Virtualization Security
Achieving Compliance for the Virtual Infrastructure

By Ted Ritter
Senior Research Analyst, Nemertes Research

Introduction

In theory, 2009 should be the year that virtualization security (VirtSec) takes off: Server virtualization has been widely deployed. VirtSec products are ready. The VirtSec vendor list has doubled since 2008. There’s just one catch: Enterprises aren’t currently planning to deploy the technology. Only 10% of the organizations that participate in Nemertes’ virtualization research have deployed VirtSec—and fully 70% have no plans to do so. Why not? As Strother Martin said in the Movie Cool Hand Luke, “What we have here is a failure to communicate.”

Vendors have been positioning their solutions by focusing on potential virtualization vulnerabilities. Yet that’s not what enterprises care most about. In fact, the overwhelming response to the vendor vulnerability message is “so what’s the big deal?” Instead, what’s top of mind for enterprise IT practitioners is compliance, yet most VirtSec vendors aren’t articulating the ways in which their products can help enterprises address compliance concerns. What’s not top of mind – and should be - is that virtualization makes the strong perimeter defense obsolete.

Top Trends

1.) Enterprises are Adopting Virtualization with Gusto

Virtualization adoption is extremely high. Ninety-three percent of organizations are deploying server virtualization, 78% have virtual machines facing users, and companies typically have virtualized 40% of the application workload, according to Nemertes’ virtualization research.

Virtualization isn’t just popular, it’s also effective: 48% of benchmark participants say virtualization reduces costs, typically by increasing hardware utilization, which cuts server capital expenditures and reduces power consumption. Another 46% say they see increased agility and flexibility, and 38% are experiencing operational efficiency improvements. For example, servers that took weeks to deploy now take minutes. And application recovery from a failed server now is measured in minutes as opposed to hours, or even days.

These benefits are achieved through creation of a new virtualized infrastructure: virtual servers, virtual machines, virtual switches and virtual systems management. To defend this new virtualized environment, vendors have developed a new class of virtual security products.
2.) Enterprises Don’t See a Clear Need for Virtualization Security

The list of VirtSec products is growing rapidly, doubling from 10 to 20, in the past six months. Yet the demand for such products remains weak. As noted, fewer than 10% of organizations use these tools, and almost 70% have no plans to use them in the next three years, though that can (and should) change as IT practitioners learn more about virtualization security. (Please see Figure 1: Adoption of Virtual Security Tools, Page 2.)

Why is the adoption rate so low? One reason is the relative newness of virtualization in production environments. Server virtualization (in production environments) has ballooned from almost nothing in 2004 to widespread deployment in 2009. In theory, this shift from physical to virtual infrastructure should require IT practitioners to take extra precautions to ensure the virtual infrastructure is as secure as the physical infrastructure it’s replacing. In practice, however, chief security officers (CSOs) say they’re generally able to mitigate virtual risk without the need of VirtSec tools through the use of existing security controls and procedures. This is not optimal, and it may impede some of the benefits of virtualization, but it is sufficient for managing most risk.

Figure 1: Adoption of Virtual Security Tools

©Nemertes Research 2009 ∙ www.nemertes.com ∙ 888-241-2685 ∙ DN0500 2
That’s not to say that VirtSec products are unnecessary, however. There are two areas in which VirtSec meets a clear need. One is compliance, which many enterprises recognize already. And the other is Defense-in-Depth (DiD), a security best practice that is emerging (and will gain momentum) as the best practice of choice for protecting virtualized environments.

3.) Compliance Concerns Drive Security Spending

Nemertes sees skyrocketing compliance concerns. For example, in 2007, 21% of organizations saw compliance as a priority. This number jumped to 30% in 2008. In 2009, 80% of the security practitioners say compliance is the only justification for security spending. “The only way I can get approval for a new technology is if the compliance officer agrees to the need,” says the CISO from a healthcare organization.

Moreover, there’s a clear connection between compliance and virtualization. Eighty percent of participants in our virtualization research say compliance regulations and legislation affect their virtualization initiatives. In some cases, organizations will not deploy virtualization because of compliance concerns. For example, some hospitals are resisting deploying patient-facing applications on virtual servers because the Food and Drug Administration (FDA) has not yet approved these applications to run on a virtual server.

Unfortunately, most compliance regulation or legislation is not prescriptive on how to address the virtual environment. That is, regulations don’t tell organizations how to comply; they just mandate that information and systems are “secure,” without providing a working definition of “security” for the virtual infrastructure. This leads to auditors making judgment calls and security teams jury-rigging existing controls to be “compliant enough” to pass the audit.

4.) The Growing Need for VirtSec to Address Privacy Requirements

Jury-rigged solutions usually aren’t good enough. They may pass an audit at one point in time, but they may lack the monitoring and logging capability to prove ongoing compliance. In particular, regulations relating to privacy pose the greatest concern. It’s especially challenging to track information flow in a virtualized environment, so it can be difficult to impossible to prove that a particular piece of information has not made its way to a specific machine.

Key privacy-related regulations include Payment Card Industry – Data Security Standard (PCI-DSS), which affects any organization that accepts or processes credit cards; Health Insurance Portability and Accountability Act (HIPAA), which affects healthcare agencies and those that handle healthcare records, such as insurance companies or companies and educational institutions that keep personnel or student health records; Gramm-Leach-Bliley Act (GLBA) which affects financial institutions’ collection and disclosure of customer personal data; Family Educational Rights and Privacy Act (FERPA), which affects public...
educational institutions’ protection and disclosure of student records; and the breach notification laws (including SB1386 and the Massachusetts “Breach Notification Law” of 2007, which affect any organization that discloses personally identifiable information (PII) about citizens or residents in, or from a state that has such a law).

None of these requirements offers prescriptive guidance on virtualization. Yet each specifies functionality that is particularly difficult to deliver (or prove) in a virtualized environment, specifically:

1. Building and maintaining a secure network, including separation of duties between development, test and production, and patch management. PCI 6.3.3 and GLBA Title V: Data Safeguards Rule.
2. Maintaining detailed access logs, protection of log integrity and storage of logs for forensic analysis. HIPAA 164.308 and PCI 10.6.
3. Implementing strong access controls to prevent unauthorized access to Personally Identifiable Information (PII) and Personal Health Information (PHI): PCI- DSS 7.2 and HIPAA 164.308 (a)(4)(i).

5.) Virtualization Needs Defense-in-Depth (DiD)

Today, most organizations focus their security efforts outward creating a strong defense at the perimeter of the network (firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), network access control, remote access controls, and penetration testing). The underlying theory is “no trust outside the strong perimeter and near-total trust for anything inside.” Since virtualization is still largely inside the perimeter, IT practitioners oftentimes dismiss the need for VirtSec with statements like, “I don’t add controls to protect my internal physical servers from each other, so why should I add controls to protect my virtual servers from each other?”

This justification is shortsighted. As discussed below, the movement dynamics of virtualization violate a fundamental assumption of the strong perimeter defense: that servers and applications don’t move. Under virtualization, they do, in fact move, sometimes outside the “perimeter” (which increasingly becomes a meaningless concept). The bottom line is these factors make the strong perimeter defense obsolete for a virtualized infrastructure.

Defense in Depth (DiD) is the best practice that must replace the strong perimeter defense in the virtualized infrastructure. The strategy originates in military practice, founded on the assumption that attackers always find a way to penetrate a defense. The practice dictates multiple barriers (wall plus moat plus barbed wire plus fire pits and dragons) rather than attempting one “impenetrable” barrier. The U.S. National Security Agency (NSA) adapted military best practice to DiD information security best practice. Logically, DiD defines an architecture of escalating levels of trust where assets of highest value are at the highest level of
trust, behind the greatest number of defenses. The value of the assets determines how many levels to create.

In a sense, DiD is the evolution from one strong perimeter defense to many strong, overlapping and focused perimeters for defense. For example, levels of trust are created via zones with gateways that monitor, authenticate and authorize traffic moving from one trust zone to the next. Zones and gateways typically include multiple independent subnets (physical or VLAN) isolated via security controls: firewalls, intrusion detection systems/intrusion prevention systems (IDS/IPS), host-based security, strong access controls, log monitoring and integrity protection.

If these controls sound familiar, they are! These are the same controls listed above for compliance requirements. This is not by chance. These requirements are not unique to compliance. They are security best practice as defined in multiple security standards and frameworks. These include International Standards Organization (ISO) 27001/27002, the National Institute of Standards and Technology (NIST) 800 Series, the Department of Defense Information Security Certification and Accreditation Process (DITSCAP) and ISACA’s Control Objectives for Information and related Technologies (COBIT).

Defense-in-Depth is the implementation of a broad set of security controls, policies and procedures that covers the compliance requirements and provides the overlapping and escalating levels of trust (depth).

6.) Defense-in-Depth (DiD) Needs VirtSec

Defense-in-Depth requires applying multiple security control points throughout the physical infrastructure to create escalating zones of trust. Virtualization eliminates these physical control points. This leads security practitioners to either route all traffic on the virtual infrastructure to the edges, where the physical control points remain, or use VirtSec to place virtual security controls (virtual firewall, virtual IDS/IPS, virtual management access controls, virtual server access controls) throughout the virtual infrastructure to restore the desired levels of depth(trust) . As discussed below, the first option is complex, difficult to manage and doesn’t scale well. The only option for DiD in the virtualized infrastructure will be VirtSec.

Technology Framework

To understand how server virtualization poses unique challenges to compliance and drives the need for VirtSec to enable DiD, it helps to start with a quick overview of virtualization and how it works.
What Is Unique about Virtualization?

Server virtualization is the abstraction of physical attributes from the underlying server hardware: IP address, MAC address and OS. This abstraction creates four key differences between physical servers and virtual servers:

- The existence of a new management layer, made up of hypervisors and associated management consoles and interfaces.
- The concentration of multiple servers onto one physical machine.
- The variable state of servers over time: They can be active, frozen, re-activated, stored and reloaded.
- The movement of virtual machines to physical servers in the same data center, a backup data center or even out to a cloud or hosting provider, which creates information flow from machine to machine.

It is these four characteristics that differentiate risk management and compliance in the virtual realm from the physical realm.

Figure 2: Typical Virtualization Environment
To clarify the real risks, we need to assess risk against the four fundamental characteristics of virtualization:

1.) **New Management Layer:** (See items 1 and 3 in Figure 2: Typical Virtualization Environment, Page 6.) This new management layer consists of the hypervisor, its interfaces and management systems. The hypervisor is the abstraction layer that connects virtual machines (VM), each hosting a guest operating system, with the underlying CPU, memory, storage and network interfaces. This connection can be made either directly or through an OS, depending on the type of server virtualization: full virtualization or para-virtualization. The connection to the virtual machines is through a virtual switch, which represents an integral part of the hypervisor.

   The hypervisor also has multiple management access points. For example, with EMC's VMware, there are four access points to the hypervisor: Virtual Network Computing (VNC) client, Secure Shell (SSH), Web and VMware Infrastructure (VI) client.

   To meet the three compliance requirements listed above, the functions required on all management access points include the:

   - Management of administrator passwords;
   - Logging of administrator actions;
   - Maintenance of the integrity of those logs;
   - Ability to use logs for forensic analysis.

2.) **Concentration:** (See item 2 in Figure 2: Typical Virtualization Environment, Page 6.) As noted, one of the key characteristics of virtualization is that it introduces virtual machine concentration. That is, multiple virtual machines operating on a single physical machine. Organizations host an average of 12 VMs per physical server, but some host 30 or more, according to Nemertes' research. The key compliance issue with concentration is separation of duties (SoD).

   In the physical network, establishing separation of duties between server administrators and network administrators is relatively easy because servers and networks are separate entities. This is not the case in a virtualized environment, where server administrators have access to reconfigure both virtual servers and virtual switches (i.e. the network).

   To address this issue, additional security controls are required. The controls might be preventive (software or virtual appliance that isolates access to the virtual servers and the virtual switches) or at a minimum detective (software or virtual appliance that immediately alerts to any SoD violation.)

3.) **Variable State:** (See items 1, 2, and 3 in Figure 2: Typical Virtualization Environment, Page 6.) As discussed above, unlike physical servers, OS, and applications that tend to operate continuously, VMs start, stop and restart with a few mouse clicks.
The existence of variable state adds two dimensions to the compliance requirements:

- Compliance requirements for building and maintaining a secure network include patch and configuration management for VMs, regardless of state. So, controls must be put in place to validate configuration and patching of VMs during all states.
- Access control and logging compliance requirements must also be state independent. How does one validate the integrity of a VM in storage? Two controls address this issue: Strong access controls to prevent unauthorized access to the VM in storage and VM integrity checks to trigger any changes to the VM upon return to an active state.

4.) Movement: (See item 2 in Figure 2: Typical Virtualization Environment, Page 6.) A fundamental benefit of virtualization is the movement of VMs via tools such as Citrix’s XenMotion or Microsoft’s Live Migration. In contrast, physical servers almost never move, and their applications rarely move. In the event of a physical hardware failure, administrators can re-launch applications on different servers, but this is infrequent.

This movement raises unique challenges for compliance and the strong perimeter defense:

- First, as noted, there must be continual logging and protection of integrity of logs to track any changes to the OS and application. So, wherever the VM moves, the log monitoring and log integrity must move with it.
- Movement directly affects SoD. For example, one aspect of SoD is a one-server-one-function. One can’t run a database and a Web server on the same machine. In a virtual environment, running multiple types of servers on the same physical platform is standard operating procedure. Auditors make judgment calls since there is no prescriptive guidance on this yet. To meet this requirement, organizations isolate specific types of applications onto the same virtual host. For example, they may put Web servers on one virtual host and Web application middleware on another. This is fine until VMs start moving. Maintaining this level of separation requires IT to hardwire virtual hosts to specific functions, creating zones to restrict VM movement, or implementing detective controls that immediately warn of a VM in a place it should not be.
- A fundamental assumption of the strong perimeter defense is information flows to and from servers and applications that stay put. Servers that require direct communications outside the perimeter are
put at the perimeter’s outer edge, in a demilitarized zone (DMZ), and the rest of the servers remain inside the strong perimeter. This is a false assumption for virtualization: Virtual machines move from one virtual server to another in the same data center; to a backup data center; and, even out to a cloud-computing environment. And, complete functions such as a DMZ or a Web server may move with these VMs around (or through) the perimeter. The dynamic repositioning of VMs and the corresponding repositioning of the information that flows to/from the VMs requires a defense that creates multiple perimeters and zones of trust.

**Primary Categories of Virtualization Security Products**

Vendors offer a multitude of products to address these unique virtualization characteristics. As with any rapidly growing market, there is much confusion. To make some sense of the technology landscape, we divide it into nine main solutions. (Please see Figure 3: Virtualization Security Products, Page 10.)

1. **Virtual Host-Based Security** - This is a mapping of traditional physical host-based security tools into the virtual environment. This includes host-based Firewall Intrusion Detection System (IDS) and anti-malware solutions designed to run on each guest OS/VM.

2. **Virtual Appliances** – The virtual infrastructure interconnects by a layer-2 virtual switch. The virtual appliance is a security device (FW, IDS, Intrusion Prevention System) that runs in a VM and connects to the virtual switch. As in the physical network, inter-VM traffic may be routed through the virtual appliance to provide network-based security.

3. **Virtual Zones** – A virtual zone is created by a virtual device (application) that connects directly to the hypervisor to establish protected zones in which a VM or group of VMs may move. Zones can extend across the virtual infrastructure. The typical application of these solutions is to create zones for servers at the same level of trust and function. For example, one could create a zone in which credit card-processing servers are isolated from any other type of server.

4. **Virtual Infrastructure Protection** – This is a general category related to locking down the virtual infrastructure. There are three primary methods:
   
   a. **Configuration approach** – Some organizations first lockdown the configuration of the hypervisor to prevent access to any unused ports. Typically, they use a best-practice configuration checklist, such as the Center for Internet Security (CIS) and VMware secure configuration guidelines. These guidelines
recommend establishing a VLAN for virtual infrastructure management. All management interfaces (hypervisor and virtual infrastructure manager) are connected to one VLAN dedicated to management. This approach limits the potential risk of attack through bypass of the management console and direct connection to one of the hypervisors control points. But IT staffs must make sure all management interfaces are connected to this VLAN with strong authentication and authorization to prevent unauthorized users from accessing the VLAN.

b. **Appliance approach** – A more recent technology option is a physical appliance that sits on the physical network and establishes protected communications with all hypervisor control points and virtual-infrastructure managers.

c. **Hybrid appliance/application** – Like the dedicated appliance, this type of solution provides a central control point for authenticated access to all hypervisor and management control points. This approach also requires a small footprint shim that runs with the hypervisor and communicates with the central-authentication server.

![Figure 3: Virtualization Security Products](image-url)
5. **VM Lifecycle Protection** – As VMs move through the infrastructure, they are susceptible to attack. There are two proprietary approaches to tracking VM movement. One approach is to tag the VM with a unique label. The other is to use a fingerprint that identifies the VM by following a proprietary algorithm that looks at specific characteristics of a VM to establish a unique identity. Implementations may just track movement, or track movement and any integrity violation of the VM during movement.

6. **Log and Patch Management** – As with the physical network, there is a class of solutions that provide log or patch management. The virtualized versions are designed to extract logs from VMs and Guest OS and manage patching of guest OS and applications, regardless of VM state.

7. **Configuration Management** – Again, as with the physical network there are solutions dedicated to configuration management. Some solutions are only active when the VM is initially configured while other solutions are actively tracking VM configuration and alerting upon any change in desired configuration.

8. **Anti-Malware** – Malware is becoming an increasing concern in the virtual infrastructure. With the advent of worms like Conficker that disable defense software, anti-malware in the guest OS is insufficient. IDS/IPS solutions can detect and block some malware at the network level during and after infection. However, to fully back up guest OS anti-malware, VirtSec solutions must perform inline and offline scanning and remediation of files and VMs. Furthermore, unlike physical machines, there are likely to be many more dormant VMs than active ones. Unless these dormant VMs are also scanned and remediated they can introduce infections when booted.

9. **Virtualization Security API** – The API is a direct interface to the hypervisor. Depending on implementation, the API presents one control point to monitor and act on all traffic moving through the hypervisor. Further, the API can provide access to memory and CPU resources for both performance monitoring and scanning/remediation of memory-resident malware. VMsafe by VMware is the only example of a security API today.

Some of the VirtSec solutions are identical to existing security solutions and others are unique to virtualization. Also, there is overlap between approaches. For example, IT can combine proactive configuration management with change-alert notification and log management to provide rudimentary VM lifecycle tracking.

The bottom line is that some subset of VirtSec tools is necessary to meet the three key compliance requirements:

1. Building and maintaining a secure network, including SoD and patch management.
2. Maintaining detailed access logs, protection of log integrity and storage of logs for forensic analysis.
3. Strong access controls to prevent unauthorized access to Personally Identifiable Information and Personal Health Information.

VirtSec for Adding Depth to a Virtualized Infrastructure

A tenet of DiD is the ability to place security controls at physical locations to create the escalating levels of depth (trust). Virtualization violates this tenet, just as it does for the strong perimeter defense. In a virtualized infrastructure, there are no physical security control points. Everything is virtual (virtual server, virtual machine, virtual network, virtual management) so the only option for physical control points is at the edges of the virtual infrastructure; the place where virtual ends and physical begins. This results in DiD looking more like a strong perimeter defense. In other words, we move from architecture with escalating levels of trust separated by physical security devices (providing depth) to separate levels of trust that are conceptually parallel, or flat.

Figure 4: DiD in a Virtual Infrastructure

Still, we do see organizations trying to use physical security devices to achieve DiD in the virtualized infrastructure through creation of a virtual trust via server pools linked together by VLAN subnets and complex routing to reach the
physical security devices. To illustrate, let’s look at a typical, three-tier Web architecture. The back-end database servers (normally physically located in the highest trust zone) run in one VLAN subnet, the Web-application servers run in a lower-trust VLAN subnet and the Web front-end runs in a DMZ VLAN subnet. All traffic from each subnet must be routed to the edges of the virtual infrastructure to use the physical security controls to achieve levels of depth. This is very complex to manage and very restrictive since it is essentially hardwiring the virtual infrastructure to look like the physical infrastructure.

To avoid hardwiring, organizations can implement VirtSec devices, applications and APIs to monitor, authenticate and authorize traffic moving between the virtual trust zones wherever virtual control points need to occur. Thus, reestablishing DiD in a virtual infrastructure. (Please see Figure 4: DiD in a Virtual Infrastructure, Page 12.)

**VirtSec Vendors**

<table>
<thead>
<tr>
<th>Selected Virtualization Security Vendors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host Based</strong></td>
</tr>
<tr>
<td>Altor</td>
</tr>
<tr>
<td>Apani</td>
</tr>
<tr>
<td>Catbird</td>
</tr>
<tr>
<td>Centrify</td>
</tr>
<tr>
<td>Check Point</td>
</tr>
<tr>
<td>Configuresoft</td>
</tr>
<tr>
<td>HyTrust</td>
</tr>
<tr>
<td>IBM-ISS</td>
</tr>
<tr>
<td>Lancope</td>
</tr>
<tr>
<td>LogLogic</td>
</tr>
<tr>
<td>McAfee</td>
</tr>
<tr>
<td>NetIQ</td>
</tr>
<tr>
<td>Red Cannon</td>
</tr>
<tr>
<td>Reflex Systems</td>
</tr>
<tr>
<td>Shavlik</td>
</tr>
<tr>
<td>Stonesoft</td>
</tr>
<tr>
<td>Trend Micro</td>
</tr>
<tr>
<td>Tripwire</td>
</tr>
<tr>
<td>VMware</td>
</tr>
</tbody>
</table>

Note: This table is intended to provide a representative, not comprehensive, list of companies offering virtualization security.

Table 1: Selected Virtualization Security Vendors

Two classes of vendors exist today: Purpose-built start-ups and established security players. (Please see Table 1: Selected Virtualization Security Vendors, Page
13.) The initial entries into the market were the purpose-built start-ups. Typically, these are companies offering virtual security appliances and software that provide preventive and detective controls. The second wave of entries includes existing security companies that have taken their physical security products and created virtualized versions; also offering the preventive and detective controls.

**Technology Forecast**

Although enterprise deployment of VirtSec solutions is low today, by 2010 we predict it will be gathering momentum, and by 2013, we estimate up to 50% of organizations running virtualization will require some form of VirtSec. (Please see Table 2: VirtSec Projections, Page 14.)

<table>
<thead>
<tr>
<th>Year</th>
<th>Adoption rates (+, -, flat)</th>
<th>Compliance Requirement Changes</th>
<th>Technology Direction</th>
<th>Vendor Landscape</th>
</tr>
</thead>
<tbody>
<tr>
<td>2009</td>
<td>10% of companies deploying virtualization</td>
<td>None</td>
<td>Dedicated virtual infrastructure solutions</td>
<td>Flattening off of total vendor count. Existing security vendors play a larger role</td>
</tr>
<tr>
<td>2010</td>
<td>13% - 15% of companies deploying virtualization</td>
<td>PCI potentially issuing prescriptive guidance</td>
<td>Incremental functionality and API adoption</td>
<td>Consolidation of vendors and multi-platform support</td>
</tr>
<tr>
<td>2011</td>
<td>20% - 25% of companies deploying virtualization</td>
<td>Prescriptive guidance from NIST</td>
<td>Cross platform security standards and interfaces</td>
<td>Almost all VirtSec will come from big security vendors</td>
</tr>
<tr>
<td>2012</td>
<td>30% - 40% of companies deploying virtualization</td>
<td>Prescriptive guidance from HIPAA and GLBA</td>
<td>Seamless integration of virtual, physical and cloud security</td>
<td>Consolidation into major security products</td>
</tr>
<tr>
<td>2013</td>
<td>40% - 50% of companies deploying virtualization</td>
<td>Further clarification of HIPAA guidance for EHR</td>
<td>Embedded VirtSec in network infrastructure</td>
<td>The emergence of virtualization lifecycle management</td>
</tr>
</tbody>
</table>

**Table 2: VirtSec Projections**

**2009:** 2009 is characterized by uncertainty and vendor refocus. We do not foresee any new breakthrough technologies in VirtSec in 2009.
There is a slight possibility of the U.S. Congress adding requirements to SOX, GLBA and HIPAA to support financial services oversight and preparation for electronic health records (EHR). As discussed below, these changes most likely occur in the 2011-2013 timeframe. Therefore, we foresee no significant changes to compliance regulations in 2009. Compliance vagueness and uncertainty will continue, auditors will continue to make judgment calls, and most enterprises will continue to use existing tools and procedures to comply, as long as they still pass their audits.

Vendors will experience extended sales cycles in 2009 because of enterprise uncertainty generated by continued lack of prescriptive compliance requirements, and the continuing down economic climate. We project adoption to remain around 10% of companies implementing virtualization.

Start-ups such as Altor and Catbird that are succeeding through an early focus on compliance and defense-in-depth, will add incremental functionality (more controls to broaden compliance support) to both expand deployment in existing accounts and acquire new accounts.

Catbird, Reflex Systems and new entry, Red Cannon, will introduce (or continue to emphasize) functionality to support the beginnings of virtualization machine lifecycle management. The ability to track, monitor and control VM movement and integrity is important to both compliance and DiD requirements.

New vendors or existing vendors with new functionality, notably HyTrust and Centrify will address virtualization infrastructure protection. These vendors will emphasize compliance issues and DiD requirements around access controls and logging.

In addition, in 2009, VMware released the full VMsafe API. The VMsafe API provides VirtSec vendors a control point directly into the hypervisor to monitor network, memory, CPU and storage. For compliance and DiD, VMsafe will facilitate Virtual Infrastructure Protection, giving vendors, such as HyTrust and Centrify, more competition. VMsafe API also will level the playing field for virtual appliances since those appliances will be dependant on VMsafe for most of their performance and functionality. This will push vendors to differentiate in other ways, one of which will be to start supporting multiple virtualization platforms.

Existing physical security vendors, such as Check Point, Configuresoft, IBM-ISS, McAfee, Shavlik, Sourcefire, Stonesoft, Trend Micro and Tripwire will focus on building out their base by leveraging their existing customers, and then use those deployments as strong references to expand into the broader market. Staying with an existing vendor relationship mitigates the potential financial risks associated with start-ups and facilitates integration of virtual and physical security management.

All of these vendors have a compliance and DiD story, often as part of a broader virtualization security message. It is critical to assess the benefits for compliance and DiD between products from existing security vendors and
products from start-ups. Performance, price and functionality of the start-ups may outweigh potential benefits of safety and integration with existing vendors.

**2010**: 2010 is characterized by consolidation, stability and hope for prescriptive guidance and multi-platform support. Potential compliance regulation changes are the greatest factor in 2010. We expect PCI-DSS’s Virtualization Security Special Interest Group (SIG) to issue guidance in 2010. If the guidance only clarifies issues related to the virtualization management layer, then adoption of VirtSec will continue to grow at a modest rate. If the guidance extends to address the other unique virtualization factors already noted (concentration, variable state and movement), then we foresee the following:

1. Requirement for monitoring and integrity of virtual machines during any state and in any location, driving the demand for virtual machine lifecycle protection and stronger configuration-management tools.
2. Requirement for stronger separation of duties driving the need for inter-VM virtual firewalls and, or required use of virtual zones.

We also project a wave of acquisition in 2010 by both virtualization platform, and networking and security vendors. Just as VMware acquired Blue Lane in 2008 to release product (VShield Zones) in late 2009, we expect additional acquisitions to add functionality to the virtualization platforms. The most likely candidates will be the companies that focus on virtual-infrastructure protection. It makes perfect sense for the platform vendor to incorporate greater protection of its own environment.

Vendor consolidation will occur through larger vendors (Brocade, Cisco, IBM, Juniper, McAfee, Symantec and Trend Micro) making strategic acquisitions to improve their current position in VirtSec or to buy into the VirtSec market.

If prescriptive guidance for virtualization compliance is issued early in the year, we expect adoption to rise to 15% of companies deploying virtualization. If the guidance is not issued, or is issued late in the year, we project a more moderate rise to 13% of companies.

All VirtSec vendors will focus on incremental upgrades or retooling their marketing and products to focus on compliance and DiD. We do not see many new entries into the VirtSec market in 2010 and we expect some attrition, primarily because of the extension of sales cycles and the tightening of credit/investment in 2009.

We expect the rise of Microsoft Hyper-V and the full release of VMSafe API to push VirtSec vendors to support multiple virtualization platforms. In 2008, 4% of organizations in our virtualization research used Microsoft, 4% used Citrix, and 82% used VMware. By 2010, we expect these numbers to have shifted radically, forcing VirtSec vendors to support VMware, Microsoft and Citrix.
2011-2013: 2011-2013 is characterized by continued guidance and a bifurcation of the VirtSec market. First, we foresee additional prescriptive guidance for compliance driving expanded need for VirtSec:

1. We expect by 2011, the National Institute of Standards and Technology (NIST) will have issued prescriptive guidance for virtualization security best-practices under the Federal Information Security Management Act (FISMA). FISMA already dictates the use of DiD and prescriptive virtualization guidance will open a huge market for VirtSec, though the sales cycles are long and certifications are expensive. For this reason, we project most of the federal business will be through large security and networking vendors that already have established presence.

2. With the focus on IT-enabled healthcare reform and the expanded relationship between government and financial services, we expect HIPAA (driven by electronic health records privacy requirements) and GLBA to be updated with more specific guidance for virtualization and expansion of security controls; since these are laws, effects may not be felt until 2013.

Requirements for cross-platform virtualization security interoperability will drive open standards and interfaces. Vendors will deliver seamless integration of security and security management: physical, virtual and cloud.

Significant consolidation of VirtSec vendors will continue. We project that by this time, Cisco and Juniper will have incorporated many of the VirtSec capabilities into their own products.

This will push VirtSec vendors in one of two directions. To compete against Cisco and Juniper, VirtSec vendors will need tight

---

Enterprise Recommendations

- Securing virtualization requires DiD with components of VirtSec; reevaluate your defense strategy now.
- If you’re among the majority of companies deploying server virtualization and subject to at least one regulation, consider VirtSec tools for specific compliance requirements.
- Meet with auditors to assess the use of in-house tools, procedures and upgrades to existing tools to meet compliance requirements.
- Grill vendors on the relationship between the unique characteristics of virtualization and their effect on compliance.
- Track compliance developments closely. VirtSec tools may become mandatory if compliance requirements become more prescriptive—something we anticipate occurring in 1-3 years.
alignment with or incorporation into mainstay security company products, such as IBM, Check Point, McAfee, Symantec and Trend Micro. It will be very tough for standalone VirtSec players to compete on this field of giants. Alternatively, VirtSec could head toward Virtualization Lifecycle Management. Today, companies such as Catbird, NetIQ, Red Cannon, and Reflex Systems already are extending VirtSec functionality to include management of virtualization resources; most notably VM sprawl management.

We project adoption to increase dramatically in this time period, primarily since VirtSec will be part of so many networking and security products. We project adoption of VirtSec to be as high as 50% of all companies deploying virtualization by the end of the period.

**Conclusion**

Virtualization introduces an entirely new environment to the data center, with unique characteristics associated with management, concentration, variable state and movement. IT staffs must evaluate each one of these characteristics for potential compliance risk. Although no compliance requirements are currently prescriptive for virtualization there are clear areas where VirtSec is required to meet compliance with PCI, HIPAA and GLBA. Moreover, as virtualization deployments mature and expand, the dynamics of virtualization will force organizations to rearchitect their security defenses from a strong perimeter defense to defense-in-depth. Furthermore, to successfully implement DiD, the virtualized infrastructure will require VirtSec.

---

**About Nemertes Research:** Nemertes Research is a research-advisory firm that specializes in analyzing and quantifying the business value of emerging technologies. You can learn more about Nemertes Research at our Website, www.nemertes.com, or contact us directly at research@nemertes.com.