A Forrester Consulting
Thought Leadership Paper
Commissioned By Fortinet

July 2017

Center Security On Advanced Technology

How A Technology-Led Strategy Helps CISOs Successfully Secure Their Organizations

FORRESTER®

Table Of Contents

Project Director:
Rudy Hernandez,
Market Impact Consultant

Contributing Research:
Forrester's Security & Risk research group

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

FORRESTER®

Security is a technology-centered discipline.

Executive Summary

An ever-expanding and -evolving cyberthreat landscape continues to challenge chief information security officers (CISOs) and other security leaders across the globe. New technologies and more open networks, a multitude of new identities, and savvier malicious actors challenge security leaders to keep pace and devote their energies to the areas that are most effective in securing their organizations. But what those areas are — those most effective in preventing security breaches and ensuring smooth business operations — can be difficult to discern.

In April 2017, Fortinet commissioned Forrester Consulting to profile how CISOs and other security leaders secure their organizations. Forrester conducted an online survey with 342 security leaders in the US, Europe, and Asia Pacific (AP) to explore the priorities and challenges they face and what successful leaders do — those who have avoided security breaches — that others do not. This study found that although people, processes, and trusted third parties are vital components in securing an organization, it is the security leaders who embraced technology that were more successful in avoiding cyberthreats and breaches.

KEY FINDINGS

- **Security is a technology-centered discipline.** Good processes and skilled staff are important, but technology is the tool that lets them work. Seventy-one percent of respondents who have never experienced a breach cite better security technologies as the key to their success.
- **A layered defense, especially with advanced technologies, is the best defense.** Defense in depth is a tried and true security concept. Organizations deploying 10 or more security technologies, including ones like threat intelligence platforms, endpoint detection and response, security information and event management (SIEM), and sandbox, experienced fewer breaches.
- **Constantly evolving cyberthreats are the greatest challenge that security leaders face.** Rapidly evolving cyberthreats present the No. 1 challenge to organizations (cited by 53% of respondents). Reducing the time to detect and respond is critical to reducing breach impact.

CISOs Trust Technology Solutions To Successfully Secure Their Organizations

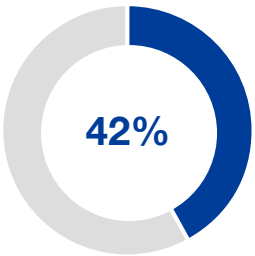
CISOs and other top security leaders face an increasingly complicated threat landscape. Cyberthreats abound like never before — hackers accessed more than 1 billion customer records in 2016, and 42% of security leaders in our study report that their organizations experienced a security breach within the last two years (see Figure 1) — yet the speed of business today demands that necessary security measures not bog down an organization's ability to act nimbly and quickly.[1]

It is in this environment that security leaders must prioritize different initiatives that can sometimes come into conflict with one another. This study of 342 final decision makers over risk and security in their organizations in the US, Europe, and AP revealed that:

- **Those who have never experienced a security breach are more likely to have adopted more and generally newer security technologies.** In this study, security leaders were asked to indicate how well they collaborated across departments within their organizations, how many of their security processes were being automated, and how many types of security technologies were currently implemented. When comparing the results between those reporting that they have never experienced a security breach and those who have reported a breach, the only significant difference was the number of security technologies used (see Figure 2).
- **Security leaders look to technology to help them succeed.** Security leaders in this study are more likely to trust security technologies as the chief driver of their success over better security processes, automation, third-party vendors, and many other staffing/organizational factors. This trend is even more pronounced among those who have been able to avoid security breaches: They are more likely to entrust technology as a factor in their success than decision makers who have reported a security breach by 17 percentage points (see Figure 3).

Figure 1

"To the best of your knowledge, has your organization ever experienced a cybersecurity breach?" (Showing percentage of those experiencing a breach within the last two years)



Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

Figure 2

	Never experienced a security breach (N = 101)	Have experienced a security breach (N = 239)
% strongly collaborating in at least three different areas	22%	19%
% automating more than 50% of their security processes	26%	28%
Average number of security technologies adopted	10.2	8.3

Indicates a difference that is statistically significant at the 95% confidence level

Base: Risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

FORRESTER®

Figure 3

"Which of the following would best contribute to achieving success in your role in securing your organization?"
(Showing those ranking as either first, second, or third priority)

Base: Risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

Security Threats Are Constantly Evolving — Businesses Must Keep Up

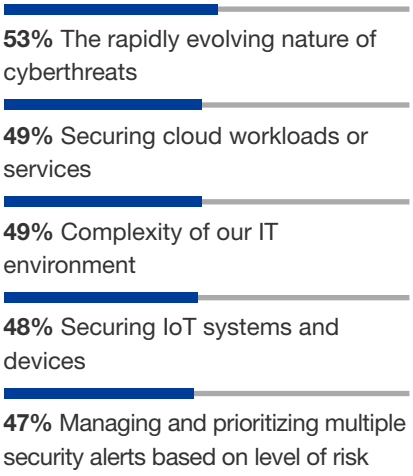
Cutting-edge security technology is highly valued by CISOs because of an increasingly complicated and threatening cybersecurity landscape. Indeed, failing to keep pace with the evolution of security technology is not just complacency — it can jeopardize an organization's existence.

Security leaders face these challenges every day and are realigning their priorities accordingly. This study reveals that:

- **The constant evolution of cyberthreats is the greatest challenge that security leaders face.** Fifty-three percent of survey respondents say that the rapidly evolving threat of cyberthreats presents the greatest challenge to their organizations (see Figure 4). This clearly shows that security leaders must aggressively keep pace and never let their guard down, especially with challenges of complexity — cloud, internet of things (IoT), and alert overload — that followed close on the heels of cyber threats.
- **In response, security leaders seek to improve their ability to react to cyberthreats.** To counter these rapidly evolving threats, security leaders are currently improving (and will continue to improve) operational efficiency (56%) and reducing time to detect (54%) and time to respond (49%), in addition to preventing breaches from happening in the first place (52%). Part of this preparation requires hiring and training qualified staff to attend to these threats — a priority that will increase by 30% in the next three years (see Figure 5).

Figure 4

"Which of the following are the most challenging factors in securing your organization?" (Showing those ranking as first, second, third, fourth, or fifth greatest challenge)



Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

Figure 5

"What are your organization's current cybersecurity priorities? How do you think these priorities will change over the next three years?" (Showing those ranking as either first, second, third, fourth, or fifth priority)

Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

FORRESTER®

Businesses Must Build Sustainable Security Programs Led By Technology

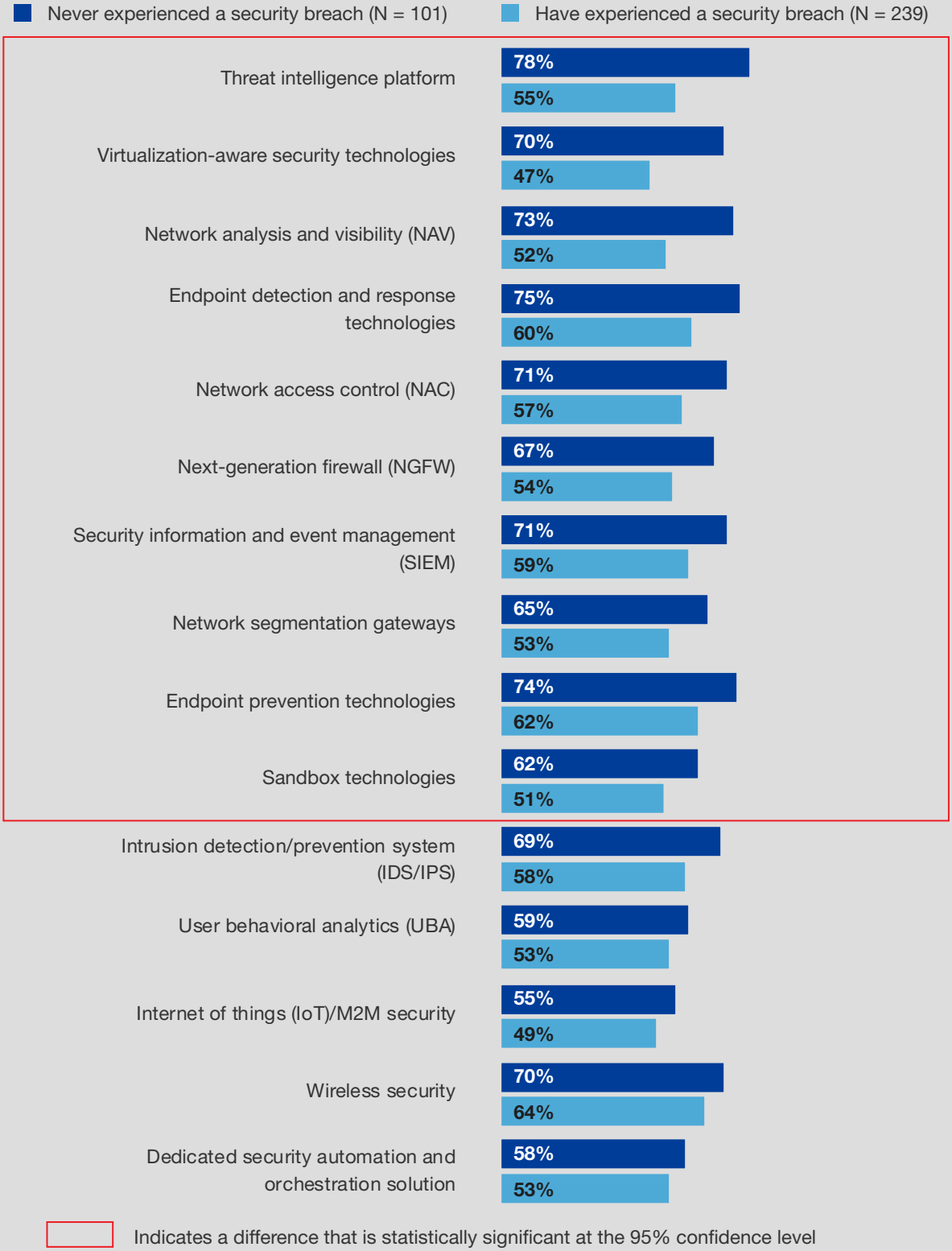
Preparation for the evolving cyberthreats of today and tomorrow requires that CISOs and other security leaders align people, processes, and technologies in order to function with the agility and efficiency needed both to counter these threats and to allow the business as a whole to stay competitive. Leaders must be aware, however, that technology is the demonstrably central component to this equation — a technology-led security practice can prevent breaches and quickly respond to ones that do occur.

Results from this study confirm that organizations that have avoided security breaches are more likely to (see Figure 6):

- **Adopt multiple types of security technologies.** From next-generation firewalls and SIEM to sandbox technologies, organizations that have never reported a security breach are more likely to adopt multiple security technologies by between 11 to 23 percentage points.
- **Gather intelligence.** Good threat intelligence provides insight into attacker methods and indicators of compromise (IOCs); 78% of those organizations that haven't experienced a breach adopt threat intelligence platforms.
- **Choose network analysis and visibility (73%), network access control (71%), and network segmentation gateways (65%) to monitor and control network activity.** Security leaders must control network and data access to avoid breaches. Network analysis and visibility (NAV) solutions monitor network activity while network access control (NAC) and network segmentation gateways control access. These security leaders segment their networks with network segmentation gateways, only allowing authorized access to sensitive data, and they employ NAC to control which devices are allowed to connect to their networks.
- **Leverage support from a wide range of sources in order to acquire security technologies.** All these technologies carry a cost to acquire, maintain, and manage. While building a business case is certainly important, security leaders indicated that obtaining technical validation — from third parties, industry analysts, and other departments — that the products work as expected were the most common approaches. How much senior decision makers value the opinion of one source versus another varies per organization, so it is important to leverage as many as possible.

Figure 6

"What are your organization's plans to adopt the following network security/security operations technologies?"
(Showing those selecting "currently adopted" or "expanding current adoption")



Base: Risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

FORRESTER®

ALIGN PEOPLE AND PROCESSES TO SUPPORT YOUR TECHNOLOGY-LED SECURITY PRACTICE

Focusing on technology does not mean neglecting other elements of your security practice; they all must work together to effectively secure your organization. Security leaders must take stock of where they stand in these areas and seek to make improvements as necessary. They specifically should:

- **Become more embedded with line-of-business (LoB) teams.** Security leaders generally feel that their relationships with LoB departments are satisfactory, but only a minority have built strong ties. Only 21% to 28% strongly agree they are effectively collaborating, interacting, or building influence with other parts of their organizations (see Figure 7). Strengthening these ties will create greater awareness of individual security needs and result in better security controls, threat discovery, and breach mitigation.
- **Drive greater automation.** Security leaders adopt numerous security processes, but only one-third to a half are automated (see Figure 8). Manual processes place a higher burden on security staff to recognize and respond to threats. Automation can foster more operational efficiency and enable security staff to put greater focus on security innovation and breach prevention.

Figure 7

"Would you agree or disagree that any of the following are true statements regarding how you and the cybersecurity department interact with the rest of the organization?"
(Select one response per row)

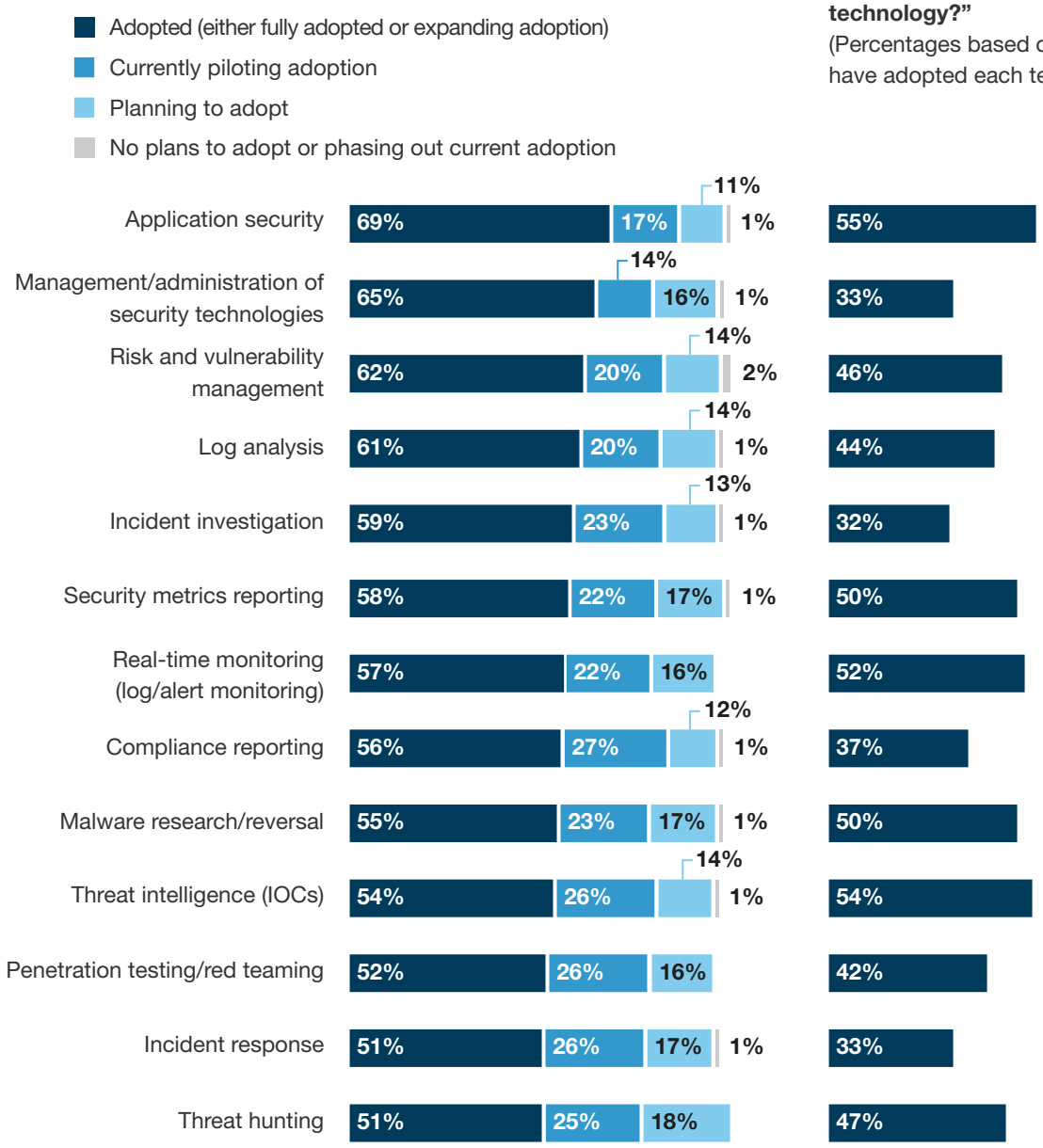
Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

FORRESTER®

Figure 8

"What are your organization's plans to adopt the following processes as part of your organization's security operations?" (Select one for each)

"Which of the processes that you use are automated through technology?" (Percentages based on those who have adopted each technology)

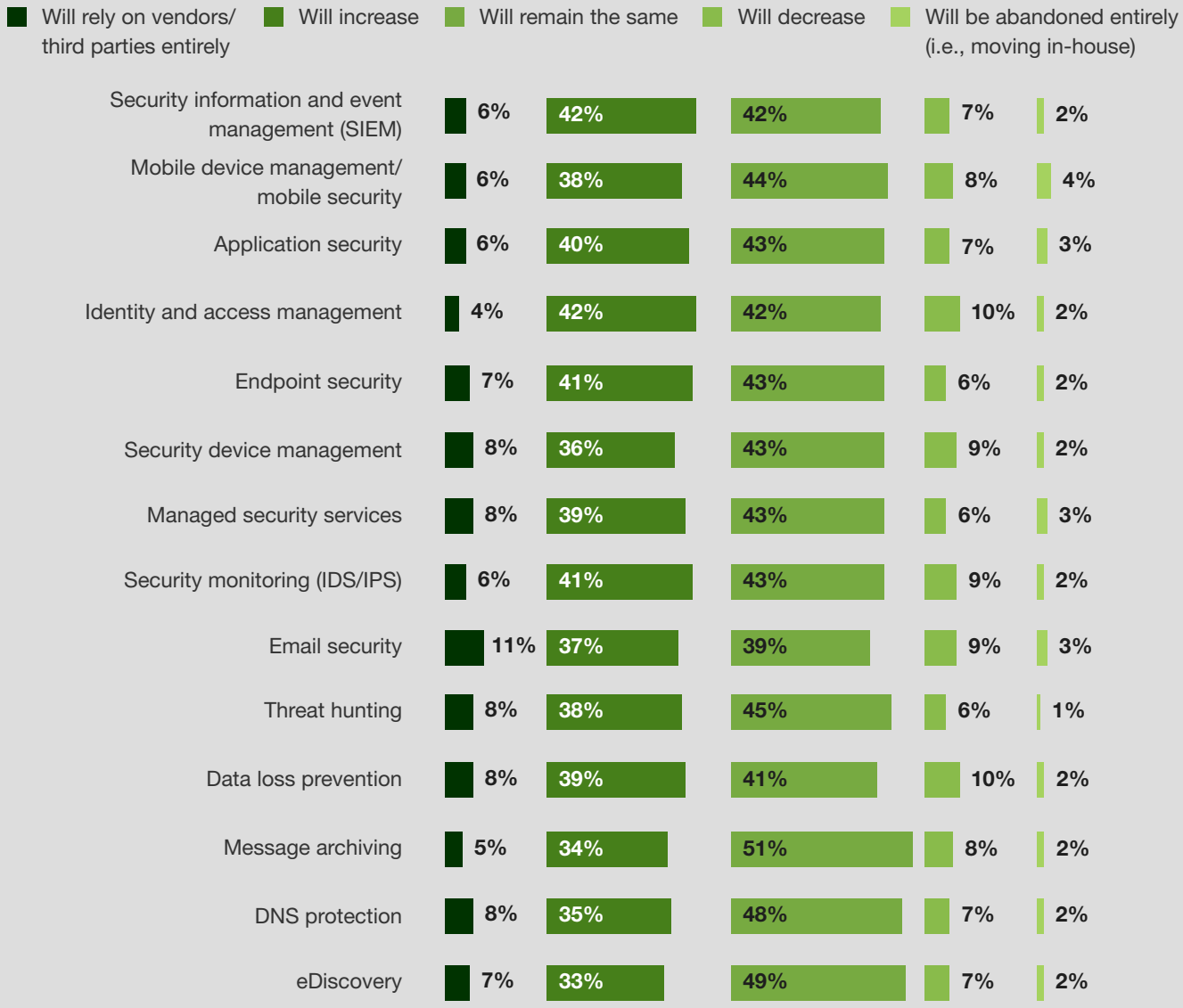


Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

› **Find the right security partners and solutions.** Many security leaders outsource various aspects of their organizations' security to vendors/third-party partners — a trend that will increase in the next 12 months (see Figure 9). Outsourcing provides various benefits, such as added expertise and experience and added technology to which organizations might not have access.

Figure 9

"Do you anticipate that outsourcing the following security services to vendors/third-party partners will increase/be adopted or decrease/be abandoned in the next 12 months?" (Select one for each)



Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

FORRESTER®

Key Recommendations

Transforming your security practice and becoming technology-led requires that you and other security leaders in your organization plot a concerted strategy to overcome organizational, budgetary, and cultural hurdles. Based on this research, Forrester recommends that organizations that wish to stay ahead of the evolution of cyberthreats:

Stay up to date. CISOs and other security leaders must investigate new innovations and technologies to remain ahead of evolving cyberthreats. You must regularly attend conferences, follow security thought leaders and consult with your peers, and work with vendors to understand and adopt new offerings.

Keep pace with the threat. Malicious actors continually innovate their methods and tools. You must match them by adopting an agile stance and ensuring your security controls don't fall behind.

Frequently assess and readjust their security strategy accordingly. Regularly assess your security program and technology stack to identify gaps. Build an iterative strategy to close those gaps and measure improvement.

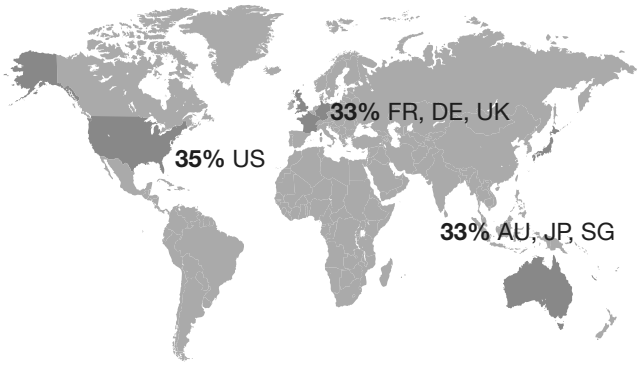
Get efficient. One reason security technology is a differentiator is because it can do the heavy lifting for your staff. Innovations in threat detection, workflow management, and automation can take some of the burden off your team and help compensate for the skills or staff shortages in key areas.

Learn the business. CISOs must accelerate their evolution to become business managers focused on protecting their brand, strengthening their reputation, and building customer trust.[2] This means building connections with leaders in your organization to learn what they are working on. Find ways in which security can fit with existing business processes to become an asset — not a hindrance — and reduce overall risk.

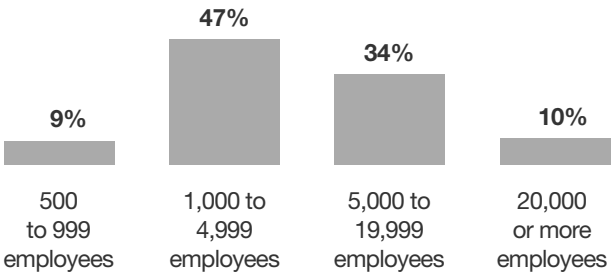
Appendix A: Methodology

In this study, Forrester conducted an online survey of 342 risk and security leaders in organizations with 1,000 or more employees in the US and in organizations with 500 or more employees in the UK, France, Germany, Australia, Japan, and Singapore. These individuals were directors or higher with final decision-making authority over information/cybersecurity and risk within their organizations. Questions provided to the respondents asked about their overall security priorities, challenges faced, technology used, and security breaches experienced. The study began in April 2017 and was completed in May 2017.

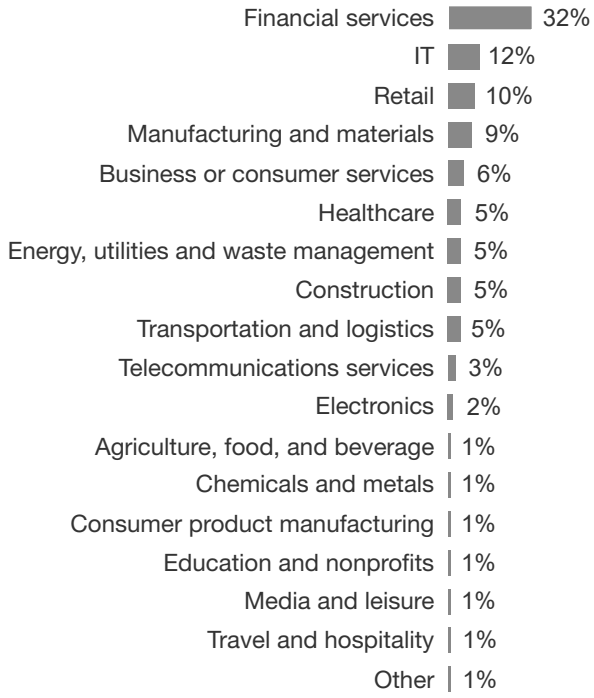
Appendix B: Demographics/Data



Company size



Industry



Base: 342 risk and security decision makers in enterprises in the US, UK, France, Germany, Australia, Japan, and Singapore
Note: Percentages may not total 100 due to rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, May 2017

Appendix C: Endnotes

[1] Source: "Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2016," Forrester Research, Inc., January 9, 2017.

[2] Source: "Build A High-Performance, Customer-Obsessed Security Organization," Forrester Research, Inc., February 9, 2016.

FORRESTER®