SOLUTION BRIEF
CLOUD COMPUTING

Security in the Cloud

Intel® Xeon® Processor E5-4600/2600/2400/1600

Intel® Technologies Enable More Secure Business Computing in the Cloud

Would you like to begin transforming your data center into a flexible, high-density private cloud that enables far more dynamic and automated control of systems and workloads? Would you like to use public cloud services to add capacity during peak demands? Like many businesses who are using the cloud, you'll find the efficiency, flexibility, and financial benefits of cloud strategies can benefit your business, yet you probably share the concerns of many other IT decision makers: namely, how can the security and privacy of sensitive data be ensured if it is being stored or processed on shared infrastructure, especially if that infrastructure is owned and managed by a third-party cloud provider?

Intel has developed technologies to help improve cloud security, and has been collaborating with leading hardware and software solution providers to enable more comprehensive and integrated solutions that can make it easier for businesses to adopt cloud computing. These technologies lay the foundation needed for:

- **Strong Data Protection.** Encryption can be implemented pervasively to protect data both at rest and in transit, without compromising performance or driving up costs. Intel technology and open source contributions for protecting data include Intel® Advanced Encryption Standard New Instructions[1] (Intel® AES-NI) and the optimizations Intel has implemented with OpenSSL.* By accelerating both data encryption, as well as the initiation of secure sessions and transfer of the bulk data, you can better utilize data center resources and implement pervasive data protection without compromising the experience of your employees, customers, and partners.
- **Trusted Infrastructure.** Hardware can verify the integrity of key platform software to help protect against sophisticated launch time attacks and establish a control point for enhancing the security of virtualized workloads. Selected applications can be constrained to run only on these trusted pools of virtualized resources, to help protect critical assets more effectively. Trusted infrastructure technologies and software products include Intel® Trusted Execution Technology[2] (Intel® TXT), which establishes a server's "root of trust" to help assure system integrity, and Intel® Identity Protection Technology[3] (Intel® IPT) which validates legitimate users with two-factor authentication that executes directly on the PC. In addition, Intel® Expressway Service Gateway (Intel® ESG) is a highly scalable software appliance that provides enforcement points at a network's edge. It securely and reliably connects on-premise applications to external cloud providers, external business partners or employees, authenticating API requests against existing enterprise identity and access management systems.
- **Security and Compliance Verification.** The security environment of a cloud infrastructure can be more thoroughly monitored, assessed, and documented. With appropriate third-party applications, compliance can be verified dynamically to mitigate risk through unified, policy-based auditing, logging, and reporting. With these capabilities integrated into the foundation of your chosen cloud solution, you can take advantage of the extraordinary benefits of cloud computing, confident that your data is safer and more secure and your business is well-protected against today's increasingly sophisticated attacks.

New Risks Require New Solutions

New security issues arise in cloud environments while more traditional security issues continue to evolve. In a public or virtual private cloud, your data resides on a server physically controlled and managed by someone else, so traditional security models aimed at protecting the perimeter of the organization are no longer sufficient. Cloud computing shares some of these security dynamics with today's cross-business and cross-supply chain collaboration models, and it is vitally important to implement appropriate solutions for controlling access, detecting malware and intrusion, and protecting data in these environments.

The growth of cloud computing has simply elevated these new security challenges, while at the same time, security issues continue to grow more and more complex. Attacks used to come primarily from individual hackers who were merely looking for personal fame or a fast profit. However, many of today's attacks are more stealthy, persistent, organized, and sophisticated. They target specific types of data and are designed to achieve and retain control of assets for financial gain. Regulatory environments are also changing. Businesses face increasing requirements for compliance, auditing, reporting, privacy protection, and indemnification, and the risks and costs of non-compliance are large and growing.

To address these challenges, Intel has introduced a number of technologies in the Intel® Xeon® processor E5 family that help to enable comprehensive and verifiable security and compliance in cloud environments. With these technologies, Intel is providing a foundation to make cloud deployments suitable for increasingly sensitive and vital workloads.

Business Requirement	Intel Technology	Description	Business Benefit
Strong Data Security	Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)[1]	Reduces performance overhead to enable the pervasive use of encryption.	Better protects the privacy and integrity of data, both at rest and as it moves through the cloud.
	Intel's advanced OpenSSL contributions: Intel's RSAX – Accelerates SSL session initiation time. Intel's Function Stitching – Interleaves instructions for the encryption and authentication processes of data transfer and executes them simultaneously for improved performance.	Accelerates data encryption, as well as the initiation of secure sessions and transfer of the bulk data.	Better utilize data center resources and implement pervasive data protection without compromising user productivity or efficiency.
Trusted Infrastructure	Intel® Trusted Execution Technology (Intel® TXT)[2]	Can block launch if hypervisor or host software doesn't match "known good states." Provides integrity-checking data that can be used for monitoring and verifying the platform trustworthiness.	Enables trusted infrastructure and trusted compute pools to be established and maintained, and protects against new launch-time attacks.
	Intel® Virtualization Technology[4] (Intel® VT)	Implements core virtualization processes in silicon to accelerate performance and improve work-load isolation.	Helps to ensure that data and applications are safely and securely isolated, even when residing on shared infrastructure.
	Intel® VT FlexMigration (a part of Intel VT)	Enables migration of running virtual machines among current and future Intel® Xeon® processor-based servers.	In combination with Intel TXT, simplifies the migration of running applications onto new, trusted infrastructure.
	Intel® Identity Protection Technology (Intel IPT) *(on PCs and Ultrabooks™ with 3rd gen Intel® Core™ i5 vPro™ and i7 vPro™ processors only)*	Provides two-factor authentication that executes directly on the PC.	Gives IT managers more visibility into security at the endpoint and in the cloud, and aids in making risk and access decisions.
Security and Compliance Verification	Intel TXT (integrated with third-party SIEM and GRC security solutions)	Provides hardware-based mechanisms that support monitoring of cloud security environments, with integrated auditing, logging, and reporting.	Enables unified, policy-based verification of the security and compliance of the platform environment in clouds.

Protecting Your Data

Encryption is one of the most effective technologies available for protecting valuable information, but encrypting and decrypting data has traditionally required substantial computing power that can increase costs and slow down the performance of business applications. Intel® Advanced Encryption Standards New Instructions[1] (Intel® AES-NI) dramatically reduces this performance overhead by introducing new instructions to accelerate the compute-intensive steps of the AES algorithms.

Because the Intel AES-NI hardware instructions also significantly reduce vulnerability to side-channel attacks, encryption is not just faster, but stronger, as well, as these types of attacks use software agents to analyze how a system processes data and searches for cache and memory access patterns to help deduce elements of the cryptographic processing—and therefore make it easier to "crack." Intel AES-NI helps hide critical elements such as table lookups, making it harder to determine what elements of crypto processing are happening. The result is that with Intel AES-NI, your data is not only encrypted faster, but is better protected, too.

In addition, Intel has worked closely with OpenSSL,* an open-source, multi-platform security library that can be used to secure web transactions, to optimize implementations of cryptographic communications functions on Intel architecture. Software's use of the OpenSSL library produces impressive performance gains along with the hardware acceleration of Intel AES-NI. In fact, Intel AES-NI coupled with Intel's optimization of OpenSSL algorithms can accelerate AES encryption performance by over 8x, and speed decryption by an incredible 33x versus software-only approaches.[5,6]

Since Intel AES-NI is built into the processor's instruction set, it eliminates the need for costly security appliances or add-on cards. Businesses can implement encryption simply, cost-effectively, and pervasively to protect business data. Intel AES-NI is supported by many of today's leading software vendors to provide comprehensive data protection.

- **Protection for Data in Transit.** Secure banking transactions such as online bill pay, e-mail services like Gmail and Hotmail, and secure video streaming require complex processing, resulting in a stiff performance penalty and often causing security to be sacrificed to maintain responsiveness. Intel recognized that these operations have the potential for a high degree of parallelism and developed innovative software approaches to take advantage of that. Microsoft Windows Server* 2008 R2 with Internet Information Services and Red Hat Linux* openSSL support Intel AES-NI. Intel's RSAX optimization to the OpenSSL RSA algorithm accelerates performance up to 1.55x.[5] This also improves the experience for users, while increasing the number of simultaneous secure sessions your Intel® Xeon® processor-based server can handle.[6]
- **Protection for Data at Rest.** Just because data is not in transit, does not mean it's secure. Encryption for data-at-rest on hard disks helps protect data from loss and theft, while facilitating decommissioning and repair. For example, if a damaged hard drive has unencrypted confidential information on it, sending it out for warranty repair could potentially expose its data. Microsoft, Checkpoint, McAfee, and PGP/Symantec support Intel AES-NI to accelerate full-disk encryption.
- **Protection for Data in Enterprise Applications.** Oracle* and IBM* DB2* support Intel AES-NI in database tablespace encryption, and SAP* and Red Hat* JBoss* Enterprise Application Platform support Intel AES-NI in business operations. Hypervisor providers, such as Microsoft, VMware, Citrix, Oracle, and the open-source based hypervisors Xen and KVM, support AES-NI running in their guest applications.

By taking advantage of the industry-leading solutions provided by these and other vendors supporting Intel AES-NI and OpenSSL optimizations, you can protect your data more effectively and implement cloud computing with greater confidence to deliver higher value to your business.

Securing Your Infrastructure

Migrating applications and workloads remains a manual process in many IT environments. Cloud computing can provide greater automation for moving running applications within and across data centers. This can make it easier to meet strict service-level agreements through load-balancing, failover, zero-downtime maintenance, and disaster recovery. However, if your data and applications are going to be moved, you must be certain they are moved into a secure infrastructure.

Intel® Trusted Execution Technology (Intel® TXT) addresses this requirement in two key ways.

- **Protection against Launch-time Attacks.** Intel TXT ensures that the systems and software are able to launch only if they match a "known good state." This protects against new launch-time attacks that could otherwise compromise the security environment of virtual infrastructure.
- **Accurate Information for Verifying Security.** Intel TXT provides information that can be used to monitor and assess the security environment. Software solution providers such as HyTrust, Parallels, and VMware are using the information generated by Intel TXT to help their customers establish and maintain "trusted compute pools," so sensitive or business-critical workloads can be deployed—and migrated—with confidence.

Intel® Virtualization Technology (Intel® VT) adds to these advantages. It helps to protect the integrity and confidentiality of data and applications by maintaining strong isolation among multiple workloads, even when they are running on shared infrastructure. Intel VT includes Intel® VT FlexMigration, which enables live migration of running applications among multiple generations of Intel Xeon processor-based servers. Combined with Intel TXT, this can allow you to move your existing applications onto new, trusted infrastructure simply, reliably, and without downtime.

Intel® Identity Protection Technology (Intel® IPT)[7] builds on security by further establishing trust to protect data at endpoints. Intel® IPT validates legitimate users with two-factor authentication that executes directly on the PC, generating one-time passwords every 30 seconds from a tamper-proof, embedded token that operates in isolation from the operating system. There is also a certificate embedded in the chipset for hardware-based security that eliminates the additional cost of supporting traditional smart card or token storage options. Multiple authentication mechanisms supported by hardware provide IT managers with more visibility into security at the endpoint and in the cloud, which is useful in making risk and access decisions.

Finally, it is crucial to protect applications as they are exposed to the cloud. Intel® Expressway Service Gateway (Intel® ESG) provides software enforcement points that sit at a network's edge by authenticating application programming interface (API) requests against existing enterprise identity and access management systems. With the API-level control of Intel ESG, you gain a measure of protection for your departmental and edge system infrastructure, and reduce the risk of content-born attacks on applications. As the number of social and enterprise APIs continue to explode, the Intel ESG helps you to scale consumption of cloud application services.

Verifying Security and Compliance in Cloud Environments

It's not enough to know your cloud infrastructure has the technology to provide a safe and secure environment for your data and applications. You need to be able to audit the security level of that environment to identify risks and verify compliance dynamically, whether your data resides in your own data center or in a public cloud infrastructure.

Intel TXT provides the data needed for enhanced security and compliance auditing of virtual environments, and Intel is collaborating with leading security solution providers, such as RSA, to enable complete solutions.

- Specialized security management tools monitor and analyze the data provided by Intel TXT to provide visibility into the events and conditions that affect security. With these tools, you can verify compliance, identify risks, and respond quickly to mitigate them.
- Security Information and Event Management (SIEM) and Governance, Risk, and Compliance (GRC) software creates a general security control point by aggregating the event and information reports from various security applications and activities—including Intel TXT. Aggregated information can be reported into a dashboard, indicating where security concerns, possible breaches, and gaps may reside. GRC software can also query infrastructure to make sure policies are active and in place. Administrators can use this information to create new or refine existing policies for the policy engine.

Making the Cloud Work for You

Intel Xeon processor-based servers provide the foundation for the industry's broadest ecosystem of cloud solutions. Intel AES-NI, Intel TXT, and Intel VT are built into the latest Intel Xeon processor E5 family to help address the security challenges inherent in cloud computing and make it easier for businesses to adopt cloud solutions.

At the endpoint, PCs with Intel® vPro™ technology[8] integrate hardware-based, built-in features your IT personnel need to be proactive and responsive, and to keep your data safe. The technology is embedded in the hardware, so it is out of view and beyond the reach of malware, and able to deliver unprecedented PC security. This means you're better protected in the office and the data center.

These technologies are a part of Intel's broader efforts to meet the challenges and reduce the risks that IT architects and managers face as the industry shifts toward cloud computing.

Intel works directly with enterprise IT organizations and service providers throughout the world, and is a technical advisor to the Open Data Center Alliance, an independent organization of leading global IT managers. The Alliance is defining a roadmap of the highest priority usage models for cloud and next-generation data centers and is laying out the requirements to support them with multi-vendor, interoperable solutions that embrace standards. Intel uses this information to deliver products and technologies that meet these usage model requirements. Intel then engages and rallies leading systems and solution providers to deliver complementary products and solutions and to enable simpler, lower-risk deployment through reference architectures and best practices developed through the Intel® Cloud Builders program.

From building a cloud to finding a cloud services provider, Intel strives to make the cloud work for you. Intel® Cloud Finder is an online resource that can simplify and shorten the selection process for cloud infrastructure service providers that match your requirements. At the highest level, you need to know if the cloud provider can provide evidence of data and platform protections for the services they provide. With Intel Cloud Finder, you can select cloud service providers based on a set of detailed criteria categorized by security, usability, quality, availability, technology, and business requirements. A search tool helps you identify which providers offer the services that are most important for your organization. Once you are comfortable that your criteria can be met, you can establish measurable, enforceable SLAs to provide ongoing verification.

Moving Forward with Confidence

Businesses have already begun integrating cloud computing into their IT strategies, and the adoption of cloud solutions will continue to accelerate in the months and years ahead. Intel is at the heart of this evolution and provides industry-leading technology advancements on the world's most widely deployed server architecture. With Intel as the foundation of your cloud solutions, you can be confident that your data is safer and more secure, so you can move into the cloud with greater confidence.

Learn More

For more information about Intel cloud computing resources,
visit: **www.intel.com/go/cloud**

For more information about Intel security technologies,
visit: **www.intel.com/technology/security/**

For more information about Intel TXT,
visit: **www.intel.com/technology/malwarereduction/index.htm**

For more information about Intel AES-NI,
visit: **www.intel.com/technology/dataprotection/index.htm**

For more information about which software providers support Intel AES-NI and Intel's OpenSSL optimizations, visit: **http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/aes-ni-ecosystem-update.html**

For more information about Intel Virtualization Technology,
visit: **www.intel.com/technology/virtualization/server/**

For more information about Intel vPro technology,
visit: **www.intel.com/go/vpro**

For more information about Intel Identity Protection Technology,
visit: **http://www.intel.com/content/www/us/en/architecture-and-technology/identity-protection/identity-protection-technology-general.html**

For more information about Open Data Center Alliance,
visit: **www.opendatacenteralliance.org**

For more information about Intel Cloud Finder,
visit: **www.intelcloudfinder.com**

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. For more information go to **http://www.intel.com/performance**

1. 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® 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://software.intel.com/en-us/articles/intel-advancedencryption-standard-instructions-aes-ni/**
2. No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer system 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 **http://www.intel.com/technology/security**
3. No system can provide absolute security under all conditions. Requires an Intel IPT enabled system, including a 2nd generation Intel Core processor, enabled chipset, firmware, and software. Available only on participating websites. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit **ipt.intel.com**.
4. Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, 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**
5. Intel's cryptographic optimizations speed up the handshake and the bulk data transfer phases of OpenSSL. The performance gains were measured on a dual Intel® Xeon® Processor X5680 [15] system, which consists of two 6-core Intel® processors based on the 32-nm microarchitecture, supporting the Intel® AES New Instructions (Intel® AES-NI) extension. We measured the performance gains for OpenSSL using the built-in speed test, as well as at the system-level running an Apache web server sending HTTP over SSL to clients on a network.
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. Configurations:OpenSSL versions 1.0.0d and a snapshot of the upcoming 1.0.1 version containing all of Intel□s cryptographic optimizations; Apache version httpd-2.2.17; Intel® Xeon® Processor X5680 EP with two processors (3.3 GHz, 12M Cache, 6.40 GT/s Intel® QPI). For more information go to **http://www.intel.com/performance**
7. No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd 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 **ipt.intel.com**.
8. PCs with Intel® vPro™ processor technology include Intel® Active Management Technology (Intel® AMT). Intel Active Management Technology requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. For more information, see **http://www.intel.com/technology/manage/iamt/**.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site www.intel.com/.

*Other names and brands may be claimed as the property of others. 1012/JRR/HBD/PDF 327990-001US