CloudPassage

What CSOs Need To Know About Software-Defined Security

CONTENTS

Is Software-Defined Security More Than Just Vendor Hype?

The “software-defined” moniker has been a hot buzzword in the technology industry since virtualization hit mainstream adoption. The explosion of advanced virtualization, cloud infrastructure, and operational automation/orchestration tools led to the term becoming over-used and under-defined. Software-defined networking, software defined data centers, software-defined storage... you name it, and it’s probably been software-defined.

The security and compliance domains have not missed out on the trend. “Software-defined security” began to appear in vendors’ literature as the need to protect virtualized and cloud infrastructure grew. But again, the term was poorly defined and failed to communicate real meaning—it was just a buzzword. As with many emerging technology concepts, software-defined security has been plagued by scattered interpretations.

These varied meanings are now coalescing into a more broadly accepted set of defining characteristics, allowing more objective consideration of software-defined security as a legitimate strategy. Leading security industry analysts have begun to converge on what software-defined security (SDSec) really means. Punctuating the growing view of SDSec as strategically important, Gartner recently identified software-defined security one of the top ten infosec technologies for 2014.

As traditional infrastructure delivery shifts to virtualized, abstracted, software-defined models, the concept of software-defined security becomes increasingly important for security managers and technologists.

> *“SDDC is a whole lot more than the IT word-du-jour. It is the logical model for creating and delivering IT resources quickly, efficiently, cost-effectively, and securely. And in a hypercompetitive, technology fueled economy, SDDC will soon become the standard for successful businesses.”*
>
> Lynda Stadtmueller
> Stratecase Program Director
> Frost & Sullivan

What Is Software-Defined Security?

Software-defined security (SDSec) is an architectural approach to protection and compliance that decouples and abstracts controls away from physically-oriented elements such as topology, hardware, or physical location. This approach is critical for enabling security and compliance to operate harmoniously with software-defined infrastructure models that also decouple application and data hosting from the hardware underneath. To support these shifts, information security services must evolve to become programmable, adaptive, scalable, and portable.

Understanding Software-Defined Infrastructure

The concept of software-defined infrastructure is important to understanding why SDSec warrants serious consideration. Software-defined infrastructure is closely related to emerging virtualization, cloud, automation, and orchestration concepts like:

- Cloud infrastructure
- Software-defined data centers (SDDC)
- Infrastructure-as-a-service (IaaS)
- IT-as-a-service (ITaaS)
- Software-defined networking
- Software-defined storage

An important factor shared by these concepts is that management of provisioning, configuration, and operation occurs via software as opposed to physical topology and hardware. Software-defined infrastructure does not mean that all hardware is completely eliminated; there will always be hardware, networking infrastructure, and other underlying physical elements. What it does mean is that software-defined infrastructure abstracts these physical components from the logical constructs of application, workload and data hosting configuration and operation.

The benefits of software-defined infrastructure typically include more automated and efficient management, flexible deployment and scalability, reduced errors, improved consistency, and far less “brittleness” in application, workload, and data hosting. The extent of these benefits is beyond the scope of this document, but suffice it to say that they are compelling enough to completely disrupt decades of infrastructure procurement, delivery, and operations strategy.

The Need for Software-Defined Security

In practice, the use of software-defined infrastructure imposes technical and operational characteristics that differ significantly from traditional infrastructure strategies. A few of these differences include broader asset distribution, high rate of change, greater diversity in deployed technologies, variability in scale, and abstraction of infrastructure from underlying physical hardware. Often, the underlying physical infrastructure is owned and operated by a third party such as an external IaaS provider.

The use of APIs to automate and orchestrate software-defined infrastructure is also very common, serving to accelerate deployment, eliminate manual effort, and reduce the potential for human error.

The need for SDSec stems from these differences. For decades, security has been built around models that assume availability of fixed perimeters, hardware security appliances, physical proximity of data and application assets, and control of physical topology. Virtualization, cloud hosting, and software defined infrastructure disrupt these assumptions dramatically. This means that new security strategies are needed; specifically, a shift in security and compliance delivery through abstraction, automation, orchestration, automatic scaling, and API enablement.

As with other software-defined technology models, the impact of software-defined security will be both disruptive and transformational. Software-defined security does not mean that some dedicated security hardware is no longer required – it is. However, like software-defined infrastructure, the value and intelligence of solutions will move from hardware into software.

Adopting a software-defined security architecture is needed to ensure that security and compliance do not hinder software-defined infrastructure, but compliment and enhance the value it delivers to technology-driven enterprises.

> *"The rise of cloud computing is a true transformation, which is fundamentally changing core security practices. Far more than a mere outsourcing model, cloud computing alters the very fabric of our infrastructure, technology consumption, and delivery models. In the long run, cloud and mobile computing are likely to mark a larger shift than the Internet itself."*
>
> Rich Mogull
> Analyst and CEO
> Securosis

Principles of Software-Defined Security

Security industry analysts and vendors are converging on a meaningful definition of software-defined security.

Five key architectural principles have emerged that are central to enabling security and compliance to keep up with software-defined infrastructure. Without building around these principles, a security strategy will not be able to address the technical and operational dynamics of new infrastructure models.

These five principles are abstraction, automation, orchestration, automatic scalability, and API enablement. Each is discussed in detail below.

Abstraction

The SDSec principle of security abstraction expresses that security and compliance capabilities must perform without dependencies on underlying physical constructs.

Hybrid and multi-cloud are fast becoming the standard for enterprise infrastructure and application delivery. Nearly 75% of enterprises already support hybrid and multi-cloud environments.

Most traditional infrastructure security strategies have been driven by, or depend upon, physical constructs such as hardware appliances, physical network segmentation, and proximity of computing components. Given that the underlying infrastructure itself is becoming more virtualized and more widely distributed, security needs to be virtualized and able to operate regardless of where underlying hardware might be physically located.

Security abstraction means all controls must be completely non-dependant on specific hardware, topologies, or physical location of the environment being protected. A true software-defined security strategy should also be independent of any specific infrastructure platform, vendor, or service provider.

Achieving infrastructure security abstraction makes security organizations adaptable in their ability to support any infrastructure model. In the future, most enterprises will have a mix of private, public, and hybrid infrastructures (a.k.a., multi-cloud infrastructure) in addition to virtualized and bare-metal systems. Abstraction also offers future agility by preventing vendor or provider lock-in, which can be a serious obstruction to an enterprise expanding or shifting its infrastructure strategy.

The principle of abstraction is critical to achieving infrastructure security that works anywhere and across complex mixed-infrastructure models—a capability that will be demanded of every enterprise CSO as cloud transformations continue.

Automation

The SDSec principle of security automation expresses that security and compliance capabilities should minimize human intervention in deployment, configuration, ongoing operation, and deprovisioning.

Until recently, the rate of change for application and data hosting infrastructure was relatively slow. Before automated orchestration and self-service infrastructure appeared, even virtualized infrastructure demanded relatively little in the way of high-speed, hands-off updates to security environments. But moving to highly automated and orchestrated infrastructure operations (e.g., devops) drives a rate of change that is orders of magnitude higher than traditional infrastructure operations.

Reinforcing the need for automation is the I.T. consumerization trend that is driving adoption of on-demand, self service infrastructure models, even within private data centers. This means changes to infrastructure, including adds and moves, can happen without notice or the opportunity to ensure security and compliance controls are in place. These factors make automated security controls more important than ever.

Automated control deployment is not enough. Keeping up with cloud infrastructure velocity means automation throughout the lifecycle of every enforcement and monitoring control.

Security automation means that any control (e.g. firewall policies, configuration vulnerability scans, intrusion detection, multi-factor authentication) can be deployed and managed without human intervention. Most desirable is full-lifecycle automation, in which policies are set once and tied to some context, after which underlying controls are 100% automated at each stage of the control's lifecycle—from deployment to deprovisioning.

Automated collection of audit and operational data is also critical, especially in environments where infrastructure components are only operational for short periods of time. Even though short-lived, these ephemeral resources are still in scope for auditor inspection, even if not running at audit time.

Automation also offers technical and operational efficiency, both in terms of initial deployment and ongoing maintenance of monitoring and enforcement controls. Well-implemented automation will enable security organizations to keep up with the scale and rate of change associated with emerging infrastructure models. Security accuracy and effectiveness are both improved by automation, and potential for human error is removed—especially if API instrumentation enables cooperation of otherwise disparate technologies.

Automation is perhaps the most important principle for CSOs to take under consideration in order to keep pace with infrastructure automation in the short term, and to provide strategic options for sustainable, future-ready capabilities.

Orchestration

The SDSec principle of security orchestration expresses that business security requirements are satisfied by dynamic, automated, centrally-managed composition of individual controls into integrated, holistic security services.

Security orchestration maintains alignment between security requirements, changing application dynamics, and control implementation through automated workflows, provisioning, and change management.

Application and infrastructure orchestration have proven the value of this technology delivery strategy. Security and compliance functions now stand to benefit from its adoption as well.

Orchestration operators define security policies and services that are associated with various contexts. A few examples of these contexts include hosting model (e.g., private vs. public), application nationality (e.g., servicing E.U. vs. U.S. citizens), or data classification. Policies and contextual information are used by the orchestration platform to dynamically synthesize higher-level security services (e.g., PCI compliance service for a public-cloud hosted web application servicing E.U. citizens).

Security orchestration platforms centrally manage the composition, deployment, and management of individual control components into more complex, service-oriented security systems. By composing many individual controls into a larger system, security orchestration is considered to be a higher order function than simple control automation. In many implementations, orchestration also addresses licensing, metering, chargeback, and other security resource consumption issues—important in service-oriented cloud computing and software-defined infrastructure environments.

A key strategic value of orchestration is the ability to rapidly create and maintain numerous security environments that are aligned with higher-level business needs while keeping pace with automated deployment, migration, and reconfiguration needs of the underlying application environment.

Security orchestration also reduces the time, effort, and potential for error associated with deploying multiple control systems across multiple application or infrastructure environments. This streamlines control deployment, integration, and change management, preventing security from becoming a speed bump in an otherwise seamlessly orchestrated environment.

And as technology delivery becomes increasing service-oriented, orchestration can relieve the administrative complexities of usage-based security resource management.

Infrastructure and application delivery are becoming increasingly orchestrated functions in an increasingly service-oriented technology world. If security organizations are to operate harmoniously in these new environments, security orchestration should be on every CSO's radar.

Automatic Scalability

The SDSec principle of automatic scalability expresses that security and compliance control capacity must scale up or down dynamically and without human intervention.

Scaling application and infrastructure environments automatically, on-demand, and in near real-time is one of the essential capabilities that makes cloud computing so valuable. Dealing with seasonality or other fluctuations in demand once required maintaining sufficient idle infrastructure capacity to meet peak demand, often on a per-application basis. This approach was operationally and economically inefficient.

With elastic compute models, data center infrastructure is shared among hundreds or thousands of applications, allowing the larger overall infrastructure pool to be highly optimized for utilization. In hybrid cloud computing models, additional capacity can be rented on-demand from an external party (e.g., a public IaaS provider). These capabilities are often referred to as cloud-bursting or elastic computing, and they offer enormous economic and operational benefits to enterprises with variable compute needs.

Security and compliance controls need to be automatically scalable to keep up with elastic compute models. This means that controls must be deployed directly into the application scaling mechanism (e.g., building controls directly into cloud-burstable virtual machines) or must have the ability to scale based on application scaling triggers (e.g., detection of a cloud-burst triggers deployment of more virtual appliances). Given that an arbitrary number of security controls may potentially be needed across an arbitrary number of diverse application environments, the SDSec principles of orchestration and automation are often leveraged to achieve automatic scalability.

Cloud-oriented application hosting models that support instant deployment and dynamic capacity will demand security that can automatically scale. Automatic scalability as a feature of an on-demand, orchestrated security service is an optimal strategy for implementing software-defined security.

API Enablement

The SDSec principle of API enablement expresses that security monitoring and enforcement control functions should be fully accessible via open application programming interfaces (APIs).

Without deep API enablement, no security technology will be able to operate in harmony with orchestrated application and infrastructure delivery.

API enablement is perhaps the most important technical principle of software-defined security. Traditional security solutions provide some level of API access for management and data access, but these APIs are often limited and/or proprietary to the vendor. This precludes even simple cross-product integration, and certainly cannot support the levels of automation and orchestration demanded by cloud computing models. Broad adoption of APIs based on open standards (e.g., SOAP or REST) has been a key factor in the development of service-oriented cloud computing models. Security

and compliance solutions are starting to catch up with the trend.

Within an SDSec environment, APIs typically exist at the individual control level (e.g., changing firewall management rules) and at the orchestration platform level (e.g., scaling security services for an application that's cloud-bursting). These APIs also allow existing systems, even those not part of an orchestrated SDSec strategy, to be extended through connection and integration with the SDSec environment. A truly open API will offer developers secure but unfettered access to complete, well-documented interfaces that enable management of any function and access to any data.

Besides making automation and orchestration possible, API enablement of security and compliance allows unique security value to be derived from security services. It can also offer a measure of future-proofing by providing flexibility and optionality as new demands emerge.

CSOs and their organizations should insist on open API enablement of any security solution, especially those oriented to software-defined and cloud computing operations.

Conclusion

Emerging models for application and infrastructure delivery are clearly more dynamic, distributed, and diverse than ever. No matter the name—cloud computing, virtualization, software-defined data centers—security and compliance management must evolve to succeed in these massively scalable, fast-moving environments.

This need requires on-demand orchestration of security controls through layers of automation. Such environments must offer automatic scalability and the ability to function anywhere, independent from the underlying infrastructure. API enablement at multiple levels is a must, serving as the linchpin of a software-defined security architecture.

The five principles of software-defined security—abstraction, automation, orchestration, automatic scalability, and API enablement—can go far to ensure the success of security and compliance support for enterprise transformation to cloud-oriented technology delivery.

Additional Resources

Gartner: Software Defined Data Centers and Security–What's in a Name?
http://blogs.gartner.com/neil_macdonald/2013/01/29/software-defined-data-centers-and-security-whats-in-a-name/

451 Group: Carving A Path Through IaaS Security
http://www.cloudpassage.com/resource-center/send/451-impact-report-cloudpassage-04-2014.pdf

Forrester: Predictions For 2014 - Cloud Computing
http://www.cloudpassage.com/resource-center/send/forrester-predictions-for-cloud-2014.pdf

Securosis: What CISOs Need To Know About Cloud Computing
https://securosis.com/research/publication/what-cisos-need-to-know-about-cloud-computing

Techopedia: Software-Defined Security Explained
http://www.techopedia.com/definition/29942/software-defined-security-sds

CloudPassage: Halo API Developer's Guide
http://www.cloudpassage.com/document_images/API_Guide/API_Guide.pdf

About CloudPassage

CloudPassage Halo® is the world's leading agile security platform that empowers our customers to take full advantage of cloud infrastructure with the confidence that their critical business assets are protected. Halo delivers a comprehensive set of continuous security and compliance functions right where it counts—at the workload. Our platform orchestrates security on-demand, at any scale and works in any cloud or virtual infrastructure (private, public, hybrid or virtual data center). Leading enterprises like Citrix, Salesforce.com and Adobe use CloudPassage today to enhance their security and compliance posture, while at the same time enabling business agility.

Learn More

Visit www.cloudpassage.com or call 800-215-7404 to find out more about how CloudPassage can help your organization address security and compliance.