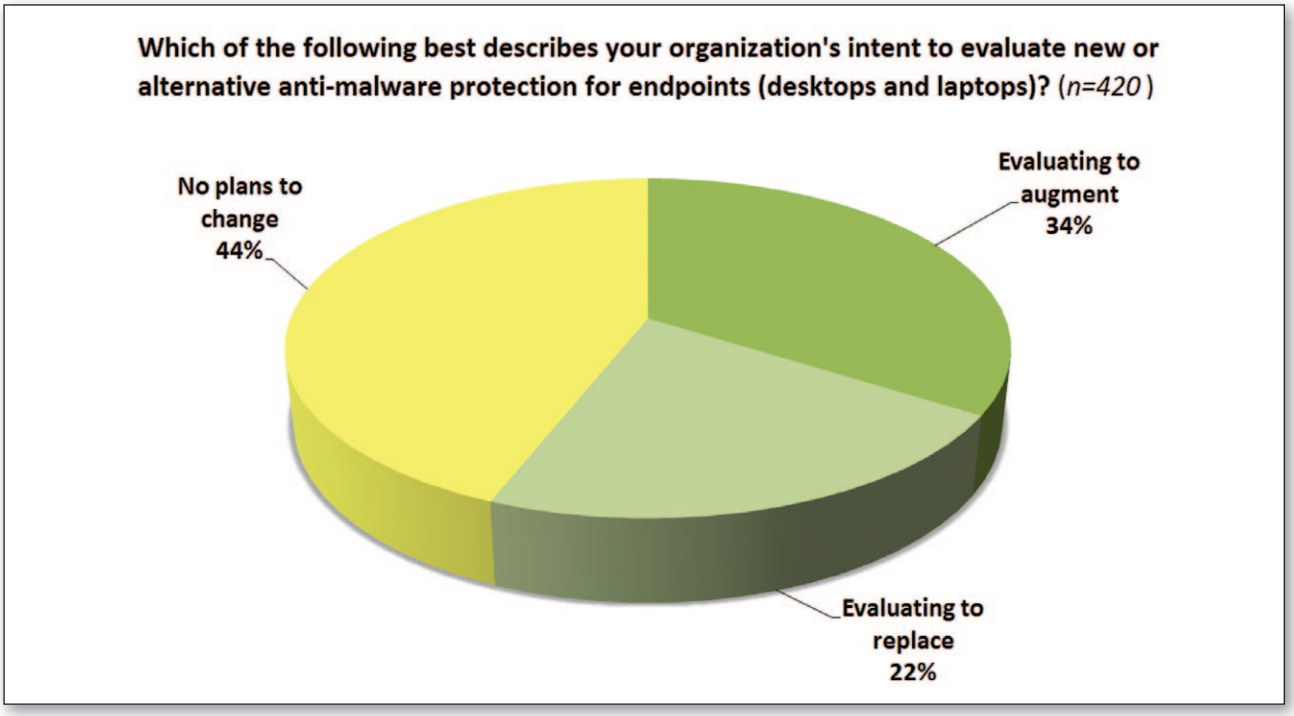

Figure 17: Plans for replacing or augmenting endpoint protection software

Survey Insight

When evaluating cyberthreat defense solutions, performance and security are slightly more important than detection accuracy to our respondents.

Top Selection Criteria

Which criteria most strongly influence an IT security team's selection of a new technology to fill a gap in its cyberthreat defenses? Conventional wisdom suggests that security effectiveness – how well a solution performs its main function (e.g., detecting known/unknown cyberthreats, detecting vulnerabilities, or blocking unauthorized transmissions) – should always lead the way.

Our data shows otherwise; or, at least, that security effectiveness –represented by "detection accuracy" and "frequency of threat intelligence updates" – is not alone at the top of the list. In fact, performance and scalability are rated slightly more important than security effectiveness by our survey population (see Figure 18).

This is not terribly surprising, however, as having one of these capabilities – security or performance/scalability – without the other is often pointless, especially for most enterprise-grade implementation scenarios.

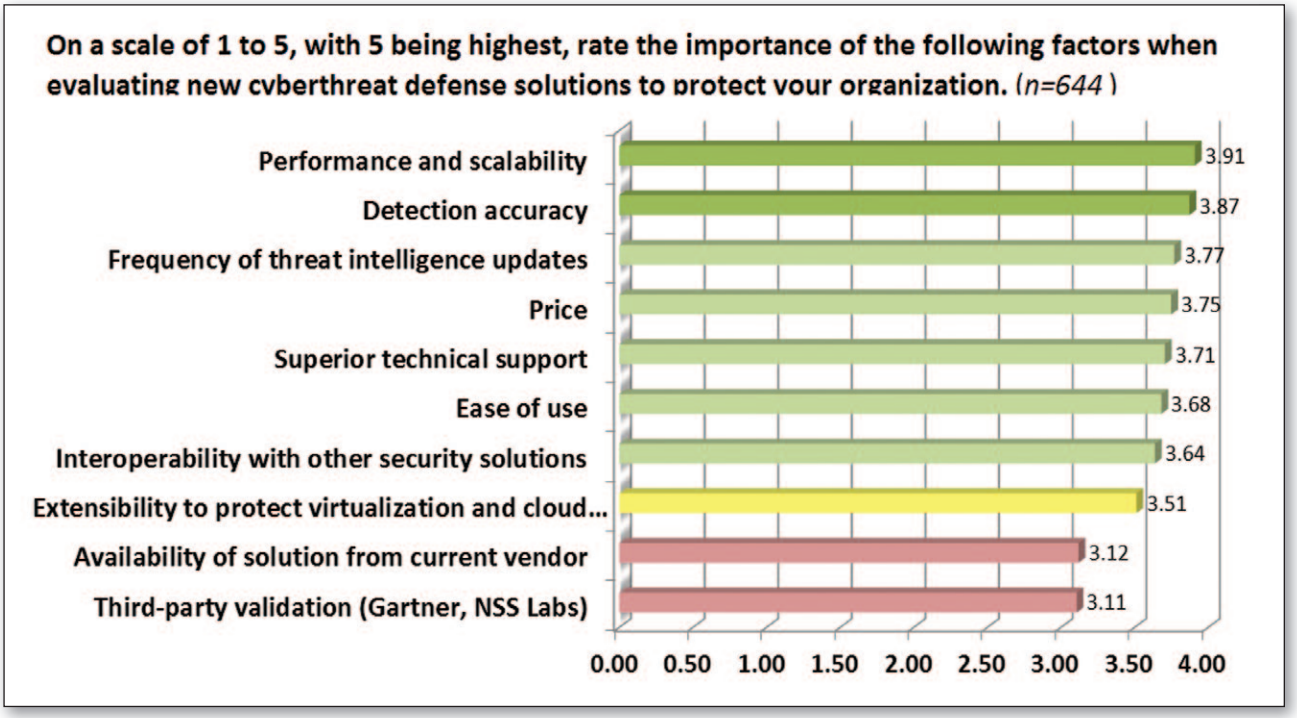

Figure 18: Prioritized selection criteria for cyberthreat defenses

Survey Insight

Validation by Gartner, NSS Labs, and other third-party entities is least important to our respondents when evaluating new solutions for cyberthreat defense.

Other observations include:

- ☑ Although performance/scalability and security effectiveness came out on top, the differences between these and the next handful of criteria on the list are not all that substantial. Price, ease of use, technical support, and interoperability with other solutions matter, too, and security solution providers that neglect any of these elements risk poor performance in the marketplace.
- ☑ Despite efforts at infrastructure and solution provider consolidation in other areas of IT, the relatively low score for "availability of solution from a current vendor" suggests this is a less important objective within IT security.
- ☑ Although external validation – for example, from Gartner or NSS Labs – may be useful for establishing a short list of candidate solutions, IT security buyers give it considerably less consideration relative to other criteria.

Form Factor Preferences

We asked our survey participants whether they had a preference for how cyberthreat defenses are packaged. The results are depicted in Figure 19.

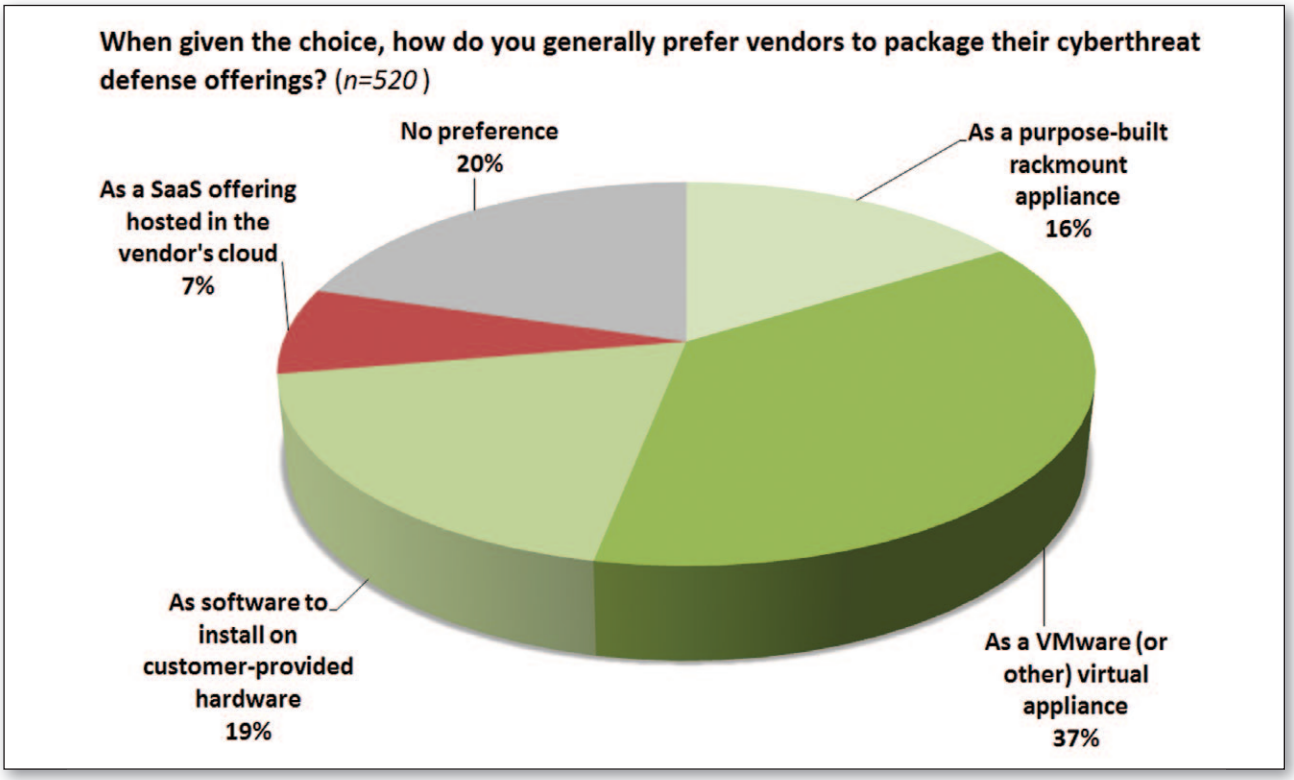

Figure 19: Preferred form factors for cyberthreat defenses

Cut to the Chase

- When given the choice, 56% of respondents prefer virtual appliances or software to install on customer-provided hardware
- Only 16% prefer purpose-built rackmount appliances
- Only 7% prefer SaaS-based solutions hosted in the vendor's cloud

Respondents signaled that the age of the virtual appliance is upon us – with 37% favoring that option. In comparison, purpose-built hardware appliances (16%) – once the form factor of choice, especially for network security technologies – trailed even the software-only option (19%). In addition, only 7% indicated a preference for a SaaS approach, where the security offering is hosted in the solution provider's cloud.

However, care must be taken in interpreting these findings. What IT security teams "generally prefer" doesn't necessarily reflect what they will ultimately purchase – or even, what's available in the market, for that matter. For example, consider cyberthreat defenses that process a lot of encrypted traffic, are otherwise compute intensive, and/or that operate in-line in high-throughput environments where the amount of introduced latency is an absolutely critical consideration. In such cases, there really is no practical alternative to a purpose-built hardware appliance, typically featuring specialized chip sets, custom silicon, and processing capacity unavailable to any general-purpose server hardware.

The Road Ahead

Although today's organizations seem relatively comfortable with many aspects of their cyberthreat defenses, it's also clear there's still work to be done.

IT security teams may be relatively satisfied with the level of investment their organizations have made in cyberthreat defenses (74%), and optimistic (perhaps overly so given last year's rates for successful cyberattacks) that the networks they are defending will not be breached over the coming year (62%). They may also be confident about the protection of IT infrastructure domains within their control (e.g., datacenter servers and the network perimeter), and their ability to get to the root cause of any significant incidents (74%).

And to be clear, this confidence is a good thing; without it, the war against cyberthreats is lost. However, as the data from the 2014 Cyberthreat Defense Report survey indicates, there is still plenty of room for improvement. For example:

- ☑ More than a quarter of our survey respondents paint a bleaker picture, one that suggests their organizations have yet to establish a reasonably effective foundation for cyberthreat defense. For them, the road ahead will be arduous, as they must first play "catch up" before gaining the opportunity to play "keep up."
- ☑ Conventional endpoint devices (desktops and laptops) continue to be a weak point in most organizations' defenses.
- ☑ Mobile devices (smartphones and tablets) are even more problematic, not only due to their greater portability, but also because of the compounding complexities introduced by inevitable BYOD initiatives (at 31% of organizations now, and at 77% within two years).
- ☑ Reining in social media/networking applications (e.g., to avoid leakage of sensitive data through these channels) remains, at best, a work-in-progress.
- ☑ Investment levels and acquisition plans are still fairly low for many of the next-generation monitoring, analysis, and threat intelligence tools most likely to be effective against advanced malware and targeted attacks (e.g., advanced malware analysis and sandboxing, big data security analytics, and network behavior analysis).
- ☑ Many organizations' efforts at reducing their attack surface are still deficient, which is surprising given the high impact such efforts are likely to yield. Increased frequency of scanning for vulnerabilities and host security misconfigurations and making more thorough use of the resulting data would certainly be beneficial in many cases.

In addition, the relative security and confidence of today can be gone tomorrow. As defenders, IT security teams can only make educated guesses at what attackers will try next, and where they will try it. This also means these teams need to provide protection for practically everything in their computing environments, even as those environments are experiencing near-continuous change (in the form of new applications, systems, technologies, and delivery models). The bottom line is that maintaining effective cyberthreat defenses not only requires constant vigilance, but also an eye on the road ahead.

Looking beyond the scope of the 2014 Cyberthreat Defense Report survey, here are a handful of additional items that we believe will warrant close attention from IT security teams going forward:

- ☑ **The cloud computing paradox.** From a cybersecurity perspective it's true that many aspects of public cloud services are no different from the managed and outsourced computing services IT security teams have already dealt with for years. However, what is significantly different – for both public and private varieties – is the emergence of all-powerful cloud management and orchestration platforms and the extensive, open APIs they (and other systems) can leverage. The power to turn on, turn off, and otherwise reconfigure entire swaths of infrastructure has never been at once so concentrated and so diffused. Among numerous other protections, this area simply screams for least privileges access control and corresponding identity and access management/governance.
- ☑ **Application-layer DoS attacks.** The omitted "D" (for distributed denial-of-service, or DDoS) is not a mistake. This relatively new and rising class of threats does not depend on an insurmountable flood of network traffic to be effective. Instead, all that is required is for a single node (or handful of them) to issue just the right commands and make just the right requests of an application to kick off a disproportionate amount of back-end processing – such as an exceedingly complex calculation or search operation. The net result is a hung application or saturated application infrastructure, triggered by a low volume of seemingly legitimate traffic. Put another way, the result is the need for a new class of DoS and web application protection capabilities.
- ☑ **Closed-loop defenses.** The current generation of solutions for dealing with advanced cyberthreats, including targeted attacks and rapidly morphing malware, focus primarily on detection – for example, by engaging out-of-band analysis techniques. Actually preventing the corresponding threat activities from continuing is typically left as a separate exercise that requires IT security staff to update and possibly re-configure in-line defenses, such as NGFWs. This approach, however, will become untenable as the frequency of advanced cyberthreats continues to increase and a growing backlog of mitigation activities leaves the computing environment unprotected for extended periods of time. As a result, IT security teams will increasingly need to pursue closed-loop defenses, where integration between different countermeasures enables automated response to out-of-band detection events.
- ☑ **Network virtualization.** The next "big thing" in infrastructure virtualization, network virtualization technology is poised to revolutionize network infrastructure and delivery of network services (e.g., routing, switching, and load balancing). It also has significant implications for deployment of network-based countermeasures and how they and other security technologies will need to be designed to maintain visibility and control despite the ever-increasing portability of computing workloads and the growing irrelevance (or at least fluidity) of certain policy enforcement attributes, such as a system's IP address or actual physical location.

For further insights on these and other emerging areas pertinent to IT security, be on the lookout for the next installment of the Cyberthreat Defense Report, currently scheduled for release in February 2015.

Appendix 1: Survey Demographics

75% of our 763 qualified survey participants specified United States of America or Canada as their country of residence. Although the balance of the survey population is spread across nine European countries, the majority of this group is from the United Kingdom, France, and Germany.

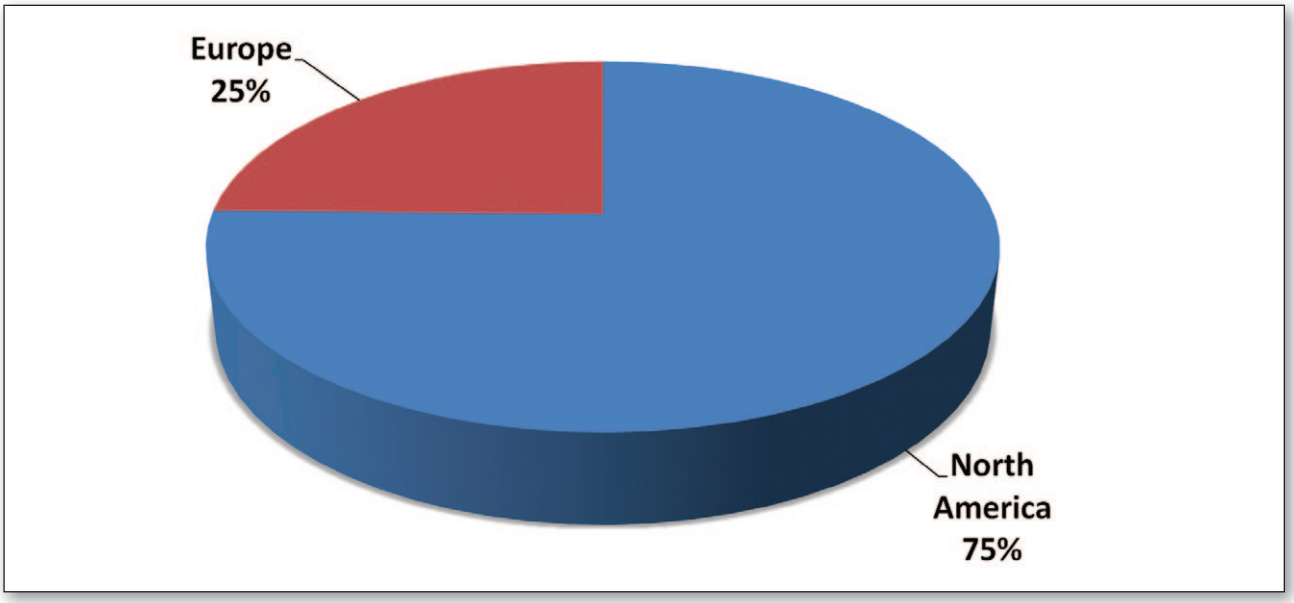

Figure 20: Survey participation by geographic region

As for the roles of our survey participants, over one-quarter hold senior positions (CIO, CISO, or IT security manager/director) within IT security. The remaining three-quarters are split almost evenly among IT security administrators/operations staff, IT security architects and auditors, and personnel identifying their position within IT security as "other."

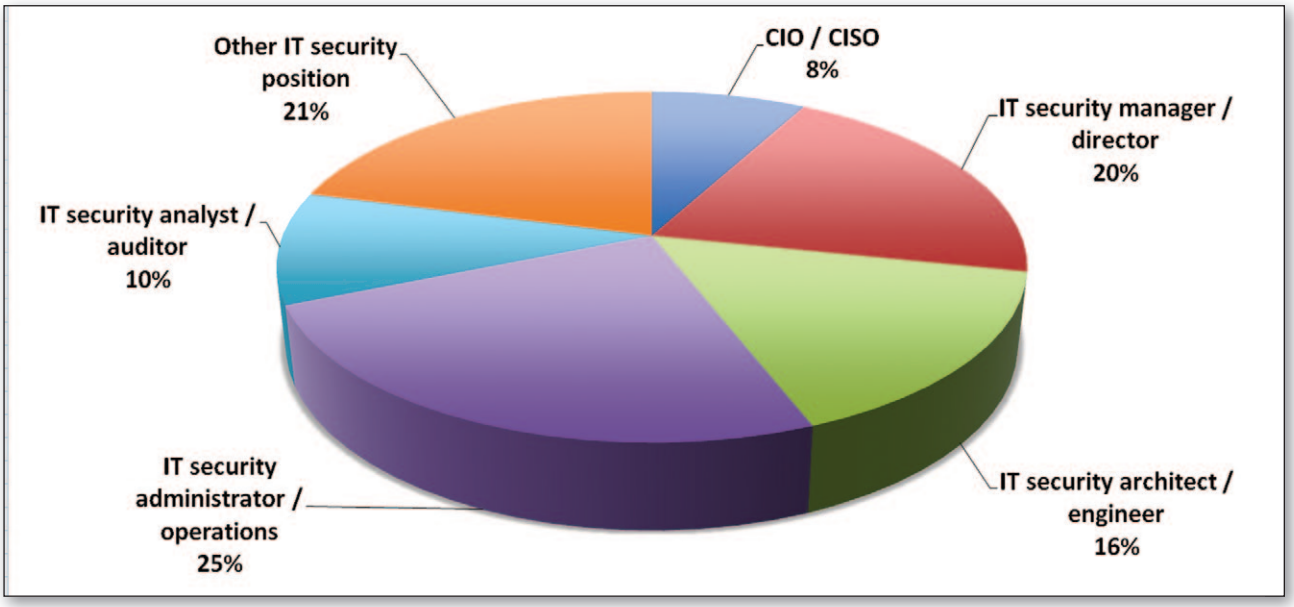

Figure 21: Survey participation by IT security role

Nearly 40% of the survey respondents are from enterprises with more than 10,000 employees. The largest segment of the survey population (46%) is from organizations with between 1,000 and 10,000 employees. Only 15% of participants are from smaller organizations of between 500 and 1,000 employees.

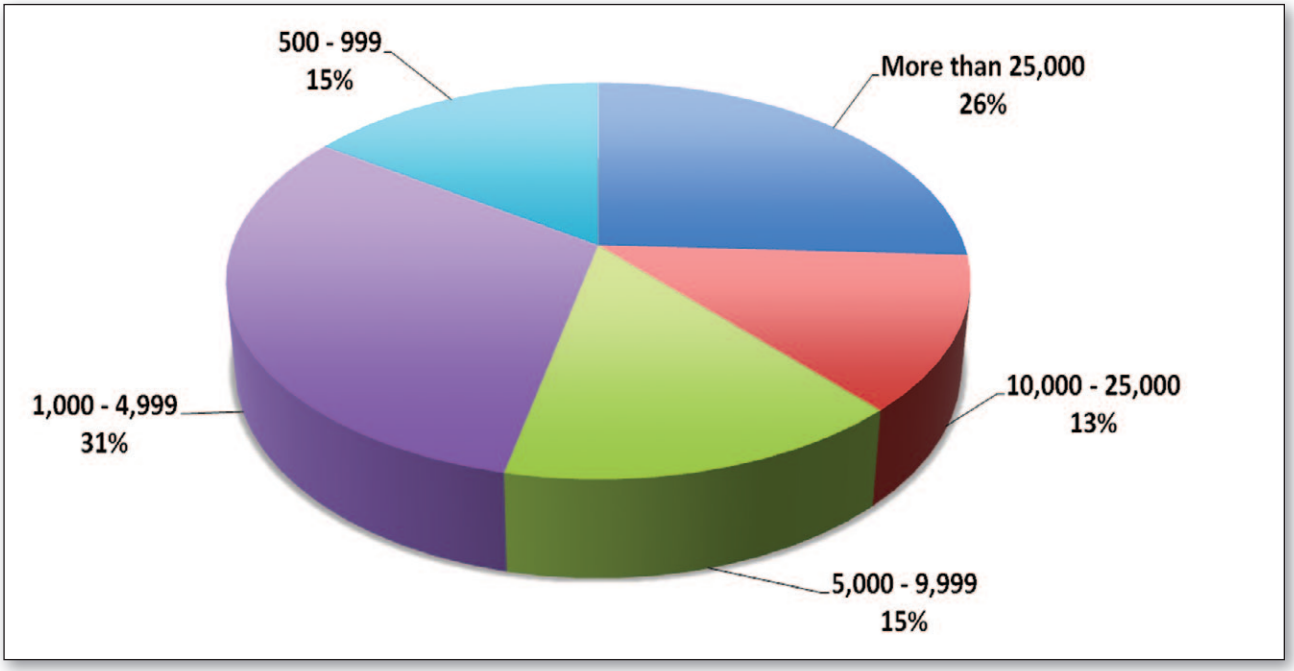

Figure 22: Survey participation by organization employee count

Distribution of survey participants by vertical industry is fairly broad, with representation across 19 industry segments. The top six segments – telecom/technology, education, financial services, government, manufacturing and healthcare – accounted for nearly 70% of all respondents. No single industry accounted for more than 16% of participants.

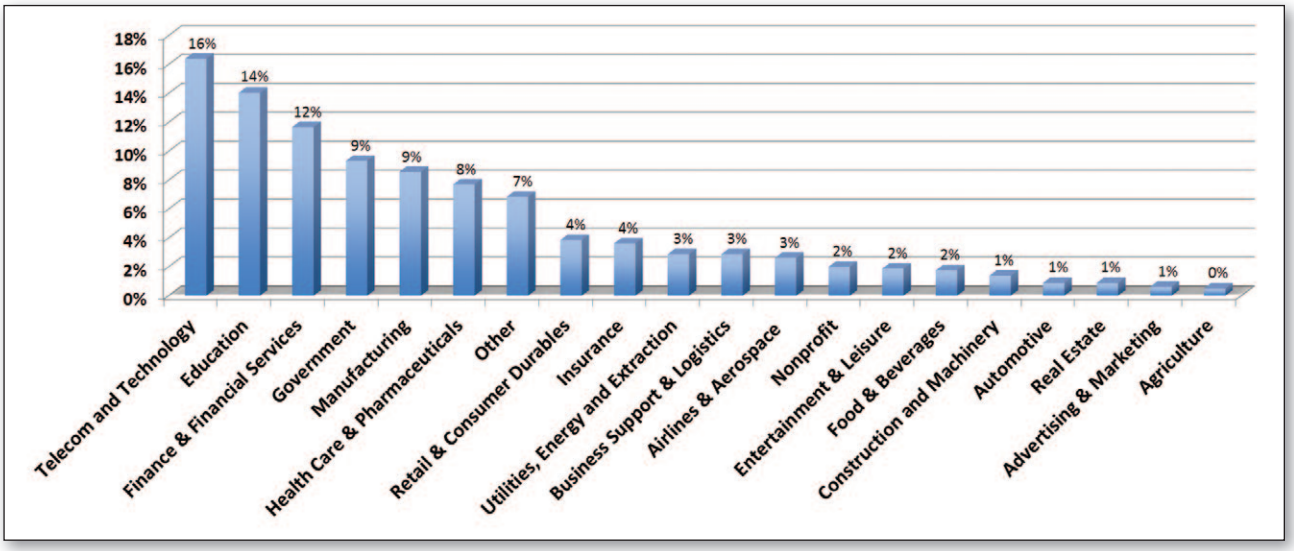

Figure 23: Survey participation by industry

Appendix 2: Research Methodology

CyberEdge Group developed a 27-question (10-15 minute) web-based survey instrument in partnership with its sponsoring vendors. The survey was promoted to information security professionals across North America and Europe in November 2013 through multiple IT security media outlets. Amazon.com gift certificate incentives were offered to the first 100 North American and the first 100 European participants to complete the survey in full.

Non-qualified survey responses were deleted from non-IT security professionals and from participants employed by an organization with less than 500 global employees. Most survey questions (aside from demographic questions) included a "Don't know" choice to minimize the potential for respondents answering questions outside of their respective domains of expertise.

All qualified survey responses were inspected for potential survey "cheaters," meaning those survey takers that 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 survey incentive. Suspected cheater survey responses were deleted from the pool of responses.

The sample size ("n") for each set of survey question responses varied for multiple reasons. In all instances, "Don't know" responses were excluded from analysis. In some instances, survey takers completed a portion of the survey but then dropped off prior to completion.

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 with dozens of IT security technologies, including:

- ☑ Advanced Threat Detection
- ☑ Big Data Security Analytics
- ☑ Endpoint Security Software
- ☑ File Integrity Monitoring (FIM)
- ☑ Intrusion Prevention System (IPS)
- ☑ Mobile Device Management (MDM)
- ☑ Network Behavior Analysis (NBA)
- ☑ Next-Generation Firewall (NGFW)
- ☑ Patch Management
- ☑ Penetration Testing
- ☑ Privileged Identity Management (PIM)
- ☑ Secure Email Gateway (SEG)
- ☑ Secure Web Gateway (SWG)
- ☑ Security Configuration Management (SCM)
- ☑ Security Information & Event Management (SIEM)
- ☑ Virtualization & Cloud 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.

CYBEREDGE GROUP

www.cyber-edge.com

info@cyber-edge.com

800.327.8711

@CyberEdgeGroup