Intel IT Center

OCTOBER 2012

Vendor Spotlight

IBM Offers Cloud Security for a Smarter Planet

Ajay Dholakia, *Senior Technical Staff Member, System x* Software Strategy, IBM*

Ajay Dholakia, senior technical staff member working on System x* software strategy at IBM, discusses the ways that IBM can help customers build a secure public, private, or hybrid cloud.

As more and more organizations adopt cloud technology, the promise of agility, efficiency, and cost savings is delivering real and tangible benefits. And even as cloud computing changes the way we think about technology, it also impacts how we address security. In fact, security is one of the top concerns for organizations looking to move their workloads to the cloud. As organizations look to the cloud, the IBM* portfolio of cloud security solutions can help IT managers protect data, secure their infrastructure, and strengthen compliance.

The IBM* Security Framework: Focus on Four Security Domains

The IBM Security Framework focuses on four security domains to protect across people (users, their roles and identity, and role-based access); data (protecting data wherever it resides and assigning different levels of security based on the type of data or solution); application (protecting the workloads on the applications that run in the cloud and are consumed through the cloud); and the IT infrastructure (securing the domain of the IT infrastructure itself).

Sponsors of Tomorrow.™ intel

Private, Public, or Hybrid?

Private cloud can serve as an entry point for building a cloud infrastructure in-house. A private cloud gives IT managers the ability to see the tangible benefits of the cloud—and become comfortable with the security capabilities—while also working within the regulatory and compliance requirements that they need to meet. IBM* private cloud offerings are built off the same technologies IBM uses for its clouds, providing full control of access, availability, and recovery and best-in-class security and open standards.

Public cloud offerings from IBM provide secure, rapidly available virtual resources, a good option for companies that need an easily scalable environment and wish to take advantage of the infrastructure as a service (IaaS) or platform as a service (PaaS) model and pay for only the resources used. A good starting point for implementing a public cloud environment? Identify those processes or workloads where regulatory requirements are less stringent than in other areas of the business.

A hybrid cloud gives you flexibility and the ability to take advantage of the best of both cloud environments. With IBM public cloud offerings, users can achieve a balance between where these requirements are being met—either by the user or the provider—and associate the right type of boundaries between the two to keep security in check.

Cloud-Ready Virtualized Infrastructures

IBM SmartCloud* Foundation. The IBM SmartCloud portfolio includes cloud architectures, cloud services, and cloud solutions. Within this portfolio, IBM SmartCloud Foundation is a set of technologies for clients to build and deploy their private and hybrid cloud. Across the IBM SmartCloud portfolio, there's a key focus on security spanning the four domains to help ensure that clients can adopt IBM cloud computing solutions with a high level of trust and confidence. For instance, IBM SmartCloud Entry software, available on IBM servers using Intel® chipsets, delivers reliable and secure private cloud capabilities by isolating virtual machines and tracking images to minimize security risks.

IBM SmartCloud Foundation offers cloud infrastructure that is designed to offer a safe environment populated with an array of security features. The servers in these families provide boot firmware security that uses the core root of trust measurement technology from the Trusted Computing Group, a standards body with industry participation from IBM and Intel. These are based on using a chip called the Trusted Platform Module (TPM), which measures and verifies the boot firmware. The TPM is designed to help establish trust, exchange information, and apply policy. This sets up a chain of trust for the next layers of the operating stack to create a trusted compute pool built from servers of known good integrity.

Intel Trusted Execution Technology (Intel TXT)[1] builds trust into each server at the server level by establishing a root of trust that helps ensure system integrity within each system. The IBM PureSystems*, IBM System x*, and IBM BladeCenter* families all use TXT-enabled processors and chipsets along with the TPM chip. In doing so, they can take advantage of the broad array of Intel TXT features when deployed in conjunction with TXT-enabled operating systems and hypervisors, which represent the next layer in the operating stack.

IBM Blade and Rack Servers

The **IBM PureFlex* and the IBM Flex System* families** have secure chassis infrastructure that includes trusted system management that is protected by a separate set of TPM chips. That allows IT managers to achieve integrity for the management controllers that are deployed in the system, through measurement and verification of the firmware that runs on the controllers. It's also used for secure inter- and intra-chassis communication links between these various management modules and controllers. And within the people security domain, PureFlex and Flex System offerings include role-based access, centralized management of user security, and associated policies, such as password protection. IBM SmartCloud Entry is included with IBM PureFlex and available for IBM Flex System.

Built using Intel chipsets and designed for use with IBM SmartCloud Entry, the **IBM BladeCenter Foundation for Cloud** is a comprehensive virtualization platform with converged networking, servers, storage, and management to deliver a cloud-ready infrastructure and enable both private and hybrid clouds. IBM BladeCenter Foundation for Cloud is beneficial for organizations that want to continue with their existing BladeCenter infrastructure.

Also built using Intel chipsets, the IBM Ready Pack for Cloud* offering is an integrated solution comprised of IBM System x servers, storage, and networking hardware that forms the foundation for a private cloud infrastructure. IBM Ready Pack for Cloud enables small and medium businesses (SMBs) to achieve operational efficiencies and faster time to market.

Intel and IBM Working Together

Together, Intel and IBM are working to provide proven security solution stacks to make the cloud work for you. In addition to being TXT enabled, these IBM solutions broadly use Intel Advanced Encryption Standard New Instructions (AES-NI)[2] technology. Use of AES-NI in the management software offerings also helps to ensure encryption within the interprocess communications.

Build a Smarter Planet with Cloud Security

Cloud computing is a disruptive force that is changing how we think about technology. And the promise of the cloud makes it an attractive option for the enterprise—helping IT manage pressures on the data center while offering tangible benefits to the organization. IBM's vision for cloud computing can help accelerate business transformation. And together, IBM and Intel can help you implement a cloud strategy that keeps security top of mind.

For more information about IBM cloud security solutions, visit http://ibm.com/cloud-computing/us/en/index.html.

Share with Colleagues

1 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 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 http://intel.com/go/inteltxt.

2 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 Intel® Xeon® processors, Intel® Core™ i5-600 Desktop Processor Series, Intel Core i7-600 Mobile Processor Series, and Intel Core i5-500 Mobile Processor Series. For availability, consult your reseller or 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.

1012/RF/ME/PDF-US 328084-001

Sponsors of Tomorrow.™