Solution Brief

HyTrust and Intel Provide a Foundation of Enterprise-class Security for Server Virtualization and Cloud

Date: January 2014 **Authors:** Jon Oltsik, Senior Principal Analyst, and Wayne Pauley, Senior Analyst

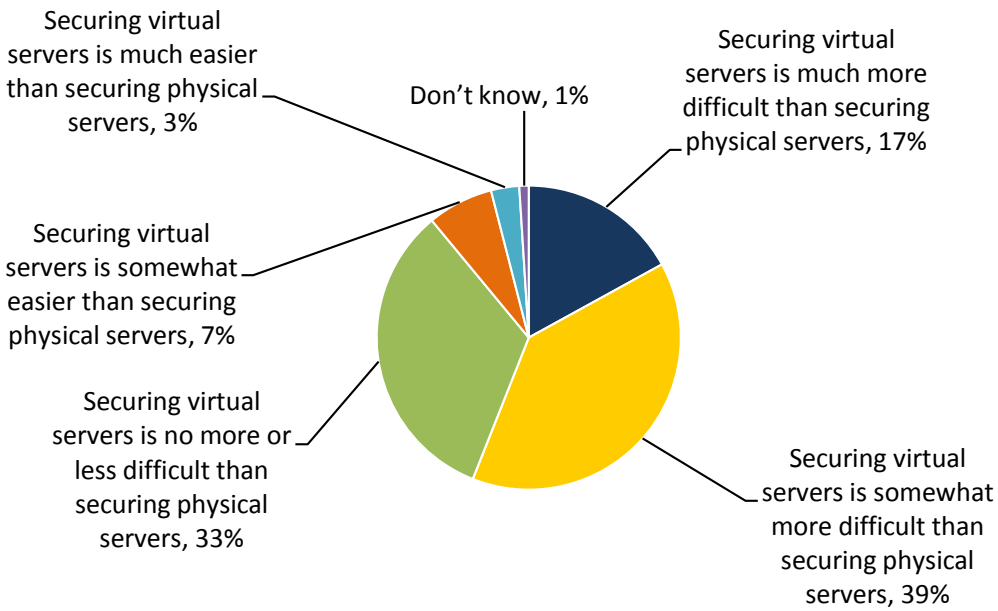
Abstract: *As companies continue to migrate from physical to virtual and cloud environments, security controls and practices also have to be modified to maintain an appropriate risk posture. Unfortunately, virtualization and cloud introduce several new challenges that need to be addressed with specific tools to align security best practices and virtualization and cloud technology integration. HyTrust and Intel have developed a security system that provides an end-to-end solution designed to mitigate the new risks commonly associated with virtualization and cloud technology. This system can help organizations accelerate server virtualization and cloud adoption for overall business benefit.*

Overview

According to ESG research, 90% of respondent enterprise organizations have deployed, or plan to deploy, server virtualization technology within their data centers. In spite of server virtualization ubiquity, however, many organizations still struggle with server virtualization security. In a survey of security professionals working at enterprise organizations (i.e., more than 1,000 employees), 17% of respondent enterprises claim that securing virtual servers is much more difficult than securing physical servers, while 39% believe that securing virtual servers is somewhat more difficult than securing physical servers (see Figure 1).[1]

Figure 1. Perceived Difficulty of Securing Virtual Servers versus Physical Servers

Which of the following statements about virtual server security do you believe is most accurate? (Percent of respondents, N=270)



Source: Enterprise Strategy Group, 2014.

[1] Source: ESG Custom Research, *Data Center Security Trends*, July 2012.

Why is virtual server security so difficult? Physical servers usually have a well-understood set of demarcations for administrators and security personnel. The server's OS and storage are managed within one physical server by the system administrator, and the network is managed by a networking person. Security policies rely on the associated separation of duties as well as the physical barriers. For example, the web server(s), applications server(s), and database server(s) can be separated by using physical servers, network segmentation, and a variety of security controls. With virtualization, the web server, application server, and database server can all reside on the same physical server. Security professionals remain somewhat uncomfortable with security zone collocation, so they hang on to awkward but familiar physical security controls.

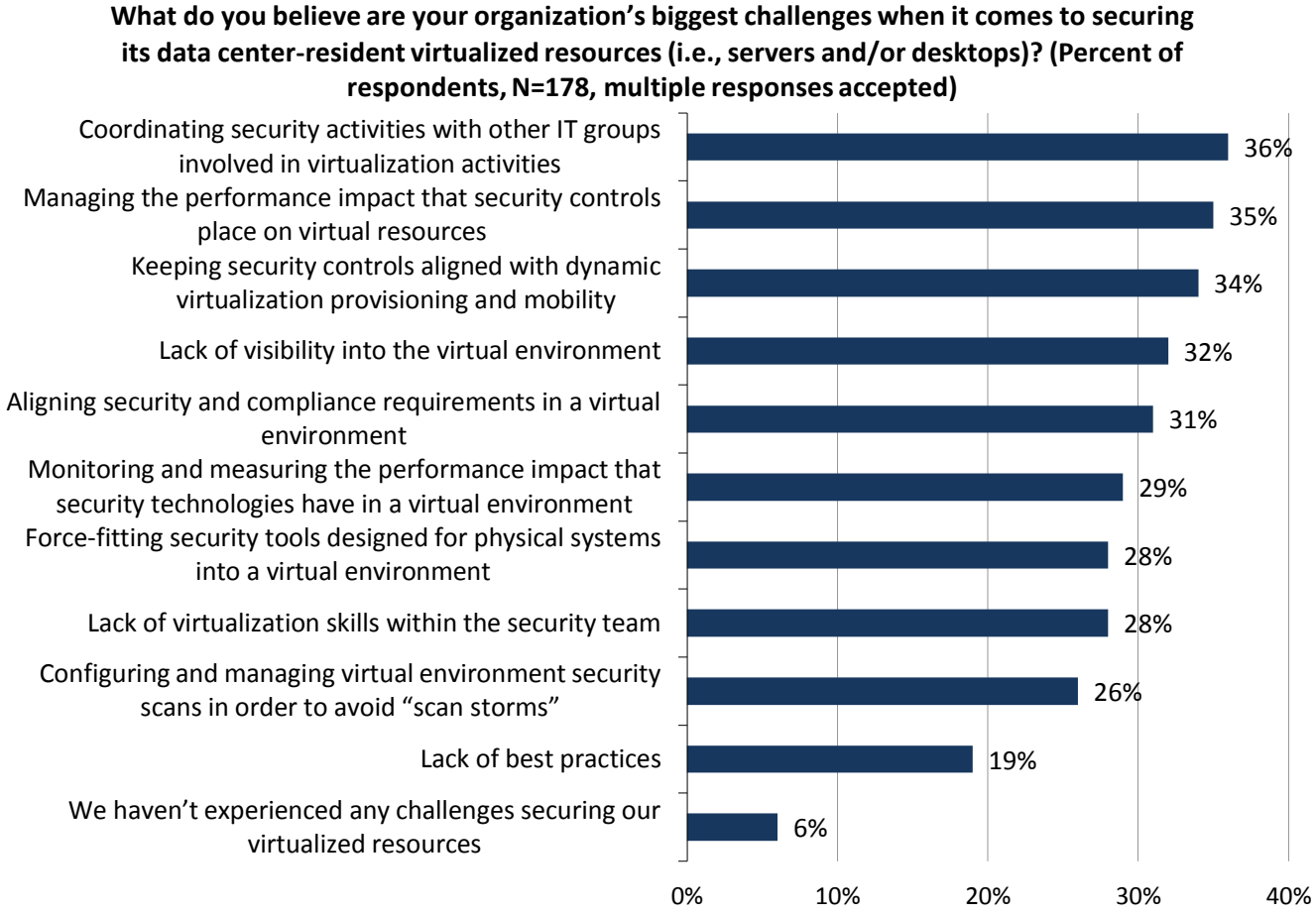
This same misalignment is also present in security roles, responsibilities, and governance. Virtualization and cloud tend to merge many IT roles and functions by virtualizing physical technology layers and consolidating provisioning and configuration tasks. This can improve systems deployment and consolidate resources while concentrating risk within technologies, groups, and processes. For example:

- In a virtualized system, a system administrator has root access to the entire infrastructure stack, breaking the security tenet of separating duties and giving the admin broad control of multiple systems and all the layers. This makes CISOs extremely uncomfortable and could be a violation of the Gramm Leach Bliley Act (GLBA), Payment Card Industry Data Security Standard (PCI-DSS), and Sarbanes-Oxley (SOX) compliance mandates.
- Many virtualization and cloud management tools have just been migrated to virtualized environments without being updated to provide separated control and visibility across the affected infrastructure stack (compute, network, and storage). In other words, one administrator may have limited or no visibility into what administrators for each component of the infrastructure stack are doing. This environment reduces the security administrator's ability to properly monitor and audit for compliance, governance, and security management.
- Consolidation of servers via virtualization leads to a higher density of information assets (e.g., shared storage) and increases the risk of unintentionally mixing assets of different values and security sensitivity on systems. Consolidation and co-mingling can radically change the risk and threat level of high-value assets.
- As software-defined networking (SDN) evolves, similar risks to server virtualization cause networks to lose their physical boundaries. This in turn has an impact on role separation as the network devices (routers, switches, ports, and IP protocols) can be consolidated to one administrator role. Additionally, it may also force management tools to be modified to support SDN role and network layer aggregation.

An ESG research survey's findings support the prevalence of these security challenges with virtual data center resources: 32% of respondents claim that visibility is a top challenge, 31% say they have problems aligning security and compliance requirements, and 29% are having trouble monitoring and measuring performance impact of security tools in a virtualized environment (see Figure 2).[2]

[2] Source: ESG Custom Research, *Data Center Security Trends*, July 2012.

Figure 2. Organizations' Biggest Challenges When Securing Data Center Virtualized Resources



Source: Enterprise Strategy Group, 2013.

Server Virtualization Must Align with Enterprise Security

To date, server virtualization security has often been an afterthought and is usually focused on security technologies such as antivirus software and firewalls as a way of emulating what was implemented in a physical environment. So what's missing? Real security command and control for server virtualization needs to include support for:

- **Security administration.** To support security best practices for separation of duties, security administration must be based on multi-factor authentication, role-based access control, a "two-person" rule, and tamperproof logging of all administrator activity. Furthermore, administrators need the capability to log and validate changes that are no longer tied to a specific location or physical server. Finally, multi-tenancy security administration must be designed for multiple "tiers" to delegate data center controls and provide "tenant" view to a range of administrators (guest OS).
- **Policy management and enforcement.** The goal is to create a centralized policy management and enforcement program with security oversight and privacy controls. Virtualized workloads require establishing a trust relationship between workloads and the hardware for tamper proofing and attestation. It is also critical to provide encryption and strong key management for data at rest across multiple VMs. The ability to create groups based on information asset value can greatly ease security operations here. Lastly, enterprises require secure provisioning based upon workload classifications, templates, and controls to verify the integrity of the platform as well as to harden it appropriately.
- **Comprehensive monitoring, reporting, and auditing.** IT and businesses need to be able to adequately assess risk without having to use separate tools, merge, or consolidate reports by hand. The foundation for this is

the integration of hypervisor APIs for visibility, plus the integration of contextual data to and from SIEM and security analytics. Security professionals also need visibility into privileged account activities at all layers: hypervisor, VM, guest OS, network, and storage. For compliance support (HIPAA, PCI, FedRAMP, EU, etc.), proof of residency is needed. As outlined by NIST in Interagency Report 7904, companies should start with platform attestation and trusted hypervisor launch, homogeneous migrations within trust zones, and support for geo-location restrictions.

These features make it possible to mitigate downtime from accidental and planned attacks, improve the efficacy of security talent (a scarce resource) by automating labor-intensive compliance reporting, and increase the benefits of virtualization by enabling higher risk assets to be virtualized.

HyTrust and Intel Solution for Server Virtualization and Cloud Security

HyTrust's solution provides the tools needed to extend enterprise data center security controls into virtualized and cloud infrastructures. In this way, HyTrust makes it possible for enterprises to meet security and compliance requirements while reducing IT risk. When the HyTrust solution is combined with Intel Trusted Execution Technology (Intel TXT), CISOs can implement strong security featuring geo-location and hardware-based root of trust controls.

The HyTrust and Intel solution can be used for end-to-end deployment to augment and extend a company's physical security posture. The following are some key features designed to improve protection of virtual and cloud infrastructures:

- The foundation of the virtualized infrastructure stack can be managed by HyTrust, which provides templates for hardening the hypervisor. When combined with Intel TXT, HyTrust can also verify the trust of the hardware layer and attest it to the hypervisor and virtual machine guest OSs. These features can help administrators defeat root kit attacks, reduce configuration drift, and enable trust pools aligned with geo-tagging.
- HyTrust works as a security hub for administrators and augments VMware vCenter security controls with fine-grained authorization that can enforce important separation of duties and strong multi-factor authentication. It also includes support for multi-tenancy, which can logically isolate each tenant's VMs from other tenants'.
- The HyTrust solution also includes a centralized policy management engine that has best-practice templates for provisioning for regulatory requirements such as PCI-DSS, FISMA, and HIPAA.
- HyTrust's monitoring and reporting tools are built on the audit-quality logs maintained by HyTrust. Regulations like PCI-DSS, FISMA, and HIPAA require that every event is logged, including change requests, user logs of actual and attempted activity, source IP addresses, and reconfigurations. Virtualization introduces several new considerations with logging such as workload migrations and shared physical servers. HyTrust provides granular virtualized-infrastructure-specific log data so that auditors can easily access all the logs from virtualized and non-virtualized resources. This can help appease auditors as enterprises embrace virtualization and cloud for regulated workloads.
- HyTrust provides support for VMware today, and for KVM and OpenStack environments in the future, allowing customers more choice in virtualization and cloud technologies. In the future, HyTrust will expand its virtualization and cloud platform support further, including support for Intel geo-tagging.
- With its recent acquisition of HighCloud Security, HyTrust adds the ability to encrypt data and automate key management in any private or public cloud, independent of the hypervisor type. Notably, HyTrust's encryption engines automatically detect when Intel chipsets with AES-NI are present, so they can achieve hardware encryption speeds.

In aggregate, HyTrust is designed to help enterprises secure their virtualized and cloud environments. When combined with Intel TXT, the solution provides a security framework that extends the traditional security controls with key features needed to manage a dynamic infrastructure while making workloads more mobile. In this way, HyTrust can certainly help CISOs align security requirements with IT/business strategy for virtualization and cloud computing.

The Bigger Truth

Large organizations have been using server virtualization and achieving pivotal consolidation benefits for years, but security concerns continue to hinder virtualization and cloud deployment. It's about time that CIOs and CISOs find the right technology, as well as organizational and process solutions, to move beyond these historical limitations.

In truth, businesses want to virtualize all their workloads, not just low-value assets like test and development. They also want to have the same enterprise-class security posture with their virtualized and cloud systems. HyTrust fills the gaps and helps mitigate the risks that can occur when systems are virtualized. HyTrust can also help address new risks created with virtualization by consolidating workloads, collapsing roles, and allowing workloads to be mobile.

HyTrust provides security administrators with the tools needed to institute an additional layer of oversight and protection for all information assets running in either a virtualized or cloud environment. CISOs would be well served to evaluate HyTrust to assess how it can help add strong security controls and oversight to server virtualization and cloud computing. This may help the security team overcome historical problems and align strong security with their organizations' server virtualization and cloud strategies.