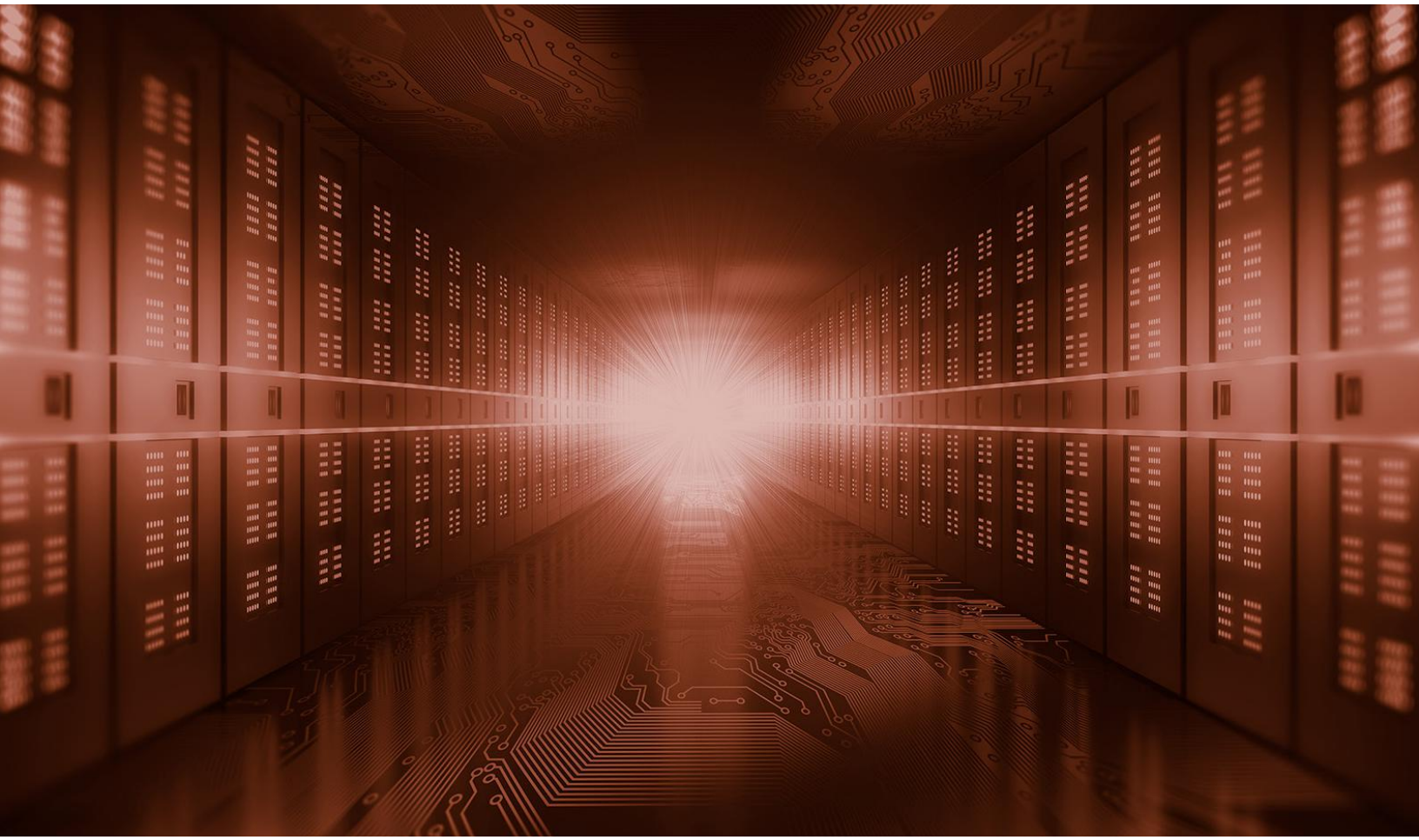
FORTINET softwerx

THE NEW PARADIGM IN NEXT-GENERATION FIREWALLS

Fortinet Modernizes Data-Center Security from the Edge to the Core



Today's data center is more than just the building where the servers reside. It's a dynamic entity spanning both physical and virtual resources. The data-center model itself has evolved from one where hard-wired connections drew a direct line to a stand-alone system, to a utility model, where users log into resources via wireless connections and care little about the who, what, and where of the processing power they harness. While this has dramatically increased the productivity and flexibility of the users, who rely on computing access, it has turned security into the cyber version of "whack-a-mole"—with security professionals chasing new threats as they emerge from an expanding attack surface.

How practitioners view security has evolved as well. Security had long been thought of as an activity at the edge of the network. Protect the points of entry into the network, and you've done your job. But threats have changed in type and sophistication. Hackers penetrating the perimeter now roam the network for days or weeks, quietly searching for the right opportunity to breach critical data. This means the threat has expanded to the core of the data center, where data moves between trusted systems, behind the point products that may have failed to stop the intrusion at its point of entry.

At the core of the data center lies the network. In fact, some might argue that the network has become the data center. Virtualization and cloud have shifted compute resource into the realm of shared systems, connected to each other and the outside world dynamically. The data center itself now manifests as more of a fabric of connections than a physical space.

The Internet of Things (IoT) has added a greater level of complexity as well. Thousands, perhaps millions, of devices that were never considered part of the network are now "on the network." Some devices are smart and are "security ready," capable of loading firmware or running security protocols on runtime operating systems, but for the vast majority of these devices, security was never even considered. The IP camera in a conference room or the cable/Internet box in a production room. These devices expand the surface area of the network to the point where even with the best perimeter protection, threats will get through. The imperative has become not only protecting the network at the edge but protecting the core as well.

FORTINET MEETS THE CHALLENGES OF DATA-CENTER MODERNIZATION AND SECURITY

With the acceleration of digital transformation comes the need for increasing bandwidth and performance on the network. Today, with even more traffic flowing east/west (within the data center, system to system) as is flowing north/south, every upgrade within the data center to improve network performance and capacity has security implications. The sheer increase in the volumes of data moving to meet application requirements increases the likelihood of a breach. A security professional must keep several critical elements in mind when considering modern data-center security.

SPEED AND BANDWIDTH

As the data center and the network are upgraded to accommodate new requirements of speed and bandwidth, security must be an enabler, not an inhibitor to this new performance paradigm. Technologies to protect the core and internal segments of the data center must not be the bottleneck. When choosing technologies, consider the approach taken by Fortinet. Fortinet offers dedicated security processing power to minimize the performance impact of even the most demanding functions. For example, users are moving rapidly to migrate to a 100GB network core. This opens up enormous possibilities but brings with it exposures. At those throughput levels, security solutions must keep up with processing mountains of data and different traffic types, without adding latency or decreasing the speed of access. It also means malware has more places to hide in an ever-increasing data stream, and threats proliferate throughout systems on the network even more quickly. This requires advanced threat protection be matched with dedicated processing.

NETWORK DESIGN

New network designs are becoming flatter and less hierarchical, harkening back to the days of two-tier networking. In many networks, traffic between systems now far outpaces the traffic coming in and out of the network. This means the network is scaling wider, to accommodate virtualized systems and traffic closer to the core. Traditional three-tier networks, oriented toward north/south traffic, aren't meeting the challenge, driving network designers to embrace two-tier leaf and spine topologies to reduce latency between systems. All of this increases the throughput requirements inside the data center. This along with IoT is expanding the threat surface and requires a fundamental rethinking, away from disparate best-in-class point products to the Fortinet approach of an intelligent security fabric that works together across all components, shares intelligence, and learns as it encounters new threats.

CONSOLIDATION

Consolidation driven by cost savings and green data-center initiatives is impacting the way security professionals think about and address security. Pressures to reduce power consumption are driving all hardware components in the data center to be more compact, modular, and energy-efficient. Security solutions must adapt to these expectations not only in physical footprint (think modular chassis) but also address the functionality issues presented by larger and larger server racks that may consist of virtualized systems, each needing a different security profile. This consolidation trend also extends to the way in which customers want to invest in technology. Point products are difficult to manage and integrate. Solutions that combine both management and physical space across security functionality allow not only for the consolidation of physical resources but the management of security in an intelligent fabric from a consolidated dashboard

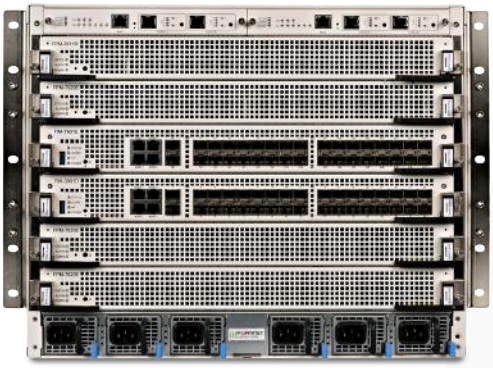
THE FORTIGATE ENTERPRISE FIREWALL DELIVERS SECURITY TO THE CORE OF THE NETWORK

To meet today's requirements, Fortinet has delivered the FortiGate series of Enterprise Firewalls for the Data Center. The FortiGate series provides options at multiple price points for scalable price/performance to address many use cases and is powered by the FortiOS Operating System, providing advanced threat intelligence. Designed for the most demanding levels of performance, purpose-built security processors deliver superior price/performance and match the demands of the new data center, without compromising latency for security. Available with multiple 100 GbE interfaces and throughput of more than 1 Tbps, the FortiGate also provides a fully redundant architecture to eliminate any single point of failure.

Because a data-center firewall typically is deployed in the fastest portion of the network, dedicated processors are essential. With analysts estimating that nearly 50% of the SSL traffic traversing the network contains hidden malware, the data center becomes vulnerable to threats moving secretly in encrypted data flows within the network. Mitigating this requires a solution which can handle inspecting the vast amounts of east/west traffic moving between systems, without impacting application performance. Also, security processors provide the power required to address SSL key exchange, IPS signature matching, and Suite B cryptography without a performance penalty.

The FortiGate series of data-center firewalls addresses the core functions any enterprise class firewall must deliver, including policy enforcement, application control services, and intrusion-prevention services. In addition, the FortiGate series provides granular policy control of users, devices, and applications, as well as SSL inspection and sandboxing, all at the network core.

At the highest end of the spectrum sits the FortiGate 7000 series, delivering a market-leading 100 Gbps NGFW throughput, 120 Gbps IPS throughput, and 80 Gbps threat protection throughput. For customers moving to IPv6, for example, this means no performance penalty for handling these transactions. Systems are capable of handling up to 320 million concurrent sessions and are flexible enough to be deployed as a next-generation firewall (NGFW) or as a data-center firewall for the edge or internal segments. The system offers both the simplicity of an appliance combined with the modularity of a chassis, so you can scale up as demands change. This flexibility extends to initial configuration as well. Systems come preconfigured for a variety of network needs and can be quickly deployed to handle the data-center edge and core, the enterprise edge, or for securing internal segments.



FortiGate 7060E Next-Generation Firewall for the Data Center

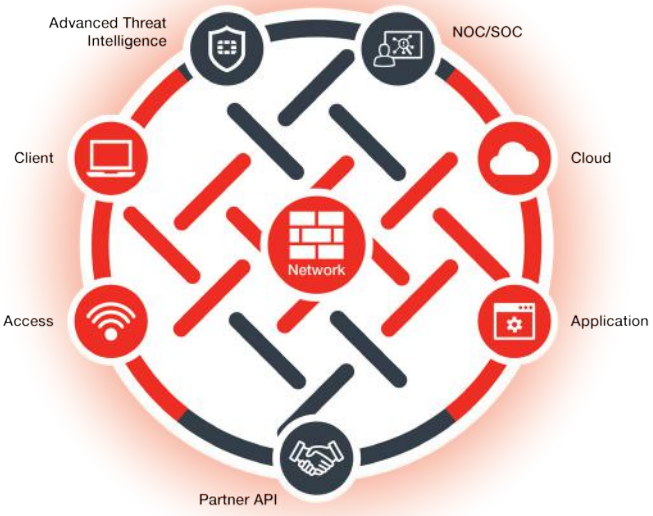
As an NGFW solution, the FortiGate series provides the flexibility to protect at the data level as well as the perimeter. It's not enough to simply defend against entry into the network. It must be assumed that threats will get through. Classifying data to be protected and gaining visibility into the data flow within the data center are paramount to stopping the attackers who have been lurking in the network for weeks, bouncing from system to system seeking targets.

Lastly, the FortiGate series provides not only best-in-class NGFW functionality; it operates as an element of a comprehensive security fabric to protect the enterprise. Traditionally, security approaches have been geared toward the deployment of point products to tackle a certain element of overall security. This has led to environments where individual products perform their function but do not share information or share a common management interface. Threats emerge too quickly not to have seamless visibility across all elements of the security landscape. For example, when malware is detected by the FortiGate Firewall, that information is dynamically shared across the entire security fabric, so the rest of the network learns immediately what the threat looks like and can counter. The Fortinet Security Fabric tying together all security elements is built around three key attributes:

Broad—The security fabric covers the entire attack surface, including the network, endpoints, applications, access, and the cloud. It extends from the perimeter all the way to the core.

Powerful—Components of the security fabric employ security processors to shift the burden off of the rest of the infrastructure, so as not to impact performance.

Automated—The security fabric enables fast response to threats where all elements can rapidly exchange information and coordinate responses.



The Fortinet Security Fabric integrates solutions beyond the enterprise firewall, including cloud security, advanced threat protection, application security, secure access, and security operations—all managed and coordinated from a single interface. This unified approach allows for seamless management and threat intelligence sharing across all components of the security architecture.

CONCLUSIONS

The threat landscape of today demands more than ever from security technology. With the network at the heart of the modern data center, and applications and use cases demanding higher and higher levels of performance and bandwidth, it's simply not possible to compromise between security and meeting user demand for access. Fortinet solutions, including the Enterprise Firewall, deliver the highest level of performance and the most advanced threat protection. They address the perfect storm of volume and speed that will overwhelm all but the highest-performing solution, with the most advanced threat intelligence.

When looking at modernizing the data center to meet the challenges of digital transformation, Fortinet solutions tied together with the Fortinet Security Fabric will serve as the unifying force to combat threats from the core to the edge of the network to the cloud.

FORTINET
softwerx

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990

102403-1-A-EN July 28, 2017 8:16 AM
Macintosh HD:Users:mbunnell:Documents:Egnyte:Shared:CREATIVE SERVICES:Team:Michael-Bunnell:WP-Data-Center-Security:wp-data-center-security_072717_214pm