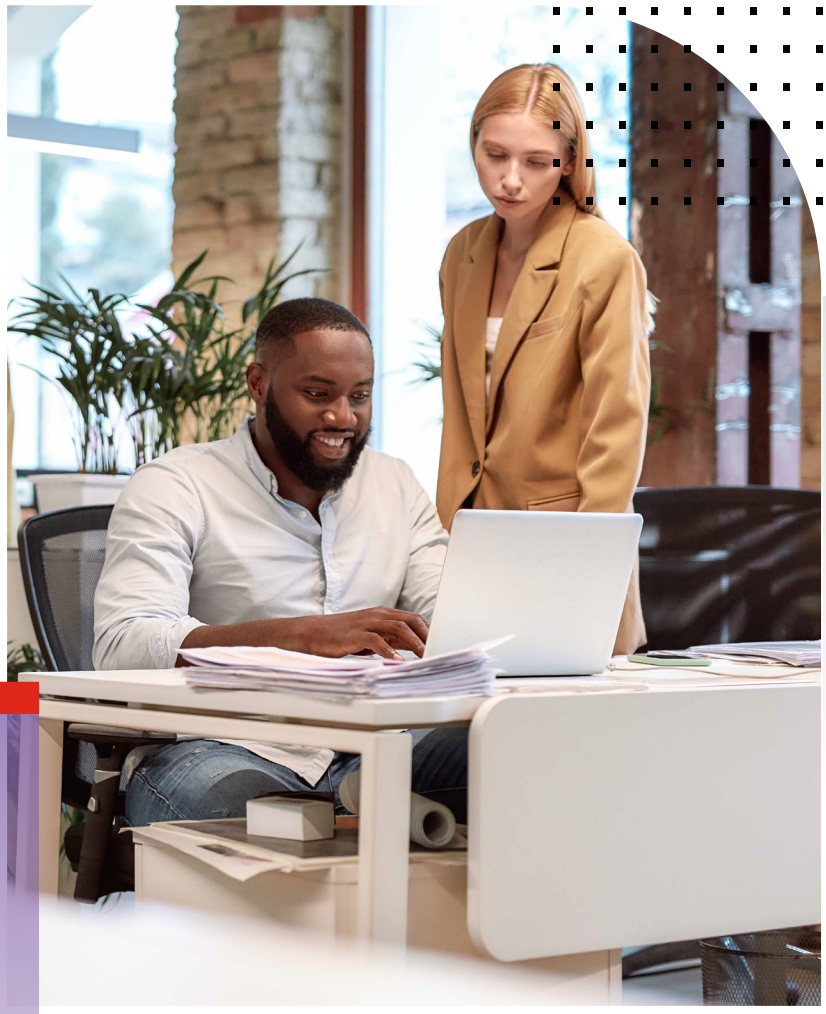
WHITE PAPER

Network Complexity Creates Inefficiencies While Ratcheting Up Risks

Understanding the Causes and Implications



Executive Summary

The rapid adoption of digital transformation (DX) makes both network and security more complex. The increased complexity ratchets up vulnerabilities as a result. This leads to a greater frequency of data breaches and a higher average cost per breach. One of the factors behind complexity is a proliferation of isolated "point" security products. Other drivers include ever-increasing demands of maintaining compliance with privacy laws and industry regulations and providing the C-suite and boards of directors with regular assessments of the risk posture. With a limited number of network and security professionals at their disposal, network engineering and operations leaders struggle to find and recruit the talent with the right skill sets needed to address these requirements.

Companies that contain breaches in under 30 days save $1 million or more in comparison to those that take more than 30 days.[2]

Nearly 80% of organizations are introducing digital innovations faster than their ability to secure them against cyberattacks.[4]

Tangled Up in Complexity

Rapid adoption of digital innovations like cloud computing, Internet-of-Things (IoT) products, and a vast array of mobile devices has changed the structure and functionality of enterprise networks. As a consequence of this digital evolution, enterprise infrastructures have become increasingly complex and fragmented—which contributes to both the rising number of data breaches as well as a higher cost per incident. The global average likelihood of a breach occurring in the next 24 months continues to creep up—rising from 27.7% in 2017 to 27.9% in 2018. The mean time to identify a breach increased to 197 days and the average cost per incident grew by 6.4% from the previous year to reach $3.86M.[1]

While increasing threat sophistication and outdated security strategies each play a part in this trend, the challenges of network complexity present their own significant risks. This can be seen in the fact that more than half (52%) of all breaches last year were caused by either human errors or system glitches (as opposed to malicious or criminal attacks).[3]

The challenges of complexity for networking leaders break down into three main areas of focus:

- Adding on disconnected tools that may only cover a single enterprise requirement, which obscures visibility while creating operational inefficiencies
- Too few employees to manage those tools and associated workflows—not to mention staff in all key positions that have the requisite training, skills, and knowledge for these tasks
- Ever-increasing compliance requirements associated with laws, regulations, and standards—which typically call for manual compilation of reports and audits from already overburdened staff resources

Too Many Point Products

Widespread use of point security products increases the complexity of network and security management for enterprises. The average enterprise uses upwards of 75 different security solutions, many of which only address a single attack vector or compliance requirement.[5] Organizations need different tools for different infrastructural environments (e.g., data center, virtual servers, public cloud). In some cases, those solutions are then managed by separate teams, which can create operational inefficiencies when it comes to coordinating policies and controls.[6]

Siloed devices create a disaggregated architecture by default, where the disparate solutions do not communicate with one another or share intelligence. Point products obscure network and security operations teams from having clear and consistent insight into what is happening across the organization. Network and security teams lack centralized visibility to monitor data movement and identify anomalous activity. This leads to wasted staff hours due to increased manual tasks and administrative work. Organizations become stuck in a perpetual reactive mode, which makes it difficult to perform strategic planning that anticipates infrastructural changes or emerging threat patterns.

Too Few Skilled Staff

The problems of disconnected point security products are often compounded by a lack of skilled personnel to manage them. Subsequently, network teams can become overburdened with the demands of maintaining these complex infrastructures. In a recent survey, 27% of security professionals reported high volumes of alerts as a result of using point security tools, making it difficult for them to prioritize and investigate incidents.[8] Most companies lack sufficient staff resources to research and respond to every alert where an anomaly has been detected. Manual security processes slow down operations while exposing the organization to greater risks—it takes longer to detect a potential security issue and longer to remediate problems once they are discovered. Even major enterprises with large, dedicated IT staffs still have difficulty monitoring their networks to keep track of which devices are connected, who has access to data, where data is stored, and which resources are needed by applications and workflows.

Beyond the time it takes to physically vet, research, and mitigate potent security issues, human error is also a significant factor when it comes to overall operational effectiveness. Mistakes and misconfigurations are the leading cause of security breaches and/or network outages.[9] The current lack of significant automation and orchestration tools also shows in the increasing time it takes to identify and remediate breaches, year over year.[10]

77% of organizations rely on non-integrated point security products to some degree within their organization—leaving gaps in security effectiveness.[7]

56% of breaches last year took months or longer to discover.[11]

Increasing Compliance Risks and Responsibilities

Regulatory compliance further complicates the picture for network leaders. As requirements continue to expand and evolve, organizations have greater responsibility (and pressure) to demonstrate due diligence. Consequences of compliance violations can include fines, sanctions, loss of reputation, negative business outcomes, or a combination of the above. In a survey by PwC, 85% of consumers said they would not engage with a business if they have security concerns about it.[12]

Some prominent examples include government regulations such as the European Union's General Data Protection Regulation (GDPR) and security standards such as the Center for Internet Standards (CIS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Many organizations must also comply with ISO 27001 risk management, Control Objectives for Information and Related Technologies (COBIT), and the Committee of Sponsoring Organizations (COSO) framework for battling corporate fraud. There are also industry-specific regulations to account for, such as the Health Insurance Portability and Accountability Act (HIPAA) within the healthcare sector.

Each organization may need to prove its accountability for multiple laws, regulations, and standards. And each of those carries its own set of evolving best practices. Tracking changes can present challenges for staff year to year. Compliance management itself is convoluted, inefficient, and time-consuming at most companies. It typically requires manual compilation done by multiple full-time staff over several months each year. To prove compliance, security data from multiple point devices has to be aggregated and normalized. For each disparate solution deployed, staff must be intimately familiar with each device vendor's individual audit tools and/or control panels. Manual auditing processes also introduce more opportunities for human errors—making them ineffective on top of being inefficient.

But compliance should also be more than an obligation to avoid punitive fines and bad press. Auditing and reporting should also be a tool to help network leaders spot security risks, eliminate exposures, and ensure the integrity of the network. If compliance management processes are too convoluted to be effective, the results of an undetected breach can be much more severe than those of a regulatory slap on the wrist.

Solving Simplicity

Complexity is the enemy of security—and networks have grown far too complex to continue to apply outdated thinking to defending data and operations from exploitation. One recent article on the subject explains the situation as follows:

The IT industry has gone through lots of changes over the past few years, yet when it comes to cybersecurity, the mindset has remained the same. The current thinking around cybersecurity falls into the definition of insanity, with many organizations doing the same thing over and over again, expecting different results, and are then shocked when their company is the latest to hit the hacking headlines.[14]

The problems associated with network complexity cannot be ignored. Security must be reimagined and rearchitected to simplify operations for both networking and security teams. Networking engineering and operations leaders should evaluate their cybersecurity strategy to address three critical shortfalls:

A French data regulator (CNIL) recently issued the largest fine to date in association with GDPR enforcement—$57 million USD.[13]

- The need for centralized management and transparent visibility that can scale with infrastructure growth
- The need for automation and orchestration for operations and enterprise workflows to unburden limited IT staff resources
- The lack of auditing and reporting tools to help expedite ever-expanding demands of compliance management

[1] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[2] Ibid.

[3] Ibid.

[4] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

[5] Kacy Zurkus, "Defense in depth: Stop spending, start consolidating," CSO Online, March 14, 2016.

[6] Jon Oltsik, "The problems plaguing security point tools," CSO Online, January 30, 2019.

[7] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[8] Jon Oltsik, "The problems plaguing security point tools," CSO Online, January 30, 2019.

[9] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[10] Ibid.

[11] "2019 Data Breach Investigations Report," Verizon, April 2019.

[12] "Consumer Intelligence Series: Protect.me," PwC, accessed May 1, 2019.

[13] Kelly Bissell, et al., "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study," Accenture and Ponemon Institute, March 6, 2019.

[14] Dave Whitelegg, "Complexity is the Worst Enemy of Security, Time for a New Approach with Network Security?," Security Boulevard, November 7, 2018.

FORTINET

www.fortinet.com

May 8, 2021 4:07 AM

D:\Fortinet\2021 Rebranded templates\White paper\May\Refresh\Network Complexity\wp-network-complexity-creates-inefficiencies-V1-582021\wp-network-complexity-creates-inefficiencies-V1-582021

367535-A-0-EN