

January 2013

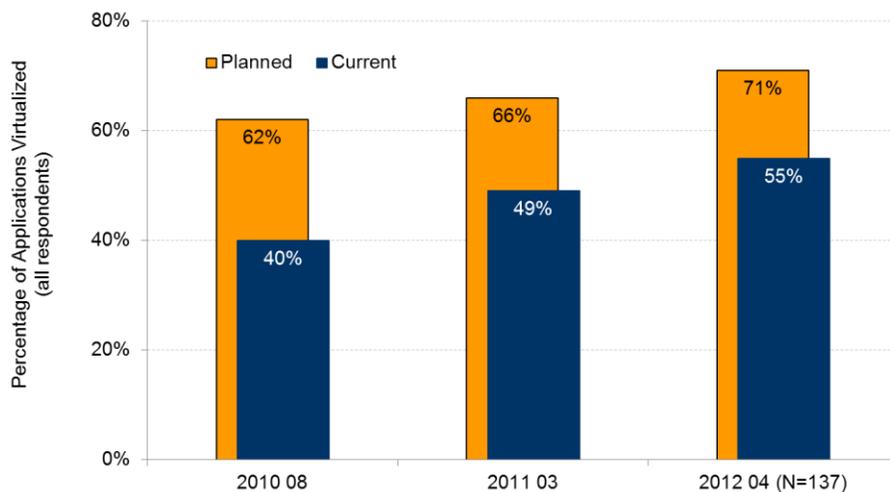
Evolving Your Datacenter? Evolve Your Datacenter Security

Your enterprise datacenter is evolving – your datacenter security should be evolving, too. Key security technologies and services – most of which are already very familiar from their traditional use in a physical, on-premise context – are being adapted by leading solution providers to work across a broad range of physical and virtual datacenter deployment scenarios.

Business Context: Your Evolving Enterprise Datacenter

Over the past three years, Aberdeen's research has shown steady growth in the average percentage of enterprise applications that are *virtualized* – from 40% in its 2010 study, to 55% in 2012 (Figure 1). In addition, the trend in "currently virtualized" in proportion to "planned to be virtualized" shows that companies continue to gain ground in terms of virtualizing their enterprise application portfolios.

Figure 1: Percentage of Enterprise Applications Virtualized



Source: Aberdeen Group, January 2013

Some of the general classes of enterprise applications that are most likely to be virtualized (whether in *private cloud* or *public cloud* scenarios) are shown in Figure 2. Most likely to be virtualized: *web applications, email, test and development environments, disaster recovery, customer relationship management (CRM), and light business apps*. Most likely to be running on physical servers: *databases, file sharing servers (e.g., SharePoint), enterprise resource planning (ERP) systems, and business-critical applications*. As virtualization platforms continue to mature, however, previous caution based on resource

Research Brief

Aberdeen's Research Briefs provide a deeper exploration of findings from one or more primary research studies, including key performance indicators, leading performance insights, and vendor insights.

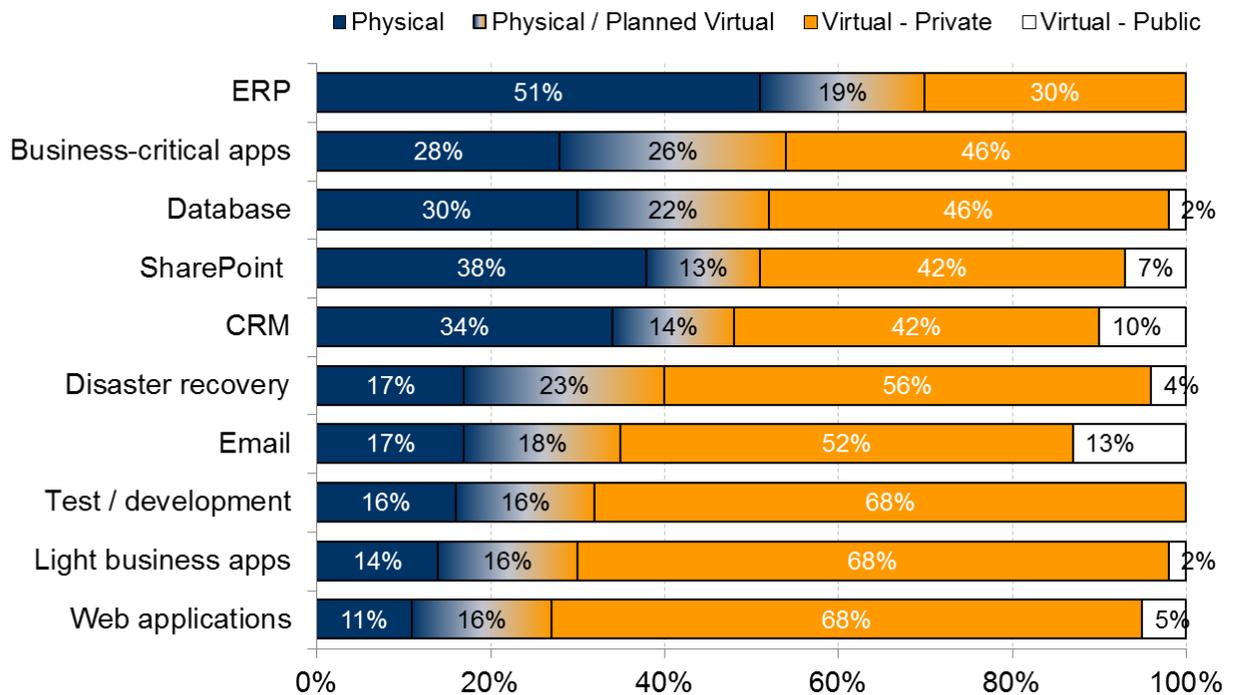
Definitions

✓ **Virtualization (V12N)** technologies break the traditional computing model of one physical server / one operating system / one application, by enabling the underutilized resources of a single physical machine to run multiple virtual machines – each of which in turn can run different operating systems and applications. In a fully virtualized on-premise computing environment, organizations can run their applications on a flexible pool of shared resources (networks, storage and hosts), which many companies refer to as a **private cloud**.

✓ **Infrastructure-as-a-Service (IaaS)** provides a fully virtualized computing environment on which organizations can run their Internet-based applications, eliminating their need to install, operate and support their own private networks, storage and hosts. IaaS is one example of a **public cloud**.

allocation restrictions or concerns about performance will continue to fade away, and we can expect that even critical workloads in private and public clouds will become mainstream.

Figure 2: Physical and Virtualization (Private, Public) by Type of Enterprise Application



Source: Aberdeen Group, January 2013

Based on Aberdeen's research findings, server virtualization is one of those rare technologies in which the leading drivers that companies identify for making an investment are actually being exceeded by the benefits they realize from deployment (Figure 3). *Fewer physical servers, faster time to deploy and upgrade enterprise applications, lower IT expense, less unplanned downtime, faster disaster recovery, and lower power and cooling expenses* are among the benefits noted by the respondents to Aberdeen's study, each generally exceeding their importance as the initial drivers for investment.

In addition, respondents noted two other benefits realized from their server virtualization deployments: *improved application control*, and *increased security* – topics which will be addressed in the next section.

Table I summarizes some selected benefits of server virtualization, as found in Aberdeen's 2012 study – and quantifies the advantages of top performance. Compared to the lagging performers (bottom 30%), the leading performers (top 20%) on average:

- Virtualized nearly 60% more applications
- Reduced the average time to deploy applications by 90%

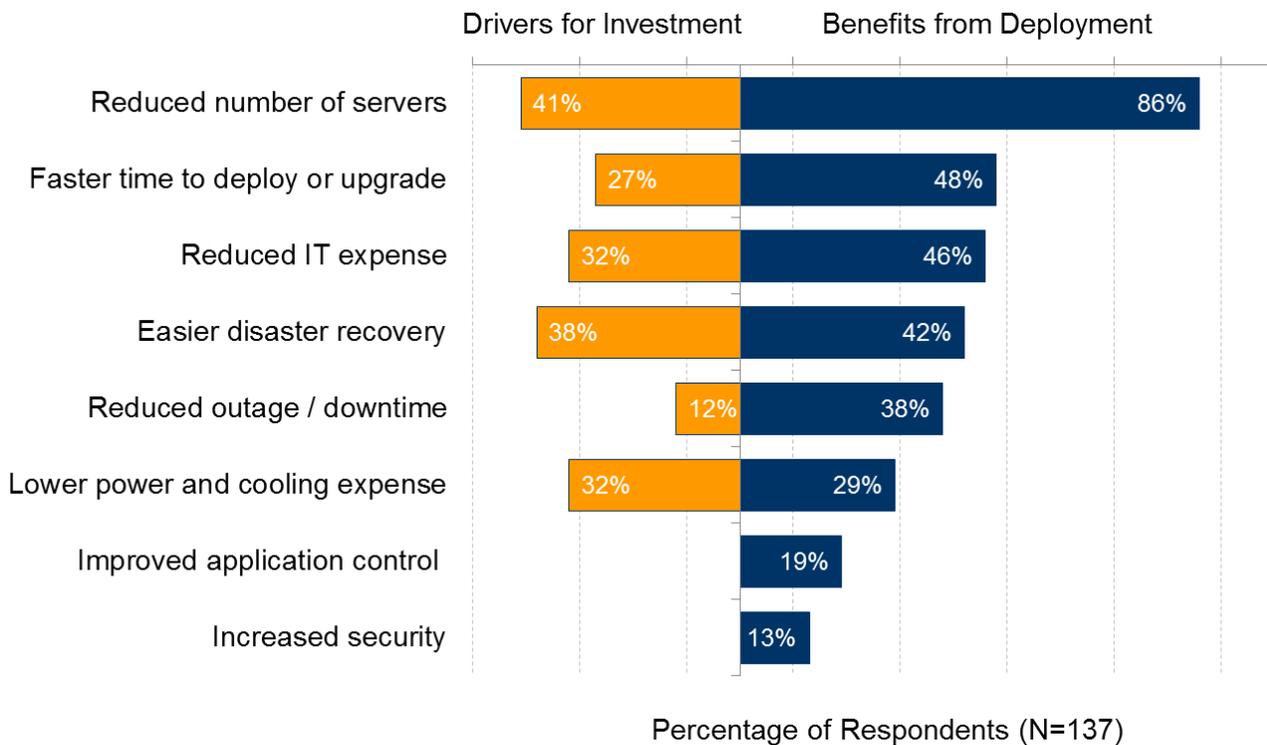
Definitions (continued)

- ✓ **Platform-as-a-Service (PaaS)** provides software services and application development interfaces, along with their underlying networks, storage and hosts, which organizations can use to develop, test and deploy their own Internet-based applications.
- ✓ **Software-as-a-Service (SaaS)** provides one or more specific applications over the Internet, eliminating the need for organizations to install, operate and support these applications on their own private networks, storage and hosts.

- Achieved nearly 50% higher server utilization
- Achieved 2.2-times higher server concentration
- Reduced the average duration of unplanned downtime by 90%

For details on the criteria used to distinguish leaders and laggards, see [The New Breed of Servers: Platforms for Server Virtualization](#) (August 2012).

Figure 3: Drivers of Investments in Server Virtualization, and Benefits Realized from Deployment



Source: Aberdeen Group, January 2013

Table 1: Selected Benefits of Server Virtualization, and Advantages of Top Performance

	All Respondents	Leaders	Laggards	Leaders Advantage
Percentage of enterprise applications virtualized	55%	71%	45%	58%
Average time to deploy applications (before virtualization)	15 days	12 days	18 days	33%
Average time to deploy applications (after virtualization)	7.6 days (49% faster)	1.1 days (91% faster)	11.8 days (34% faster)	91%
Average server utilization	45%	58%	39%	49%
Average server concentration	11.8 to 1	15.5 to 1	7.1 to 1	2.2-times
Average duration of unplanned downtime	3.7 hours	0.7 hours	9.1 hours	92%

Source: Aberdeen Group, January 2013

Your Datacenter Security Needs to Evolve, Too!

As we have seen, investments in server virtualization and cloud computing are motivated by pressures for **greater consistency and efficiency of operations**. These do not come as a surprise; they reflect the generally well-understood promise of virtualization and cloud computing.

Investments in *security* for virtualization and cloud initiatives, on the other hand, are driven primarily by pressures related to **risk and compliance**, such as *sensitive business information, increasing mobility, external users (e.g., business partners, customers, guests) and internal users (e.g., employees, temporary employees, contractors)*. These too are not particularly surprising, as concerns about assuring the confidentiality, integrity and availability of sensitive data have consistently been among the leading inhibitors to faster enterprise adoption of cloud computing identified in Aberdeen's research.

Why Some Security Solutions Need to be Different

But many traditional enterprise security solutions need to be re-architected to work well in a virtualized environment.

Take **anti-virus / anti-malware**, for example – the most basic, foundational security solution for securing datacenter hosts, which literally all (100%) of the top performers in Aberdeen's studies have deployed. Given an average server concentration ratio of about 12-to-1 (refer again to Table 1), this means that a traditional anti-virus solution would have a scan engine for each of 12 virtual machines, all running on a single physical server. Early adopters of virtualization were quick to realize some of the problems with this approach, including:

- **Resource overload**, as in when all the memory and processing power of the hypervisor host is consumed by multiple scanning engines running at the same time – sometimes referred to as a *scan storm* – as might happen with a traditional policy of scanning all hosts at 3:00am.
- **Functionality gaps**, which can easily occur when the latest security updates are difficult to maintain on all virtual machine images (including active, inactive, and image templates or masters).
- **Instant-on gaps**, in which delays for booting and scanning detract from the "instant-on" experience that end-users want from the flexible, real-time provisioning and de-provisioning of virtual machines.
- **Always-on gaps**, in which ever-higher server utilization makes it even more difficult to find predictable times for routine patches, updates and maintenance – and amplifying the impact of unplanned downtime.
- **Management inefficiencies**, in environments with a mix of hypervisors, and potentially a mix of security solutions, from multiple vendors.

Fast Facts

Percentage of all respondents with server virtualization initiatives

- ✓ Already in place: 77%
- ✓ Planned < 12 months: 11%
- ✓ Planned > 12 months: 7%
- ✓ No plans: 5%

Percentage of all respondents with server virtualization initiatives in place, by type

- ✓ On-premise / private cloud: 68%
- ✓ Infrastructure as a Service (IaaS) / public cloud: 31%
- ✓ Platform as a Service (PaaS) / public cloud: 22%
- ✓ Software as a Service (SaaS) / public cloud: 50%

(multiple responses accepted; does not add to 100%)

Faced with these challenges, the age-old choice between security and productivity or security and convenience comes back into play – a choice in which security often loses. Many administrators simply turn off scanning or forgo regular patches and updates. All in all, these and other challenges have a negative affect not only on security risk, but also on compliance requirements and the ongoing cost of operations.

How have leading security vendors responded? Staying with the example of anti-virus / anti-malware, some of the ways that leading providers have evolved their traditional security solutions include:

- **Externalizing the scan engine.** By separating the scan engine into a physical (or virtual) appliance, the appliance can specialize in scanning, updating signatures, integrating other threat intelligence, etc., freeing up the resources of the hypervisor host to support virtual machines. One way to achieve this is by incorporating a small software agent within each virtual image, to manage policies locally and communicate with the external scan engine – an approach that readily supports environments with a mix of hypervisors. McAfee's [Management for Optimized Virtual Environments \(MOVE\) Anti-Virus](#) solution is an example of this approach. Another approach leverages the [VMware vShield Endpoint](#) API, to achieve an agentless option specifically for VMware-only environments – an approach supported by McAfee MOVE, [Trend Micro Deep Security](#), and other [VMware Integrated Partners](#).
- **Intelligent scanning and scheduling.** Another benefit of externalizing and centralizing scanning and management functions is the enablement of services that have the visibility and intelligence to keep scans and updates current, while staying out of the way of active images – helping to keep server utilization high, and unplanned downtime low.
- **Managing the virtual footprint.** In addition to externalizing the scan engine (the purpose of which is to keep out the "known bad"), complementary technologies such as *application control* or *application whitelisting* (the purpose of which is to manage and enable the "known good") can help to manage the virtual footprint more cost-effectively. Solutions such as [McAfee Application Control](#) are designed to create and manage an inventory of all software (e.g., executables, dynamic link libraries, drivers, scripts) to enable applications that are trusted and reputable, and block applications which are unauthorized or harmful.

Another Example: Enterprise Security for Cloud Services

In the steady state, there should be no fundamental difference between a well-managed server virtualization / private cloud infrastructure, and a well-managed public cloud infrastructure – but solution providers and markets as a whole naturally take time to develop and mature to such a point. In [Security and Cloud: Augment, or Abdicate?](#) (July 2011) and [Security and Cloud:](#)

Analyst Insight

The architectural notion of externalizing certain aspects of IT security is well-established. For example, Aberdeen described the externalization of access privileges in [Managing Access: Roles, Rules, Privileges and Entitlements](#) (August 2009), a study which showed that Best-in-Class companies are 10-times more likely than all others to enforce access policies external to applications and services, as opposed to enforcing access policies using their embedded native capabilities. In this case, the strategy of abstracting common elements of identity and access from the applications and services themselves is the key to breaking the cycle of perpetually "setting the clocks" and yet never being in synch or on time.

[Private, or Public?](#) (September 2011), for example, Aberdeen's analysis found that for companies pursuing cloud computing initiatives while also addressing material requirements for security and compliance, the old adage "if you want something done right, do it yourself" still tends to apply. The more recent findings on virtualization by type of enterprise application (refer again to Figure 2) reinforce this point.

Why is this the case? Reasons why relying solely on the capabilities of cloud service providers is less consistent, less efficient, and less secure include:

- Security policies and controls of cloud service providers are often different, and sometimes unknown
- Visibility and verification efforts with multiple cloud service providers are a drain on already limited enterprise IT resources
- The average results in security seen for this approach are consistent with accepting the security that is provided

Similarly, reasons why a more hands-on approach to security and compliance for server virtualization – whether private, public or a hybrid – is more consistent, more efficient, and more secure include:

- Existing security policies and controls (e.g., identities and access, data protection, host security, network security) can be applied and extended into the enterprise's portfolio of virtualized / cloud-based applications
- Companies can leverage familiar, proven enterprise security technologies for their cloud computing initiatives
- Critical data can be identified, classified and protected as it flows between the enterprise and the public cloud

A number of innovative solutions have emerged that augment the security and compliance capabilities of cloud computing, both private and public, while remaining under enterprise control – including the following illustrative examples: [Intel Expressway Cloud Access 360](#), [McAfee Cloud Security Platform](#), [RSA Cloud Trust Authority](#), [SecureAuth Identity Enforcement Platform](#), and [Symplified Identity Manager](#), [Access Manager](#), and [Sign-On](#).

Evolve Your People and Process, Not Just Technologies

In every benchmark study, Aberdeen routinely asks about the people, processes and technologies that correlate most strongly with best practices and top performance. By leveraging the guidance developed by the **Cloud Security Alliance** (see [Cloud Controls Matrix v1.3](#)) within its time-tested benchmark framework, Aberdeen has confirmed that organizations are in fact implementing these recommended capabilities – and more importantly, that having these capabilities in place actually correlates with the achievement of leading results.

Table 2 lists some of the key *technologies* for securing the evolving enterprise datacenter – most of which are already very familiar from their traditional use in a physical, on-premise context. Leading solution providers have diligently been adapting these security technologies and services to work across a broad range of datacenter deployment scenarios.

Table 2: Core Technologies for Securing the Evolving Datacenter; Solutions Landscape

Layer	Security Services (illustrative)	Solution Providers (illustrative)
Management	<ul style="list-style-type: none"> ▪ Incident management (correlation of logs, information and events from across the virtual infrastructure; global threat intelligence) ▪ Centralized compliance monitoring ▪ Centralized policy administration 	<ul style="list-style-type: none"> ▪ McAfee (ePolicy Orchestrator) ▪ Symantec (Management Console) ▪ Trend Micro (Deep Security Manager)
Identities	<ul style="list-style-type: none"> ▪ Federation of identities ▪ Device authentication ▪ User authentication 	<ul style="list-style-type: none"> ▪ RSA (Cloud Trust Authority) ▪ Intel (Expressway Cloud Access 360) ▪ SecureAuth (Identity Enforcement Platform) ▪ Symplified (Identity Manager, Sign-On)
Data	<ul style="list-style-type: none"> ▪ Encryption for data at rest ▪ Encrypted communications for data in transit ▪ Content monitoring / filtering (DLP) 	<ul style="list-style-type: none"> ▪ TrendMicro (SecureCloud) ▪ McAfee (Endpoint Encryption, DLP) ▪ Symantec (Endpoint Encryption, DLP)
Applications	<ul style="list-style-type: none"> ▪ Content monitoring / filtering (file shares) ▪ Content monitoring / filtering (DAM) ▪ Content monitoring / filtering (web security) ▪ Content monitoring / filtering (email security) 	<ul style="list-style-type: none"> ▪ McAfee (Cloud Security Platform)
Hosts	<ul style="list-style-type: none"> ▪ Integrity assurance (application whitelisting, file integrity) ▪ Vulnerability management (patches, configurations, changes) ▪ Anti-virus / anti-malware 	<ul style="list-style-type: none"> ▪ McAfee (Application Control) ▪ VMware (vCenter Protect (Shavlik)) ▪ McAfee (MOVE) ▪ Trend Micro (Deep Security) ▪ Symantec (Critical System Protection) ▪ Symantec (Endpoint Protection) ▪ VMware (vShield Endpoint)
Network	<ul style="list-style-type: none"> ▪ Network access control ▪ Network behavior analysis ▪ Network intrusion detection / prevention ▪ Network firewall 	<ul style="list-style-type: none"> ▪ IBM (Network Intrusion Prevention System) ▪ HP (TippingPoint Network Security) ▪ McAfee (Network Security Platform) ▪ Barracuda Networks, Check Point, Dell (SonicWALL), Fortinet, Global DataGuard, Juniper Networks, Palo Alto Networks, Sophos (Astaro), WatchGuard

Source: Aberdeen Group, January 2013

Leading Solution Providers are Adapting, So You Can Adapt

Enterprise buyers should look for solution providers that have adapted their solutions to work together in a layered, defense-in-depth approach for datacenter security, including support for:

- Both *physical implementations* (whether a single location, or multiple locations) and *virtual implementations* (whether private cloud or public cloud)
- *Multiple vendors*, including all major hypervisors
- *Industry standards*, building on generally accepted best practices and frameworks such as ISO 27001/27002, ISACA COBIT, PCI, NIST, NERC CIP, and the Cloud Security Alliance
- *Automated, dynamic management* of virtualized infrastructure
- *System-wide collection and correlation* of intelligence
- *Common, centralized visibility, management and reporting*

Summary and Recommendations

When it comes to server virtualization and other cloud computing initiatives, Aberdeen's research shows that:

- Four out of five respondents have a server virtualization or cloud computing initiative currently in place
- More than half of enterprise applications have currently been virtualized

The leading drivers that companies identify for making an investment are actually being exceeded by the benefits they realize from deployment, including:

- *Fewer physical servers*
- *Faster time to deploy and upgrade enterprise applications*
- *Lower IT expense*
- *Less unplanned downtime*
- *Faster disaster recovery*
- *Lower power and cooling expenses*

Compared to the lagging performers, the leading performers in Aberdeen's study realized substantial benefits from their server virtualization initiatives, including:

- Nearly 60% more *applications virtualized*
- 90% reduction in the *average time to deploy* applications
- Nearly 50% higher *server utilization*
- 2.2-times higher *server concentration*
- 90% reduction in the average duration of *unplanned downtime*

Using the example of **anti-virus / anti-malware** as a case-in-point, some of the problems with using traditional security solutions in virtualized environments include *resource overload, functionality gaps, instant-on gaps,*

Success Factors (illustrative)

Collection and measurement of the performance of virtualized systems

√ Leaders: 91%

√ Average: 44%

√ Laggards: 9%

Automated, dynamic management of virtualized infrastructure

√ Leaders: 38%

√ Average: 18%

√ Laggards: 6%

always-on gaps, and *management inefficiencies*. To address these issues, some of the ways that traditional security solutions have evolved include:

- **Externalizing the scan engine**, in both agent-based and agentless approaches
- **Intelligent scanning and scheduling**, to help keep server utilization high and unplanned downtime low
- **Managing the virtual footprint**, using common management and complementary technologies such as *application whitelisting* to enable the trusted and reputable, and block the unauthorized or harmful

As another example, companies that *augmented* their server virtualization initiatives with complementary solutions that remain under enterprise control were found to be more consistent, more efficient, and more secure:

- Existing security policies and controls (e.g., identities and access, data protection, host security, network security) can be applied and extended into the enterprise's portfolio of virtualized applications
- Companies can leverage familiar, proven enterprise security technologies for their cloud computing initiatives
- Critical data can be identified, classified and protected as it flows between the enterprise and the public cloud

Traditional technologies for securing the evolving enterprise datacenter are being adapted by leading solution providers to work across a broad range of datacenter deployment scenarios. Enterprise buyers should look for solution providers that have explicitly adapted their solutions to work together in a layered, defense-in-depth approach for datacenter security.

For more information on this or other research topics, please visit www.aberdeen.com.

Related Research

[New Breed of Servers: Platforms for Server Virtualization](#); Aug. 2012
[FFIEC Guidance on Cloud: Mapped to Aberdeen Research](#); Aug. 2012

[Security and Cloud: Private, or Public?](#); Sept. 2011
[Security and Cloud: Augment, or Abdicate?](#); July 2011
[Security and Cloud Best Practices](#); June 2011

Author: Derek E. Brink, Vice President and Research Fellow for IT Security & IT GRC (Derek.Brink@aberdeen.com)

For more than two decades, Aberdeen's research has been helping corporations worldwide become Best-in-Class. Having benchmarked the performance of more than 644,000 companies, Aberdeen is uniquely positioned to provide organizations with the facts that matter — the facts that enable companies to get ahead and drive results. That's why our research is relied on by more than 2.5 million readers in over 40 countries, 90% of the Fortune 1,000, and 93% of the Technology 500.

As a Harte-Hanks Company, Aberdeen's research provides insight and analysis to the Harte-Hanks community of local, regional, national and international marketing executives. Combined, we help our customers leverage the power of insight to deliver innovative multichannel marketing programs that drive business-changing results. For additional information, visit Aberdeen <http://www.aberdeen.com> or call (617) 854-5200, or to learn more about Harte-Hanks, call (800) 456-9748 or go to <http://www.harte-hanks.com>.

This document is the result of primary research performed by Aberdeen Group. Aberdeen Group's methodologies provide for objective fact-based research and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, distributed, archived, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc. (2013a)