NTT Ltd. and Fortinet

Fortifying and Protecting Valuable Infrastructure and Assets from Malicious Cybersecurity Attacks

Challenges

According to FBI reports, cybercrime losses have doubled in recent years, reaching over $3.5 billion.[1] Account Takeover (ATO) losses have tripled, and fraud has doubled.[2] Ponemon Institute, a leading security research firm, notes that the average cost of a security breach is now almost $4 million.[3] Moreover, digital transformation (DX) now accounts for over 40 percent of most IT budgets and has expanded security requirements and boundaries.[4] Enforcing cybersecurity protection across physical and virtual environments has become more complicated and expensive for most global enterprises.

Given these extraordinary challenges, IT departments must spend tremendous time and resources protecting their organizations from attack. In addition, governments and other regulatory agencies have implemented a variety of compliance mandates to protect valuable assets that may include Personally Identifiable Information (PII) or intellectual property. Information security professionals are stretched thin and most organizations have difficulty meeting these demands. Solving these challenges requires a modern approach, purpose-built for advanced security and networking needs.

The Fortinet Security Fabric

Fortinet's fast, secure, and global cybersecurity solutions provide broad, high-performance protection against dynamic security threats while simplifying IT infrastructures. Fortinet's solutions are fortified by the industry's highest level of threat research, intelligence, and analytics. The Fortinet Security Fabric and solutions, combined with NTT's comprehensive portfolio of cloud and managed security services, offer organizations the advanced security controls and unified management required to protect their data from malicious attacks. Enhanced by NTT's integration, support, and managed security services expertise, our global partnership provides you with high-quality and cost-efficient security solutions that deliver multiple layers of threat protection and management, increased deployment flexibility, and the ability to scale your business.

More than 465,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their firms' most valuable assets. The Fortinet Security Fabric enables organizations to implement DX initiatives without compromise by delivering a complete cybersecurity platform that provides:

- Broad visibility across the entire digital attack surface to better manage risks
- Integrated solutions that reduce the complexity of supporting multiple point products
- Automated workflows to increase the speed and efficiency operations and responses

Global Technology Leader

The NTT Group is the largest ICT company in the world by revenue.

Keeping You Secure

We mitigate 2 billion security threats every year.

Global Implementation

The NTT group invests USD 3.6 billion in research and development.

Global Scale

40,000 people across five continents.

NTT Services and Solutions

NTT is a leading Global Technology Integrator that understands your need to be resilient, yet agile, and innovative for the future of your intelligent business. Therefore, knowing the security risks you face and being prepared to address them amidst constant change is crucial. We work with you to identify the technologies and services you need to create, build, deliver, and manage a cybersecurity posture that keeps you secure while you transform.

NTT offers proven business and technology advisory services, delivered by experts with advanced cybersecurity knowledge. We have both vertical-specific and regional expertise that enables you to evaluate the most appropriate activities to prepare effectively. NTT security experts provide the help you need to identify the technologies required, assist in implementation, and monitor systems for ongoing security and integrity from our security operations center (SOC).

The NTT and Fortinet Partnership

NTT and Fortinet can help protect your firm from cyberattacks as your organization expands from data centers to endpoints and the cloud, well beyond traditional boundaries. Our goal is to help you build a comprehensive security platform that provides multiple layers of threat protection and management, increased deployment flexibility, and the ability to scale with business requirements, while maximizing your existing IT investment. With cybersecurity at the core of our strategy and digital programs, NTT has partnered with Fortinet to help enterprise firms create a digital business infrastructure that is **secure by design**. With our combined threat intelligence, we help identify, predict, detect, and respond to cyberthreats while supporting business innovation and managing risk. Unlike others in the security industry, we support your team across the full cybersecurity lifecycle, including:

- Consultative advice on the emerging threats and the best practice security posture needed to enable your business goals
- Designing, architecting, and implementing the best solutions globally by aligning controls that best suit your environment
- Managed service on a global basis to help overcome resource gaps and implement and manage best-in-class security technologies

A Comprehensive Approach

NTT's extensive global experience, combined with our Fortinet Technical Professional Certifications, ensure our ability to help your team plan and build defensible infrastructures that incorporate solutions from Fortinet. Implementations will always exceed business requirements and create fortified foundations for a secure infrastructure. The NTT and Fortinet global partnership offers you a consistent level of service and support, as well as the latest solutions needed to remain secure. NTT's proactive teams monitor and maintain security devices through our six Global Security Operations Centers using ITIL-aligned Global Services Operating Architecture Service capabilities, which include 24×7 technical support, product education, and professional integration services.

By leveraging the ISA99/IEC 62443 standard and integrating with third-party partners, NTT Security experts and the Fortinet Security Fabric deliver a comprehensive security approach that implements a progressive strategy across three major phases:

Phase I: Reconnaissance

NTT begins by passively observing and monitoring your network. We then create an updated and comprehensive inventory of every network segment, device, application version, connectivity detail, and security score. We also perform real-time behavioral analytics that identify normal and abnormal activities. This provides a visibility overview to adequately plan the best tactics and strategies and provide the appropriate security solutions and services.

Phase II: Risks

NTT Security experts identify your security vulnerabilities and map the risks to the operational level. We use a variety of common benchmarks including the National Institute of Standards and Technology (NIST) framework, the EU's Directive on Security of Network and Information Systems (NIS Directive), and IEC 62443 to identify risks and how they relate to your organization's infrastructure, business, and operational goals. Benchmarks and identified risks are used to guide your firm and prioritize the fortifications, weapons, and armor needed reduce risks and maintain operational uptime.

Phase III: Response

Responding to threats in today's dynamically changing environment requires a more proactive rather than reactive approach. NTT's Security Division can help you identify potential threats and attackers before they invade. To help with this, we employ the most appropriate Fortinet solutions and Security Fabric, based on the insights and recommendations obtained from the previous two phases, to help fortify your firm against attacks. The Fortinet Security Fabric and solutions offer some of the most comprehensive and proven solutions in the industry that include:

1. **An Integrated Platform:** Fortinet delivers a flexible platform and next-generation firewall (NGFW) technology for building an end-to-end, integrated security architecture. From the data center to the endpoint to multiple clouds, Fortinet offers an integrated Security Fabric. Also, an open application programming interface (API) and Fabric Connectors that can help you integrate third-party tools to leverage prior investments.
2. **Remote Location Security:** Fortinet offers a comprehensive software-defined wide-area network (SD-WAN) and secure networking for remote locations. This eliminates the need for expensive multiprotocol label switching (MPLS) bandwidth, provides optimal security, and improves network performance.
3. **Networking, Cybersecurity, and Physical Security:** Fortinet delivers the ability to consolidate networking, cybersecurity, and surveillance functions into a single pane of glass—whether at a main site or remote branch.
4. **Insider Threat Protection:** Fortinet delivers a comprehensive and multilayered solution to guard against accidental and deliberate insider threats with identity and access management supplemented by network access control (NAC), intent-based segmentation, deception technology, and user and entity behavior analytics (UEBA)—all integrated for centralized visibility and control.
5. **Robust Threat Intelligence:** FortiGuard Labs delivers comprehensive intelligence from a large global network of firewalls and an artificial intelligence (AI)-powered self-evolving detection system (SEDS) that has refined its algorithms using machine learning (ML) for nearly eight years. This has resulted in extremely accurate, real-time identification of zero-day, and unknown threats.
6. **Industry Leadership:** Fortinet is recognized as a Leader in the Gartner Magic Quadrant for Network Firewalls, achieved the best score in the NGFW Security Value Map from NSS Labs, and has achieved nine "Recommended" ratings from NSS Labs.

FortiGate Firewall Use Case

A financial services company used multiple legacy vendors to meet firewall, NAC, endpoint protection, and WAN edge router requirements. They managed these devices in-house and maintained separate relationships with each vendor. When a new CISO joined the firm, he asked his team to review the entire Fortinet Fabric solution across all areas including switching and wireless infrastructure. NTT Managed Security Services offered the ability to manage all aspects of the Fortinet Fabric with a single vendor, thereby lowering efforts and costs. NTT helped improve the customer's overall security posture and increase the performance of the WAN edge branch network through a fully-integrated solution.

Secure Edge/SD-WAN Use Case

A large foods manufacturing and processing company based in the United States had invested in Fortinet FortiGates for their data centers and DMZ, which was fully managed by the NTT Managed Security Services team. When the company decided to transform their edge branch deployments by implementing SD-WAN technology, NTT recommended a security-focused approach that leveraged the existing FortiGate infrastructure. Having the SD-WAN feature native within a security appliance allowed seamless, automated, and preemptive failover capabilities for the network and the defined applications. Continuous health monitoring is performed on the FortiGate appliances, and if connectivity becomes an issue, the FortiGate will fail over to another node before network performance is impacted. This can be enhanced by assigning roles to critical applications that prioritize connectivity. The customer now benefits from consistent security policies across the core and branch network, application awareness at the edge, and lower Total Cost of Ownership (TCO). In managed Fortinet environments, NTT clients have consistently relied on NTT to manage global rule sets and security policies, and enable SD-WAN features. NTT ensures that the edge is secure while maintaining the integrity of the wider network.

OT Use Case

A municipal water & wastewater systems operator in the United States had difficulty balancing limited resources against OT security needs to keep critical Water sites operational, as well as reduce operational cyber risks while meeting corporate guidelines. The company had not yet implemented an OT cybersecurity roadmap to address cybersecurity requirements or focus IT budgets on high impact OT assets. The NTT Security Consulting team helped the customer build a comprehensive OT cybersecurity roadmap. NTT worked collaboratively with Fortinet to provide a complete solution to address all OT security requirements including perimeter protection and systems baselining. The Fortinet-NTT solution proactively limited OT network risks through dynamic network segmentation and enforced security policies across all OT devices. The solutions also analyzed traffic for ongoing threats and vulnerabilities.

Teleworker Use Case

Recent research revealed that 84 percent of firms plan to continue supporting more teleworkers but less than 30 percent are ready to ensure adequate security.[5] Remote work is the new norm where the current environment requires employees to complete work-related tasks through remote internet connections. The Fortinet Security Fabric addresses remote worker scenarios with three primary levels of connectivity. NTT Managed Security Services provides deployment and managed services for all these elements of the Fortinet Security Fabric, to ensure the most cost-effective and reliable solutions available for remote workers. FortiGate with the FortiClient Fabric Agent provides a VPN tunnel back to a primary office, to ensure that communications stay private while traveling across open networks. FortiAuthenticator and FortiToken provide multi-factor authentication (MFA) to verify user identities.

And for individuals handling company confidential communications, deploying a FortiGate NGFW at a remote office provides key personnel with the highest levels of security and performance available for remote locations. With secure traffic tunnels, as well as application control and traffic inspection, a low-end FortiGate NGFW provides an economical and powerful solution with several levels of protection, backed by artificial intelligence (AI) security processes. By deploying the Remote Work solution from Fortinet and NTT, firms can benefit from the agility required to support remote workers, thereby increasing employee productivity, morale, and retention.

Conclusion

Avoiding the serious consequences of ransomware or other malicious cybersecurity attacks, or compliance-related fines or lawsuits, now requires more advanced and effective network security technologies, expertise, and services. Rather than complex and costly point solutions or services, IT and security teams need augmentation from trained security experts combined with the latest security solutions that seamlessly integrate into networks and simplify and automate security tasks.

Organizations need to identify risks and how they relate to infrastructure, business, and operational goals, and then implement a Security Fabric, solutions, and managed services to mitigate attacks while creating seamless and frictionless user experiences. To accomplish this, firms require transparent visibility and real-time security workflows underscored by global threat intelligence. In today's dynamic, remote, and risk-filled environment, protecting valuable assets requires the right combination of security solutions and services provided by NTT and Fortinet.

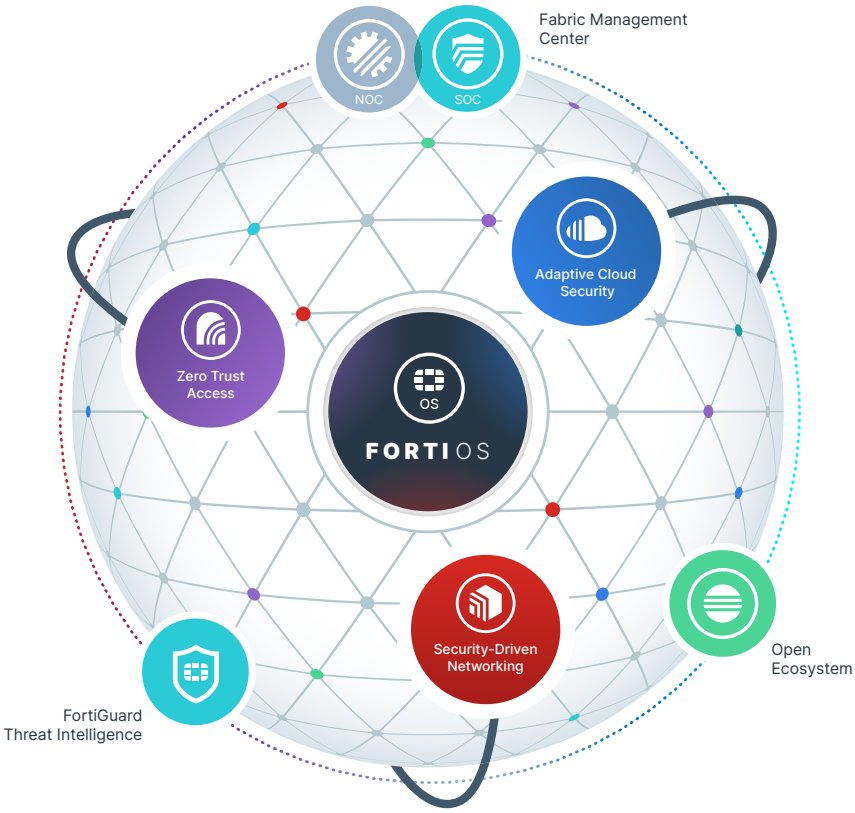

Figure 1: Fortinet Security Fabric diagram.

The Security Fabric

The Fortinet Security Fabric platform provides true integration and automation across an organization's security infrastructure, delivering unparalleled protection and visibility to every network segment, device, and appliance, whether virtual, in the cloud, or on-premises.

Contact Information, Trademarks, and Copyrights

References

[1] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[2] https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

[3] https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/

[4] https://www.idc.com/getdoc.jsp?containerId=prUS45612419

[5] https://www.bitglass.com/press-releases/bitglass-report-84-of-organizations-will-continue-to-support-remote-work-but-most-arent-equipped-to-do-so-securely

FORTINET

www.fortinet.com

May 2, 2021 3:09 AM

D:\Fortinet\2021 Rebranded templates\Marketing or Comms Request\April\942806 - NTT\ntt-ltd-and-fortinet-V1-522021\ntt-ltd-and-fortinet-V1-522021

645625-A-0-EN