WHITE PAPER

Market Pulse

# Safeguarding the Next-Generation Data Center

## SAFELY CAPITALIZING ON PRIVATE AND HYBRID CLOUD COMPUTING TAKES A COMPREHENSIVE SET OF INTEGRATED SECURITY TECHNOLOGIES.

Understanding the appeal of private and hybrid cloud computing isn't hard. With their intuitive self-provisioning, dynamic scalability and "do more with less" efficiency, cloud environments liberate IT departments from a wide range of demanding, time-consuming responsibilities.

Security, alas, isn't among them. "A lot of the same security issues that you might have in your traditional environments still apply in private and hybrid cloud environments," says Marcia Kaufman, principal analyst and COO of Needham, Mass.-based analyst firm Hurwitz & Associates LLC.

What's more, many of the cloud's defining characteristics may limit the effectiveness of traditional security approaches. Unlike conventional infrastructures, cloud environments feature highly mobile virtualized resources that may move between shared hosts in third-party data centers or across on-premises hardware. "Securing the platform may be more challenging if organizations are not willing to reexamine their security tools and operational processes," Kaufman observes.

Indeed, as a new study from IDG Research Services indicates, many technology executives question their ability to safeguard the so-called next-generation data center. Fully 61 percent of the respondents to the study's survey, in fact, said they're either only somewhat or not very confident that they can protect applications in a private or hybrid cloud. The upshot, moreover, is a parallel lack of confidence in private and hybrid clouds generally: Some 48 percent of the poll participants said that perceived security limitations are slowing or preventing deployment of mission-critical applications in private clouds to some or a great extent. An even larger 64 percent said the same of hybrid clouds.

According to Kaufman and other experts, though, security needn't be a barrier to private and hybrid cloud adoption.

Companies can secure cloud infrastructures at least as effectively as they do traditional ones, provided that they take a comprehensive approach using solutions designed from top to bottom with the cloud's unique qualities in mind.

### » Advanced Functionality

Evidence from the IDG Research Services study reveals which of those risks most worry IT executives. A whopping 69 percent of the respondents with hybrid clouds and 68 percent of those with private clouds cited reduced visibility into the security posture of virtual machines as a top security-related anxiety. Another 62 percent of the hybrid cloud users and 56 percent of the private cloud operators named diminished ability to replicate internal security controls as a concern, and 46 percent of the executives with hybrid clouds and 56 percent of those with private clouds listed greater data center complexity.

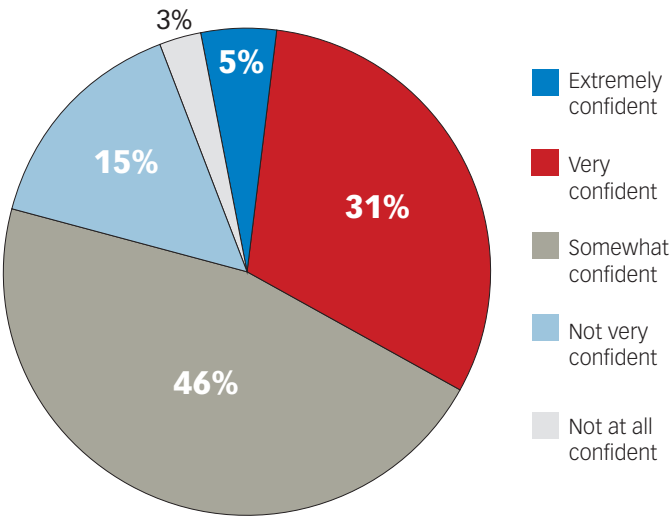
None of that surprises Kaufman. "There are so many different parts when you're dealing with cloud environments that it's hard to maintain the right level of control over who has access, who should have access and how that should change over time," she says.

Overcoming such obstacles takes tightly integrated technologies capable of protecting a company's physical, virtual and cloud-based assets, according to Joakim Lialias, director of data center and server security marketing at McAfee Inc., of Santa Clara, Calif.[1] "Most companies are going to have all three kinds of resources for the foreseeable future, so they're going to need good security solutions for all three areas," he says.

Protecting physical assets begins with using host servers featuring hardware-based security technologies. "Advanced processors today have built-in functionality you could previously get only from software or costly, hard-to-implement dedicated processors or appliances," says James Greene, senior product marketing engineer for security technologies at Intel Corporation, of Santa Clara, Calif. "You end up not only with better security but with better performance too. Almost anything you do directly on silicon is usually going to be faster, more efficient, less complex and more tamper-resistant."

Greene points to Intel's Virtualization Technology (Intel® VT) as an example. Most public clouds are multitenant environments in which companies can wind up sharing server space with their biggest competitor and never know it. "Intel VT supplements the logical separation between workloads that the hypervisor provides with an added layer of hardware-assisted physical separation," Greene says. The net results are both faster responsiveness and better protection from data leaks. "By executing such lower-level functions in hardware instead of software, Intel VT accelerates the entire virtualized environment," Greene states.

**Confidence in maintaining data center security as data is moved to public/ hybrid clouds**




SOURCE: IDG RESEARCH SERVICES, JUNE 2013

Fully 61 percent of the respondents to the study's survey, in fact, said they're either only somewhat or not very confident that they can protect applications in a private or hybrid cloud.

The same principle applies to data encryption as well. Historically, companies have often left cloud-based information potentially exposed to unauthorized viewers solely because software-based encryption tools imposed steep processing burdens. Hardware-assisted technologies such as Intel's Advanced Encryption Standard New Instructions (AES-NI) enable organizations to leverage sophisticated encryption algorithms more pervasively without slowing down servers and storage systems.

Servers containing trusted platform modules such as Intel's Trusted Execution Technology (Intel TXT) arm cloud managers with similarly powerful capabilities that software alone can't provide. Such systems verify that the host hardware and the critical firmware and hypervisor environment are in a verified, secure state and pass that information on to virtualization, security and cloud management systems.

That's an especially welcome feature in heavily regulated industries such as healthcare and financial services. "For some organizations, it may be very important to make sure that certain workloads run only on cloud infrastructure that's met certain security criteria," observes David Herrald, a network architect at Denver, Colo.-based solutions integrator Global Technology Resources Inc. Close integration between Intel TXT, VMware vSphere and management solutions such as McAfee ePolicy Orchestrator equip companies to automatically gain visibility into the security status of cloud-based systems such as Intel TXT-based hosts. "That's a big step forward," Herrald says.

## » Insight Everywhere

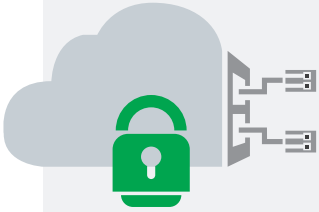
Securing virtual servers is as important to safe cloud computing as securing physical devices, but virtual security is not the same as physical security. For example, scanning a single stand-alone server for malware takes a distinct but manageable toll on performance. Scanning dozens of virtual machines on the same host simultaneously is another matter. "You can essentially bring a server to its knees," Lialias says.

[1] McAfee is a wholly owned subsidiary of Intel Corporation.

That's why private and hybrid clouds need antivirus software tailor-made for virtualized infrastructures. When run alongside VMware's vShield Endpoint security solution, for instance, McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus offloads malware scans to a separate, dedicated virtual appliance, sparing host machines from the "A-V storms" that can occur when multiple VMs perform scans at the same time. This enables companies to protect virtual machines from malware without imposing a performance penalty.

Solutions such as MOVE take a "blacklisting" approach to security that safeguards servers from a large set of known dangers (identified, in McAfee's case, by its Global Threat Intelligence technology). Companies can improve performance and efficiency even further, however, by employing a virtualization-aware "whitelisting" solution such as McAfee Application Control as well. Such products prevent freshly launched virtual machines from running anything not found on a specific list of approved applications. "Companies can verify that only those trusted and certified systems are referenced in the operating system boot sequence," Lialias says. "It's a low-resource way to protect a complex cloud environment."

So are identity management solutions such as McAfee Cloud Identity Manager, which give employees single-sign-on access to multiple cloud-based solutions while empowering IT departments



## McAfee, Intel and VMware: Partners in Cloud Protection

**COMPREHENSIVE, INTEGRATED SECURITY TECHNOLOGIES** are the key to protecting private and hybrid clouds. That's exactly what McAfee, Intel and VMware are uniquely equipped to deliver, thanks to their close working relationship.

Each company brings unique capabilities to the table. VMware provides market-leading proficiency in server and network virtualization via an open, extensible platform. McAfee contributes demonstrated expertise in endpoint, network and cloud security. Intel adds deep knowledge of hardware-assisted security technologies. And all three companies collaborate to ensure that their products interoperate seamlessly.

For example, hardware-based security systems from Intel, such as its Virtualization Technology (Intel VT) and Trusted Execution Technology (Intel TXT), integrate closely with VMware's vSphere and vCenter solutions to add extra layers of hardware-based protection to private and hybrid cloud environments. "VMware has been supporting Intel VT functionality for years, and it was one of the first commercial hypervisor makers to instrument support for Intel TXT," says James Greene, senior product marketing engineer for security technologies at Intel. As a result, VMware users in organizations that have deployed Intel-based servers enjoy enhanced security and faster performance, because the Intel and VMware security technologies share processing tasks that VMware's software would otherwise have to perform alone.

Tight integration between VMware's vShield Endpoint security software and McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus similarly spares businesses from compromises between speed and security. When used in tandem, those products enable companies to perform scans on a separate, dedicated virtual appliance instead of directly on virtual images themselves. "That keeps virtual machines safe without slowing them down," says Joakim Lialias, McAfee's director of data center and server security marketing.

To simplify security management, McAfee ePolicy Orchestrator works closely with VMware platform technologies to give businesses centralized, single-pane control over all their physical, virtual and cloud-based resources. "You get complete visibility into VMware-based virtual data centers and fine-grained policy management capabilities," Lialias says.

Since most businesses have specialized cloud security requirements, ePolicy Orchestrator also supports open APIs that enable an ecosystem of more than 100 software vendors to add industry-specific security capabilities and other supplemental features. "You can manage all of it through the same console too, so customers get complete visibility into the entire security posture of their data center," Lialias says.

Looking ahead, McAfee Network Security Platform will work in harmony with VMware's NSX network virtualization platform to help companies with software-defined networks monitor and protect traffic flows that never cross physical boundaries. "We know that that's where our customers are going and that they expect us to be able to protect them," Lialias observes.

In the end, protecting businesses more fully and effectively while delivering maximum agility and flexibility is what the McAfee/Intel/VMware partnership is all about. "It's three leaders delivering a comprehensive set of solutions that really addresses the full spectrum of challenges a next-generation data center faces in securing physical, virtual and cloud environments," Lialias says. Just what today's enterprise increasingly needs.

**When attempting to extend conventional security levels to private, hybrid and public clouds, organizations are most often concerned about a loss of visibility into their security posture.**

| | PRIVATE CLOUD | HYBRID/PUBLIC CLOUD |
|---|---|---|
| Loss of visibility into security posture | 68% | 69% |
| Cloud service providers (CSPs) are unable to replicate security controls we have internally | 56% | 62% |
| Adding layers of security increases data center complexity | 56% | 46% |
| Making changes to security strategy can compromise the ability to meet compliance requirements | 49% | 56% |
| Bolted-on security technologies decrease data center and/or application agility | 44% | 43% |

to revoke those privileges quickly and easily when someone leaves the company. "Companies need a consistent approach to provisioning and deprovisioning user access rights. Lack of control over who has access to which service at what time puts a company at high risk for a security breach," Kaufman says.

Virtualization-aware policy management solutions such as McAfee ePolicy Orchestrator further strengthen private and hybrid cloud defenses, by enabling companies to define, monitor and enforce security policies on virtual as well as physical machines. "All of a sudden, you have insight into everything everywhere," observes Michelle Drolet, CEO of Towerwall Inc., a security solution provider headquartered in Framingham, Mass. Better yet, she adds, you're getting that control through the same centralized console many companies have been using on their LANs for years.

## » The Software-defined Future

In the near future, servers and desktops won't be the only virtual entities that companies with private and hybrid clouds will need to secure. Virtual networks will be increasingly common too. Enabling software to handle work usually done by routers and switches today saves money and enhances IT agility, but it can also conceal network activity from conventional security systems. "Administrators may not even be aware of how much traffic they're not seeing, because it never leaves the virtual host," Herrald says.

To close that gap, companies need security solutions such as McAfee Network Security Platform that integrate with network virtualization solutions such as VMware NSX to provide visibility into traffic and protection from threats on the virtual network.

Enabling software to handle work usually done by routers and switches today saves money and enhances IT agility, but it can also conceal network activity from conventional security systems.

Policy management solutions, such as McAfee ePolicy Orchestrator, capable of applying security policies to virtual as well as physical networks are essential as well.

In fact, although fully software-defined data centers are more vision than reality at present, many experts believe that organizations should be mindful of the requirements they'll face in the future when evaluating security solutions. "You're eventually going to need a single, unified view and approach across an entire virtual and physical environment," Lialias says.

Implementing integrated, end-to-end private and hybrid cloud security technologies today will give you a head start. "Companies with next-generation data centers have demanding security needs, but solutions exist for all of them," Lialias says. Together, those solutions offer more than enough protection to give IT leaders complete confidence in their ability to utilize private and hybrid cloud computing safely. ■