SOLUTION BRIEF

Protect Hyperscale Data Centers From Cyber Threats

Executive Summary

The amount of data crossing today's networks is growing exponentially, changing the network landscape. CIOs and IT Leaders must focus on risk management and protecting data that's stored on premises as well as distributed across the network. However, these protections are often disjointed, bringing complexity and risk into the enterprise.

To combat this, enterprises are leveraging hybrid IT, distributed Internet of Things (IoT) and endpoint devices, and 5G performance to build scalable architectures that interconnect all edges, including home offices, branches, campuses, data centers, and multi-cloud environments into a unified network. A hybrid approach is critical, because while cloud adoption is transforming networks, on-premises data centers remain essential for applications, data, and workloads that can't be moved to the cloud but are still needed. And all of these systems need to work as a single, unified network.

The World Economic Forum estimates that 463 exabytes of data will be generated worldwide each day by 2025.[2]

However, hybrid networks also expand the attack surface. And, the expanding attack surface has created a lucrative opportunity for bad actors to exploit old and new vulnerabilities. Ransomware, in particular, offers a low-investment, high-profit business model that's irresistible to cybercriminals. Without an integrated security strategy designed to span the distributed network, blind spots and security gaps emerge. When organizations add isolated point security products, there can be no end-to-end visibility and control, increasing risk. The resulting disjointed security can't provide a holistic view of the attack surface or effectively stop and contain increasingly sophisticated attacks.

In addition, most data center security is focused solely on securing north-south data flows to create airtight, Layer 4 perimeter protection at the edge. But such measures are often ineffective against ransomware or volumetric distributed denial-of-service (DDoS) attacks. And to make things worse, these attacks are now increasingly being combined.[1]

Fortinet's unified security approach provides end-to-end visibility and response across distributed networks, including distributed data centers. By converging networking, branch, and secure access service edge (SASE) solutions, our security can interoperate seamlessly and scale effortlessly across complex, hybrid environments, leveraging 20+ years of innovation to deliver consistent enterprise-class protection and optimal user experience across all network edges.

Protect Data Centers From Ransomware and Volumetric DDoS Attacks

Fortinet Next-Generation Firewalls (NGFWs) are powered by the industry's only purpose-built security processing units (SPUs). These specialized processors are specifically designed to offload critical security and networking functions to help scale business, meet escalating user demands, and protect application and hosted services edges.

The Fortinet firewalls offer a single operating system (FortiOS) that provides a unified security and management framework across all form factors and edges, supporting hybrid environments in a consistent and coordinated way. FortiOS consolidates many key capabilities for both security and networking, allowing explicit access to application and data center resources thereby enabling a Zero Trust strategy.

One of the biggest challenges of fending off a volumetric DDoS attack is the amount of specialized processing power needed to mitigate an attack. Fortinet's custom application-specific integrated circuit (ASIC) technology not only delivers a staggering firewall performance rate of up to 1.9 Tbps but also provides hardware-accelerated anti-DDoS capabilities to prevent volumetric attacks.

- Built-in anti-DDoS mitigation detects and prevents volumetric attacks to ensure business continuity and service availability.
- Anti-DDoS, anomaly detection and protection, policy-based intrusion prevention, firewall FastPath, dynamic segmentation, and behavior-based technologies also prevent the spread of DDoS attacks.

To detect ransomware, the SPU enables FortiGate to inspect encrypted traffic as well as streaming video, looking for hidden malicious traffic—the only solution in the industry able to do this. In addition:

- The intrusion prevention system (IPS), updated regularly with threat intelligence feeds from FortiGuard Labs, detects known ransomware variants.
- A built-in sandbox leverages machine learning that enhances the static and dynamic analysis of threats to detect and detonate unknown ransomware.
- FortiGuard Web Filtering service provides comprehensive threat protection to address web-based ransomware, blocking known and unknown malicious URLs with near-zero false negatives.

Secure Internal Network Segments

The FortiGate NGFW also delivers dynamic internal segmentation firewall (ISFW) capabilities combined with access control to prevent the lateral spread of threats, keeping the network available even during a DDoS attack. The NP7 makes scalable segmentation possible through Virtual Extensible LAN (VXLAN) termination and re-origination, combined with essential Layer 4 firewall rules. This helps enterprises build hybrid IT architectures that can securely connect legacy physical database domains to virtualized application and web server domains for agility and on-demand scalability.

The average cost for an enterprise to find and recover from a data breach is $2.4 million and it takes a median of 37 days to complete.[3]

Intent-based segmentation intelligently segments network and infrastructure assets to prevent the lateral movement of ransomware, restricting its access to a controlled sector.

Enable Comprehensive, Up-to-Date Threat Protection

Full data center threat protection is achieved by consolidating all required best-of-breed security functions within a single FortiGate NGFW platform. FortiGate NGFWs stay ahead of the latest threats with near real-time threat intelligence services from FortiGuard Labs. Together, they deliver:

- Unprecedented traffic load protection with hyperscalability and ultrafast performance
- A full stack of security functions designed to detect and mitigate ransomware attacks
- Hardware-assisted IPv4 or IPv6 DDoS metering to prevent volumetric-based flooding attacks
- Stringent access control list enforcement at both the physical network interface and the in-built host protection engine to limit DDoS packets-per-second
- Optimal TCO by consolidating point products onto a single integrated platform

Hyperscale and Hybrid Data Centers Require Powerful Security

To secure the most demanding data center architectures, FortiGate NGFWs deliver up to 520 Gbps of threat protection with anti-DDoS and ransomware protection for full visibility and control across the network. Powered by purpose-built SPUs, they consolidate tens of millions of connections per second and up to 1.9 Tbps firewall performance.

By weaving security deep into hyperscale and hybrid IT architectures, FortiGate can protect any workload, anywhere, anytime, including from sophisticated DDoS and ransomware attacks. The entire attack surface is covered by contextual, actionable, coordinated, and fully automated threat protection.

FortiGate secures organizations while simplifying operations, automating workflows, and saving time with easy-to-use, single-pane-of-glass management across the Fortinet Security Fabric and 400+ ecosystem partners.

[1] Derek Manky, "Fortinet Featured at INTERPOL's First Global Conference on Ransomware," Fortinet, August 6, 2021.

[2] Jeff Desjardins, "How much data is generated each day?" World Economic Forum, April 17, 2019.

[3] Forrester: "The 2021 State Of Enterprise Breaches," April 2022

January 19, 2023 5:29 PM

1907432-A-0-EN