

Planning Guide

Cloud Security

Seven Steps for Building Security in the Cloud from the Ground Up

Why you should read this document:

This guide provides practical information to help you integrate security planning into your cloud computing initiatives and:

- Makes suggestions and recommendations for strengthening data and platform protection in cloud implementations.
- Provides guidance on encryption to protect data.
- Describes the importance of a trusted foundation to secure platform and infrastructure.
- Explains how to build higher assurance into auditing to strengthen compliance.
- Discusses extending trust across federated clouds.

Planning Guide Cloud Security

Seven Steps for Building Security in the Cloud
from the Ground Up

SEPTEMBER 2011



Contents

- 3 Security in the Cloud:
What It Is (and What It Isn't)
- 5 Security Challenges for Cloud Environments
- 6 Step 1: Start Security Planning Early
- 10 Step 2: Identify Vulnerabilities for Your
Selected Service(s)
- 12 Step 3: Four Things an IT Manager Can Do
To Mitigate Security Vulnerabilities
- 13 Step 4: Protect Data—in Motion, in Process,
and at Rest
- 15 Step 5: Secure Your Platform
- 16 Step 6: Extend Trust across Federated Clouds
- 17 Step 7: Choose the Right Cloud Service Provider
- 19 Intel Resources for Learning More

Cloud Security: What It Is (and What It Isn't)

The cloud seems to be on everyone's mind these days. If you've been considering how to make the leap to cloud computing, you've also had to start thinking about how to extend security to this new technology environment. Despite potential savings in infrastructure costs and improved business flexibility, security is still the number-one barrier to implementing cloud initiatives for many companies.

Security challenges in the cloud are familiar to any IT manager—loss of data, threats to the infrastructure, and compliance risk. What's new is the way these threats play out in a cloud environment.

Cloud Security Is ...

- The response to a familiar set of security challenges that manifest differently in the cloud. New technologies and fuzzier boundaries surrounding the data center require a different approach.
- A set of policies, technologies, and controls designed to protect data and infrastructure from attack and enable regulatory compliance.
- Layered technologies that create a durable security net or grid. Security is more effective when layered at each level of the stack and integrated into a common management framework.
- The joint responsibility of your organization and its cloud provider(s). Depending on the cloud delivery model and services you deploy, responsibility for security comes from both parties.

Cloud Security Isn't ...

- A one-size-fits-all solution that can protect all your IT assets. In addition to different cloud delivery models, the cloud services you deploy will most likely require more than one approach to security.
- A closed-perimeter approach or a "fill-the-gap" measure. Organizations can no longer rely on firewalls as a single point of control, and cobbling together security solutions to protect a single vulnerability may leave you open in places you don't suspect.
- Something you can assume is provided at the level you require by your cloud service providers. Make sure you spell out and can verify what you require.

Cloud computing security is a broad topic with hundreds of considerations—from protecting hardware and platform technologies in the data center to enabling regulatory compliance and defending cloud access through different end-point devices. The focus of this planning guide is to provide you with suggestions and

recommendations for strengthening data and platform protection in your cloud implementations. The remainder of this guide walks you through seven key steps that will help you plan your cloud security from the ground up.

Intel Experience with Cloud Security

Much of the information in this document comes from our experience working with cloud providers, virtualization and security solution vendors, OEMs, and large enterprise customers—as well as the experience of our own Intel IT building and deploying cloud technology.

Intel IT has embarked on a radical five-year redesign of the Intel information security architecture. This redesign moves us away from a traditional binary trust model to a multitiered trust model with a particular emphasis on data and people as the new perimeter. This new architecture is designed to support key initiatives such as cloud computing as well as IT consumerization.

Our Intel Cloud Builders¹ program continues to yield in-depth guidance that you can use, including reference architectures, education, and a forum for discussion of technical issues. In addition, Intel's strategic partnership with McAfee² provides the foundation for a holistic security and compliance management platform to ensure overall integrity of the cloud infrastructure.

Three Major Trends That Impact Cloud Security

To manage cloud security in today's world, you need a solution that helps you address threats to enterprise data and infrastructure, including the major trends you are up against.

- **Changing attackers and threats:**
Threats are no longer the purview of isolated hackers looking for personal fame. More and more, organized crime is driving well-resourced, sophisticated, targeted attacks for financial gain.
- **Evolving architecture technologies:**
With the growth of virtualization, perimeters and their controls within the data center are in flux, and data is no longer easily constrained or physically isolated and protected.
- **Dynamic and challenging regulatory environment:**
Organizations—and their IT departments—face ongoing burdens of legal and regulatory compliance with increasingly prescriptive demands and the high penalties for noncompliance or breaches. Examples of regulations include Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and the Health Insurance Portability and Accountability Act (HIPAA).

1 [Intel Cloud Builders](#) is a cross-industry initiative to help enterprises, telecommunications companies, and service providers build, enhance, and operate secure cloud infrastructures.

2 McAfee is a wholly owned subsidiary of Intel.

Security Challenges for Cloud Environments

The Cloud Security Alliance, an industry group promoting cloud computing security best practices and standards, has identified seven areas of security risk.³ Three of these apply directly to our focus on protecting data and platform: multitenancy, data loss, and unknown risk.

Multitenancy and shared technology issues. Clouds deliver scalable services that provide computing power for multiple tenants, whether those tenants are business groups from the same company or independent organizations. That means shared infrastructure—CPU caches, graphics processing units (GPUs), disk partitions, memory, and other components—that was never designed for strong compartmentalization. Even with a virtualization hypervisor to mediate access between guest operating systems and physical resources, there is concern that attackers can gain unauthorized access and control of your underlying platform with software-only isolation mechanisms. Potential compromise of the hypervisor layer can in turn lead to a potential compromise of all the shared physical resources of the server that it controls, including memory and data as well as other virtual machines (VMs) on that server.

Experience at Intel found that virtualization brings with it an aggregation of risks to the enterprise when consolidating application components and services of varying risk profiles onto a single physical server platform. This is a key limiter faced by most IT organizations in achieving their virtualization goals—and subsequently in moving workloads to the cloud.

Data loss or leakage. Protecting data can be a headache because of the number of ways it can be compromised. Some data—customer, employee, or financial data, for example—should be protected from unauthorized users. But data can also be maliciously deleted, altered, or unlinked from its larger context. Loss of data can damage your company's brand and reputation, affect customer and employee trust, and have regulatory compliance or competitive consequences.

Unknown risk. Releasing control of your data to a cloud service provider has important security ramifications. Without clearly understanding the service provider's security practices, your company may be open to hidden vulnerabilities and risks. Also, the complexity of cloud environments may make it tempting for IT managers to cobble together security measures. Unfortunately, that same complexity and the relatively new concept of cloud computing and related technologies make it difficult to consider the full ramifications of any change, and you may be leaving your cloud open to new or still undiscovered vulnerabilities.

Intel and Best Practices in Cloud Security

Intel is a member of several industry groups that develop standards and best practices for security and cloud computing, such as the Cloud Security Alliance (CSA). For example, Intel is the nonvoting technical advisor to the Open Data Center Alliance (ODCA), an independent IT consortium comprised of global IT leaders who have come together to provide a unified customer vision for long-term data center requirements represented by more than 280 member companies. ODCA released a roadmap of hardware and software requirements in June 2011⁴ with the goal of promoting more open and interoperable cloud and data center solutions. Intel is also an active participant in the Trusted Computing Group (TCG), formed to develop and promote open, vendor-neutral standards for trusted computing building blocks; and the Distributed Management Task Force (DMTF), a global organization leading the development, adoption, and promotion of interoperable management initiatives and standards.

⁴ Information about the Open Data Center Alliance roadmap can be found at opendatacenteralliance.org/publications.

³ *Top Threats to Cloud Computing, v1.0*. Cloud Security Alliance (2010). <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf> (PDF)

Step 1: Start Security Planning Early

Your security profile in the cloud is defined by what your organization needs and the workloads you plan to move to the cloud. The best way to approach cloud security is to integrate it with your overall cloud planning early in the process. That way you can use a threat-based approach to planning for deployments of your specific workload(s), the security requirements, and the specific cloud delivery model and architecture.

As you embark on your own cloud initiatives, here are a few of the considerations that will affect your risk profile in the cloud.

- Are your physical compute resources located on-premises or off-premises?
- What types of assets, resources, and information will be managed?
- Who manages them and how?
- Which controls are selected, and how are they integrated into the overall cloud architecture?
- What compliance issues do you face?

The Fundamentals

The first step in planning security for your proposed cloud environment is to think about the fundamentals: data and platform. Use the following as a checklist for what you need to know (at least at a high level) about the specific deployment you're planning. The idea is to understand your risk tolerance, identify the best deployment models for your specific needs based on security and compliance considerations, and detect potential exposure points for sensitive data and processes. With this information, you will be in a better position to understand what your organization really needs.

Task	Purpose	Additional Considerations
Identify the business priorities for moving the specific workload(s) to the cloud.	You can more effectively weigh security concerns once you've defined the business context for what you hope to achieve by moving workloads to the cloud.	<ul style="list-style-type: none">▪ What drivers make cloud technology a good option for this workload?▪ Do you need to:<ul style="list-style-type: none">◦ Reduce operational costs?◦ Scale seasonally?◦ Support remote or mobile workers?
Evaluate the sensitivity of the asset(s).	This helps you understand the importance of the data or function. You can make this evaluation as a rough assessment or follow a specific valuation process.	<ul style="list-style-type: none">▪ What harm would result if the asset was compromised?

Task	Purpose	Additional Considerations
<p>Map the security workload to the appropriate cloud delivery model and hosting models under consideration.</p>	<p>Now that you understand the importance of your asset, you can evaluate the risks associated with various deployment models.</p>	<ul style="list-style-type: none"> ▪ Are you considering a private, public, or hybrid cloud delivery model? ▪ For a private cloud, will your deployment be: <ul style="list-style-type: none"> ◦ On-premises? ◦ Off-premises with a dedicated or shared infrastructure? ▪ For hybrid models, where will the various components, functions, and data reside? ▪ How will you mitigate risk within the cloud delivery model?
<p>Determine whether the available services are capable of meeting your requirements for handling data, especially for compliance purposes.</p>	<p>At this point, you need to understand your risk tolerance for the workload. If you have a cloud service provider in mind, you can conduct a more detailed risk assessment.</p>	<ul style="list-style-type: none"> ▪ What are the specific requirements for handling regulated data?
<p>Map the data flow, especially for public or hybrid cloud providers.</p>	<p>You need to know how data moves in and out of the cloud. For specific deployment options, you should understand how data will flow between your organization, the cloud services, and any customers (or other areas).</p>	<ul style="list-style-type: none"> ▪ Can the provider continue to deliver protection as the workload continues to evolve?

Cloud Delivery Models at a Glance

Cloud delivery models used by enterprise organizations generally fall into three types, each with its own unique advantages and disadvantages in terms of security.

Model	Description	Advantages and Disadvantages
Private	<ul style="list-style-type: none">▪ An internal infrastructure that leverages virtualization technology for the sole use of an enterprise behind the firewall▪ Can be managed by the organization or by a third party▪ Located on-premises or off-premises on shared or dedicated infrastructure	<ul style="list-style-type: none">▪ Most control over data and platform▪ Potential for multitenancy of business units to cause compliance and security risk▪ May lack bursting capabilities when additional performance or capacity is required
Public	<ul style="list-style-type: none">▪ Resources dynamically provisioned over the Internet, via web services, or from a third-party provider▪ Located off-premises, typically on a shared (multitenancy) infrastructure▪ May offer dedicated infrastructure as a response to growing security concerns	<ul style="list-style-type: none">▪ Potential for greater cost savings if infrastructure owned and managed by public provider▪ Loss of control of data and platform▪ Potential for multitenancy with other organizations to cause security risk▪ Third-party security controls possibly not transparent (and may cause unknown risks)
Hybrid	<ul style="list-style-type: none">▪ A combination of private and public cloud services▪ Organizations that often maintain mission-critical services privately with the ability to cloud burst for additional capacity or add selective cloud services for specific purposes▪ Located on-premises and off-premises depending on the architecture and specific services	<ul style="list-style-type: none">▪ Often a compromise:<ul style="list-style-type: none">◦ Retention of control over the most mission-critical data, but relinquishing that control when additional capacity or scale is required during peak or seasonal periods◦ May involve retention of control for mission-critical data at all times while taking advantage of public cloud provider services for less sensitive areas▪ Potential for complexity to cause unknown vulnerabilities (and unknown risks)

Intel Vision for Cloud Security

One key element of the Intel vision for cloud security is to build in balanced controls instead of designing an environment based primarily on preventive controls. For example, the architecture is designed to dynamically adjust a user's access privilege as the level of risk changes, taking into account factors such as location and type of device. This new approach is both proactive to minimize occurrences and reactive to minimize damage if a breach occurs.

Intel IT uses a hybrid approach that leads with a private cloud as the core strategy. In part based on security concerns, we selectively use a public cloud for nondifferentiated IT services such as staffing, benefits, expense, stock, and travel. We host the vast majority of our applications in our private cloud, such as enterprise, user profile management, productivity, and collaboration applications. We expect that more of our applications could burst to public clouds over time as security and vendor service level agreements (SLAs) improve and overall costs, including transition costs, become more favorable.

Step 2: Identify Vulnerabilities for Your Selected Service(s)

Cloud computing, which depends heavily on virtualization to realize operational savings and efficiencies, has elastic boundaries, and potentially pushes out the perimeter of the enterprise and security controls far beyond the data center.

It's important to recognize that the traditional border behind which data and platform are constrained and protected—typically physical separation and isolation—is no longer viable for dynamic cloud

architecture models. It's also important to understand that while a fill-the-gap approach may seem to work on a particular vulnerability, it may expose unknown vulnerabilities in other areas.

Regardless of the cloud delivery model you choose, your best approach is to review the specific service architecture, and then layer technologies to develop a strong security net that protects data, applications and platform, and network at all levels.



Spotlight on Cloud Service Architecture⁵

There are three types of cloud services: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS).

IaaS

- Delivers computer infrastructure as a utility service, typically in a virtualized environment
- Provides enormous potential for extensibility and scale

PaaS

- Delivers a platform or solution stack on a cloud infrastructure
- Sits on top of the IaaS architecture and integrates with development and middleware capabilities as well as database, messaging, and queuing functions

SaaS

- Delivers applications over the Internet or intranet via a cloud infrastructure
- Built on underlying IaaS and PaaS layers

⁵ Security Guidance for Critical Areas of Focus in Cloud Computing, v2.1. Cloud Security Alliance (2009). <https://cloudsecurityalliance.org/csaguide.pdf> (PDF)

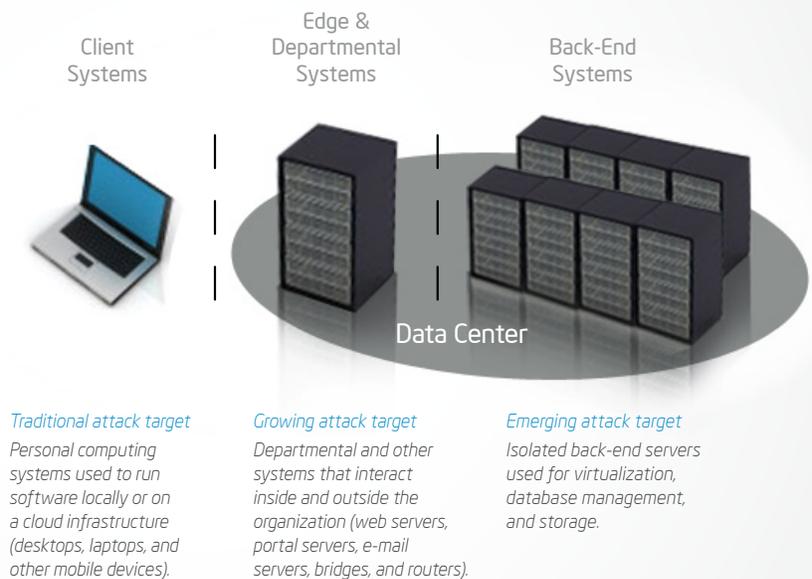
The Cloud Security Net—Build It from the Ground Up

Because the model for your cloud services may be very different from other organizations—and indeed may evolve and change over time—Intel recommends that, in addition to security software solutions and application features, you should strengthen your security net by protecting data and platform at the most basic level—the system hardware. This best practice is built into Intel’s own private cloud infrastructure.⁶

The following illustration shows how protection at the hardware level can enable security deeper in the data center. Compute resources complement your perimeter controls, enable more advanced security and compliance capabilities in existing solutions, and provide needed protection even below the hypervisor—an area of emerging threat.

Physical Layers at Risk in the Enterprise

The dynamic perimeter of cloud computing can expose edge systems to people and applications more than most other elements of the data center architectures—offering more opportunities for compromise. Attacks of server infrastructure at the deepest levels are an emerging area of risk and increasingly target the hypervisor, firmware, and BIOS. The attackers are professionals—more sophisticated, determined, and better resourced. The potential for harm from a single attack in either of these two areas can be devastating.



6 An Enterprise Private Cloud Architecture and Implementation Roadmap. IT@Intel (2010). intel.com/content/www/us/en/cloud-computing/cloud-computing-private-cloud-roadmap-paper.html (PDF)

Step 3: Four Things an IT Manager Can Do To Mitigate Security Vulnerabilities

With protection at the hardware level, you can build trust and compliance into your data center. This means you can:

- Provide the foundation for a more powerful layered security net of solutions and software features
- Put more granular controls closer to where your data lives and critical platform services
- Trust that the physical and virtual infrastructure provisioning your workloads is reliable
- Trust where your servers are located
- Control where the VMs are distributed
- Complement your audit and compliance requirements (for the business unit tenants in your private cloud or as a tenant in a public cloud)
- Protect confidential data and meet compliance requirements

Intel IT is enabling new ways to provide the foundation for cloud controls that can secure data and workloads. We are adding new levels of visibility into what is running and who is running it so you can trust that the infrastructure is reliable and can support compliance. As Intel continues to move to the cloud, we are starting to increase the security level of our environment through greater understanding of what is running in the environment; what it should look like when it is “normal”—not compromised; strengthened data protection; and secure access.

Intel recommends prioritizing your security investment through a risk assessment to determine the order and timing for building this level of trust and compliance into your data center in four areas.

- Encrypt to protect data.
- Establish a trusted foundation to secure the platform and the infrastructure.
- Build higher assurance into auditing to strengthen compliance.
- Establish and verify identities before you federate by controlling access to trusted clients from trusted systems.

The remainder of this planning guide will look at how advanced server technologies—in particular, Intel® technologies—can help you build trust and compliance into your data center and set the foundation for cloud security.

Step 4: Protect Data— in Motion, in Process, and at Rest

Encryption is an effective, well-established way to protect sensitive data because even if information is lost, it remains unusable. Encryption is critically important for protecting data covered by regulations and standards such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), and Payment Card Industry (PCI). Increasingly, these and other regulations are encouraging—and specifying—encryption in certain usage scenarios. And the penalties for noncompliance are stiffer than ever.

There are a number of ways to perform encryption, but typically it comes with a cost—what is often referred to as a performance tax. As an IT manager, you must be able to justify the trade-off in performance with the requirement for secure data.



What Types of Data Should You Encrypt?

Data in motion

- Data in flight over networks (Internet, e-commerce, mobile devices, automated teller machines, and so on)
- Data that uses protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPsec), Hypertext Transfer Protocol Secure (HTTPS), FTP, and Secure Shell (SSH)

Data in process

- Transactional data in real time, such as encrypted fields, records, rows, or column data in a database

Data at rest

- Files on computers, servers, and removable media
- Data stored using full disk encryption (FDE) and application-level models

Encrypt without the Performance Tax

What if you didn't have to make a performance trade-off? Intel Advanced Encryption Standard⁷ New Instructions (Intel AES-NI) is a set of seven new instructions in the Intel Xeon® processor 5600 series that eliminate the performance tax by speeding up parts of the AES algorithm encryption/decryption execution. It makes encryption practical, stronger, and more efficient for data in motion, in process, and at rest.

Benefits of these hardware-based instruction set extensions include the following:

- Improved performance. Intel AES-NI can accelerate performance 3 to 10 times faster than a software-only AES solution.
- Improved security. The new instructions help address recently discovered side-channel attacks on AES. Intel AES-NI instructions perform the decryption and encryption more completely at the hardware level without the need for software lookup tables that could be susceptible to snooping. Therefore using AES-NI can lower the risk of side-channel attacks.
- Multiple usage scenarios. Intel AES-NI can be used in any application that uses AES, including network, disk, and file encryption solutions.

⁷ The Advanced Encryption Standard (AES) is a popular encryption standard first adopted by the U.S. government in 2001. It is generally displacing the older, less secure Data Encryption Standard (DES) encryption algorithm and is now widely used to protect network traffic, personal data, and corporate IT infrastructures.

Step 5: Secure Your Platform

Rootkit attacks are increasing. They are difficult to detect with traditional antivirus products and use various methods to remain undetected. Rootkit attacks infect system components such as hypervisors and operating systems, and the malware can operate in the background and spread throughout a cloud environment, causing increasing damage over time.

The best way to secure your platform is to enable a trusted foundation—starting with a root of trust at the platform level and extending the chain of trust through measured firmware, BIOS, and hypervisor virtualization layers. A root of trust hardens the platform against attack and is extremely difficult to defeat or subvert and substantially reduces the security risks of using a remote or virtualized infrastructure. It enables a more secure platform for adding tenants and workloads. Essentially you build protection into your hardware to protect your software.

A root of trust helps ensure system integrity within each system. Integrity checking is considered a key capability for software, platform, and infrastructure security.⁸ Intel Trusted Execution Technology (Intel TXT) checks hypervisor integrity at start-up by measuring the code of the hypervisor and comparing it to a known good value. Launch is blocked if the measurements do not match.

The root of trust enables a trusted foundation within your cloud environment so you can:

- **Specify trusted server pools.** You can make decisions about how much to expose your data and workload based on whether a trusted pool is established. The most sensitive workloads should always use a trusted pool.

- **Prove host software is good.** Although the chain of trust is a hardware-based mechanism, you can use the integrity-checking data with Governance, Risk Management, and Compliance (GRC) or security information and event manager (SIEM) dashboards for audit purposes.
- **Respond quickly to attack and minimize damage.** Detect attacks more quickly, contain the spread of malware, and reduce the need to rebuild hypervisors if a compromise is detected.

About Intel® TXT

Intel® Trusted Execution Technology (Intel TXT) protects against malware, key stealth attacks, and other threats by:

- Establishing a root of trust
- Providing a launch environment signature to enable trusted software launch and execution
- Providing the trust foundation so that policy engines can restrict or allow virtual machine (VM) and data migration based on platform security profiles
- Providing the trust foundation to enable environment monitoring for auditing function tied to a root of trust
- Enabling an IT manager to verify that the specific physical machine in the cloud is running the expected operating system or hypervisor

⁸ *Evolution of Integrity Checking with Intel® Trusted Execution Technology: An Intel Perspective*. IT@Intel (2010). [intel.com/content/www/us/en/pc-security/intel-it-security-trusted-execution-technology-paper.html](https://www.intel.com/content/www/us/en/pc-security/intel-it-security-trusted-execution-technology-paper.html)

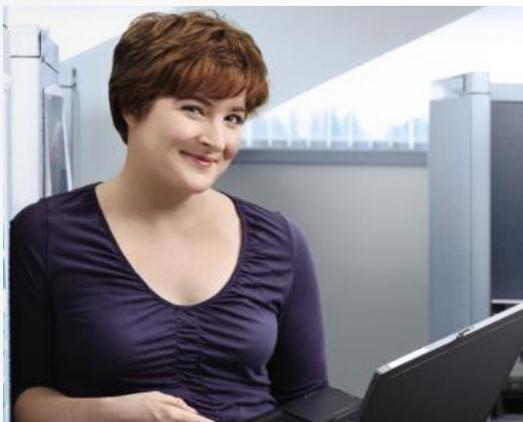
Step 6: Extend Trust across Federated Clouds

As cloud computing evolves, the vision of federated clouds—across which communications, data, and services can move easily within and across several cloud infrastructures—adds another layer of complexity to your security equation. Intel is working toward providing solutions that extend trust across federated clouds via secure gateways between the service provider and the service consumer with policy enforcement for centrally defined policies.

Intel Expressway Cloud Access 360 (Intel ECA 360) is a software solution designed to control the entire life cycle of secure access for enterprises connecting to cloud environments. It serves as a gateway to broker single sign-on (SSO) access from the enterprise into various clouds by authenticating employees against internal systems such as Active Directory* or other identity management systems. It records the user activity against these systems, and the metrics can be used for audit reporting and monitoring through an administrative console. In addition to providing SSO, Intel ECA 360 creates virtual identities built from data in enterprise systems—such as human resource applications and the telephone system—that establish user identity and verify the trusted systems where a user comes from.

The gateway can operate as a virtualized instance and can run either on-premises or at a third-party hosted or managed service provider. The gateway can also function as a proxy, where it performs as a secure token service and point of policy enforcement, or in look-aside mode, where it passes on the identity logic to a third party to perform the transformations.

Intel's partnership with McAfee delivers a coordinated security approach that spans network, servers, databases, storage, and data, as well as connecting policies and controls across physical, virtual, and cloud infrastructures. The McAfee infrastructure proactively identifies and blocks attacks by communicating with McAfee* Global Threat Intelligence technology. The foundation of the McAfee security management platform, McAfee ePolicy Orchestrator*, is an open, scalable platform that connects third-party security solutions to the infrastructure, strengthening protection and providing visibility into security, compliance, and risk management activities.



About Intel® ECA 360

Intel® Expressway Cloud Access 360 (Intel ECA 360) provides secure access for enterprises connecting to and across cloud applications by:

- Account deprovisioning and account identity data synchronization
- Enforced context-aware authorization with seamless single sign-on (SSO) from multiple devices
- Monitoring user, administrative, and API access activity
- Soft/hard one-time password (OTP) authentication
- Activity reporting for compliance and correlation of cloud user activity with on-premises logs for end-to-end compliance

Step 7: Choose the Right Cloud Service Provider

Choosing a cloud service provider is complicated on many levels—from the cloud delivery model and architecture to specific applications. Add to that the countless interdependencies and relationships, both technological and business-related, among vendors. To complicate matters, some companies offer not only software, but also hardware and services. Nevertheless, you must be vigilant about making sure the security you need to protect your data and platform are part of the offering.

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. Once you are comfortable that your criteria can be met, you can establish measurable, enforceable SLAs to provide ongoing verification.

The following is a list⁹ of additional security considerations to think about when choosing a cloud service provider.

Security Selection Criteria	Considerations
Data center risk management and security practices	<ul style="list-style-type: none"> What are the patch management policies and procedures? How does technology architecture and infrastructure impact the cloud service provider's ability to meet SLAs?
Hardware-based security	<ul style="list-style-type: none"> Can the cloud service provider offer trusted pools for your most sensitive workloads? Is encryption a software-only solution?
Technology segmentation	<ul style="list-style-type: none"> How are systems, data, networks, management, provisioning, and personnel segmented? Are the controls segregating each layer of the infrastructure properly integrated so they do not interfere with each other? For example, investigate whether the storage compartmentalization can easily be bypassed by management tools or poor key management. What cloud access and identity protocols are used?
Attack response and recovery	<ul style="list-style-type: none"> How are attacks monitored and documented? How quickly can the cloud service provider respond? What recovery methods are used?
System availability and performance	<ul style="list-style-type: none"> How does the cloud service provider handle resource democratization and dynamism to best predict proper levels of system availability and performance through normal business fluctuations? How does the cloud service provider measure performance?
Vendor financial stability	<ul style="list-style-type: none"> Is the cloud service provider financially stable? How long has the vendor been in business? What is their current financial standing?

⁹ Adapted and expanded from *How to Choose a Cloud Computing Vendor*. Inc.com (November 29, 2010). inc.com/guides/2010/11/how-to-choose-a-cloud-computing-vendor.html

Security Selection Criteria	Considerations
Product long-term strategy	<ul style="list-style-type: none"> ▪ What is the vision for the service provider's cloud offering? ▪ Does the cloud service provider have a product roadmap for their offering? Cloud service providers seeking to provide mission-critical services should embrace the ISO/IEC 27001 standard for information security management systems. If the provider has not achieved ISO/IEC 27001 certification, they should demonstrate alignment with ISO 27002 practices.
Limits of responsibility	<ul style="list-style-type: none"> ▪ What is the limit of the cloud service provider's responsibility for security? ▪ What security responsibilities are expected of the enterprise? ▪ What is the legal accountability in a breach?
Compliance capabilities	<ul style="list-style-type: none"> ▪ Does the cloud service provider have the ability to comply with regulatory requirements that you face? ▪ Is the cloud service provider able to provide you with full visibility into compliance-related activities? ▪ Can you perform your own audit?

As you and other IT managers continue to explore options for moving workloads to the cloud, security considerations will continue to influence your buying decisions. As a result, cloud service providers are becoming more aware of the need for transparency into their security practices.

Intel Resources for Learning More

Intel Technologies for Cloud Security

Evolution of Integrity Checking with Intel® Trusted Execution Technology: An Intel Perspective

In 2010, Intel began transitioning to a private cloud environment to improve efficiency and agility. The highly virtualized multitenant environment creates new security challenges, including those presented by emerging threats such as rootkit attacks. Intel evaluated Intel TXT as part of its analysis of technologies that can potentially address these issues.

intel.com/content/www/us/en/pc-security/intel-it-security-trusted-execution-technology-paper.html

Securing the Enterprise with Intel® AES-NI

This white paper describes AES usage scenarios, performance implications, and the cryptographic libraries that ISVs can use to replace basic AES routines with the Intel AES-NI optimizations.

intel.com/content/www/us/en/enterprise-security/enterprise-security-aes-ni-white-paper.html

Intel® Advanced Encryption Standard Instructions (AES-NI)

This article by Intel expert Jeffrey Rott is an in-depth look at using Intel AES-NI, with specific focus on the 2010 Intel Core™ processor family and its performance and security benefits.

<http://edc.intel.com/Link.aspx?id=5093>

Taking Control of the Cloud for Your Enterprise: Addressing Security, Visibility, and Governance Challenges

This white paper is for enterprise security architects and executives who need to quickly understand the risks of moving mission-critical data, systems, and applications to external cloud providers. The concept of a dynamic security perimeter is presented to help explain how to address insecure APIs, multitenancy, data protection, and tiered access control for the cloud.

dynamicperimeter.com/download/Taking_Control_of_the_Cloud/?partnerref=intelsoaesite

Intel Cloud Builders Reference Architectures

Take advantage of proven guidance for building and optimizing cloud infrastructure. Each reference architecture is based on real-world IT requirements and gives detailed instructions on how to install and configure a particular cloud solution using Intel Xeon processor-based servers and technologies.

Intel® Cloud Builders Guide: Enhancing Server Platform Security with VMware

intel.com/content/www/us/en/cloud-computing/cloud-computing-xeon-server-platform-security-vmware-guide.html

Intel Cloud Computing Ecosystem

Additional Resources

Intel® Cloud Builders Guide: Enhanced Cloud Security with HyTrust® and VMware®
intel.com/content/www/us/en/cloud-computing/cloud-computing-security/cloud-computing-enhanced-cloud-security-hytrust-vmware-architecture.html

Intel® Cloud Builders Guide: Trusted Compute Pools with Parallels®
intel.com/en_US/Assets/PDF/general/icb_ra_cloud_computing_Parallels_TCP.pdf

Intel® Cloud Builders—An Ecosystem of Cloud Computing Companies

A list with information about leading Intel ISV and OEM partners who perform joint, hands-on engineering and testing to deliver proven cloud solutions and cloud services on Intel Xeon processor-based servers.

intel.com/content/www/us/en/cloud-computing/cloud-builders-ecosystem-works-together.html

The New Reality of Stealth Crimeware

This white paper discusses how stealth technology from sophisticated attackers, such as Stuxnet and Zeus, enables malware to launch rootkit attacks to gain intelligence or take over systems and data. The authors describe their vision of how to fend off rootkit-style attacks: monitor operations from a vantage point closer to and integral with the hardware.

mcafee.com/us/resources/white-papers/wp-reality-of-stealth-crimeware.pdf

Security Guidance for Critical Areas of Focus in Cloud Computing, v2.1

This Cloud Security Alliance (CSA) guide contains in-depth information to help you conduct a risk assessment of initial cloud risks and make informed decisions about how you can adopt cloud computing services and technologies. In addition to general guidance, the document covers 13 critical domains, including cloud computing architecture; governance and enterprise risk management; legal and electronic discovery; compliance and audit; information life cycle management; portability and interoperability; traditional security, business continuity, and disaster recovery; data center operations; application security; encryption and key management; identity and access management; and virtualization.

<https://cloudsecurityalliance.org/csaguide.pdf>

Top Threats to Cloud Computing, v1.0

This CSA 2010 report catalogs best practices for managing seven threats in the cloud environment. It is designed to provide organizations with needed context to assist them in making informed risk management decisions based on their specific cloud deployment strategies.

<https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>

Share with Colleagues

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 processors. For availability, consult your reseller or system manufacturer. For more information, see <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/>.

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, a chipset, a 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 intel.com/content/www/us/en/data-security/security-overview-general-technology.html.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION, OR SAMPLE. Intel disclaims all liability, including liability for infringement of any property rights, relating to use of this information. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Copyright © 2011 Intel Corporation. All rights reserved.

Intel, the Intel logo, Core, Xeon, Intel Sponsors of Tomorrow., and the Intel Sponsors of Tomorrow. logo are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

Active Directory is a registered trademark of Microsoft Corporation in the United States and/or other countries.

