Intel IT Center

JANUARY 2013

Industry Brief

Securing the Cloud for Government Entities

An Overview of Cloud Security Issues Facing Governmental Organizations and Intel® Technologies for Securing the Government Cloud

Why You Should Read This Document

This industry brief provides an overview of the benefits and security challenges of cloud-based infrastructures for government agencies and organizations, with an introduction to Intel technologies that can help strengthen the government cloud. This brief:

- Discusses how the cloud computing model can lower operational costs for government agencies and improve delivery of services to citizens and other constituents
- Examines legitimate security, regulatory, and compliance concerns that have slowed implementation of the cloud in government
- Describes how data encryption can help safeguard sensitive personal data as it moves in and out of the cloud
- Explains how hardware-based authentication can validate identity and access in the government cloud to help ensure that only authorized users can enter
- Examines how service gateways provide API enforcement points at the network edge to reduce the risk of content-born attacks against government organizations
- Discusses how virtualized platforms can be made more secure with hardware roots of trust that help assure system integrity and provide a foundation for trusted computing across dynamic environments

Intel IT Center

JANUARY 2013

Industry Brief

Securing the Cloud for Government Entities

An Overview of Cloud Security Issues Facing Governmental Organizations and Intel® Technologies for Securing the Government Cloud

Nigel Ballard, *Director of Federal Marketing, Intel Americas*

Kevin Fiftal, *Federal Civilian Director, Intel Americas*

Sponsors of Tomorrow.™

Contents

Securing the Cloud for Government Entities

Cloud computing presents a new model for improving delivery of government services and increasing the business agility of government agencies, enabling them to operate with greater efficiency and cost effectiveness. In February 2011, the government issued the Federal Cloud Computing Strategy[1] that describes cloud computing as a "profound economic and technical shift (with) great potential to reduce the cost of Federal Information Technology (IT) systems while … improving IT capabilities and stimulating innovation in IT solutions."

However, government also operates in a regulated environment and cloud computing heightens concerns over privacy, security, access and compliance. Government agencies need a comprehensive cloud-computing platform that can power a new generation of public sector services and initiatives while providing security and compliance, as well as data and infrastructure protections to meet regulatory standards. This paper describes the benefits that cloud computing environments can bring to government entities, and examines the security and compliance considerations that government IT infrastructures must meet. It discusses how cloud security is strengthened with Intel® technologies that make it easier for government organizations to secure data, authenticate identities and access requests, and increase trust and compliance across the cloud environment.

Benefits of Cloud Computing for Government

Government is undergoing enormous change and reform. Agencies and organizations are under pressure to provide greater and better services while also lowering costs. As "do more with less" becomes the new mantra, government institutions are increasingly required to find more efficient and effective ways to address the needs of citizens.

Cloud computing can help address some of these challenges. The efficiencies and cost-savings made possible by cloud environments directly help lower operational expenses of government institutions. The amount of potential savings through modernization of aging government computing infrastructures is staggering—the U.S. Department of Defense estimates that data center consolidation within its agency alone could lead to as much as $680 million in annual savings by 2015. And of that, some $58 million would come just from energy savings (from improved power management available in today's computers).[2]

The agility provided by on-demand and flexible cloud-based computing resources can also help empower a new generation of services and initiatives that allow agencies to respond more quickly and creatively to the needs of the public they serve.

Improved Delivery of Government Services

The flexible, highly scalable computing resources delivered through cloud computing environments enable faster, easier deployment of e-government and citizen self-service initiatives to improve flow of information. Cloud-based solutions offer the availability to expand security-enhanced services and data access to:

- Other agencies and departments
- State and local governments
- External organizations where government plays an oversight role, including healthcare and finance
- The public

Cloud infrastructures can also provide government agencies improved information management, with centralized data storage and high-speed networks enabling increased productivity, improved support of government services in the field, and enhanced data sharing and collaboration.

A scalable, efficient, and agile computing infrastructure. The basic IT benefits of cloud computing—higher compute availability, greater efficiency, on-demand self-service, and IT agility—provide abundant advantages to government agencies.

High availability cloud infrastructures scale according to need, and provide the compute power for any type of workload. Services can be delivered through secure broadband network access to authenticated devices, or via self-service portals. Additionally, redundancy and disaster recovery is built into cloud environments, providing failover assurance for sensitive information. Cloud-based infrastructures are also more efficient than traditional data centers, and provide cost reductions through server consolidation, reduced IT management, improved network performance, and greater energy savings.

The agility of cloud infrastructures is demonstrated in the ability to provision services in a matter of hours—as opposed to provision times of days and weeks using traditional data center operations. This agility is particularly important to government organizations facing an environment of reform in uncertain economic times, allowing them to address the need to quickly evolve both business processes and workflow design without incurring significant capital and infrastructure expenditures.

Concerns with Cloud Computing Meeting Government Security and Standards

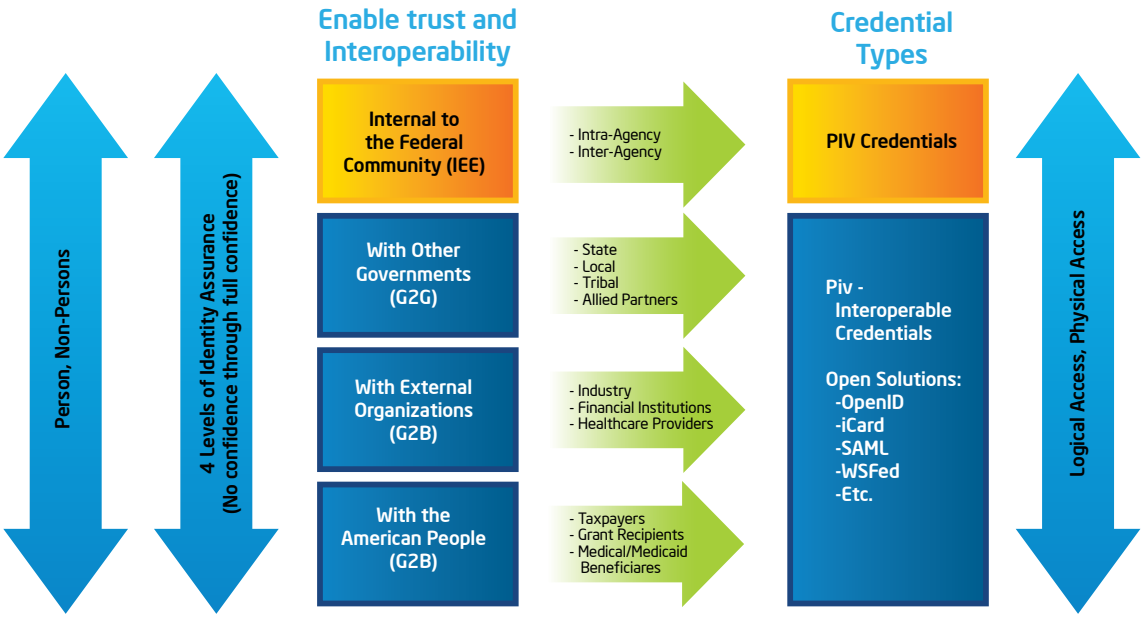
While cloud computing promises significant IT infrastructure benefits, legitimate security and compliance concerns have slowed cloud implementation within many government agencies, particularly those that handle classified and protected data. Cloud infrastructures for government agencies must meet regulatory standards and guidance, including:

National Strategy for Trusted Identity in Cyberspace (NSTIC), which defines an online environment where individuals, organizations, services, and devices can trust each other because authoritative sources establish and authenticate their digital identities.

Homeland Security Presidential Directive 12 for Common Identity Standards for Federal Employees and Contractors (HSPD-12), a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and contractors to enhance security, reduce identity fraud, and protect personal privacy. Federal Information Processing Standard (FIPS) 201, entitled Personal Identity Verification (PIV) of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12.

Federal Risk and Authorization Management Program (FedRAMP), a government-wide risk management program focused on standardizing authorizations and continuous security monitoring services for cloud computing systems intended for multi-agency government use.

Federal Identity Credential and Access Management (Federal ICAM), a federal initiative to merge the digital identities, authentication credentials, and access control into single comprehensive management approach.



Federal ICAM provides a comprehensive architecture to enable trust and interoperability for digital transactions within the U.S. federal government and its constituents, including required credential types for access.

National Institute of Standards and Technology (NIST), which works with industry to develop and apply technology, measurements, and standards. The U.S. Commerce Department's NIST has released a draft "roadmap" that is designed to foster federal agencies' adoption of cloud computing, support the private sector, improve the information available to decision makers and facilitate the continued development of the cloud computing model. As part of the Federal Cloud Computing Strategy, NIST has been assigned "a central [role] in defining and advancing standards, and collaborating with U.S. government agency CIOs, private-sector experts and international bodies to identify and reach consensus on cloud computing technology and standardization priorities." [3]

This draft publication is designed to support the secure and effective adoption of the cloud-computing model by federal agencies to reduce costs and improve services. It defines high-priority requirements for standards, official guidance and technology developments that need to be met in order for agencies to accelerate their migration of existing IT systems to the cloud-computing model. "A key contribution of the roadmap effort is to focus the discussion to achieve a clear understanding between the government and private sector," said Senior Advisor for Cloud Computing Dawn Leaf, "particularly on the specific technical steps (standards, guidance and technology solutions) needed to move federal IT from its current early-cloud state to a cloud-based foundation, as envisioned in the *U.S. Federal Cloud Computing Strategy*."

Cloud Environments Present a Range of Security Challenges

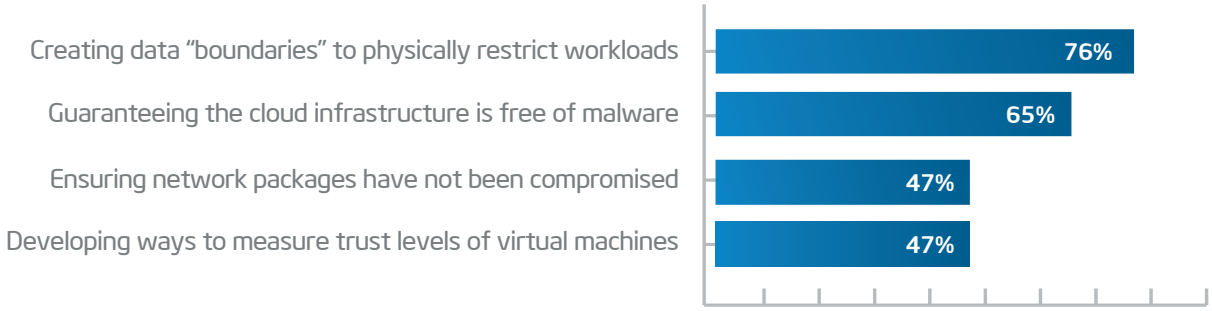
Identity and access management. Existing organizational identification and authentication frameworks may not extend into the cloud, and if these are based on unique username/password combinations for individual applications, they can represent a weak link in the security chain. In the cloud, identity management is key to maintaining security, visibility, and centralized IT control of identities and access.

Data protection. Data stored in the cloud typically resides in a multi-tenant environment, sharing virtualized server space with data from other customers of the cloud provider. Government organizations that move sensitive and regulated data into the cloud must ensure that the data is controlled and secure. One of the inherent risks of multi-tenancy and shared compute resources within cloud infrastructures is the potential failure of isolation mechanisms that serve to separate memory, storage, and routing between tenants.

Meeting federal standards and baselines. Federal laws, rules and standards call for a complex weaving together of security and privacy mandates, making compliance a potentially complicated issue for cloud computing. To support compliance within these strict data privacy laws, it is desirable for cloud infrastructures to be auditable for such features as encryption, security controls, and geo-location.

Trust. In cloud infrastructures, government organizations relinquish direct control over many aspects of security, shifting an enormous burden of trust onto the cloud provider. The cloud provider's role is critical in performing incident response, including attack analysis, containment, data preservation, remediation and service continuity. For highly regulated government organizations, deploying data management tools that provide visibility across the cloud to ensure agreed-to policies are being enforced is a requirement.

Government IT pros reveal abilities that would increase private cloud confidence*



*Extended analysis of data from "What's Holding Back the Cloud?" Intel's survey on increasing IT professionals' confidence in cloud security.

Secured architecture. For cybercriminals, virtualized cloud infrastructures offer an even larger potential attack surface than a traditional data center. Onslaughts using malware and rootkits can infect cloud system components such as hypervisors, BIOS, and operating systems and spread throughout the environment. Protecting a government cloud from malware requires management of identities and APIs at the network edge to ensure that only authorized users can gain access, and the establishment of roots of trust to assure system integrity.

Mobile access. Using mobile devices to extend government services beyond the office provides obvious benefits to staff and the public alike. However, accessing confidential data on unsecured mobile devices runs the risk of data theft or loss—and of regulatory noncompliance. The increasing numbers of mobile devices and mobile workers in government are driving the need for device management solutions and regulated API environments that provide secure transmission of data and solutions across broadband networks, protecting devices from data breach and unauthorized access.

NIST has published a draft guideline that outlines the baseline security technologies mobile devices should include to protect the information they handle. Smart phones, tablets and other mobile devices, whether personal or "organization-issued," are increasingly used in business and government. NIST's goal in issuing the new guidelines is to accelerate industry efforts to implement these technologies for more cyber-secure mobile devices. Guidelines on Hardware-Rooted Security in Mobile Devices defines the fundamental security components and capabilities needed to enable more secure use of products.

Protecting the Government Cloud with Comprehensive Security Approaches

Today's cloud technologies can significantly reduce the security risks previously associated with cloud environments. Intel hardware-enhanced security technologies provide tamper-resistant capabilities to better protect identities, data, and the cloud infrastructure. Solutions that use these capabilities can strengthen identity protection, encourage pervasive encryption to better protect data, measure platform integrity, and enforce security policies to better meet compliance requirements.

Protecting data in motion and at rest. Protecting confidential and regulated data is a fundamental responsibility of government, and the best way to protect data, whether at rest or as it moves in and out of the cloud, is encryption, which makes data unusable if compromised. It also demands secure communication connections, which locks down browser access and encrypts content as it is transferred over the network and throughout the cloud.

However, data encryption based on the Advanced Encryption Standard (AES) relies on compute-intensive algorithms that can impact the performance of the computing network, particularly when used pervasively to protect the massive volumes of information that pass to and from the cloud. Traditional encryption solutions can create computing logjams due to high performance overheads, making them less than optimal for protecting cloud data traffic.

Intel has worked to mitigate these performance penalties. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), built into Intel® Xeon® processors, Intel® Core™ vPro™ processors, and select Intel® Core™ processors[4], enhances encryption performance by speeding up the execution of encryption algorithms by as much as 10 times.[5, 6] Intel AES-NI delivers faster, more affordable data protection, making pervasive encryption standard in cloud networks where it was not previously feasible.

The browser security protocols Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are used to assure safe communications over networks, including the Internet, and are widely used for secure web browsing (HTTPS), electronic mail, instant messaging, and voice over IP. These protocols are also critical for secure cloud computing, preventing undetected content tampering or "eavesdropping" on content as it's transferred.

However, traditional SSL and TLS protocols involve two compute-intensive phases—session initiation and bulk-data transfer. Intel has made two contributions to the widely used, open-source protocol, OpenSSL* which greatly improve performance during these phases. One is a library function that accelerates session initiation and a second enables simultaneous execution of data encryption and authentication for bulk data. Any software that incorporates OpenSSL can automatically take advantage of these Intel advancements.

By accelerating data encryption, secure session initiations, and transfer of bulk data, government organizations can better utilize network resources and implement pervasive data protection to and from the cloud without compromising compute performance.

More secure access in the cloud. Realizing cloud-computing advantages while meeting stringent requirements for data security and regulatory compliance requires hardening the underlying platform, including hardware, software and process methodologies. Securing both server and client platforms safeguard cloud infrastructures, and managing identities and access-control points at the network edge ensures that only authorized users can enter the cloud. With malware attacks now moving beyond software to target the platform, organizations face new risks from rootkit and other low-level exploits that can infect system components such as hypervisors and the BIOS to quickly spread throughout the cloud environment.

Protecting identity in the cloud. Protecting a cloud platform begins with managing who has access to it. Intel® Identity Protection Technology (Intel® IPT), found in Intel® Core™ vPro™ processors, builds tamper-resistant, hardware-based authentication that provides a simple way for government organizations to validate that legitimate employees or authorized users are logging in from a trusted device. Intel IPT offers token generation built into the hardware, eliminating the need for (and cost of) a separate physical token. It also verifies transactions and protects against malware.[7]

Establishing API security at the edge. Application programming interfaces (APIs) are the fundamental method to expose cloud applications to third parties and mobile services. To reduce the risk of content-born attacks on cloud-accessed applications and to protect edge-system infrastructures requires controlled, compliant API governance, particularly at the gateway layer where security policy enforcement and cloud service orchestration and integration take place. Intel® Expressway Service Gateway (Intel® ESG)[8] is a software appliance that provides enforcement points at the network's edge to authenticate API requests against an organization's existing identity and access-management systems. Service gateways offer a centralized way for IT and developer teams to collaborate on cloud security policy and enforcement, and deliver standards-based security for consistent API-level controls across the organization.

Ensuring cloud infrastructure is more secure and auditable. Cloud computing, with its dynamic resources and dependence on virtualization, pushes the perimeter of the government organization far beyond the traditional data center, and with the addition of hypervisors and multi-tenant environments, creates a much larger attack surface for malware and other exploits. The threats against this larger target involve not only malware assaults at the application level, but also attacks against lower-level components in the platform itself.

In addition, reduced visibility into cloud infrastructures also makes it difficult to verify that applications and data are secure and meet statutory and regulatory compliance.

Intel® Trusted Execution Technology (Intel® TXT), found in Intel® Xeon® processors, can help government organizations reduce the security risks and compliance complications that derive from virtualized computing platforms.[9] Intel TXT establishes a more secure platform based on a hardware root of trust at the level of the chipset and CPU. This root of trust helps assure system integrity, providing a solid foundation upon which to build more secure virtual platforms and pools of trusted computing, substantially reducing the security risks of using a virtualized cloud infrastructure by restricting sensitive workloads to trusted compute pools.

Intel TXT measures platform components such as the BIOS and hypervisor in their "known good" state. These trusted measurements are stored in hardware and compared to boot-time measurements made during subsequent launch sequences. If the measurements do not match, Intel TXT can block the launch of the platform, mitigating boot-level attacks.

Intel TXT Enables the Following Characteristics:

Verified launch. Using a hardware root of trust and cryptographic measurements, Intel TXT establishes a safe environment for launching virtual machines (VMs); it also interacts with governance, risk, and compliance tools to report on verified launch status of VMs to improve insight and visibility into the underlying infrastructure.

Policy-based live migration. For sensitive workloads, organizations can enforce policies such as the following: VMs shall only be migrated between hosts that have successfully undergone a verified launch.

Protected execution. For highly sensitive or protected information, Intel TXT enables applications to run in isolated environments on dedicated resources managed by the underlying platform.

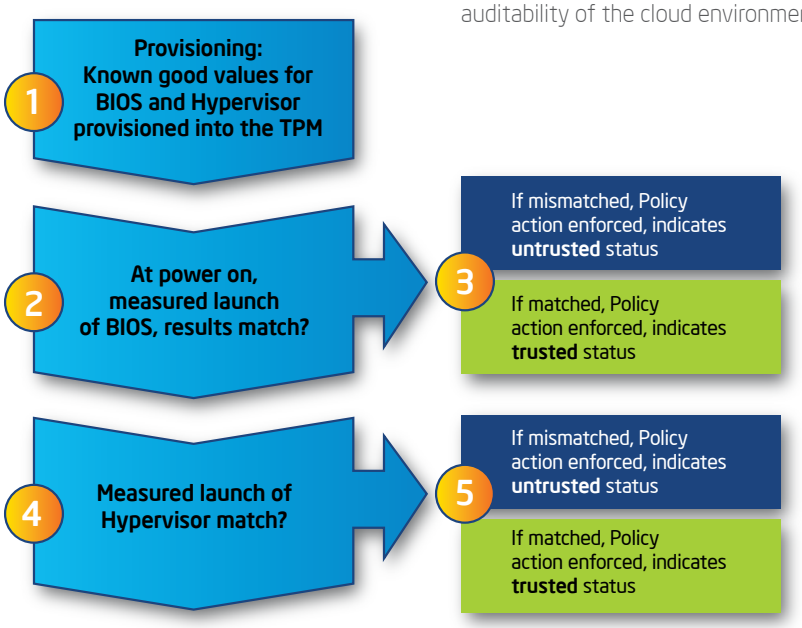
Protected input. Through the use of cryptographic keys, Intel TXT protects communication between input devices (such as mice and keyboards) and execution environments to guard against the data being observed or otherwise compromised by unauthorized software processes.

Data protection. The risk of insecure or incomplete data deletion in shared cloud resources raises the security risk of data migration from virtual machines and reuse of cloud hardware. Intel TXT scrubs memory during environment shutdown to mitigate memory snooping or reset attacks

Auditable compliance. For government organizations, meeting standards and compliance requires significant time, effort, and budget. Regulations often demand security enforcement and can create audit requirements, with the need to understand, document, and report what's happening in the cloud environment to verify that security policies are set, monitored, and certified. Increasingly, Intel TXT is being utilized by software solutions that manage governance, risk and compliance of virtualized infrastructures based on different security framework requirements.

Trusted compute pools are foundational for building trust across dynamic environments. When grouped together with similar policies, trusted compute pools of virtualized servers can be validated by external entities based on known, trustworthy signatures. Intel TXT can establish and verify adherence to data protection and control standards—enabling hardware-based reporting of platform trust both locally and remotely, enhancing the auditability of the cloud environment.

How Intel TXT protects a virtual server environment.



Conclusion

Intel technologies help government organizations gain the benefits of cloud computing by building a comprehensive foundation for a more secure virtual environment. Intel provides the tools to help manage the most important security challenges to the government cloud—data and infrastructure protection and compliance—with technologies that promote pervasive data encryption, provide more secure data movement, and build higher assurance into compliance efforts.

Intel's comprehensive set of security technologies and solutions cover end-to-end cloud deployment models, but these are only a part of Intel's efforts to secure the cloud. Intel is working to develop best practices, standards, design principles, deployment considerations, and governance models to accelerate cloud adoption by government entities. Intel® Cloud Builders provides proven security reference architectures in conjunction with Intel partners to ease deployment. The Intel® Cloud Finder program can help identify cloud service providers that meet your specific requirements.

Intel is also participating with partners and key industry alliances worldwide to accelerate cloud security standards and interoperable solutions by working with such industry organizations as:

Open Data Center Alliance (ODCA)

Cloud Security Alliance (CSA)

Trusted Computing Group (TCG)

As government organizations look to more securely integrate their data and business structures in the cloud, Intel continues to drive hardware-enhanced security technologies and software solutions that improve protection of identities, data, and infrastructure in the cloud. These innovations will further increase confidence in the government cloud by providing increasingly robust methodologies to better manage, monitor, and enforce security policies and enable automated auditing of cloud environments to meet compliance requirements.

For more information on cloud security, visit intel.com/cloudsecurity.

1 Federal Cloud Computing Strategy

2 InformationWeek Government: Cloud in Action

3 U.S. Government Cloud Computing Technology Roadmap, Release 1.0 (NIST Special Publication 500-293)

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. 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 http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html.

5 Source: Testing with Oracle Database Enterprise Edition 11.2.0.2 with Transparent Data Encryption (TDE) AES-256 shows as much as a 10x speedup when inserting 1 million rows 30 times into an empty table on the Intel Xeon processor X5680 (3.33 GHz, 36 MB RAM) using Intel IPP routines, compared with the Intel Xeon processor X5560 (2.93 GHz, 36 MB RAM) without Intel IPP.

6 Software and workloads used in performance tests may have been optimized for performance only on Intel® microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations, and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

7 No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd or 3rd gen Intel® Core™ processor, enabled chipset, firmware, and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://www.intel.com/content/www/us/en/architecture-and-technology/identity-protection/identity-protection-technology-general.html.

8 Requires Intel® Xeon® Multi-Core server with 4GB RAM (16GB Recommended); recommended for use on Red Hat* AS4/A5 (32 or 64-bit), SUSE Linux Enterprise* 10 (32 or 64-bit), Oracle* Enterprise Linux, Solaris* 10, Microsoft* Windows 2003 Server (32 or 64-bit), VMWare* ESX, Windows* 2008 R2

9 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.s. For more information, visit www.intel.com/go/inteltxt.

Share with Colleagues

0113/GL/PDF-USA 328393-001

Sponsors of Tomorrow.™