FORTINET

WHITE PAPER

Protecting Communications Service Providers with the Fortinet Security Fabric

Executive Summary

Communications service providers (CSPs) are typically large enterprises, managing distributed network infrastructures that span multiple on-premises and cloud-based data centers, as well as numerous branch office and retail locations. As prime targets for cyber crime, CSPs must close every security gap, while continuing to meet service-level agreements (SLAs) for application performance and customer experience. The Fortinet Security Fabric represents an optimal architecture for CSPs, offering a unique combination of robust protection and high throughput. Its coverage includes a broad, integrated, and automated suite of solutions for the headquarters, branch offices, and retail stores, and for public and private clouds.

$9.21 million

Average annual cost of cyber crime in the communications service provider sector[1]

Complex Networks, Costly Breaches

CSPs face security challenges on multiple fronts. In addition to customer account and call-log data, the vast CSP enterprise networks contain a wealth of other sensitive assets and critical applications. If these are accessed, exfiltrated, or sabotaged, CSPs can incur significant damage to brand reputation and profits. The last available data reveals that the average annual cost of cyber crime in the communication sectors is $9.21 million.[2]

In their retail brick-and-mortar stores, CSPs face threats to the point-of-sale (POS) systems. Not only must they protect their customer data but they must also comply with the Payment Card Industry Data Security Standard (PCI DSS) and upcoming PCI Software Security Framework (SSF) standards. Additionally, CSPs must protect the branch networks themselves, as the employees and customers who access these networks can be both sources and targets of cyberattacks.

Key Communications Service Provider Cybersecurity Challenges

Network service is what customers pay for. Consequently, anything that hampers network performance—including security—can negatively affect a CSP's competitive edge. However, in-store experience matters, too. Because more than half (57%) of customers use mobile apps when in a store,[3] cumbersome Wi-Fi access or slow page loads can be as frustrating as on an ecommerce site, where shopping cart conversion rates drop 7% for every one-second delay in page loading.[4]

Time is also at a premium for CSP security teams. A typical CSP network encompasses various security hardware and software tools and they are deployed at scale. Managing each of these separately—and manually compiling and analyzing disparate security logs—is extremely inefficient. It invariably increases operating expenses (OpEx), both in administrative time and in training on multiple tools. As the network grows, and the supply of skilled security professionals does not keep pace, this point-product approach is unsustainable.

In addition to accumulating inefficiencies, CSPs face the risk of security gaps when managing disaggregated tools. These gaps result from lack of end-to-end security visibility, difficulties in obtaining and sharing real-time threat information throughout the network, and an inability to mount a timely, coordinated response.

As prime targets of data theft, distributed denial-of-service (DDoS), and ransomware attacks, CSPs cannot afford any security lapse. Cyber threats are increasingly driven by artificial intelligence (AI), and they are proliferating at such a rate that it is now impractical to aim for complete breach prevention. The security game has shifted to detection and impact mitigation.

CSPs are also (unintentionally) giving cyber criminals increasing opportunities to attack, as they deploy geofencing sensors, cameras, and kiosks in their retail environments and offer in-store Wi-Fi access. Many CSPs also operate remote offices, which process sensitive user data while onboarding customers and troubleshooting. These branch locations are often less protected than corporate headquarters, making them an easier target for cyber criminals trying to gain access to sensitive data or to stage an attack on the headquarters data center. The migration of corporate applications to the cloud also expands and fragments the CSP's network attack surface. As such, CSPs must now look to multilayered security strategies to protect their networks.

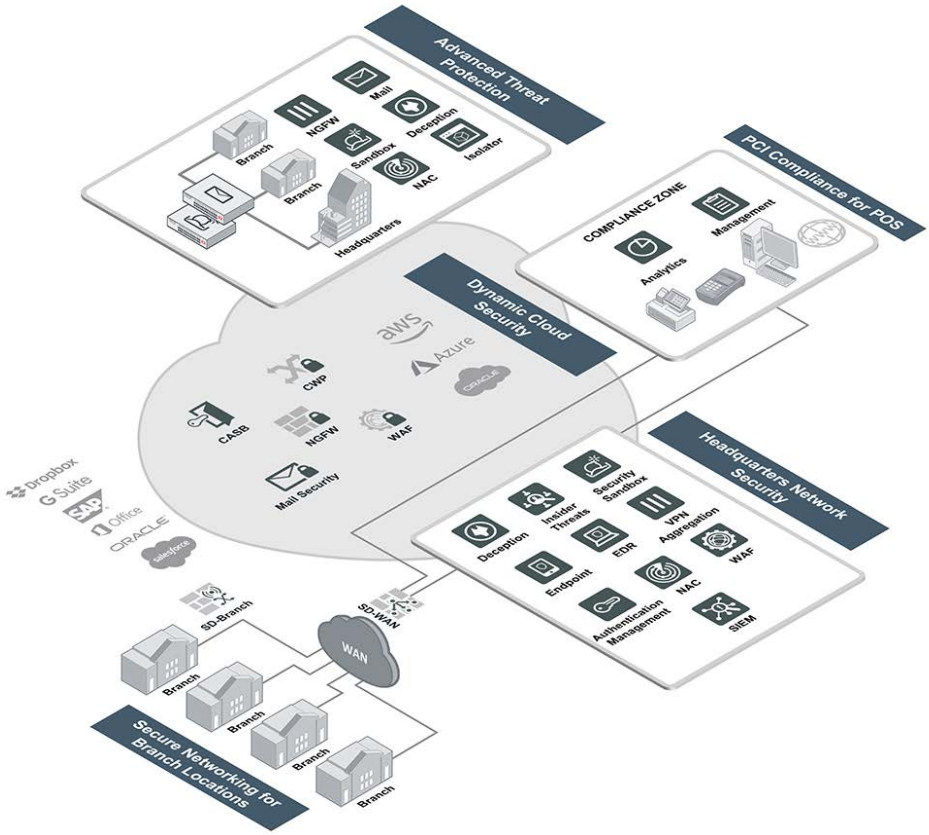

Figure 1. The Fortinet Security Fabric helps CSPs address their key security challenges so they can confidently roll out innovative mobile services and deliver superior customer experiences.

It is not enough, however, to implement robust protection. CSPs must also prove to regulators, customers, and partners that they are doing so. As retailers, CSPs collect payment card and other sensitive data from customers, both at brick-and-mortar retail locations and through online portals. As service providers, they also log call data. This highly private and often sensitive information may be subpoenaed in certain cases by the authorities. All this data is stored and processed across the organization's network, both in on-premises data centers and in private and public clouds. This complex arrangement makes complying with audit and reporting requirements a formidable challenge.

CSP Enterprise Cybersecurity Use Cases

Leveraging best-in-class solutions within the Fortinet Security Fabric, CSPs can address the following cybersecurity use cases:

Headquarters Network Cybersecurity

The headquarters network of a CSP is the heart of the entire operation and contains massive amounts of sensitive information. Payment card and billing information collected from customers flows through and is stored on this network. Customer traffic is routed through and processed at the enterprise data centers, providing a wealth of valuable data to any attacker able to gain access. As a consequence, the enterprise must be capable of protecting all of this data and maintaining compliance with applicable regulations.

However, a CSP's cyber-threat exposure is not limited to data theft. A DDoS attack or ransomware infection could knock critical services offline. In doing so, an attacker who has compromised the enterprise network can exploit and misuse internet-connected monitoring devices on the network.

Key Security Challenges:

- Inefficient security processes can encumber mobile services and retail experience
- Disaggregated point products inhibit visibility, enabling security gaps
- Expanding corporate and retail footprints make the attack surface harder to defend
- Lateral network communications between applications accessed by different players in the ecosystem including employees, suppliers, customers, partners, contractors, etc.
- Acquisition of customer, payment, and call-log data leads to extensive compliance requirements

Compromising the enterprise network is relatively easy with perimeter-based security architectures. Hackers can find their way around even the strongest edge security technologies, and once inside the network, they can move laterally unless impeded by additional layers of threat protection. In the Fortinet Security Fabric, these layers consist of **FortiGate** next-generation firewalls (NGFWs), which provide zero trust-based internal segmentation, enabling least-privilege, role-based, and continuously verified access to resources. FortiGate internal segmentation NGFWs perform all of the Layer 3 through Layer 7 controls, including firewall, intrusion prevention system (IPS), and application control.

Digital innovation drives many CSPs to migrate some workloads and applications to public and private clouds while continuing to run others in existing corporate data centers. Protecting such a heterogeneous network environment requires a fully integrated, comprehensive cybersecurity solution. **FortiManager, FortiSIEM,** and **FortiAnalyzer** enable security teams to achieve centralized visibility and control across their network and easily perform compliance reporting. **FortiClient** and **FortiEDR** (endpoint detection and response) provide integrated, advanced endpoint security solutions for employee workstations and POS systems alike. **FortiWeb** and **FortiNAC** provide website security and automatic identification and vulnerability scanning of Internet-of-Things (IoT) devices connecting to the network, with **FortiAuthenticator** simplifying identity management.

Features That Improve the Efficiency of Securing Distributed CSP Networks:

- Native integration with major cloud providers and 250-plus third-party security solutions
- Centralized visibility, management, and policy enforcement from a single pane of glass
- Out-of-the-box support for compliance management, monitoring, and reporting
- Built-in analytics solutions to increase application availability and save network and security resources

Features That Facilitate Management of PCI DSS and SFF Compliance:

- Out-of-the-box reporting templates for PCI DSS and other major regulations
- Centralized security policy management and enforcement
- Automated device identification for networkwide topology mapping
- Real-time telemetry data from Fortinet products and Fabric-Ready Partner solutions
- Automated threat detection and response, including automation stitching

PCI Compliance for POS

PCI DSS is a major concern for CSPs. With retail outlets scattered across the country, tracking and securing consumer payment card data is complex. Upon the release of the upcoming PCI SSF, these requirements will be more strongly enforced, and the complexity of achieving and maintaining compliance will grow.

Achieving and maintaining compliance requires an integrated and intentional approach to compliance. Otherwise, companies risk compromising their network defense in order to perform actions necessary for demonstrating PCI DSS compliance.

As a company's network of retail locations expands and PCI requirements grow more complex, it becomes increasingly difficult to achieve the networkwide visibility and centralized management necessary for maintaining and demonstrating regulatory compliance. Digital innovation initiatives add to the burden on IT and security teams as new devices are added to the network and the company's digital footprint expands to the cloud. This is further exacerbated with the growth of cloud computing, where organizations are required to appropriately secure and control access to protected data processed and stored on devices outside their network perimeter and not under their complete control.

With the Fortinet Security Fabric, CSPs can achieve the centralized visibility and control needed for PCI DSS/SSF and other areas of compliance. The Security Fabric includes 12 Fabric Connectors and over 135 Fabric APIs (application programming interfaces) for out-of-the-box integration with third-party solutions. An open API ecosystem, collaboration with over 30 threat-sharing organizations, and integration with more than 100 third-party vendor products enable trouble-free integration and centralized management of any security solution.

Secure Networking for Branch Locations

CSPs' branch locations need access to fast, reliable, and scalable network connectivity. Frequently, retail locations must perform troubleshooting and repairs for their customers, which require rapid access to customer data and the ability to perform diagnostic tests that need a stable, reliable network connection.

Deploying this connectivity via traditional multiprotocol label switching (MPLS) lines is an inflexible solution, and turning on new deployments or making changes takes long lead times. In comparison, software-defined wide-area networking (SD-WAN) provides the reliability guarantees of MPLS but operates over any WAN transport including broadband. More importantly, it brings a much higher level of automation, which speeds up deployment and change implementation. By optimizing the usage of multiple transport media, SD-WAN offers faster connection speeds with a lower total cost of ownership (TCO). This improves network performance and decreases loads at the enterprise data center, boosting operational efficiency.

In order to make full use of SD-WAN's capabilities, it is necessary to deploy security at the network edge. Because it replaces the controls that were previously applied by data-center firewalls, the edge security for SD-WAN must be just as robust. With most SD-WAN solutions, this requires additional products, which results in more complicated network administration.

Fortinet Secure SD-WAN, on the other hand, is an all-in-one solution. The built-in NGFW provides security controls for Layer 3 through Layer 7 and industry-leading performance. These dual benefits are made possible by the industry's first purpose-built SD-WAN application-specific integrated circuit (ASIC) chip. The Fortinet Secure SD-WAN appliance also includes an integrated IPS, providing full traffic inspection at the branch location. This enables traffic to be routed directly to its destination, improving network performance, especially of cloud-bound traffic, without sacrificing security.

With **Fortinet SD-Branch**, CSPs can take security a step further, centralizing visibility and management of security infrastructure at branch locations from the internet down to the switching layer. This increases the efficiency of security operations, simplifies security control enforcement and data collection for compliance activities, and improves visibility and security of the enterprise WAN. Fortinet SD-Branch solutions include FortiAP wireless access points, which deliver high-performance, secure network access for business and guest networks; FortiSwitch, which provides secure and simple branch local-area network (LAN) connectivity; and FortiNAC, which, together with FortiGate NGFWs, performs automated identification and access control for all devices connecting to the network. Zero-touch provisioning of all these devices facilitates branch expansion while avoiding truck rolls and IT staff expansion.

With the reliable and secure network connectivity provided by Fortinet Secure SD-WAN, branch locations can also deploy Voice over IP (VoIP) in place of a separate phone service without concerns about bandwidth consumption, availability, or quality of experience. Here, **FortiVoice** offers an easily configured and flexible VoIP solution that can be isolated from other business and public Wi-Fi networks using the switching and access control capabilities built into Fortinet SD-Branch. To ensure connectivity in the event of a network outage, **FortiExtender** offers a 3G/4G/LTE/5G backup solution.

Features That Optimize the Performance of Globally Distributed Branch Networks:

- Over 5,000 signatures for automatic recognition and optimal routing of application traffic
- Malware signature updates from FortiGuard Labs for application databases
- Integrated NGFW, IPS, and application control
- High-throughput inspection of secure sockets layer (SSL) and transport layer security (TLS) traffic
- Integrated web filtering, eliminating the need for a standalone secure web gateway (SWG)
- Scalable, high-throughput overlay virtual private network (VPN) tunnels to ensure encryption of confidential traffic

Advanced Threat Protection Requires a Multilayered Defense, Including Features Such As:

- Identification and protection against both known and unknown threats
- Detection and remediation of internal threats
- Automatic quarantine and analysis of suspicious content within sandboxes
- Leveraging deception techniques to identify internal threats
- AI- and ML-driven real-time threat intelligence
- Continuous threat intelligence and malware signature updates

Advanced Threat Protection

CSPs need to be able to detect and block malware operating on their networks. However, according to analysis performed by **FortiGuard Labs**, 40% of new malware detected each day is zero-day or previously unknown.

Identifying and responding to cyber threats requires access to real-time, proven threat intelligence. Using data derived from analysis of over 10 billion security events per day, **FortiGuard Labs** rapidly collects, analyzes, and classifies threats with an extremely high degree of accuracy. It leverages AI and machine learning (ML) to write malware signatures and publish them across the entire Fortinet Security Fabric in real time. The integration provided by the Fortinet Security Fabric across the organization's network also enables security teams to leverage the latest in security orchestration, automation, and response (SOAR).

The widely distributed networks of CSPs offer many possible avenues for unknown threats to gain access, including public Wi-Fi, mobile devices, and connected IoT devices. Any suspicious content detected by a FortiGate NGFW is forwarded to FortiSandbox for quarantine and inspection—including decryption of secure sockets layer (SSL)/transport layer security (TLS) content—before it reaches the network. Threat intelligence generated by FortiSandbox is then shared with other security elements via the Fortinet Security Fabric. The FortiEDR endpoint detection and response solution provides advanced endpoint protection, offering high availability in a small footprint.

Of course, cyber threats are not limited to external attackers. Using FortiDeceptor, an organization can identify malicious insiders or attackers who have gained access to the network. The user and entity behavior analytics (UEBA) features of FortiInsight help to identify anomalous, noncompliant, or suspicious behavior by endpoints or users that may threaten the business.

Dynamic Cloud Security

Organizations are increasingly embracing cloud services for business-critical data storage and applications, and these resources require robust security. While most cloud service providers offer built-in security settings, they are often incorrectly configured by organizations, leaving sensitive data vulnerable to exfiltration. Achieving centralized visibility and consistent security configuration management is also complex in the cloud, with every cloud vendor offering different built-in security controls and interfaces. Securing the cloud requires centralized visibility across on-premises and cloud deployments and cloud-native security solutions for cloud-based applications.

The first step in securing a multi-cloud network is achieving networkwide visibility and centralized configuration management. The Fortinet Security Fabric natively integrates with major cloud providers and over 250 third-party security solutions. This eliminates silos between different cloud deployments, enabling centralized visibility and enforcement of security policies across the entire network. Centralized control makes it unnecessary for security teams to manually configure the security settings offered by each cloud service provider.

With full visibility in place, the next step is securing cloud-based applications. Many regulations, like the PCI DSS/SSF, require a web application firewall (WAF). **FortiWeb** WAF is available as a physical appliance, a virtual machine (VM), or as a Software-as-a-Service (SaaS) offering for cloud-native protection of the organization's websites, payment portals, and APIs.

Organizations also must manage access to their cloud deployments as a whole. **FortiCASB** and **FortiCWP** provide cloud-native access control and workload protection, simplifying visibility and security management across multi-cloud deployments. Finally, FortiGate NGFWs are available in a cloud-native Infrastructure-as-a-Service (IaaS) form factor, offering scalable security for any deployment environment.

Key Features of Fortinet Dynamic Cloud Security:

- Native integration with security features of all major cloud service providers
- Networkwide visibility and management of multi-cloud environments from a single pane of glass
- Cloud-native website protection, email, and firewall solutions
- Real-time, AI-driven threat intelligence distributed throughout the security infrastructure
- Automated identification of 5,000 types of application traffic, including encrypted cloud application data
- Secure, high-performance connectivity to cloud resources with Fortinet Secure SD-WAN

Applications and data storage are not the only cloud-based assets that an organization needs to secure. Organizations are increasingly taking advantage of cloud-based SaaS email solutions such as Google Mail and Microsoft Office 365. The **FortiMail** secure email gateway protects both SaaS and on-premises email deployments with the same email gateway.

Fortinet Differentiators for CSPs

Fortinet possesses unique capabilities and a proven track record in the service provider industry. Key differentiators include:

- **Visibility**
  The Fortinet Security Fabric, which offers out-of-the-box integration with more than 250 third-party security solutions, enables CSPs to achieve single-pane-of-glass visibility and configuration management for security elements across their network. This enables consistent security policy enforcement, even in cloud environments, while speeding threat detection and response.
- **Automation**
  Fortinet solutions enable the latest in SOAR capabilities. This strengthens CSPs' security companywide and enables the enterprise to scale and address resource constraints by maximizing the effectiveness of available skilled personnel. Centralized security management enables enforcement of policies throughout the network and automated report generation for regulators, the C-suite, and the board.
- **Proactive, AI-driven Threat Intelligence**
  Threat intelligence generated by AI and ML at FortiGuard Labs is communicated to security devices in real time via the Fortinet Security Fabric. This provides comprehensive protection against known and unknown threats across the network, from an organization's POS systems to its cloud-based infrastructure.
- **High Performance**
  FortiGate NGFWs, with corroborated performance testing by NSS Labs, offer the industry's lowest latency.[5] The highly efficient custom FortiGate ASIC, as well as the world's first SD-WAN ASIC, enables Fortinet to provide high-performance security at the WAN edge and throughout the network. Moreover, turning on advanced features such as SSL/TLS encryption inspection does not impact network performance in speed or throughput. In addition, **FortiGate VM** series NGFWs support packet acceleration technologies such as data plane development kit (DPDK), Single Root I/O Virtualization (SR-IOV), and Intel QuickAssist Technology (QAT). These are combined with Fortinet virtual security processing unit (vSPU) technology to deliver the best performance needed in CSPs' data centers, whether on-premises or in a private or public cloud.

Conclusion

Because the CSP business is driven by the network, the network must be security-driven. As fifth-generation (5G) technology enables CSPs to support more applications—such as remote precision medicine, connected cars, virtual and augmented reality, and a wide array of IoT applications[6]—they will find their networks increasingly targeted by cyber criminals. Regulators will no doubt follow suit, penning additional rules to safeguard customers. CSPs should be ready for this and other eventualities by ensuring that they have a broad, integrated, and automated security architecture in place.

Such an architecture is readily deployable with the Fortinet Security Fabric. When CSPs leverage security solutions and services from Fortinet and the vast ecosystem of technology alliances, they do not need to compromise on quality of service or customer experience to protect their network assets or data privacy.

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

[2] Ibid.

[3] "Data: Over Half of Consumers Use Mobile Apps When Shopping In-store," Cision PR Newswire, January 7, 2019.

[4] Dan Shewan, "13 Ways to Combat Shopping Cart Abandonment," WordStream, August 27, 2019.

[5] "Deterministic Communications for Secure High-speed Performance: Fortinet Protects Connections to Electronic Trading Platforms with the Industry's Lowest Latency and Jitter Rates," Fortinet, September 23, 2019.

[6] Nicol Turner Lee, "Enabling opportunities: 5G, the internet of things, and communities of color," Brookings Institution, January 9, 2019.

February 5, 2020 3:56 AM

516738-0-0-EN

D:\Fortinet\White Paper\SP Ent Protection\wp-protecting-communications-service-providers-with-the-fortinet-security-fabric-V1-252020-356AM