FORTINET

WHITE PAPER

Security Complexity Spirals Out of Control

Analytical Fragmentation Creates Challenges for Security Architects

Executive Overview

Cybersecurity teams are deploying more security solutions and getting more data from them than ever, but the resulting picture is not encouraging. Complexity in managing those disparate solutions, aggregating and reconciling data from them, and demonstrating compliance with government and industry regulations—not to mention security standards—is overwhelming many already overstretched security teams. At the same time, complexity obfuscates visibility and bogs down security responses, ratcheting up risk. Security analytics, in particular, has never been more difficult to track and manage—and business and technology leaders see the security architecture as a critical contributing factor.

Introduction: More Money and Tools Are Part of the Problem

For security architects, the big picture is ironic. Budgets are growing: organizations currently spend $168 billion per year on information security and may increase that amount to as much as $248 billion by 2023.[1] Point security tools are also increasing: the average enterprise deploys security solutions from 75 different vendors.[2]

However, cybersecurity is becoming less effective: the annual number of confirmed data breaches reported in 2018 grew 15% to 2,216.[3] One of the primary reasons is that complexity is increasing. As risks multiply, bigger budgets and more security tools are actually making companies less safe.

Security teams have too much to monitor and manage. And because security architectures are not integrated, teams must spend substantial time and resources manually analyzing security logs and correlating data between solutions. Traditional security analytics approaches are being overwhelmed, with the result being a reactive security posture. This eBook pinpoints six factors that are driving this complexity.

1. Threats Are Harder for Analytics to Detect and Remediate

Cyber criminals and nation-states are making it increasingly difficult for security teams to detect and prevent attacks. There were only 50 threat types to detect a decade ago, and now there are more than 1 million.[4] Attack methods are more sophisticated as well: up to 40% of new malware detected on a given day is now zero-day or previously unknown,[5] and 97% of viruses now employ polymorphism.[6]

The result is a growing number of both intrusions, breaches, and outages, as security teams find it more and more difficult to detect, prevent, and respond to these advanced threats. Over the last year, the mean time to identify a data breach incident increased from 191 days to 197 days,[7] and the average cost of a data breach has increased 6.4% to $3.86 million.[8]

These are all indications that the resources of threat actors exceed the ability of traditional security analytics to spot and stop them.

2. Growing Digital Attack Surface Is a Bigger Challenge to Monitor

Compounding the problem, security analytics must account for a proliferation of digital environments and devices that need to be monitored. For instance, organizations use an increasing number of clouds (now averaging five), and are putting more workloads in them (83% of workloads will run in the cloud by 2020).[9,10] Additionally, security teams must monitor not only multiple cloud environments but also dozens of cloud software services, software containers, endpoint form factors, and virtualized workloads, all with different vulnerabilities.

Another factor expanding the attack surface, and challenging traditional security analytics, is the Internet of Things (IoT). There are 1 million new IoT devices being added to networks daily, with 25% of all attacks predicted to target IoT by next year.[11] And the IoT challenge is going to become even worse: IoT device and network proliferation poses serious problems around data collection, correlation, and analysis for threat detection.

25% of all attacks will target IoT by next year.

27% of IT professionals receive more than 1 million alerts daily.

There are nearly 3 million unfilled security positions worldwide.

3. Security Tools Have Proliferated Without Consolidated Detection and Response

Over three-quarters of organizations admit their security architectures are disjointed due to nonintegrated security products.[12] Teams have multiple management portals to inspect, and they must manually correlate the data from them. As a result, security teams respond more slowly to alerts, have time for fewer investigations, and work with a greater chance of error.

A staggering 27% of IT professionals indicate receiving more than 1 million alerts daily, while 55% report more than 10,000 alerts. Even more alarming, more than half (56%) of security professionals admit to having ignored an alert. Moreover, almost half (47%) of security operations center (SOC) staff spend four or more hours a day dealing with security alerts, and investigations are more complex because of proliferation of tools.[13]

4. Cybersecurity Skills Shortage Makes Investigations Harder

Successful security analytics requires analysts with appropriate training. However, finding and retaining professionals with the right cybersecurity skill sets has never been more difficult, with nearly 3 million unfilled security positions worldwide today—a number that is expected to grow in coming years.[14]

Almost two-thirds (65%) of CIOs express that a lack of cybersecurity talent is holding their organizations back.[15] More than half (54%) of security professionals report experiencing a high amount of stress and frustration due to excessive security alerts.[16] For security analytics to succeed, overwhelmed teams need help that they are not currently getting.

5. New Regulations and Best Practices Add Complexity

When security teams do not adequately safeguard data, governments step in and mandate how it should be protected. The result is an increasing volume of regulations, including the European Union's General Data Protection Regulation (GDPR), the U.S. Clarifying Lawful Overseas Use of Data (CLOUD) mandate, and China's Internet Security Supervision and Inspection regulations.

In response, security leaders recognize the importance of managing risk based on established standards. They embrace best practices such as the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. About one-third (30%) of organizations use the NIST Cybersecurity Framework, and half are projected to use it by 2020.[17] However, this adds more work and complexity for security architects and teams.

6. Overall Risk Needs to Be Measured

Security architects know that risk can be managed, but only if it is measured. Business executives and boards of directors want to understand how their organization's security posture stacks up against industry averages and to track their security scores in team time. This helps translate security issues into business intelligence they understand. However, 58% of organizations score a failing grade when evaluating their efforts to measure cybersecurity investments and performance against best practices.[18]

Cybersecurity architects need to put in place the right analytics tools to deliver a consolidated and centralized measurement of risk. This is not easy, but until risk is measured, it cannot be truly managed.

117 countries have cybersecurity laws in place.

58% of organizations fail to measure cybersecurity performance against best practices.

A New Security Analytics Strategy Is Needed

Data generated by a growing volume of cybersecurity tools and threats can be part of the problem or part of the solution. With today's traditional analytics approaches, it is part of the problem:

- Increasingly sophisticated threats evade detection with growing success.
- An expanding attack surface presents more vectors to monitor.
- More and more security tools are overwhelming teams with threat alerts.
- Because of a global cybersecurity skills shortage, there are fewer analysts to investigate security alerts.[19]
- Added compliance challenges pull resources from threat detection and response.[20]

These are signs that traditional analytics strategies are being overwhelmed. A new strategy is needed that centralizes visibility, prioritizes threats, maps the network against regulations and security standards, and automates responses to threats.

[1] "Cybersecurity Market worth $248.26 billion by 2023," MarketsandMarkets, September 21, 2018.

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

[3] "2018 Data Breach Investigations Report," Verizon, March 2018.

[4] David Petraeus, "The Cybersecurity Mega Cycle Aftermath," Optiv, September 7, 2017.

[5] According to internal data from FortiGuard Labs.

[6] Kevin Williams, "Threat Spotlight: Advanced polymorphic malware," SmarterMSP.com, June 13, 2018.

[7] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[8] Sydny Shepard, "The Average Cost of a Data Breach," Security Today, July 17, 2018.

[9] Marc Wilczek, "IT governance critical as cloud adoption soars to 96 percent in 2018," CIO, April 2, 2018.

[10] Louis Columbus, "83% Of Enterprise Workloads Will Be In The Cloud By 2020," Forbes, January 7, 2018.

[11] "25% Of Cyberattacks Will Target IoT In 2020," Retail TouchPoints, accessed September 6, 2018.

[12] "State of the CIO and Security Report," Fortinet, May 23, 2019.

[13] Tami Casey, "Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily," Imperva, May 28, 2018.

[14] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

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

[16] Tami Casey, "Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily," Imperva, May 28, 2018.

[17] "Cybersecurity Framework," NIST, accessed May 25, 2019.

[18] "Most companies fail to measure cybersecurity effectiveness," Help Net Security, July 27, 2017.

[19] "Cybersecurity Skills Shortage Soars, Nearing 3 Million," (ISC)², October 18, 2018.

[20] "Cost of Compliance 2018 Report: Your biggest challenges revealed," Thomson Reuters, accessed May 25, 2019.

FORTINET

www.fortinet.com

369441-0-0-EN

D:\Fortinet\White Paper\FortiAnalyzer Security Architect\FortiAnalyzer Security Architect V2.2