IT@Intel White Paper

Intel IT
IT Best Practices
IT Consumerization and IT Innovation
February 2012

Improving Security and Mobility for Personally Owned Devices

The presence of personally owned devices in the workplace or other environments such as schools and classrooms is a significant trend that transcends industry and geographical boundaries.

Dave Buchholz
Principal Engineer, Intel IT

John Dunlop
Enterprise Architect, Intel IT

Alan Ross
Senior Principal Engineer, Intel IT

Executive Overview

Intel IT has made significant progress in responding to the growing demand for use of personally owned devices, such as smart phones and tablets, in the Intel work environment. The presence of personally owned devices in the workplace or other environments such as schools and classrooms—often called "IT consumerization" or "bring your own device" (BYOD)—is a significant trend that transcends both industry and geographical boundaries.

In early 2010, about 3,000 Intel employees were using personally owned smart phones—this number increased to 17,000 by the end of 2011. These employees each gained an average of 57 minutes of productivity per day—an annual total productivity gain for Intel of 1.6 million hours.

Based on the success of supporting personally owned smart phones, we are working to expand our efforts to other models and more devices, including personally owned PCs.

- We have developed an end-to-end security model that calculates to what degree a personally owned device can be trusted and then dynamically moves users to the appropriate security level. This approach enables varying degrees of access and authorization to applications and data.
- We are also enabling workspace mobility—a concept for providing trusted access to applications and data "workspaces" from any device. With workspace mobility employees can enjoy a more consistent user experience across multiple devices—those that Intel provides as well as those they personally own.

We found that the business benefits of supporting personally owned devices include enhanced employee productivity and job satisfaction, reduced cost to the company of providing these devices, and greater business agility gained by the use of a wider array of usage model. These benefits far outweigh the costs associated with installing new infrastructure and controls necessary to reduce potential information security risks.

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

The increasing use of consumer devices, technologies, and usage models is continuing to shape employees' expectations about the work environment. Many employees are bringing their own computer, or tablet or other consumer device to the workplace, a trend referred to as "IT consumerization." Employees want to be able to perform their jobs using the platforms, applications, online tools, and services they choose. "Bring your own device" (BYOD) enables employees to choose the platforms and devices that best fit their needs, providing them with greater flexibility and ultimately making them more productive.

IT consumerization, especially the desire for BYOD, is a significant trend that both offers benefits and incurs expenses. In our experience, the benefits include the following:

- Enhanced employee productivity and job satisfaction
- Reduced cost to the company compared to the cost of providing the devices
- Greater business agility gained by the use of a wider array of usage models, many of which offer a greater degree of mobility

The expenses associated with BYODs include those related to developing new infrastructure and implementing the controls required to bolster back-end device support because of potential information security risks. However, we consider the benefits to far outweigh the costs.

In 2010, Intel IT worked closely with Human Resources (HR) and Intel Legal to define security and usage policies that allow us to offer secure access to Intel e-mail, contacts, and calendars from personal smart phones and tablets, enabling employees to use these as companion devices to their corporate mobile business PCs. By the end of 2011, about 17,000 employees were using personally owned smart phones at Intel and saving an estimated 57 minutes per day—an annual productivity gain for Intel of 1.6 million hours.

In implementing our BYOD program, Intel IT has evaluated several service-delivery models, and supporting technologies and policies, and we are continuing to expand our efforts to other models and additional devices. In 2011, some employees began using their personal Apple computers. On a Mac* we use partitioning to separate personal and corporate data securely and implement a virtualized environment on each system to support application compatibility. In 2012, using a similar approach, employees will be able to bring their own Microsoft Windows*-based PCs to work.

Overview of Best Practices

During the process of expanding support for personally owned devices in the Intel IT environment, we developed several best practices in the following areas:

- Human resources and legal considerations
- Device management
- Technical infrastructure
- Training

HUMAN RESOURCES AND LEGAL CONSIDERATIONS

Using personally owned devices in a non-personal setting—whether in the corporate or classroom environment—raises many privacy and policy issues. To address these concerns, we created an employee service agreement that employees must sign before using a personally owned device at work. This agreement covers Intel's expectations regarding appropriate use of a personal asset to conduct Intel business.

In the agreement we remind employees of specific Intel policies that they have

previously agreed to that still apply to the use of personally owned devices. These policies include a code of conduct, software licensing guidelines, and information security policy obligations. In addition, we call out specific data storage and backup requirements, and Intel's monitoring and audit rights.

We specifically state in the agreement that employees should maintain their personal data separate from the corporate data where possible, based on the type of device. We provide a way to segregate corporate and personal data on the device where possible, through the creation of either separate partitions or data containers, and the use of encryption. For example, on a Mac we create separate user accounts and expect users to store personal data in only their personal account. For some smart phones, where we do not have the ability to cleanly separate the data, we recommend through the service agreement that users back up their personal data regularly so that if a system wipe is necessary, they are able to access and restore the data.

Another core tenet of the agreement specifies that employees are not allowed to let other users of the device access Intel data or the device itself while it is connected to Intel's network.

The agreement also requires that employees be responsible for the support and maintenance of their own device. However, for a Mac or PC, Intel provides the employee with a loaner Windows laptop while a personally owned system is out for service, helping maintain employee productivity.

DEVICE MANAGEMENT

A mobile device management (MDM) solution acts as an important enabler of 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, enabling the secure delivery of at least a limited set of services.

BYOD: The New Reality for Enterprises and Education

Through conversations with customers and colleagues, it is obvious that IT consumerization and the desire to bring personally owned devices to the workplace or classroom transcends industry and geographic boundaries.

For example, Germany has a major government-sponsored initiative that enables all school children to have access to their own mobile computing device in school, during lessons, and at home. However, the national budget does not support governmental purchase of these devices. Therefore, "bring your own device" (BYOD) is a natural solution—research indicates 90 percent of German families have access to a PC in their homes.

Although a classroom environment differs in many respects from an enterprise environment such as Intel, there are similarities:

- Security is a top concern in both the enterprise and the education environments. For Intel, the primary issue with BYOD is protecting intellectual property and users' personally identifiable information, while in a classroom environment, the focus may be on protecting children from inappropriate content, preventing copyright infringement of digital publications, and preventing students from accessing sensitive administration data. In either environment, implementing an effective security model is paramount to a successful BYOD program.
- Both the enterprise and classroom environments can benefit from device configuration and service management, including implementing a mobile device management solution. This approach helps mitigate many of the security risks associated with BYOD and makes the management process more cost effective.
- Allowing expanded—but secure—access to data enables Intel employees to be more productive. In a similar manner, making educational content more accessible provides school children with greater opportunities to learn, independent of their physical location.
- Both businesses and schools must address the challenge of providing a consistent user experience, including access to data and applications, across a wide array of devices—a concept referred to as "workspace mobility." A lack of consistency results in confusion and frustration on the part of the end users and escalating support costs for IT.
- Supervisors and teachers share a concern that although Internet-enabled devices can enhance mobility and access to information, they may also tempt employees or students to spend too much time off-task. At Intel, we have found the productivity gains to be far more significant than the time employees spend browsing the Web.
- Controlling support costs is a major concern in both environments. Allowing the use of any mobile PC or device and any operating system can result in a multitude of different platforms with dramatically different capabilities. A better approach might be to define a set of required features and functions that limits the devices eligible for BYOD. For some situations, the list of devices might be limited to a selection of a finite number of different models.

Recognizing the important part that BYOD can play in education environments, Intel's World Ahead Program is working with governments worldwide on programs that increase access to technology. For more information, see http://www.intel.com/content/www/us/en/company-overview/world-ahead.html.

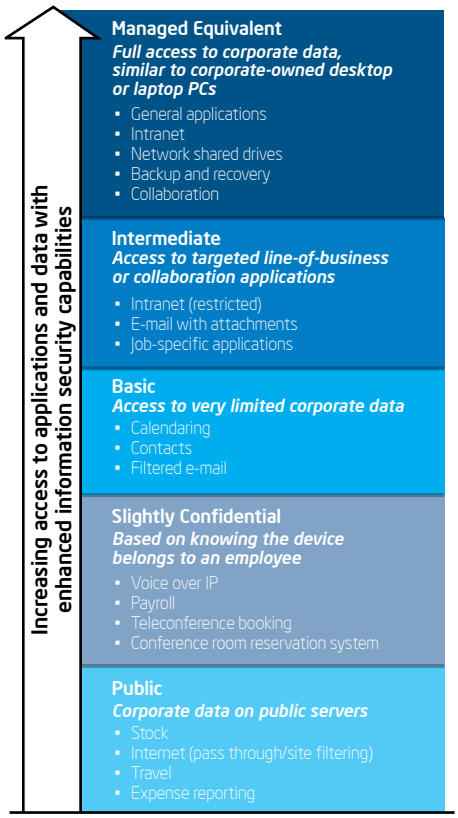


Figure 1. Varying levels of access help protect corporate data while allowing employees to use their personally owned devices at work.

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

MDM solutions 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 operating systems (OSs) and we must use a separate corporate management system for PCs, MDM does not solve 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 smart phones, unless the device's owner decides to opt in to corporate management capabilities.

TECHNICAL INFRASTRUCTURE

Supporting multiple devices and OSs requires several modifications, such as additional firewall controls, to our infrastructure. These adjustments are necessary because each OS has different security features, and some are more secure than others.

To support a broad range of BYODs, we are building an infrastructure that uses a flexible combination of delivery methods, including workspace and application containers, application and desktop virtualization, remote display technology, HTML 5, and web portals, to deliver services to a wide variety of form factors, including PCs and Macs, tablets, and smart phones.

To help prevent unauthorized or unintended use of technology that could raise licensing issues, we have implemented a managed virtualization infrastructure. Further maturation in the industry will help alleviate licensing concerns. For example, original equipment manufacturers of software could modify their licensing policies to allow corporate application and service use across both corporate and personally owned devices.

In our environment, we have found that it simply isn't practical to deliver the same set of services to every personally owned device because devices have varying levels of capabilities, and the availability of a diversity of user interfaces and screen sizes impacts 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. As shown in Figure 1, we have defined five levels of access, ranging from "Public," which offers no access to corporate data, to "Managed Equivalent," which allows full access to corporate data.

We also do not support every OS in our BYOD program. For example, for PCs, we currently support Macs and plan to support Microsoft Windows-based systems in 2012, but we do not plan to support Linux*-based systems; for smart phones we support five mobile OSs.

TRAINING

We have found that conducting training sessions is an important element of a successful BYOD program.

- **User training.** We train users about the content and ramifications of the employee service agreement. We also teach employees how to protect information on their devices. We explain unacceptable usages, such as peer-to-peer software sharing, and unacceptable behaviors, such as loaning a personal device that has access to corporate data to a family member. Focusing on behavior modification has helped us improve information security.
- **Service Desk training.** We maintain a list of frequently asked questions to guide IT Service Desk personnel in answering users' questions about the employee service agreement. For example, if a user has a question about what form of monitoring Intel IT is performing on personal devices, we've trained our Service Desk personnel to provide a specific and defined response in accordance with HR and legal guidelines.
- **Developer training.** We train our developers how to best develop applications and services for mobile OSs. We have created guidelines and technical documentation that explain data protection practices, authentication, and how to securely connect to the Intel network. We also help link developers with other resources. For example, we have a mobile application developer's forum where developers can interact with their peers and with experts both inside and outside of Intel.

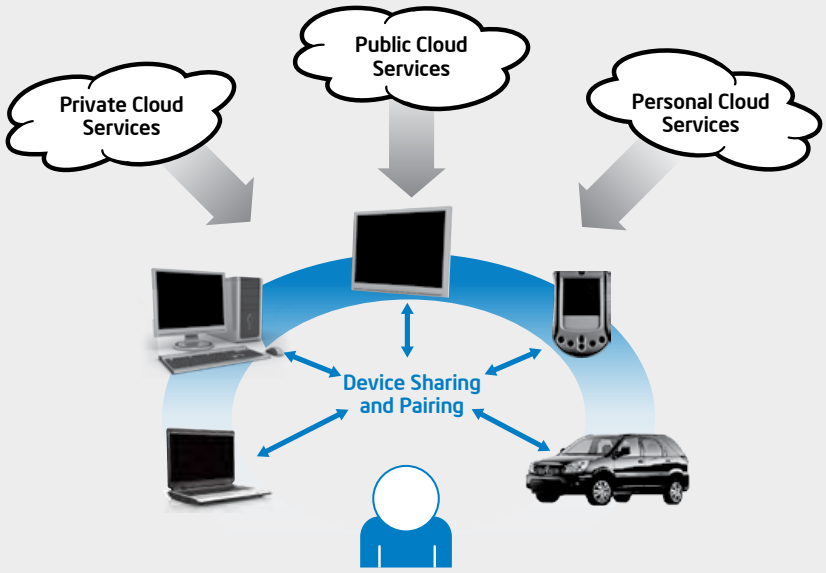
Enabling the Compute Continuum

The number and variety of connected devices in the marketplace is increasing every year. Intel envisions a Compute Continuum that provides a seamless, consistent experience across devices so that employees can access information anywhere, at any time. We are taking advantage of a range of new technologies and computing trends—including Internet connectivity, cloud computing, and virtualization—to make the transition to the Compute Continuum.

A key aspect of the transition is a shift toward delivering services across multiple devices instead of focusing on managing client hardware. The devices may range from mobile business PCs to smart phones, tablets, in-car systems, wireless displays, and projectors, as shown in the figure.

We anticipate that transitioning to the Compute Continuum, which is already underway at Intel, will be completed in three related phases:

- Supporting IT consumerization
- Delivering IT as a service
- Delivering the Compute Continuum, with increasing use of cloud-based services



The Compute Continuum. Devices work together to enable a common user experience.

TAKING BYOD TO THE NEXT LEVEL

Building on the successes we've already achieved with BYOD, we are now furthering our support of multiple devices through information security enhancements and enabling a workspace that remains consistent across many devices.

End-to-End Security

When we began planning the BYOD program, we realized our existing security model would not work with IT consumerization. We developed a new strategy that outlined what we would do and why, and a new architecture that described how and when solutions would be implemented. We also worked with strategic suppliers in order to build a supported approach.

Our new security model, which consists of four pillars, is a major breakthrough in dealing with the challenges associated with BYOD.

Our overall approach is not to secure the physical hardware, but rather to focus on the data that the hardware accesses and provide tiered services based on the security capabilities of the device.

The four pillars of our security model are summarized in Table 1.

The security business intelligence (BI) system includes an integrated security dashboard and common logging service that helps us put security BI into the hands of the users and also gives administrators and security operations the appropriate views to support investigations and other core security functions.

The new security BI solution is flexible and extensible, and offers several significant benefits to Intel:

- Improved granular controls and access methods
- More aggressive protection of intellectual property
- Increased flexibility for the user
- Increased employee productivity
- Support for new customer-driven usage models and faster adoption

SECURITY MODEL PROOF OF CONCEPT

We conducted a proof of concept (PoC) focused on user access to enterprise applications and data through multiple trust levels. The PoC demonstrated the effectiveness of differentiated trust establishment and enforcement with security BI. The PoC included 11 different devices and 8 different OSs. We tested devices and users both onsite and offsite.

The PoC showed that we can develop a fully integrated system that calculates trust and dynamically moves users to various trust levels. These trust levels can then be enforced on several gateways, exposing applications at the appropriate trust levels. We are developing a service deployment architecture that will move these capabilities into production in 2012.

Table 1. Foundational Pillars of Intel IT's New Security Model

Pillar	Description
Security business intelligence (BI)	Our security BI system uses device, user, and location information gathered from many sources, including the following: ▪ Mobile device management system ▪ Authentication and user registration processes ▪ Data protection tags ▪ Wide local area network ▪ Public key infrastructure This information is used to monitor, log, correlate, and predict information security threats. The system features enhanced reporting and real-time responses to threats.
Identity and access management	Using technologies such as federation, multi-factor authentication, and certificate services, we can control access to data by performing role-based trust calculations and managing access privileges appropriately.
Integrated infrastructure	We provide advanced protection and enforcement capabilities through endpoint security, network security, and a trust foundation. ▪ **Endpoint security.** Includes verifying system integrity, memory protection, system-call monitoring, and browser security. ▪ **Network security.** Includes an advanced sensor network, increased network access control, and a remediation and forensics environment. ▪ **Trust foundation.** Includes policy decision and enforcement, application gateways, and firewalls.
Data protection	Data tagging and encryption enable the protection to travel with the data because the system is platform- and network-aware. Our system performs real-time, intelligent monitoring and can provide a corrective response to protect data from unauthorized access attempts.

Workspace Mobility

Supporting multiple devices raises issues 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.

To support a more portable workspace, we are shifting 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.

This enables us to deliver an optimal service to each device or, when appropriate, not deliver a particular service based on device type, user location, or other criteria. For example, smart phones can access contact list, calendar, and e-mail services only; for tablets, we are investigating delivering collaboration tools, in addition to the services that smart phone can access.

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

WORKSPACE MOBILITY PROOF OF CONCEPT

We recently completed a successful PoC that tested different workspace mobility solutions for four use cases, summarized in Table 2.

We are now targeting certain workspace mobility solutions for limited production deployment, including private-mode virtual desktops and application presentation across multiple devices.

FUTURE PLANS

As we evolve our BYOD program at Intel, we will continue to enhance security and workspace mobility.

For security, future focus areas include the following:

- Determine a trust level for both the device and the user
- Perform additional work with different gateways and implement a single sign-on process to eliminate multiple logon procedures, user IDs, and passwords
- Extend our data protection strategies to include rights management attributes that can be enabled or revoked as needed
- Deliver applications that work across multiple trust levels with differentiated access capabilities
- Use location-based security to enable greater access from more trusted locations, such as on an Intel campus

For workspace mobility, we hope to expand available applications to include collaboration tools, our expense reporting application, Intel's intranet, and possibly other services.

In parallel with our BYOD program, we are building an enterprise private cloud with client-aware capabilities that can detect device type, capabilities, and other attributes; employee location; and preferences defined in user and device profiles. We are also assessing emerging enterprise usages and designing new solutions based on intelligent desktop virtualization and client-aware web services delivered through the cloud.

Table 2. Use Cases for Workspace Mobility Proof of Concept

Use Case	Description
Private Mode: Virtual desktop environment running on the back end in a dedicated manner	Each user has a dedicated container they can change and modify as necessary. These changes—including changes to the image itself, such as installing new software—are persistent from logon to logon. Standard applications are streamed into the container or may also be loaded natively.
Pooled Mode: Shared or pooled virtual desktop environment	Instead of private images, users are given a shared image that is one gold master used by several users. Applications are streamed into these environments based on user requirements, and where necessary we provide access to user data in the cloud.
Streamed applications	Applications are streamed into an encrypted, managed storage container. With this use case, we tested the feasibility of providing streamed applications in a secure manner on unmanaged devices.
Application presentation across multiple devices	This particular use case shows great promise across the enterprise because we can deliver services without having to engineer for each platform. We delivered the following components across any device: web browser session, office productivity software, PDF reader, and an interface to Intel's enterprise resource planning application.

CONCLUSION

IT consumerization is a significant trend that is transcending both industry and geographical boundaries. At Intel, we are already seeing significant benefits from the support of personally owned devices in our environment. These benefits include enhanced employee productivity and job satisfaction, and greater business agility achieved by supporting a wide array of usage models.

To further take advantage of these benefits, we have developed a security model that uses BI to calculate the degree to which a personally owned device can be trusted and then dynamically moves users to the appropriate security level. This approach enables varying degrees of access and authorization to applications and data. We are also enabling workspace mobility, a concept for providing trusted access to applications and data workspaces from any device, so employees can enjoy a more consistent user experience across multiples devices.

Our work with security BI and workspace mobility will enable us to expand our BYOD program to include more devices and models, including personally owned PCs.

FOR MORE INFORMATION

- "A Roadmap for Connecting Smart Phones to the Intel Wi-Fi* Network"
- "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"
- "The Future of Enterprise Computing: Preparing for the Compute Continuum"
- "Maintaining Information Security while Allowing Personal Hand-Held Devices in the Enterprise"
- "Pre-Evaluating Small Devices for Use in the Enterprise"
- "Preparing the Enterprise for Alternative Form Factors"
- "Virtualizing High-Security Servers in a Private Cloud"

ACRONYMS

BI	business intelligence
BYOD	bring your own device
HR	human resources
MDM	mobile device management
OS	operating system
PoC	proof of concept

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