IT@Intel White Paper

Intel IT

IT Best Practices

Cloud Computing and IT Consumerization

June 2012

Delivering Cloud-based Services in a Bring-Your-Own Environment

By taking advantage of the unique strengths associated with client devices and the cloud, we are systematically building a private enterprise cloud that can determine device attributes and user preferences, and tailor services accordingly.

Dave Buchholz
Principal Engineer, Intel IT

Ed Goldman
IT Chief Technology Officer, Intel IT

Dennis Morgan
Senior Security Strategist, Intel IT

Chris Peters
Industry Engagement Manager, Intel IT

Executive Overview

As Intel IT builds cloud infrastructure and enables cloud services, one of the goals is to make those services available to as broad a range of devices as possible. Therefore, we are integrating our cloud computing efforts with our bring-your-own device initiatives, enabling Intel to obtain the maximum business value from both.

Several years ago, we determined that addressing the consumerization of IT head-on by formalizing implementation could actually improve enterprise security by eliminating unsecured, unmanaged use of personal devices. With that realization in mind, we are actively integrating employee-owned devices—including smartphones, tablets, and PCs—into our enterprise environment.

We have also been building Intel's enterprise private cloud, and now deliver 80 percent of our enterprise services through that cloud. We plan to increasingly use a mix of private and public cloud-based services, called hybrid cloud.

Today, we are implementing foundational capabilities that will eventually create a two-way awareness between cloud and client. We are adapting our communications infrastructure, service delivery model, and application development processes to support a client-aware cloud and cloud-aware clients.

- To manage, protect, and deliver cloud-based services to a broad range of devices, we have significantly revised our information security model, mobile device management practices, and personal workspace portability capabilities.
- We provide information about device features and services to employees, which helps guide them in selecting a device that will help them be as productive as possible and have an optimal user experience.
- We are implementing a data and application virtualization framework that enables us to assemble existing enterprise data and application capabilities and quickly integrate them with new capabilities.

By taking advantage of the unique strengths associated with client devices and the cloud, we are systematically building a private enterprise cloud that can determine device attributes and user preferences, and tailor services accordingly.

Contents

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BACKGROUND

Intel employees want to be able to use a broad range of companion devices, including personally owned smartphones and tablets, with their Intel-supplied mobile business PCs. They also want to be able to use their personally owned Macs* and PCs. We determined that addressing the consumerization of IT head-on by formalizing implementation could actually improve enterprise security, helping to eliminate unsecured and unmanaged use of personal devices. Intel IT is actively integrating employee-owned devices into our enterprise environment.

In early 2010, about 3,000 Intel employees were using personally owned smartphones; by the end of June 2012, this number had increased to 19 ,000. Also in 2011 some employees began using their personal Apple* computers, and this year we are expanding our bring-your-own-device (BYOD) initiative to include PCs. We are transitioning from the traditional client computing model of a limited number of device types under tight and direct IT control to a future compute continuum model that focuses on a seamless, consistent experience across devices. We see great business value in allowing employees more choice in the devices they can use at work. At the same time, we realized we need to protect Intel information security by maintaining control of the underlying communication infrastructure that supports those devices.

There are parallels and interdependencies between IT consumerization, which provides employees with a wider range of choices for compute capability, and the advent of cloud computing, which offers businesses additional options for IT services. At Intel, we have built an extensive private enterprise cloud, and we now deliver 80 percent of our enterprise services through that cloud. We plan to continue moving toward a mix of private and public cloud services, called a hybrid cloud.

As we continue to build cloud infrastructure and enable cloud services and applications, it is important that we consider our BYOD initiatives at the same time. This integrated approach will enable Intel to obtain the maximum business value from both BYOD and cloud computing.

SOLUTION

We have found that the key to delivering cloud-based services to a wide variety of devices, including BYO devices, is to create a two-way awareness between the cloud and the client. Not all client devices have the same capabilities, and the cloud is not always available to a client device. Therefore, a one-size-fits-all service delivery model is not appropriate. A misalignment between the delivery model and the device could negatively affect employee productivity and business functionality, introduce security risk, and invalidate the investment made in developing cloud-based services and applications.

By taking advantage of the unique strengths associated with the device and the cloud, we are systematically building a private enterprise cloud that can determine device attributes and user preferences, and tailor services accordingly. Although it will take several years to complete our efforts, we are already working to establish the necessary foundational capabilities over the next few months.

As illustrated in Figure 1, our intelligent, client-aware cloud will be able to determine the following:

- Whether an application provides the best user experience if executed locally or remotely
- Which native features, such as a location-based service provided by the Global Positioning System or accelerometer, are available on a device
- How to use predefined user and device profiles to customize services to user preferences and the device's security access level

Conversely, we are also establishing foundational capabilities to enable cloud-aware client devices. For example, a client device will be able to determine the following:

- Whether the cloud is available
- What services are available to the client device at the time
- Its security level and available bandwidth

For example, if the cloud is available, the device stores a document in a cloud-based document repository. But, if the cloud isn't available, the device stores the document locally and possibly automatically uploads the document to the cloud when it becomes possible.

Cloud-aware devices can also offload work from the cloud that might be more efficiently done on the device, helping to enhance the quality of service for end users. This type of work might include image and video processing, data compression, and 2D and 3D graphics. The 3rd generation Intel® Core™ processor family with Intel® Turbo Boost Technology 2.0 and next-generation graphics facilitate local execution on the device. Taking advantage of local resources in this manner helps reduce both the data center workload and the associated network traffic. We are currently conducting several proofs of concept to evaluate these types of technologies and to establish enterprise usage models.

Implementing a client-aware cloud and cloud-aware devices requires changes to the communications infrastructure, service delivery model, and application development processes.

Communications Infrastructure Changes

Providing cloud-based services to multiple devices and OSs requires several modifications to our communications infrastructure, such as additional firewall controls. These adjustments are necessary because each OS has different security features, and some are more secure than others. To support a broad range of personally owned devices, we are building a communications infrastructure that uses a flexible combination of delivery methods, including workspace and application containers, application and desktop virtualization, remote display technology, HTML5, and web portals, to deliver services to a wide variety of form factors, including PCs, Macs, tablets, and smartphones.

To manage, protect, and deliver this flexibility we have made significant enhancements and adjustments to our information security model, mobile device management practices, and personal workspace portability capabilities.

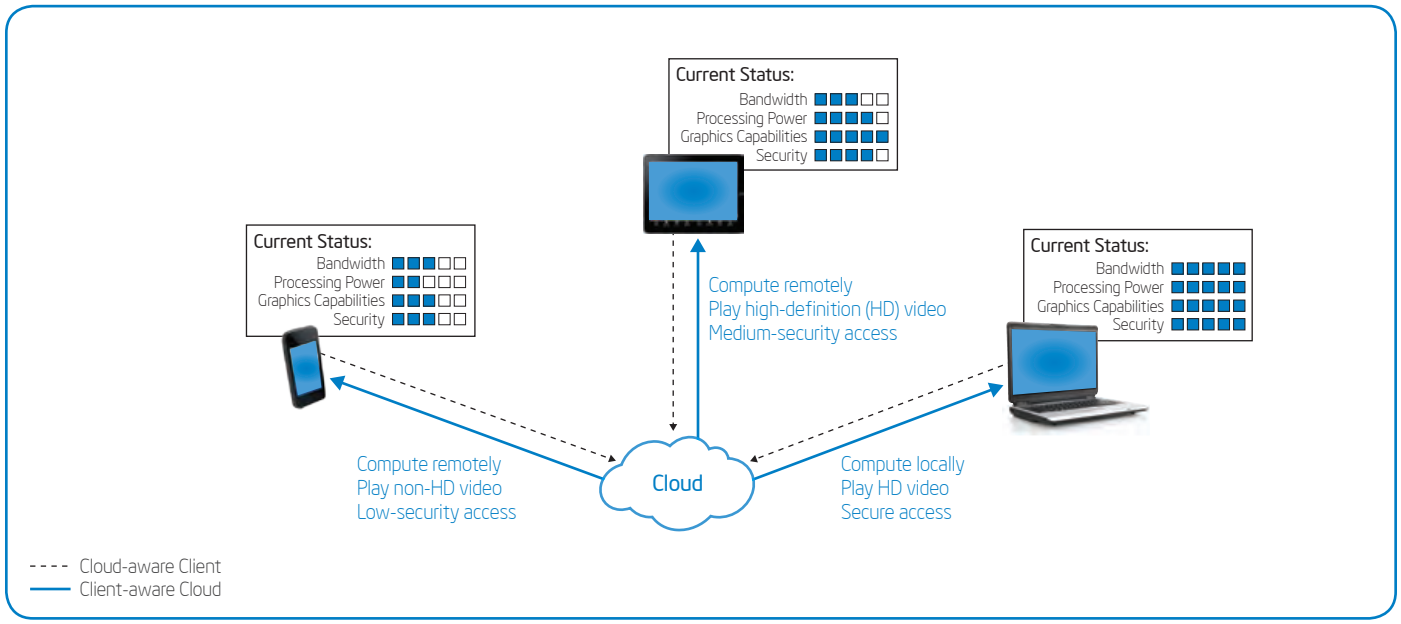

Figure 1. We are laying the foundation for a bidirectional awareness between the cloud and a client device that will enhance service delivery, user experience, and productivity.

INFORMATION SECURITY MODEL

We have found that security is of paramount importance in being able to fully embrace cloud computing and BYOD, and to seamlessly deliver services to a broad range of devices. We have radically redesigned our security architecture to enable different degrees of access. Our new security model is based on four pillars.

- Identity and access management. Intel IT has created a unique integrated trust calculation technology that enables us to support devices with differing levels of security. The system dynamically adjusts users' access privileges as their level of risk changes. For example, employees have less access to corporate information from personal smartphones than from corporate laptops.
- Security business intelligence. As we allow access to enterprise services from more devices, we need improved detection, monitoring, and analysis capabilities. We deployed a dashboard that provides detailed information about infected clients and servers, boosting our ability to intervene quickly and accurately. We also plan to add a predictive engine that will help improve our ability to respond to threats.
- Data protection. We are implementing technologies that protect data when it is created, stored, and in transit. We expanded the deployment of enterprise rights management software to nearly 20,000 employees, and we implemented data loss prevention technology to better track sensitive data as it moves through Intel.
- Infrastructure. We implemented secure trust zones within our enterprise private cloud that enable us to virtualize internally and externally facing applications with higher security requirements. As a result, we reduced malware incidents by 30 percent, despite a 50-percent increase in the number of malware detections in 2011.

DEVICE MANAGEMENT

A mobile device management (MDM) solution provides several important benefits with regard to BYOD. By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM helps reduce support costs and business risks, helping to enable the secure delivery of at least a limited set of services.

The main functions of an MDM solution are deploying software, including patch deployment and configuration management, enabling remote troubleshooting, and providing the ability to remotely lock and wipe a device.

MDM solutions also provide a cost-effective and efficient method for system maintenance, such as the ability to replace a corrupted or failed image with a working image. For example, at the beginning of a training session, an instructor can verify that all the classroom devices are functional and, if necessary, can quickly re-install the image on any non-functioning devices.

However, because our current MDM solution works only for devices that run mobile OSs and we must use a separate corporate management system for PCs, MDM does not resolve all of Intel's remote device management problems. For example, our MDM remote wipe capability doesn't work on larger form factors such as PCs. For this reason, we currently consider personally owned PCs to be at a lower trust level than some mobile devices, such as tablets and smartphones, unless the device's owner decides to opt in to corporate management capabilities.

WORKSPACE MOBILITY

Supporting BYOD devices raises challenges about how to make data available regardless of the user's location—whether at work, at home, or traveling—and how to deliver a consistent workspace across a user's many devices, whether accessing cloud services or locally installed applications.

To support a more portable workspace, we are moving away from our traditional model of locally installed applications to exploring how we can deliver more modular services to many different devices. One approach we have investigated is to separate the layers of the traditional tightly coupled solutions stack, a technique IT architects refer to as abstraction. By using virtualization to divide the platform, OS, application, user data, and user profile layers into separate services, we can set rules individually on each abstracted layer of the service.

Using abstraction we can determine whether, based on the type of device, user location, or other criteria, it's appropriate to deliver an optimal service to a particular device. For example, smartphones can access contact lists, calendars, and email services only; for tablets, we are investigating the feasibility of delivering an expanded set of business-to-business collaboration tools, such as note-taking and archiving services, instant video collaboration, and instant meetings.

Workspace mobility also raises the issue of how to synchronize cloud-based and local data. We are currently exploring how content synchronization may affect backup-and-restore processes.

Service Delivery Changes

Because our goal is to enable cloud-based services that take advantage of features on employees' devices, we need to act as a trusted advisor, providing employees information about a device, whether it's a smartphone, tablet, or PC. We encourage employees to consider how they want to work and where they want to work with each device. We then help them choose the device and OS that is best suited for their situation, helping them to be as productive as possible and to have an optimal user experience.

Employees can choose among many different devices with varying levels of capabilities. The availability of a diversity of user interfaces and screen sizes affects device and application interaction. Some devices do not have the features necessary to meet the minimum security configuration for even the lowest level of confidential data classification. Other devices can access certain data and services, but not others. A small subset of devices can access corporate data and services, with restriction.

With those factors in mind, it isn't possible to deliver a one-size-fits-all service delivery model that delivers the same set of services to every personally owned device. Nor is it practical to support every possible compute model and OS. For example, we limit our mobile device support to five mobile OSs; for BYOD computers, we currently support Macs* and plan to support Microsoft Windows*-based systems in 2012, but we do not plan to support Linux*-based systems.

To educate employees about which devices can access which enterprise services and which devices and OSs are best for certain work scenarios, we have created a web portal that provides a wide variety of information to employees enrolling in our BYOD programs.

BRING YOUR OWN PHONE

Table 1 shows a part of our web site that compares smartphone features, helping employees choose the best device for their situation. For example, if an employee's job requires good access to cloud-based business and Internet applications, as well as Wi-Fi* access and access to the Intel intranet, the chart indicates that a smartphone with OS #5 is the best choice. On the other hand, if an employee needs only calendar and contact information, any of the supported smartphones is adequate.

Table 1. Intel Employees Can Use the Information on Our Handheld Services Web Portal to Compare Smartphone Features

Feature	OS 1	OS 2	OS 3	OS 4	OS 5
Email	✔	✔	✔	Additional security software may be required, depending on the supported device	
Calendar	✔	✔	✔	✔	✔
Contacts	✔	✔	✔	✔	✔
Global Positioning System (GPS)		✔	✔	✔	✔
Wi-Fi* Allows you to connect to your home network or public Wi-Fi in airport or coffeeshop, and other areas	Varies	Varies	Varies	✔	✔
Internet Usability	Good	Varies	Varies	**Best**	**Best**
Internet Applications Examples: mapping applications, currency converters, and so on	Good	Good	Good	Better	**Best**
Intel Intranet Availability	Some Available	✘	✘	✘	Some Available
Business Application Availability Examples: Instant messaging, bridge speed dialer, and so on	More Available	Some Available	Some Available	Less Available	Some Available
Battery Life Standby or talk	**Best**	Good	Good	Good	Good
Global Roaming Capability	Varies by Rate Plan				
Tethering Connect your phone to your laptop and use the phone as a modem to connect to the Internet (like a wireless data card). Performance varies by phone model and service provider network speed	✔	Varies by Country or Service Provider			

✔ available; ✘ unavailable

BRING YOUR OWN COMPUTER

If an employee uses a corporate PC, they can expect certain capabilities, such as offline access to data, network connectivity, the ability to store Intel data on the PC, and disk encryption software and management agent software installed on the device. In certain situations, employees prefer to use their own Mac or PC, in which case, there are several options and a considerable number of trade-offs for the employee to consider.

The Participant Usage Model Matrix shown in Table 2 shows how we encourage employees participating in the BYO Mac and PC programs to think about how they will use a device so they can choose the best solution for their work environment. For example , using the chart, an employee who travels frequently and needs to store Intel data on the device can determine that the best choice is either the Intel build or client-hosted virtualization using a Type 2 hypervisor on a personally owned PC. For employees who work mostly onsite and simply need a companion device to quickly access standard applications, a personally owned tablet is sufficient.

Table 2. Participant Usage Model Matrix

	Server-Hosted Virtualization – Virtual Application Suite Browser-based Connection to Intel	**Intel Corporate Layer Installation** Special Build on Your PC	**Server-Hosted Virtualization – Desktop in the Cloud** Server-hosted Virtual Windows* 7 Desktop	**Client-Hosted Virtualization – Type 2 Hypervisor** Local Application on Your PC
	Secondary Companion Tablet	Primary Windows PC	Primary Windows PC	Primary Windows PC
Best Use Case Scenario	▪ Access to common applications, executed full screen ▪ Ability to copy and paste among virtualized applications	▪ Use standard applications and require high-speed performance	▪ Need a customizable desktop but don't want the Intel build ▪ Want to participate in both Companion Tablet and Primary programs	▪ Don't want the Intel build but want the ability to access Intel data and applications when not connected to the Internet
Works well for those enrolling in both bring-your-own Primary and Companion Tablet	✔	✕	✔	✕
I travel a lot and may have low bandwidth connections	Good	Best	Not Recommended	Better
I usually work on-campus or at home with a broadband connection	Better	Best	Better	Good
I frequently use rich media applications at work (video calls, 3D graphics, web-based training)	Not Recommended			
Offline Access	✕	✔	✕	✔
Network Connectivity	▪ **Onsite**: Employee hotspot ▪ **Off-site**: Your own broadband service	▪ **Onsite**: Direct connection to Intel network ▪ **Off-site**: Your own broadband service and VPN	▪ **Onsite**: Employee hotspot ▪ **Off-site**: Your own broadband service	▪ **Onsite**: Employee hotspot ▪ **Off-site**: Your own broadband service and VPN
Intel Data on Device	✕	✔	✕	✔
Disk Encryption Software Installed on Device	✕	✔	✕	✕
Management Agent Software Installed on Device	**Yes**. If you regularly access and manipulate IRS data, a specific mobile device management (MDM) solution must be installed	**Yes**. a specific MDM solution must be installed	✕	✕
Pluses	Need quick access to applications and occasional use	Similar to the standard PC offerings today, but it's your own PC and has the fastest network speed	Not a lot of IT overhead on the PC. Nothing installed on the PC	Your PC build remains intact, and the Intel environment runs as its own application on your system
Minuses	Only standard applications available	Some IT applications installed on your PC	Application performance can be slow	Large hard-drive space requirement

✔ available; ✕ unavailable

Application Development Changes

As more cloud-based software-as-a-service solutions solve more of our business problems, multiple vertical solutions could tend to fragment our core business data. To prevent this from happening, we are implementing a data and application virtualization framework that allows us to decouple our enterprise applications that follow more traditional software development methodology from many of our newer capabilities that demand a faster pace. This allows us to create assemble-to-order, cloud-based solutions by combining the capabilities of existing enterprise data and applications and integrating them with new capabilities.

The popularity of consumerization continues apace, with one in every four Intel employees now using smartphones. We are using the new virtualization framework to provide a broader set of business applications specifically designed to work well on mobile devices with small screens and limited features. About 28 applications are in the development pipeline, and seven applications are already in production: onsite navigation, corporate portal, shuttle and conference room scheduling, a speed dialer for dialing in to bridges, and collaboration and sales force productivity tools.

The new assemble-to-order application virtualization framework enabled us to deliver six of those seven applications to several mobile OSs in just a few weeks by re-assembling all business, data, and security services into an HTML5 solution.

CONCLUSION

There are parallels and interdependencies between IT consumerization, which provides employees with a wider range of choices for compute capability, and the advent of cloud computing, which offers businesses additional options for IT services. Intel IT is coordinating our cloud computing efforts with our BYOD initiatives, to enable Intel to reap maximum business value from both.

The availability of a diversity of user interfaces and screen sizes impacts device and application interaction, because not all devices have the same security features and performance capabilities. Therefore, we are moving away from a one-size-fits-all approach to developing and delivering cloud-based services. Instead, we are building foundational capabilities to enable a client-aware cloud as well as cloud-aware clients.

A client-aware cloud will be able to tailor services to the security level and performance capabilities of a particular device in a particular context, considering location, type of use, and other criteria. Conversely, cloud-aware client devices will be able to determine if the cloud is available and other information, such as how much bandwidth is available, and tailor client activity accordingly.

To bring this vision to reality, we are adapting our communications infrastructure, including redesigning our information security model, improving our mobile device management practices, and enhancing personal workspace portability capabilities. We also act as a trusted advisor, guiding Intel employees in their selection of a BYOD, helping them to select a device that will be able to best consume cloud-based services and enhance their productivity. We are using a new virtualization framework to provide a broader set of business applications specifically designed to work well on mobile devices with small screens and limited features.

In these ways, we are systematically building a private enterprise cloud that can determine device attributes and user preferences and optimally deliver services to a broad range of devices—including BYO devices.

FOR MORE INFORMATION

Visit www.intel.com/it to find white papers on related topics:

- "Best Practices for Enabling Employee-owned Smartphones in the Enterprise"
- "Enabling Emerging Enterprise Usages with Client-Aware Technologies"
- "The Future of Enterprise Computing: Preparing for the Compute Continuum"
- "Improving Security and Mobility for Personally-Owned Devices"
- "Pre-Evaluating Small Devices for Use in the Enterprise"
- "Why the Device Matters in a Cloud-centric World"

For more information on Intel IT best practices, visit www.intel.com/it.

ACRONYMS

BYOD	bring your own device
MDM	mobile device management

0612/JGLU/KC/PDF 327462-001US