FORTINET

Untangling Security Complexity Through Integration and Automation

4 Strategies for the CIO

Table of Contents

Executive Overview

CIOs are accelerating business cycles and enabling radical new capabilities through innovative tools such as cloud-based applications and advanced development operations (DevOps) processes. But the same digital innovations that turbocharge productivity simultaneously expose new risks. As CIOs increase the speed and complexity of their network infrastructures, they also need to consider the appropriate cybersecurity protections that will keep their systems, data, and users safe in the face of rapid change. Fortinet helps CIOs reduce network security complexity as well as the costs of continuously adding on more isolated products to cover new threats or risk exposures.

01 Introduction: Complexity Is the Enemy of Security

Without question, CIOs are embracing strategic innovation as a path toward greater business efficiency and effectiveness. Transformative digital technologies are enabling new capabilities and growth across all industries. Breakthroughs such as cloud-based applications, Internet-of-Things (IoT) devices, as well as internal or external development operations (DevOps) services are helping boost productivity, improve scalability, reduce costs, and accelerate time to market through automation.

But the impacts of these changes on organizations are not all positive. Networks are becoming much more complex, and this creates an expanded attack surface with new risk exposures. Using de facto security that is piecemeal and conducted in solution silos is inefficient, costly, and unable to address security or compliance requirements. According to a recent survey of enterprise CIOs, 77% of organizations rely on nonintegrated point security products to some degree within their organization—leaving gaps in security effectiveness.[1]

Complicating matters even further are the demands of increasingly strict compliance rules such as the European Union's General Data Protection Regulation (GDPR) and security standards such as the National Institute of Standards and Technology (NIST). Organizations must manage, govern, and ensure compliance for the overwhelming amount of data they produce. This becomes increasingly difficult when factoring in employee personal devices, unpatched software as a result of Shadow IT, and managing vendors or partners who have some network access.[2]

These intersecting forces are driving a demand for greater technology expertise and leadership within the CIO role.[3] To keep pace, CIOs can start addressing the problems of security complexity by focusing on four strategic solution areas:

- **Integrated Security**
- **Automated Security Workflows**
- **Automated Compliance Governance**
- **Simplified Risk Management**

78%

of CIOs believe their digital strategy is only moderately effective—or worse.[4]

02 Integrated Security

In addition to attack surface expansion, advanced threats targeting network vulnerabilities are growing in both number and sophistication at the same time. The widespread use of one-off additions of point security products in an attempt to address new vulnerabilities in a "whack-a-mole" fashion has created a disjointed security infrastructure within most organizations.

This lack of integration creates two significant problems for CIOs. First, it limits threat intelligence. Disconnected security solutions cannot share information about potential threats across the organization, which makes coordinated responses to multipoint attacks slow and inefficient. Second, a lack of integration forces organizations to over-rely on manual processes overseen by already overburdened security staff. Human compilation of threat intelligence data and audit trails for compliance reporting requirements is time-consuming, expensive, prone to errors, and cumulatively inefficient when compared to the complementary automated capabilities that are enabled by an integrated security architecture.

An integrated security architecture connects disparate security products into a cohesive system that shares real-time intelligence across all parts of the organization. This, in turn, supports:

- Prebuilt application programming interfaces (APIs) as well as the ability to quickly integrate those outside of the architecture with representational state transfer (REST) APIs
- Centralized management (single-pane-of-glass console) for transparent visibility and application of consistent control policies across all deployed security solutions throughout the organization
- An open ecosystem that can incorporate third-party solutions to maximize existing security investments
- Reduction of complexity and costs from adding on more isolated products to cover new risk exposures
- And perhaps most importantly, a foundation for automated security capabilities

Lack of end-to-end integration is a top security concern for almost one-third (32%) of CIOs today.[5]

03 Automated Security Workflows

A recent survey of CIOs from around the world showed that 65% of respondents felt that a lack of talent was holding their organization back.[6] Automation can help address this problem by helping to free up security staff and scale limited skill sets. Human focus can then be placed on more delicate initiatives, such as risk governance and management.

Manual workflow processes such as deployment and provisioning, threat alert research, or access management of users and devices can all be automated and orchestrated through policy-based controls. CIOs can address automation needs in two main incident response workflow areas.

Network operations center (NOC) automation needs may include:

- DevOps security controls that help accelerate (rather than inhibit) time to market
- Zero-touch provisioning across distributed organizations
- Access management for devices and users
- Real-time insights around branch network performance to help manage things like spikes, scaling, and priority routing of traffic

Security operations center (SOC) automation needs may include:

- Proactive threat detection
- Threat correlation and intelligence sharing
- Alerts and threat research/analysis
- Event responses and remediation

67%

of CIOs plan to use automation to remove the need for additional headcount.[7]

04 Automated Compliance Governance

CIOs should be looking for ways to automate compliance governance. The cumulative burdens of manually tracking and reporting for the organization's adherence to industry standards and privacy laws is both time-consuming and costly.

With the first major fines for violations of the GDPR already being handed down,[8] compliance should be a front-of-mind concern for executives and boards of directors. A majority of organizations must provide audit trails to show compliance with data privacy laws, including the GDPR, the new California Consumer Privacy Act (CCPA), as well as established industry regulations like the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act (SOX).

Ensuring compliance with data privacy throughout its life cycle is good for business in that organizations can demonstrate they are worthy of customer trust.[9] And CIOs are invariably responsible for maintaining privacy of customer data—either directly or indirectly.[10] As visibility problems such as Shadow IT become more prevalent, ensuring and maintaining compliance will become more complex for CIOs, who must ensure that sensitive information is not being stored in third-party systems without proper oversight.[11]

Look for security solutions that offer both visibility and the agility to scale across a growing and changing network. A defensive system also needs the flexibility to accommodate evolving security and regulatory compliance requirements without re-architecting the security infrastructure. This includes reporting that encompasses all security solution elements to eliminate manual log pulls and wasted staff time. Automated compliance tracking and reporting capabilities can provide custom dashboards for specific executive roles and boards of directors to facilitate internal oversight.

69%

of companies see compliance mandates driving spending.[12]

05 Simplified Risk Management

CIOs must also adhere to security standards used to manage and assess risk such as **NIST**, the **International Organization for Standardization (ISO)**, and the **Center for Internet Security (CIS)**. Many of these are becoming de facto government standards. For example, an estimated 50% of all U.S. organizations will adopt the NIST framework by 2020 for evaluating, tracking, and reporting security status—including those in healthcare, retail, financial services, and all sectors of critical national infrastructure.[13]

Analysis-based risk scoring tools and services offer dynamic vulnerability assessments and peer comparisons that can help CIOs visualize the current state of exposure across their entire organization. Risk scoring provides measurable benchmarks and meaningful feedback in terms of configuration recommendations to help manage risk indicators and improve the company's security posture. Multi-factor risk scoring can specifically address potential data vulnerabilities by looking at access frequency, user activity, proliferations, and volumes to enable risk-based prioritization of privacy issues.[14]

In addition, **intent-based segmentation** capabilities help translate business intent into the "where," "how," and "what" that control access to sensitive data and systems. Intent-based segmentation provides fine-grained access control that adjusts based on a continuous trust assessment of users. As part of an integrated security architecture, intent-based segmentation can effectively improve an organization's defensive posture, mitigate risks, support compliance, and boost operational efficiency.

In a recent survey, CIOs reported that the leading measure of their success is cybersecurity risk management.[15]

06 Reducing Security Complexity (Summary Checklist)

Within the four aforementioned general solution areas, CIOs should look for these six specific capabilities when evolving their security architecture for greater simplicity and efficacy:

□ Integration that connects disparate security products into a cohesive, intelligent security architecture

□ Single-pane-of-glass management for centralized visibility and control of the entire security infrastructure

□ Features and/or solutions that can automate workflows to simplify things like deployment, access management, and threat analytics for greater contextual awareness

□ Automated compliance tracking and reporting capabilities

□ Analysis-based risk scoring to measure and help manage exposures in real time

□ Intent-based segmentation for granular, policy-based control of internal network traffic

[1] "State of the CIO and Security Report," Fortinet, March 2019.

[2] Jennifer Lonoff Schiff, "5 biggest IT compliance headaches and how to address them," CIO, May 9, 2018.

[3] "Role Of CIO Is Changing And Growing In Importance, Say New Forbes Insights Studies," Forbes, March 28, 2018.

[4] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, May 25, 2018.

[5] "State of the CIO and Security Report," Fortinet, March 2019.

[6] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, May 25, 2018.

[7] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, May 25, 2018.

[8] Adam Satariano, "Google Is Fined $57 Million Under Europe's Data Privacy Law," The New York Times, January 21, 2019.

[9] Nancy Couture, "How data governance can support data privacy compliance," CIO, February 7, 2019.

[10] "State of the CIO and Security Report," Fortinet, March 2019.

[11] "CIO Survey 2018: The Transformational CIO," Harvey Nash and KPMG, May 25, 2018.

[12] Josh Fruhlinger, "Top cybersecurity facts, figures and statistics for 2018," CSO, October 10, 2018.

[13] Jonathan Nguyen-Duy, "The Cybersecurity Regulations Healthcare, Financial Services, and Retail Industries Must Know About," Fortinet, August 21, 2018.

[14] Nancy Couture, "How data governance can support data privacy compliance," CIO, February 7, 2019.

[15] "State of the CIO and Security Report," Fortinet, March 2019.

www.fortinet.com

323378-0-A-EN

March 20, 2019 5:35 PM

ebook-untangling-security-complexity.indd