REPORT

# The Security Architect and Cybersecurity

## A Report on Current Priorities and Challenges

# Table of Contents

# Executive Summary

**The “Security Architect and Cybersecurity Report” looks closely at how security architects are approaching cybersecurity as well as the changing role of the security architect. Based on survey findings, the following are some of the key takeaways:**

1. The security architect has an increasingly high-profile role with responsibilities spanning a wide range of infrastructure capabilities. Nearly **two-thirds** report directly to a C-level executive.
2. The role of the security architect is **primarily strategic** and not tactical. Their top success metrics focus on issues such as integration, automation, and DevOps security. Tactical metrics such as vulnerabilities found, intrusions stopped, and breach mitigation are less important in the grading of the security architect’s performance.
3. Security architects have confidence in their organization’s protection level and ability to manage risk, but they still struggle with **unknown** and **zero-day** threats. All believe that they can defend against known threats, but **more than half** acknowledge challenges in protecting against unknown and zero-day exploits.
4. Security architects track a wide range of metrics, but **fewer than half** track risk outcomes or vulnerabilities.

Given these trends and challenges, we analyzed the data more deeply and identified a subset of respondents who reported no intrusions in the past year that we deem top-tier security organizations. At the same time, we pinpointed another subset that had more than six intrusions in the same time frame and deemed them bottom-tier security organizations.

The differences in practice between these two groups are instructive—specifically, the traits of top-tier organizations/security architects. In a nutshell, these best practices reflect a holistic, integrated approach to cybersecurity that eliminates silos, enables automation of security response, and provides the best protection against advanced threats.

## Infographic: Key Findings

**66%**

of security architects report to a C-level executive—typically the **CISO.**

**82%**

are directly responsible for **cloud security.**

More security architects list **DevOps security** as the #1 performance measure than any other security area.

**92% had at least one intrusion in the past 12 months.**

**54%**

have had **3+** intrusions.

**13%**

have had **6+** intrusions.

**54% have challenges defending against unknown threats.**

**68%**

lack an end-to-end **integrated security system.**

**45%**

cite **integration difficulty** as one of their top three security concerns.

**66%**

use **MSSPs** to supplement their security staff.

## Best-in-class security architects are:

**3x** as likely to **track and report** cost reduction from cybersecurity

**2x** as likely to **deploy integrated solutions** for some or all of their security infrastructure

**3x** as likely to **cite undetected intrusions** as one of the organization's top three cybersecurity issues

**33%** more likely to **report directly to the CISO**

# Introduction

According to the World Economic Forum, business leaders believe that cyberattacks are the single greatest existential threat to their organizations, ahead of terrorist attacks, financial crisis, and climate change.[1] For organizations, cybersecurity responsibility is invested in a dedicated C-level executive—the chief information security officer (CISO).[2]

While the CISO owns the cybersecurity strategy, much of the work needed to implement that strategy falls to the security architect who is charged with planning, analyzing, designing, configuring, testing, implementing, maintaining, and supporting the organization's security infrastructure. Today, security architects are under increasing pressure to simplify the management of security systems and processes while maximizing the value of investments in security products and services.

Adding to the challenge is the widespread adoption of advanced technologies such as multiple cloud architectures, the Internet of Things (IoT), and artificial intelligence (AI), each which brings specific—often unfamiliar—vulnerabilities.

In addition to these internal pressures, the challenges of the threat landscape continue to evolve and create greater pressures on the security architect. These challenges include:

1. **Expanded attack surface.** In the past, the central challenge for the security architect was to defend the perimeter of the data center. Today, the enterprise perimeter has largely disappeared, thanks to developments such as software-defined wide-area network (SD-WAN), multi-cloud deployments, architectures, IoT, mobile, and more. The erasure of the network perimeter makes it more difficult to maintain transparent visibility and unified policy controls across the entirety of the expanded attack surface. This, in turn, increases inefficiencies and cost while diminishing an organization's risk posture.
2. **Increasing security complexity.** To address these threat dynamics of the expanded attack surface, many organizations turn to point security products, but this increases complexity. The resulting siloed security architecture escalates manual workflows that further stretch already overburdened security teams. This, in turn, degrades an organization's overall security posture. Evolving compliance requirements also contribute to increased security complexity. Network and security teams are charged with managing audit trails and generating customized compliance reports for varying recipients—regulatory bodies, boards of directors, CEOs, CFOs, among others.
3. **An advanced threat landscape.** The threat landscape continues to become more sophisticated, and threats are harder to detect and prevent than ever. Part of the challenge is the sheer volume and velocity of attacks. But that is not the only factor. Unknown and zero-day attacks are a serious problem—both in terms of completely new virgin threats and the permutation of existing threats into new attack vectors. Unknown and zero-day attacks now comprise as much as 40% of all threat traffic, and the execution of attacks—from exfiltration of data, to encryption of data (viz., ransomware), to manipulation and disruption of operations—happens in minutes versus days or weeks.[3]

# Methodology for This Study

This report is based on a survey of security architects at organizations with more than 2,500 employees. Respondents come from a variety of industries, including technology, financial services, retail, and manufacturing.

The report has three primary sections. The **first** one identifies **current trends** that characterize the position, job duties, and attitudes of security architects. The **second** one analyzes the **key challenges** security architects indicate are facing them. The **final** one compares **top-tier security architects** (i.e., those with no reported intrusions in the past year) versus **bottom-tier security architects** (i.e., those with the most reported intrusions in the past year) and identifies the most notable traits of top-tier security architects.

# Cybersecurity Trends Per the Security Architect

### Trend: The security architect has a high-profile role—and an expanding set of responsibilities.

Security architects tend to reside high in the corporate hierarchy. Two-thirds of security architects report to C-level executives—either the CISO (58%) or the CTO (8%). The remainder report to functional roles—the network engineering and operations leader (19%), enterprise IT architect (9%), or the security operations center (SOC) director/manager (6%) (Figure 1).

In terms of departmental residency, nearly two-thirds (65%) of security architects work within the cybersecurity department. A little more than one-quarter (27%) reside in the IT organization, and another 8% are found in the organizations of the CTO (Figure 2).[4]

More than 8 in 10 security architects cite cloud security as one of their top responsibilities. The next five responsibilities appear at least 70% of the time—mail security (79%), identification of security gaps (76%), integration of security elements (74%), adherence to security standards (70%), and DevOps security (70%) (Figure 3). None of these should be a huge surprise. For example, while DevOps staff does not directly report to the CISO in most organizations, its line of reporting is going to change within the coming year; 70% of organizations indicate they plan to move the primary responsibility for DevOps security to the CISO this year.[5] Likewise, mail security remains a top attack vector, with 94% of malware arriving via mail,[6] and thus it makes sense that it shows up as a top priority for security architects.

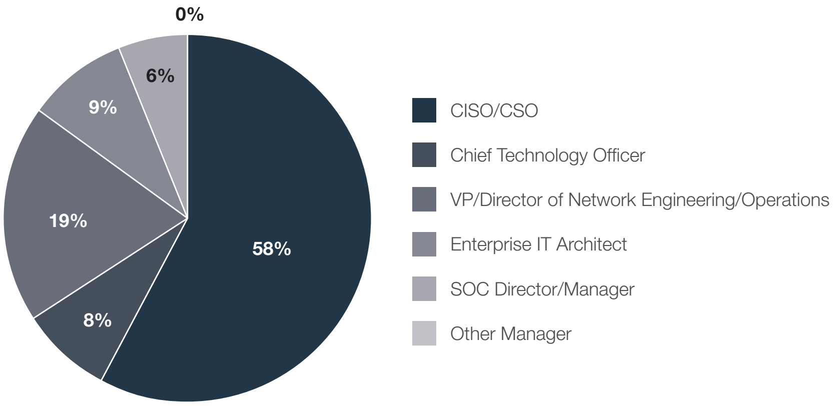

Figure 1: Positions to whom the security architect reports.

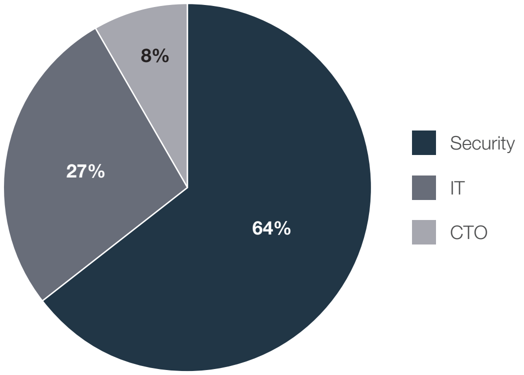

Figure 2: Departmental reporting for the security architect.

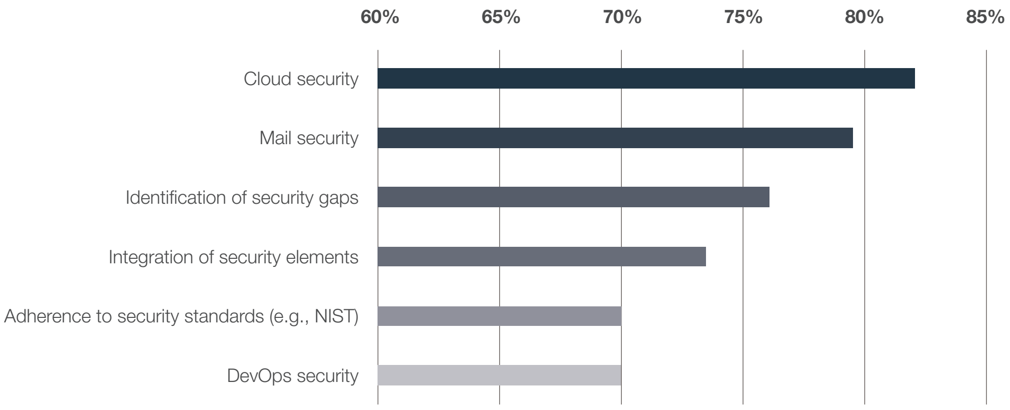

Figure 3: Direct responsibilities of the security architect.

### Trend: Top success metrics for security architects include DevOps security and key infrastructure improvements.

As enterprises adopt DevOps to accelerate software releases, they may create security vulnerabilities in their public cloud. For example, a common mistake is misconfiguring access permissions to storage and computing resources, which can expose sensitive personal information and intellectual property. Given the risks, it is unsurprising that DevOps security is the most important success metric for security architects (37%).[7]

The next three success metrics are security infrastructure integration (32%), security controls centralization (30%), and security workflow automation (29%). These metrics are related to reducing operational complexity, a key determinant of successful technology adoption. A recent survey asked why CISOs decided to scrap security technologies before or soon after deployment, with 77% attributing this decision to overly complex technology and operational difficulties.[8]

In contrast, tactical factors are less important as metrics for security architects. Hands-on activities such as vulnerabilities found (17% of respondents), intrusions stopped (14%), and breach mitigation (12%) were at or near the bottom of the list (Figure 4).

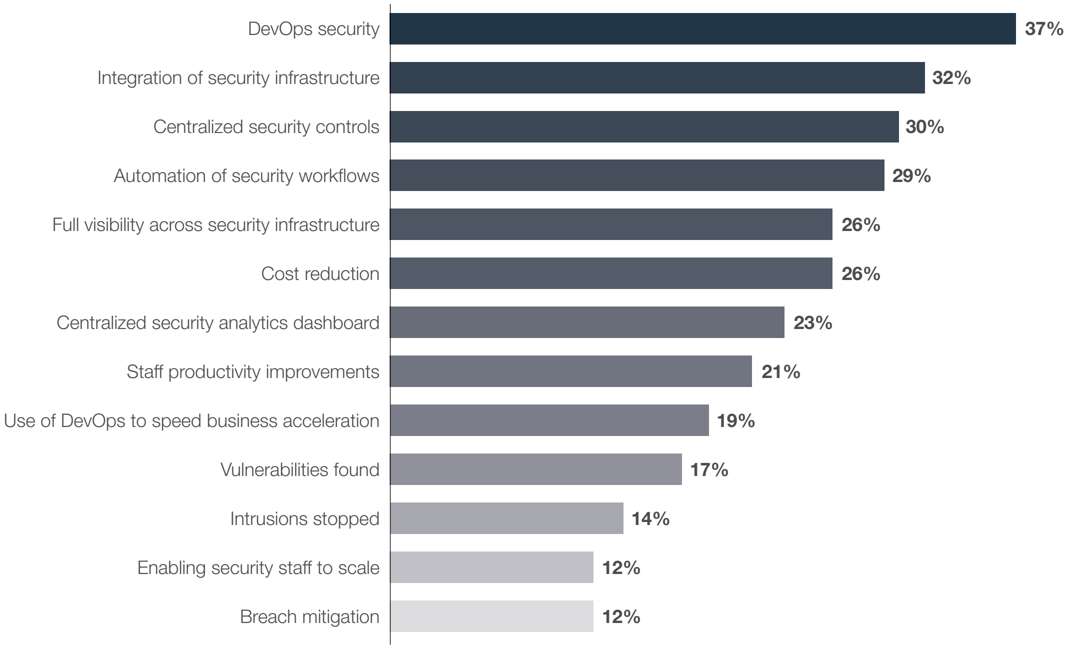

Figure 4: How security architects measure their success.

## Trend: When the security architect role is a shared function, risk increases significantly.

Facing the challenges of an expanded attack surface, increased security complexity, and an advanced threat landscape, seven out of eight (87%) organizations have a dedicated security architect. However, 13% of organizations vest the security architect's duties in the CISO, CIO, or VP of IT security—in effect, relegating the role to part-time status (Figure 5).

In light of the large number of responsibilities of the security architect as well as the growing challenges of cybersecurity, this role sharing could have a detrimental effect on overall security. One result lends credence to this hypothesis: Organizations where the role is shared are 70% more likely to have had six or more intrusions in the previous year compared to those with dedicated security architects.

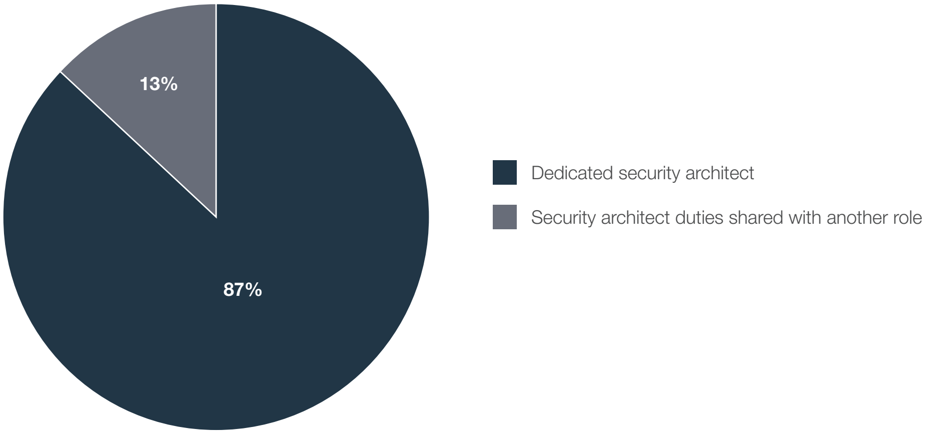

Figure 5: Security architect: dedicated versus shared function.

## Trend: Security architects have confidence in their organization's overall protection level but still struggle with unknown threats.

In general, security architects are confident in their organizations' security posture. Eight in 10 believe that they are protected because they have full visibility and control, and over three-quarters assert that their risk management posture is strategic and proactive.

However, that confidence level erodes when it comes to unknown and zero-day threats: 58% of security architects admit to challenges in that area. In addition, 44% say that they are too reactive in managing risk (Figure 6).

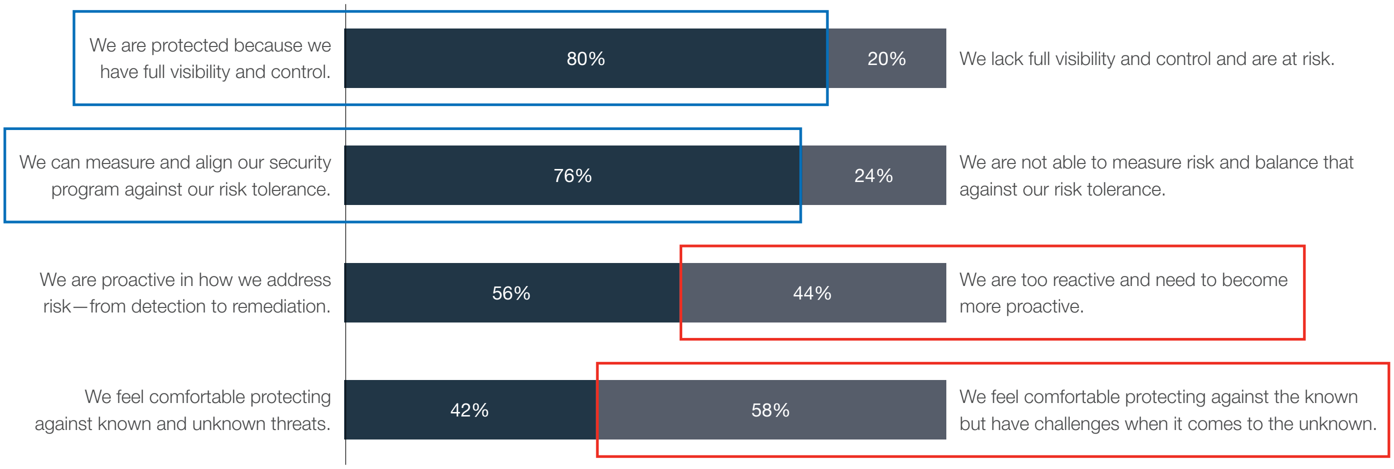

Figure 6: Cybersecurity capabilities per the security architect.

## Trend: Security architects are grappling with fragmented security architectures.

Less than one-third (32%) of security architects have an end-to-end, fully integrated security solution. On the other end of the spectrum, nearly one in five (18%) have no integration and instead rely entirely on point products. The other half are either integrating point products (37%) or working with a mixture of integrated solutions and point products (14%) (Figure 7).

These findings should be viewed in the context of increased security complexity, a key challenge for security architects throughout this report. While many factors contribute to complexity, a poorly integrated security infrastructure is inherently more difficult to operate than a security fabric architectural approach. In addition, managing a collection of disparate point products requires manual intervention, an error-prone process that can introduce vulnerabilities.

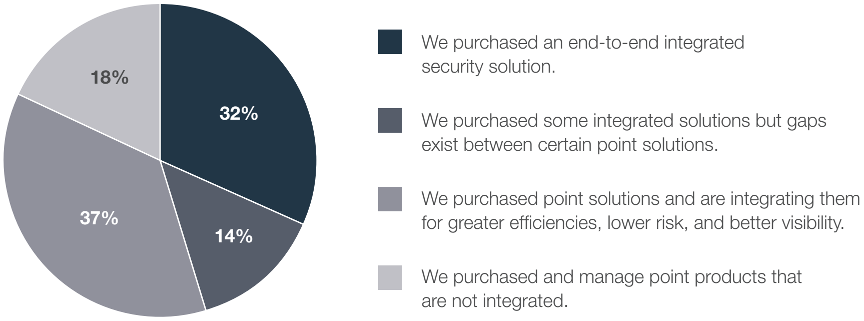

Figure 7: Level of security architecture integration.

## Trend: Nearly half of security architects say security solutions are too difficult to implement.

Security architects cite a wide range of security issues facing their organizations. The top category they name is implementation difficulty (45%). The security skills gap is problematic for many, with 37% indicating lack of expertise and knowledge is a problem for their organizations. This suggests a need for more learning and development opportunities (Figure 8). These findings are confirmed by a recent survey in which 55% of respondents reported lack of in-house expertise prevents deployment of new security technologies.[9] A different study reveals 26% of security professionals lack sufficient job experience to succeed in their roles.[10]

> "Cyberattacks have a drastic effect on our company. An attack can cause us to lose millions."
> – Survey Respondent

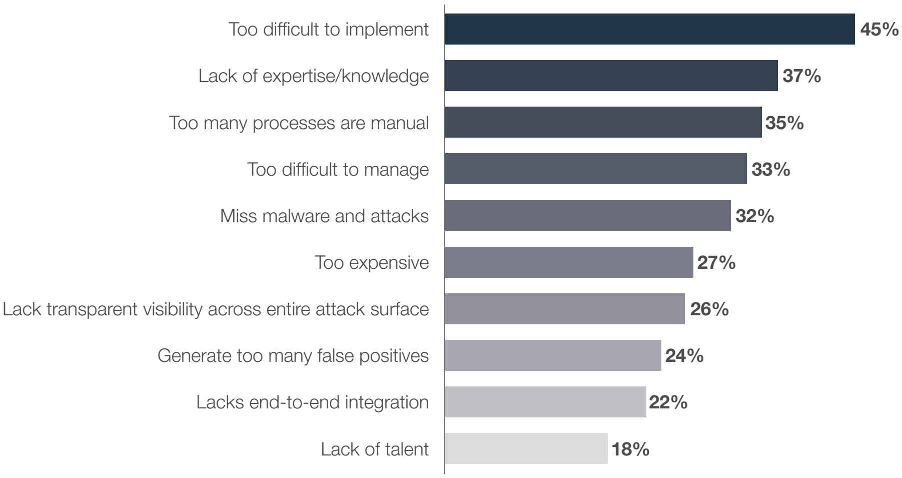

Figure 8: Security challenges reported by security architects.

# Key Personal Challenges for Security Architects

The survey also included open-ended questions to provide a deeper understanding of the key challenges that security architects face in their daily work. While responses vary, the answers were categorized to get a picture of what is top of mind for security architects.

## Challenge: Detecting and preventing intrusions is a top focus for security architects.

A worrying development in cybersecurity is the increasing effectiveness of attackers: successful data exfiltration rose 43% year over year. One outcome is a rapid increase in the cost of security incidents, up 57% over the past year to an average of $4.3 million.[11] Preventing breaches is also getting harder, thanks to increasingly sophisticated attacks that make use of Malware-as-a-Service (MaaS), AI and machine learning (ML), IoT, and other advanced technologies.[12]

> "Successful malware spreads further and faster than ever before, due in large part to the expansion of the potential attack surface."
> – Survey Respondent

It is not a surprise that security architects are focused on this advanced threat landscape. 42% indicate pre-intrusion detection and prevention is the number one factor driving change in their organization's security posture. And with upwards of 40% of attacks employing unknown or zero-day exploits,[13] post-intrusion response and remediation are quickly becoming critical initiatives for many organizations. Thus, it is no surprise that 15% of security architects cite post-intrusion response and remediation as their top challenge (Figure 9). Other top challenges security architects cite include risk management (32%) and pace of change (20%).

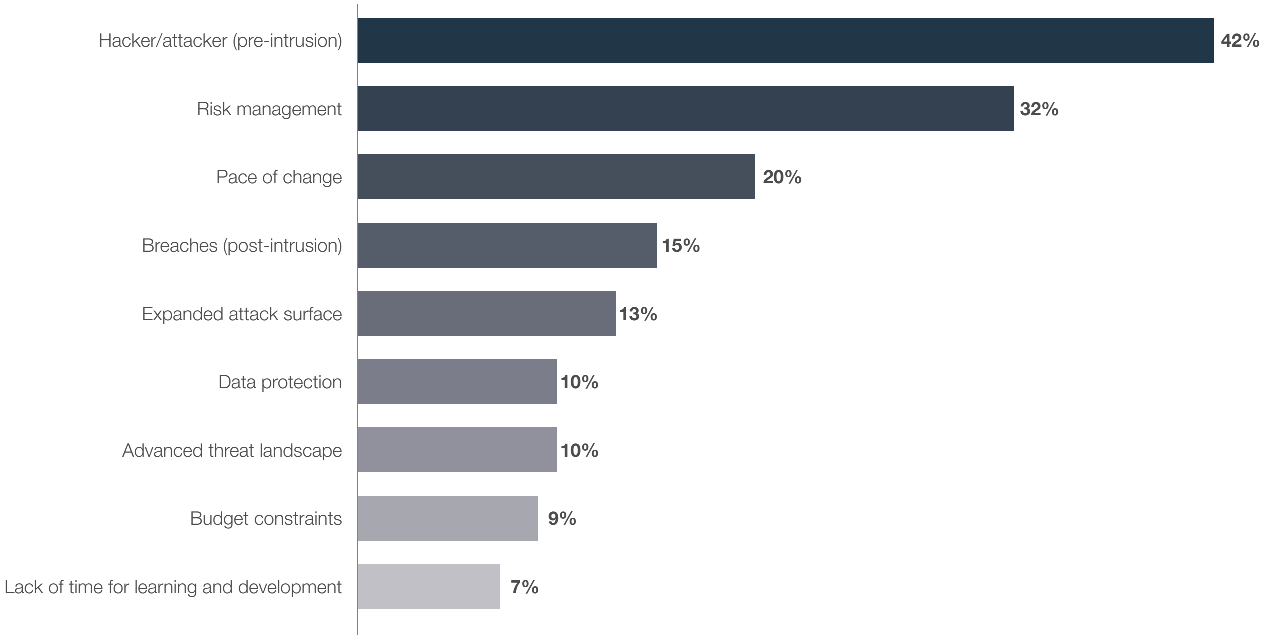

Figure 9: Top challenges for security architects.

## Challenge: The increasing complexity of cybersecurity makes risk management more difficult for security architects.

As described earlier, more than three-quarters (68%) of security architects do not have a fully integrated, end-to-end security architecture, but instead must work with a complex mixture of point products and partially integrated components (Figure 7). In addition to communicating security investments and the business implications of security investments and threats to the C-suite and boards of directors, security organizations also have a growing list of new and evolving compliance requirements. All these factors have direct consequences for security architects: 44% say that increased security complexity is making it more difficult to manage risk (top issue when it comes to increased complexity) (Figure 10).

"My job can get in the way of life. I've missed certain personal milestones because of my professional responsibilities."

"Working hours are getting longer. It is definitely not a nine-to-five job anymore."

– Survey Respondents

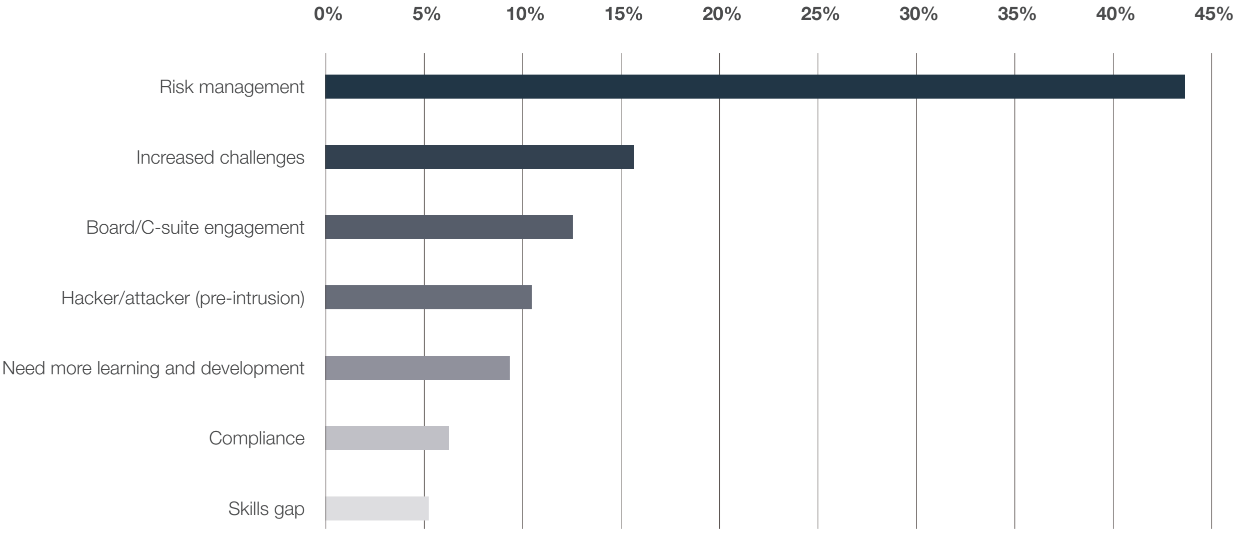

Figure 10: Top effects on security architects due to increasing complexity of managing cybersecurity.

## Challenge: Security architects are experiencing higher rates of burnout due to job pressures.

Advances in the threat landscape are prompting security architects to experience higher rates of job stress and burnout (18%). Given the natural reluctance of high-functioning professionals to admit burnout, the actual numbers are likely much higher. As a reference point, recent research showed that 91% of CISOs face moderate to high stress, while nearly three in 10 (27.5%) report a noticeable strain on their physical or mental health.[14]

Cybersecurity burnout has become a critical issue for productivity, innovation, and talent retention. Burnout reaches crisis proportions in so-called "high-adversity" professions such as cybersecurity, where mistakes are costly, every task is mission-critical, and hypervigilance is the default state.[15] The sheer magnitude of the task is a key factor: 66% of security professionals say their teams are overburdened with an increased workload, leading to burnout.[16]

18% of security architects indicate they are experiencing high rates of job stress and burnout.

## Challenge: Security architects need more learning and development to respond to current trends in cybersecurity.

Security architects indicate they are struggling to keep pace with the expanding attack surface, increased security complexity, and the advanced threat landscape. In each of these categories, respondents cite a need for additional learning and development (Figure 11).

While cost-conscious business executives may balk at increasing learning and development costs and making time for their staff to attend training and certification sessions, a strong case can be made for investing in existing staff. Indeed, in order to evolve security postures to address the expanded attack surface and advanced threat landscape, security architects need to stay current on technology developments in both attack methods and security countermeasures. In addition, learning and development helps retention. For example, a recent study finds that 93% of employees indicate they would stay at a company longer if it invested in their careers.[17] And in a field where there is an acute cybersecurity skills shortage, retention of top cybersecurity staff is particularly important.[18]

> "Efficient security features need higher financial investments; however, justifying these expenses can be tricky."
> – Survey Respondent

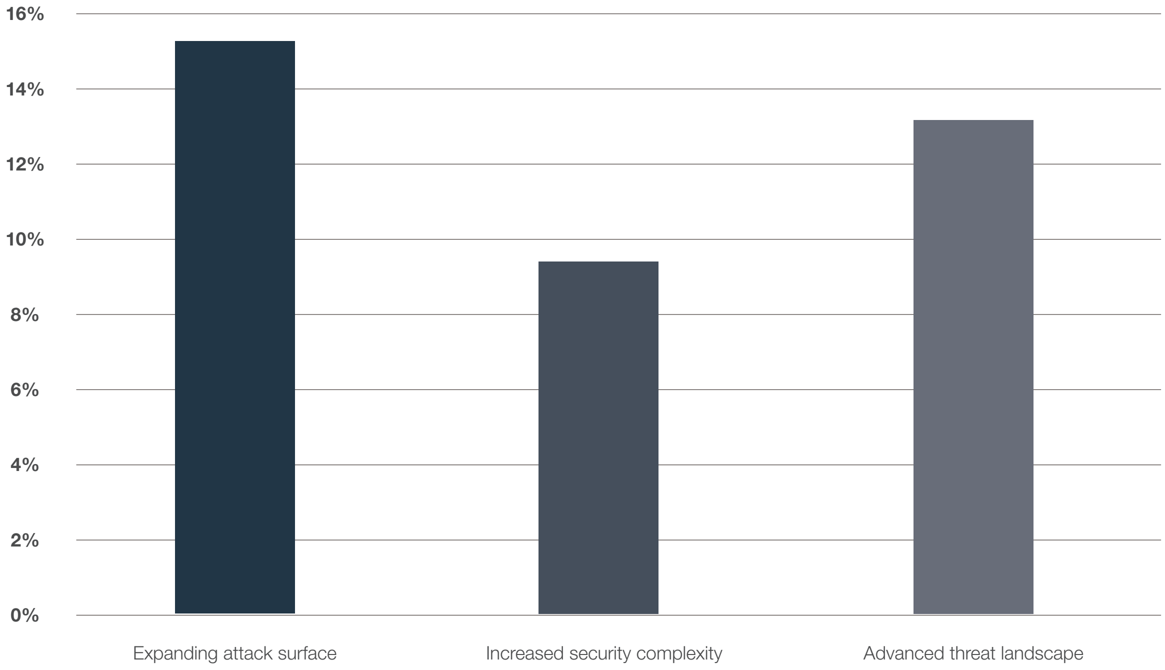

Figure 11: Need for more learning and development per three cybersecurity challenges.

# Best Practices of Top-tier Enterprises

Data from the survey shows security architects face significant challenges protecting their organizations from increasingly sophisticated threats. However, some respondents are more successful than others in combating cyberattacks and reducing risk for their organizations. To better understand the best practices that can explain these differences, the responses for top-tier security organizations (security architects) with no intrusions over the past 12 months were compared to bottom-tier peers who experienced six or more intrusions in the past 12 months.

### 1. Top-tier security architects are 3x more likely to focus on undetected intrusions as a top security issue.

Security architects are confident of their ability to protect against known threats, but they are not as confident when it comes to unknown exploits and zero-day threats. Specifically, top-tier security architects respond proactively to these risk uncertainties by focusing their attention on undetected intrusions, something that they are 3x more likely to do than bottom-tier counterparts.

### 2. Top-tier security architects are nearly 3x as likely to report security cost reductions and their organizations are 21% less likely to cut security budgets.

Top-tier security architects have the right security tools in place to measure and report security cost reductions almost 3x as often as bottom-tier security architects. This level of transparency and value demonstration resonates with business executives; thus, it is not surprising that top-tier security architects are 21% more likely to have budgetary increases.

### 3. Top-tier security architects are more than twice as likely to have purchased integrated solutions.

More than two in five top-tier security architects have either purchased an end-to-end security system (22%) or some integrated solutions (22%) as compared to bottom-tier architects who have much more fragmented security architectures (7% and 13%, respectively). Other findings add texture: top performers are also more likely to track and report the levels of centralized controls (67%) and security integration (11%) than bottom-tier peers. These measures are needed because of the expanded attack surface, which makes it increasingly difficult to combat threats using disaggregated point products.

### 4. Top-tier practitioners are 67% more likely to measure vulnerabilities found and blocked.

This finding appears at first glance to be at odds with the earlier finding where vulnerabilities rank low in terms of importance as a success measure for security architects. However, the two results can be easily reconciled. While security architects are not directly graded on the tactical measure of vulnerabilities found, they nevertheless regard this metric as an important indication of the efficacy of their security strategies and are held responsible for designing and implementing a security architecture that enables the CISO to produce dashboards, which corroborate the value of security investments and measure and track risk.

### 5. Top-tier security architects are 46% more likely to have direct responsibility for risk management.

Security architects in the top echelon are far more likely to be directly responsible for managing risk than their bottom-tier counterparts.

### 6. Top-tier security architects are 33% more likely to report directly to the CISO.

This report shows that top-tier security architects are 33% more likely to report directly to the CISO than to other executives within the organizational pyramid. This reporting structure makes sense considering the CISO is charged with understanding their organization's risk tolerance, designing a security architecture and implementing security tools that satisfy risk requirements, and measuring and reporting risk to executive management and boards of directors.[19]

### 7. Top-tier security architects are 30% more likely to be involved in IoT security.

The convergence of physical things and cybersecurity is creating an expanded attack surface, one that cyber criminals are increasingly exploiting. For example, half of the top 12 global exploits in 2018 targeted IoT devices.[20] Notably, security architects in the top tier are 30% more likely to work on IoT security. With 25% of all cyberattacks projected to target IoT devices within a year, this attribute directly ties to an organization in preventing intrusions. [21]

"The scale of security risks in the IoT era is much greater than in the pre-IoT environment, and the attack surface is much larger."
– Survey Respondent

# Conclusion

Our research shows that security architects play an increasingly important role in designing and building cybersecurity infrastructure and have a critical stake in protecting their organizations from malicious attacks. Some organizations realize better results than others, and their security architects embody certain attributes that differentiate themselves from other security architects. Some of the notable ones include:

Preference for end-to-end integrated security solutions over point products and partially integrated architectures

Directly report to the CISO and charged with risk management

Tie the success of security initiatives to outcomes such as vulnerabilities blocked due to architectural initiatives

Measure cybersecurity program effectiveness in terms of both risk as well as business (e.g., cost reduction, efficiencies)

Security architects are a critical linchpin when it comes to organizational success in managing risk and achieving optimal value from security investments. Those who are most successful design and maintain security architectures that exhibit certain traits (e.g., integration), focus on specific threat areas (e.g., IoT devices, tracking vulnerabilities), and hold an influential position within the organizational structure (e.g., report to the CISO).

# References

[1] Mark Wilczek, "Why Cyberattacks Are the No. 1 Risk," Dark Reading, January 15, 2019.

[2] In some cases, the C-suite role for cybersecurity is designated as the chief security officer (CSO). This study elects to use chief information security officer (CISO) as the designation for both the CSO and CISO.

[3] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[4] The reporting structure for the CTO varies in organizations. For organizations where the CTO is responsible for product development, the role is a peer to the CIO (parallel organization). But in other organizations, the CTO often reports to the CIO and is charged with technology development. See Rob van der Meulen, "Understand the 5 Common CTO Personas," Gartner, April 12, 2018.

[5] "2019 State of DevOps Security Report," Fortinet, May 10, 2019.

[6] "2019 Data Breach Investigations Report," Verizon, May 2019.

[7] "2019 State of DevOps Security Report," Fortinet, May 10, 2019.

[8] Sam Friedman, "Taking cyber risk management to the next level," Deloitte Center for Financial Services, 2016.

[9] Ibid.

[10] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," (ISC)$^2$, accessed June 12, 2019.

[11] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar, February 20, 2019.

[12] For example, see Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018; Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[13] "Fortinet Security Fabric Powers Digital Transformation: Broad, Integrated, and Automated," Fortinet, March 29, 2019.

[14] "91% of CISOs Reveal They Experience Moderate to High Stress," The CISO Collective, February 15, 2019.

[15] Karen Worstell, "Cybersecurity Burnout: What It Is, Why It Matters, and What to Do About It," Security Boulevard, November 20, 2018.

[16] "What CISOs Need to Know About the Cybersecurity Skills Gap," The CISO Collective, June 4, 2019.

[17] Meghan M. Biro, "Developing Your Employees Is The Key To Retention—Here Are 4 Smart Ways To Start," Forbes, July 23, 2018.

[18] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ICS)$^2$, October 18, 2018.

[19] Patrick Spencer, "6 CISO Strategies for Building Collaborative Rapport with the Boardroom," The CISO Collective, November 30, 2018.

[20] "Cyber and Physical Convergence is Creating New Attack Opportunities for Cybercriminals," Fortinet, February 20, 2019.

[21] Nick Ismail, "The Internet of Things: The security crisis of 2018?," Information Age, January 22, 2018.

FORTINET®

www.fortinet.com

June 29, 2019 2:36 PM

D:\Fortinet\Work\2019\June\062919\report-security-architect-and-cybersecurity

330866-0-0-EN