Solution Showcase

Securing Hybrid Clouds and the Software-defined Data Center (SDDC)

Date: July 2016 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: Large organizations are actively developing cloud-based applications, embracing SDDC technologies, and moving production workloads to the public cloud. This strategy delivers benefits like lower cost, simpler operations, and accelerated application deployment but also has a profound impact on cybersecurity. Why? These emerging technologies aren't well understood and organizations often lack the right skills or controls to address cloud/SDDC risks or respond to security incidents. Smart CISOs will address these gaps with security policies, controls, and monitoring that align current best practices with burgeoning cloud and SDDC security requirements. Check Point Software's vSEC offerings can help by providing broad infrastructure support, strong management, granular policy enforcement, and end-to-end traffic visibility across physical, virtual, cloud, and SDDC infrastructure.

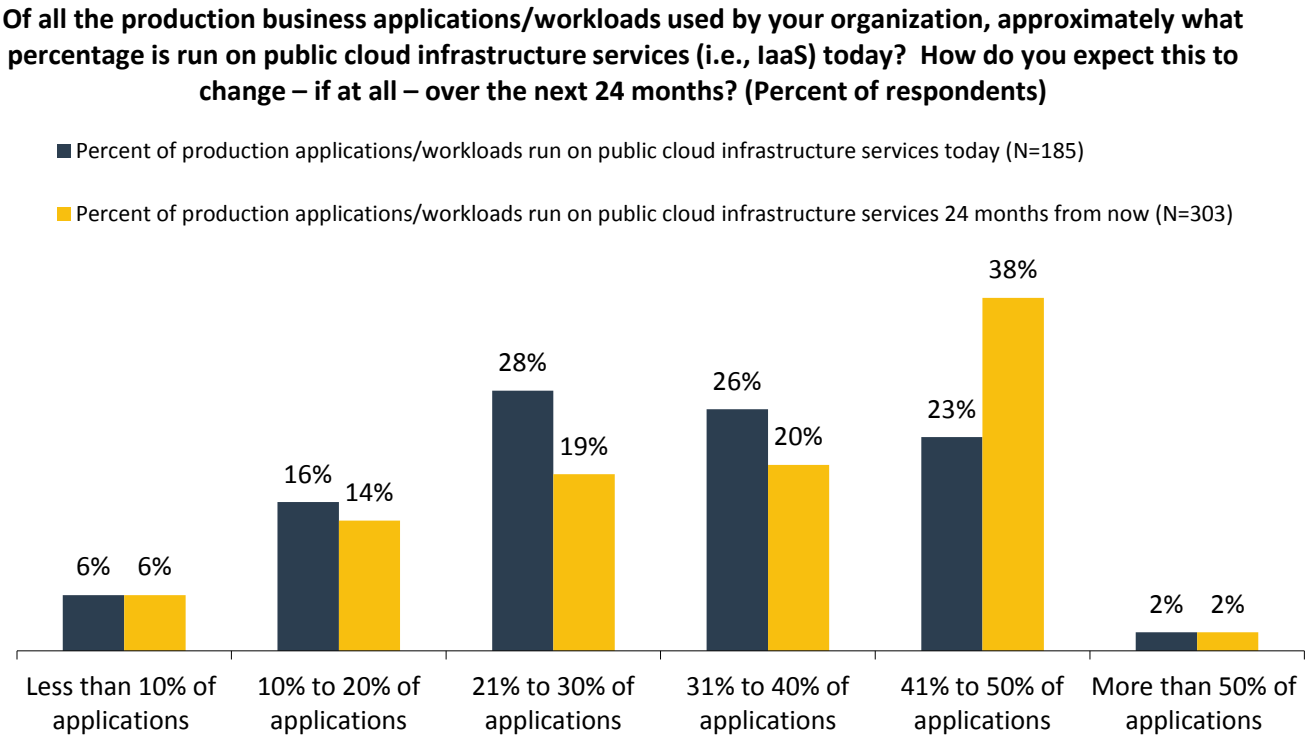
Overview

Enterprise organizations have witnessed massive changes in data center computing over the past ten years. The first move was simple data center consolidation. For example, the U.S. Federal Government instituted the Federal Data Center Consolidation Initiative (FDCCI) in 2010. This effort led to the closing of 746 facilities by 2014. Following the success of data center consolidation projects, many organizations moved on to server virtualization to increase data center efficiencies.

Large organizations continue to transition their data centers aggressively today. Many firms are adding private cloud and software-defined data center (SDDC) technologies (i.e., OpenStack, VMware NSX, Cisco ACI, etc.) to internal data centers, and embracing cloud computing to not only streamline IT overhead but also improve its responsiveness to the business. According to ESG research, 75% of organizations use public cloud services in some capacity today,[1] and as organizations gain experience and confidence with cloud infrastructure services, they will begin to deploy more production apps/workloads in this capacity. Cloud use will continue to increase over time. In a recent ESG research survey, 23% of organizations said that they run between 41% and 50% of their applications/workloads in the cloud today. Cloud-based workloads will increase substantially by 2018—38% of organizations plan to run 41% to 50% of their applications/workloads in the cloud in 24 months' time (see Figure 1).[2]

[1] Source: ESG Research Report, *2016 IT Spending Intentions Survey*, February 2016.
[2] Source: ESG Research Report, *Securing Cloud Environments*, to be published.

Figure 1. Percentage of Production Workloads Run on Public Cloud Infrastructure Services



Source: Enterprise Strategy Group, 2016

Cloud Computing Comes with Security Challenges

As the ESG research illustrates, organizations are rapidly moving forward with cloud and SDDC initiatives to lower costs, streamline operations, and improve IT agility. In spite of the benefits, however, cloud and SDDC are relatively new and emerging technologies—especially with regard to security. As organizations accelerate their use of cloud and SDDC to gain business and IT benefits, they simultaneously fall behind from a security perspective because:

- **Security teams lack strong cloud computing skills.** According to ESG research, 46% of IT and cybersecurity professionals claim that their organizations have a "problematic shortage" of cybersecurity skills. Furthermore, the skills gap is especially pronounced when it comes to cloud security—one-third of cybersecurity professionals believe that cloud security represents the biggest skills deficiency at their organizations.[3] Cloud security skills insufficiencies only increase IT risk as enterprises continue to move workloads to the cloud. Conversely, infrastructure and security decisions are often being made by DevOps teams who traditionally don't understand the security implications of provisioning new services or infrastructures. The knowledge gap needs to be bridged by both the security and DevOps teams in order to mitigate exposure to threats.

- **Cloud automation and orchestration are antithetical to security.** Cloud computing tends to go hand-in-hand with agile development and DevOps orchestration but these methodologies are designed to accelerate application delivery and maximize application performance rather than provide adequate security protection and oversight. Alternatively, provisioning security controls can be time-consuming, involving policy decisions, workflows, and approval cycles.

[3] Source: ESG Brief, *Cybersecurity Skills Shortage: A State of Emergency*, February 2016.

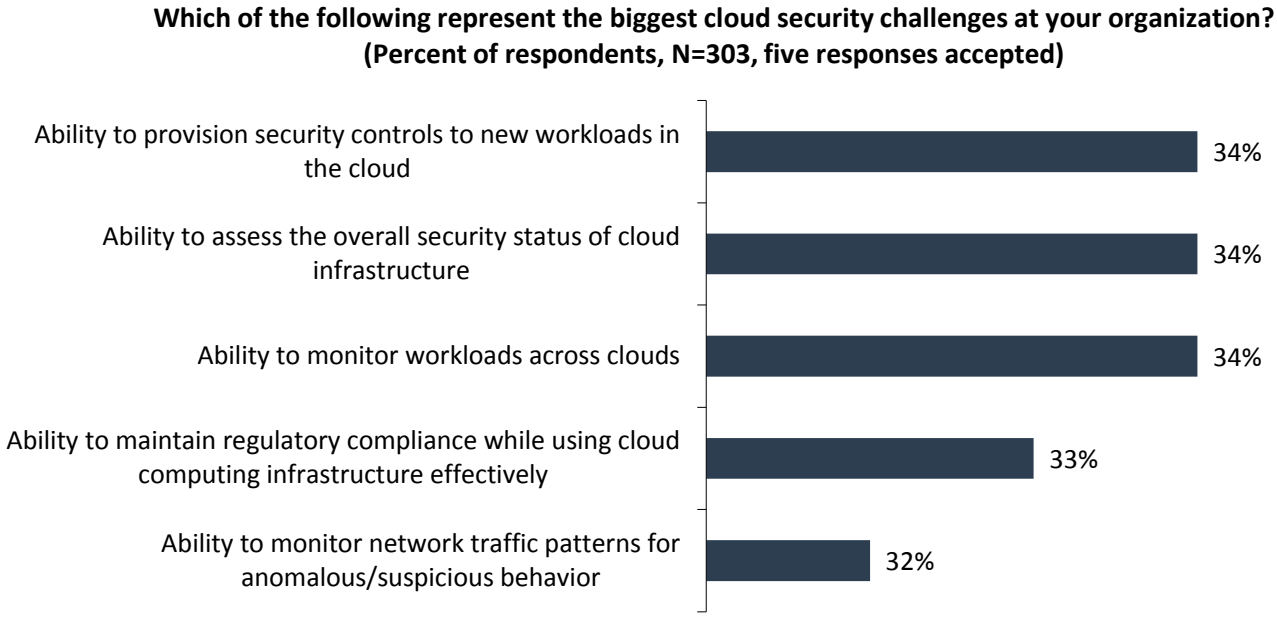
CISOs must somehow adjust their security schedules so they align with the accelerated pace of cloud security without sacrificing the rigor of risk management and emergency response processes.

- **Traditional security monitoring and controls don't always align with cloud and SDDC.** Traditional security controls were designed to reside on networks and servers to examine packets, detect anomalous activities, and block actions based upon rule sets. These methods don't always work well with cloud computing and SDDC as these technologies add virtualization technology, layers of abstraction, and physical distance to workloads and networks. For example, network traffic flowing from one cloud-based workload to another may never cross a physical network path, remaining invisible to traditional network controls. Cybersecurity technologies will need their own abstraction, virtualization, and cloud connectivity to bridge this divide. This is especially important with regard to the dynamic nature of the cloud where VMs are provisioned, go dormant, or move around. Additionally, in cloud-based environments, cyber-attacks can proceed unimpeded across virtual networks in search of sensitive workloads and data, while security and access controls remain fixed at the perimeter. Cloud security controls must be designed to detect and prevent lateral movement before it leads to damaging data breaches.

These issues are just the tip of the iceberg. ESG research reveals a number of other cloud security challenges, including provisioning cloud security controls to new cloud-based workloads (34%), assessing overall cloud security status (34%), the ability to monitor workloads in the cloud (34%) and the ability to maintain compliance with various regulatory bodies (33%, see Figure 2).[4] While it can be difficult to secure cloud and SDDC in general, it is especially problematic when organizations pursue a strategy of heterogeneous cloud and SDDC deployment. Unfortunately, this is exactly what is happening at large organizations that are adopting a diverse mix of private, public, and SDDC technologies simultaneously. As enterprise infrastructures rapidly grow in complexity, so too are the threats targeting them. Thus organizations should seek a consistent level of protection wherever corporate data goes while maintaining comprehensive visibility of both physical and virtual threat information.

[4] Source: ESG Research Report, Sec*uring Cloud Environments*, to be published.

Figure 2. Top Five Cloud Security Challenges



Source: Enterprise Strategy Group, 2016

Cloud Security Requirements

CISOs must improve cloud security skills, processes, and technologies or quickly face a future of ever-increasing and unacceptably high IT risk. Does this mean shunning traditional security processes and controls? No. ESG believes a pragmatic cloud security strategy can build upon existing security best practices and leading technologies that extend their support to cloud and SDDC. To achieve synergy between security best practices, cloud, and SDDC, security technologies should include:

- Familiar management tools and techniques. Security teams must change their management perspectives to focus on securing workloads and cloud-based data rather than just servers and network segments. For example, a cloud-based workload containing regulated data should be secured with similar controls and oversight as a mission-critical server residing on the corporate network. Similarly, SDN policies should emulate those associated with firewall rules and network segmentation. This should be done by extending management techniques for policy management, provisioning, and configuration management, based upon workload classification, location, and access requirements. To achieve this goal, cybersecurity professionals can work with tried-and-true security management tools that are also extensible to support cloud and SDDC infrastructure.

- Comprehensive visibility, monitoring, and reporting. As the old management saying goes, "you can't manage what you can't measure." In this instance, this applies to the ability to monitor all security activities as they relate to physical, virtual, cloud, and SDDC infrastructure. CISOs need the right security monitoring and analytics tools that cover this entire spectrum in order to mitigate risk, detect problems, and respond to incidents when necessary.

- Support for cloud automation and orchestration. Cloud and SDDC security management must align with DevOps processes and tools like Chef and Puppet. This demands the ability to create security templates that automatically provision the right security controls based upon workload classification, regulatory compliance requirements, or corporate governance. To accomplish this goal, security tools must support open and documented APIs to promote technology integration.

- **Advanced security controls designed for cloud and SDDC.** New types of security controls are evolving in lock-step with cloud and SDDC technology evolution. For example, cloud and SDDC technologies build upon network security with support for micro-segmentation, using software to create virtual network segments for network communications between assigned assets only. This can help decrease the attack surface, especially when network traffic flows "east-west" between workloads and never crosses the network perimeter. In this way, micro-segmentation can be an important first step in avoiding cyber-attacks within the virtual network. Similarly, cloud and SDDC security can include service-chaining, where security operations teams can assign advanced security services like threat emulation, IPS, antivirus, or bot detection to particular workloads or network communications to maximize protection. When used correctly, software-based security can be used to apply granular controls, providing a level of security that exceeds all but the most sophisticated traditional cybersecurity countermeasures.

- **Heterogeneous technology support.** Large organizations are pursuing data center strategies that include open source (i.e., OpenFlow, OpenStack, etc.), on-premises private cloud and SDDC technologies (i.e., Cisco ACI, VMware NSX, etc.) and public cloud infrastructure (i.e., AWS, Microsoft Azure, IBM SoftLayer, etc.). Cloud security technologies must integrate with leading cloud and SDDC technologies with common command-and-control management and reporting in order to provide enterprises with appropriate security oversight AND technology flexibility.

Cloud and SDDC Security from Check Point Software

Check Point Software is recognized as a market leader in network security, and the company is now building upon its expertise by extending its security coverage to cloud and SDDC with its vSEC offerings. Like its traditional security products, Check Point vSEC features strong configuration management, policy management, and end-to-end threat prevention security services for full coverage—even against advanced malware and zero-day attacks. Check Point then builds upon this foundation with:

- **Broad support.** Check Point vSEC is designed to support a wide array of cloud and SDDC infrastructure, including AWS, Cisco ACI, Microsoft Azure, and OpenStack, as well as VMware NSX and vCloud Air. With this type of heterogeneous support, vSEC can act as a security hub to protect and monitor all types of data center options.

- **Automated provisioning and configuration management.** As part of its integration, Check Point vSEC supports cloud and SDDC orchestration tools while also providing APIs for custom integration. These APIs are well documented and supported so developers can get the security functionality they need without impacting other applications. For example, advanced integrations with leading tools such as VMware vRealize Orchestrator automate policy generation at the same time new apps or services are provisioned, ensuring security gets seamlessly embedded into the overall process.

- **Traffic visibility.** The Check Point Smart dashboard monitors network traffic across physical, virtual, and cloud-based infrastructure. This can help organizations fine-tune security controls based upon changes in risk. Furthermore, vSEC can work directly with threat intelligence feeds to quickly identify suspicious network behavior or known indicators of compromise (ioCs). This helps the security operations team take proactive steps to defend the network against sophisticated cyber-attackers or respond quickly when necessary.

- **Granular policy creation and management.** Check Point vSEC supports micro-segmentation but goes beyond for sub-policy support. Sub-policies can be used to enforce segregation of duties. This provides granular network protection and process automation while assuring that security policy provisioning and change management follow security best practices. Check Point security policy orchestration also allows for service insertion so policies are automatically set and follow a particular service regardless of its location. Additionally, the granularity of sub-policies extends to the API rule level, allowing APIs to be in-scope with policy provisioning and change management procedures, thus eliminating

the possibility of developers inadvertently modifying the security posture and exposing the entire organization to new threats.

- **Contextual knowledge for security policy enforcement.** With tight integration into SDN controllers, vSEC can actually discover and learn about the details of virtual networks like VMs, tags, groups, labels, etc. In VMware NSX environments, Check Point goes even further by providing two-way integration with SDN controllers for policy enforcement. When vSEC identifies an infected VM, it can tag the VM as quarantined and send the new VM tag to NSX. If NSX has an auto-remediation workflow—even with other third party vendors—the workflow can be triggered automatically by vSEC updating the VM classification/tag. Once the remediation workflow is completed and the VM is cleaned/fixed, NSX re-tags the VM and the new classification is automatically forwarded to vSEC for updated security policy. Check Point vSEC is also tightly coupled to applications so that strong security remains linked to application workloads even if they change location or configuration. Finally, vSEC supports multiple data sources, including NSX, vCenter, and Cisco ACI. This obviates the need for multiple redundant operations tasks, reducing cost and complexity.

With vSEC, Check Point can do something that most other cybersecurity technology vendors can't—bridge traditional, cloud, and SDDC infrastructure with a central platform for policy management, enforcement, and comprehensive monitoring. This is really what enterprise organizations need to gain cloud and SDDC benefits while managing risk.

The Bigger Truth

Cloud computing and SDDC represent a major IT transition requiring new skills, policies, and processes. DevOps teams are moving ahead in these areas but unfortunately, some CISOs have not been able to keep up with an accelerated pace, leaving organizations at risk.

What can organizations do? Marry security best practices with specific policies, processes, and controls designed for cloud and SDDC environments that include comprehensive monitoring, tight integration, and granular policy enforcement. Check Point vSEC does exactly this, combining traditional Check Point management, controls, and visibility with new capabilities for cloud and SDDC. Furthermore, Check Point supports leading cloud and SDDC technologies, providing organizations with the coverage they need for heterogeneous environments. Given these strengths, CISOs looking for strong cloud security may be well served by evaluating how Check Point can help them address short- and long-term cloud security requirements.