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—from data center to endpoint devices—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 compliance to streamline audit processes
- Discusses extending trust across federated clouds
- Provides a checklist for making sure security is built into your evaluation of cloud service providers
Planning Guide
Cloud Security
Seven Steps for Building Security in the Cloud from the Ground Up
Contents

3 Cloud Security: What It Is (and What It Isn’t)
5 Security Challenges for Cloud Environments
7 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
17 Step 6: Extend Trust across Federated Clouds
19 Step 7: Choose the Right Cloud Service Provider
21 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, infrastructure, and clients 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.

• About providing protection whatever delivery model you deploy or use: private, public, or hybrid cloud environments.

• The joint responsibility of your organization and your cloud service provider(s). Depending on the cloud delivery model and services you deploy, security is the responsibility of both parties.

Cloud Computing 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 and what is delivered.

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 endpoint devices. The focus of this planning guide is to provide you with suggestions and recommendations for strengthening data, identity, and platform protection in the data center and for client devices. 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 as they build and deploy cloud technology.

Intel IT has embarked on a five-year rearchitecting of the Intel information security architecture. This redesign moves Intel IT 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.

The Intel Cloud Builders\(^1\) program continues to yield in-depth guidance that you can use for your cloud initiatives and education and as a forum for discussion of technical issues. Resources include reference architectures developed with ecosystem and solution leaders that focus on building or simplifying a cloud, enhancing security, and improving efficiency in your cloud environment.

Intel's strategic partnership with McAfee\(^2\) uniquely extends security capabilities across the entire security stack—from silicon to software to network—for a holistic security and compliance management platform and overall integrity of the cloud infrastructure.

Four 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.

- **Consumerization of IT:** As mobile devices and technologies continue to proliferate, employees want to use personally owned devices to access enterprise applications, data, and cloud services.

- **Dynamic and challenging regulatory environment:** Organizations—and their IT departments—face ongoing burdens of legal and regulatory compliance with increasingly prescriptive demands and high penalties for noncompliance or breaches. Examples of regulations include Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), 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. Five of these apply directly to our focus on protecting data and platform: nefarious use of cloud services, multitenancy, data loss, account hijacking, and “unknown” risk.

Abuse and nefarious use of cloud services. Many infrastructure-as-a-service (IaaS) providers make it easy to take advantage of their services. With a valid credit card, users can register and start using cloud services right away. Cybercriminals actively target cloud services providers, partially because of this relatively weak registration system that helps obscure identities, and because many providers have limited fraud-detection capabilities. Stringent initial registration and validation processes, credit card fraud monitoring, and subsequent authentication are ways to remediate this type of threat.

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.

Account or service hijacking. Attacks using methods such as phishing and fraud continue to be an ongoing threat. With stolen credentials, hackers can access critical areas of your cloud and potentially eavesdrop on transactions, manipulate or falsify data, and redirect your clients to illegitimate sites. IT organizations can fight back with strong identity and access management, including two-factor authentication where possible, strong password requirements, and proactive monitoring for unauthorized activity.

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.

Accelerating Cloud Security Standards

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. ODCA membership includes more than 300 companies representing more than U.S. dollar (USD) 100 billion in annual IT spend. ODCA released a roadmap of IT requirements in 2011 and updates in 2012 with the goal of defining IT needs that lead to more open and interoperable cloud and data center solutions. These include security-related usage requirements, such as Security Monitoring, Identity Management, and Security Provider Assurance, among others. The ODCA and the CSA formed a partnership to further link ODCA needs with CSA development of cloud security guidelines. 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 usage models can be found at opendatacenteralliance.org/ourwork/usagemodels.
Step 1: Start Security Planning Early

Your security profile in the cloud is defined by what your organization needs, the workloads you plan to move to the cloud, and the way users will access data and applications. 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 client devices will you support, and what security capabilities are available with those devices?
- What types of assets, resources, and information will be managed? What are the security requirements for these?
- 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, platform, and users. 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.

<table>
<thead>
<tr>
<th>Task</th>
<th>Purpose</th>
<th>Additional Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify the business priorities for moving the specific workload(s) to the cloud.</td>
<td>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.</td>
<td>• What drivers make cloud technology a good option for this workload? • Do you need to: ○ Reduce operational costs? ○ Scale seasonally? ○ Support remote or mobile workers?</td>
</tr>
<tr>
<td>Evaluate the sensitivity of the asset(s).</td>
<td>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.</td>
<td>• What harm would result if the asset was compromised?</td>
</tr>
<tr>
<td>Task</td>
<td>Purpose</td>
<td>Additional Considerations</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------------------------</td>
</tr>
</tbody>
</table>
| Map the security workload to the appropriate cloud delivery model and hosting models under consideration. | Now that you understand the importance of your asset, you can evaluate the risks associated with various deployment models. | • Are you considering a private, public, or hybrid cloud delivery model?  
• For a private cloud, will your deployment be:  
  • 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? |
| Determine whether the available services are capable of meeting your requirements for handling data, especially for compliance purposes. | 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. | • What are the specific requirements for handling regulated data? |
| Map the data flow, especially for public or hybrid cloud providers. | 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). Pay close attention to where security capabilities and requirements can be enforced, monitored, and reported. | • Can the provider continue to deliver protection as the workload continues to evolve through their entire physical and virtual infrastructure? |
| Understand how users will access applications and data. | Once you understand your user groups, you can identify which clients to support, and evaluate their data needs, their tools, and the capability of their devices to protect data. | • Do you need to support call-center workers? Office workers? Remote or mobile workers? |
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.

<table>
<thead>
<tr>
<th>Model</th>
<th>Description</th>
<th>Advantages and Disadvantages</th>
</tr>
</thead>
</table>
| Private | • 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 (internal private cloud) or off-premises on shared or dedicated infrastructure (external private cloud) | • Most control over data and platform  
• Potential for mutitenancy of business units to cause compliance and security risk  
• May lack agility for bursting when additional performance or capacity is required                                                                                                                                            |
| Public  | • Resources dynamically provisioned over the Internet, via web services, or from a third-party provider  
• Located off-premises, typically on a shared (mutitenancy) infrastructure  
• May offer dedicated infrastructure as a response to growing security concerns | • Potential for greater cost savings if infrastructure owned and managed by public provider  
• Loss of control of data and platform  
• Potential for mutitenancy with other organizations to cause security risk  
• Third-party security controls possibly not transparent (and may cause unknown risks)                                                                                                                    |
| Hybrid  | • 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 | • Often a compromise:  
  « Retention of physical 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 physical 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)                                                                                                                                   |
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. And it often comes at the added cost of operational complexity.

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.

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\(^5\) and applies to both data center and client systems.

The following illustration shows how the growing threat to clients and data centers applies to each layer in your IT infrastructure.

Protection at the hardware level can enable security deeper in the data center—and deeper into the devices themselves. 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.

Extending this model to cloud architectures makes additional foundational protections and controls even more vital. In short, new compensating controls are needed to offset the physical control capabilities lost to increased virtualization and mobility.
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. Plus, the proliferation of different types of client devices accessing cloud resources also provides hackers with many potential access points and targets.

Attackers are increasingly professional—more sophisticated, organized, determined, and better resourced. The potential for harm from a single attack in any of these areas can be devastating.

Growing attack target
Personal client devices that run software locally or access cloud infrastructure (desktops, laptops, and other mobile devices)

Growing attack target
Departmental and other systems that interact inside and outside the organization (web servers, portal servers, e-mail servers, bridges, and routers)

Emerging attack target
Isolated back-end servers used for virtualization, database management, and storage
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 infrastructure and endpoint clients. 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.
- Make it possible for users to utilize a variety of devices without compromising the client or data center infrastructure.

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 cloud ecosystem in four areas.

- Encrypt to protect data that rests or moves in the cloud—especially public clouds.
- Establish a trusted foundation to secure your data center platform and infrastructure and protect clients.
- Build higher assurance into compliance to streamline auditing.
- Establish and verify identities before you federate by controlling access from trusted clients and trusted systems.

The remainder of this planning guide will look in more detail at how advanced server and client technologies—in particular, Intel® technologies—can help you build trust and compliance into your data center, protect client platforms and data, 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. It is widely regarded as a best practice to use encryption on any sensitive data that might be at risk of loss of physical control—for example, many companies have policies that data on laptops must be encrypted. It is critically important in cloud environments—especially in hybrid or public cloud models, where data may move outside the traditional IT environment, but also in internal private clouds, where data can be exposed on shared compute resources.

Certain industries, such as healthcare and financial services, require organizations to meet certain regulations and standards for the way they protect data. Increasingly, these and other regulations are encouraging—and specifying—encryption in certain usage scenarios, including cloud computing. The penalties for noncompliance are stiffer than ever.

However, data encryption is often not used broadly due to the performance impact. With user expectations for the cloud to provide instant access to resources, it can be a tough sell as an IT manager to justify the trade-off in performance with the requirement for secure data.

When to Encrypt Data

Typically data doesn’t stay in one place on your network, and this is especially true of data in the cloud. Encrypt your data wherever it is in the cloud: at rest, in process, or in motion.

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, or sensitive personal financial data stored 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
Accelerate Encryption for Broad Use

It's possible to enable the pervasive use of encryption and overcome concerns about performance. Intel Advanced Encryption Standard® New Instructions (Intel AES-NI) is a set of seven new instructions that enhance performance by speeding up parts of the widely used AES algorithm encryption/decryption execution. It makes encryption stronger and more efficient—on physical systems or in the cloud.

Intel AES-NI is built into the Intel Xeon® processor family servers as well as clients with 2nd generation Intel Core™ processors. 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 (depending on application).
- **Improved security.** The new instructions help address recently discovered side-channel attacks on encryption. 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 optimized to use AES, including network, disk, and file encryption solutions.

---

6 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 and other low-level malware 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, BIOS, and operating systems, and can hide malware that operates in the background and spreads throughout a cloud environment, causing increasing damage over time.

With sophisticated threats and malware an ongoing and growing threat, securing both client and server platforms provides an additional enforcement point that builds trust between servers and between servers and clients.

The best way to enable a trusted foundation is to start with a hardware-based root of trust and extend the chain of trust through the critical controlling software layers, including firmware, BIOS, and hypervisor virtualization layers. A root of trust hardens the platform against attack and is extremely difficult to defeat or subvert. It substantially reduces the security risks of using a remote or virtualized infrastructure and enables a more secure platform for adding tenants and workloads. Essentially you build protection into your hardware to better 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. 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 can be blocked or an untrusted launch event reported if the measurements do not match.

About Intel® TXT

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

- Establishing a hardware-based 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 (trust) 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 environment

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 and management purposes.

Deeper Security Footprint for PC Endpoints Connected to Cloud

McAfee DeepSAFE* technology, developed as a joint effort by Intel and McAfee, enables McAfee hardware-assisted security products to provide a deeper security footprint. In the case of a cloud environment, McAfee DeepSAFE can help ensure the integrity of the PC endpoints that connect to it.

McAfee DeepSAFE technology sits below the operating system, close to the silicon, and monitors kernel memory events in real time for stealthy attacks, including kernel-mode rootkits and malware on PCs. It takes advantage of technology already built into the processor, including Intel Virtualization Technology (Intel VT-x), to provide security beyond the operating system. This puts security a step ahead of more traditional operating system–based software that may detect a rootkit attack—but only after it has been installed and had a chance to hide or propagate malware.

McAfee Deep Defender is the first endpoint security solution enabled by the McAfee DeepSAFE technology platform to provide deep, hardware-assisted client protection. It leverages Intel VT-x to get a new vantage point on security beyond the operating system to proactively report, block, quarantine, and remove known and unknown malware in the kernel. This way, McAfee Deep Defender can provide higher levels of protection and ensure that stealth attacks do not impact critical cloud-based assets.

Learn more about McAfee DeepSAFE or McAfee Deep Defender.

About McAfee* Server Software

McAfee* Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) offloads scan processing from VMs, delivering improved performance and resource utilization for virtual desktops and servers while delivering optimized anti-malware and advanced threat protection.

McAfee server technologies, such as McAfee Application Control and McAfee Change Control, work together to reduce overhead on servers and virtual machines, while proactively mitigating the risk of data breaches, targeted attacks, and unplanned downtime for servers and virtual machines.
Step 6: Extend Trust across Federated Clouds

As cloud computing evolves, the vision of federated cloud relationships—across which users, data, and services can move easily within and across several cloud infrastructures—adds another layer of complexity to our security equation.

Trusted access to the cloud and across clouds is based on managing identities and access-management policies, including standards-based single sign-on (SSO), strong authentication, account provisioning, API security, and audit capabilities. For cloud security, simple user names and passwords are no longer adequate because they can be easily compromised. Secure SSO based on strong second-factor authentication is essential in federated cloud environments, where the cloud service provider is relying on the authentication performed by the enterprise to grant access to applications.

Secure Cloud Access across the Life Cycle

Intel and McAfee have ready solutions that extend trust across federated clouds:

- McAfee Cloud Identity Manager, an on-premises federation gateway
- Intel Cloud SSO, an outsourced identity-as-a-service offering that can broker user access between the enterprise and the cloud service provider

Both software solutions are designed to control the entire life cycle of user-to-cloud access by authenticating employees against internal identity management systems such as Active Directory* and recording user SSO activity and applied authentication strength, which can be used for audit reporting and monitoring through an administrative console. These solutions also enable provisioning, updating, or deprovisioning accounts as needed across one or all cloud providers. At any point, administrators can elevate the authentication level to require client context controls, such as time of day or browser restrictions. Plus, administrators can conveniently push out one-time passwords (OTPs) to mobile devices, or if the client is Intel Identity Protection Technology (Intel IPT)–enabled, enforce hardware-based OTPs.

After SSO, enterprise and cloud-provider applications may communicate to consume or request data for user interactions with the cloud applications. This is done using application-to-application web services protocols such as representational state transfer (REST), simple object access protocol (SOAP), or JavaScript object notation (JSON). As a network edge security gateway, McAfee Services Gateway can route, manage, and secure APIs exposed from back-end applications or middleware. As the number of social and enterprise APIs continues to explode, service gateway control points for the cloud will become increasingly important.

Client-Based Identity Management

Intel IPT provides two-factor authentication that executes directly on the PC. The second factor is generated from a tamper-proof, embedded processor that runs independently from the operating system and changes every 30 seconds. This embedded processor also performs the operations that link the computer to a validated site, ensuring strong authentication at the endpoint of the cloud ecosystem. 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.
About McAfee* Cloud Security Platform

Intel’s identity solutions are integrated as part of the McAfee* Cloud Security Platform. The platform is modular in design and combines data-loss protection, e-mail, web, and identity security to protect cloud traffic during transit, including during private-to-public cloud interactions and mobile-to-cloud access. The platform also leverages McAfee Global Threat Intelligence technology to proactively identify and block attacks.

Using this suite of cloud technologies, an enterprise can create an intervening, policy-driven layer between users, app services, and device endpoints, centered on a model of identity services. Identity and app security capabilities include:

- Single sign-on (SSO), provisioning, and strong authentication
- Context-aware authorization based on client or network parameters
- Software- and hardware-assisted one-time passwords (OTPs) across mobile and Intel IPT–enabled clients
- Ready SSO and account provisioning connectors to hundreds of popular software-as-a-service providers based on standards such as Security Assertion Markup Language (SAML), OAuth, and OpenID
- On-premises or identity-as-a-service deployment models
- Data loss prevention (DLP) and web service security for app-to-app cloud APIs

See intel.com/go/identity and mcafee.com/cloudsecurity to learn more.
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 list of additional security considerations to think about when choosing a cloud service provider.

<table>
<thead>
<tr>
<th>Security Selection Criteria</th>
<th>Considerations</th>
</tr>
</thead>
</table>
| Data center risk management and security practices               | • 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                                          | • Can the cloud service provider offer trusted pools for your most sensitive workloads?  
• Is encryption a software-only solution?                          |
| Technology segmentation                                          | • 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?               |
| Identity and access management                                   | • How is identity managed and authenticated?  
• Is two-factor authentication utilized?                           |
| Attack response and recovery                                     | • How are attacks monitored and documented?  
• How quickly can the cloud service provider respond?  
• What recovery methods are used?                                 |
| System availability and performance                              | • 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                                       | • Is the cloud service provider financially stable?  
• How long has the vendor been in business? What is their current financial standing? |

(Continued)

### Security Selection Criteria

<table>
<thead>
<tr>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product long-term strategy</strong></td>
</tr>
<tr>
<td>• What is the vision for the service provider’s cloud offering?</td>
</tr>
<tr>
<td>• Does the cloud service provider have a product roadmap for their offering?</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Limits of responsibility</strong></td>
</tr>
<tr>
<td>• What is the limit of the cloud service provider’s responsibility for security?</td>
</tr>
<tr>
<td>• What security responsibilities are expected of the enterprise?</td>
</tr>
<tr>
<td>• What is the legal accountability in a breach?</td>
</tr>
<tr>
<td><strong>Compliance capabilities</strong></td>
</tr>
<tr>
<td>• Does the cloud service provider have the ability to comply with regulatory requirements that you face?</td>
</tr>
<tr>
<td>• Is the cloud service provider able to provide you with full visibility into compliance-related activities?</td>
</tr>
<tr>
<td>• Can you perform your own audit?</td>
</tr>
</tbody>
</table>

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.
More about Cloud Security from Intel

Planning Guide: Cloud Security is part of a series of documents produced by Intel to help IT professionals plan security into cloud implementations in their organizations. This series also includes:

**Cloud Security Insights for IT Strategic Planning**
Results from a survey of 200 IT professionals who provide insight into the business and technology drivers behind security in their cloud implementations, investment levels, return on investment, and outsourcing.

**Cloud Security Vendor Round Table**
The round table is designed to help IT managers better evaluate different cloud technology vendors and service providers based on a series of questions posed to three cloud infrastructure providers, three managed or hosted infrastructure providers, and three cloud technology providers.

**Inside Intel IT: Security Issues in Cloud Computing**
In this podcast, Alan Ross, who leads the Security Architecture and Technology Development Team at Intel IT, discusses security issues in cloud computing at Intel, including data security, application security, compliance, and privacy, as well as the Intel strategy for managing security issues in cloud computing—segregating the virtual environment and employing balanced controls.

**IT Managers Speak Out about Cloud Security: Results from a Survey of Your Peers**
Bryce Olsen from Intel presents a video report of the key findings from a survey of IT managers that provides insights into cloud security planning.
intel.com/content/www/us/en/cloud-computing/cloud-security-peer-research-video.html

**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® 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
**Malware Protection with Intel® Trusted Execution Technology**

This paper describes a highly scalable architecture called Intel Trusted Execution Technology (Intel TXT) that provides hardware-based security technologies to build a solid foundation for security. Built into Intel’s silicon, these technologies address the increasing and evolving security threats across physical and virtual infrastructure by complementing runtime protections such as antivirus software.

intel.com/go/txt

**McAfee Cloud Security Platform with New Security Capabilities from Intel**

In this video, Scott Chasin, McAfee chief technical officer, talks about the Intel-McAfee cloud security platform. McAfee contributes security modules for data loss protection, web, and e-mail that extend across mobile users, users behind endpoints, and applications channels. Integration with Intel Expressway Cloud Access 360 (Intel ECA 360) provides SSO and the ability to securely provision users from the enterprise into cloud assets. In addition, Intel Expressway Service Gateway provides security on top of the APIs used to access the cloud.


**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.


**XML Gateway, Application Security & Cloud Identity**

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.


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® Cloud Builders Guide: Enhanced Cloud Security with HyTrust® and VMware®**

Intel® Cloud Builders Guide: Trusted Compute Pools with Parallels*

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.

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.

Open Data Center AllianceSM Usage: Identity Management Interoperability Guide Rev. 1.0
This usage model provides structure and guidelines that promote interoperability between identity management and access management systems, so that users within organizations can utilize resources in the cloud as if they were located within the organization.

Open Data Center AllianceSM Usage: Security Monitoring Rev.1.1
Once a standard framework for security capabilities is established through delivery to the Security Provider Assurance Usage Model, companies need to be able to determine that service providers are meeting the levels promised. They need mechanisms that allow real-time monitoring of security level delivery to organizational and regulatory policy.
opendatacenteralliance.org/docs/ODCA_SecurityMonitoring_Rev1.1_Final.pdf

Open Data Center AllianceSM Usage: Provider Assurance Rev. 1.1
This usage model outlines the granular specification needed from every solution provider to enable security in multitenant shared infrastructure. It uses a tiered model of gold, silver, bronze, and platinum classifications for differentiation of service delivery to enable competitive offerings with trade-off features. There are implications at each level of stringency, with a standard way of determining where every cloud provider stands.
opendatacenteralliance.org/docs/ODCA_ProviderAssurance_Rev%201.1_Final.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
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/](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 v1.1. For more information, visit [intel.com/content/www/us/en/data-security/security-overview-general-technology.html](http://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 © 2012 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.