Intel IT Center

NOVEMBER 2012

Vendor Spotlight

Always-On Security in the Cloud and across the Data Center

Scott Gainey, *Senior Director, Products and Solutions Marketing for Security, Cisco*

Scott Gainey, senior director of products and solutions marketing for security at Cisco, discusses the key components of the Cisco* cloud security platform and how you can simplify security management across virtual and physical environments.

Data centers today continue to undergo significant transformation. In fact, by 2015, Cisco predicts there will be a nearly 3,000 percent growth rate in the overall application, traffic, and network connections required. On top of this, data centers are increasingly moving from physical to virtual workloads, and ultimately, the cloud. Mobility and consumerization of IT are also pushing out the perimeter of the data center, and with more devices accessing company data, these trends are creating a significantly larger attack surface for IT to manage.

To tackle this significant change and protect the enterprise, IT needs always-on and scalable security that spans traditional and cloud environments.

Cisco helps keep security at the forefront as organizations deploy private, public, and hybrid cloud infrastructures by:

- Providing threat defense and a stronger level of control and granularity for applications that are accessed through the cloud.
- Delivering the ability to create better and more secure segmentation in these multitenant environments. Cisco's ASA 1000V solution helps you create firewalls between virtualized environments within a cloud, so you can manage the virtual and physical environment with a single tool. Now you can create a single set of policies to govern access to information and applications from both a physical and a cloud-based environment.
- Delivering greater visibility into what is happening within the network. The ability to recognize emerging threat patterns is critical in defending against them. From insight gained by having 70 percent of the world's Internet traffic traverse its systems and by monitoring 35 percent of the world's e-mail traffic, Cisco can share knowledge with customers for informed policy decisions.

Cisco's Cloud Security Solutions

Cisco offers a range of products that can help IT managers take advantage of cloud computing, reaping the return-on-investment benefits of a flexible, virtualized environment while keeping the enterprise secure.

Cisco SecureX Architecture*

This context-aware security framework helps ensure a trusted network infrastructure as organizations embrace a mobile, dynamic, and cloud-based working environment. With this framework, IT managers can easily define and manage business-relevant security policies and add enforcement elements in the form of appliances, modules, and cloud services.

Cisco cloud security consists of three key solution components:

- **Secure cloud infrastructure.** A comprehensive offering that includes the Cisco ASA 5585-X Adaptive Security Appliance and Cisco Catalyst* 6500 Series ASSA Services Module, the Cisco Nexus* 1000V Series Switches, Cisco Virtual Security Gateway, and Cisco IPS 4500 Series Sensors. Combined, these solutions provide in-depth capabilities to secure your private, public, or hybrid cloud environment.
- **Cloud security services.** Cisco offers e-mail, web, and threat intelligence via the cloud to help protect the enterprise while providing scalability options and helping to reduce costs.
- **Secure cloud access.** Supports a multidimensional defense strategy that includes secure software-as-a-service (SaaS) and network access. You retain full control over authentication and authorization of SaaS application users while providing them with the seamless access they need to stay productive while mobile.

What IT Managers Are Looking for in Cloud Security

When it comes to maintaining security when moving workloads to the cloud, IT managers are looking for the ability to:

- Drive a consistent set of policies and enforcement across a mixed physical and virtual environment.
- Rapidly scale their security infrastructure to meet increasing performance needs.
- Mitigate against increasingly complex threats.
- Choose from deployment models that include virtualized options for the security infrastructure.
- Easily align business requirements with the necessary security policies.

Cisco Unified Computing System* Built on Intel® Technologies

Cisco works closely with Intel on its overall Cisco Unified Computing System* (Cisco UCS*) product portfolio, which serves as the most central element of Cisco's cloud offerings. For example, Cisco UCS is architected to take advantage of the Intel® Xeon® processor E5 family, enabling the entire line of M3-class servers to deliver increased I/O and storage performance capabilities that complement other internal features such as Cisco Flexible Flash. In addition, the M3 line of servers provides enhanced security through Intel Virtualization Technology (Intel VT)[1] and Intel Trusted Execution Technology (Intel TXT)[2] integrated in the system,[3] and takes full advantage of Intel Advanced Encryption Standard New Instructions (Intel AES-NI)[4] technology, an instruction set for best-in-class performance on encryption.

Cisco has a long history of working collaboratively with Intel to bring innovation to the marketplace. The Cisco UCS M3 line of servers powered by Intel Xeon technology is the latest in this shared vision to improve performance in the data center and deliver fundamentals for cloud architecture that are secure and efficient.

For more information about Cisco UCS and Cisco cloud security solutions, visit cisco.com/go/ucs.

For recent customer stories on cloud security or other issues facing IT professionals, visit unleashingit.com.

Share with Colleagues

[1] Intel VT requires a computer system with an enabled Intel processor and 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 intel.com/go/virtualization.

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

[3] No computer system can provide absolute security under all conditions. Built-in security features available on select Intel® Core™ processors may require additional software, hardware, services, and/or an Internet connection. Results may vary depending upon configuration. Consult your PC manufacturer for more details. For more information, visit intel.com/technology/security.

[4] Intel AES-NI requires a computer system with an Intel AES-NI–enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. Intel AES-NI is available on select Intel Core processors. For availability, consult your system manufacturer. For more information, see intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html.

1112/RF/ME/PDF-USA 328281-001

Sponsors of Tomorrow.™