IDC SOLUTION BRIEF

Assessing the Business Value of SDN Datacenter Security Solutions

Sponsored by: Cisco

Pete Lindstrom
Matthew Marden
Richard L. Villars

May 2015

Overview

CTOs, CIOs, and application architects need access to datacenter facilities capable of handling the broad range of content serving, Big Data/analytics, and archiving functions associated with the systems of engagement and insight that they depend upon to better service customers and enhance business outcomes. They need to enhance their existing datacenters, they need to accelerate the building of new datacenters in new geographies, and they need to take greater advantage of advanced, sophisticated datacenters designed, built, and operated by service providers. IDC terms this business and datacenter transformation the shift to the 3rd Platform.

Today, virtually all business innovations are based on the 3rd Platform, with hundreds of thousands to millions of high-value, industry-transforming solutions and services that will alter the end-customer experience. This change affects all elements of the IT organization, including procurement, design, operations, development, and long-term data and asset management. This new datacenter world is more dynamic, more data intensive, and more fraught with business risks that must be addressed and overcome. As a result, the next-generation network architecture is a critical consideration.

This new architectural model must address the technological and operational limitations of traditional network architectures and meet the datacenter requirements of 3rd Platform workloads. For example, software-defined networking (SDN), which features a decoupling of the network control plane from its data-forwarding plane, was conceived as a means of giving the network the agility and flexibility required by organizations building cloud computing environments.

Cisco's Application Centric Infrastructure (ACI) seeks to address the datacenter operator's need for automated provisioning, programmatic management, and comprehensive orchestration. Rather than decoupling the control plane from the data plane, ACI applies a policy model designed to capture application requirements and automate deployment across the network, regardless of whether the applications are virtualized or running on bare metal. This approach is what Cisco calls a declarative management model, which involves the voluntary cooperation of individuals or agents that publish their intentions via commitments to each other. The intentions are abstract; thus, for example, an application policy would state its requirements, and the underlying infrastructure (e.g., datacenter switches) would interpret how best to satisfy those requirements based on their inherent capabilities.

Another networking option for cloud computing is provided by OpenStack, which provides a default framework — called Neutron — for customers to consume networking services, as well as a set of northbound and southbound APIs. The OpenStack networking model features a modular architecture,

giving each customer the flexibility to select a back end that is suited to its requirements. Some customers start with the default reference implementation but then adopt vendor-provided extensions as warranted by their use cases and networking needs.

Key Forces Shaping Datacenter Change

Many external factors have a direct or an indirect impact on datacenter operations and investments. They come from business, social/cultural/political, and technological realms:

- **Business:**
  - **Everything as a service:** Shifting models for financing physical and digital assets drive the restructuring of internal budgeting, cost, and investment practices.
  - **Industry digitization:** The transition from a physical business model to a digital business model dramatically changes data growth rates, performance needs, and functional IT requirements.
  - **Business entanglement:** Extended business ecosystems drive standardization of interconnection and data sharing across organizations and industries.
- **Social/cultural/political:**
  - **Data use norms:** Individual beliefs and government policies about collection, retention, and use of personal data and intellectual property become volatile and fragmented.
  - **Data exploitation:** Nations, corporations, and organized crime entities institutionalize cyberwarfare.
  - **Customer interaction/engagement:** Social media creates a venue for direct customer-to-business and direct customer-to-customer engagement, which creates a constant requirement for fresh and updated information.
- **Technology:**
  - **Modularized IT:** Cloud, converged, software-defined, and hyperscale packaging models change the purchase and management of the basic units of IT.
  - **Data gravity:** Data used to engage with customers and gain business insight is increasingly generated, collected, and archived in service provider datacenters.
  - **Variable IT:** Demands for IT to support short-lived mobile campaigns and analytics efforts force businesses to purchase/deploy/redeploy capacity on short notice and for short time frames.

The realignment and rebalancing of datacenters and IT assets that these forces are spurring also have major implications for organizations' existing wide area networks. Organizations will need to change existing connection paths to link internal datacenters with third-party facilities. They must also deal with significant changes in traffic volume and traffic variability as businesses seek to move large volumes of information between many locations in less predictable patterns.

The Role of Security in the Modern Datacenter

A key factor underlying these drivers and fast-evolving datacenter workloads is the need for greater agility and flexibility related to datacenter security. In each use case, security means something different – integrity, fidelity, visibility, content control, and data control. IT organizations need a common platform that they can use to quickly and reliably set, reset, and extend a broad spectrum of security functions within datacenters and across the entire organization.

At the network level, inline security functionality consists of monitoring capability (intrusion detection), policy-oriented segmentation (firewalls), and communications encryption (virtual private network). However, enterprises often treat datacenter resources as a unit, making no distinction among usage or risk levels. This approach allows enterprises to put all resources into a single large "zone" and focus their protection on the perimeter ingress/egress points (sometimes called the "north" and "south" access points to the datacenter).

As datacenters grow and evolve into multifaceted collections of resources providing many different functions for separate lines of business, multiple user constituents, and varied platforms, security must evolve to be able to protect these more dynamic, richer resources against more focused threats. Enterprises must consider how to address the way resources are shared and how the communications are monitored and encrypted at a more granular level.

The modern datacenter must evaluate how to deploy its intrusion detection and prevention systems as well as its firewall segmentation to determine where existing controls should be redeployed and whether new capabilities should be added to cover the "east" and "west" communications that occur among servers and other resources. A part of this exercise involves identifying smaller collections of resources, typically at the application level but having other possible delineations as well, and inserting more monitoring and policy controls to manage the traffic between applications.

As more controls are deployed throughout the datacenter, centralized management capabilities become a key requirement. As the resources being protected become increasingly dynamic in their location and use, security functions must adapt to the new architectures.

This IDC Solution Brief leverages IDC research among users of security products in the changing datacenter landscape and quantifies the business benefits they can achieve, including 33.5% more productive IT security staff operations, 80.7% less unplanned downtime because of security breaches and threats, and 63.8% faster deployment of security for new applications and services. On an annual basis for an organization with 1,000 users, this leads to improved reliability worth $48,700, IT staff efficiency gains worth $71,700, and productive time from improved operations worth $92,600.

Business Benefits of Security Solutions for Next-Generation Datacenters

Security solutions for next-generation datacenters must enable organizations to generate maximum business value from their investments in these datacenters. This requires that such security solutions drive value by being integrated, policy based, robust, agile, and scalable. Well-designed and well-implemented security solutions with these characteristics create value by saving time and effort for management and provisioning of security solutions, by reducing the operational and business impact of security threats, and by ensuring that security does not inhibit the datacenter's ability to support and drive the business. As a result, such security solutions enable next-generation datacenters by being:

- **Integrated for efficiencies and reduced risk.** Security products that integrate both with solutions supporting organizations' traditional datacenter environments and with other security products being used in the next-generation datacenter environment generate time savings and reduce risk. This occurs as integration minimizes the time security teams must spend redoing policies, breaks down costly and inefficient IT security silos, and reduces the time during which applications and services are exposed to potential security threats.

- **Simplified to ease burden of management.** Security products in next-generation datacenters are employed in environments that rely on automation and orchestration. To fit within such an environment, security products should also be policy based to enable their provisioning as a service. This not only supports the overall architecture of next-generation datacenters but also increases the productivity of IT security staffs when they spend less time on hands-on administration and management of security settings, configuration, and deployments.
- **Robust capabilities to minimize the impact of security threats.** Security products in next-generation datacenters must provide a full spectrum of security capabilities with coverage for all traffic entering, leaving, and moving within the datacenter. This helps organizations minimize the user and business impact of security threats, giving productive time back to users and keeping business disruptions to a minimum.
- **Agility and scalability to support the business through applications.** Next-generation datacenters are configured to enable business operations by speeding up application development cycles and easing the burden of managing applications. To support this objective, security products need to be deployable on an as-needed basis and in the minimum time possible to support efforts to speed the time to market for applications and services.

Cisco Application Centric Infrastructure

Software-defined networks separate control plane functions from data plane functions and are often defined in narrow technical terms. Software-defined security leverages the philosophy and fundamental architecture of SDN but broadens the opportunity by integrating into more environments. The SDN "hub and spokes" approach ties together a controller where security policies are defined and evaluated with enforcement nodes that implement the policies, all done dynamically and in real time. Leveraging a policy language that is abstracted to the application layer enables applicable policies to be applied at the appropriate enforcement nodes to maintain flexibility and alignment with the components of the application in use. The result is a security architecture that is easier to manage efficiently and an opportunity for maximum effectiveness.

Cisco's Application Centric Infrastructure is designed to address the data and security needs of the modern datacenter. It is managed by a central controller, the APIC. The APIC maintains control over all datacenter security devices, both physical and virtual, so they can be managed closely and aligned with the resources they are intended to protect. This controller can provision and manage Cisco network and security devices, supports an ecosystem of third-party security vendors, and is building in more capabilities for additional third-party support.

With its ability to leverage an organization's existing security architecture, Cisco ACI provides a way for enterprises to maintain their existing investment in physical security controls while adding more functional controls in hardware or virtual machines to protect increasingly important east-west communications. To address the dynamic resources of a modern enterprise, policies can be created and matched to an application profile and then distributed throughout an environment. In this way, when resources are moved, the correct policy moves with them.

For organizations that already have a significant investment in Cisco security solutions and an established set of existing security policies, ACI provides a way to securely evolve a datacenter architecture rather than completely overhaul it. At the same time, it can address the newer needs of virtualized and distributed architectures to ensure that an appropriate level of security can be provided to the enterprise.

Quantified Business Benefits of Security Solutions for Next-Generation Datacenters

Table 1 presents metrics for business value that organizations can achieve by using security solutions in next-generation datacenters, based on ongoing IDC research.

Figure 1 presents the annual value of IT staff and user productivity improvements related to the use of security solutions in next-generation datacenters for a 1,000-user organization.

TABLE 1

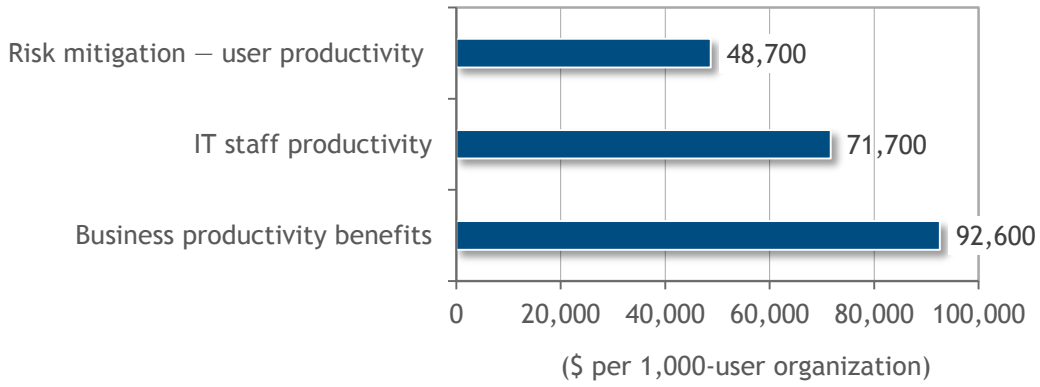
Improvements Related to Use of Security Products in Next-Generation Datacenters

	(%)
IT staff productivity benefits	
Reduced time for security management	33.5
Increase in security threats proactively identified	50.9
Reduced time to respond to security threats	82.1
Risk mitigation — user productivity benefits	
Unplanned downtime reduction	80.7
Business productivity benefits	
Reduction in time to deploy security	63.8

Source: IDC, 2015

FIGURE 1

Typical Annual Benefits for a 1,000-User Organization Using Security Solutions in Next-Generation Datacenters



Source: IDC, 2015

Appendix: Methodology

IDC compiled the data used in this document from interviews it conducts every year with organizations using security solutions for their datacenters. Business value results were normalized by expressing them in terms of dollar benefits for an average organization with 1,000 IT end users.

To quantify benefits related to IT staff operations, IDC multiplied time savings and efficiencies by an average annual loaded salary of $100,000 while using an average annual loaded salary of $70,000 to quantify time savings and productivity benefits for other non-IT staff employees.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com