FORTINET

How to Boost Digital Innovation with Fully Integrated Security

Embracing Zero Trust, AI, and Security Automation to Drive Better Outcomes

Table of Contents

Executive Overview

Digital innovation (DI) efforts, which often include investment in new technologies, increase the complexity of enterprise security environments. Addressing this complexity and securing the enterprise against next-generation cyber threats calls for a new and more effectively integrated approach to security.

This approach must include zero-trust principles to mitigate the risk of malicious or vulnerable devices and users. It also must include cloud-native security solutions for multiple provider environments. Implemented correctly, it mandates access to real-time threat intelligence to detect and respond to accelerating and sophisticated cyberattacks. And it gives lean security teams an integrated security platform to monitor and manage all these solutions, enabling them to scale to meet the organization's security needs.

Introduction

DI initiatives are transforming enterprise networks. As part of these initiatives, organizations commonly deploy new solutions and operating environments, such as Internet-of-Things (IoT) devices, cloud-based data storage and applications, mobile devices, and new branch locations. Many of these new devices have unique vulnerabilities, such as the use of default manufacturer credentials in IoT devices and cloud deployments' use of infrastructure outside of the organization's control.

In all organizations, devices are moving outside of the traditional network perimeter, creating new security complexities and risks. For example, a business continuity scenario necessitates a more remote workforce. At the same time, the cyber-threat landscape is evolving, with cyber criminals deploying new tools and techniques to perform their attacks. Addressing these new risks and attack vectors requires new solutions.

78%

of security teams are planning to deploy zero-trust network access.[1]

Zero-trust Security Reduces Organizational Risk

With “trusted” devices deployed outside an organization’s network perimeter and “untrusted” ones often roaming freely inside it, a legacy, perimeter-based security model is no longer applicable or effective. Best practices now dictate a zero-trust security model, under which no user or device is trusted by default. Instead, access to resources is granted or denied based upon the user’s identity. Permissions are assigned to them based upon current job duties and responsibilities.

Implementing and enforcing a zero-trust security model requires strong network segmentation and access control. The organization’s security architecture should be able to automatically identify devices connecting to the network, securely authenticate the user, and provide or deny access to resources based upon the permissions associated with the user’s account. A strongly enforced zero-trust security policy also requires internal network segmentation, which limits lateral movement of attackers and malware and decreases the probability and impact of a data breach.

“72% of the respondents [in a Gartner survey] found that security was their topmost concern when it comes to their WAN.”[2]

Enterprise Growth Requires Network and Security Integration

The deployment of new devices off-premises and the creation of branch locations further expand the network perimeter. Security must expand with it. Regardless of where they are deployed, sanctioned devices and users require a reliable and efficient means of securely connecting to the corporate network.

To avoid the latency and throughput issues associated with routing all traffic through their corporate data center, organizations are turning to software-defined wide-area networking (SD-WAN), placing SD-WAN capabilities at the edges of every remote location. To enable enterprise-grade secure SD-WAN, however, requires next-generation firewall capabilities at every site.

The most efficient and effective way to do this is to integrate networking and security functionality into a single appliance at the network edge. In order for organizations to take full advantage of such an integrated solution, the security and SD-WAN hardware must be designed and optimized to work together.

This provides a strong foundation for extending integrated security further into the branch network by deploying SD-Branch solutions. Secure SD-Branch enables an organization to implement centrally managed user and device authentication and access control.

“Through 2025, 99% of cloud security failures will be the customer’s fault.”[3]

Cloud Migration Requires Cloud-focused Security

Over 94% of organizations have adopted cloud computing,[4] and 84% of them use a multi-cloud deployment. Cloud deployments have unique security requirements, but managing cloud security with custom solutions provided by an organization's cloud service provider is complex and makes it difficult to maintain consistent security controls across the corporate WAN.

Most significant risks in cloud deployments are caused by security misconfigurations, so a security configuration management solution is essential for cloud security. Additionally, cloud environments should have automated monitoring, alerting, and response to enable quick responses to threats taking advantage of these security misconfigurations.

Cloud deployments are located outside the network perimeter and accessible from the public internet, so solutions should be in place to protect them from unauthorized access. Cloud-based applications, such as webmail and web servers, require cloud-native security solutions to provide security without incurring additional network latency.

Top-tier CISOs are 35% more likely to take a proactive approach to addressing cyber risk, which requires automation of threat detection and response.[5]

AI-driven Security Enables Real-time Response

Cyber criminals are increasingly using automated and targeted attacks. These short-duration campaigns give cyber defenders a limited window to detect them and respond. In order to effectively protect the organization against the latest, fast-moving malware variants, security teams must have real-time access to the most recent threat intelligence.

The strategic use of artificial intelligence (AI) is essential to rapid detection, prevention, and response in sprawling enterprise environments. A well-trained machine-learning (ML) classifier is capable of differentiating true threats from false positives, enabling security teams to focus their investigation and remediation efforts on real attacks.

These classifiers can be integrated into a wide range of security solutions. Solutions deployed in-line can automatically detect threats based on behavioral anomalies and respond using predefined playbooks. ML can also be used to aid data collection and analytics, providing threat hunters and security operations center (SOC) analysts with the information required to rapidly detect and respond to advanced and quick-moving attacks.

35%

of IT leaders rely upon nonintegrated security architectures.[6]

Security Integration Requires an Open Security Ecosystem

To manage the growing array of devices on their networks and the cyber threats associated with them, many organizations deploy a range of unintegrated ("point") security products that are difficult to monitor or manage. This increases the complexity of securing network environments.

Organizations should not have to sacrifice security for operational efficiency. The solution is a best-of-breed security platform capable of integrating with a wide range of third-party vendor solutions via application programming interfaces (APIs), connectors, and DevOps automation tools and scripts.

An open API architecture enables communication and synchronization between different devices. Custom-built connectors provide a higher level of integration and interoperability, allowing real-time communications and automatic updates across the ecosystem. A library of DevOps tools and scripts enables rapid, customizable deployment and management, scaling the capabilities of lean security teams.

32% of IT leaders say that a reliance on "too many manual processes" is a leading security challenge.[7]

Complex Networks Require Broad, Integrated, and Automated Security

As networks grow more complex and heterogeneous, organizations require a broad, integrated, and automated security platform to simplify and optimize incident detection, prevention, and response. This enables visibility across the entire digital attack surface and the ability to reduce security complexity and speed operations and incident response.

[1] "Zero Trust Adoption Report," Cybersecurity Insiders, February 4, 2020.

[2] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[3] Kasey Panetta, "Is the Cloud Secure?" Gartner, October 10, 2019.

[4] "2019 State of the Cloud Report," Flexera and Rightscale, February 27, 2019.

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

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

[7] Ibid.

www.fortinet.com

623095-0-0-EN

May 22, 2020 12:14 AM

ebook-digital-innovation