


IT Security at the Speed of Business: Security Provisioning with Symantec Data Center Security

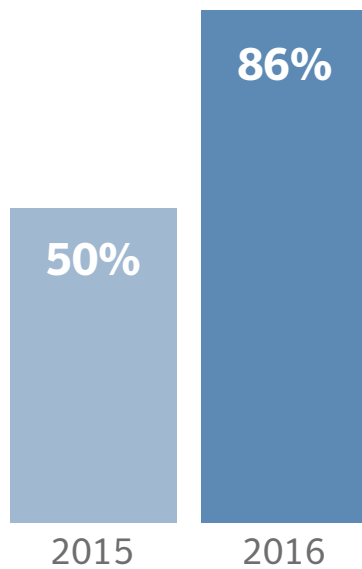


Today's data centers are transitioning into software-defined data centers (SDDC). In the SDDC, the core elements of the infrastructure—storage, server and compute, networking, databases, and business applications—are virtualized and delivered as services. The deployment, provisioning, configuration, management and operation of the entire infrastructure is abstracted from hardware and implemented through software. The infrastructure resources across the stack are application-centric, and customers have the ability to provision IT assets across their public cloud, private cloud, and on-premise domains. These SDDC capabilities are intended to enhance an enterprise's ability to quickly respond to new opportunities and emerging threats.

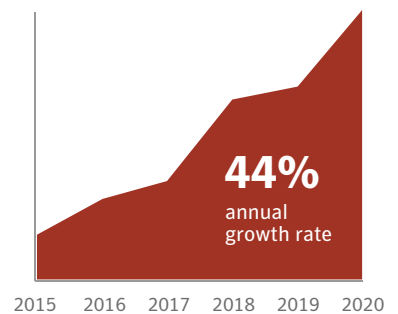
Virtualization, cloud, and policy-based automation and orchestration technologies are the lynchpins of the SDDC. The rates at which enterprises adopt these technologies therefore function as indicators of the rate of SDDC migration.

Today, more than half of all server and storage workloads are virtualized, a number that is forecasted to reach to 86 percent by 2016¹. Cloud computing is just as popular, with a forecast annual growth rate of 44 percent over the next five years². Adoption of network virtualization is also starting to take off, and is forecasted to grow from \$960 million in 2014 to \$8 billion in 2018³. The promise of increased IT and business agility, lower Capex, and economies of scale in IT operations underpins the adoption of SDDC technologies.

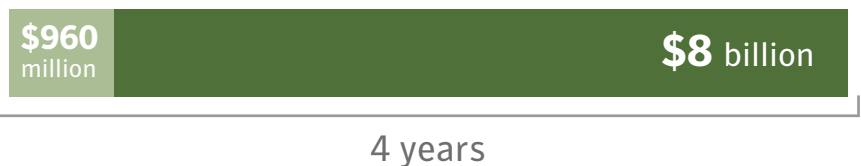
 **Server and storage virtualization**



 **Cloud Computing**



 **Adoption of network virtualization**



¹ [CIOInsight, August 28, 2015](#)

² [SiliconANGLE, January 27, 2014](#)

³ [IDC Study, SDN Momentum Builds in Data Center and Enterprise Networks](#)

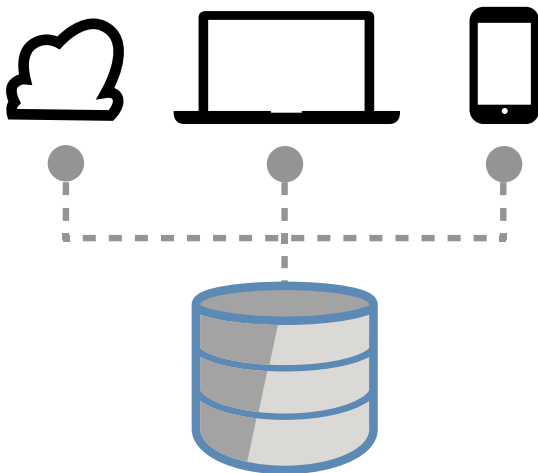
Confidence in a connected world.



IT Security that Keeps Up with Business and IT Operations

The adoption of software-defined technologies underscores the need for enterprises to re-evaluate their existing security practices and to ask themselves the following:

- “Is security an enabler or a hindrance to business agility?”
- “How can security keep up with business and IT?”
- “What is the impact of these new technologies on my organization’s current security model?”
- “How do I adapt my existing security frameworks and models to account for these developments?”
- “How do I take advantage of these technologies to enable security across my existing and new data center infrastructure environments?”



Enterprises today operate geographically distributed, heterogeneous, complex, and increasingly fluid data center infrastructures. These enterprises have not only adopted virtualization technologies within their data centers, but are also using a combination of public and private cloud assets and colocation facilities. These enterprises are also enabling partners to connect to their networks, and are allowing their highly mobile employees to connect to their networks using a myriad of mobile endpoints. With these capabilities, enterprises are more agile and responsive to opportunities for creating new revenue streams and for realizing operating efficiencies. As a result, business owners now expect IT assets to be quickly provisioned in a matter of hours if not minutes.

Despite these developments, security remains a laggard for many organizations. Many enterprises today continue to utilize rigid, perimeter-centric security models that are based on physical security frameworks.

Security and provisioning for newly created workloads and applications remains a manual process for many enterprises, and can take days or even weeks. In contrast, the process for provisioning new workloads can take minutes or hours in modern virtualized data centers. This lag between IT operations and security is a disadvantage in today’s fast-changing business environments. When a company wants

Confidence in a connected world.



to launch a new online business or needs to scale up quickly in response to a spike in demand for its online services, IT operations and security must be able to deliver these services quickly or the customer's customers will go elsewhere. In this scenario, enterprises have two choices:

- Release the new workload into production without the appropriate security and compliance settings, or
- Wait for IT operations, security, business owners, and compliance to complete their manual assessment and decide on the appropriate security settings.

Enterprises Have Two Choices

1. *Release the new workload into production without appropriate security and compliance.*
2. *Wait for IT operations, security, business owners, and compliance to complete their assessment and define appropriate security settings.*

The former exposes the organization to potential security breaches and compliance violations, while the latter approach is a potential tax on business agility and responsiveness.

These challenges are not unique to cloud environments. Even customers who have not fully adopted virtualization and cloud technologies are under pressure to decrease overall provisioning time in order to keep up with the pace of business, as well as to rein in rogue IT. Customers running applications on physical and legacy platforms also have an urgent need to enhance their abilities to quickly respond to zero-day threats and vulnerabilities, as these attacks become increasingly more sophisticated.

Enterprises now have an opportunity to adapt their security frameworks so that these are aligned with dynamic and highly abstracted software-defined environments, yet still deliver robust hardening and security monitoring for their legacy and physical environments. These security frameworks are enabled by solutions that embed security into the platform, support policy-based automation and orchestration across security domains, are application-centric, and integrate point technologies. With this application-centric approach, enterprises no longer have to make the traditional trade-off between security and agility. They can have both.

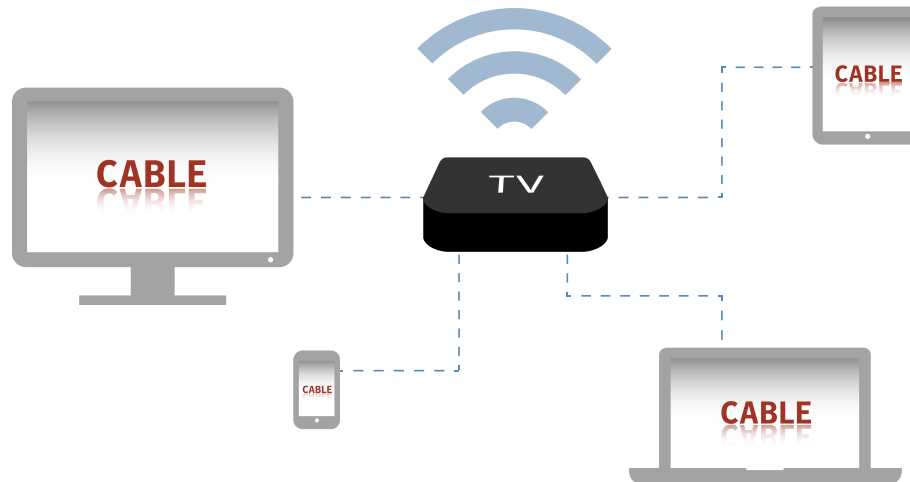
Business Use Case: Security That Moves at the Speed of Business

Background: The Business Unit of a Global Digital Media Company plans to pilot a new non-cable subscription, live streaming service to customers. With this service, customers can access the live

Confidence in a connected world.



streaming service without a monthly cable subscription and via various multimedia devices. The Digital Media Company also partnered with a large social media organization so that customers can sign-up for the new service using their social media accounts.




Business Challenges

The Business Unit wants to launch this service within two weeks of a major sporting event. The Business Unit will be collecting payment card information from new subscribers. The social media partner will also collect payment information from customers who sign up for the new service with their accounts. The new service will initially be available only to U.S. customers, but there are plans to expand this live streaming service to other global regions.

Demand for the new service is forecast to initially fluctuate, with higher than normal volumes expected during major sports events. Since this new service targets a new market segment, there is a lot of pressure to ensure that there are no service interruptions.

Global Digital Media Company has an existing automated business service requisition process, which is rolled into its IT service provisioning and change control process. Here, the Business Unit fills out the relevant forms requesting IT assets and defining the business requirements to support this new live streaming service. These business requirements are fed into an IT service provisioning, automation, and service orchestration tool like VMware vCenter.



IT Operations leverages vCenter templates to automate the provisioning of the guest virtual machines. Although the company's business service provisioning process is automated, security provisioning and compliance assessments remain manual processes.

IT Security Challenge: Manual Security Provisioning Process Impedes Business Agility

Provisioning Takes Time

The disconnect between the time it takes to provision IT business services and to provision security is a tax on business agility and time-to-market.

Once VMware vCenter provisions the virtual application, the Server Operations team notifies the Security Operations team to initiate security provisioning and compliance assessments. Security Operations works with the IT Compliance team to review the security and compliance requirements, and will recommend the appropriate security policies and controls. For many organizations, including Global Digital Media Company, this could involve a series of face-to-face meetings with key stakeholders. Once policies are approved,

IT tickets are raised for each individual Security Point product administrator to deploy the respective security policies on the virtual application and configure the security point products to monitor/protect the application. Once security provisioning is completed, the new service will then be released into production. In this model, provisioning could take several days (if not weeks). This disconnect between the time it takes to provision IT business services and to provide the necessary security is a tax on business agility and time-to-market.

Meeting Compliance Requirements

Given the types of data transmitted, the Global Digital Media Company is concerned with PCI-DSS, consumer privacy, and intellectual property. As the service rolls out globally, local data protection, and IP and content distribution rights will introduce additional controls that must be applied on the applications. The current manual process for compliance and security provisioning introduces more delays.

Static Security Zones Tax IT Resource Optimization

The Global Digital Media's current security practice relies on a hardware-based, perimeter-centric security framework. In this model, the customer's virtual applications are organized into security zones that mimic their hardware-based networks. This static perimeter-centric model means that the customer has to ensure that its virtual applications can only vMotion (for load balancing and scale out) to another physical server or to networks with similar security and compliance profiles. This approach can hamper IT resource optimization objectives.

Confidence in a connected world.



The Solution

Automate Security Provisioning with Symantec Data Center Security for Always-on Infrastructure Hardening and Protection

With Symantec Data Center Security (DCS): Server Advanced, the Global Digital Media Company is able to dramatically simplify and streamline the security provisioning process for newly created workloads. Symantec DCS 6.5 enables policy-based security orchestration through Operations Director. This recently introduced feature addresses the security provisioning dilemma by enabling customers to automate the provisioning of multiple security services for virtual environments, and align these activities with the IT provisioning process. These security services include anti-malware; server, device, OS and application hardening; firewall; and network intrusion prevention. The next release will add vulnerability scanning and threat assessment.

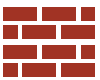
Using the Operations Director feature of DCS: Server Advanced, a typical automated workflow for security provisioning of new created virtual assets will have the following activities:

1. During the application request process, the Business Unit will answer a brief security assessment in addition to defining the business requirements. Once an application request is submitted by the Business Unit, the Operations Director feature in Symantec Data Center Security (DCS): Server Advanced will determine the security requirements using the information provided about the nature of the data processed by the application, its location, overall service level requirements, and security and compliance mandates governing the data and the application.
2. Operations Director will use the results of the security survey to recommend the relevant security policies and security controls that need to be applied to the workload. The policies, security assessment questionnaire, and requisite mapping to security standards and technical controls across security tools are set up ahead of time by the customer's security team, in accordance with the organization's security and compliance best practices. By automating the process across new application and security provisioning, the customer's security and IT organizations are able to eliminate or minimize the time and effort spent on manual security assessments, reviews, and approvals.

Confidence in a connected world.



3. Once the application is started, Operations Director will detect the application and will orchestrate the application of the relevant security settings across security products. Operations Director will then orchestrate security monitoring and hardening settings for the virtual applications that are protected by DCS: Server Advanced.
4. For customers that have VMware NSX, Operations Director will support security provisioning across the following security products:



Security monitoring, server hardening, and host-based IPS/IDS policies with DCS: Server Advanced.



Agentless anti-malware, agentless network IPS, and in-guest file quarantine delivered by Symantec DCS: Server.



Firewall policies with Palo Alto Networks VM Series Firewall appliances.

5. Operations Director is flexible and allows the security operations team to choose the level of automation they would allow in the security provisioning process. Customers can design the Operations Director workflows so that:
 - The security provisioning process for common application requests can be fully automated, or
 - The Security Operations team can review the recommend policies and security settings and override any policies that cater to any exemptions that need to be applied.
6. Once the security settings are applied, the security and server teams are notified that the application is ready to be added to the production network.
7. The security settings applied to the virtual application are defined at an application-level, allowing virtual applications with different trust levels to securely co-exist within a host.

The workflow described in the previous section illustrates the power of DCS: Server Advanced to accelerate business agility and responsiveness by eliminating manual processes associated with the security review and provisioning process. Using the Operations Director functionality, customers are able execute the security provisioning for new virtual workloads in a matter of minutes- Truly, security at the need of speed!

Confidence in a connected world.



Orchestrating Security Across Third-Party Security Tools

Symantec Data Center Security: Server Advanced orchestrates security across third-party products via REST API-based connections. The current version has built-in integration with VMware NSX, VMware's networking platform, allowing Operations Director to orchestrate any security product integrated with the VMware NSX ecosystem, starting with Palo Alto Networks Next Generation Firewalls. Future releases will allow Operations Director to orchestrate security across a broader set of certified NSX-compatible security tools.

Benefits of Security Microsegmentation

Symantec Data Center Security: Server Advanced also leverages the new Operations Director functionality to execute a security microsegmentation model, thus eliminating the limitations of static security zones. With microsegmentation, customers can create discrete security containers or profiles per application instance. Relevant security policies are then applied to these discrete security containers, based on the application's security and compliance characteristics. Application instances with varied security profiles and trust levels can, therefore, co-exist securely within a physical host. Even if one of the applications is compromised, the rest of the application instances on the host and network are isolated and protected.

Using microsegmentation, customers will also be able to move a virtual application to another physical host using vMotion, and ensure that the security policies and settings are maintained. The vMotioned virtual application is still able to co-exist with other applications with different trust levels within the new physical host and network environment- thus delivering Always on Protection and Hardening!

In addition to delivering unprecedented automation of security for VMware environments, Symantec Data Center Security: Server Advanced also delivers microsegmented security provisioning for physical server assets and non-VMware virtual environments. Customers can do this by utilizing a rich set of APIs to enable Chef/Puppet integration and full automation of the security provisioning process in these non-VMware environments.

Confidence in a connected world.



Security at the Speed of Business

Speed or Security? It is a False Choice.

Symantec Data Center Security: Server Advanced will enable organizations like the Global Digital Media Company to deliver security that is able to keep up with the pace of business and IT. It enables businesses to quickly provision application-level security for newly provisioned workloads by automating several manual steps.

Today, customers will have the ability to automate and orchestrate micro-segmented security provisioning across heterogeneous environments—Cloud, VMware, OpenStack, and physical servers on any platform. Customers can choose the security automation and orchestration approach that best fits their environment. They can:



- Leverage Symantec Data Center Security: Operations Director to automate and orchestrate security provisioning for VMware environments and streamline this process with the new security provisioning workflow integrated into VMware vCenter.
- Take advantage of fully instrumented rest APIs to integrate security provisioning into any data center security automation frameworks (like Chef or Puppet).

Both options offer customers the ability to define and apply security policies at the application level, thus doing away with the inefficiencies associated with static, perimeter-centric network security zones.

Symantec Data Center Security: Server Advanced demonstrates Symantec's commitment to enable customers to securely migrate their existing data centers into the SDDC by embedding security into the platform, integrating point security technologies, and automating and orchestrating security.

Confidence in a connected world.



Symantec Data Center Security: Server Advanced - Features

Symantec Data Center Security: Server Advanced delivers the following protection capabilities:

- Out of the Box Host IDS and IPS Policies to monitor and prevent suspicious server activity.
- Sandboxing and Process Access Control (PAC) offers prevention against a new class of threats.
- Host Firewall, to control inbound and outbound network traffic to and from servers.
- Compensating HIPS Controls restricts application and operating system behavior using policy-based least privilege access control.
- File and System Tamper Prevention locks down configuration, settings, and files.
- Application and Device Control locks down configuration settings, file systems, and use of removable media.
- Security monitoring and hardening of OpenStack Keystone.
- Security monitoring across physical and virtual servers and across AWS and all OpenStack modules.

Customers of Data Center Security: Server Advanced will also have access to the features available in Symantec™ Data Center Security: Server including the following:

- Agentless anti-malware, agentless network IPS and file reputation services
- Auto-deployment and provision of Security Virtual Appliance to ESX host in a cluster
- Network based threat detection and protection (Network IPS)
- Operations Director to automate and orchestrate security provisioning for newly created workloads
- Unified Management Console (UMC) delivers a consistent management experience across Data Center Security products

Confidence in a connected world.

