IDC SOLUTION BRIEF

# Assessing the Business Value of the Secured Datacenter

Sponsored by: Cisco

Pete Lindstrom
Richard L. Villars
Matthew Marden
December 2014

## OVERVIEW

The world of IT is in the midst of a massive structural shift – from the enterprise-centric, client/server-based "2nd Platform" to what IDC calls the "3rd Platform" era built on a foundation of mobile, social, Big Data, and cloud technologies. Today, virtually all business innovation is based on this new platform, with hundreds of thousands to millions of high-value, industry-transforming solutions and services that alter the end-customer experience being built on this new platform. The three characteristics that define datacenters in the 3rd Platform are:

- **Scale**: Supporting up to 10x increases in supported users and/or data sets without comparable increases in datacenter footprint
- **Speed:** Creating and updating applications and services in weeks/days, not years/months, without increasing IT operations and development staff levels
- **Scope:** Enabling the coordination of multiple applications and data sources, internal and external, to deliver new services to customers without sacrificing data integrity and user experience

In this world of mobile, social, cloud, Big Data, and intelligent industries, the datacenter can no longer just be the place where an organization keeps its servers and stores its corporate data. It's the first point of contact with the organization's customers, so the datacenter must provide the most reliable and secure services. The datacenter is the foundation for new business models in a growing set of industries.

With the change in datacenter architectures and use cases in reaction to these developments, datacenter security concerns are becoming top-of-mind for organizations. With recent high-profile breaches at some of the largest retailers and financial institutions worldwide, there has been an increase in awareness, rising to the executive and even board levels. Next-generation firewalls, sandbox solutions, secure Web gateways, and other solutions help address these concerns at the perimeter. However, the datacenter presents a different set of problems that security solutions must address.

First and foremost, the management and provisioning process is vastly different at the perimeter versus at the datacenter. As mentioned above, the dynamic nature of today's datacenter requires security solutions that can support policy management and scalability in an environment where new

resources are constantly created, shifted, and torn down. Asking administrators to manually complete these tasks is not an option, and typically leads to a breakdown in the security posture. Security solutions must be tightly integrated with the other components of the datacenter fabric to ensure a consistent approach and streamlined orchestration.

Additionally, many datacenters leverage a wide variety of technologies. Only a few organizations are able to build their datacenters from scratch and, as a result, most have a mix of new and legacy systems and applications utilizing both physical and virtual resources. Consequently, security solutions must address both today's disparate environments, as well as offer a path for more intelligent environments that take advantage of software-defined networking solutions and make it easier to leverage new network function virtualization (NFV) solutions from network service providers. These intelligent network functions will make it easier to develop and support hybrid cloud and geographically dispersed environments by treating the entire infrastructure as one logical location.

Assuming these initial criteria around deployment and management are met, the security implications of the different traffic patterns present in datacenters must be accounted for. To begin with, the vast majority of traffic in the datacenter travels between virtual machines without ever reaching a physical appliance. Visibility into and control over this traffic is essential to a secure datacenter design. Without a virtual security instance that can scan traffic traveling between virtual machines, a secure design would require routing the flow outside the virtual segment to a physical appliance for inspection, before routing back to the virtual destination. This model negatively impacts performance and creates latency. Further, with resources spread across geographies and migrated often, security solutions must support the ability to inspect asymmetric traffic flows without performance degradation.

Finally, the application traffic in the datacenter is very different from that at the enterprise perimeter. As the home to custom enterprise applications, the datacenter is a poor fit for traditional next-generation firewall (NGFW) technologies that are better equipped to defend the corporate edge from threats emanating from public Web applications (e.g., Facebook, Twitter, and YouTube). Datacenter security solutions must support visibility into custom corporate applications, as well as the use of increasingly digitized corporate data assets to understand security context and ensure optimum performance.

## Business Benefits of the Secured Datacenter

First and foremost, security solutions in the datacenter must be part of the central management process, either from an overall security standpoint or from a software-defined networking (SDN) orchestration perspective. IT staff cannot manually configure security in a datacenter environment. Security solutions that do not support dynamic provisioning and scale up and down to match resource consumption will not be used.

Organizations can leverage datacenter security products that are policy-driven, scalable, and robust to enable substantial efficiencies for their security staffs. Staff time spent trying to monitor and identify security threats can be reallocated to other, more value-generating activities. Policy-driven security solutions help organizations capture efficiency benefits from automation, and centralization of datacenter security solutions enables more consolidated, efficient threat identification and remediation efforts. As a result, IT security staff reclaim time spent on managing their security solutions and consolidating information from disparate pieces of their datacenter security architectures.

Arguably of equal importance to management is security efficacy. Solutions must be able to detect both known and unknown threats, and assist in remediation. Organizations increasingly realize that they need their security solutions to support proactive policies towards managing threats rather than funneling their resources towards reactive policies. By identifying more Datacenter security threats before they cause user-impacting outages or disruptions, organizations can capture both security staff and business efficiencies.

When security threats are identified and dealt with proactively, IT staff benefits from spending less of their time responding to incidents and dealing with the painful clean-up process. IT can now focus its resources on tasks meant to drive productivity of the organization (e.g., test and deployment of new applications and services). Having a robust datacenter security solution is an important component of helping IT staff identify security threats and avoid breaches and infections, while advanced analytics can be leveraged to limit the impact of user-impacting events when they do occur. By limiting the frequency with which security events occur, organizations can not only reduce IT staff time spent on incident response by a commensurate amount, but they also can ease the burden of associated responsibilities such as meeting audit requirements.

Further, datacenter security solutions improve the security and performance of business applications, so that end users are more productive. Since end users depend to a significant extent on the performance and availability of business applications that are frequently custom-developed applications, their productivity increases when there are fewer and shorter service interruptions to those applications. In addition, organizations with confidence in the security of critical IT infrastructure such as datacenters are often more willing to explore new business opportunities. This can help them capture both more revenue and implement more proactive, forward-looking business strategies. Further, loss of revenue as a result of datacenter downtime is a persistent worry for many organizations; to the extent they can limit unplanned downtime due to security incidents, they can also minimize revenue disruptions when systems and applications used by their internal and external customers go offline.

## Example of Security Solution: Cisco Secure Datacenter Architecture

Cisco's approach to providing scalable and dynamic security functionality to datacenter environments is woven throughout much of its product portfolio. Integrations between its core networking products, unified computing offerings, and virtualization and SDN portfolios present a holistic datacenter vision. Security has become a key part of Cisco's core strategy in the last 12 months, and as such is an important part of its overall datacenter solution set. Cisco Validated Designs (CVDs), which provide best practices for deploying Cisco security products easily and effectively, assist customers in deploying the right mix of solutions to address their specific environment. The Cisco Secure Data Center Solution is delivered through three core offerings: Cisco ASA 5585-X, FirePower services, and ASAv:

- The 5585-X Adaptive Security Appliance is Cisco's flagship firewall product. Purpose built for Datacenter environments, the ASA 5585-X leverages a two-blade modular architecture to provide up to 40Gbps throughput, 350,000 connections per second, and 10 million concurrent connections as a 2RU standalone appliance. When necessary, port density can be increased through additional I/O modules. The 5585-X also supports the clustering of up to 16 individual appliances to provide linear throughput scalability of up to 640Gbps. The 5585-X appliance can be deployed as a traditional Layer 2 or 3 firewall and VPN concentrator or utilize FirePower Services for more advanced functionality.

- FirePOWER Services for ASA firewalls, or FirePOWER stand-alone appliances, provide advanced threat detection across a variety of use cases, including the datacenter. Next-generation IPS (NGIPS) and Advanced Malware Protection (AMP) protect against targeted attacks utilizing custom malware. The FireSight Management Center correlates indicators of compromise across the entire infrastructure to speed remediation efforts, and limit the amount of time attackers have access to resources. Further, FirePOWER Services are powered by threat intelligence via Cisco's TALOS group – the primary team at Cisco for conducting security research on malware, attacks, and other threats in support of its other groups – to improve detection across the entire customer base.
- Finally, the ASAv is a fully virtualized instance of Cisco's physical Adaptive Security Appliance. The ASAv is hypervisor agnostic, providing deeper visibility into, and control over, all datacenter traffic between virtual machines, regardless of platform. Policy profiles can be managed through the Cisco Security Manager to ensure consistency across both physical and virtual environments, or through Cisco's Application Policy Infrastructure Controller (APIC) for Application Centric Infrastructure (ACI) deployments. Through APIC, security policies can be tied to specific applications and security services spun up or down as network demands change.

## IDC's Methodology for Quantifying the Business Benefits of the Secured Datacenter

To understand the quantifiable benefits to organizations of using datacenter security products such as Cisco Secure Data Center architecture solutions, IDC has translated key metrics into financial savings based on research conducted over the last two years with users of these types of datacenter security products. To do this, IDC analyzed key metrics surrounding IT efforts to maintain secure IT and datacenter environments, including: the ability of IT security staffs to identify threats proactively, the time needed for IT security staffs to respond to threats, the time costs for IT security staff and end users associated with datacenter security incidents, and other costs organizations incur as a result of datacenter security breaches. IDC has then grouped benefits from using datacenter security products into three main categories of cost savings – increased IT staff productivity, improved end-user productivity from security risk mitigation, and improved end-user productivity from operational efficiencies. We normalized these results by expressing them in terms of dollars benefits for an average organization with 1,000 IT end users.

### *Cost Reduction*

Organizations can potentially achieve a number of types of cost savings with datacenter security products. By upgrading to datacenter security products that offer improved visibility and performance, organizations can reduce security-related product costs, including the number of firewalls they require. Further, better integration of security products with each other and the hardware and software supporting them can reduce hardware and software costs. For example, deeper integration of datacenter security products can enable organizations to extend virtualization, thereby reducing costs. In addition, datacenter security products that perform better can help organizations reduce bandwidth costs, or improve their network performance, without having to increase their spending on bandwidth. In addition, reducing the number of impactful datacenter-related security events lessens organizations' exposure to fines, reimbursement costs, and legal fees associated with security breaches.

## IT Staff Productivity

IT security staffs are more efficient and productive with centralized and consolidated datacenter security solutions at their disposal. They can spend less of their time monitoring disparate solutions and trying to create usable insights from these solutions. In addition, when datacenter security solutions limit the number of user-impacting breaches and infections that occur, IT security staff can spend less time dealing with security-related downtime and service desk incidents. Most organizations typically have relatively small IT security staffs, so shifting some of these staff members' time away from reactive tasks to more innovative, forward-looking strategic responsibilities can be a substantial operational benefit. To quantify the benefits from IT staff time savings associated with use of datacenter security products, IDC multiplied time savings by an average annual loaded salary of $100,000.

## Risk Mitigation/End User Productivity

Datacenter security solutions that identify and mitigate more security threats create productivity benefits across their employee bases. By improving datacenter security, organizations reduce the frequency with which security breaches and infections impact the availability of business applications running through their datacenters, and also minimize the time it takes to get these applications up and running again. As a result, end users who depend on these applications face less disruption and have more fully productive time. IDC measures the impact of user productivity gains, IDC multiplies the time of increased availability of applications, programs, and data that end users need to do their jobs by a loaded annual salary of $67,500, scaled by a productivity factor to account for the fact that users can continue to work during disruptions caused by datacenter-related security events.

## Business Value Results

IDC's research into organizations' use of datacenter security products shows that they can generate business value by limiting the amount of productive time lost for users and IT staff caused by security threats and by limiting costs associated with such threats. While benefits accrue across IT security staffs' operations, they are most evident in terms of time spent responding to incidents, with researched organizations reducing the time burden of incident response by 62.9% on average. Organizations also benefit from datacenter security products by minimizing the time needed to perform security audits (28.2% less) and for managing and maintaining their security efforts (15.0% more efficient).

### TABLE 1

### Improvements Related to Use of Datacenter Security Products

| IT Staff Productivity Benefits | |
|---|---|
| Reduced Time for Security Management | 15.0% |
| Reduced Time for Incident Response | 62.9% |
| Reduced Time on Security Audits | 28.2% |

## TABLE 1

### Improvements Related to Use of Datacenter Security Products

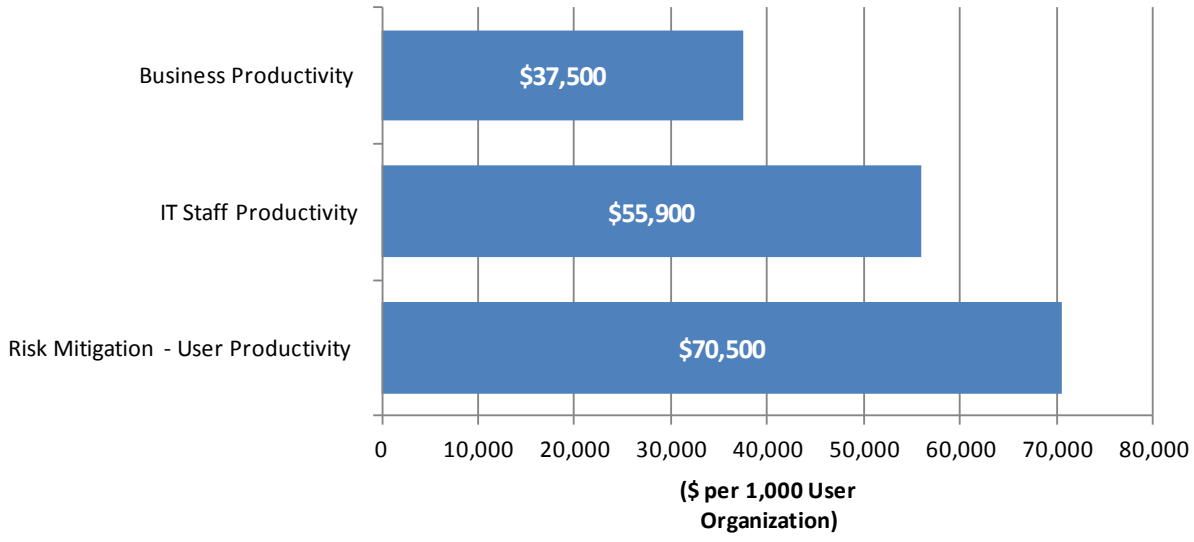
| | |
|---|---|
| **IT Staff Productivity Benefits** | |
| Reduced Time for Security Management | 15.0% |
| **Risk Mitigation Benefits** | |
| Reduced Number of Hours of Downtime | 51.9% |

Source: IDC, 2014

IDC's research demonstrates that a 1,000-user organization employing datacenter security solutions can achieve user productivity benefits stemming from fewer user-impacting breaches, infections, and downtime of a value of $70,500 per year. Such datacenter security solutions also create efficiencies and time savings for IT security staff worth an average of $55,900 per year for a 1,000-user organization. In addition, by driving operational efficiencies that result in capturing more revenue, datacenter security solutions can deliver on average an additional $37,500 of benefits for a 1,000-user organization per year.

## FIGURE 1

### Typical Benefits for 1,000 User Organizations by Limiting Impact of Security Incidents on Datacenter Operations




Source: IDC, 2014

## 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

---