A Forrester Consulting
Thought Leadership Paper
Commissioned By IBM

May 2019

Complexity In Cybersecurity Report 2019

How Reducing Complexity Leads To Better Security Outcomes

FORRESTER®

Table Of Contents

Project Director:
Josh Blackborow and
Sophia Christakis,
Market Impact Consultants

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®

Disjointed security solutions that operate independently and generate a large volume of data have contributed to a complexity crisis.

Organizations that have taken steps to simplify their security ecosystems are reaping benefits, including greater resilience to security threats.

Executive Summary

A rapidly changing threat landscape has made organizational security more crucial and challenging than ever. Organizations have responded by investing in an enormous number of disconnected point solutions. However, a combination of disjointed products that all operate independently and generate a large amount of data has culminated in a crisis of complexity. As a result, security teams are unable to get the most out of their investments and must spend even more to properly secure their environments. The need to reduce complexity has never been clearer.

IBM commissioned Forrester Consulting to evaluate the state of security complexity and the effect it is having on security efficiency and effectiveness. To explore this topic, Forrester conducted a survey with 200 global security professionals with responsibility for security strategy and/or security technology purchases. We found that nearly all respondents report concerns over complexity. However, organizations that have taken steps to simplify their security ecosystems, including consolidating solutions onto a single management platform, have seen meaningful benefits.

KEY FINDINGS

- **Security environments are increasingly complex.** Security pros tend to operate in siloed teams, so it is rare — if not impossible — to get a full picture of data and processes across the entire security discipline, much less the entire company. Making matters worse, data volumes across locations, and particularly in the cloud, have skyrocketed in the past few years, and that trend is likely to continue.
- **Organizations are spending more but not necessarily wisely.** Increases in security budgets and organizational pressure to avoid a damaging data breach have led organizations to adopt a plethora of disconnected point solutions. Our study found that, on average, 52% of security products and 77% of vendors have been added within the last two years. This buying frenzy has added to organizations' security complexity, but it has not necessarily added to the overall maturity of their security programs.
- **Complexity erodes ROI.** Security complexity has become a problem that organizations can no longer ignore. Our study found that 91% of organizations are concerned with complexity, and those with very complex environments are more likely to cite cost challenges and inefficiencies with technology and staff.
- **Simplification can unlock security value.** Organizations that are effective at simplifying their environments make the most out of existing security investments. They are connecting data and processes and integrating solutions into consolidated management platforms. They're also reaping several benefits, including improved ability to detect, respond to, and recover from threats.

FORRESTER®

Reactive Tactics Have Spun A Tangled Web Of Security Solutions

Highly publicized data breaches have moved security into the minds of executive teams. This has made it easier for security leaders to make the case for budget and get executive buy-in to fund security projects. In fact, security spending as a percentage of IT budgets is on the rise.[1] At the same time, the industry has responded with a flood of intriguing solutions to protect against new threats.[2] The result? Reactive security spending and widespread inefficiency.

Our research of 200 security decision makers who are prioritizing optimization of security assets and resources over the next year reinforces these trends: "Improving return on security investments" is one of their top priorities, behind only "improving advanced threat capabilities." In addition, many are focused on increasing the productivity of their staff, simplifying their environments, and improving operational efficiency (see Figure 1). However, they face an uphill battle in these efforts as they now need to secure:

- **A soaring number of point solutions.** Security pros, particularly those at companies that have suffered a breach, have dipped into their growing budgets to pay for new security solutions. However, many are solving for short-term needs without giving enough thought to how each addition contributes to the long-term maturity of their security programs. As a result, teams are overladen with a multitude of disparate and disconnected point solutions. Our respondents' organizations are managing an average of 25 different security products/services from 13 vendors — and many have even more. In a sign of the buying frenzy of recent years, 52% of the security products added and 77% of the new vendors added were done so within just the last 24 months.
- **Skyrocketing data volumes.** Over the past two years, data — on-premises, in endpoints, in virtual servers, and especially in the cloud — has increased substantially. In every location we tested, respondents report at least a 55% increase in data stored, on average, and many have seen data double, triple, or more in the same time period (see Figure 2). Yet unlike the increase in security products, security teams have little to no control over data increases that will likely persist in the years to come.

Figure 1

Top Security Priorities Over The Next 12 Months

Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

On average, 77% of the security vendors at respondents' organizations were added in the last 24 months.

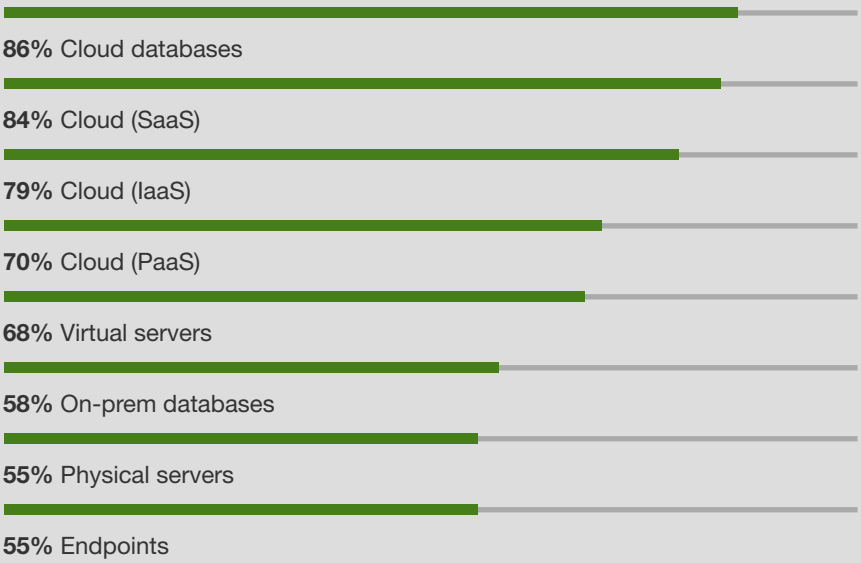
› **Data living across a heterogenous environment.** Increasingly, data is moving out of endpoints and on-premises servers and is proliferating across the enterprise. Given that many organizations have embraced cloud-first strategies, it's not surprising that much of organizations' data is moving to the cloud, and their security assets and processes have followed. In fact, respondents predict that by 2020, the percent of security assets and processes their organizations have in the cloud will increase by more than 200% over 2016 levels. Data dispersed across heterogenous architectures threatens security teams' visibility: They cannot protect valuable data assets they cannot see.

Despite the broad range of security defenses to which organizations have flocked, most security pros struggle to maximize the value of their investments and protect their organizations.[3] In fact, fewer than a quarter say they're completely satisfied with their security portfolios in supporting them to develop advanced threat intelligence capabilities; increase productivity of security staff; extract insight from data; and drive efficiencies. Moreover, just 50% or fewer respondents report they are using all or most of the available functionality in any of the 11 security technology categories in our study. Notably, fewer than 25% say their technologies are fully optimized in internet-of-things (IoT) security; identity and access management; security automation and orchestration; and security information and event management (SIEM).

Respondents predict that by 2020, the percent of security assets and processes their organizations have in the cloud will increase by more than 200% over 2016 levels.

Figure 2: Data Volumes Across Locations Have Soared In The Last Two Years

"How has the amount of data your organization is storing in each of the following locations changed over the past two years?" (Showing average percent increase)



Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

FORRESTER®

Complexity Threatens Cybersecurity Effectiveness

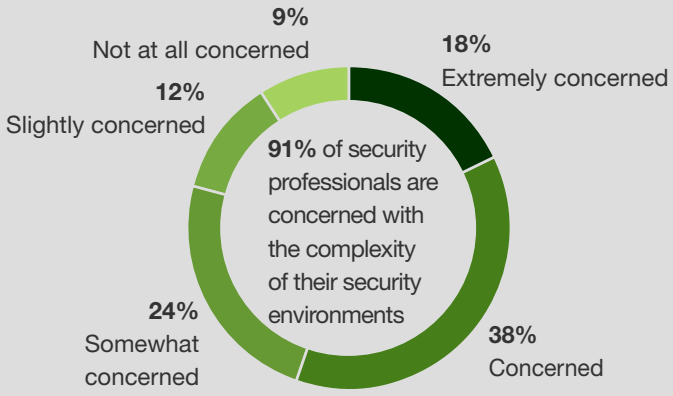
As today's security leaders struggle to manage the complexity of their security environments, they are learning the tough lesson that adding more point solutions doesn't simplify anything. The lengthy deployment cycles, difficult integrations, and user training involved with managing an influx of solutions present risks that make technology investments fail.[4] Respondents recognize that this poses a very real threat: 91% express some level of concern over their organzations' security complexity (see Figure 3). It ranks second highest among their top concerns, only slightly behind the changing and evovling nature of threats.

While nearly every respondent indicated some concern over complexity in their environment, the results from those who responded with the highest levels of concern made it clear just how complex organizations have become (see Figure 4). Predictably, the greater the concern over complexity, the more products and data organizations had. The respondents who indicated a higher concern for complexity also, on average, have 45% more security products and 36% more vendors than respondents who were less concerned. In addition, they are managing more data across locations. As a result, they're twice as likely as other organizations to describe integrating disparate security technologies and data sources as challenging and to struggle with gaining visibility into security-related data and insights (see Figure 5). And any insight they do glean is difficult to build on: Over half of them cite collaborating with peers inside and outside of the organization on security insights as a barrier, making it more difficult for them to develop their threat intelligence capabilities and to uncover patterns of vulnerability.

91% of security professionals express concern over their organzations' security complexity.

Figure 3: Concerns Over Complexity Are Top Of Mind For Security Professionals

"How concerned are you with each of the following when it comes to protecting your organization's security posture?"
(Showing responses for "Complexity of our security environment")



Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Note: Percentages do not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

Security complexity ranks among respondents' top concerns and rivals the level of concern they express over the changing nature of IT threats and regulatory compliance.

FORRESTER®

Figure 4: Defining Complexity Concern

"How concerned are you with security complexity when it comes to protecting your organization's security posture?"

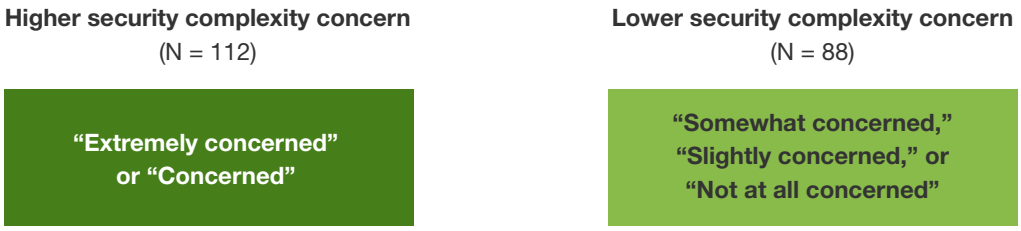
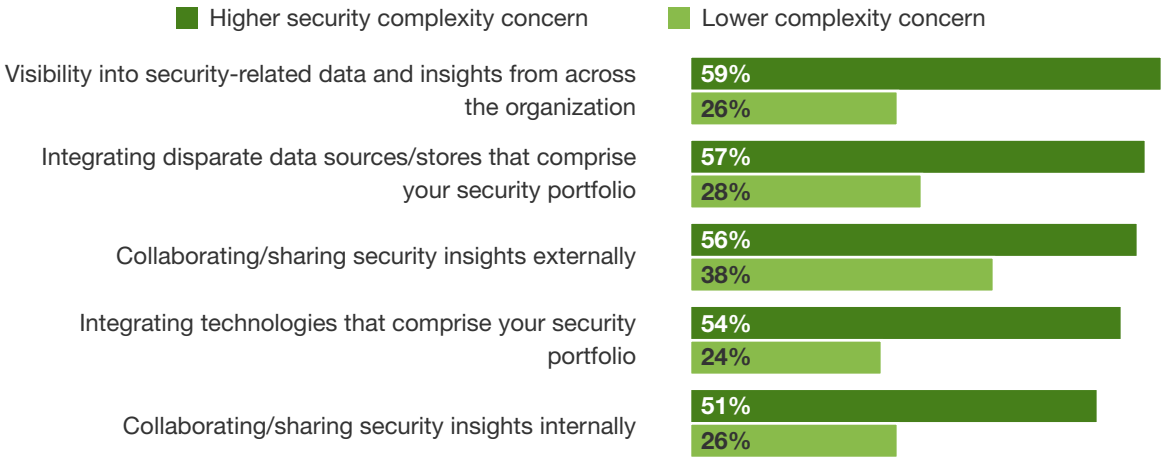


Figure 5: Higher Complexity Leads To Greater Challenges

"How challenging is each of the following for your security team?" (Showing "Challenging" or "Extremely challenging")



Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

Those with higher concern (whom we've shown to have greater complexity) are also at a distinct disadvantage because:

- **Complexity erodes ROI.** Security complexity exacerbates an already challenging issue: an inability to make the most of security resources. Those with greater complexity concern are more likely to say that the complexity of their security environment has led to high costs. They also are more likely to cite inefficiencies in the use of security technology and security staff time and to find it difficult to train staff on new security products (see Figure 6).
- **Complexity inhibits innovation.** Market uncertainty stemming from government agencies, competitors, and customers requires companies to constantly change. Only those that are fast, connected, and innovative will be able to thrive in a shifting landscape. Unfortunately, those with security complexity struggle to evolve with the agility required: 50% report that their complexity has made it difficult to replace outdated security technology and 37% say that it has caused them to defer purchases in fear of adding further complexity. Making matters worse, 29% feel locked in on specific vendors. While companies with highly complex security environments could benefit greatly from a more streamlined ecosystem, they face an uphill battle in their efforts to modernize relative to organizations with less complexity.

Organizations saddled with high complexity are more likely to cite cost struggles as well as technology and staff inefficiencies.

FORRESTER®

SECURITY SIMPLIFICATION UNLOCKS INVESTMENT VALUE

Despite the challenges that stand in their way, organizations with the greatest levels of complexity concern see simplification as a worthwhile effort. They associate several benefits with a more simplified environment — from an improvement in their ability to extract insight from data, to threat intelligence, to internal collaboration and user experience. Notably, 72% believe simplification would have a "moderate" or "significant" improvement in operational efficiency, security staff productivity (68%), and security investment return (58%) — addressing their highest priorities.

Organizations believe a simplified environment would allow them to improve operational efficiency, security staff productivity, and security investment return.

Figure 6: Security Complexity Erodes ROI, Limits Flexibility, And Stifles Modernization Efforts

"What challenges have you encountered due to the complexity of your security environment?" (Select all that apply)

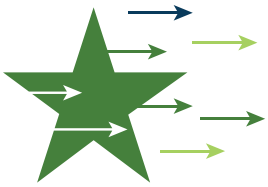
Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

Simplified Cybersecurity Portfolios Are The Way Forward

Recognizing the challenges that come with security complexity and the benefits of simplification, the question becomes: What can organizations do to reduce security complexity? While all respondents report taking at least some steps to reduce complexity, fewer than half (44%) describe their efforts as effective. For the purposes of this study, we refer to these organizations as "Champions," and all others (i.e., those who cite their efforts as "somewhat," "slightly," or "not at all" effective) as "Challengers" (see Figure 7).

Although Champions are more effective in their simplification efforts, their simplification journeys are not complete. In fact, many of them still cite concerns with complexity. They have, however, started to make significant inroads in streamlining their security and have lessons to teach organizations that are still struggling. In particular, Champions:

› **Prioritize simplification.** While it may seem obvious, one of the most distinct differences between Champions and Challengers is the level of priority they're placing on simplification. Not only are Champions significantly more likely to make simplification a priority, they're also more likely to dedicate specific resources to the effort (see Figure 8). Seventy-five percent of Champions have dedicated resources relative to just 56% of Challengers. Additionally, 63% or more of Champions have employed each of the simplification tactics we tested.



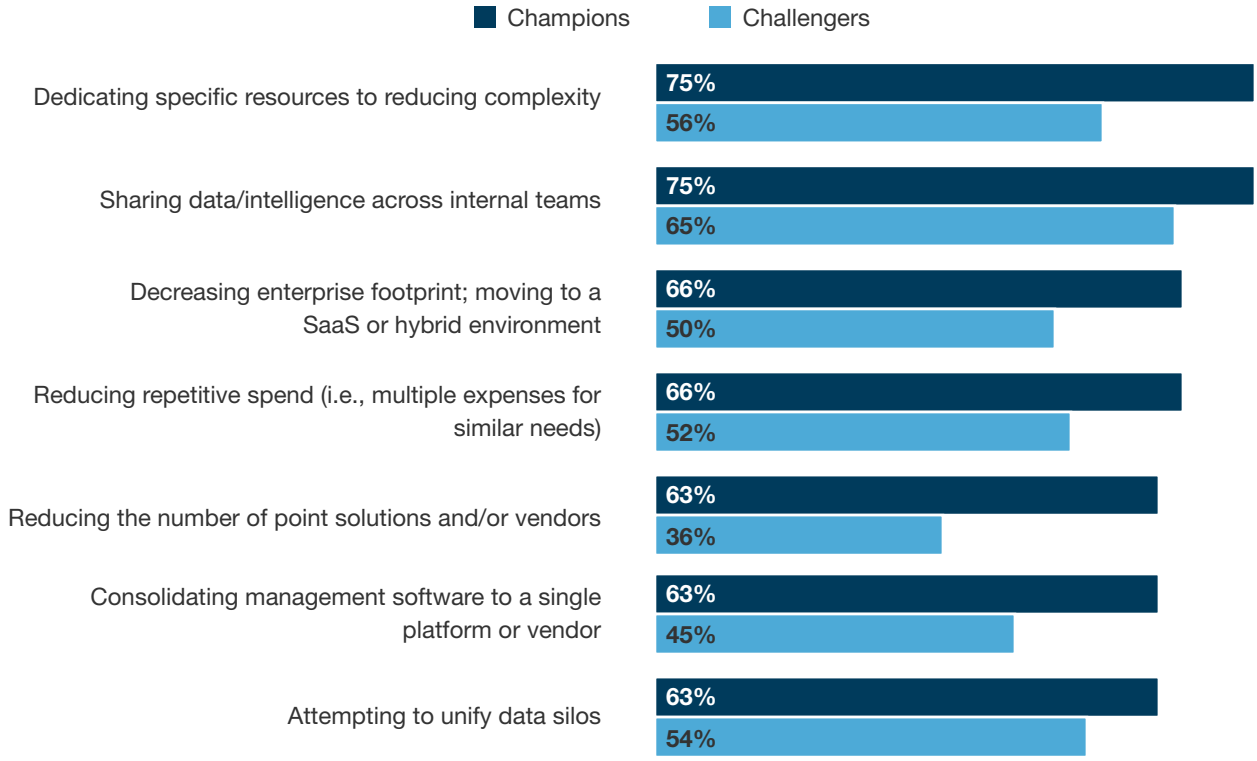
"Champions" are those that have made greater progress toward reducing security complexity.

Figure 7: Defining "Champions" And "Challengers"

"How effective have your efforts to reduce security complexity been thus far?"

Figure 8: Champions Have Made More Progress On Simplification Initiatives

"Which of the following are actions your organization has taken, or plans to take, to simplify your security environment?"



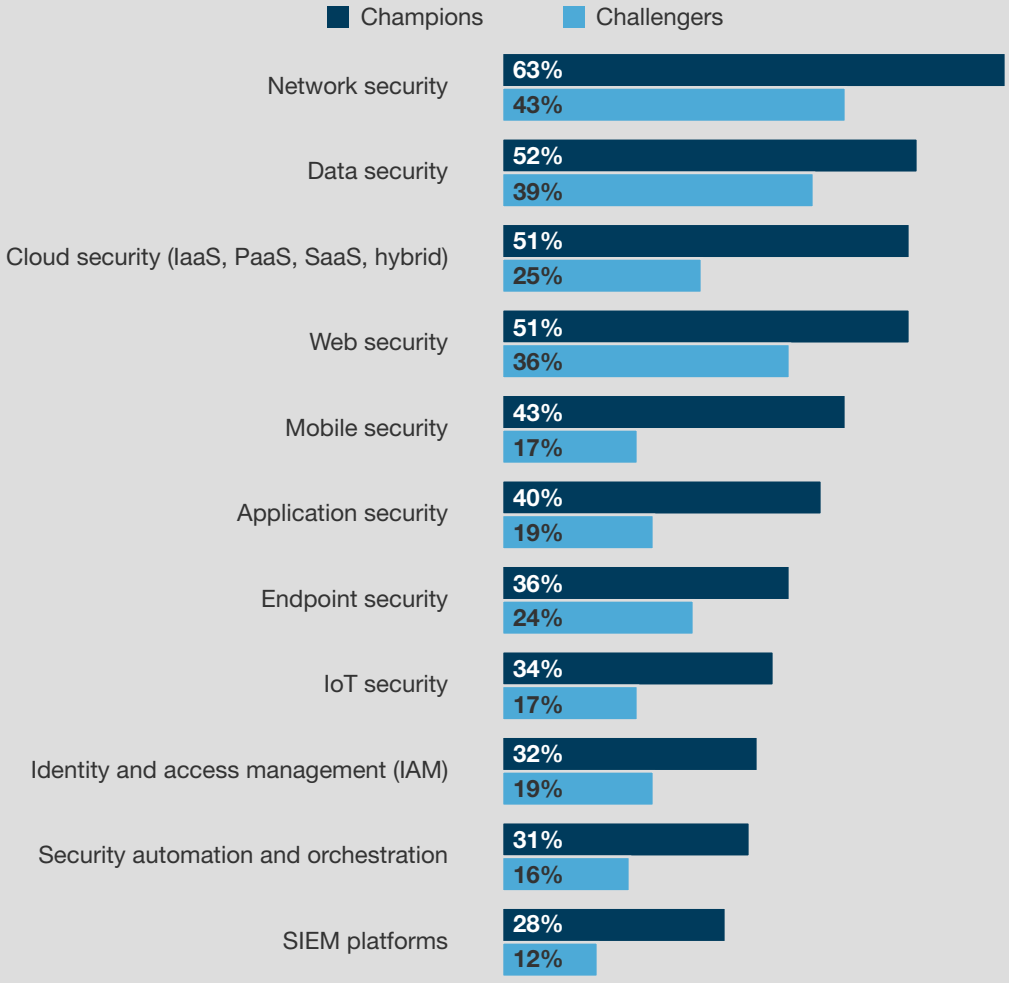
Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

› **Maximize existing investments.** Chasing shiny new point solutions instead of optimizing technology that already exists can lead to multiple disconnected tools for similar needs. A more efficient approach is to look for opportunities to reinvent and reinvest in a smaller set of existing tools, maximizing their utility.[5] Champions are doing just that: 63% have worked to reduce the number of point solutions or vendors in their security portfolios, relative to just 36% of Challengers. In addition, Champions are more likely to have reined in repetitive spending (66% versus 52%). Finally, Champions squeeze more value out of existing security tools — they enjoy a much higher utilization rate across a range of security investments (see Figure 9).

Champions are more likely to be consolidating their management software to a single platform or vendor.

Figure 9: Champions Extract More Value Out Of Existing Security Investments

"To what extent is your organization fully utilizing your security technologies in the following areas?"
(Showing "Fully optimized — we utilize all or most of the available functionality of these solutions")



Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

FORRESTER®

› **Consolidate management to a single platform.** Champions are more likely to be consolidating management software to a single platform or vendor (63% vs. 45%). By managing their security assets in a consolidated platform, they can transform disparate solutions into a cohesive and connected security suite. Consolidated offerings give security teams more visibility and control into their environments; they also reduce the operational complexity and cost of managing individual point products and lay the foundation for automation and orchestration of security defenses.[6]

ADDRESSING COMPLEXITY MAKES ORGANIZATIONS MORE RESILIENT

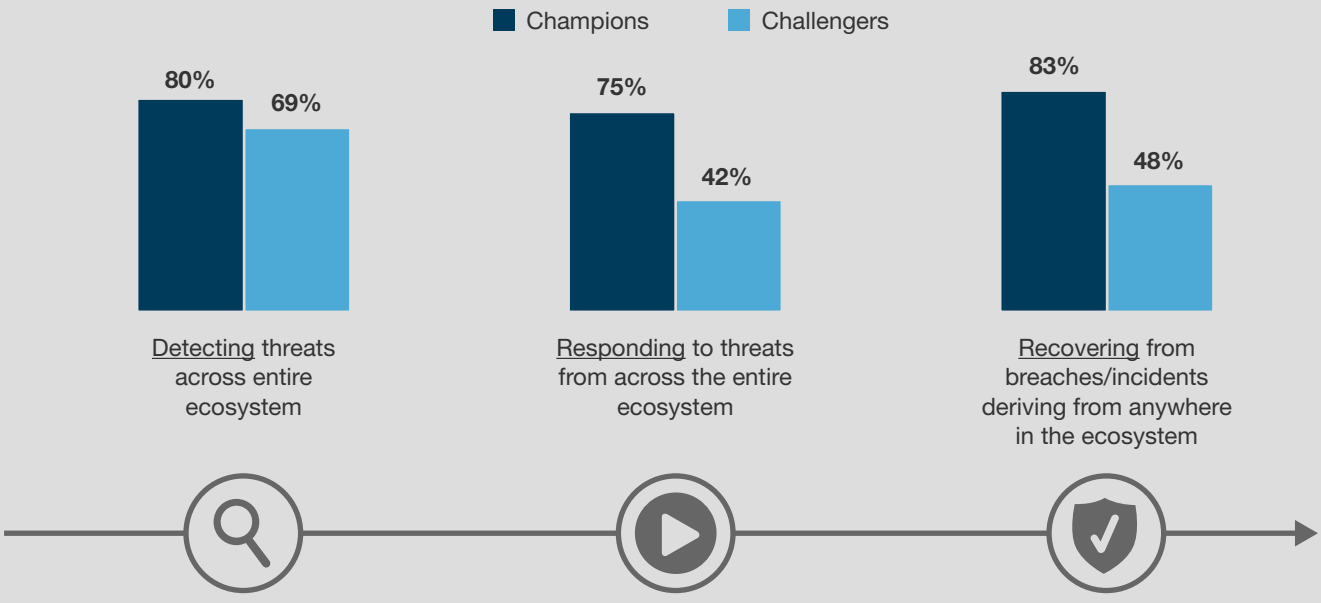
A particularly fascinating finding of this research was that Champions are not only benefiting from efficiency gains, they're also more successful at protecting their companies from cybersecurity threats.

Champions are more likely than their less effective peers to say they're satisfied with their security portfolio's ability to detect threats across their ecosystem — and they're significantly more likely to be satisfied in its ability to *respond* to threats and *recover* from security incidents, with margins ranging from 33 to 35 points. Even though Champions still have more work to do to overcome complexity, their approach to the issue — prioritizing the effort, maximizing existing investments, and consolidating management to a single platform — makes them far more prepared to protect their organizations from security disruptions (see Figure 10).

Champions are more effective at detecting and responding to threats and recovering from security incidents.

Figure 10: Champions Are More Resilient To Threats

"How satisfied are you with how well your security portfolio supports you in each of following?"
(Showing "Completely Satisfied" or "Satisfied")



Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

FORRESTER®

SECURITY VENDORS PLAY AN IMPORTANT ROLE IN SIMPLIFICATION

For their part, many organizations have made some progress in their efforts to simplify their security ecosystems. However, the benefits they've seen will be short-lived if security vendors don't make changes that support these efforts. Organizations must look past vendors that perpetuate the cycle of inefficiency. In fact, 98% of surveyed decision makers want help from their security vendors to reduce complexity. They want vendors to offer solutions that (see Figure 11):

- **Are easy to use, integrate, and buy.** Forrester's research has found that security leaders face major challenges with staff and skill deficits.[7] Our research reinforces this trend: 44% percent of security leaders in our study cite a lack of staff as a concern in protecting their companies. Too many technologies that are poorly integrated only worsen the human capital problem. It also makes it more difficult for organizations to address the issue: 40% say skill shortages are a barrier in their efforts to simplify their environments. Many security vendors are developing new platforms that consider ease of use and simplified controls.[8] Security professionals in our research express an appetite for these types of tools, as well as ones that are easy to integrate and buy.
- **Can optimize and connect to solutions already in place.** Security decision makers want their vendors to understand their existing security landscapes. They want vendors to extend the value of existing security investments and integrate only those capabilities that contribute to long-term maturity of their cybersecurity programs. This includes being able to seamlessly integrate with products from other vendors, not only ones within that vendor's portfolio.
- **Activate and connect data regardless of where it's stored.** With data growing and spreading to every corner of the enterprise, organizations cannot reasonably consolidate all data in a centralized location for insight and analysis — at least not without incurring significant costs. Security teams see value in vendors that can help them activate and connect data no matter where it's stored, reducing their need for pricey, time-consuming, and complex data migration projects.

Figure 11: Security Professionals Want Vendors To Support Their Security Simplification Efforts

"What do you want from your vendors to help you reduce security complexity?" (Select all that apply)

Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

Key Recommendations

Complexity is becoming an increasingly urgent issue in today's security landscape and will continue to grow if not addressed. Security teams that wish to avoid this pitfall should make reducing security complexity a priority and focus within their organizations. Take these three key actions to do so:

Consolidate capabilities to focus on business objectives. Limiting the number of individual solutions reduces the amount of management and maintenance required to keep the security ecosystem running smoothly. Finding ways to reinvest and reinvent current solutions helps organizations keep staff increases in check and helps increase ROI.

Decrease data silos to limit friction for security teams. Firms that fail to integrate security, information technology, and application data together will not possess the necessary information to make quick, accurate decisions about the potential ramifications of security events. The more concerned firms were with complexity, the more isolated data came up as a symptom. Tools and technology that allow security teams to receive and analyze disparate data sources will help security teams act decisively.

Simplify your ecosystem to enhance response and recovery. While detecting threats is reasonably improved by a simplified security portfolio, massive gains were identified in responding to, and recovering from, incidents, no matter where those events came from in the customer's ecosystem. If the adage holds true that "it's if, not when" for security leaders, then response and recovery must take center stage as areas of emphasis. Simplifying security is one clear way to make that happen.

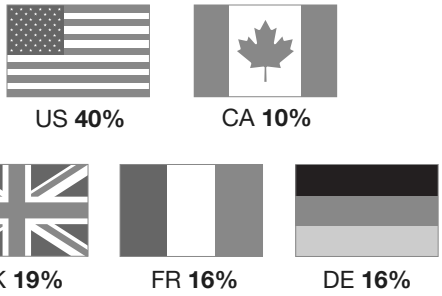
FORRESTER®

Appendix A: Methodology

In this study, Forrester conducted an online survey of 200 security professionals with decision-making responsibility for, or influence over, their organizations' security strategy and/or technology purchases. Respondents came from organizations with at least 500 employees in the US, Canada, the UK, France, and Germany. The study evaluated the state of organizations' security technology portfolios and the extent to which complexity has impacted their effectiveness. Questions provided to the participants asked about the primary objectives driving their security strategies, challenges that inhibit their success, tactics they've employed to simplify security, and the value they expect from optimizing security assets and resources. Respondents were offered a small incentive as a thank you for time spent on the survey. The survey fielding began in December 2018 and was completed in January 2019.

Appendix B: Demographics

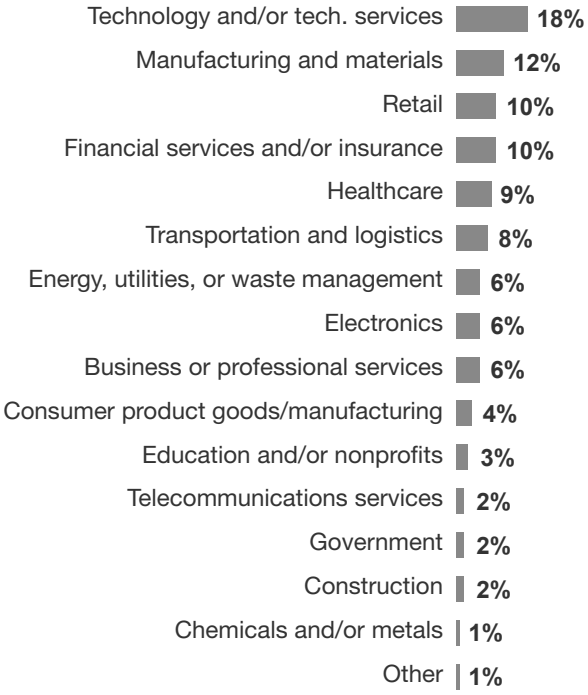
COUNTRY



US **40%** CA **10%**

UK **19%** FR **16%** DE **16%**

INDUSTRY



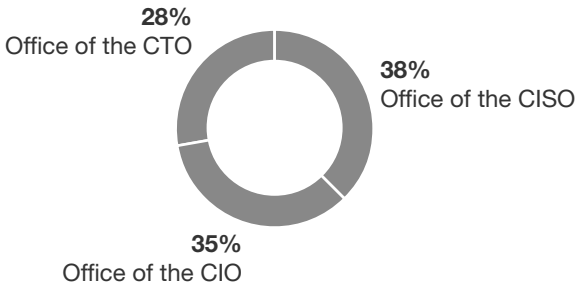
SENIORITY

30% C-level
11% VP
60% Director

NO. OF EMPLOYEES

40% 500 to 999
36% 1,000 to 4,999
16% 5,000 to 19,999
10% 20,000 or more

DEPARTMENT



Base: 200 global security professionals with responsibility for security strategy and/or security technology purchases
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of IBM, January 2019

FORRESTER®

Appendix C: Endnotes

[1] Source: “Security Budgets 2017: Increases Help But Remain Reactionary,” Forrester Research, Inc., November 23, 2016.

[2] Source: “The Top Security Technology Trends To Watch, 2017,” Forrester Research, Inc., April 26, 2017.

[3] Source: “The Top Security Technology Trends To Watch, 2017,” Forrester Research, Inc., April 26, 2017.

[4] Source: “Security Budgets 2019: The Year Of Services Arrives,” Forrester Research, Inc., December 17, 2018.

[5] Source: “Security Budgets 2019: The Year Of Services Arrives,” Forrester Research, Inc., December 17, 2018.

[6] Source: “The Zero Trust eXtended (ZTX) Ecosystem,” Forrester Research, Inc., January 19, 2018.

[7] Source: “The Zero Trust eXtended (ZTX) Ecosystem,” Forrester Research, Inc., January 19, 2018.

[8] Source: “The Zero Trust eXtended (ZTX) Ecosystem,” Forrester Research, Inc., January 19, 2018.