January 12, 2012

The CISO's Guide To Virtualization Security

by Rick Holland
for Security & Risk Professionals

FORRESTER® Making Leaders Successful Every Day

January 12, 2012

The CISO's Guide To Virtualization Security

Get Off The Bench And Look Into Your Virtual Environment

by Rick Holland
with Stephanie Balaouras, John Kindervag, and Kelley Mak

EXECUTIVE SUMMARY

In today's data centers, IT often virtualizes new applications and workloads by default. Virtualization is the norm; deploying a physical server is the exception. The technology is mature and enterprise adoption is high, yet information security does not have a significant focus on virtual security. Given the converged nature of virtual environments, security incidents can result in significant damage; therefore, it is critical that security professionals redouble their efforts and make securing their virtual infrastructure a priority. This guide describes the security challenges within virtualized environments and shows how to apply the concepts of Forrester's Zero Trust Model of information security to secure the virtual environment effectively.

TABLE OF CONTENTS

NOTES & RESOURCES

Forrester interviewed vendor and user companies that deal with virtualization security, including both security and risk professionals and enterprise architects.

Related Research Documents

"Pull Your Head Out Of The Sand And Put It On A Swivel: Introducing Network Analysis And Visibility"
January 24, 2011

"No More Chewy Centers: Introducing The Zero Trust Model Of Information Security"
September 14, 2010

"Fear Of A Hyperjacked Planet"
October 16, 2009

VIRTUALIZATION SECURITY MATURITY LAGS BEHIND OPERATIONS

Server virtualization is nearly ubiquitous. According to our survey data, 85% of organizations have adopted or are planning to adopt x86 server virtualization (see Figure 1-1). In addition, 79% of firms have or are planning to institute a "virtualization first" policy.[1] The majority of clients we interviewed for this report require justification for any physical x86 server deployments; virtualization is the norm, and we have moved passed the days of only virtualizing noncritical workloads. Today, IT professionals have virtualized, on average, 52% of the x86 servers in enterprise environments; in two years, they expect that number to grow to 75% (see Figure 1-2).

This data confirms what we already know: Virtualization has been top of mind for IT professionals such as enterprise architects (EA) as well as IT infrastructure and operations professionals (I&O) for years. What about security professionals? Has it been top of mind for them? Many chief information security officers (CISOs) are not aware of the virtualization security risks, while other CISOs are very concerned about their virtual environments but don't always have the authority or the influence over I&O to enforce policy or implement new security controls.

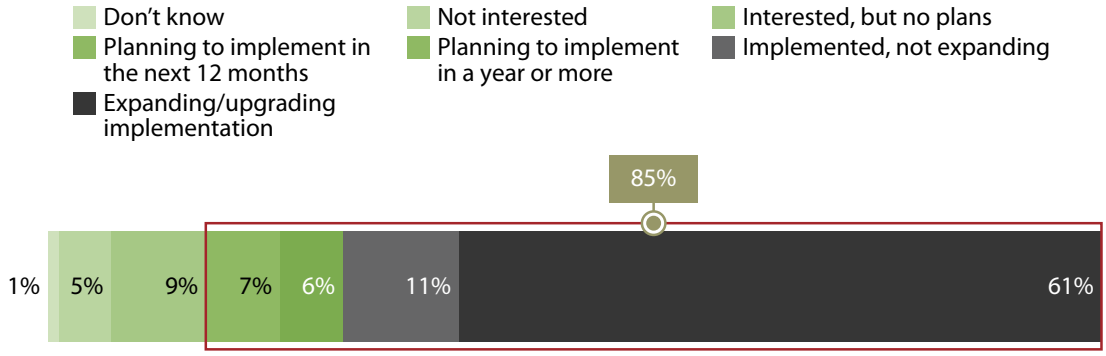
Security Incidents In A Virtual Environment Can Be Disastrous

Let's consider the recent security incident at the Japanese pharmaceutical company Shionogi. In February 2011, a terminated IT administrator, Jason Cornish, used a service account to access the company's network. Once connected, he used an unauthorized installation of VMware vSphere to delete 88 virtual servers. According to the criminal complaint: "the deleted servers housed most of Shionogi's American computer infrastructure, including the company's email and BlackBerry servers, its order tracking system, and its financial management software. The attack effectively froze Shionogi's operations for a number of days, leaving company employees unable to ship product, cut checks, or communicate by email."[2]

Figure 1 Virtualization Is Nearly Ubiquitous

1-1 x86 server virtualization adoption

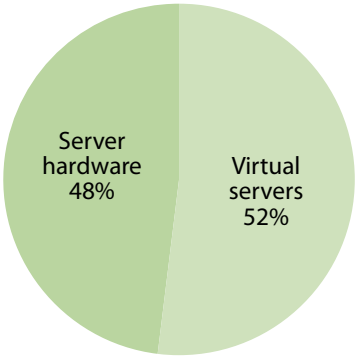
"What are your firm's plans to adopt x86 server virtualization?"



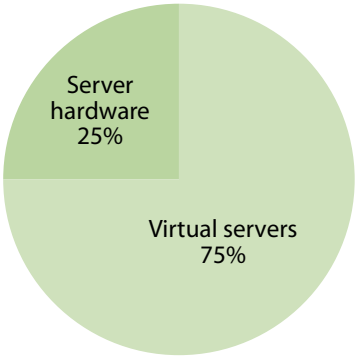
Base: 1,201 North American and European executives and technology decision-makers who are responsible for x86 servers

1-2 The percentage of x86 server virtualization

"Today, approximately what percentage of your x86 server OS instances are operated as virtual servers rather than run directly on server hardware?"
(N = 771)



"In two years, approximately what percentage of your x86 server OS instances do you believe will be operated as virtual servers rather than run directly on server hardware?"
(N = 768)



Base: North American and European executives and technology decision-makers at companies with 20-plus employees and who are responsible x86 servers

Source: Forrsights Hardware Survey, Q3 2011

61230 Source: Forrester Research, Inc.

Security Professionals Are Playing Virtualization Catchup

While I&O professionals have rapidly virtualized the environment to reduce costs and improve flexibility, security professionals have remained on the sidelines — either by choice or because I&O has marginalized them. This is true regardless of the size of the organization. Our research interviews with IT professionals in enterprise architecture, IT operations, and security revealed several troubling themes:

- **Business as usual is the status quo.** IT departments rely upon traditional security solutions to secure their virtual environments. For example, they use endpoint security agents and network security devices designed for physical environments to secure virtual workloads. One security leader said, "We rely on our existing solutions; we haven't yet altered our approach for the virtual environment."

- **Many security pros aren't aware of the available solutions.** We found that most security professionals have very limited knowledge of the efficacy and availability of virtualization-aware solutions that can more effectively secure their virtual environments. One CISO we spoke with wasn't aware that his organization's current antivirus vendor offered an endpoint virtualization solution.

- **Many security pros have a general discomfort with virtualization.** Security pros, especially CISOs and other security leaders who have risen up the technical ranks, aren't as confident in their virtualization knowledge as they would like to be. This is particularly the case when we compare virtualization with more mature security areas, such as network security. One CISO remarked, "We haven't touched this technology as much as we'd like, and we have to physically sit at the console next to operations to see the environment."

EVERYONE KNOWS VIRTUALIZATION'S BENEFITS — BUT NOT ITS RISKS

Lower total cost of ownership (TCO), flexibility, improved high availability and disaster recovery capabilities, and faster time-to-market are just a few of virtualization's benefits. However, all IT professionals — most importantly, security professionals — need to have an understanding of the risks. These include:

- **Limited visibility into intra-virtual-machine traffic.** Depending on your network architecture, virtualization can create blind spots in your network, and many security professionals don't have the tools to inspect intra-virtual-machine (VM) communication (i.e., traffic between two virtual machines on the same virtual server). All of the security professionals we interviewed rely upon traditional network security devices, but if the intra-VM traffic never routes through the physical network, how can you inspect it? Our interviews revealed that many CISOs aren't comfortable with the level of visibility they have into their virtualized environments. One CISO stated, "I know I am wearing rose-colored glasses; we just haven't looked into this."

- **Increased vulnerability to insider threats.** The Shionogi incident illustrates the significance of the insider threat. The collapsed nature of virtual environments exacerbates the impact of insider threats. Forrester estimates that almost half of security breaches were the result of so-called "trusted" insiders and business partners — whether their actions were malicious or unintentional.[3] We can't forget about this scenario — the well-meaning employee who clicks in the wrong place at the wrong time. As the statistics indicate, this is a much more likely situation than a malicious insider.

  The insider threat elevates privileged user management to a whole new level: "I'll see your domain admin and raise you one virtualization admin account." In our interviews, we found that the majority of IT professionals have relatively flat administration roles with excessive permissions. An enterprise architect from a large multinational corporation told us: "Our administrators have complete access to the environment; all admins have access to all zones. We realize it isn't ideal." You don't want to gamble with your privileged users; the administrator is the weakest link.

- **The inability to maintain security controls in a dynamic environment.** Change and configuration management can be challenging in a virtual environment. Even the most junior of IT professionals can quickly provision and delete a VM, and VM sprawl is a reality for many organizations. Additionally, how can you be sure that you have scanned offline VMs for vulnerabilities and patched them?

  Technologies such as live migration help organizations harness the power of virtualization and make the environment extremely dynamic. Today, 50% of enterprises use live migration, and 13% are planning to implement it in the next 12 months.[4] How confident are you that when an IT pro migrates a guest VM from one virtual server to another that its security posture follows?

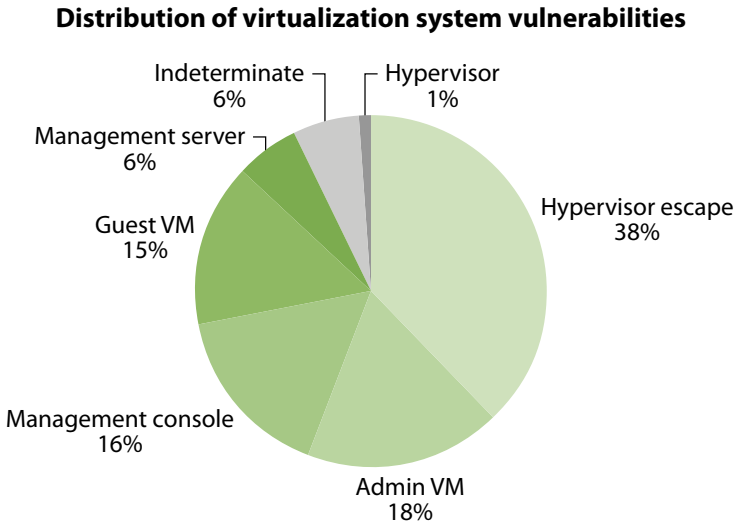
- **An increased compliance footprint.** Virtualization also increases our compliance efforts. As with any new technology, the auditors are playing catchup. In June 2011, the PCI Security Standards Council issued its first guidance on virtualization security, and you can expect challenges as auditors interpret and organizations attempt to comply with the PCI DSS Virtualization guidelines.[5] There is inconsistency among Qualified Security Assessor (QSA) firms; some firms permit virtual mixed mode segmentation, while others do not. You can also expect other compliance organizations to follow PCI's lead and offer guidance on virtual environments.

- **The requirement to secure more layers of infrastructure and management.** Virtualization brings new layers that we must secure. We have additional infrastructure and management layers to protect as well as the hypervisor itself. If an insider or cybercriminal compromises either, all bets are off. Virtual systems aren't unique and are just as vulnerable as any other system running code. If it runs code, someone can compromise it. In 2011, VMware had released 14 security advisories as of December 17.[6] In its X-Force 2010 Trend and Risk Report,

IBM researched 80 vulnerabilities and found that more than 50% could compromise the administrative VM or lead to hypervisor escapes (see Figure 2).[7]

In previous research, we addressed the security of the hypervisor and concluded that it introduces some marginal risk to the server environment but that concerns are largely overblown.[8] As the CISO of one large manufacturing company put it: "Am I worried about hypervisor attacks? Absolutely, but they are very low on a long list of more likely scenarios."

Figure 2 IBM X-Force Virtualization Vulnerability Classes



Base: 80 vulnerabilities that impact server-class virtualization products

Source: "IBM X-Force 2010 Trend and Risk Report," IBM, March 2011

61230 Source: Forrester Research, Inc.

BETTER LATE THAN NEVER: HERE'S HOW TO GET INTO THE VIRTUALIZATION SECURITY GAME

You should strive for virtual security that is at least on par with your traditional security approach and look for opportunities to implement better security within your virtual environment. To do this, Forrester recommends that you: 1) apply the Zero Trust Model of information security to your network architecture; 2) consider virtualization-aware security solutions going forward; 3) implement privileged identity management; and 4) incorporate vulnerability management into the virtual server environment.

Eliminate The Chewy Centers In Your Virtual Environment

Forrester's Zero Trust Model of information security should serve as the foundation of your virtual infrastructure.[9] In the Zero Trust Model, you eliminate the traditional security concept of the data center with a hard crunchy outside and a soft chewy center. In Zero Trust, there is no longer a trusted internal network and an untrusted external network. In Zero Trust, all network traffic is untrusted. Also in this model, IT and security architects redesign the traditional hierarchical network to be segmented, parallelized, and centralized. Future Forrester research will take a much deeper look at virtualization within the context of the Zero Trust Model.

Consider Virtualization-Aware Security Technology

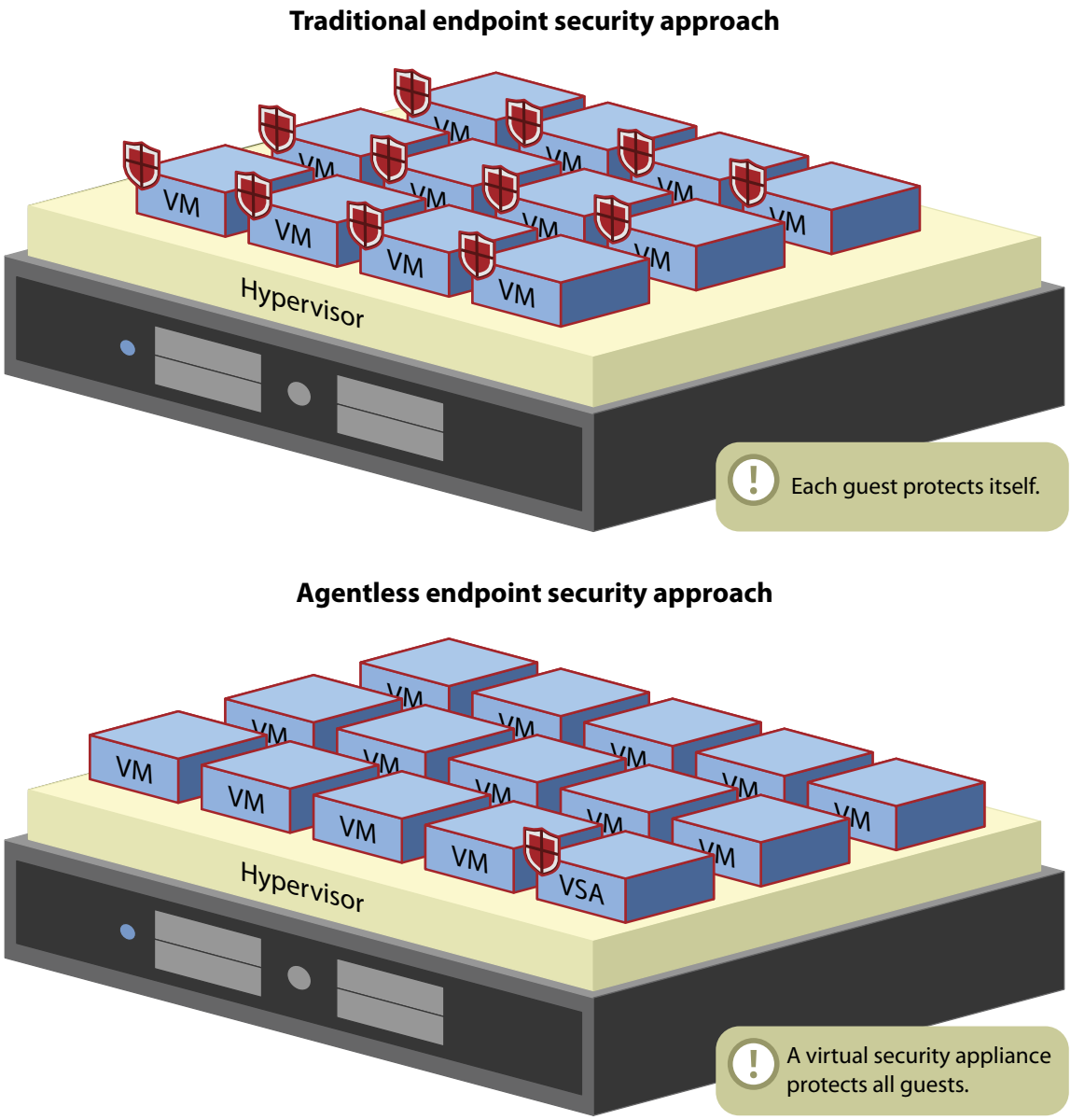
You don't have to rely on traditional security solutions alone to secure your virtual environments; there are many virtualization-aware security solutions available on the market. Although the technologies continue to mature, they can:

- **Deliver business value by increasing virtual server density.** Most security pros are using traditional endpoint point security solutions in their virtual environments. Consider this example: You have a virtual server running 15 VMs. Each of the 15 VMs runs an endpoint security agent that requires memory and CPU. Those resources aren't available for other virtual servers, thus reducing the number of VMs you can effectively run on the server. The CTO at one highly virtualized enterprise said, "At 80% virtualization, we are looking for any opportunity to increase the density and return on investment (ROI) of our virtualization investment."

  To eliminate the requirement to deploy an endpoint agent in each VM, consider hypervisor introspection. Hypervisor introspection allows third-party vendors such as Bitdefender, Kaspersky Lab, McAfee, and Trend Micro to deploy a single virtual security appliance on the virtual server, which then takes over endpoint security responsibilities. This frees up memory and CPU that additional virtual machines can use, thereby increasing your density and improving your ROI (see Figure 3).[10]

- **Provide better visibility and security.** Virtualization-aware technologies provide much-needed visibility into intra-VM communication. There are many security solutions available, including Cisco Systems' Virtual Security Gateway, Fortinet's FortiGate virtual appliance, and Juniper Networks' vGW Virtual Gateway. Virtualization-aware solutions can also provide a wealth of operational data, allowing both security and IT operations staff to leverage them. For example, Reflex Systems offers virtual security capabilities as well as utilization capacity planning and forecasting.

Figure 3 Agentless Endpoint Security



61230 Source: Forrester Research, Inc.

Take A "Zero Trust" Approach To Privileged Identity Management

The principals of the Zero Trust Model are critical for identity and access management (IAM) within your virtual environment. As the Shionogi incident illustrates, managing privileged users is one of the most important duties in a virtual environment. As such, we recommend that you:

- **Ensure that users access all resources securely regardless of location.** Your privileged users should be using two-factor authentication to access and administer the virtual environment. You should also ensure that service accounts aren't permitted to access the environment externally.

- **Adopt a "least privilege" strategy and strictly enforce access control.** Eliminate flat administrative access where feasible and set up one management plane to manage access to your virtual environment. You must consider access to the virtual network, the virtual servers, as well as virtual storage. CA and HyTrust offer a combined solution that controls management plane access as well as privileged user monitoring. BeyondTrust's PowerBroker for Virtualization also addresses privileged user management in virtual environments.

- **Log all traffic so that you can quickly respond and recover.** The greater the access levels of your administrators, the more important your logging and auditing facilities become. If you suffer from an accidental or malicious insider event, you need to have the right tools in place so that you can quickly detect a policy violation or suspicious activity. The hypervisor or the virtualization management layer can provide some logging capabilities. Audit and logging are critical for highly regulated organizations; solutions from Catbird Networks can assist organizations with achieving compliance in virtualized environments.

Incorporate Vulnerability Management Into Your Virtual Environment

You must extend your vulnerability management program into your virtual environment. Server hardening, including patch management and configuration management, is a core element of vulnerability management. A number of good resources are available to assist you with hardening your virtual servers.[11] You must also ensure that you are conducting regular vulnerability assessments, including scanning and penetration testing, of the environment. Rapid7 recently released Nexpose 5, which integrates with VMware to provide the capabilities to scan workloads as they come online.[12] You should include virtualization-specific penetration tests to validate the hardening and security controls of the environment.

INCREASE YOUR TEAM'S VIRTUALIZATION KNOWLEDGE

None of this can be done if your team doesn't have the right knowledge and skills. Look at your team and assess its virtualization knowledge. Is it lacking? More than likely, you will need to rely heavily upon your firm's EA and I&O knowledge. It isn't necessary to hire a virtualization guru; rather, you need competent staff that can have virtualization conversations and understand the security implications. Look for ways to increase your team's knowledge of virtualization. You can do this in two ways:

- **Take the organic approach.** It takes more time, but you can develop the skills in-house. A number of training organizations offer virtualization security courses, including The SANS Institute.[13] VMware also offers courses on securing VMware technologies.[14] Additionally, spending time with professionals in your EA and I&O team will help grow skills organically.

- **Acquire the talent externally.** Information security professionals with strong virtualization skills are in high demand, but if you're willing to pay a competitive salary, you can find them. Look for staff coming from managed service or cloud service provider environments. To scale economically, these providers have massive virtualized data centers. These practitioners live and die in multitenant environments and often have deep knowledge of securing multitenant workloads. This knowledge can easily transition to your environment.

WHAT IT MEANS

STICK TO YOUR IT COLLEAGUES LIKE GLUE

You have heard it before, but it bears repeating: You must collaborate with your IT peers in EA and I&O. If you don't have regular interaction with the IT leaders in these areas, you need to. Additionally, you need to establish regular interaction between your team and the virtualization team. Hold a virtualization summit, and get teams together to spend some time talking about the environment. In our interviews, the security teams that embedded themselves and worked closely with their peers had much greater familiarity with the virtual environments of their organizations. One security and risk professional said, "We are more keenly aware of our virtual environment due to our close relationship with operations; our regular meetings have paid off."

SUPPLEMENTAL MATERIAL

Methodology

Forrester's Forrsights Hardware Survey, Q3 2011, was fielded to 2,343 IT executives and technology decision-makers located in Canada, France, Germany, the UK, and the US from companies with two or more employees. This survey is part of Forrester's Forrsights for Business Technology and was fielded during July and August 2011. The LinkedIn Research Network fielded this survey online on behalf of Forrester. Survey respondent incentives include a choice of gift certificates or charitable donations. We have provided exact sample sizes in this report on a question-by-question basis.

Forrester's Forrsights for Business Technology fields 10 business-to-business technology studies in 12 countries each calendar year. For quality control, we carefully screen respondents according to job title and function. Forrester's Forrsights for Business Technology ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of IT products and services. Additionally, we set quotas for company size (number of employees) and industry as a means of controlling the data distribution and establishing alignment with IT spend calculated by Forrester analysts.

We have illustrated only a portion of survey results in this document. For access to the full data results, please contact Forrsights@forrester.com.

Companies Interviewed For This Document

BeyondTrust
Catbird Networks
CA Technologies
Cisco Systems
Citrix Systems
Fortinet
HyTrust
IBM
Juniper Networks
McAfee
Microsoft
Rapid7
Reflex Systems
Trend Micro
VMware

ENDNOTES

[1] Source: Forrsights Hardware Survey, Q3 2011.

[2] Source: "Former Shionogi Employee Sentenced To Federal Prison For Hack Attack On Company Computer Servers," The United States Attorney's Office, District of New Jersey press release, December 9, 2011 (http://www.justice.gov/usao/nj/Press/files/Cornish,%20Jason%20Sentencing%20News%20Release.html).

[3] According to Forrester survey data, "trusted" insiders and business partners, intentionally or unintentionally, are responsible for 43% of security breaches. The recent WikiLeaks breach illustrates how a trusted user with unrestricted access to vast amounts of sensitive information is the perfect recipe for an international scandal. Protecting against a breach is difficult because you have an enormous amount of data to protect stored in many silos and growing at an alarming rate. Security professionals often turn to technologies such as data leak prevention (DLP) and enterprise rights management (ERM), but these don't perform well alone without an identity context. You need to have a full understanding of how users join, move, and leave the enterprise so that you can assign and revoke access to sensitive data assets. Adding identity context for information protection, mapping Active Directory groups to file shares, and slowing the explosion of unstructured information are key to preventing a breach. See the June 27, 2011, "Your Data Protection Strategy Will Fail Without Strong Identity Context" report.

[4] Source: Forrsights Hardware Survey, Q3 2011.

[5] Source: Virtualization Special Interest Group PCI Security Standards Council, "Information Supplement: PCI DSS Virtualization Guidelines," PCI Security Standards Council, June 2011 (https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf).

[6] Source: "Security Advisories & Certifications," VMware (http://www.vmware.com/security/advisories).

[7] Source: "IBM X-Force 2010 Trend and Risk Report," IBM (https://www.ibm.com/services/forms/signup.do?source=swg-spsm-tiv-sec-wp&S_PKG=IBM-X-Force-2010-Trend-Risk-Report).

[8] Asked to do more with less, CIOs are using virtualization to pack more services into fewer physical boxes, reduce energy consumption, and provide greater flexibility. But security and risk professionals worry that in the headlong rush to embrace virtualization, their companies may have failed to secure their new virtual infrastructures. Chief among these concerns include hyperjacking and the risks of deploying virtual machines (VMs) in the demilitarized zone (DMZ). Forrester feels hyperjacking fears are overblown. The real risks are operational. Virtual infrastructures can be kept secure by: 1) segregating administrative, hypervisor, and live-migration traffic away from production traffic; 2) keeping VMs with different security classifications on separate physical hosts; and 3) enforcing zone boundaries with separate hardware. See the October 16, 2009, "Fear Of A Hyperjacked Planet" report.

[9] There's an old saying in information security: "We want our network to be like an M&M, with a hard crunchy outside and a soft chewy center." For a generation of information security professionals, this was the motto we grew up with. It was a motto based on trust and the assumption that malicious individuals wouldn't get past the "hard crunchy outside." In today's new threat landscape, this is no longer an effective way of enforcing security. Once an attacker gets past the shell, he has access to all the resources in our network. We've built strong perimeters, but well-organized cybercriminals have recruited insiders and developed new attack methods that easily pierce our current security protections. To confront these new threats, information security professionals must eliminate the soft chewy center by making security ubiquitous throughout the network, not just at the perimeter. To help security professionals do this effectively, Forrester has developed a new model for information security, called Zero Trust. This report, the first in a series, will introduce the necessity and key concepts of the Zero Trust Model. See the September 14, 2010, "No More Chewy Centers: Introducing The Zero Trust Model Of Information Security" report.

[10] VMware has provided access to its APIs, and Trend Micro was one of the early adopters. VMware recently announced additional partners, including Kaspersky Lab, Bitdefender, and others. Source: Ellen Messmer, "VMware strives to expand security partner ecosystem," Network World, August 31, 2011 (https://www.networkworld.com/news/2011/083111-vmware-security-partners-250321.html).

McAfee and Citrix announced a similar partnership to utilize hypervisor introspection on the Xen platform. Source: "McAfee, Inc. and Citrix Deliver First Phase of Virtual Desktop Security Partnership," Citrix Systems press release, October 6, 2010 (http://www.citrix.com/English/NE/news/news.asp?newsID=2304351).

[11] There are a number of good resources available to assist you with hardening your virtual servers:

The NIST's Guide to Security for Full Virtualization Technologies provides vendor-agnostic guidance on securing virtual environments. Source: Karen Scarfone, Murugiah Souppaya, and Paul Hoffman, "Guide to Security for Full Virtualization Technologies," National Institute of Standards and Technology (NIST), January 2011 (http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125-final.pdf).

The Center for Internet Security provides security benchmarks for both VMware and XenServer. Source: "Security Configuration Benchmark For VMware ESX 4," The Center for Internet Security, December 30,

2010 (https://benchmarks.cisecurity.org/tools2/vm/CIS_VMware_ESX_Server_4_Benchmark_v1.0.0.pdf) and "Center for Internet Security Benchmark for Xen 3.2," The Center for Internet Security, May 2008 (https://benchmarks.cisecurity.org/tools2/xen/CIS_Benchmark_Xen_32_v1.0.pdf).

The VMware vSphere 4.1 Security Hardening Guide provides specific guidance on security vSphere 4.1. At this time, a hardening guide has not been created for vSphere 5. Source: "VMware vSphere 4.1 Security Hardening Guide," VMware, June 2011 (http://www.vmware.com/resources/techresources/10198).

Defense Information Systems Agency (DISA) has a template for hardening virtual systems to military specifications that could also appeal to organizations with a low risk tolerance and high security requirements. Source: Defense Information Systems Agency (http://iase.disa.mil/stigs/os/virtualization/esx.html).

[12] Source: Sean Michael Kerner, "Nexpose 5 Goes After Virtual Security," eSecurity Planet, September 20, 2011 (http://www.esecurityplanet.com/malware/rapid7-goes-after-virtual-security-in-nexpose-5.html).

[13] Source: The SANS Institute (https://www.sans.org/security-training/virtualization-security-fundamentals-1412-mid).

[14] Source: VMware (http://mylearn.vmware.com/mgrreg/courses.cfm?ui=www_edu&a=one&id_subject=19217).

FORRESTER®

Making Leaders Successful Every Day

Headquarters

Forrester Research, Inc.
60 Acorn Park Drive
Cambridge, MA 02140 USA
Tel: +1 617.613.6000
Fax: +1 617.613.5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Forrester has research centers and sales offices in more than 27 cities internationally, including Amsterdam, Netherlands; Beijing, China; Cambridge, Mass.; Dallas, Texas; Dubai, United Arab Emirates; Frankfurt, Germany; London, UK; New Delhi, India; San Francisco, Calif.; Sydney, Australia; Tel Aviv, Israel; and Toronto, Canada.

For the location of the Forrester office nearest you, please visit: www.forrester.com/locations.

For information on hard-copy or electronic reprints, please contact Client Support at +1 866.367.7378, +1 617.613.5730, or clientsupport@forrester.com.
We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research, Inc. (Nasdaq: FORR) is an independent research company that provides pragmatic and forward-thinking advice to global leaders in business and technology. Forrester works with professionals in 19 key roles at major companies providing proprietary research, customer insight, consulting, events, and peer-to-peer executive programs. For more than 28 years, Forrester has been making IT, marketing, and technology industry leaders successful every day. For more information, visit www.forrester.com.

FORRESTER®