*ESG Brief*

# Addressing Virtual Security with Boundary Controls from HyTrust and Intel

**Date:** August 2014 **Author:** Jon Oltsik, Senior Principal Analyst

***Abstract:*** *Everyone knows that server virtualization and cloud computing can introduce new security risks and limit security visibility and control. In spite of this reality, many organizations continue to secure virtual environments with legacy security technologies built for physical servers in tightly-controlled data centers. This is a complete mismatch that only increases IT risk. So what's needed? New types of virtual security controls that allow organizations to create and enforce policies at the virtual workload level. Furthermore, virtual security technologies should provide VM encryption and enforce policies whereby more sensitive VMs can only run on specified trusted server environments. HyTrust Boundary Controls offer these exact capabilities by integrating with the Intel Trusted Execution Technology (Intel TXT). In this way, global organizations can use HyTrust Boundary Controls to create, audit, and enforce security policies for geographic data privacy mandates, application security, high-availability, and data security.*

## Overview

Over the past few years, enterprise organizations have consolidated data centers, embraced server virtualization and are exploring opportunities for the use of public and private cloud computing. It is safe to say that these trends will only accelerate. For example, ESG research indicates that 72% of organizations will increase spending on cloud computing in 2014. Furthermore, 32% of organizations say that server virtualization is one of their top IT priorities for 2014 as they continue to make virtualization the corporate standard and replace legacy applications with cloud/virtual alternatives. [1]

While these trends may help organizations cut capital and operating costs, they can be a nightmare for the security team. Why? Server virtualization introduces the concepts of rapid provisioning, software-based orchestration, and mobility to data centers. In other words, server virtualization and cloud add an element of massive and constant change to IT, and as every security professional knows, change is the enemy of strong security. Cloud computing exacerbates IT risk even further as it provides a technology platform for moving business-critical applications and sensitive data outside the confines of the data center and thus beyond the purview of the security team.

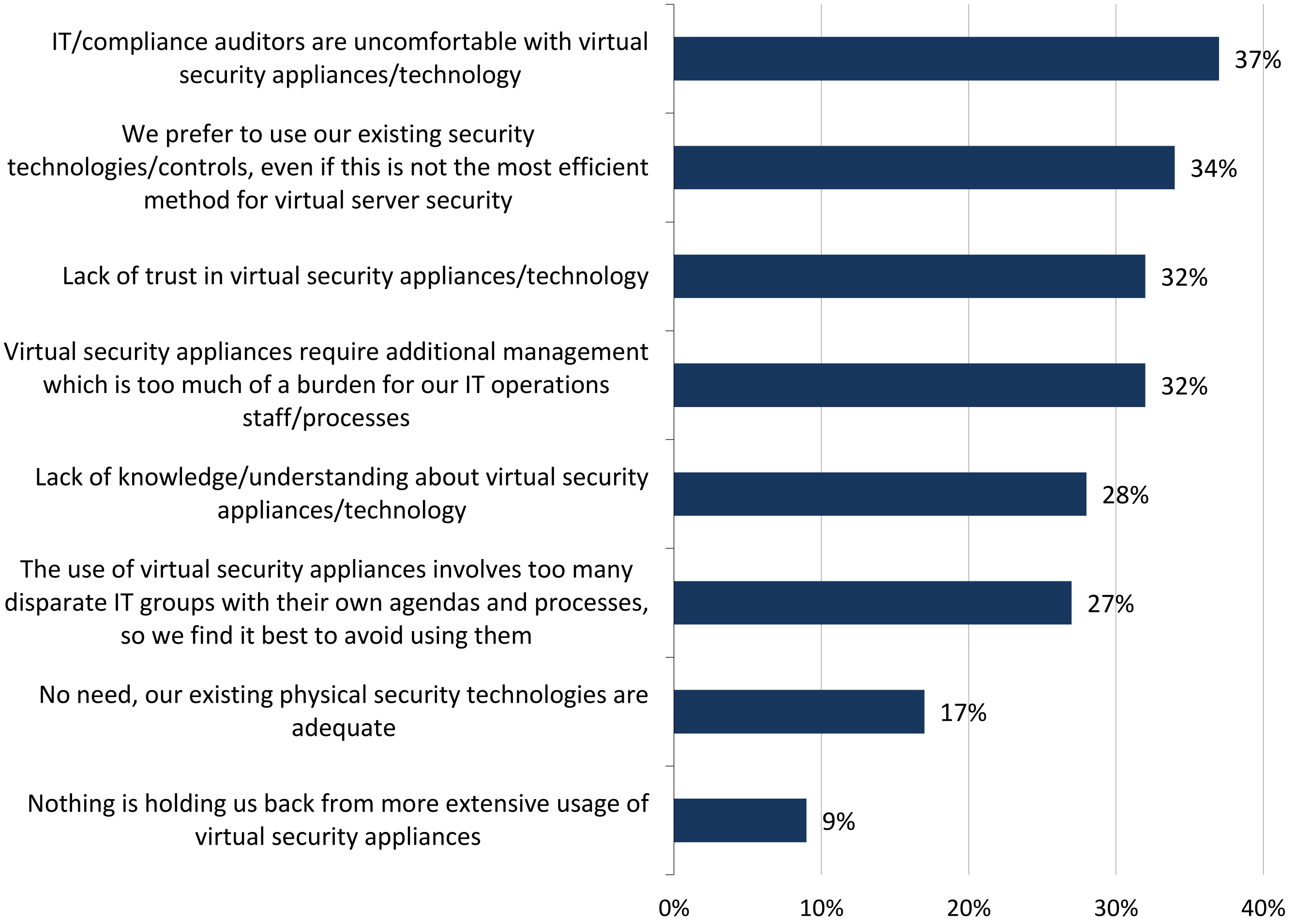
### Server Virtualization, Cloud Computing, and Status Quo Security

Many organizations have years of experience with server virtualization and are moving quickly with private and public cloud initiatives. In spite of this progress however, some enterprises continue to secure these new IT initiatives with legacy security controls, like physical firewall appliances and IDS/IPS or network segmentation, designed for protecting physical servers and their associated data. This is due to the fact that a good number of organizations remain uncomfortable with more modern virtual security appliances/controls. Furthermore, many firms don't have the right skills, knowledge, or organizational structure to deploy and manage virtual security controls on an ongoing basis (see Figure 1).[2]

[1] Source: ESG Research Report, *2014 IT Spending Intentions Survey*, February 2014.
[2] Source: ESG Research Report, *Network Security Trends in the Era of Cloud and Mobile Computing*, August 2014.

*Figure 1. Reasons Why Enterprise Organizations Aren't Using Virtual Security More Extensively*

**Which of the following factors, if any, have held your organization back from more extensive use of virtual security appliances for filtering traffic between virtual servers?(Percent of respondents, N=294, multiple responses accepted)**



*Source: Enterprise Strategy Group, 2014.*

Physical security technologies may be as comfortable as an old pair of shoes and they were probably adequate for protecting small virtual server farms or private cloud proof-of-concept projects of the past. Unfortunately however, legacy security controls are no match for the scale, mobility, and software-based orchestration of enterprise-class server virtualization and cloud implementation. Furthermore, virtual workloads often contain sensitive data subject to the requirements of regulations like the EU privacy directive, FISMA, HIPAA, or PCI DSS. Legacy security controls may meet these stipulations when virtual workloads are first deployed, but security oversight quickly dissipates as workloads migrate across servers, data centers, and from private to public clouds. Finally, sensitive data—like customer information and intellectual property—is a targeted asset for cybercriminals and state-sponsored hackers. Since legacy security controls can't provide adequate protection for virtual servers, large organizations using server virtualization and cloud computing face increasing IT risk.

### Server Virtualization and Cloud Computing Need Tighter Security Control

While server virtualization and cloud computing create a number of information security challenges, the primary issue is an overall lack of control. VMs are mobile by design, which means that they can move from a secure to an insecure server or migrate from a secure internal data center to the public cloud. Virtual workload mobility also adds the risk of physical or cyber-theft, where a VM containing sensitive data may be stolen and then reveal all its secrets while running on a generic hypervisor as a "pay-as-you-go" cloud workload.

This mismatch between server virtualization and cloud computing flexibility and information security/compliance requirements creates a vulnerability gap that needs to be bridged as soon as possible. To gain the right level of security control for sensitive applications and data in virtual environments, large organizations require more than legacy security controls and DMZs. Virtual workloads must be protected with:

- **Strong encryption.** Sensitive VMs should remain encrypted whenever they are not used for application processing. When actually in use, VMs' decryption should also be controlled so that sensitive workloads can only execute on authenticated servers when the IT, security, compliance, and risk teams allow them to. This can help eliminate the risk of lost or stolen VMs falling into the hands of cyber adversaries.
- **Fine-grained server zoning.** Network segmentation works well when IT controls all components of the network but provides little protection when workloads move beyond the security team's view. To gain control over virtual servers, CISOs need the ability to create and enforce policies aligning workloads with execution environments. For example, the European Commission's Safe Harbor policy limits the export of personal data of European citizens and pending European laws may further limit or even prohibit data export in some cases. To comply with this law in a server virtualization or cloud computing infrastructure, large organizations will need to enforce policies that restrict the execution of VMs containing European citizens' PII to servers that physically reside on the continent within the EU.
- **Comprehensive auditing.** As VMs move and execute, CISOs and compliance officers need an audit trail to make sure they remain in compliance. Additionally, CISOs will want to know about VMs that may violate policies so they can fine-tune security controls and investigate policy violations.

## Introducing HyTrust Boundary Controls

HyTrust is quite familiar with security and compliance challenges associated with server virtualization and cloud computing. In fact, many enterprise organizations are using HyTrust CloudControl and HyTrust DataControl for fine-grained administrative control, VM-level visibility, detailed auditing, and data security for private, hybrid, and public cloud initiatives. With its introduction of HyTrust Boundary Controls, the company now extends these competencies by giving its customers the ability to enforce policies governing where virtualized applications and data can execute.

Boundary Controls are based upon HyTrust's tight integration with Intel's Trusted Execution Technology (Intel TXT). The combination of HyTrust's policy engine and Intel TXT can enable enterprises to set policies ensuring that sensitive applications and data workloads can only run on authenticated trusted hosts, physically located in specific trust zones, data centers, or geographic locations.

With Boundary Controls, HyTrust can actually improve upon existing security best practices by extending the concept of a security zone beyond the network layer alone. In fact, Boundary Controls can actually add three additional layers of protection:

1. **Platform hardening.** Intel TXT provides the capability for server attestation, allowing security teams to validate server configuration integrity and identify any unauthorized changes to the system.
2. **Geo-fencing and location-based controls.** With Boundary Controls, users can put policies in place to ensure that virtual workloads only run in specific geographies or locations. This is essential for compliance with existing and burgeoning privacy regulations.
3. **Encryption/decryption.** Virtual workloads remain encrypted and can only be decrypted when executed on a TXT-validated server. When a hacker in Odessa steals a VM containing sensitive data, she will be unable to read the data using a generic hypervisor or cloud service.

Given these capabilities, HyTrust Boundary Controls align well with use cases for application security, data security, high-availability, and regulatory compliance. In this regard, HyTrust Boundary Controls are well suited for bridging the gap between cloud computing benefits and cybersecurity concerns. As such, they may be a perfect fit for large global organizations with aggressive cloud computing agendas and strong security requirements.

## The Bigger Truth

Server virtualization and cloud computing have become IT staples and these initiatives will only grow in the future so it's imperative that CISOs find new ways to support IT and the business with the strong security controls and oversight necessary. Since this objective can't be accomplished by relying on legacy security technology, security professionals must assess the capabilities of existing controls and processes, research innovative new options, and implement the right security as soon as possible.

ESG offers the following advice to enterprise CISOs: Before cloud computing usurps control, put policies and technologies in place to maintain control. With virtual server and cloud technology, this means that security controls must be tightly aligned with each virtual workload to enforce policies wherever these workloads move.

HyTrust has long recognized the challenges associated with server virtualization and cloud computing security and has provided a number of solutions for application security, data security, and regulatory compliance. With the introduction of Boundary Controls, HyTrust is expanding this role by marrying server virtualization and cloud with trusted computing. This should make Boundary Controls quite popular with global organizations looking for cloud computing flexibility, risk management, and regulatory compliance.