Securing the Private Cloud

Advanced Threats Require Advanced Security

Bigger Breaches, Higher Stakes

In the wake of recent headline-grabbing data breaches, FBI Director James Comey's oft-quoted statement rings especially true:

> *"There are two kinds of big companies in the United States. There are those who've been hacked…and those who don't know they've been hacked."*

Year after year, the list of high-profile data breaches gets longer. Attackers range from nation states to unknown cybercriminals, all with varied and sophisticated strategies. Regardless of the perpetrator, vector, or techniques employed, these events share one common element: vast amounts of data were stolen and exfiltrated.

As data center architectures evolve to improve efficiency and take advantage of the latest advances in software-defined networks, virtualization, and cloud infrastructure, security solutions need to not only keep up but stay ahead of the threat curve. They must also have the performance and throughput characteristics to support the latest data center requirements and anticipated needs in the years to come.

New Architectures, New Vectors

Traditionally, private clouds relied on extensive internal routing, physically separated servers, and completely self-contained operation. Architectures were heavily tiered and operational access was necessarily limited to IT.

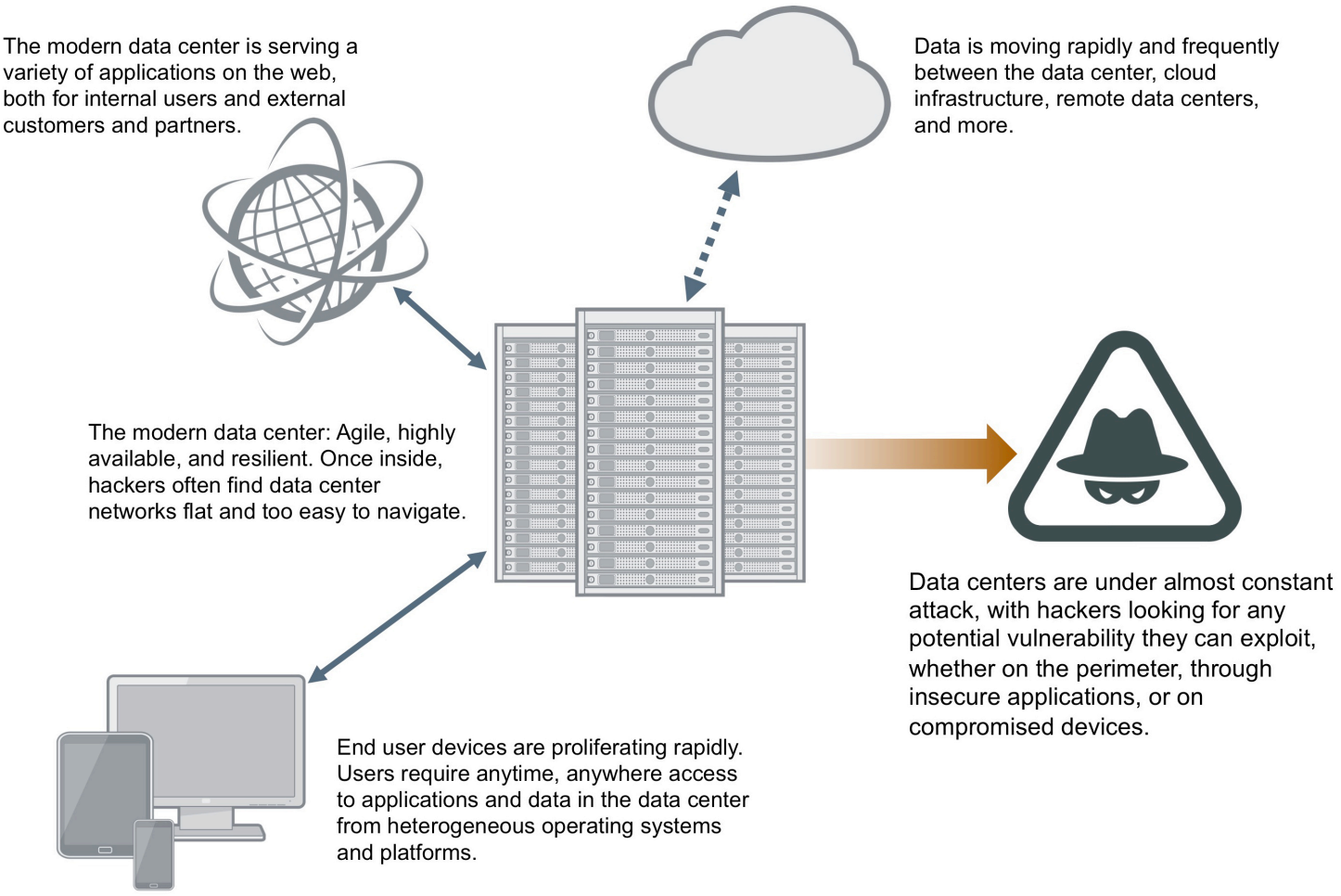
Fast-forward to today, though, and the purpose, operation, architecture and functions of the modern data center have fundamentally changed to a private cloud approach:

- Networks are now much flatter to accommodate the shift from client-server applications ("north-south" traffic) to high volumes of server-to-server ("east-west") communication.
- Servers, storage, and even networking functions are highly virtualized, making the concept of physically separate servers (and potentially separate security measures) irrelevant.
- BYOD, remote access, employee- and customer-facing applications, DevOps, and SDN have increased and diversified demands.
- All of this amounts to a simpler architecture for hackers to compromise once they've breached the perimeter and a larger attack surface through which they can infiltrate private cloud resources.

New Architectures, More Speed

In today's highly virtualized data centers, more workloads running on fewer physical machines are driving requirements for much higher core network speeds. Interconnected cloud architectures also demand greater performance at the network's edge. All this, in combination with the move to IPv6 and application- and service-oriented architectures, is driving the need for cloud security hardware that supports:

- High-density 10GbE ports
- 40GbE/100GbE high-speed ports
- Core network speeds in excess of 100Gbps



Building a Secure, Scalable Private Cloud

The rapid evolution of the cloud, as well as changing business needs, have resulted in dramatically different security requirements from legacy applications. At the same time, operators are pushing the envelope on performance. Security, however, cannot take a back seat to performance considerations.

Performance and Security Are Not Mutually Exclusive

Exceptional performance is critical to the scalability and varied functions of the private cloud. Achieving the necessary throughput (both on the LAN and via WAN connections) requires perimeter protection and internal security measures that are fast enough to deeply scan traffic and remediate threats at wire speeds.

Where legacy data centers relied on their architecture, perimeter defenses, and a far less complex threat landscape for protection, new data centers must employ extremely high-performance firewalls and move protection closer to their cores to balance security with agility, speed, and scalability. These new devices can be configured with multiple 100 GbE ports to physically segment the core network without introducing additional core switching mechanisms. Others employ replaceable modules that let operators choose dense 10 GbE ports or scale to 40/100 GbE.

In all cases, custom ASICs (application-specific integrated circuits), purpose-built for security processing, allow these units to achieve sustained throughput of up to hundreds of gigabits per second while minimizing latency. COTS processors simply can't deliver equivalent throughput while also implementing a variety of next-generation firewall functions and operating flexibly in either core or edge deployments.

Best Practices for Private Cloud Security

While the reasons for upgrading firewalls are many, the most common reasons relate to performance in high-speed network environments and convergence of security functions. Hardware alone, though, won't deliver the necessary combination of

performance and security. As organizations look to upgrade existing facilities, several best practices have surfaced that address emerging security threats. Taken together, these best practices, next-generation hardware, and robust management ecosystems can avoid bottlenecks while deeply scanning network traffic and ensuring the safety of data and applications.

The Security-First Mindset

Security cannot be an add-on or an afterthought when architecting private clouds. Because of the threats to which networks are exposed and the high value of the data and applications they house, security must be baked in. This means leveraging high-performance, high-port-density next-generation firewalls, as well as conducting ongoing vulnerability assessments.

Balance Security and Performance

The current (and future) threat landscape doesn't mean that data centers should disregard performance considerations in favor of security. Instead, operators need to identify best-of-breed appliances and the appropriate network architecture to maximize both.

Next-generation firewalls that can integrate with software-defined networks and be as agile as the data centers they are designed to protect can deliver equal measures of performance and security. These appliances should also leverage hardware and software custom-designed for security applications and optimized for performance.

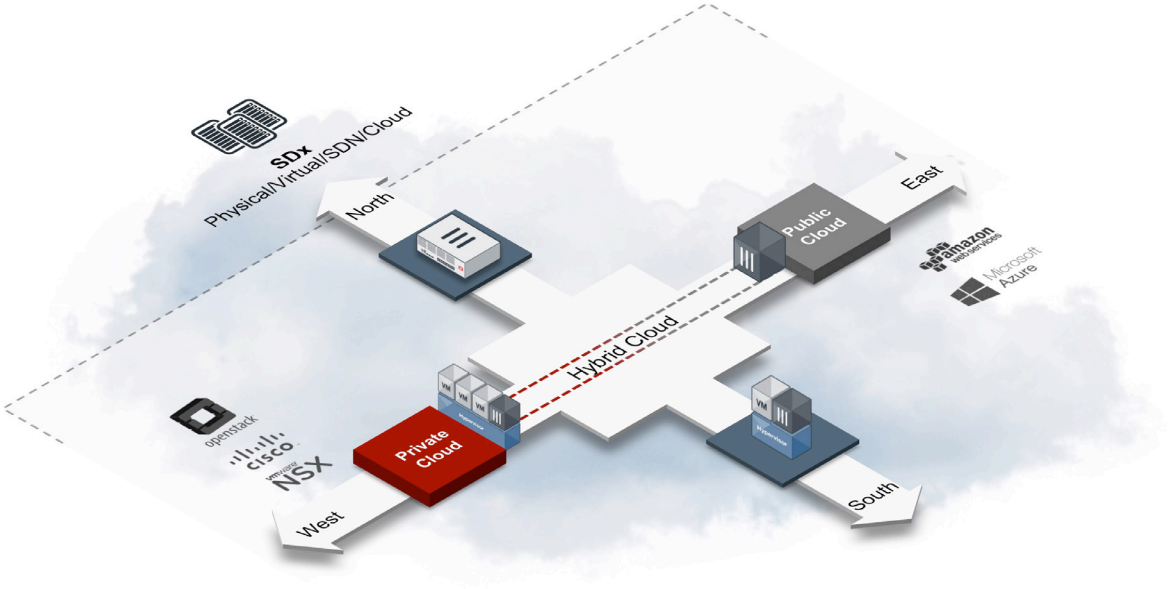


FIGURE 2: The enterprise data center is part of a much larger IT ecosystem that must be able to securely access its applications and resources.

Virtualization Awareness

While there are many firewalls on the market today, not all are designed to be aware of virtual environments and the nearly instantaneous changes that can occur in highly virtualized networks. Reliance on legacy approaches to routing or a lack of built-in support for software-defined networks and orchestration will leave critical vulnerabilities open in the agile data center.

Orchestration and Automation

As organizations provision workload instances and networks more elastically in private clouds, security provisioning must be automated and coordinated by orchestrating security management with SDN controllers, hypervisors, and cloud management to deploy security policies at the right place and right time in these very agile, dynamic environments.

Converge Devices

The next-generation firewall promised the ability to combine many different security functions in a single device, reducing complexity and simplifying management and deployment. However, as more security features were turned on, performance often suffered, making them less suitable for data center applications. Now, though, appliances with purpose-built ASICs and custom software can deliver converged security with outstanding performance.

Build for Multitenancy

Modern, highly virtualized environments must often support multitenancy with the ability to differentiate security policies by user, application, etc. Firewalls that natively support virtual domains (VDOMs) and logical network segmentation give

operators highly granular control over the network while still retaining flat, performance-optimized architectures.

Securing the Edge Isn't Enough

Finally, continuing to rely on edge protection is no longer sufficient to mitigate advanced threats. Instead, moving protection closer to the core and deploying additional internal firewalls, all under central management and control, ensures:

- Faster detection and protection
- Stronger defenses against internal threat through segmentation
- Higher performance from a more robust security solution

Conclusion

The demands on the modern private cloud all too often leave operators in a position of favoring performance and agility over security. Throughput at the edge and within the core network is of paramount importance with these facilities relying heavily on cloud integrations and virtualization. For many, legacy approaches to security haven't kept up with either performance requirements or, more dangerously, a sophisticated threat landscape that has enterprises under nearly constant attack.

The solution is to build security into the network that can accommodate powerful threat detection technologies while maximizing throughput and flexibility. Firewalls and converged security protection deployed closer to the core with high degrees of application and virtualization awareness are key to robust security. While threat coverage must be a top consideration for the private cloud itself, operators should also look to the performance of their firewall solutions and expect third-party validation of performance claims. The right security appliances deployed in the right architecture can deliver stellar performance without compromising security.

About Fortinet

Fortinet is a global leader and innovator in Network Security. Our mission is to deliver the most innovative, highest performing network security platform to secure and simplify your IT infrastructure. We are a provider of network security appliances and security subscription services for carriers, data centers, enterprises, distributed offices and MSSPs. Because of constant innovation in our custom ASICs, hardware systems, network software, management capabilities and security research, we have a large, rapidly growing and highly satisfied customer base, including the majority of the Fortune Global 100, and we continue to set the pace in the Network Security market. Our market position and solution effectiveness has been widely validated by industry analysts, independent testing labs, business organizations, and the media worldwide. Our broad product line of complementary solutions goes beyond Network Security to help secure the extended enterprise.

Fortinet FortiGate data center firewalls deliver NSS-Recommended levels of security effectiveness and ten times the performance of equivalently priced solutions in the industry. FortiGate is the best value on the market with exceptional security and throughput at prices within reach of all organizations.

For more information about Fortinet and our FortiGate line of data center products, visit www.fortinet.com.

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
Valbonne
06560, Alpes-Maritimes,
France
Tel: +33.4.8987.0500

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

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

Copyright © 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 28, 2016