IT@Intel White Paper
Intel IT
IT Best Practices
Cloud Computing and IT Consumerization
May 2012

Why the Device Matters in a Cloud-centric World

In our experience, more capable and powerful devices can provide a number of benefits, even when accessing cloud-based services.

Dave Buchholz
Principal Engineer, Intel IT

Doug DeVetter
Technology Evangelist, Intel IT

John Dunlop
Enterprise Architect, Intel IT

Executive Overview

As services and data move to the cloud, Intel IT has found that the end-point device is not only retaining its relevancy, but is also becoming even more important. This belief runs contrary to the industry assumption that the abstraction of service and data from the device makes the end-point device less relevant.

In our experience, more capable and powerful devices can provide the following benefits, even when accessing cloud-based services:

- Better overall user experience for maximum end-user productivity
- Enhanced support for the security and manageability capabilities that IT demands
- Best fit for emerging enterprise usage model requirements

We have identified three business use cases in which the choice of device (including the OS) and device features is critical.

- Bring-your-own device (BYOD). An increasing number of mobile devices in use at Intel are owned by employees. Through our web portal we provide guidance to these employees helping ensure they purchase appropriate devices for the enterprise environment.
- Client-aware cloud. Cloud service providers are increasingly offering rich Internet applications (RIAs), which distribute processing between the cloud and the client device and can take advantage of the device's hardware capabilities to provide better performance and a richer user experience.
- Device-to-device interoperability. We envision a continuum of computing devices, all of which will be able to seamlessly communicate with each other to share information and services. Only devices with adequate information security features and other capabilities will be able to take advantage of this new usage model in a corporate setting.

We are continuing to expand the guidance that we provide to end users in their choice of device, depending on the business use case for the device, to ensure they select devices with the appropriate set of capabilities and features.

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

More and more service providers—including Intel IT—are turning to the cloud for service delivery. There is a common misperception across the industry, as well as among end users, that the increased reliance on services delivered through the cloud means the end-point device is becoming less relevant.[1] In our experience, we have found that the opposite is true. As services and data move to the cloud, the end-point device is not only retaining its relevancy, but is also becoming even more important.

End users want to accomplish more and therefore require devices with increased capabilities. Instead of becoming smaller and simpler, with fewer features, devices are actually becoming more capable, with a flexible footprint and richer end-point computing capabilities. Additionally, the consumerization of IT is being driven by users who want to be able to refresh their devices faster than the typical enterprise refresh rate. As soon as a new model is released with new productivity features, users naturally gravitate to that new model.

The growth of cloud computing, along with the consumerization of IT, is driving Intel IT to support a compute continuum in which users will increasingly be able to access applications and services using a spectrum of client devices in a variety of form factors, including PCs, netbooks, tablets, and smartphones. The web is evolving to offer real-time, rich content, and users are spending more time online with devices ranging from PCs to tablets to smartphones. Intel IT is looking for ways to deliver services across the continuum of devices while offering an optimal user experience. Web development techniques such as HTML5; hybrid, native, and web applications; and client-aware capabilities offer the ability for IT to deliver robust services based on the capabilities of the client.

In 2010, we conducted a study that compared the performance of mobile business PCs to other types of end-point devices when accessing cloud services.[2] Our results showed that the choice of client device significantly affects the user experience. Of all the applications tested, mobile business PCs completed typical user operations up to 10 times faster than the other devices we tested.

We can extrapolate from our 2010 PC-based study that whatever the form factor and whoever the owner, more capable and more powerful devices will provide a richer user experience, which is something our end users expect for optimal end-user productivity. In addition, these types of devices are generally better equipped to provide the security and manageability capabilities that IT requires. Finally, emerging enterprise usage models will continue to push the capabilities of the end-point device.

BUSINESS USE CASES IN WHICH THE DEVICE IS IMPORTANT

In many cases, the cloud is a repository for data, but native applications provide the best user experience. For example, at Intel, documents are stored in our private enterprise cloud, but users prefer local computing for creating, editing, and viewing those documents while collaborating on a project. Even in situations where both the data and the service may reside in the cloud, a fully-featured device will be able to take best advantage of all service features and provide the richest experience.

We have identified several business use cases in which the choice of device based on its features is critical. These include:

- Bring-Your-Own Device (BYOD). As more users bring their personally owned devices into the enterprise, they need to know

[1] In this paper, the term "device" includes the combination of hardware, the OS, and locally executing applications.

[2] See "Cloud Computing: How Client Devices Affect the User Experience." Intel Corp., October 2010.

which features a device must have to support the desired enterprise services.

- **Client-aware cloud.** Rich Internet applications (RIAs) and HTML5-based web services will be able to determine the device's capabilities and deliver services tailored to that context. A more robust device feature set will enable expanded application functionality and a richer experience.
- **Device-to-device interoperability.** Advances in technology are making direct communication between devices more common. Even when the cloud is used to help pair devices that are not near to each other, both devices must have the necessary communication and security capabilities to enable this use case.

In each of these business use cases, several categories of device features determine the user experience and full functionality of services, whether they are cloud-based or native.

- CPU power
- Graphics processing unit power
- Connectivity, including near-field communication, Intel® Wireless Display technology, and Wi-Fi Direct*
- Storage and I/O capabilities
- Location-based services
- Sensor capabilities, including accelerometer, camera, and microphone
- Security features, including privacy protection, authentication, and encryption

The guidelines we provide assist end users in their choice of device, depending on the business use case for that device.

Influencing the Purchase Decisions of Personally Owned Devices

We launched our BYOD program in 2010 to allow employees to use consumer-based smartphones at work. We addressed many HR and Legal concerns, and consequently not all devices have access to the same services; their level of access depends mainly

Security Concerns Apply to All Use Cases

We have found that security is the linchpin of fully embracing cloud computing, IT consumerization, and the compute continuum. Therefore, we began a significant five-year redesign of our security architecture in 2010. We are developing a more flexible security model to enable degrees of access depending on dynamic trust and device capabilities. In 2011, we made significant progress in implementing this architecture.

- **Identity and access management.** We reached a key milestone by successfully testing our unique integrated trust calculation technology. This enabled us to embrace consumerization, including supporting 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 they do from corporate laptops. We tested this capability in our innovation labs across a broad range of devices, locations, and infrastructure technologies. Our next steps include an enterprise pilot in 2012, in preparation for enterprise-wide deployment.
- **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 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.
- **Privacy protection.** In addition to intellectual property protection, a primary concern is the protection of personally identifiable information. We specifically state in our bring-your-own end-user agreement that employees should maintain their personal data separate from the corporate data where possible, based on the type of device. On the Mac*, for example, we provide a way to separate corporate and personal data through the creation of separate partitions or containers, and the use of encryption. If a user has a question about what form of monitoring Intel IT is performing on personal devices, our Service Desk personnel can provide a specific and defined response in accordance with HR and Legal guidelines.
- **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. This removed a key barrier to achieving our goal of virtualizing 75 percent of our enterprise environment. We continue to evolve our infrastructure, detecting malware to minimize outbreaks and reduce active infections. As a result, we reduced malware incidents by 30 percent, despite a 50-percent increase in the number of malware detections in 2011.

on the capabilities of the device. Today these capabilities are very OS-centric; in the future we expect more attention to be focused on key hardware features that will enable more enterprise use cases.

To date, we support over 30,000 devices through our BYOD infrastructure. We support five mobile OSs and supply requested services to end-point devices only if the device meets our requirements for using that service. Our current BYOD program also includes support for personal Macs*, and we plan to extend support to personal PCs later this year.

The consumerization of IT is transforming the role IT plays across the enterprise, although the transformation is occurring more slowly in some segments (such as Manufacturing) than others. Instead of dictating what device, platform, OS, and services are available to users, we now educate users about the choices they can make. For example, if employees want to use their personally owned devices at work, we assist them in making a decision about what device to purchase to help ensure the device provides an optimal level of productivity and functionality while meeting IT requirements.

This helps employees make intelligent, data-based purchasing decisions instead of basing their decisions on only aesthetic factors such as the latest or trendiest model. We encourage employees to consider how they will use a device, both for personal use and for corporate use. For example, when considering a device to purchase, employees can ask themselves the following questions:

- The device can access the newspaper, but can it access corporate news?
- The device can stream consumer movies, but can it stream a training video to another device or to a TV?
- The device can display an online book, but can it display a corporate paystub?
- If the device is docked, does it have sufficient processing power to support a full suite of corporate productivity applications?
- Does the device offer the security features necessary to be useful both at home and at work? For example, some banks now allow digital signatures on documents sent directly from a device, if it is deemed secure. Similarly, Intel IT has firm security guidelines in place that describe what security features are necessary for a device to be fully trusted and therefore be granted access to appropriate corporate data.

To help users answer these types of questions, we have created a web portal that provides information to employees enrolling in our Handheld Services and bring your own computer (BYOC) programs. For example, Table 1 shows a part of the web site that provides smartphone feature comparisons, while the Participant Usage Guide shown in Table 2 on page 6 focuses on assisting employees in choosing the best solution for their work environment by encouraging them to think about how they will use a specific device.

In addition to meeting Intel's information security requirements, we have specific base minimum hardware and OS requirements for both our Handheld Services and BYOC programs, as discussed in the following sections.

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
E-mail	✓	✓	✓	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

REQUIREMENTS FOR BYO SMALL FORM-FACTOR DEVICES

We allow only specific mobile OSs that we have determined meet our information security requirements. Today we support five mobile OSs. In some cases, we restrict access to specific device models.

For smartphones and tablets, we provide users access to a number of handheld services. These provide enterprise applications directly to a device running a mobile OS. Typical services include e-mail, calendar, and contacts, and specific enterprise applications such as a travel expense tool and conference room scheduler.

We also offer tablet users an extended list of collaboration capabilities through the use of server-hosted virtualization. Tablet users have access to office productivity applications, Intranet access, and synchronous and asynchronous collaboration tools, such as data conferencing and instant messaging.

We require that various IT management solutions be installed on the device, depending on the security level of the device and the type of information being accessed. For example, a mobile device management (MDM) solution is required on certain smartphones in order to be able to access native e-mail with attachments; similarly, tablet users who need access to Intel restricted secret data for collaboration services also must install an MDM solution, which enables remote patch deployment, configuration management, troubleshooting, and device lock-and-wipe.

For smartphones, we require the following system capabilities:

- Encryptable OS
- Root or jailbreak detection
- MDM capabilities
- Device service partition for secure storage of enterprise environment
- PIN, password, and policy enforcement

Evaluating Consumer Devices for Enterprise Use at Intel

Many IT organizations are experiencing expectations from their end users to support additional types of consumer devices, technologies, and services. Many of these devices and technologies, while appropriate for personal use, pose corporate security, capability, and integration issues. These devices may also have usage models that are not appropriate for the corporate environment.

To date, we have reviewed several major consumer devices and evaluated their fit in our environment. These include consumer laptops and Ultrabook™ devices; consumer desktops and all-in-one systems; tablets, smartphones and other small form-factor devices; and consumer peripheral devices such as motion-sensing devices, wireless display devices, and streaming entertainment devices.

We also continue to explore several consumer-related software and service offerings, such as content synchronization services, social media, online collaboration tools, and device continuum services. IT is testing consumer technology in the enterprise ecosystem and testing enterprise technology in consumer settings.

In our evaluation of consumer devices, we considered usage models such as offshore development centers, call centers, and contingent workers to see which platforms might work in these scenarios. We also inform our end users of our requirements for device usage in the enterprise and what is currently available in the marketplace that meets our requirements.

Our evaluation revealed that many consumer-based systems lack the core capabilities and features that Intel IT requires to be able to deliver services to end-point devices securely and consistently. We have identified the absence of or limited availability of the following:

- Hardware-based management capabilities
- Stable platforms, such as that provided by the Intel® Stable Image Platform Program, and a reliable footprint configuration that is available worldwide.
- Higher-end components for displays, keyboards, cases, battery, ports, storage, and WLAN
- Higher-end directed I/O virtualization support, such as the support Intel® Virtualization Technology for Directed I/O
- Advanced capabilities such as Thunderbolt™ technology or USB 3.0
- Security controls such as Trusted Platform Module and Intel® Identity Protection Technology
- Efficient docking of the device to a workstation

In addition, our evaluation determined that most consumer devices are not designed for typical corporate use but instead are designed for a few hours of use per day in a less mobile environment. In particular, device keyboards are not designed for prolonged used, storage is not meant to sustain the I/O operations per second that corporate use generates, and the WLAN focus is on just a few personal access points (APs), not blanketed APs in an extremely mobile environment with several bands of wireless interference.

Integration of a wider range of consumer devices may become easier as consumer platforms suppliers begin to resolve these types of issues.

Many of these requirements are met today only with a native OS or with software on top of the OS. We continue to experience concerns associated with licensing, software differentiation across devices, and lack of hardware-based capabilities.

Currently, we are enabling BYO tablets using the same ecosystem as we use for smartphones. We have not experienced great demand from employees for more than phone-like services for tablets, but we continue to explore opportunities for tablets to supplement mobile business PC use at Intel. In addition, due to the portability and popularity of thin and lightweight consumer devices such as Ultrabook™ devices, we anticipate that in the next few quarters we will see a growing end-user demand to use these devices within Intel.

REQUIREMENTS FOR BYO COMPUTERS

For BYO Macs, we require a minimum hardware specification of Intel® Core™ i3, Core™ i5, and Core™ i7 processor-based MacBook Pro* and MacBook Air* devices to support the added performance footprint of a Virtual Machine Manager and a corporate IT virtual machine (VM). We then create a separate partition on the Mac to enable a corporate workspace, which can be used both natively and to run legacy applications through a Microsoft Windows* VM. We provide BYO Mac systems with access to a limited list of predefined applications, including office productivity applications, collaboration products, and intranet access. So far, fewer than 200 users are participating in the BYO Mac program.

We are planning for support of BYO PCs. For Microsoft Windows-based systems we will require the 2nd generation Intel® Core™ i5 processor or better, with either Windows 7 Professional or Windows 7 Ultimate, and with English as the base language. For access to our virtualization BYO solutions, the BYO systems must be equipped with a minimum of 4 GB of available RAM and Intel® Virtualization Technology. We also require the systems to have approved antivirus software installed. We are currently evaluating which services make sense and what capabilities we require on these devices to supply the services.

As shown in Table 2, users participating in the BYOC program have options for how services may be delivered to their PC. For example, they can choose an Intel build, server-hosted virtualization, or client-hosted virtualization. Each service delivery approach is associated with certain performance and convenience trade-offs, as well as differing levels of Intel IT support.

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	Not Recommended	Not Recommended	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

For our BYOC program, we realize that employee productivity is paramount; therefore, we offer a loaner Mac or PC in case a personally owned computer suffers a hardware failure.

Using the Power of the Client-Aware Cloud

Traditional cloud services are accessed through a browser; most of the code executes within the cloud. As a result, much of the industry assumes the cloud service is agnostic to the device that is accessing the service and that a web browser is the only requirement for accessing cloud services. There is also the assumption that all client devices can provide similar user experiences as long as they are capable of running a browser. However, end-point devices differ widely in their attributes, such as screen size and keyboard, and in capabilities such as performance, security, and portability. These attributes and capabilities can greatly affect the user experience.

Cloud service providers are increasingly offering RIAs, which distribute processing between the cloud and the client device as a way to improve application responsiveness and overall user experience. With RIAs, application code is transparently downloaded to the client device and executes on the client using an RIA software framework. The RIA can therefore take advantage of the client hardware to provide better performance and on-device capabilities, some of which are equivalent to traditional native applications. Because they execute locally on the client, RIAs also reduce the load on the network and on the cloud infrastructure.

Intel is investing in APIs that allow developers to write RIAs that detect real-time hardware information from the client, such as processor performance, battery life, and network bandwidth. Applications can use this information on a dynamic basis and remove the limitation of developing applications for the lowest common denominator.

Products exist today that can use this type of information to make intelligent decisions about what the user experience should be and how applications should run. Here are some examples of how RIAs can improve user experience and application performance:

- A web site delivers a multimedia version of the site to customers on a high-speed Wi-Fi network and a simplified version to customers on a weak cellular connection.
- A web site can query what graphics applications are installed locally, what type of CPU and screen size the device has, and how much free memory is available. The application can then use that information to determine whether to launch an advanced graphics editor or a simpler application with lower-quality graphics and less advanced graphic manipulation capabilities.
- A web application can sense if a laptop is plugged in and provide an error message if it is not.
- An e-commerce site can advise customers with full online shopping carts to check out because their laptop battery is running low.

Application development and deployment strategies for mobile devices are evolving to take advantage of device capabilities to provide for a better user experience. Developers and IT organization want to take advantage of end-point device capabilities in the hardware and OS to maximize the user experience, but they do not want to develop a separate version of an application for each mobile OS, due to the cost for essentially redundant work. As a result, HTML5 is rapidly emerging as a standard for mobile applications, because it allows a single application to run on multiple OS platforms while still taking advantage of device-side capabilities.

Intel IT has developed an architecture that includes web portals, hybrid-web containers, and native applications that can prescribe the right development approach, depending on application and use case requirements.

For maximum productivity, whether Intel IT is purchasing the device or the end user makes the purchase, it is important that the chosen device be able to take full advantage of the growing number of RIAs, both those external to Intel and those developed in-house.

Enabling Device-to-Device Interoperability

The cloud is essentially a repository, both for data and for services. For example, Intel's online applications store, the Intel AppUp^{SM} center, plays a vital role in our new services model. Intel IT provides hosting capabilities for a core function of Intel AppUp services and can respond quickly to spikes in consumer demand.

Although in certain situations sharing information using the cloud is the fastest and most efficient method, we envision a computing environment that allows devices to work together and share services through new interfaces and methods beyond the traditional cloud and web interface.

Consider the following scenarios—some are possible today; others we anticipate being possible in the near future:

- Securely provision one device and use it to enable capabilities on other devices.
- Use the capability of a device to sense the presence of and communicate with another device so that, for example, if a laptop user walks too far away from the laptop, the system automatically locks.
- Share the compute power of neighboring devices to display the video locally instead of having to upload a video to the cloud to enable viewing it on various devices.
- Transfer an entire training video, which could be hundreds of megabytes in size, from one device to another, using Thunderbolt™ technology. One port can provide high-definition video and the ability to move an entire movie in 30 seconds.
- Use a tablet to reserve the nearest conference room using client-aware services and sensors, easily set up collaboration, and display a presentation on the conference room's high-definition TV, using the device and Intel Wireless Display Technology.
- Partition the device to separate personal and corporate data, with the ability to back up each type of data to the appropriate public or private cloud, and the ability to easily—or automatically—switch between

home and corporate workspaces, based on device location.

- Wirelessly synchronize data between devices using a multi-gigabit speed wireless communications technology such as the one being developed by the Wireless Gigabit Alliance.

To be able to use these types of productivity-enhancing technologies, choosing the right client devices, especially in terms of the security features of both the sending and receiving devices, is important.

CONCLUSION

Because we believe the capabilities of the end-point device are paramount even when accessing cloud-based services, we are working to guide end users in their choice of device, depending on the business use case for the device. For example, through our web portal we provide information that allows employees to compare smartphone features, as well as answer questions that assist them in evaluating their work habits, travel and mobility requirements, and other expectations, and how various device options relate to these aspects of their work environment.

We have identified three business use cases in which more capable and more powerful devices can provide better overall user experience and optimal end-user productivity, enhanced support for the security and manageability capabilities that IT requires, and the best fit for emerging enterprise usage model requirements.

- BYOD. An increasing number of mobile devices in use at Intel are owned by employees, and it is important that employees purchase devices that are appropriate for the enterprise environment.
- Client-aware cloud. Rich Internet applications and other client-aware services can take advantage of client hardware to provide better performance and advanced capabilities.
- Device-to-device interoperability. Even when the cloud is used to help pair devices that are not near each other, both devices must have the necessary communication and security capabilities to support interoperability.

Even in situations where both the data and the service may reside in the cloud, we believe a fully-featured device will be able to take best advantage of all service features and best display results.

FOR MORE INFORMATION

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

- "Applying Client-aware Technologies for Desktop Virtualization and Cloud Services"
- "Benefits of Enabling Personal Handheld Devices in the Enterprise"
- "Best Practices for Enabling Employee-owned Smart Phones in the Enterprise"
- "Cloud Computing: How Client Devices Affect the User Experience"
- "Enabling Emerging Enterprise Usages with Client-Aware Technologies"
- "Enabling Smart Phones in Intel's Factory Environment"
- "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"
- "Preparing the Enterprise for the Impact of Alternative Form Factors"

ACRONYMS

AP	access point
BYOC	bring your own computer
BYOD	bring your own device
MDM	mobile device management
RIA	rich Internet application
VM	virtual machine

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

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 patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Printed in USA
0512/JGLU/KC/PDF

♻ Please Recycle
327236-001US