From Silicon to the Data: A Multi-Point Approach for Protecting Cloud Environments

Private and public cloud platforms offer a wide range of potential benefits to organizations, including greater agility and flexibility in responding to business conditions, lower costs, and reduced workloads for IT departments. However, there's an understandable reluctance to fully embrace cloud platforms due to the complexity of protecting the varied layers of those platforms from viruses and other malware. Intel and McAfee, along with industry partners, are providing comprehensive solutions to better address the challenges of security for cloud computing.

Yet there is justifiable hesitation over the widespread migration of core business applications and data to cloud platforms. Cloud computing raises real concerns about the security of data and the necessary adherence to compliance and policy guidelines. IT managers and other C-level executives fear that moving critical information and processes to the cloud can lead to less control, reduced visibility into workloads and data, exposure to unexpected threats to the IT infrastructure, and the risk of non-compliance to internal standards and external regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA).

Reconciling Data Security and the Cloud

In most organizations today, cloud computing has pushed its way to the top of the IT planning agenda. It's easy to understand why: key executives and IT departments see the potential for immediate gains in addition to the established long-term benefits that virtualization can deliver with technologies from vendors such as VMware. By moving applications and processes to the cloud, businesses can respond faster to shifting business opportunities and challenges. They can lower costs by taking increased advantage of investments in computing hardware and IT infrastructure, and they can reduce IT workloads by giving end users and departments greater control over virtual resources.
Studies of security and data breaches bolster these concerns. With cloud computing, threats can come from almost any direction or device, and increasingly they are targeting data centers. According to the Verizon 2012 Data Breach Investigations Report, produced with help from the U.S. Secret Service and several international law enforcement agencies, 98 percent of all the data breaches examined came from external sources—and 94 percent of all the data compromised involved servers.1 Given that servers are targeted because they contain so much valuable data, it is logical that cloud infrastructures—especially large, multi-tenant environments—would be appealing targets. This is supported by a study by IDC, in which 70 percent of C-level executives indicated that cloud computing technologies are responsible for introducing the highest level of security concerns for their organizations.2

The security risks of cloud computing are, to a large degree, a natural consequence of the technology’s evolution. Typical cloud data centers are characterized by virtualization, multiple tenants, and abstracted resources that might not be dedicated to any particular organization or line of business. Standard IT security tools are often inadequate because they are designed to protect physical resources and not the abstracted, multilayered architectures of virtualized environments.

Protecting the Entire Server Stack

Intel and McAfee not only understand these concerns, they provide a comprehensive approach that addresses cloud security at every level. This paper offers an overview of the technologies that Intel and McAfee—along with industry partners such as HyTrust and Trapezeo—provide for the entire server stack. The solutions start at the silicon...
layer, continue to the operating system, and move on to applications and data. These tools also provide a comprehensive view of the security posture for both physical and virtual environments, in addition to continuous monitoring and response support for enhanced platform security and data access protection.

With the combined technologies of Intel, McAfee, and their partners, organizations have the tools they need to enforce policies across clouds, protect their workloads, and ensure the integrity of IT infrastructures.

Malware such as viruses is a constant and growing threat to data centers and businesses in general. The mechanisms of malware vary, but it is all designed to perform malicious acts such as corrupting systems, disrupting businesses, stealing data, or entirely seizing control over IT systems.

Because cloud environments offer many potential points of entry for malware, they require more than basic security solutions designed with the assumption that attacks will come from a single direction. Cloud environments need protection at every layer of the server stack, including processors, virtual machines, operating systems, applications, and data. This section takes a closer look at the layered protection offered by Intel, McAfee, and their partners.

**Processor Layer**
Organizations can start building protection for their data centers at the very foundation of the server stack—the processor layer—using Intel® Trusted Execution Technology (Intel® TXT) and enabling trusted compute pools (TCPs) in tandem with partners like HyTrust.

Intel TXT is a hardware-based security solution that protects IT infrastructures against software-based attacks from malware by validating the behavior of key components within a server or PC at startup. By establishing a root of trust foundation in the processor, Intel TXT can take measurements at each stage of startup and compare them to known good configurations. It does this by establishing a cryptographically unique identifier for each approved launch-enabled component. Intel TXT then provides hardware-based enforcement mechanisms to detect the launch of any code that does not match the approved code.

Intel TXT provides a foundation for TCPs. The root of trust established by Intel TXT is established through measurements when the hardware and prelaunch software components are in a known good state. The trustworthiness of the launch process can be reported to virtualization, cloud, or security management tools. Using these measurements, administrators can identify their highest integrity platforms, group these into trusted pools, and then set policies for sensitive data and workload placement onto the TCPs. This is the essence of a new capability for greater visibility and control in virtual environments.

HyTrust is one of the leading partners working with Intel on TCPs, providing its HyTrust Appliance*. The HyTrust Appliance is a policy engine that works with VMware vCenter® and other cloud infrastructure components to enable security controls in virtualized environments. When used with Intel TXT, the HyTrust Appliance can detect platform trust status as reported by the measured launch environment on Intel® Xeon® processor-based servers, which then allows IT administrators to validate trusted hypervisors and create an audit trail in their cloud environments. The appliance also allows the identification and labeling of sensitive workloads and creation of policies that can ensure that these workloads are restricted to trusted systems.

**Hypervisor Layer**
Intel and McAfee work together at the hypervisor layer to provide security through Intel® Virtualization Technology (Intel® VT). Intel VT, which is available in select Intel Xeon processors, enhances traditional software-based virtualization solutions with hardware-based technology that accelerates key functions of virtualized platforms. Intel VT isolates virtual workloads to help prevent tampering on shared infrastructures, which is critical in multi-tenant environments. Intel VT can also speed up the transfer of platform control between guest operating systems and the virtual machine manager (VMM) or hypervisor, enable VMs to uniquely assign input/output (I/O) devices to guest operating systems, and optimize the network for virtualization with adapter-based acceleration. When combined with Intel TXT, Intel VT delivers a more protected, high-performance virtualized platform for server and client deployments.

**Virtual Machine Layer**
An important benefit of virtual machines is the ability to gain resource savings and agility for essential business operations. However, when traditional—and resource-intensive—antivirus technologies are applied to virtual machines, they can impair performance. This performance impact can lead to fewer virtual machines that can be realistically deployed and supported, and less potential for good operational benefits.

In response to this, McAfee developed its McAfee<sup>®</sup> Management for Optimized Virtual Environments (MOVE) AntiVirus. McAfee MOVE AntiVirus reduces the overhead resources that traditional endpoint security solutions require by providing essential antivirus protection that is designed to minimize any degradation to system performance.

---

*From Silicon to the Data: A Multi-Point Approach for Protecting Cloud Environments*
Using the processing features of McAfee VirusScan® Enterprise, McAfee MOVE AntiVirus is designed to support on-access scans, on-demand scans, and update functions within virtual desktop and server environments. It also supports all major hypervisors, delivering enormous flexibility.

McAfee MOVE AntiVirus provides continuous malware protection while minimizing any degradation to the user experience or affecting hypervisor loads. It does this using a unique approach to building and maintaining a cache of scanned files, which helps avoid excessive scanning. Common file sets are scanned only once, and the security diligence of file scanning is performed from the off-load server, ensuring malware will be caught and stopped from entering the environment.

McAfee MOVE AntiVirus also leverages McAfee Global Threat Intelligence (McAfee GTI), which is a comprehensive, real-time, cloud-based file reputation service that enables McAfee products to protect customers against both known and emerging malware-based threats.

And, when used in tandem with the McAfee ePolicy Orchestrator® (McAfee ePO™) platform, McAfee MOVE AntiVirus provides manageability of virus scanning across both physical and virtual environments. More details on the McAfee ePO platform can be found in the section “Providing a Unified View of Security.”

Operating System Layer

The operating system layer presents many opportunities for external attacks. McAfee has developed various editions of its McAfee Data Center Security Suites to provide comprehensive protection for data center components, including the McAfee Data Center Security Suite for Server, which provides a complete set of blacklisting, whitelisting, and optimized virtualization support capabilities for operating system security. There are three core technologies that form a part of this solution that can help protect data center operating systems:

- **Whitelisting with McAfee Application Control** provides an effective way to block unauthorized applications and code on servers, corporate desktops, and fixed-function devices. McAfee Application Control provides a centrally managed whitelisting solution that uses a dynamic trust model and innovative security features to fight advanced threats without requiring signature updates or labor-intensive list management.

- **Blacklisting with McAfee VirusScan Enterprise** provides a comprehensive antivirus solution that protects against all known threats using a comprehensive database of threat intelligence. The combination of whitelisting and blacklisting orchestrates an effective protection layer for servers while maintaining a high level of server performance—a distinct advantage contrasted with the use of antivirus alone on servers.

- **Virtualization with McAfee MOVE AntiVirus**, in addition to its role in securing the virtual machine layer, can provide protection for operating systems. It offers antivirus, anti-spyware, firewall, and intrusion-prevention technologies that can stop and remove malicious software. It is designed to extend coverage to emerging security risks, helping to reduce the cost of responding to outbreaks while minimizing the impact on system performance.

These tools can be managed from a single pane of glass using the McAfee ePO security management console.

Applications and Data Layer

Protecting the data is an essential objective for almost any type of sensitive or regulated workload. Encryption is a well-established way of providing a line of defense for data protection. But historically, the performance overhead of encrypting and decrypting data typically has caused IT to use this technology sparingly. At the applications and data layer, Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)
provides hardware-based acceleration for encryption. This technology, which is used by McAfee encryption solutions for improved performance, provides stronger and more efficient encryption, which adds up to better data protection in the cloud.

Intel AES-NI is an encryption instruction set that builds on the Advanced Encryption Standard (AES) algorithm and accelerates the encryption of data in the Intel Xeon processor family and in 3rd generation Intel® Core™ processors.

AES is the most widely used standard when protecting network traffic, personal data, and corporate IT infrastructures. With cloud computing—where business-critical information leaves the traditional IT environment—a more usable and secure encryption standard such as AES is essential to protecting this data from misuse.

Composed of seven new instructions, Intel AES-NI delivers faster, more affordable and efficient data protection and greater security, making pervasive encryption possible in areas where it was previously unfeasible.

Providing a Unified View of Security

The stratified nature of cloud environments not only increases the threat potential to data centers, it also makes monitoring and response activities more complicated. In an Intel survey of 800 IT managers around the world, 62 percent of the respondents said a major concern with cloud security was lack of visibility into the abstracted resources of virtualized environments, which exacerbated their concerns over lack of control. Nearly all of those surveyed—98 percent—said they would be interested in having tools that would allow them to measure the security posture of their cloud service provider.

To help enterprise administrators, managed service providers, and system integrators address these concerns and efficiently manage complex cloud systems, McAfee offers McAfee ePO, which can be augmented with a partner solution from Trapezoid—the Trapezoid Trust Control Suite.*

The McAfee ePO security management console gives IT administrators an intuitive, unified view of server, network, endpoint, and data security conditions and parameters for public and private cloud data centers. It uses an open architecture that ensures compatibility with a wide range of hardware platforms and offers drillable, drag-and-drop dashboards that let administrators add and rearrange windows for the tasks that are most relevant to their operation. With this unified view, the McAfee ePO platform helps administrators understand and create policies that can be implemented for physical and cloud environments. It offers features such as:

- Streamlined installation and guided configurations for rapid deployment
- Automated policy assignment, task scheduling, and incident responses that provide fast mitigation of potential problems
- Automatic communication within and between endpoints, networks, data, and compliance solutions, which reduces security gaps and management complexity
- System-wide detection of unknown assets that gain network access, which facilitates faster mitigation and increased protection
- Customizable report templates that can be personalized for diverse audiences with run-time parameters, which reduces the amount of time developing reports

• A new web API that lets administrators take advantage of existing enterprise assets and streamline workflows to enhance efficiencies and simplify compliance

The McAfee ePO platform can be used with Trapezoid Trust Control Suite, a security solution that works with Intel TXT to provide enhanced visibility into the server stack. The Trapezoid solution also integrates with the HyTrust Appliance to provide a full view into VMware vCenter events for better awareness and protection of the organization’s virtual machines. These event and asset monitoring capabilities are available as dashboards in McAfee ePO.

A Comprehensive Approach to Cloud Security

Greater business agility, resource savings, reduced IT workloads—these and other benefits make cloud platforms alluring for organizations, but security concerns stand in the way of more wholesale migrations to the cloud. Organizations have good reasons to be wary of increased risk when they are considering moving vital business information into virtualized environments.

Intel and McAfee, along with their industry partners, understand these concerns. Based on their established leadership roles, their expertise, and their presence worldwide in data centers and large organizations, they offer a comprehensive approach to providing security that can give IT managers peace of mind when moving their vital information assets to the cloud. By providing security solutions at every layer of cloud platforms—from the silicon to the applications and data—the joint solutions of Intel, McAfee, and their partners can give organizations the security assurances that will enable them to take advantage of all the benefits cloud computing has to offer.
From Silicon to the Data: A Multi-Point Approach for Protecting Cloud Environments

Learn more by visiting us online:


3 No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.x. For more information, visit www.intel.com/go/inteltxt.

4 Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/content/www/us/en/virtualization/virtualization-technology/hardware-assist-virtualization-technology.html.

5 Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) requires a computer system with an AES-NI-enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® Core™ processors. For availability, consult your system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.


7 McAfee, the McAfee logo, McAfee ePolicy Orchestrator, McAfee ePO, and McAfee VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications, and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2013 McAfee, Inc.

8 Intel, the Intel logo, Intel Core, and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

Copyright © 2013 Intel Corporation. All rights reserved. Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95052-8119, USA.

*Other names and brands may be claimed as the property of others. Printed in USA 6113UL/PRW/PDF Please Recycle 328586-001US