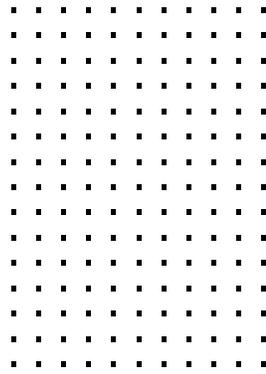


SOLUTION BRIEF

# Protecting Hyperscale Data Centers From Ransomware and Volumetric DDoS Attacks



## Executive Summary

Enterprises are adopting hybrid IT, Industrial Internet of Things (IIoT), and 5G to gain operational agility. These tools help them build composable and scalable architectures that interconnect distributed branches, campuses, on-premises data centers, and multi-clouds into a unified network. And yet, in the midst of this change, the enterprise on-premises [data center](#) remains an essential component of most networks. Its role is vital because it protects applications, data, and workloads that can't be moved to the cloud but that still need to be consumed by employees, customers, and partners.

However, the data center infrastructure is also becoming more distributed, greatly expanding its attack surface. Without a holistic security strategy that can seamlessly span distributed environments, blind spots emerge. Point security products deployed in different parts of the network create security gaps that reduce visibility and increase the potential for breaches and attacks. The resulting disjointed security is unable to provide a holistic view of the attack surface or effectively stop and contain increasingly sophisticated attacks, such as ransomware and distributed denial of service (DDoS).

To complicate things further, most data center security policies are focused on north/south data flows. By applying essential Layer 4 protection at the edge, they aim to create airtight perimeter protection. But most data center traffic flows east/west, across the data center, especially across distributed data center environments. This means perimeter-focused security measures are ineffective if threat actors launch a sophisticated ransomware or volumetric DDoS attack (in fact, these attacks are increasingly being combined) to overwhelm the foundation of your security.

## Fortinet Advanced Innovations Protect Today's Hybrid Environments at Scale

By leveraging 20+ years of innovation, Fortinet solutions are designed to provide consistent enterprise-class protection and optimal user experience across all network edges. And Fortinet solutions also converge networking and security, including Branch and Secure Access Service Edge (SASE) solutions, enabling protections and visibility to interoperate and scale across complex, hybrid environments.

Because of these innovations, the FortiGate Next-Generation Firewall (NGFW) has received the highest score in Gartner's Enterprise Data Center Use Case<sup>1</sup> two years in a row and has maintained a leadership position in their Network Firewall Magic Quadrant<sup>2</sup> for the last several years.

Part of the reason for these accolades is that Fortinet NGFWs are powered by the industry's only security processing units (SPUs). The most recent release, called the Network Processor 7 (NP7), is designed to scale your business to meet escalating user demand while protecting your application and hosted services edge. It delivers a staggering firewall performance rate of up to 1.9 Tbps. And it includes hardware-accelerated anti-DDoS capabilities to prevent volumetric attacks—all in a single FortiGate platform managed through an easy-to-use, single-pane-of-glass console.

The NP7 offers the following unique and unparalleled capabilities:

- Ultrafast speeds are delivered by offloading user connections from the CPU using innovative FastPath acceleration. FortiGate NGFWs deliver up to 10 million connections per second, resulting in enhanced network performance.
- The NP7 also offers anomaly-based intrusion prevention, checksum offload, and packet defragmentation. Its multilayered protection starts with anomaly checking at the packet level to ensure that each packet has not been compromised. Next, a sophisticated set of interface-based anomaly protection, DDoS protection, policy-based intrusion protection, firewall FastPath, and behavior-based methods are employed to prevent DDoS attacks from spreading to the rest of the system.
- Anti-DDoS mitigation is also embedded in the NP7's hardware, ensuring business continuity and service availability in case of a DDoS attack. Its anti-DDoS hardware acceleration policy offloads the processing of IPv4/IPv6, interface, and access control list (ACL) policies from the CPU for efficiency and performance, making the NP7 very effective at detecting and preventing volumetric attacks.



- The NP7 can also be used to secure high-performance data center interconnect (DCI) to build data recovery (DR) sites and replication. The NP7 stores session and Internet Protocol security (IPsec) security association keys, performs all necessary encryption/decryption, and accelerates all sessions. It delivers Suite B IPsec throughput of up to 310 Gbps in a compact form factor.

## Security Beyond the Edge

Today's NGFWs must also be able to support dynamic secure segmentation with dynamic internal segmentation firewall (ISFW) capabilities. ISFW prevents the lateral spread of threats and establishes strong compliance and application access control combined with a broad defense-in-depth portfolio of fully integrated solutions to root out and terminate malicious activity.

But today's networks are also highly dynamic, adapting to changing bandwidth and application requirements. The scalable segmentation such environments require is only possible because NP7-powered FortiGate platforms also support virtual extensible local-area network (VXLAN) termination and re-origination combined with essential Layer 4 firewall rules. These help enterprises build hybrid IT architectures that connect legacy physical database domains to virtualized application and web server domains, helping organizations achieve agility and on-demand scalability.

## Full Threat Protection

Full threat protection is achieved by consolidating all required best-of-breed security functions within a single FortiGate NGFW. NP7-powered FortiGate solutions reach up to 500+ Gbps of throughput, helping organizations realize optimal total cost of ownership (TCO).

FortiGate [NGFWs](#) designed for the [data center](#) combine the industry-leading performance of the [FortiGate product portfolio](#) with the coordinated and actionable threat intelligence of FortiGuard Security Services from [FortiGuard Labs](#) to deliver the following benefits:

- Enables seamless user experience because Fortinet NGFWs are powered by the industry's only SPUs
- Handles unprecedented customer traffic loads with hyperscalability and ultrafast performance
- Protects applications and infrastructure hosted at the data center edge with hardware-assisted IPv4 or IPv6 DDoS metering controls to prevent volumetric-based flooding attacks
- Applies stringent controls to enforce access control lists at both the physical network interface and in-build host protection engine to limit packets per second for various packet types, helping to make the NGFW more robust and resilient
- Protects any workload, anywhere, anytime by building hyperscale Security-Driven Networks that weave security into the networking of hybrid IT architectures
- Consolidates and eliminates point products by running multiple, industry-leading [FortiGuard services](#) on a single platform to achieve optimal TCO
- Extends security across the entire attack surface with actionable, coordinated, and fully automated threat protection
- Simplifies operations, automates workflows, and saves time with an easy-to-use, single-pane-of-glass management system that can cover the entire distributed Security Fabric, including support for over 400 ecosystem partners

Today's agile networks and hybrid data center environments allow organizations to compete effectively in today's digital marketplace. But to do so, they need security solutions designed to see, scale, and adapt to dynamic changes and defend against advanced threats, such as ransomware and DDoS attacks. Fortinet FortiGate solutions, built on an integrated platform and powered by the industry's only custom security processors, enable organizations to build the networks they need without ever compromising on the security those environments require.

<sup>1</sup> ["Analyst Report: 2020 Gartner Critical Capabilities for Network Firewalls,"](#) Fortinet, November 10, 2020.

<sup>2</sup> ["Fortinet is a Leader in the 2020 Gartner Magic Quadrant for Network Firewalls,"](#) Fortinet, November 9, 2020.

