FORTINET

WHITE PAPER

Fortinet Security Fabric Enables Digital Innovation

Broad, Integrated, and Automated

Executive Summary

Organizations are rapidly adopting digital innovation (DI) initiatives to accelerate their businesses, reduce costs, improve efficiency, and provide better customer experiences. Common initiatives involve moving applications and workflows to the cloud, deploying Internet-of-Things (IoT) devices on the corporate network, and expanding the organization's footprint to new branch locations.

With this evolving infrastructure also come security risks. Organizations must cope with growing attack surfaces, advanced threats, increased infrastructure complexity, and an expanding regulatory landscape. To accomplish their desired DI outcomes while effectively managing risks and minimizing complexities, organizations need to adopt a cybersecurity platform that provides visibility across their environment and a means to manage both security and network operations easily.

The Fortinet Security Fabric solves these challenges with broad, integrated, and automated solutions that enable security-driven networking, zero-trust network access, dynamic cloud security, and artificial intelligence (AI)-driven security operations. Fortinet offerings are enhanced with an ecosystem of seamless integrated third-party products that minimize the gaps in enterprise security architectures, while maximizing security return on investment (ROI).

84% of security executives believe the risk of cyberattacks will increase[1]

77% of security professionals state that their organization has moved applications or infrastructure to the cloud despite known security concerns.[3]

Digital Innovation Is Transforming All Industries

Across economic sectors worldwide, DI is seen as an imperative to business growth and improved customer experience. CIOs are generally positive regarding their DI initiatives, with 61% stating that they have significant cloud, IoT, and mobile operations already in place.[2]

From the perspective of cloud service provider IT and cybersecurity leaders, DI translates into a variety of changes to their network environments. Users are increasingly mobile, and they are accessing the network from locations and endpoints that are not always under corporate IT control. They are also connecting directly to public clouds to use key business applications, such as Office 365. Outnumbering the human-controlled endpoints are IoT devices, which are widely distributed, often in remote and unsupervised locations. Finally, cloud service provider business footprints are diffusing into numerous and far-flung branches, most of which connect directly to cloud and cellular services, bypassing corporate data centers.

All these changes render obsolete the concept of a defensible network perimeter, requiring cloud service providers to adopt a new multilayer defense-in-depth strategy.

Migration of applications and workloads to the cloud

Almost every business has started to move some workloads and applications to the cloud—or at least plans to do so. These decisions are often driven by the desire to reduce costs and to improve operational efficiency and scalability by taking advantage of the flexibility that the cloud provides.

Cloud service providers offer a wide range of possible deployment models. Businesses can take advantage of Software-as-a-Service (SaaS) applications and services such as Salesforce or Box. Alternatively, applications designed and deployed in on-premises environments can be lifted to Infrastructure-as-a-Service (IaaS) or Platform-as-a-Service (PaaS) deployments such as Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, Oracle Cloud Infrastructure, and IBM Cloud.

Wary of cloud service provider lock-in and aiming to deploy each application and workload in the cloud for which it is best suited, many organizations have adopted a multi-cloud infrastructure. The downside of such freedom of choice is the need to learn the idiosyncrasies of each cloud environment. In addition, they must use different tools to manage the environment and its security provisions, which obfuscates visibility and necessitates the use of multiple management consoles for policy management, reporting, and more.

Profusion of endpoints across multiple environments

Endpoints are arguably the most vulnerable nodes in the cloud service provider's network. The larger providers have thousands of employees, each using multiple work and personal devices to access network resources. Ensuring cyber hygiene and up-to-date endpoint security on all these devices is a formidable task. Even more daunting is the proliferation of IoT devices. By the end of 2019, the number of active devices exceeded 26.66 billion, and, during 2020, experts estimate that this number will reach 31 billion.[5]

IoT devices are present in numerous business contexts. They provide personalized experiences to retail and hospitality customers, track inventory in manufacturing and logistics, and monitor devices on factory floors or in power plants.

Often ruggedized and power-efficient, IoT devices focus on performance, often at the expense of security features and secure communication protocols. And unlike most network-attached devices, IoT equipment is commonly deployed in remote locations, out of doors, or in unstaffed or infrequently staffed facilities (such as power stations). From these insecure locations, the equipment frequently transmits critical, sensitive data to on-premises data centers and to cloud services.

Expanded business presence across distributed markets and geographies

As companies expand their global footprint by opening new facilities, branch offices, and other satellite locations, they experience increasing wide-area network (WAN) bandwidth constraints. Although SaaS applications, video, and Voice over IP (VoIP) boost productivity and enable new services, they also contribute to an exponential growth in WAN traffic volume.

Highly reliable multiprotocol label switching (MPLS) has been the WAN connectivity technology of choice for many years. However, with MPLS it is difficult to optimize WAN bandwidth use and to vary quality-of-service levels as needed for different applications. As a result, branch expansion and service enhancements can quickly lead to exploding WAN costs.

Consequently, organizations are turning to software-defined WAN (SD-WAN), which makes efficient use of MPLS, internet connections, and even telecommunications links. Plus, SD-WAN dynamically routes each kind of traffic over the optimal link.

Four Considerations for Security Architecture Design

As organizations proceed enthusiastically with DI initiatives, the implications for network security are often overlooked or minimized. In fact, almost 80% of organizations are adding new digital innovations faster than they can secure them against cyber threats.[9]

IT leaders face four key challenges in designing secure architectures for their digitally innovating businesses:

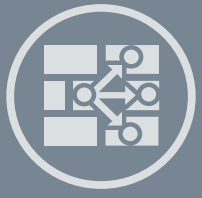
Expanding attack surface

Sensitive data can potentially reside anywhere—and it can travel over numerous connections outside enterprise control. Applications in the cloud are exposed to the

Cloud environments are dynamic: 74% of companies have moved an application to the cloud and then brought it back on-premises.[4]

84% of enterprises have a multi-cloud strategy. 81% point to security as a major cloud challenge.[6]

From 2017 to 2019, there was a 73% increase in the number of organizations experiencing data breaches due to unsecured IoT devices or applications.[7]



SD-WAN provides better performance and security at a lower cost than MPLS.[8]

internet so that every new cloud instance creates a new facet of the enterprise attack surface. IoT devices extend the attack surface to remote, unstaffed locations. In these dark parts of the attack surface, intrusions can fester unnoticed for weeks and months, wreaking havoc on the rest of the enterprise. Mobile devices and user-owned endpoints bring unpredictability to the attack surface, as users roam between corporate locations, through public spaces, and across international borders. In fact, extensive cloud migration, extensive use of mobile platforms, and extensive use of IoT devices are factors amplifying the per-record cost of a data breach by hundreds of thousands of dollars.[10]

This expanded, dynamic attack surface dissolves the once well-defined network perimeter and the security protections associated with it. It is much easier for attackers to infiltrate the network, and once inside, they often find few obstacles to moving freely and undetected to their targets. Therefore, security in DI enterprises must be multilayered—with controls on every network segment—based on the assumption that the perimeter will be breached sooner or later. And access to network resources must be based on least privilege and continuously verified trust.

Advanced threat landscape

The cyber-threat landscape is rapidly growing as bad actors attempt to circumvent and defeat traditional cybersecurity defenses. Up to 40% of new malware detected on any given day is zero day or previously unknown.[15] Whether this is driven by increased use of polymorphic malware or the availability of malware toolkits, the growth of zero-day malware makes traditional, signature-based malware detection algorithms less effective. In addition, bad actors continue to utilize social engineering by exploiting static trust methods used in traditional security approaches. Studies reveal that 85% of organizations experienced phishing or social engineering attacks this past year.[16]

As cyber threats become more sophisticated, data incidents and breaches are more difficult to detect and remediate. Between 2018 and 2019, the time to identify and contain a data breach grew from 266 to 279 days.[17] Beyond the ability to detect and prevent an attempted attack, organizations must also be capable of rapidly identifying and remediating a successful attack. Over 88% of organizations have reported experiencing at least one incident in the last year, demonstrating that all organizations are at risk of an attack and that cyber resiliency is critical.[18]

Greater ecosystem complexity

According to almost half of CIOs, increased complexity is the biggest challenge of an expanding attack surface.[19] This increased complexity is due to the fact that many organizations rely upon an array of nonintegrated point products for security. In fact, the average enterprise uses upwards of 75 distinct security solutions.[20]

This lack of security integration means that these organizations are unable to take advantage of automation in their security deployment. In fact, 30% of CIOs point to the number of manual processes as a top security issue in their organization.[21] Without security automation, CIOs require more skilled cybersecurity professionals to monitor and secure their network.

However, many organizations are unable to acquire the cybersecurity talent that they require. Estimates indicate that over 4 million cybersecurity positions are currently left unfilled, and the number is steadily growing.[22] This lack of access to necessary talent is putting organizations at risk, with 67% of CIOs saying that the cybersecurity skills shortage inhibits their ability to keep up with the pace of change.[23]

Attackers understand these challenges well, and use it to their advantage.

61% of CISOs state that they have significant cloud, IoT, and mobile operations already in place.[11]

Up to 40% of new malware detected on any given day is zero day or previously unknown.[12]

DI initiatives mean that enterprise security teams must deploy protections for 17 different types of endpoints.[13]

One-third of enterprises suffered a breach of business-critical data in the last year, which could lead to regulatory penalties.[14]

Increasing regulatory demands

The European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are two of the most well-known of the data protection regulations. However, they are far from the only ones. Every U.S. state currently has a data breach notification law, and many of them are enacting additional consumer privacy protections. Driven by political and social pressure, regulations are expected to expand in coming years, and penalties for noncompliance are becoming larger and more common.

Organizations must also comply with industry standards, and many struggle to do so. Indeed, less than 37% of organizations pass their interim Payment Card Industry Data Security Standard (PCI DSS) compliance audit.[24] As PCI DSS is superseded by the PCI Software Security Framework (PCI SSF), these organizations are likely to face even greater obstacles to remain compliant.

Fortinet Security Fabric

- Broad
- Automated
- Integrated

FORTINET Fabric-Ready

The need to achieve and maintain regulatory compliance has significant impacts on an organization's ability to achieve security transformation objectives. For example, of the 71% of organizations that have moved cloud-based applications back to on-premises data centers, 21% did so to maintain regulatory compliance.[25]

The Fortinet Security Fabric

The Fortinet Security Fabric addresses the security challenges mentioned above by providing broad visibility and control of an organization's entire digital attack surface to minimize risk, an integrated solution that reduces the complexity of supporting multiple point products, and automated workflow to increase the speed of operation.

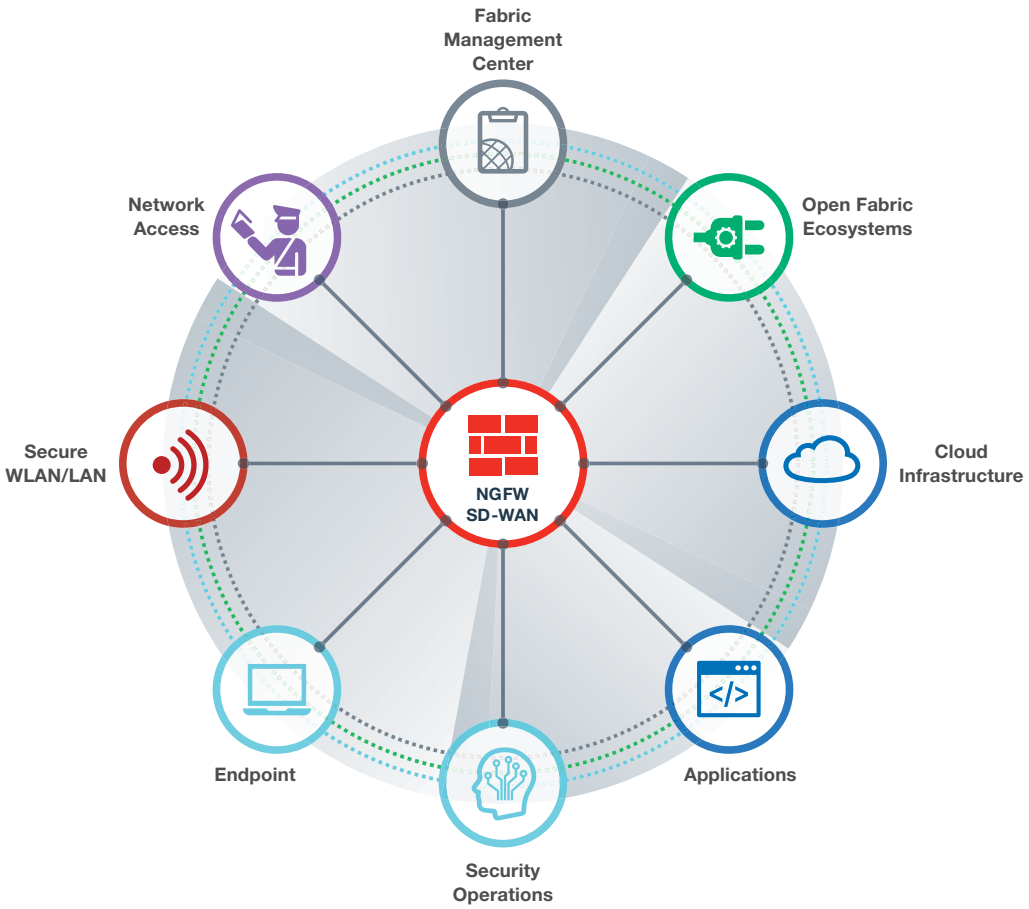


Figure 1: The Fortinet Security Fabric enables multiple security technologies to work seamlessly together, across all environments and supported by a single source of threat intelligence, under a single console. This eliminates security gaps in the network and hastens responses to attacks and breaches.

Broad attack surface visibility

With organizational perimeters expanding as a result of DI transformations, the attack surface also expands. The Fortinet Security Fabric addresses the challenge of an expanding attack surface by providing an organization with end-to-end security and visibility across their network infrastructure. With the broadest range of high-performance, security-driven networking solutions for data centers, branch offices and small business, and all major cloud providers, the Fortinet Security Fabric flexes to protect every segment of the network.

All components are configured, managed, and monitored from a single centralized management system. In addition to eliminating the silos associated with point product security infrastructures, the single interface for all security components reduces the training burden on lean staffs. The management system also facilitates zero-touch deployment of remote components, saving truck rolls and further reducing operating costs.

Integrated security architecture

With all components driven by the same FortiOS network operating system, the Fortinet Security Fabric enables consistent configuration and policy management and effortless, real-time communication across the security infrastructure. This minimizes threat detection and mitigation times, reduces security risks resulting from configuration errors and manual data compilation, and facilitates timely and accurate compliance audit response.

In addition to integrating Fortinet products and solutions, the Security Fabric includes prebuilt application programming interface (API) connections for more than 70 Fabric-Ready Partners that ensure deep integration across all of the Security Fabric elements.

For security products that are not part of the Fabric-Ready Partner ecosystem, representational state transfer (REST) APIs and development operations (DevOps) scripts make it easy and fast for customers to add them to the Security Fabric.

Automated operations, orchestration, and response

In addition to seamless integration, the Fortinet Security Fabric is leading the industry in applying machine-learning (ML) technologies to keep up with the rapidly evolving cyber-threat landscape. The Fortinet Security Fabric includes advanced security orchestration, automation, and response (SOAR) capabilities, as well as proactive threat detection, threat correlation, intelligence-sharing alerts, and threat research and analysis.

Expediting incident response activities also requires ensuring that security staff is not distracted by other concerns, such as collecting data for and generating reports for regulatory compliance or the C-suite. Here, the Fortinet Security Fabric offers automated log aggregation, data correlation, and generation of reports using built-in templates.

Almost half of CISOs point to security integration and improved analytics as a major priority for their cybersecurity technology strategy.[26]

FortiGate NGFWs provide the highest price-performance ratio in third-party evaluations while scanning encrypted traffic. They achieve 5.7 Gbps SSL performance while blocking 100% of evasions.[27]

Driving down breach detection and response time can result in a 25% reduction in the overall costs of a data breach. [28]

Security Fabric Solutions

The Fortinet Security Fabric delivers solutions in five key areas: zero-trust access, security-driven networking, dynamic cloud security, AI-driven security operations, and the alliance ecosystem. Each of these includes best-in-class, award-winning solutions that have been evaluated and recommended by leading third-party tests, such as NSS Labs, and recognized by leading analysts, such as Gartner.[29,30]

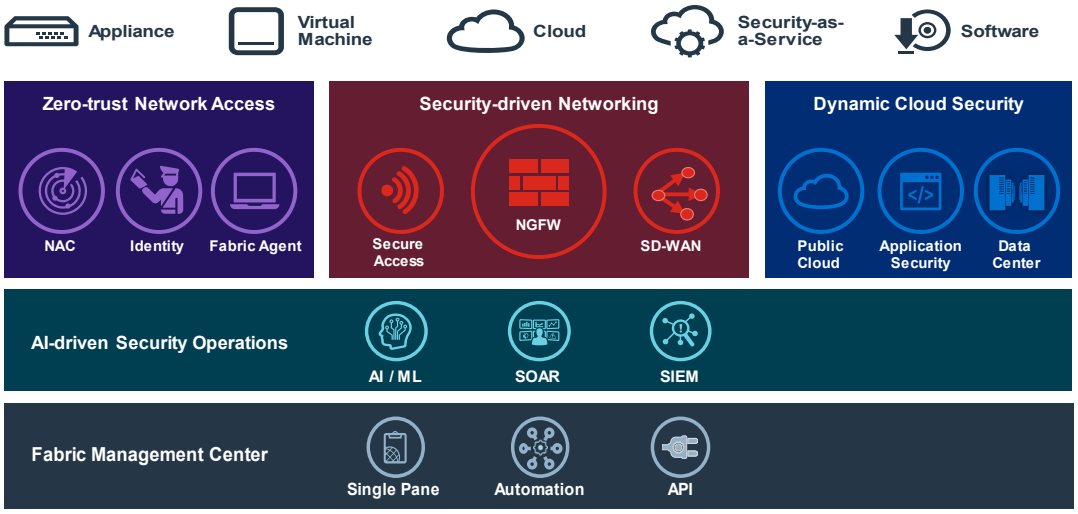


Figure 2: Conceptual framework for the Fortinet Security Fabric.

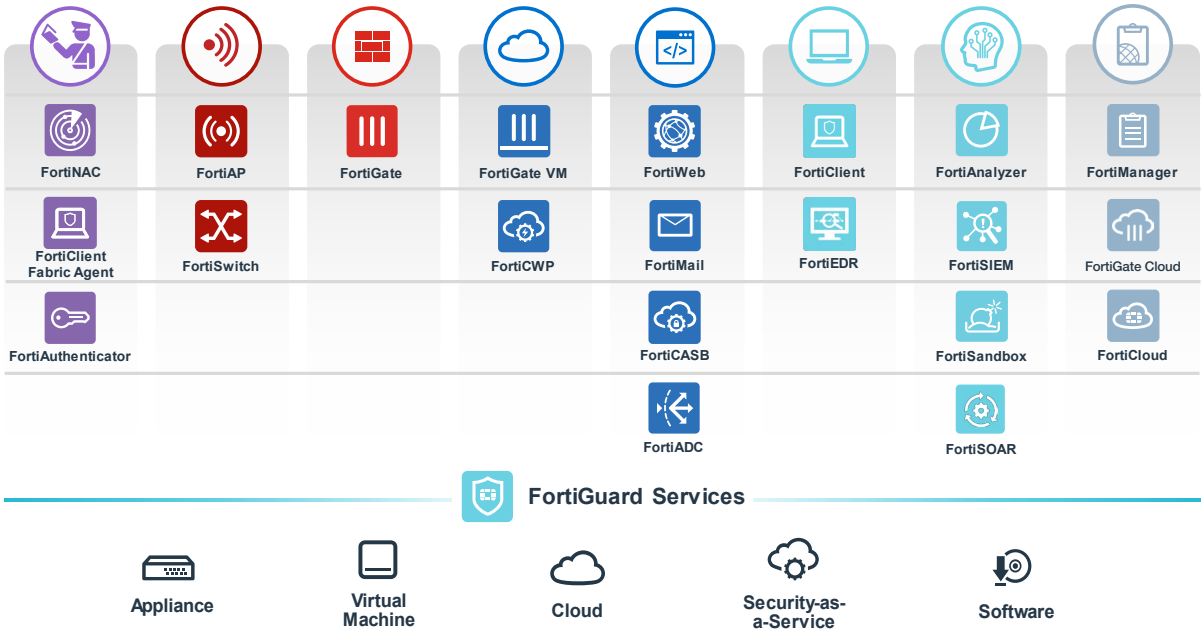


Figure 3: Key offerings in each of the Security Fabric solution areas.

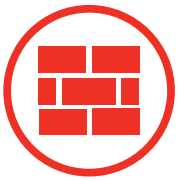
Zero-trust network access

As cyber threats become more sophisticated, a perimeter-focused security model is no longer sufficient. Credential theft and malware enable external threats to gain access to legitimate accounts within the corporate network. The Fortinet Security Fabric enables businesses to implement a zero-trust network access policy throughout their entire corporate WAN.

The first step in enforcing zero-trust access on a network is discovery of the devices connected to the network. **FortiNAC** network access control (NAC) solutions provide automated detection of devices connecting to the corporate WAN. Connected devices are subjected to security scanning, and an organization's security team can define device-specific policies to enforce. Once a device has been approved to access the network, it is monitored continuously to detect any behavioral anomalies that could indicate an infection or use by a malicious actor.

Able to identify the devices connected to its network, organizations can then implement zero-trust access to determine who is using these devices. FortiAuthenticator user identity management server offers built-in authentication and role-based access control (RBAC), allowing organizations to implement least privilege and separation of duties on their networks. FortiToken two-factor authentication tokens strengthen user authentication by enabling multi-factor authentication. This ensures that compromised user credentials do not provide an attacker with authenticated access to a user's account.

When devices are connected to the corporate network, device monitoring and policy enforcement can be performed over the network. However, enterprise use of mobile devices is growing rapidly, so enterprise devices may be used offline or on other networks. Installation of **FortiClient** Fabric Agent provides visibility into endpoints and implements dynamic access control both on and off of the corporate network.



Security-driven networking

As enterprise networks and attack surfaces expand with DI, the need to secure these networks grows. Security-driven networking tightly integrates an organization's network infrastructure and security architecture, enabling the network to scale and change without compromising security. Such integration reduces complexity by minimizing the number of disparate point products. It also makes it easy to leverage performance improvements, since networking and security appliances are optimized to work together.

Security-driven networking comes to the forefront in **FortiGate** next-generation firewalls (NGFWs); they are an organization's first line of defense against advanced threats. They are much more than firewalls, however. Because almost one-third of data breaches involve phishing attacks[31]—which rely upon malicious links or attachments to infect endpoints or steal user credentials—FortiGate NGFWs include a secure web gateway (SWG), which identifies and blocks attempted connections to malicious or suspicious URLs.

FortiGate NGFWs also perform secure sockets layer (SSL)/transport layer security (TLS) packet decryption and inspection. This is a critical requirement today, with an estimated 75% of enterprise network traffic protected with SSL/TLS, and about 82% of malicious traffic using encryption.[32,33] in response, **FortiGate NGFWs** use purpose-built security processors (SPUs) to minimize the performance impact of SSL/TLS traffic inspection. Integration of high-performance encrypted traffic inspection into an organization's NGFW also enables the business to avoid the overhead associated with acquiring and deploying standalone appliances throughout their network infrastructure.

If threats go undetected at the network perimeter, it is essential to prevent them from moving laterally throughout the network. Intent-based segmentation allows organizations to painlessly accomplish this by enabling segmentation of the network based upon business needs. Suspicious or malicious internal connections are blocked by default, and if a zero-day threat is identified after infection, threat intelligence is communicated through the Security Fabric to ensure that no secondary infections occur.

For this to work, an organization requires security integration across their entire enterprise network, including branch locations. **Fortinet Secure SD-WAN** provides optimized network performance and security integration for branch locations. FortiGate NGFWs integrated into SD-WAN appliances perform traffic inspection at each branch location. This improves network performance by enabling direct-to-internet connectivity for SaaS applications and services and enables WAN cost reductions.

Within a branch location, **Fortinet Secure SD-Branch** enables extension of an organization's visibility and centralized security management down to the switching layer. Fortinet Secure SD-Branch consists of FortiNAC solutions, FortiSwitch secured access switches, and **FortiAP** wireless access points monitored and controlled from a FortiGate NGFW. By integrating security across the corporate WANs, businesses simplify operations by eliminating redundancy and enable rapid, coordinated response to advanced threats.

Dynamic cloud security

As organizations transition to the cloud, expanding the organization's security deployment to cloud-based resources is essential. The Fortinet Security Fabric integrates a range of cloud-native solutions to provide security for any application and deployment environment.

Fortinet security solutions offer network security, visibility, and control in both public and private cloud deployments. FortiGate NGFWs are available in a VM form factor. This allows them to provide cloud-native security automation, VPN connectivity, network segmentation, intrusion prevention, and an SWG.

Beyond protecting against malicious content, organizations also must ensure that their cloud deployments are properly configured. Security misconfigurations are a major issue in the public cloud, with 99% of issues going unreported.[34] **FortiCWP** cloud security analytics provides visibility and control in public cloud infrastructure, including monitoring of configurations, data security, and compliance as well as integrated threat management.

Once the cloud infrastructure itself is secured, it is necessary to protect the applications running on it. A common use of public cloud deployments is hosting web applications and web APIs. **FortiWeb** provides these with cloud-native security. FortiWeb web application firewalls (WAFs) protect web applications from both known and unknown threats using a combination of signature detection, ML, and AI. In addition, as most web applications use APIs to link to web services and integrate with other tools, it is critical to secure those web APIs using schema validation and OpenAPI security to protect against potentially malicious bot activities such as scraping and analytics.

Organizations are also increasingly moving to cloud-based email solutions like Google G Suite and Microsoft Office 365. Since phishing attacks are a leading cause of security incidents and data breaches, securing cloud-based email is essential. Available as physical and virtual appliances or as a hosted service, **FortiMail** messaging security solutions protect both on-premises and cloud-based email deployments, including blocking traditional and advanced email threats and providing backup functionality to avoid the loss of sensitive information.

Beyond web applications and email, many organizations are reliant upon SaaS applications such as Google G Suite, Box, Microsoft Office 365, Dropbox, and Salesforce. **FortiCASB** cloud access security brokers (CASBs) manage the risks of security misconfiguration, provide centralized visibility and administrative control, deliver data security in SaaS applications, and ensure that SaaS application configurations maintain regulatory compliance.

AI-driven security operations

The increased volume and sophistication of malicious attacks render traditional cybersecurity solutions insufficient. Signature-based malware detection solutions are capable of detecting only half of malware attacks.[35] The use of AI and ML capabilities is essential to detecting and preventing these attacks.

FortiGuard AI enables organizations to keep ahead of cyber criminals. FortiGuard Labs collects threat data from millions of sensors worldwide and partners with over 200 global organizations. Using 5 billion-plus nodes, FortiGuard AI identifies unique features for both known and unknown threats. The volumes handled by FortiGuard Labs are immense: The team processes over 100 billion web queries every day and blocks over 3,600 malicious URL requests each second.

As threats grow in sophistication, 100% prevention is no longer possible. Advanced threat detection capabilities are essential to helping organizations avoid breaches. AI and ML capabilities integrated into **FortiDeceptor, FortiSandbox,** and **FortiInsight** help organizations to identify unknown adversaries and malware and to uncover and respond to insider threats.

As cyber threats accelerate, organizations must take advantage of strategic automation to more quickly contain and remediate threats. Using **FortiSIEM** and **FortiAnalyzer,** an organization can achieve global visibility of their network infrastructure and access AI-driven security analytics. Based on the collected data, security analysts can determine the nature and severity of threats, with support from **FortiAI** virtual analyst. But it does not stop at threat detection and prevention; **FortiSOAR** employs orchestration and automation to remediate threat intrusions that help overstretched security operations center (SOC) teams to scale and focus on threat hunting and other mission-critical tasks.

Endpoints also require AI-driven resources throughout their incident response process. **FortiEDR** endpoint detection and response (EDR) and FortiClient deliver advanced endpoint protection that includes vulnerability scanning, patching, and virtual patching and exploit prevention in both online and air-gapped environments. Additionally, if an endpoint becomes infected, FortiEDR threat detection and post-infection protection prevents malware from communicating with command and control servers or moving laterally through the network. Finally, FortiEDR offers risk-based threat response and online remediation with support for automated remediation recipes.

Fabric management center

The Fortinet Security Fabric is designed to simplify management of an organization's entire security architecture. The Fabric accomplishes this by integrating all deployed security point products, enabling them to be centrally monitored and managed.

The **FortiManager** centralized management platform and **FortiAnalyzer** centralized logging and reporting combine to provide single-pane-of-glass visibility and management of an organization's entire network infrastructure. This includes single console management, analytics, and workflow automation.

These capabilities are supported by a number of API-based integrations with Fortinet Fabric-Ready Partners. Twelve Fabric Connectors provide deep integration with third-party solutions, and API-based integration is available for over 135 Fabric-Ready Partners. For non-partner solutions, the Fortinet Security Fabric includes a REST API and DevOps scripts to enable easy integration.

As many organizations are moving operations to the cloud, a single-point-of-access and single-sign-on (SSO) solution is needed to reduce the complexity of multi-cloud deployments. **FortiCloud** provides SSO and portals to 15 Fortinet SaaS and Metal-as-a-Service (MaaS) solutions as well as a **FortiCare** services portal. With support for all major public cloud providers, the Fortinet Security Fabric simplifies any multi-cloud deployment.

By combining FortiManager, FortiAnalyzer, and FortiCloud, an organization can completely integrate their on-premises and cloud deployments. This integration enables the use of automation and orchestration to simplify security management. Additionally, by leveraging Fabric Connectors and APIs, security teams can receive real-time network health information, automate network log management, and simplify compliance reporting, all from a single pane of glass.

Manage the Risks, Pursue the Opportunities

DI enables organizations to achieve new levels of efficiency and cost savings for itself and improved experiences for its customers. However, DI initiatives also expand and change the organization's attack surface, opening up new attack vectors for cyber threats to exploit.

For organizations leading the charge in DI, acknowledging, accepting, and properly managing risks is of paramount importance. The Fortinet Security Fabric is the foundation for this. It unifies security solutions behind a single pane of glass, makes the growing digital attack surface visible, integrates AI-driven breach prevention, and automates operations, orchestration, and response. In sum, it enables organizations to create new value with DI without compromising security for business agility, performance, and simplicity.

[1] Nick Lansing, "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources," Forbes and Fortinet, 2019.

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

[3] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, 2019.

[4] Ibid.

[5] Gilad David Maayan, "The IoT Rundown For 2020: Stats, Risks, and Solutions," Security Today, January 13, 2020.

[6] "2019 State of the Cloud Report," Flexera, 2019.

[7] Larry Ponemon, "Third-party IoT risk: companies don't know what they don't know," ponemonsullivanreport.com, accessed February 4, 2020.

[8] Nirav Shah, "SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019," Fortinet, September 9, 2019.

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

[10] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

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

[12] According to internal data from FortiGuard Labs.

[13] "6 Obstacles to Effective Endpoint Security: Disaggregation Thwarts Visibility and Management for IT Infrastructure Leaders," Fortinet, September 8, 2019.

[14] According to data from internal Fortinet research.

[15] According to internal data from FortiGuard Labs.

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

[17] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[18] Based off of internal Fortinet research.

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

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

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

[22] ""Strategies for Building and Growing Strong Cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study, 2019," $(ISC)^2$, 2019.

[23] "CIO Survey 2019: A Changing Perspective," Harvey Nash and KPMG, 2019.

[24] "2019 Payment Security Report," Verizon, 2019.

[25] Jeff Wilson, "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, 2019.

[26] "Making Tough Choices: How CISOs Manage Escalating Threats And Limited Resources," Forbes and Fortinet, 2019.

[27] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[28] "2019 Cost of a Data Breach Report," IBM Security and Ponemon Institute, 2019.

[29] "Independent Validation of Fortinet Solutions: NSS Labs Real-World Group Tests," Fortinet, October 14, 2019.

[30] "Gartner Magic Quadrant Reports," Fortinet, accessed January 22, 2020.

[31] "2019 Data Breach Investigations Report," Verizon, 2019.

[32] Alex Samonte, "TLS 1.3: What This Means For You," Fortinet, March 15, 2019.

[33] Robert Lemos, "Attackers Are Messing with Encryption Traffic to Evade Detection," Dark Reading, May 15, 2019.

[34] Charlie Osborne, "99 percent of all misconfigurations in the public cloud go unreported," ZDNet, September 24, 2019.

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

February 13, 2020 1:29 AM

570099-0-0-EN

D:\Fortinet\White Paper\grey white paper\GREY - Update Security Fabric\wp-FA-fortinet-security-fabric-enables-digital-innovation-2132020-129AM