WHITE PAPER

Fortinet Technology Cybersecurity Solutions

Bolstering Protection Against Advanced Cyber Threats While Optimizing Cost and Efficiency

Executive Summary

The technology sector is a growing target for cybercriminals, who seek to steal intellectual property, create disruptions, and exfiltrate customer data. As a result, cybersecurity is a top concern in the industry. However, companies also face pressure not to slow operations for any reason in a fast-paced, quickly evolving marketplace. Fortinet solutions provide an integrated cybersecurity approach along with unmatched performance. This ensures that the entire network benefits from layers of protection without impacting application performance—even in demanding research and development (R&D) environments. Fortinet end-to-end integration also supports centralized visibility, operational efficiency, and simplified compliance reporting.

Technology companies exist to deliver innovation to their customers, and their success is ultimately tied to how well they execute this endeavor. R&D is at the core of the business and represents an intrinsic part of corporate culture at these organizations. Cutting-edge technology used in both R&D and production environments enables firms to stay ahead of the competition, but it also expands the attack surface and creates complexities for corporate network security.

Leading the list of priorities is the need to safeguard valuable intellectual property, in the form of software, hardware designs, and the data from research. Customer information is also a prime target. Consumer-facing brands often possess not only personally identifiable information (PII) and payment card data but also geolocation and behavioral analytics. Business-to-business (B2B) technology providers often possess confidential data about their customers' operations, financials, and critical infrastructure.

The average breach is not discovered for seven months,[1] enabling intruders to move laterally within the network.

With a current average of 50 connected devices per household, the exposure can be significant.[2]

Beyond the risks of data exposure, advanced cyber threats can also create vulnerabilities in the products that are sold to customers. A successful attack on design or production systems could ultimately endanger customers' cyber safety—or even their physical safety in some cases. And it certainly could cause major damage to a company's brand reputation.

Key Technology Cybersecurity Challenges

Supporting digital acceleration

Beyond the cutting-edge hardware and software often used in R&D, technology companies tend to be early adopters of new technologies for back-office operations, sales and marketing, customer experience, and product support—to name a few. Digital acceleration is increasing the urgency of IT infrastructure improvements as organizations try to stay competitive in a rapidly evolving marketplace. The volume of data is increasing at an alarming rate, and proliferating Internet-of-Things (IoT) devices often lack adequate security protections. And IoT risks aren't just on-site—remote workers can pass home-based IoT risks back to their companies.[3]

For cybersecurity teams, plugging every security hole in a growing attack surface is often an arduous struggle, let alone doing so in a strategic way. Operations certainly cannot be constrained by security tools that slow network performance or manual security processes. The security architecture must be resilient and flexible enough to adapt to rapid change in the threat landscape and in the organization. It also must be effective. The average time to identify a breach in 2021 was 212 days, with an additional 75 days needed for containment.[4]

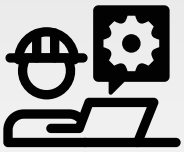
Productivity and uptime

Any unplanned interruption in operations can incur significant costs for a technology organization, whether in a manufacturing plant, R&D systems, or customer support. Disrupting operations is a common goal of cyberattackers, in other cases, it is a damaging side effect. Operational technology (OT) and IT systems alike can be targeted, and adversaries can infiltrate a network through an OT system and move laterally to gain access to the IT network.

Operational efficiencies

As security tools proliferate, lack of integration between them results in architectural fragmentation—and big operational inefficiencies for the cybersecurity team and for other departments. A lack of connection between different security logs reduces visibility and requires many security workflows to be managed manually. These manual processes often interrupt daily business and cause delays in everything from manufacturing to DevOps.

Architectural silos also increase operational expenses with overlapping functionalities in software licenses, multiple licensing contracts to maintain, and troubleshooting difficulties when something goes wrong.



As OT systems are connected to IT networks, they introduce risk in the security chain given their lack of integrated controls.

Advanced threats targeting high tech

Nearly one-third (31%) of global technology CEOs report cybersecurity as the greatest threat to their organization's growth over the next three years.[5] Threat actors target intellectual property and operations systems along with consumer and business customer data, employee HR data, financials, and compliance information, to name a few. Nation-state competitors can even target data about the internal deployment and testing of a company's current and future products. As adversaries use increasingly advanced technology in their attacks, even technology companies can sometimes have trouble keeping up.

Product integrity

Technology products must adhere to precise specifications in order to maintain product quality. As a result, adversaries, including nation-state competitors, often target OT systems or IT systems containing product designs or code. They can alter product designs to introduce flaws or sabotage the production process to reduce the quality of finished product. A company's brand suffers when significant quantities of defective products are shipped. Likewise, when consumers or businesses download compromised software from a company's website, this creates both reputational and legal liability. Even infected downloads from spoofed websites accessed through phishing emails can degrade a company's reputation—even though the company is clearly not at fault.

Compliance

Regulatory requirements are increasing for technology companies—especially regarding consumer data, financial data for public companies, and product safety. Penalties for noncompliance are sometimes high, but an even higher cost can come from diminished brand reputation in the event of a breach. Companies do well to include compliance in a larger risk management and data governance strategy. Regardless, audits are frequent enough that companies must be able to prepare for them without redeploying staff from strategic initiatives.

Use Cases

For technology companies, Fortinet solutions break into the following use cases:

Corporate infrastructure

The corporate IT network at technology companies houses important data related to finance, intellectual property, HR, product support, field support, and more. The value of that data is irresistible to cybercriminals. Theft of trade secrets costs the U.S. economy $180 billion each year.[6] In the technology industry, it also hosts several endpoint devices per employee, plus numerous IoT devices across the infrastructure. Additionally, websites and other customer-facing marketing content, which form customers' primary experiences with a company's brand, can pose serious risk.

As a result, corporate network security is vital in the industry. Technology companies need to be strategic and proactive about cybersecurity, eliminating silos and achieving single-pane-of-glass visibility across the network. Such an approach unlocks automation, enables automated response to fast-moving attacks, and optimizes operational efficiency.

The Fortinet Security Fabric delivers a broad, integrated, and automated security solution with end-to-end integration that brings centralized visibility and control spanning the entire organization. A wide array of Fortinet cybersecurity tools integrates seamlessly into the Security Fabric, along with dozens of third-party solutions delivered by Fabric Partners. Additionally, an open ecosystem and extensive application programming interface (API) tools give technology companies options regarding the integration of other tools. This provides flexibility for an ever-changing threat landscape and a rapidly evolving marketplace.

The Security Fabric is built on the foundation of **FortiGate** Next-Generation Firewalls (NGFWs) and artificial intelligence (AI)-powered threat intelligence from **FortiGuard Labs**. **FortiManager** and **FortiAnalyzer**, along with tools for security orchestration, automation, and response (SOAR) integrate seamlessly to enable a strategic and coordinated response to advanced threats. **FortiClient** and **FortiEDR** advanced endpoint security tools and **FortiNAC** network access control protect endpoints and IoT devices at the network edge. Physical security can be added to the Fabric with **FortiCamera** and **FortiRecorder**.

The Fortinet Security Fabric enables technology companies to move from a tactical stance toward cybersecurity to a strategic one. Companies can make informed decisions about best practices based on real-time information and advanced analytics. And an automated approach to security processes, threat response, and compliance reporting maximizes operational efficiency while improving security.

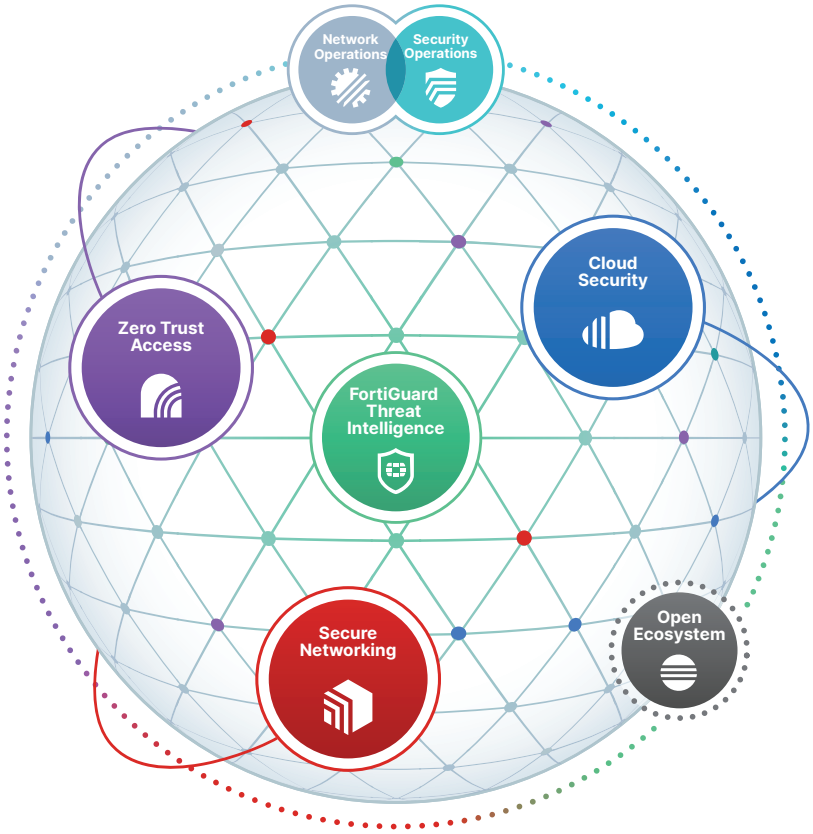


Figure 1: The Fortinet Security Fabric.

Manufacturing floor cybersecurity

IT and OT are increasingly co-dependent, and many technology companies were early adopters of this trend. Supervisory control and data acquisition (SCADA) systems are often based on older technology, and connection to the internet was not envisioned when they were designed. As a result, many SCADA systems have vulnerabilities that are not easily fixed. Compounding the risk, IoT devices that measure and convey critical information at the manufacturing facility are often headless, meaning that security patches cannot be applied.

To protect these critical but vulnerable systems, plant managers and security teams need to achieve centralized visibility into the entire cybersecurity infrastructure, from IT to OT. They must also be able to segment the network according to business need and centrally control both wired and wireless networks.

The Fortinet Security Fabric provides centralized visibility and control across the IT and OT systems of technology companies. **FortiGate NGFWs**, including the FortiGate **Rugged Series** for different environmental needs, provide the foundation for integration of OT into the security architecture. The intent-based segmentation capabilities included in FortiGate NGFWs enable IT and OT networks to be intelligently segmented to support zero-trust access and prevent lateral movement of threats. **FortiNAC** helps companies track and protect their IoT devices. Further, **SOAR** tools and **FortiAnalyzer** help organizations automate security response strategically, improving efficiency and helping stop threats that move at machine speed.

Nearly three-fourths (74%) of workers say they want to continue to work remotely following the pandemic, regardless of their business's hybrid work plans.[7]

The Fortinet Security Fabric enables technology companies with manufacturing operations to integrate the security architecture across IT and OT environments, unlocking automation and optimizing operational efficiency. This can protect the manufacturing floor against both targeted and recycled threats and minimize production disruptions that impact the bottom line.

Remote workforce

The start of the pandemic sent tech company employees home and IT teams scrambled to support and secure a fully remote workforce. Even though companies are shifting to hybrid and even going back to fully on-site work models, there are still many remote or frequently traveling workers.

To preserve employee productivity, users need the same access in a residence, an airport, or a hotel room that they would have if they were sitting in a company office. Yet, providing such access introduces cybersecurity risk—especially for companies that operate with a perimeter-based approach to security. To provide secure remote access, companies must adopt a holistic approach to cybersecurity that includes a zero-trust approach to access, making no distinction between "trusted" internal traffic and traffic from the outside. Robust network segmentation must be bolstered by behavior-based ways to detect when user accounts and devices are compromised.

Our work-from-anywhere (WFA) solution enables technology companies to provide extensive access to remote workers while protecting network segments that specific employees do not need. **Fortinet Zero Trust Network Access (ZTNA)** safely connects users to applications no matter where the user is located and no matter where the application is hosted. **FortiAuthenticator** and **FortiToken** identity and access management solutions help companies limit access to authorized users. FortiGate intent-based segmentation enables the network to be divided according to business need, enabling zero-trust access. Advanced endpoint protection tools, such as **FortiEDR** (endpoint detection and response) and **FortiClient**, help prevent infiltration through the endpoint devices used by remote workers.

These Fortinet solutions enable technology companies to provide full and secure access to remote workers while protecting corporate assets against attacks from remote locations.

Secure branch networks

Technology companies often have small and large branch offices around the world. Many have large overseas locations that are involved in resource-intensive work like R&D—often in coordination with managers residing at headquarters. Secure and reliable connections between these sites and headquarters are often critical for time-sensitive projects.

The multiprotocol label switching (MPLS) infrastructure that traditionally provided connectivity to branch offices is expensive, cumbersome, and difficult to scale. As hybrid-cloud networks grow, network traffic increases, and workers at branch locations frequently notice latency in cloud-based services. And as companies struggle when they try to prioritize traffic, the latency can apply to a company's most-critical applications.

In response to these problems, companies are rapidly adopting software-defined wide-area networks (SD-WAN), which enable network traffic to travel on the public internet. To keep such a network secure, SD-WAN technology should ideally be integrated with the cybersecurity infrastructure—and with the networking infrastructure at the branch.

Fortinet Secure SD-WAN technology is included in FortiGate NGFWs, enabling highly secure and cost-effective connections on the public internet, but also over a virtual WAN (vWAN) within select public clouds. At the branch, **Fortinet SD-Branch** solutions extend the SD-WAN solution to the access layer. This enables secure networking at branches and consistent security coverage from the internet to the wireless network, down through the switching infrastructure.

Fortinet solutions for secure branches enable companies to provide secure, high-performance networking with branches, with multiple choices for routing of traffic depending on volume. This helps support network performance at branches while protecting the network against intrusions that enter through branch locations.

The vast majority (98%) of security professionals report that relying on multiple cloud providers creates additional security challenges.[8]

Multi-cloud security

Technology organizations were early adopters of cloud-based services, and most now operate in multiple public and private clouds. And in many cases, their most valuable and sensitive data is contained within this hybrid-cloud infrastructure. As organizations adopt services across this distributed architecture, the default is to leverage the built-in cybersecurity tools offered by each cloud provider.

However, these solutions do not communicate with one another, and indeed have different underlying structures. The result can be multiple security silos—one for each cloud provider, one for the private cloud infrastructure, and one for the corporate data center. This makes centralized visibility and automation impossible. The result can be team members being pulled away from strategic projects to do manual work when compliance audit reports are due.

To address this lack of visibility and operational inefficiency, organizations must unify the security architecture from the hybrid cloud to the data center. Policy management must be consistent across the board, and threat intelligence should be made available across the company in real time.

Fortinet Cloud Security solutions accomplish these objectives by providing a single-pane-of-glass view of the entire cloud infrastructure. They feature native integration with all major public cloud providers, broad protection to cover all elements of the attack surface, and management and automation features that enable consistent, timely threat detection and response through automation.

Fortinet enables technology companies to protect disparate cloud-based applications and infrastructure in a consistent way—with multiple layers of cybersecurity protection. As a result, technology companies can confidently deploy any service in any cloud at any time.

Fortinet Differentiators

Integrated platform

The **Fortinet Security Fabric** is built on a flexible platform based on **FortiOS**, a purpose-built operating system. On this foundation, technology companies can build an end-to-end, integrated security architecture from the data center to the network edge to multiple clouds. Multiple Fortinet tools integrate into the Security Fabric, and third-party solutions can be added seamlessly via **Fabric Connectors**. Other third-party products can be integrated with a Fortinet open API and a library of API tools.

High performance and low latency

FortiGate NGFWs provide the industry's best performance during secure sockets layer/transport layer security (SSL/TLS) inspection and experience extremely low latency rates—even in demanding technology industry networks. With 95% of traffic now encrypted across Google,[9] this ensures that a necessary function does not impact operations.

Branch location networking and security

Fortinet offers comprehensive **Secure SD-WAN** technology, along with cybersecurity infrastructure for branch locations that eliminates the need for expensive MPLS bandwidth, provides optimal security, and improves network performance.

Insider threat protection

Fortinet delivers a comprehensive and multilayered solution to guard against insider threats with identity and access management supplemented by NAC, intent-based segmentation, deception technology, and user and entity behavior analytics (UEBA)—all integrated for centralized visibility and control.

Robust threat intelligence

FortiGuard Labs delivers near-real-time protection based on threat intelligence from a large global network of firewalls and an AI-powered self-evolving detection system (SEDS). This results in extremely accurate, real-time identification of zero-day and unknown threats before they can cause problems on a network.

Conclusion

Technology companies deliver digital innovation to their customers, but their brands can be tarnished quickly if their products lack quality, have technical glitches, or do not have adequate cybersecurity protection. By helping to thwart the tactics of a variety of threat actors, the Fortinet Security Fabric helps prevent these outcomes. As a result, technology organizations can focus on what they do best: innovate and delight customers.

[1] "2021 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 28, 2021.

[2] "The Ultimate List of Internet of Things Statistics for 2022," FindStack, February 15, 2022.

[3] "Understand the risk of IoT vulnerabilities in the remote work era," SC Magazine, February 4, 2022.

[4] "2021 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 28, 2021.

[5] "How Tech Companies Can Boost Cyber Defenses: Building a Cyber-First Culture," eWeek, September 20, 2021.

[6] "Intellectual Property Enforcement," U.S. Department of State, April 26, 2021.

[7] "Top cybersecurity statistics, trends, and facts," CSO, October 7, 2021.

[8] "Multi-cloud environments creating additional security challenges," HelpNetSecurity, July 15, 2021.

[9] "Google Transparency Report," Google, accessed April 19, 2022.

April 28, 2022 8:01 AM

516779-A-0-EN