CHECKLIST

5 Challenges with Hybrid and Hyperscale Data Center Security and How to Solve Them with Fortinet

Enterprise organizations are taking advantage of data center evolution, but face a number of security challenges as they transition to hybrid and hyperscale data center architectures. Fortunately, Fortinet security-driven networking solutions were designed to solve these challenges, delivering security and performance right-fit for the unprecedented needs of hybrid and hyperscale architecture.

Following are common challenges and how to apply Fortinet solutions, with links to detailed solution guides.

1. CHALLENGE: Limited visibility

As organizations transition from traditional data center architecture to a hybrid architecture, networking and IT infrastructure spreads across on-premises, colocation, and multiple clouds—a trend that typically reduces overall visibility into network segments. At the same time, encrypted traffic is rising, resulting in more blind spots and further challenging network visibility. The wrong solution won't provide adequate visibility of all deployed security elements across all the various environments, nor will it provide comprehensive visibility and control of users, applications, and devices on the network.

Fortinet FortiGate Network Firewalls remove those blind spots by detecting unsanctioned applications and hidden threats, consolidating key security functions such as web filtering and threat protection into a single solution.

For more: Solution Brief

2. CHALLENGE: Expanding attack surface

Many organizations lack adequate internal security controls that would keep assets separate from each other to keep threats contained (i.e., from not spreading laterally if they successfully breach a network). The solution is segmentation, which not only prevents the lateral spread of threats but can also help organizations better protect applications and meet compliance standards by demonstrating multiple layers of security controls.

Fortinet solutions protect any type of segmentation—including network-level, port-level and application-level segmentation—as long as the traffic is directed to or flows through a FortiGate. This can be achieved at any scale, using flexible and high-performance security inspection capabilities.

For more: Solution Brief

3. CHALLENGE: Shield vulnerabilities

Intrusion prevention systems (IPS) must also rise to the challenge of securing hybrid and hyperscale data centers. Organizations need fully integrated IPS to help protect hard-to-patch legacy systems that are business critical, and shield them against known and zero-day vulnerabilities.

Fortinet Network Firewalls with IPS allow customers to preserve their network design, are powered by the Fortinet Security Fabric, feature artificial intelligence/machine learning (AI/ML)-enabled FortiGuard Labs threat intelligence, and uniquely offer on-premises or cloud-based FortiSandbox services to prevent from unknown threats, delivering the industry's best price/performance and security effectiveness (as verified by third-party entities such as NSS Labs).

For more: Solution Brief

4. CHALLENGE: Hyperscale performance

The hyperscale era means massive datasets needing to move around at breakneck speeds—with data-in-transit security and with no loss in performance. How about dealing with a very large volume of user connections without sacrificing user experience? Easier said than done, but if networking and security teams can't deliver the kind of user experience modern employees or customers require, they face losses in productivity and reputation.

Hyperscale data centers require hyperscale security. Fortinet Network Firewalls are powered by the latest security processing units delivering unmatched user and application experience and offer the industry's best security compute rating of **12x** performance for connections per second. Fortinet Network Firewalls also uniquely enable the transfer of data at 10x speed, **11x** performance for IPsec encryption (high-performance secure connectivity), and hardware-assisted Virtual Extensible LAN (VXLAN) to accelerate hybrid IT (i.e., turn up services quickly).

For more: Solution Brief

5. CHALLENGE: Management headaches

As data centers scale and become more distributed, management gets more complex, especially if multiple management tools serve different needs for different technologies and points of connectivity.

The Fortinet Fabric Management Center (FMC) includes FortiManager combined with FortiAnalyzer to enable an effective network operations center that efficiently manages integrated security architecture with single-pane-of-glass management. The FMC's industry-leading capabilities include centralized management, reporting, analytics, and automation. Teams can also use FMC to easily integrate with third-party tools like Ansible (Automation), Terraform (Automation), ServiceNow (ITSM), Splunk (SIEM), Tufin (NSPM), and many others across large-scale, multivendor deployments.

For more: Solution Brief

September 5, 2020 2:52 AM

760844-0-0-EN

D:\Fortinet\Checklist\758331 - BOFU Data Center Asset\cl-FA-red-bofu-data-center-asset-932020\cl-FA-red-bofu-data-center-asset-932020