FORTINET

Distributed Hybrid Data Centers Require Additional NGFW Capabilities

Table of Contents

FORTINET

Executive Overview

The evolution of modern data centers has led to applications and data being increasingly distributed across hybrid infrastructures. While this helps to enable greater agility for business-critical workflows, it simultaneously expands the organizational attack surface while obscuring visibility and inhibiting controls. Network engineering and operations leaders require integrated security with advanced capabilities designed for protecting hybrid IT data-center environments. Specifically, they need a next-generation firewall (NGFW) that includes critical risk management capabilities, scalability that extends data-center protection across all parts of the organization, resiliency for ensured business continuity, as well as automation and orchestration features to reduce the burden on staff while accelerating response times.

Distributed Data Centers Expand the Attack Surface

Business users now access critical applications from increasingly distributed data centers that extend across a hybrid IT infrastructure. Their workflows and data exist across on-premises, colocations, and private and public clouds—and this broad distribution of vulnerable content creates an ever-expanding attack surface for organizations.

To compensate for these increasing risk exposures, many network engineering and operations leaders have tried adding on individual point security solutions to patch new defensive gaps and to cover evolving regulatory compliance requirements. Unfortunately, this piecemeal approach cannot address the full spectrum of current and future vulnerabilities. The odds of a malicious cyber activity or natural disaster disrupting the business increase, as do the total cost of ownership (TCO) and operational complexity of security for the organization.

The average total cost of downtime is $67.2 million per company over two years, including damage to trust and reputation.[1]

Securing Hybrid IT Environments

To address this expanding data-center attack surface, network engineering and operations leaders must first integrate security across all parts of their hybrid IT environments. They also need NGFW security that ensures end-to-end visibility, policy controls, and intrusion prevention (IPS), along with advanced capabilities for:

- **Performance.** Managing risks requires security that can keep pace with high-performance networks, along with robust features that effectively help to reduce the attack surface.
- **Resiliency and scalability.** As hybrid IT environments expand and diversify, data-center security must provide scalability, resiliency, and availability to ensure reliable business continuity. The overall network and security architecture should also be able to withstand disruptions caused by network outages and natural disasters.
- **Automation and orchestration.** An integrated security architecture unlocks the power of intelligent automation across the hybrid IT infrastructure. Automated security responses and accelerated management features shrink the windows of risk exposure while reducing staff workflow burdens, human errors, and operating expenses (OpEx).

Top concerns about hybrid data workloads include data security/regulatory compliance (71%), performance (62%), and ease of management (53%).[2]

Performance to Manage Risks

Data-center firewalls are typically deployed in the fastest portion of the network. Therefore, an effective NGFW solution deployed in these use cases must be able to apply advanced L7 security with minimal impact on network performance. To achieve this, the solution needs **dedicated security processors** that allow the NGFW to reliably perform security functions without creating a network bottleneck.

Securing a modern distributed data center also requires visibility of all deployed security elements across all the various environments (on-premises, colocations, clouds, etc.), as well as visibility of users, applications, and devices. With over one-third (34%) of breaches now originating from trusted internal sources,[3] access control of the internal network becomes an imperative. Network engineering and operations leaders can achieve this through **network segmentation** that is scalable and flexible enough to address various use cases (including dynamic trust of users, devices, and applications). But stand-alone segmentation by itself cannot provide many critical security functions for today's advanced threats, including content inspection. Therefore, an NGFW deployment for data centers must be able to adapt to various segmentation techniques, be able to communicate with third-party security solutions to share threat intelligence, and also provide content inspection and automated threat protection.

Keeping up with the volume and velocity of today's threats demands security that shares intelligence in real time across an integrated security architecture. At the same time, it should apply artificial intelligence (AI) to identify unknown threats. Most importantly, this **AI-powered threat detection and prevention** must be applicable to digital assets in any and all locations.

77%

of organizations currently rely on nonintegrated point security solutions to some degree within their organization.[4]

Resiliency and Scalability

The ever-expanding nature of digital innovation has a direct impact on security. As data-center workloads become increasingly decentralized across a hybrid IT infrastructure, security demands **elasticity to expand at scale** with new applications and growing workloads—beyond traditional appliances in on-premises locations, into cloud and virtual machine (VM) deployment iterations.

Data-center security must also adapt to address the demands of ever-increasing traffic—both unencrypted and encrypted data flows. More than 72% of total network traffic is now made up of encrypted data—a nearly 20% increase year over year.[5] Greater volumes of encrypted traffic require advanced visibility via HTTP and HTTPS traffic inspection tools.

Distributed data centers are especially vulnerable to threats moving secretly in encrypted data flows. Mitigating this requires security that provides advanced **secure sockets layer (SSL)/transport layer security (TLS) encryption inspection** (as well as sandboxing and decoy/honeypot integration) for vast amounts of traffic moving between users and systems as well as across systems—without impacting application performance. This should include the latest **TLS 1.3** inspection capabilities.[6]

In terms of resiliency and availability, the solution must ensure system real-time failover in the event of a component failure. Built-in **N+1 clustering** offers a fully redundant architecture to eliminate any single point of failure. **Third-party validation testing** by independent industry experts also helps to ensure reliability of the solution under real-world conditions.

60%

of encrypted traffic contains malware;[7] 28% of breaches involves malware.[8]

Automation and Orchestration

The ongoing cybersecurity skills shortage places many understaffed security organizations under heavy workload burdens. Reducing operational complexity is the key to limiting OpEx costs and freeing up technical security resources to focus more on business outcomes and achieving optimizations rather than on manual tasks. In this regard, an effective data-center firewall should include capabilities such as **optimized workflows** for streamlined deployment and management.

An integrated security architecture offers a foundation for intelligence sharing and automated responses that coordinate security across hybrid infrastructures. An NGFW solution that supports **open application programming interfaces (APIs)** enables critical advantages such as workflow automation, orchestration, and synchronized security responses for unpatched applications and ever-changing DevOps environments. The solution should also be able to **apply business logic that establishes continuous trust of users, devices, and applications** to help automate security processes (such as provisioning and access control). This reduces staff workloads and OpEx costs while boosting operational efficiency and security effectiveness.

NGFW features that help **automate compliance reporting and audit processes** can also help network engineering and operations leaders reduce workflow burdens while keeping pace with evolving government and industry regulations, as well as security standards such as the National Institute of Standards and Technologies (NIST) and the Center for Internet Security (CIS).

More than half of IT decision-makers (54%) said talent retention is part of the problem with adopting a hybrid model.[9]

Choose Integration Plus Best-of-Breed NGFW Firepower

An organization's attack surface expands as data centers become more distributed and evolve to a hybrid IT approach. And despite a demand for ever-increasing levels of data-center performance, network engineering and operations leaders cannot compromise between security and meeting user demand. In the face of growing risks, increasing chances of network outages, and rising costs, organizations must revisit security for modern data centers.

To deliver both security and performance, network engineering and operations leaders must embrace an integrated security architecture based on a robust NGFW solution—one that delivers performance, resiliency, scalability, and automation capabilities.

[1] Filip Truta, "Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation," Security Boulevard, February 21, 2019.

[2] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model," TechRepublic, November 15, 2018.

[3] "2019 Data Breach Investigations Report," Verizon, April 2019.

[4] "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.

[5] John Maddison, "Encrypted Traffic Reaches A New Threshold," Network Computing, November 28, 2018.

[6] Alex Samonte, "TLS 1.3: What This Means For You," Fortinet, March 15, 2019.

[7] Omar Yaacoubi, "The hidden threat in GDPR's encryption push,"PrivSec Report, January 8, 2019.

[8] "2019 Data Breach Investigations Report," Verizon, April 2019.

[9] Alison DeNisco Rayome, "91% of tech leaders say hybrid cloud is 'ideal' IT model," TechRepublic, November 15, 2018.

FORTINET

www.fortinet.com

472724-0-0-EN

November 12, 2019 1:28 PM

eb-advanced-ngfw-security