FORTINET

WHITE PAPER

Top Security Concerns Stemming from Digital Innovation

Evolving Networks and Threat Ecosystems Increase Security Complexity

Executive Summary

Digital innovation (DI) initiatives are designed to improve a company's efficiency and customer experience. However, this is often accomplished by deploying new systems and solutions, including Internet-of-Things (IoT) devices, mobile devices, cloud computing, and new branch locations. These create additional security and operational complexities that open up an organization to new cyber risks.

As digital attack surfaces expand and the cyber-threat landscape evolves, security teams commonly attempt to address new risks through deployment of point security products. However, the additional complexity associated with monitoring and managing these point solutions, exacerbated by new data protection regulations, leaves security teams unprepared to protect the organization against cyber threats.

46% of organizations fear that they will lose market relevance if they do not pursue digital innovation.[1]

Organizations are spending an average of $27 million annually on digital innovation.[2]

80% of IT decision-makers say that digital innovation increases cyber risk.[3]

Introduction

DI initiatives provide organizations with a number of benefits but also have their costs in terms of infrastructure and security. New devices deployed as part of DI initiatives increase the complexity of network environments. This increased complexity creates new security challenges.

New Devices Introduce New Threats

DI initiatives often include the deployment of new devices and work locations. However, these additions to the corporate WAN expand the organization's attack surface:

- **IoT devices are insecure.** IoT devices rarely receive patches and use insecure protocols and default passwords. The Mirai botnet compromised hundreds of thousands of devices by logging in with a list of 61 common username and password combinations.[4]
- **Mobile devices bypass security.** Mobile devices commonly hop between internal and external networks, potentially carrying malware behind the corporate firewall. Additionally, "always-on" mobile devices increase employees' susceptibility to phishing attacks.
- **Cloud computing is foreign territory.** Nearly three-quarters of cybersecurity professionals have trouble understanding the cloud shared responsibility model,[5] which is a foundational concept of cloud security. This lack of understanding puts the organization at risk.
- **Branch networks expand security requirements.** Each new location has devices that must be secured. Additionally, organizations increasingly rely upon latency-sensitive Software-as-a-Service (SaaS) applications, and routing all traffic through the headquarters network for security scanning is not always feasible.
- **Telework creates unique challenges.** Organizations are increasingly allowing employees to work remotely. However, telework introduces new challenges, such as a lack of virtual private network (VPN) scalability and increased exposure to malware infections.

Monitoring and securing these new devices and environments often requires specialized security tools. This increases load on security teams expected to monitor and manage these additional solutions and dashboards.

Cyber Threats Grow More Sophisticated

Cyber crime is a profitable profession, and adversaries are becoming more sophisticated. The increased maturity of cyber-threat actors is made evident by the tools and techniques used in their attacks:

- **Most malware is zero-day.** The use of polymorphic malware means that half of malware attacks use zero-day malware.[7] This increases the difficulty of detecting and remediating these attacks.
- **Malicious traffic is encrypted.** A growing percentage of malware command-and-control traffic is encrypted.[8] This can decrease an organization's visibility into ongoing attacks.
- **Targeted attacks are more effective.** Cyber criminals are increasingly using targeted attacks, with 65% of cybercrime groups using spear phishing as their primary attack vector.[9] These more targeted attacks are more likely to trick employees into clicking on a link or opening a malicious attachment.

As the cyber-crime industry evolves, cyber defenders are often unable to keep up. A cybersecurity talent gap with over 4 million unfilled positions has left organizations understaffed.[10] Those that are on the payroll are hobbled by manual security processes that do not scale with the frequency and complexity of cyberattacks.

Point Products Increase Security Complexity

As their digital attack surface grows and cyber threats become more sophisticated, organizations ultimately come under pressure to implement immediate remedies. Many organizations accomplish this by deploying "best-of-breed" standalone cybersecurity solutions to address each potential attack vector as it is discovered.

As a result, the average enterprise has 75 different point security products deployed on its network.[13] The lack of integration between the tools in such multivendor portfolios means security teams must manually collect, aggregate, and analyze data from multiple platforms in order to gain the context required to detect and remediate threats on their networks.

Expert security analysts might save time by collecting only a subset of significant data. But such experts are scarce, leaving less-experienced analysts in a bind: Do they manually collect all sources of data regarding an incident, potentially wasting valuable remediation time? Or do they risk overlooking a piece of data that is crucial to understanding and remediating an incident? Even experts will soon be overwhelmed, if they are not already, by the sheer quantity of alert data generated by proliferating security products and triggered by the increasing attack volume.

New Regulations Strain Security Resources

Data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), are designed to protect the privacy of their constituents. However, these regulations place significant strain upon organizations collecting and securing this data:

- **Regulatory compliance is costly.** New laws, such as the GDPR, have stringent security requirements, which are expensive to implement. One-third of enterprises spend over $1 million on achieving compliance with the GDPR alone.[15]
- **Data subjects have new rights.** Data subjects may request access to, modification of, or deletion of their data under new privacy laws. If done manually, "the average costs of these workflows are roughly $1,400 USD."[16]
- **The compliance landscape is expanding.** The GDPR is the first of many new data protection regulations. While these laws have the same goals, they often have very different security, process, and reporting requirements. The complexity of maintaining compliance with all applicable regulations is increasing exponentially.

60% of organizations have suffered a serious cybersecurity incident within the past two years. 31% have suffered more than one.[6]

35% of IT leaders have deployed and manage an array of unintegrated point security products.[11]

32% of IT leaders say that a reliance on too many manual processes is one of their top three security issues.[12]

70% of organizations state that existing processes and systems with not scale as new privacy regulations come into effect.[14]

Achieving, maintaining, and demonstrating compliance with these new data protection laws is expensive both financially and in terms of the security team's time and resources. However, noncompliance can be even more costly, with GDPR penalties reaching €20 million or 4% of global revenue, as well as sanctions, such as bans on data processing or public reprimands.[17]

Digital Innovation with an Integrated Security Architecture

DI initiatives create new security challenges as expanding attack surfaces and an evolving cyber-threat landscape create new threats. While best-in-breed security products are necessary for security, nonintegrated point products increase security complexity. Achieving scalable, effective security requires tight integration, combined with broad visibility and automation, across an organization's security architecture.

[1] Joe McKendrick, "Digital Transformation Not Very Transformational, Three In Four Organizations Find," Forbes, September 10, 2019.

[2] Ibid.

[3] "60% of businesses have experienced a serious security breach in the last two years," Help Net Security, May 3, 2019.

[4] Steve Ragan, "Here are the 61 passwords that powered the Mirai IoT botnet," CSO, October 3, 2016.

[5] Ray Lapena, "Survey: 84% of Security Pros Said Their Organizations Struggled to Maintain Security Configurations in the Cloud," Tripwire, August 22, 2019.

[6] "60% of businesses have experienced a serious security breach in the last two years," Help Net Security, May 3, 2019.

[7] Robert Lemos, "Only Half of Malware Caught by Signature AV," Dark Reading, December 11, 2019.

[8] Kevin Townsend, "Rise in Malware Using Encryption Shows Importance of Network Traffic Inspection," SecurityWeek, February 18, 2020.

[9] "Internet Security Threat Report (ISTR) 2019," Symantec, February 2019.

[10] "(ISC)² Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide," (ISC)², November 6, 2019.

[11] "The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, August 18, 2019.

[12] Ibid.

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

[14] "The Age of Privacy: The Cost of Continuous Compliance," DataGrail, May 2019.

[15] Ibid.

[16] "Gartner Says Over 40% of Privacy Compliance Technology Will Rely on Artificial Intelligence in the Next Three Years," Gartner, February 25, 2020.

[17] GDPR website, accessed April 23, 2020.

May 12, 2020 8:35 AM

592582-0-0-EN

v