SOLUTION BRIEF
Cloud Security

Enhancing End-to-End Cloud Security

Cloud computing can help enterprise IT departments deliver IT as a service using a more flexible, efficient, and self-service infrastructure than in the past, which can result in agile application provisioning and greater operational efficiencies. However, security remains a substantial barrier to cloud adoption because IT departments are concerned about having less control, reduced visibility into workloads and data, dealing with new and unexpected threats to the infrastructure, and the risk of non-compliance. These concerns reduce confidence in security within and across private, public, and hybrid cloud environments.

Building a Foundation of Security from Client to Cloud

Together, Intel and McAfee are taking a holistic approach to address cloud security challenges and to establish confidence in the use of private, public, and hybrid clouds. The shared, multi-year mission is to enable worry-free cloud computing that is as secure as, or even more secure than, traditional, best-in-class enterprise IT security.

Creating highly secure cloud computing environments starts with building a foundation of security and integrity by securing cloud data centers, the network connections, and the devices that connect to the data centers (Figure 1). Developing common security standards with the industry is also vital to help ensure consistent security across clouds and to help achieve end-to-end visibility into and control over data, identities, and applications in cloud environments. Intel and McAfee are also working with a broad ecosystem of systems and software providers to enable open, interoperable security solutions to achieve this mission.

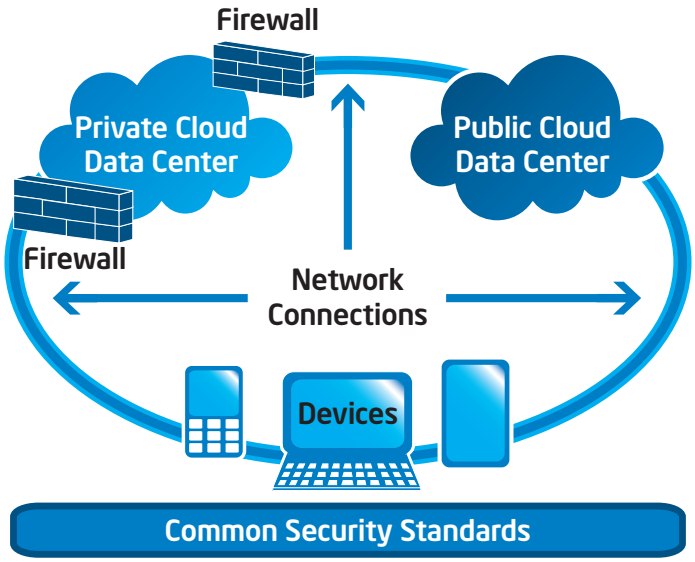

Figure 1. A foundation of security helps protect the data centers, the connections, and the devices

Proven security solutions from Intel and McAfee help enterprise IT departments strengthen cloud security today by:

- Safeguarding the applications and data in data centers
- Securing traffic and data between data centers and devices
- Protecting devices and identity of people accessing cloud services
- Aggregating security information to enable improved audit and compliance reporting

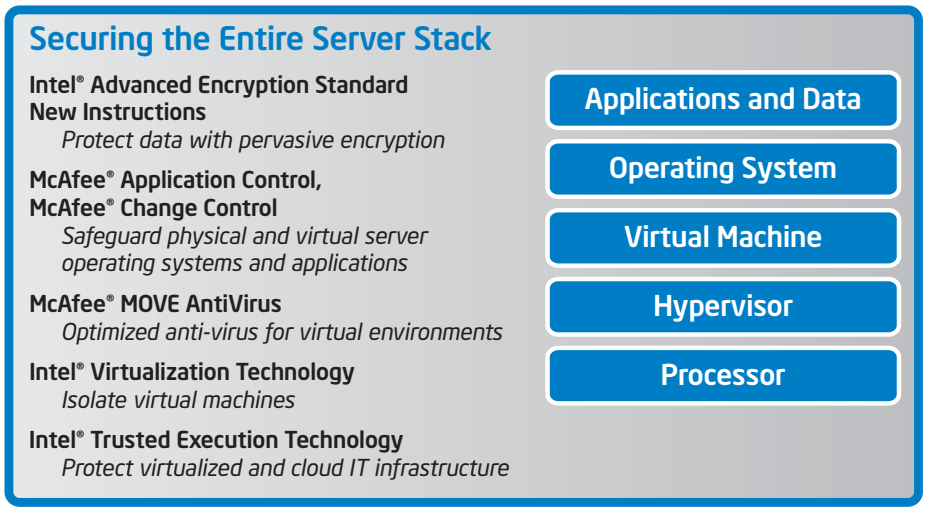

Figure 2. Intel and McAfee help secure the entire server stack

Securing Cloud Data Centers

In cloud computing, traditional methods of implementing and enforcing security policies and controls in data centers are no longer sufficient to keep attackers from gaining unauthorized access to and control of the underlying platform. Moreover, performing necessary auditing to meet compliance requirements is challenging in cloud environments. Intel and McAfee deliver technologies and solutions that help secure the entire server stack—from the underlying silicon and hardware through the hypervisor, operating system, applications, and data (Figure 2). These technologies strengthen the security of the IT infrastructure used in the cloud and better protect applications and data.

Starting at the silicon layer, Intel® Trusted Execution Technology (Intel® TXT) is a hardware security solution that helps protect IT infrastructures against software-based attacks by validating the integrity of key components within a server at startup. Moving up the server stack, Intel® Virtualization Technology (Intel® VT) offers hardware-assisted virtualization to strengthen the isolation of virtual machines on physical servers in cloud data centers.[1] When combined with Intel TXT, Intel VT creates a more secure and protected virtualization platform for server deployments.

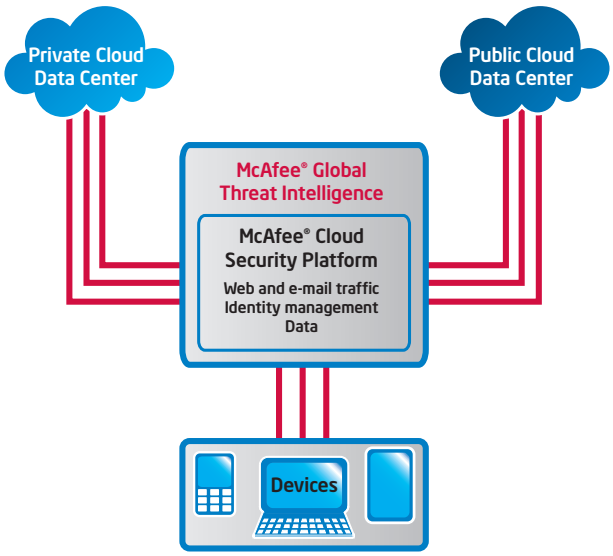

Figure 3. Secure connections between data centers and devices with McAfee® Cloud Security Platform

For virtual machines, McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus) offloads scan processing from virtual machines, delivering improved performance and resource utilization for virtual desktops and servers, along with optimized anti-malware and advanced threat protection. McAfee server technologies, such as Application Control and Change Control, work together to reduce overhead on servers and virtual machines, while proactively mitigating the risk of data breaches, targeted attacks, and unplanned downtime.

Data is the lifeblood of business. Encryption is one of the best ways to secure data at rest, but it is not widely implemented because of performance limitations. Comprised of seven new instructions, Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) provides up to ten times faster

encryption/decryption, more affordable data protection, and greater security, making pervasive encryption feasible in areas where previously it was not.[2,3]

Securing the Connections

Hybrid cloud environments that link multiple cloud data centers increase the amount of data, web, and e-mail traffic between private and public infrastructure and client devices. These connections expose confidential and business-critical data that is in flight or in use to attack. McAfee® Cloud Security Platform is the industry's first and only comprehensive cloud security platform that helps secure the primary forms of cloud traffic: e-mail, web, identity, and data (Figure 3). It provides a modular cloud platform to manage all data moving between private and public infrastructure and client devices or being stored in the cloud. It helps IT departments avoid data loss by protecting, identifying, and classifying data while it moves as e-mail, web, and authentication traffic.

With McAfee Cloud Security Platform, IT departments can restrict information access by extending and applying access and security policies into the cloud. McAfee Cloud Security Platform takes advantage of the unique McAfee® Global Threat Intelligence™ (McAfee® GTI™) technology to provide real-time protection against known and emerging threats. With visibility across all key threat vectors—file, web, e-mail, and network—and a view into the latest vulnerabilities across the IT industry, McAfee correlates real-world data collected from millions of sensors around the globe to deliver the most comprehensive protection in the market for cloud connections. Also, when data is in-flight between applications via web services, McAfee® Services Gateway provides application API management and security to control and authenticate users and data.

Securing the Devices

Employees are using an increasing number of devices and user name/password combinations to access enterprise and cloud services, which can lead to increased risk of identity theft or infection by new forms of malware. To mitigate this risk, Intel and McAfee are working to secure devices by protecting data and improving the ability to better control access to data and applications (Figure 4).

Simplifying and strengthening identity management across clouds. Two-factor authentication protects user identities in the cloud by combining something the user knows (a user name and password) with something the user has (a six-digit number, valid only for a short period of time). Intel® Identity Protection Technology (Intel® IPT) supports two-factor authentication by embedding this capability directly in hardware, eliminating the need for discrete hardware token generators. To further enhance identity management across clouds, McAfee® Cloud Identity Manager, which is part of the McAfee Cloud Security Platform, provides on-premises comprehensive software-based access control for cloud applications that use enterprise identities. This solution provides cloud account provisioning, deprovisioning, identity synchronization, single sign-on connectors to common SaaS applications, and two-factor authentication using one-time password soft tokens. For outsourced identity solutions that reside completely in the cloud, Intel® Cloud SSO offers these same capabilities.

Protecting data against stealth attacks. McAfee® Deep Defender, a joint solution developed by McAfee and Intel, represents the next generation of hardware-enhanced endpoint security.

UNIFIED SECURITY MANAGEMENT

As the foundation of McAfee security management, the McAfee® ePolicy Orchestrator® (McAfee® ePO™) platform enables consistent security-policy management across physical, virtual, and cloud environments. It provides a unified view of endpoint, server, network, and data security. McAfee ePO software enables end-to-end visibility for immediate insight and intelligence, greatly reducing the complexity of security and compliance administration in cloud environments. Its open architecture enables integration with a broad ecosystem of technology providers.

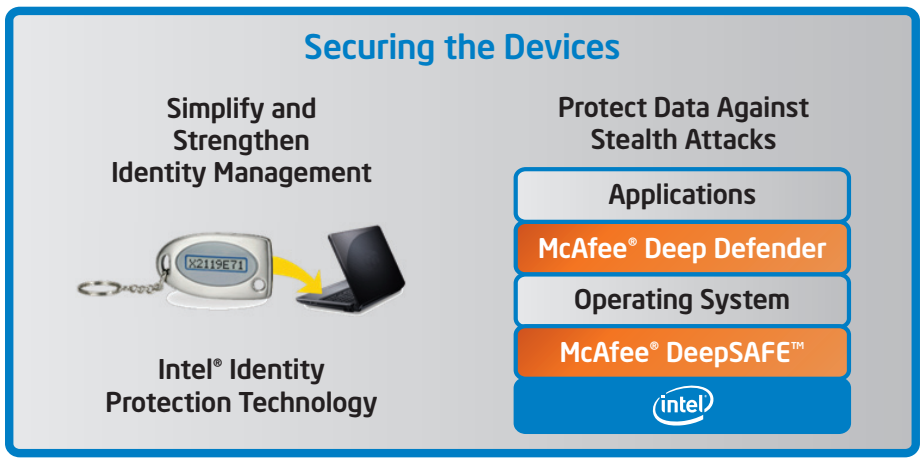

Figure 4. Securing devices through hardware-enhanced security features

Enabled by McAfee® DeepSAFE™ technology, McAfee Deep Defender resides between the memory and operating system on an endpoint device to perform real-time memory and processor monitoring. It is designed to detect, block, and remediate advanced stealth attacks, including zero-day malware that uses kernel-mode rootkits to embed itself underneath the operating system and evade current security solutions.

Conclusion

Intel and McAfee have a shared, multi-year mission to enable over time highly secure cloud computing where, for any given workload running on any connected infrastructure, IT departments can know that:

- Data, applications, and infrastructure are secure
- Corporate compliance requirements are automatically met
- Corporate security policies are automatically applied throughout the workload lifecycle
- Solutions that provide 24/7 reporting are easy to implement

You might have imagined this kind of world. With hardware-enhanced security technologies, plus software solutions and services available from Intel and McAfee, along with solutions enabled with a broad ecosystem of partners, you can start building a secure foundation today on a path toward worry-free cloud security of the future.

BROAD PARTNER ECOSYSTEM

Intel and McAfee are working with a broad ecosystem of system and software providers to enable security solutions. The McAfee Security Innovation Alliance (McAfee SIA), a technology partnering program, accelerates the development of interoperable security products and simplifies the integration of these products with complex customer environments. The Intel® Cloud Builders program brings together leading systems and solutions providers to provide practical guidance and reference architectures on how to deploy and optimize a cloud infrastructure and enhance security.

Learn More

For more information about security technologies and solutions from Intel, McAfee, and solutions partners, visit these links:

- Intel Cloud Security initiatives and technologies: www.intel.com/cloudsecurity
- Intel Cloud Security Planning Guide: www.intel.com/content/www/us/en/cloud-computing/cloud-computing-security-planning-guide.html
- Intel Cloud Builders: www.intelcloudbuilders.com
- Intel Cloud SSO: www.intelcloudsso.com
- Intel Identity Protection Technology: http://ipt.intel.com/welcome.aspx
- McAfee Data Center Security: www.mcafee.com/us/solutions/data-center-security/data-center-security.aspx
- McAfee Cloud Security Platform: www.mcafee.com/us/solutions/cloud-security/cloud-security.aspx
- McAfee Deep Defender: www.mcafee.com/us/products/deep-defender.aspx
- McAfee Global Threat Intelligence: www.mcafee.com/us/mcafee-labs/technology/global-threat-intelligence-technology.aspx
- McAfee Security Innovation Alliance: www.mcafee.com/us/partners/security-innovation-alliance/index.aspx

[1] 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/go/virtualization

[2] Source: http://www.oracle.com/us/corporate/press/173758

[3] 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/.

Printed in USA 0412/JL/PRW/PDF Please Recycle 327233-001US