Planning Guide

Client Computing in the Cloud

Using Intelligent Clients to Address Security, Performance, and Manageability Issues in Your Cloud Environment

Why you should read this document:

- Deploy two-factor authentication and hardware-based protection to help enhance security.
- Boost system performance and improve the user experience with hardware-based support.
- Use remote control, diagnosis, and repair capabilities to simplify IT management.
- Understand the role of a client-aware cloud in achieving a balanced compute model.
Planning Guide
Client Computing in the Cloud
Using Intelligent Clients to Address Security, Performance, and Manageability Issues in Your Cloud Environment
SEPTEMBER 2011
Contents

3  Cloud Planning: Not Just for the Data Center

4  Improving Cloud Security, Performance, and Manageability Using Intelligent Clients
   • Security
   • Performance and User Experience
   • Manageability

14  Client-Aware Cloud
   • Enabling the Client-Aware Cloud
   • Intel IT Explores the Client-Aware Cloud

16  Intel Resources for Learning More
   • Clients in a Cloud Environment
   • Intel Technology
Most IT departments have concentrated their cloud planning efforts on the data center. But it’s extremely important for IT to understand the role of clients in delivering cloud services and applications.

Moving to the cloud introduces security, performance, management, and user experience issues into your computing environment. The clients you choose to deploy in this new environment can help alleviate—or exacerbate—these issues. As a result, they have a direct impact on the success of your cloud initiatives.

Your cloud infrastructure will, of course, need to accommodate many different kinds of clients, including PCs, smart phones, tablets, and more. This guide focuses on how you can use a particular type of PC client—an intelligent PC client—to resolve some of the challenges you will likely face as you move to a cloud infrastructure.

The first section, “Improving Cloud Security, Performance, and Manageability Using Intelligent Clients,” discusses how you can use client capabilities available today. The second section, “Client-Aware Cloud,” discusses client capabilities that will be available in the near future to significantly improve IT flexibility and user experience.

Defining “Intelligent Client”

This guide frequently uses the term “intelligent client.” Intel defines an intelligent client as a client device that provides the following:

- Hardware-based security capabilities
- Advanced manageability
- Energy-efficient performance capabilities
Improving Cloud Security, Performance, and Manageability Using Intelligent Clients

With all the industry excitement about cloud environments, it’s easy to forget that we’re still in the early stages of cloud implementations, whether private, public, or hybrid. As both organizations and vendors gain experience with full-scale cloud implementations, we’re beginning to see how clouds affect the basic tenets of IT service delivery, including security, performance, and manageability.

Security

Moving to a cloud environment introduces a host of security considerations for IT managers. For a complete look at security in the cloud and the steps you can take to plan for data and platform protection in your cloud implementation, see Intel’s Cloud Security Planning Guide.

This guide focuses on three cloud security concerns for which clients can play a direct role in safeguarding corporate data in a cloud environment.

- Authentication
- Secure execution of virtual applications
- Protection against malware and spyware

Using Intel® Identity Protection Technology

Intel® Identity Protection Technology (Intel IPT) uses a one-time password (OTP) methodology for two-factor authentication.

- Users must be on a PC powered by a select second-generation Intel Core™ processor produced by an OEM that has enabled Intel IPT (consult http://ipt.intel.com for a complete list of models).

- The cloud service or application being accessed needs to have incorporated Intel IPT protection, as supported by one of Intel’s IPT software partners: Symantec or VASCO.
## Authentication

### Issue

Authentication can become a significant issue in a public or hybrid cloud environment when IT organizations need to ensure that only trusted users and devices can access corporate data and services hosted outside the organization’s own four walls. You may be asked to meet corporate compliance specifications that require some sort of multifactor authentication.

### How intelligent clients can help

Intelligent clients can provide a straightforward method of two-factor authentication. The client becomes part of the two-factor equation, enabling IT organizations to move easily to two-factor authentication and to do so, in general, less expensively than they can with some of the other available methods, such as physical tokens.

### Details

Intel has developed a way for two-factor authentication to be built directly into the processor of the client device. This technology, called Intel® Identity Protection Technology (Intel IPT), uses a one-time password (OTP) methodology.

Calculations to create OTPs are performed in a protected place within the computer hardware. When an OTP is entered into the cloud service or application, a comparison is made with a number created by the server with the same seed and algorithm. A match signifies positive authentication and ensures that the user’s identity has been confirmed.1

---

## Secure execution of virtual applications

<table>
<thead>
<tr>
<th>Issue</th>
<th>In a cloud-based environment, IT must ensure that virtualized applications running on the client execute in a secure and protected environment.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How intelligent clients can help</td>
<td>Intelligent clients establish a &quot;root of trust&quot; that validates the behavior of key components within the client device start-up. This hardware-based protection safeguards the client against software-based attacks at the infrastructure level (i.e., the BIOS and hypervisor).</td>
</tr>
</tbody>
</table>
| Details | An intelligent client is able to perform integrity checking, which enables the client to "boot" software into a trusted state. It also protects secrets during both orderly and disorderly shutdowns. | Intel provides this capability through what is known as Intel Trusted Execution Technology, or Intel TXT, which is a component of the Intel Core™ processor family with vPro™ technology.  
Intel TXT validates the behavior of key components within the client at start-up. Known as the "root of trust," the system checks the consistency in behaviors and launch-time configurations against a "known good" sequence. Using this verified benchmark, the client can quickly assess whether any attempts to alter or tamper with the launch-time environment have been made.  
Intel TXT does this by creating a cryptographically unique identifier for each approved launch-enabled component—including the hypervisor used for virtualized applications—and then provides hardware-based enforcement mechanisms to block the launch of any code that does not match the approved code. In a cloud-based environment, this integrity checking enables the client to determine whether the client's virtual infrastructure meets IT security and compliance requirements. |

---

2 For more information about Intel TXT, see Technology Overview: Intel® Trusted Execution Technology.  
3 Learn more about a high-performance virtualization solution developed jointly by Citrix and Intel for federal agencies.  

---

---
Protection against malware and spyware

<table>
<thead>
<tr>
<th>Issue</th>
<th>Even in a cloud-based environment, IT must address and manage the ongoing threat of malware and spyware.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How intelligent clients can help</td>
<td>Intelligent clients can perform regular client checking to ensure the active presence of security agents. If an agent fails to &quot;check in&quot; as expected, it is presumed the agent has been removed, tampered with, or disabled, triggering an alert to the security console.</td>
</tr>
<tr>
<td>Details</td>
<td>By using an intelligent client, you can virtually eliminate the ability of users or malware to circumvent virus protection. For example, if a user disables virus scan agents—unintentionally or intentionally—or malware attacks and infects a platform, that action triggers an alert, quarantines the system, and reinitializes the agent. Intel provides this capability through Intel Active Management Technology, or Intel AMT, which is a component of the Intel Core processor family with vPro technology. In a traditional environment, management consoles poll or scan to ensure that software agents are present. However, this takes up network bandwidth and only occurs if the operating system is present and operational and the platform is powered on and attached to the corporate LAN. It also means that many mobile client systems, along with systems that are powered off, cannot be scanned. Intel AMT overcomes these limitations by enabling third-party software agents to register with Intel AMT firmware. After registration, the third-party management console software periodically checks for agent presence according to corporate policy—and since it's all done locally, it doesn't affect network performance. If agents don't respond, an alert is sent to the management console, and configuration settings determine next steps. For example, the system can take immediate action, such as isolating the system from network access while leaving a port open to allow the reinstallation of the disabled agent. With Intel AMT, you can reduce the number of support calls required to remedy the effects of agent disabling or misconfiguration. You can also realize user productivity gains through increased platform stability and faster problem resolution.</td>
</tr>
</tbody>
</table>

A basic rule of thumb for IT planning is to always analyze potential changes from the perspective of your users. In general, taking away as little as possible from the current user experience will increase user acceptance of your cloud strategy. IT organizations can’t afford to underestimate the importance of user experience in the success of their cloud initiatives.

While performance isn’t the only measure of user experience, it is generally the most important for users. Moving to a cloud environment can cause performance slowdowns—and, subsequently, user unhappiness and push-back—in three different areas.

- Application performance
- Performance of software-based virtualization (remote slowdowns)
- Cloud-based data backup

**Intel IT Recommends: Four Questions to Ask When Moving Applications into the Cloud**

- What specific effects does moving the application to the cloud have on the user experience?
- How is “quality of experience” defined for the application?
- What factors contribute to the quality of the experience?
- For each factor, what are the trade-offs between user experience and IT control of the application?
## Application performance

<table>
<thead>
<tr>
<th>Issue</th>
<th>As applications are moved into the cloud—whether private or public—performance can suffer when the applications are compute intensive or bandwidth constrained.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How intelligent clients can help</td>
<td>Enabling client-side execution for compute-intensive or bandwidth-constrained applications will generally deliver a better user experience.</td>
</tr>
<tr>
<td>Details</td>
<td>In the fall of 2010, Intel's IT department ran a series of tests to determine the effect that client type has on the performance of a variety of cloud-based applications. It tested three client types.</td>
</tr>
</tbody>
</table>

### A high-end client:
- Mobile PC
- Second-generation Intel Core processors with vPro technology
- Microsoft* Windows* XP (32 bit)
- 3 GB RAM

### A midrange client:
- Entry-level desktop
- Intel Atom™ processor
- Microsoft Windows XP (32 bit)
- 2 GB RAM

### A thin client:
- Single-core processor
- Microsoft Windows XP Embedded (32 bit)
- 2 GB RAM

The applications tested include:
- Intel's internal enterprise resource planning (ERP) portal, hosted on a private cloud
- Two versions of the same customer relationship management (CRM) application hosted on the vendor's public cloud: one version a traditional cloud application; the second a rich Internet application (RIA) version of the same application (RIAs provide for client-side application execution)
- A mapping application (also an RIA), hosted on a public cloud
- Intel's employee portal, hosted on a private cloud
- An external e-commerce site

In each application test, Intel IT assessed the user experience by measuring the time taken to complete common user operations.

In the cases of the employee portal and e-commerce site, the performance difference among client types was measured in milliseconds, with generally not enough of a difference to substantially affect user experience. For users who only access these types of applications, a lightweight client may be appropriate.

But in the cases of the ERP portal, both versions of the CRM application, and the mapping application, performance differences among clients were measured in seconds and, in the case of the ERP portal, in minutes. For users who typically work with these types of applications, the thin client and midrange client delivered a significantly poorer experience. The best performance was delivered by a combination of the mobile PC and the RIAs, which took advantage of client-side execution.5

---

### Performance of software-based virtualization (remote slowdowns)

<table>
<thead>
<tr>
<th>Issue</th>
<th>Software-based virtualization affects system performance because the software translation is slower than direct hardware access; other events happening on the virtual machine can cause slowdowns.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How intelligent clients can help</strong></td>
<td>With an intelligent client, much of the burden of software-based virtualization can be shifted to the hardware. This helps make virtualization more efficient and can improve performance to near-native levels, depending on the model.</td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td>All virtualization technologies impact system performance, but you can gain efficiencies by using a specific virtualization model. With a Type 1 hypervisor, you can improve performance and enhance security because the hypervisor operates directly with the hardware. In addition, you can use Intel TXT to achieve greater security efficiencies at the hypervisor level. Intel TXT provides a hardware-based security foundation that protects against software-based attacks by validating the behavior of critical software components at start-up, protecting against malicious intent.</td>
</tr>
</tbody>
</table>

### Cloud-based data backup

<table>
<thead>
<tr>
<th>Issue</th>
<th>Cloud-based data backup can become a performance bottleneck, particularly for organizations that require encryption for any data sent off-site. Encryption and decryption processes can add a significant performance burden when sending large volumes of data to a cloud-based storage provider.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>How intelligent clients can help</strong></td>
<td>Using hardware-based instruction sets that are built into client hardware increases the speed of applications performing encryption and decryption using the Advanced Encryption Standard (AES). AES is widely used across the software ecosystem to protect network traffic, data, and corporate IT infrastructure.</td>
</tr>
<tr>
<td><strong>Details</strong></td>
<td>Certain Intel client processors—including the Intel Core processor family, both first and second generation—include Intel Advanced Encryption Standard New Instructions (Intel AES-NI).&lt;sup&gt;5&lt;/sup&gt; AES is a symmetric block cipher that encrypts and decrypts data through several rounds. Intel AES-NI offloads several compute-intensive parts of the AES algorithm from software onto client hardware, so that encryption and decryption processes can be accelerated. The performance improvement realized through the use of Intel AES-NI depends on the specific application and how much application time is spent in encryption and decryption. Intel has run tests using the Intel Core i7 processor Extreme Edition that show a two- to tenfold speed increase over software-only execution of AES.</td>
</tr>
</tbody>
</table>

---


For more information on the performance tests described above, see Breakthrough AES Performance with Intel® AES New Instructions. [http://software.intel.com/file/27067](http://software.intel.com/file/27067)
Manageability

Supporting end users accessing the cloud in a cost-effective, efficient way can present challenges for IT departments. With intelligent management capabilities from Intel, help-desk staff can remotely repair and secure clients even if they are asleep, hibernating, or powered down, or if the operating system is inoperable—whether inside or outside the corporate firewall and whether using a wired or wireless connection.

Intelligent clients can help improve manageability in the cloud in two different areas.

- Remote control
- Remote diagnosis and repair

Key Functionality of Intel AMT

The following capabilities are provided by Intel AMT or enabled by Intel AMT in third-party software:

- Out-of-band (OOB) access – Platform is diagnosed and repaired in a crashed state via OOB access to Intel AMT, KVM Remote Control, or Serial over LAN (SOL) and IDE Redirection (IDE-R) with third-party diagnostics.
- Remote troubleshooting and recovery – Diagnostic and recovery capabilities of the third-party management application can be used remotely.
- Tamper-resistant agent – This agent is accessible by the third-party management application to gain remote control with little risk of user tampering.
Remote control

<table>
<thead>
<tr>
<th>Issue</th>
<th>Fully encrypted client hard drives are essential in a cloud-based environment, but remote systems with encrypted hard drives can be difficult to manage.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How intelligent clients can help</td>
<td>Intelligent clients offer remote control capabilities that enable IT staff to access and manage remote systems that are encrypted—including unlocking encrypted drives and managing data security settings even when the client is powered off.</td>
</tr>
</tbody>
</table>
| Details | The second-generation Intel Core i5 or i7 processor with vPro technology and with Intel processor graphics includes a hardware-based Intel KVM Remote Control capability that lets IT staff remotely see what the user sees—even beyond the firewall. With KVM Remote Control, you can:  
  - Diagnose a network driver issue  
  - Remotely observe events causing a catastrophic failure as well as the actual failure  
  - Gain visibility and control of remote system boot processes  
  - Reset a forgotten password  
  - Gain remote control of any recovery operating system  
  
The ability to gain remote control of system boot processes with KVM Remote Control simplifies and speeds problem resolution. After gaining access to a PC, you can remotely boot the PC by redirecting the PC's boot process. You can boot from a different image such as a network share, bootable CD-ROM or DVD, remediation drive, or other device. KVM Remote Control also supports the ability to remotely boot a PC with a corrupted or missing operating system.  
  
KVM Remote Control only operates with Intel processor graphics. However, a platform may also have a discrete, external graphics system so that users can switch back and forth between the graphics interfaces. Intel AMT 6.0 adds KVM Remote Control to the existing redirection features of Serial over LAN (SOL) and IDE Redirection (IDE-R). That way, a remote console can open a session with an Intel AMT platform, control the platform using a mouse and keyboard, and display what is showing on the local monitor at the console. |
## Remote diagnosis and repair

<table>
<thead>
<tr>
<th>Issue</th>
<th>Diagnosing and repairing platform boot failures in the cloud can be difficult, time intensive, and costly.</th>
</tr>
</thead>
<tbody>
<tr>
<td>How intelligent clients can help</td>
<td>Intelligent clients can help reduce the overhead associated with repairing platform boot failures by increasing remote resolution rates and saving valuable time—for the end user and IT—and eliminating reactive and lengthy diagnostic processes.</td>
</tr>
</tbody>
</table>
| Details | In a conventional help-desk scenario, the user contacts the help desk and the support technician tries to diagnose the problem. However, in instances where the system will not boot, the technician will likely need to make an onsite visit. For remote scenarios such as a cloud-based computing environment, it is critical for IT to be able to problem-solve from any location.  

As shown earlier in the “Authentication” section of this document, Intel AMT delivers powerful remote protection. By using Intel vPro technology with Intel AMT, you can remotely diagnose problems and perform remote remediation (using third-party management software) to minimize user downtime and reduce the IT time spent on resolution.  

Intel AMT sends an alert to a management console that identifies a soon-to-fail hardware unit before the boot failure occurs. If the system fails without warning and refuses to boot, you can use Intel AMT IDE-R to redirect the platform to a known good boot image, diagnose the problem, and perform remote remediation. |
Client-Aware Cloud

IT departments must deliver cloud services to many types of clients with the expectation of high security, performance, and manageability. Intel believes that it is essential for cloud architectures to incorporate clients if they are to deliver on these expectations—and provide the user experience and the IT flexibility needed to make widespread cloud adoption feasible.

This is why one of the three tenets of our cloud computing vision—called Intel’s Cloud 2015 Vision (intel.com/content/www/us/en/cloud-computing/intel-s-cloud-computing-vision.html)—is that clouds must become “client aware.” When a cloud is client aware, the solutions delivered over the cloud can make realtime decisions about how to optimally execute a given task based on what they detect about the capabilities of individual clients.

For example, if the application detects that the end point is a smart phone, it can choose to run tasks entirely from the cloud-based server. But if the same application detects a PC capable of meeting security policy requirements, it can choose to push execution of that task to the client.

A client-aware cloud infrastructure benefits both IT and users.

• For users, it delivers better responsiveness and productivity—both essential to delivering a quality user experience.
• For IT, it improves application delivery and provides a more flexible architecture.

Ultimately, we believe that a client-aware cloud is essential for achieving a “balanced compute model.” The balanced compute model uses the strengths of both cloud and client to deliver the optimal cloud environment: secure, manageable, and offering a high-quality user experience.

Balanced Compute Model
Capitalizing on the capabilities of the cloud and the client.
Enabling the Client-Aware Cloud

To make the client-aware cloud a reality, Intel is developing APIs so that developers can enable their cloud-based applications to detect the capabilities of the local client device. Currently, three APIs are available for developers to download.\(^8\)

- **Network bandwidth API**: Detects wireless signal strength
- **Processor performance API**: Detects the CPU type
- **Battery life API**: Provides periodic power-level updates

Intel will continue to develop additional APIs that enable the client-aware cloud. The current APIs work for devices that use Intel processors; Intel is currently working on fully supported APIs to enable other processor manufacturers to take advantage of this technology.

Intel IT Explores the Client-Aware Cloud

At Intel, the IT department acts as a service provider to Intel users. Intel IT views client-aware cloud applications as a key component to balancing execution between the cloud server and the client device. Intel IT believes this balance is essential for delivering services with the performance that users expect and the security that Intel requires.

Intel IT is currently exploring data isolation, in which applications sense the security capabilities of the client device to determine which activities are allowed on the device. For example, some devices may only be allowed to view data, while others will be allowed to manipulate it. Moving forward, Intel IT will continue to investigate new ways to enable client-aware clouds.

---

\(^8\) These APIs are still in production. Therefore, Intel does not currently provide support or functionality guarantees.
## Intel Resources for Learning More

### Clients in a Cloud Environment

*Cloud Computing: How Client Devices Affect the User Experience*

*Client Computing: The Next Step toward a Better Cloud*

*Benefits of a Client-Aware Cloud*

*Cloud Computing Technology (Intel Cloud 2015 Vision)*

### Intel Technology

*Intel® vPro™ Technology: Reference Guide*

*2nd Generation Intel® Core™ vPro™ Processor Family Overview*

*Intel® Advanced Encryption Standard Instructions (AES-NI)*

*Access Accounts More Securely with Intel® Identity Protection Technology*

*Technology Overview: Intel® Trusted Execution Technology*

*Architecture Guide: Intel® Active Management Technology*
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.

Intel vPro technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html.

Intel Active Management Technology (Intel AMT) requires activation and a system with a corporate network connection, an Intel AMT–enabled chipset, and network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host-operating-system-based VPN when connecting wirelessly or when on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit intel.com/technology/platform-technology/intel-amt.

Intel Advanced Encryption Standard New Instructions (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/.

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, Intel Sponsors of Tomorrow., the Intel Sponsors of Tomorrow logo, Atom, Core, and vPro 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.

Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and/or other countries.