Three Must-Have Security Measures to Empower Data Center Transformation

White Paper

Executive Summary

Because of the pivotal, business-critical role of data centers, an increasing component of the "traditional" data center workload is being shifted to virtualized and nontraditional cloud computing environments. Specialized tactics and additional controls are required to enable safe data center innovation.

Security needs to be adaptive and responsive, securing boundaries while demarcating physical and virtual resources, detecting problems, and enforcing policies. Comprehensive policies need to "stick" to workloads as they are processed—for instance, when a data archive migrates to the cloud. And compliance needs to be proven in auditor-friendly reports.

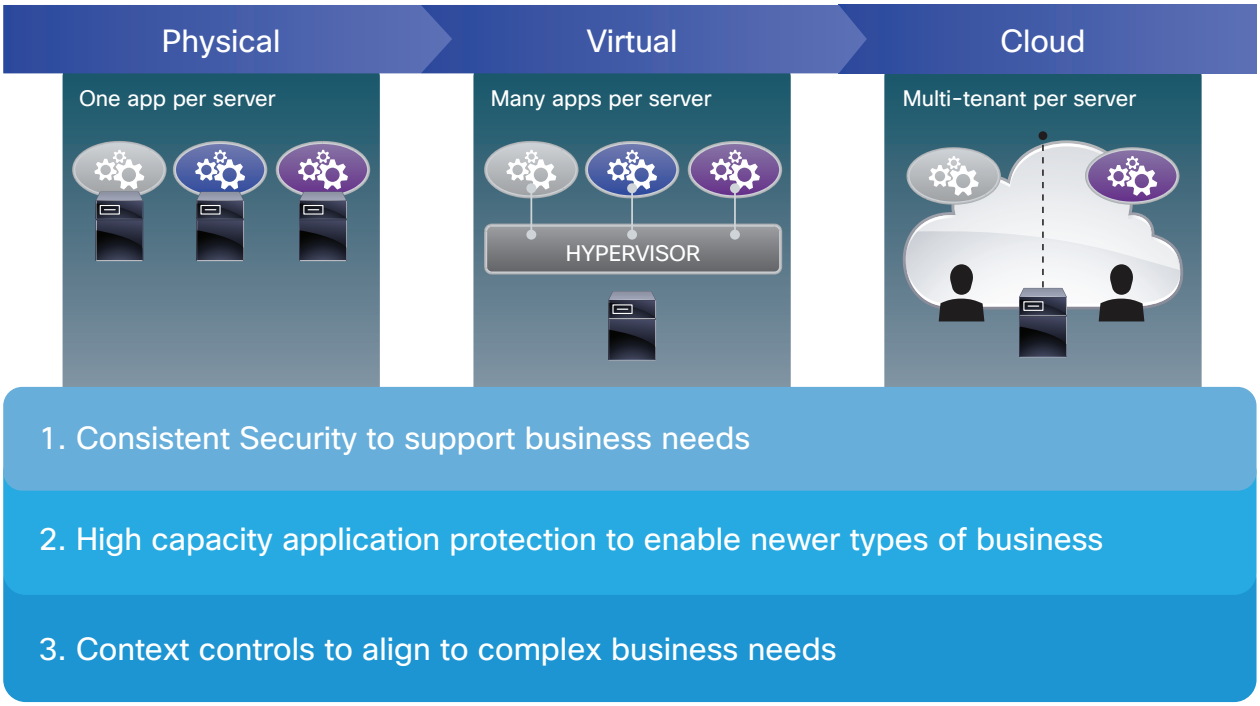
As data centers virtualize and take advantage of the cloud, C-level executives and data center teams will have the opportunity to make security a programmable element that can be seamlessly integrated into the underlying data center fabric. This is an architecture and capability that Cisco uniquely delivers. Cisco platforms allow for security to be easily built in at the design phase rather than being bolted on post-implementation. And Cisco's security architecture eliminates the all-too-familiar tradeoff between business needs and security.

To securely enable data center innovation and to move the business forward quickly, IT organizations must implement the following measures:

1. Consistent security and policy enforcement across physical, virtual, and cloud infrastructures to support unpredictable and rapid business demands.
2. Context-based security controls that are aligned to business requirements to fully support the real-time and complex ways that information is transacted.
3. High-capacity protection for application environments to support the business in adopting new and more capable services.

> "Security is top of mind for our customers. We will continue to evolve and put security into every ASIC, every product, every software capability, and bring that together in a way that no one else can."
>
> —John Chambers, Chairman and Chief Executive Officer, Cisco

Figure 1. The Three Security Must-Haves to Enable Business Innovation Across a Rapidly Changing Infrastructure



Why Security Must Evolve to Support Mission Critical Needs

According to the Cisco Global Cloud Index (2011–2016)[1], cloud traffic will account for nearly two-thirds of data center traffic by 2016. In addition, research from the Enterprise Strategy Group (ESG)[2] projects aggressive server virtualization and greater consolidation of data centers, leading to more multitenant facilities. Organizations are no longer virtualizing commodity workloads; they are starting to focus on mission-critical workloads in order to make their largest and most important applications more efficient.

Conventional security approaches present some challenges that are inhibiting faster adoption:

- Because virtualized applications are decoupled from the underlying physical resources they use, traditional security approaches can lead to traffic bottlenecks, inconsistent network policies, management blind spots, and security loopholes.
- Cloud computing is built around shared and virtualized resources. As a result, it has the same issues that affect virtualization but with an extra set of risks introduced by cloud design, independent personnel, and multiple, unknown tenants sharing virtualized physical resources.

For these reasons, many IT teams are electing to use a hybrid approach, in which an organization provides and manages most resources across an in-house mix of physical, virtual, and private cloud deployments and uses other resources that pose minimal security risk, including externally provided resources such as public clouds.

1 Cisco Global Cloud Index (2011–2016)

2 Data center environmental changes will open the door for technologies like fabric architectures, SDN, and OpenFlow in 2012, Jon Oltsik, Network World, Data Center Networking Discontinuity, January 2012

A Strategic and Architectural Approach to Security

Cisco prepares the customer for any type of physical, virtual, or hybrid data center implementation.

Cisco brings a unique approach to security, using its core strengths across the infrastructure, networking, and security arenas. Security is a programmable element that not only takes advantage of the underlying network infrastructure, but also spans multiple form factors and uses a greater number of enforcement points in the network to speed security decisions and serve business needs without introducing latency.[3] Security is also a unifying factor that enables uninterrupted, trusted information flows from endpoint to server and from user to application. This approach contrasts sharply with what some analysts refer to as "dinosaur" networking capabilities[4] and with the siloed security functions that we typically see in the platforms of other networking vendors

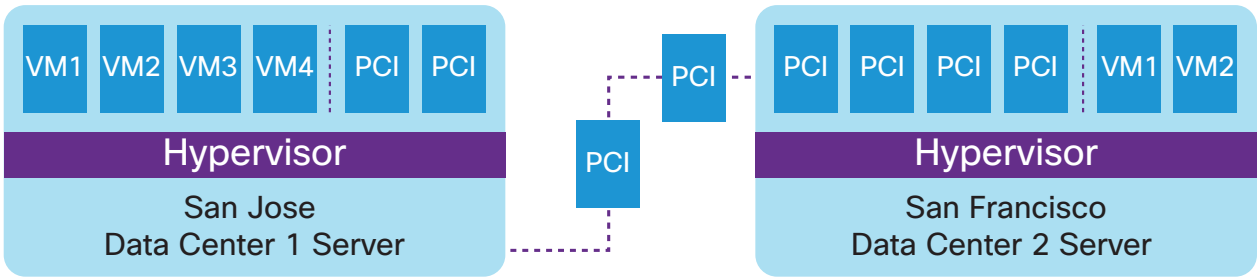
Must-Have #1: Consistent Security to Support Business Demand

Significant advances in technologies have accelerated data center performance and made the data center more responsive to business demands. Higher port densities, faster fabrics, and a unified fabric that breaks down the previous siloes of network, storage, and server computing have resulted in new levels of performance. Similar advances in security are needed to advance the data center to a seamless, hybrid world spanning physical, virtual, and cloud.

Cisco's approach to delivering consistent security across physical, virtual, and cloud environments offers these key business benefits:

- **Centralized security policy leads to greater automation:** A policy framework that is template-driven and has corresponding push mechanisms speeds IT tasks and can enable end users and businesses to process virtual and cloud workloads as part of a self-service model.
- **Consistent security maximizes the efficiency gains of cloud computing:** Consistent security policy attributes applied to templates enable rapid provisioning and scaling of virtual machines. They also mitigate compliance violations such as workloads of different sensitivities running side by side.
- **Dynamic security zoning provides greater flexibility:** Security zones that are based on dynamic policies containing virtual machine and other security trust-level attributes (versus static IP attributes only) can better demarcate physical and virtual resources, enable flexible migration of workloads across physical, virtual, and cloud infrastructures, and pave the way for secure multitenancy.

Figure 2. Dynamic Security Zoning Provides Greater Flexibility, for Example, Secure Migration of Virtual Workloads



3 The Future of Network Security: Cisco's SecureX Architecture

4 Data center environmental changes will open the door for technologies like fabric architectures, SDN, and OpenFlow in 2012, Jon Oltsik, Network World, Data Center Networking Discontinuity, January 2012

> "Context-aware and adaptive security will be the only way to securely support the dynamic business and IT infrastructures emerging during the next 10 years"[6]
>
> –Neil MacDonald Vice President, Distinguished Analyst and Gartner Fellow Emeritus

Must-Have #2: Context-Based Security Controls Aligned to Complex Business Needs

Rapidly changing business requirements and the rise of a mobile workforce have forced IT teams to change user access policies and have introduced new security requirements. Today's users require ubiquitous access to applications and critical assets in the data center. This contrasts sharply with the static data center of a decade ago, when only a trusted few had access to data center resources and when data centers were essentially repositories of information with few data transactions.

Most industry pundits and analysts agree that context-aware security can correctly identify users and help ensure legitimate use. Cisco uses next-generation scanning elements to build in contextual intelligence at multiple enforcement points in the network and provide the following benefits:[5]

- **Anywhere, anytime, secure access for a mobile workforce:** Context-based permutations that factor in who, where, what, and when with more granular dimensions enable more intelligent security access decisions. For example, correlating data such as an employee who is logged into the network from an office building but appears to be accessing a CRM portal from a coffee shop at another location might reveal and help block a potential data breach.
- **Secure data transactions based on business context:** Using programmable elements, security policy can be dynamically extended to encrypt user data based on context. For example, an employee in the finance department accessing the payroll must have their data securely encrypted.
- **Security policy that spans to non-authenticating devices:** Devices such as printers and cameras play an increasing role in business and need to be accounted for, as they also can be a vector for emerging threats.
- **Flexible deployment and multiple security form factors to fit hybrid environments:** A firewall, antivirus engine web proxy, router, and access control policies all work in tandem to share intelligence and to push security closer to the user. Multiple form factors, such as an appliance at an enterprise on-premises data center, a module in a branch office router, or an image in a cloud, support increasingly distributed and hybrid environments.

Must-Have #3: High-Capacity Protection for Applications to Enable Services That Are More Capable

Keeping up with application demand continues to be challenging for IT business leaders and data center teams. Web-based applications are at the core of the business function, enabling businesses to provide services, collaborate with partners, and facilitate employee productivity. The makeup of enterprise applications is changing, with a higher adoption of business intelligence, CRM, custom workflow, and video and web conferencing applications, some of which often hog valuable network bandwidth. But with millions of applications, how do you tell which are legitimate and which are risky? When you add to this the immediacy users expect in their experience of the network, the result is a tremendous strain on network speeds, reliability, and security.

5 The Future of Network Security: Cisco's SecureX Architecture

6 Gartner, "The Future of Information Security Is Context Aware and Adaptive", Neil MacDonald, 2012

By contrast, Cisco enables an uninterrupted chain of trust that extends from the user to the application through a broad array of parameters encompassing context-based intelligence. Cisco applications build in application visibility and control across multiple scanning elements in the data center fabric, as well as intelligent inspection and management of IP packets in high-throughput appliances. Key benefits include:

- **More immediate end-user experience:** By enabling an endpoint (whether a laptop or one of many other supported device types) to automatically find the nearest scanning element in the fabric (for example, a router) and make a seamless connection, Cisco platforms mitigate the network latency and architectural complexity common in most other approaches, where application traffic has to be routed halfway around the world to flow through a Layer 3 firewall.
- **Enhanced visibility and control of application usage:** The intelligent inspection of network packets, together with context-aware security, helps to ensure that applications can be quickly classified so that any associated malicious activity or untrusted elements can be blocked.
- **Improved network capacity management:** A high number of connections per second and of maximum connections better assures IT of the back-end server flows needed to support business needs. Additionally, the range of actions that can be taken includes using current network conditions to determine whether to allow the session to proceed or throttle back bandwidth for overall increased application performance.

The Road Ahead

Cisco's approach to security helps to speed implementation with validated designs and reference architectures that can accelerate the time it takes to deploy a hybrid data center model. Cisco uniquely supports customers with programmable security that integrates into the underlying data center fabric at the design phase of a project, rather than being added on at a later stage. Customers benefit from solutions built to maximum performance and to reduce operational and hardware footprints. A vast partner and integrator ecosystem enables customers to easily integrate security across a rapidly changing infrastructure. With continued innovations in networking and security, IT leaders can feel confident that Cisco will empower them to transform their data centers into a hybrid structures that will securely serve future business requirements.

For More Information

For more information on Cisco Secure Data Center solutions, please visit www.cisco.com/go/securedatacenter.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C11-720386-00 12/12