WHITE PAPER
Intel® vPro™ Technology
Consumerization of IT

Thrive on Consumerization

How to manage the revolution and enhance user productivity

Do You Know What Your Users Are Doing?

Imagine that you could stand behind your users and watch for a day as they go about their business on their corporate PCs. You might not like what you see. Though it might not surprise you, it would probably cause you significant stress to watch user behavior on supposedly clean and secure corporate PCs. Through their browsers, users employ a variety of software and services to do their jobs, including services not vetted or controlled by corporate IT.

You might observe users like Karen—a participant in a study by Intel Insights and Market Research—who installed and used Dropbox*. She reported, “Our company file share drive is too slow and bloated, so we use Dropbox on the hush-hush.” Another technically adept user complained, “Don’t ask me to produce more and with greater speed and still slow me down with inflexible or outdated technology.”[1]

If users don’t get the tools and services they want from corporate IT, then despite your best efforts, users will go around you. Today’s tech-savvy users have high expectations for workplace technology—expectations shaped by their consumer computing experience—and they find ways to use non-managed services and devices to do their jobs. As a result, the once-clear boundaries between work and personal lives are increasingly blurred. Your management tasks are much more complicated than they were a few years ago because of the wide availability of non-managed services and applications and users’ eagerness to use those services and applications in their jobs. Additionally, users bring their personal devices to work, including laptops, smart phones, and tablets, creating a perfect storm of unmanaged technology with unpredictable effects. There is a term for this storm: consumerization.

Bring Order to Chaos

Consumerization is about much more than bring your own device (BYOD), which is what many people think of when they hear the term. More accurately, it refers to a set of trends that is transforming the way your users interact with technology in the workplace. As predictable and manageable tools, desktops and laptops have served the enterprise well for decades. However, the user’s computing environment now reaches far beyond the corporate desktop or laptop to include an ever-evolving mixture of technologies ranging from the corporate-provided PC to unmanaged web-based services and personal devices.

Table of Contents

Consumerization is a current hot topic in IT news, but it is not a new condition. It began in the mid-1990s with the wide availability of Netscape Navigator*, which opened the door to information and networks outside the managed enterprise network. Then Microsoft included Internet Explorer* with Windows* 95 Service Release 1, building the assumption of external connectivity into the operating system. Next, search engines, popular Internet service providers (ISPs), and web-based email meant people relied on the Internet for information and communication at home—perhaps even more than at work. This was a pivotal development because consumers saw what was possible with an Internet connection, and workplace IT departments have struggled to keep up ever since. Internet technology evolved naturally into what we see today: a large number of applications and services that are easy to install and easy to use. Users can now access these applications and services across multiple devices almost anywhere they go.

Consumerization introduces chaos into your carefully planned environment because it brings additional unknown variables. For example, you cannot manage a smart phone you do not see and cannot verify the security status of web-based services that employees use to store and share large files.

Some organizations resist consumerization and lock down the user experience in an attempt to minimize the chaos that comes from unmanaged devices and risky behavior.[2] However, fighting it is not your only option. You can also embrace consumerization as an opportunity to increase user productivity and job satisfaction. To seize this opportunity, you must reimagine your IT department's approach to client management. The traditional model, in which management is centered on IT's control of a monolithic Windows image on each PC, is ill suited to the realities of consumerization because the user computing environment has expanded beyond the traditional desktop.

DOES CONSUMERIZATION HAVE AN UPSIDE?

"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."[2]

Instead of resisting the consumerization trend and inhibiting user flexibility, what if you could manage and support the evolving user computing environment? What if you could secure users' computing environments while enabling freedom and mobility and delivering a consistent user experience on any device? When you change your management approach, you can bring order out of chaos by combining the control and manageability of Windows desktops with user freedom and the ability to be productive anywhere.

This change means you respond to consumerization with *consumerization of IT*—a proactive approach to managing the user computing environment. This new model is people-centered instead of device-centered because centrally managed context and policies are tied to users across environments and devices to securely enable productivity no matter where, when, and how users choose to work.

Which of These Top Challenges Are You Already Facing?

The reality of consumerization is simply this: personal computing in the workplace is changing dramatically, driven by technologies in users' consumer computing experience. Table 1 organizes these changes based on consumerization trends that you probably already face and discusses the management challenges associated with those trends. The table also suggests steps you can take to manage these challenges—steps discussed in more detail later in this paper. One important approach to have in your toolbox is *intelligent desktop virtualization*, or IDV. It is a desktop management model in which the traditional Windows image is divided into centrally managed layers that execute on intelligent PCs to provide a great user experience. The model also takes advantage of operating system–independent management capabilities to enhance management of these PCs. You will read more about IDV later in this paper.

Table 1. Management challenges associated with consumerization trends

TREND	WHAT IT MEANS	MANAGEMENT CHALLENGES	HOW TO MEET THE CHALLENGES
Consumer Behavior on Corporate-Provided Assets	▪ Users go around IT by using unsanctioned web-based services to do their jobs. ▪ Users install consumer applications and their own productivity tools, such as browsers and plug-ins.	▪ IT administrators cannot confirm the security state of web-based services. ▪ IT has little control over what happens to corporate data. ▪ Risky user behavior exposes enterprise data to threats from malware and data theft.	▪ Use IDV.
Bring Your Own PC or Apple Mac* (BYOC)	▪ Some users prefer to bring personal computers to work and expect IT to support them. ▪ Users mix personal and business data and applications on a single platform.	▪ Consumer-grade operating systems are not designed for IT management and can include undesirable or risky applications. ▪ Resistance to IT intrusion on personal computers can lead to tampering with agents and IT settings. ▪ IT administrators have trouble enforcing security policies. ▪ It is difficult for IT administrators to determine security state, patch state, and compatibility for unmanaged platforms. ▪ Management solutions must be reversible.	▪ Use IDV.
Bring Your Own Mobile Device (BYOD)	▪ Users conduct corporate business on their personal smart phones and tablets. ▪ Users expect constant connectivity and on-demand access to data and applications. ▪ Users mix personal and business functions on a single platform. ▪ Users want to maintain privacy and usability.	▪ The management framework for these devices is completely different from that of corporate-issued Windows* PCs. ▪ There is a large variety of mobile devices and operating systems, all of which support different management and security capabilities. These capabilities even vary between operating system versions. ▪ It is difficult to define and enforce policies that address the endless combination of devices, operating systems, and capabilities. ▪ IT administrators must determine the right level of management of the device according to each user scenario. ▪ Management solutions must be reversible.	▪ Deploy Mobile Device Management (MDM) or Mobile Application Management (MAM) solutions. ▪ Provide a native experience whenever possible.

How to Harness the Storm

You can take advantage of these trends and user behaviors through a user-centric approach to PC management. This approach combines the control and manageability of Windows desktops with user freedom and the ability to be productive anywhere.

User-centric management grows from three fundamental guidelines:

- **Execute locally on each device:** While you explore your options in the face of consumerization, remember that user experience is king. Users want a native experience—fast responsiveness, great graphics, offline freedom, and plug-and-play simplicity for all their peripherals. This native experience is best achieved on a PC when execution is local, where the compute resources are closest to the user. As an added benefit, local execution with media redirection in a server-hosted desktop environment improves the user experience and server virtual machine density, which lowers costs.

- **Divide the Windows image into flexible layers and deliver them intelligently to devices:** Consumerization complicates the traditional approach to desktops—which is to deploy and manage a monolithic Windows image on each PC. You can thrive with consumerization when you divide that image into a flexible series of layers, and then deliver those layers as services to a wide range of devices. For example, a Windows image could be divided into the following layers: operating system, applications, user settings, and data. This approach lets you centrally manage the layers from the data center while the image executes on the local device to ensure the best possible user experience. Users' changes to data are available to them no matter where they work because the data layer is synchronized between the data center and the local device. Many technologies from a variety of vendors are available to help you divide and manage Windows layers.

- **Use hardware-based capabilities to manage and secure devices:** Hardware-based management capabilities let you manage and secure PCs remotely, even if the operating system or software agents are unresponsive. For example, you can wake and patch PCs based on Intel® Core™ vPro™ processors remotely from the data center, even if the PCs are powered off.[3] Similarly, a PC that uses a type-1 hypervisor, or other bare-metal client virtualization solution, would allow you to remotely restore a PC's operating system layer if it became corrupted. These hardware-based capabilities can also enhance security. For example, you can remotely lock down a stolen laptop to protect sensitive corporate data, and can restore functionality if the laptop is recovered.

When you follow these guidelines, users can work when and how they like while you enjoy improved manageability and better security. Intel calls this user-centric approach IDV.

IDV does not prevent the chaos introduced by consumerization, but it helps you harness that user energy and drive it toward positive outcomes for the enterprise. For example, IDV does not prevent users from using web-based services. Instead, it supports user productivity with those services through local execution for the best possible user experience. IDV would not prevent a malware infection that was inadvertently downloaded from a website, but it would help the user easily recover from the infection. Or, with hardware-assisted remote management and security, you could quarantine the infected system and prevent the infection from spreading.

Similarly, IDV is not meant as a management approach for smart phones and tablets that are not running Windows. These devices fit within a different management framework than IT is used to. Additionally, the software components

WHY YOUR WINDOWS* TOOLBOX SHOULD INCLUDE LAYERS

When you divide the Windows image into centrally managed layers, you gain additional flexibility beyond the benefits of centralized management. Those benefits extend through each distinct layer:

Operating System

- Improve patch saturation by propagating changes from a single master image to multiple target computers.
- Maintain a pristine base image by locking down the operating system layer.
- Streamline help-desk operations by easily reverting the operating system layer back to its original state when user behavior disrupts it.

Applications

- Associate a distinct Windows application layer with users rather than devices.
- Deliver applications in a format that responds to context (device type, connectivity, security status, location, and so on).
- An isolated application layer helps maintain system integrity.

User Settings

- Separate users' personalization settings from the underlying operating system.
- Deliver the settings to any device for a consistent experience no matter where users access their Windows applications.
- Control settings at a granular level if necessary, based on policies you define.

Corporate Data

- Synchronize data between users' devices and the data center.
- Give users access to data across devices.
- Enhance user productivity by quickly restoring data on a different device if a laptop is lost or stolen.

of these devices are often already layered—applications run in isolation and do not affect the operating system in the way they do on Windows PCs.

IDV greatly simplifies the process of provisioning new desktops and updating those that are already deployed. When the desktop image is centrally managed as distinct layers, you can quickly assemble a golden image from its parts and deliver the image to target PCs over the network. This delivery can be optimized for speed and low bandwidth consumption with data deduplication technology. You can easily move a user's desktop to another device if it becomes necessary, thanks to centralized synchronization and storage of the desktop layers. Updates and other changes to the desktop image are simpler with IDV because you can make a change to the centrally stored image and then propagate it to the target PCs.

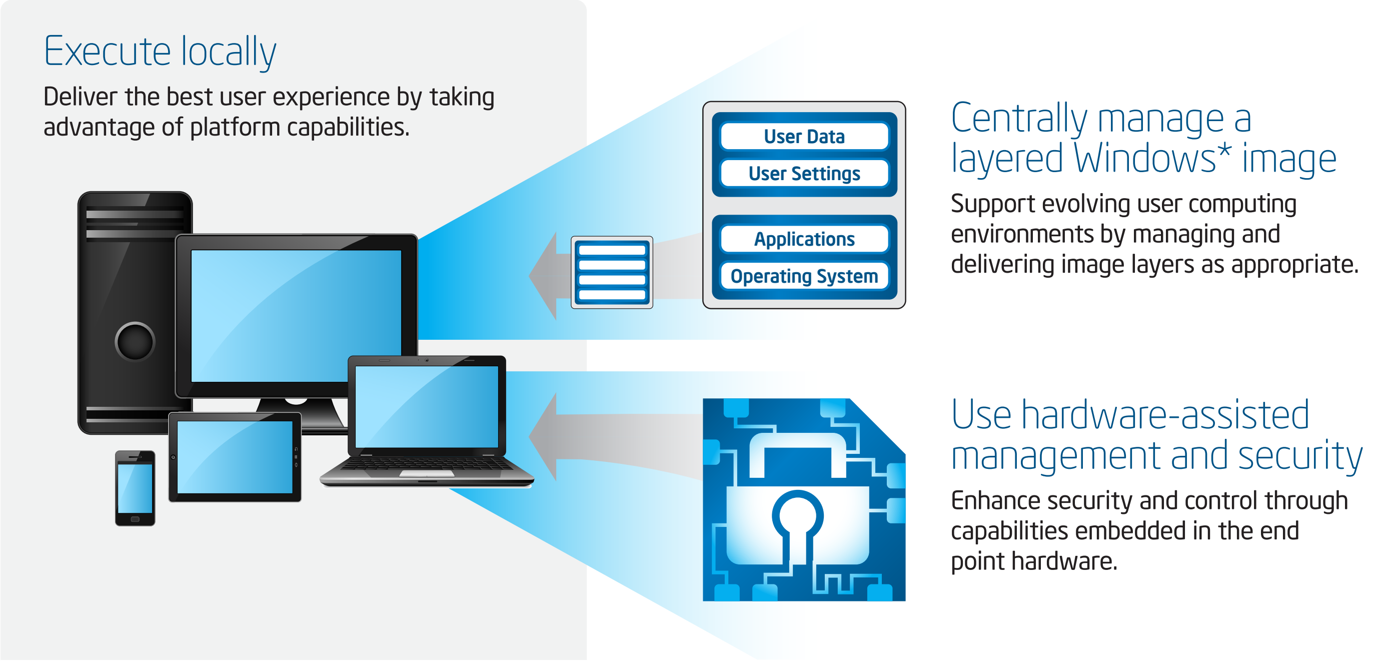
When you deploy solutions built on an IDV foundation, you can greatly reduce the old tension between IT's need for security and control and users' need for an unfettered user experience. Let's take a closer look at how you could apply these principles to manage and support consumerization rather than fight it.

Transformation Begins with Corporate-Provided PCs

The traditional approach to managing PCs has served IT organizations well for a long time. With that approach, each user gets a domain-joined PC running a corporate image that contains the software users need to do their jobs. The image also contains an enterprise-grade operating system that features settings, capabilities, and agents that give IT administrators a full range of options for troubleshooting, managing, and securing the PC. Intel vPro technology on corporate-provided PCs enhances these capabilities with out-of-band manageability and security features. Administrators could choose a light management touch that might include only an unalterable antivirus agent, or they could fully manage the computer and the user experience by locking down the desktop and preventing the user from making any changes.

However, consumer behavior on corporate-provided PCs complicates this picture. While your IT organization was once the only provider of vital services such as e-mail, file sharing, and collaboration tools, users can now access those services through their web browser outside of your control. Users want to, can, and should be allowed to use web services to enhance their productivity. IT organizations sometimes want to lock down the PC and prevent users from accessing these services, but this approach harms productivity and user satisfaction. It is a better choice to let go of some of that traditional control and embrace consumerization.

Because consumer behavior on corporate-provided PCs is the most prevalent form of consumerization, it is appropriate that your management transformation should begin here. In the consumerized environment, IDV guidelines can give you



Execute locally

Deliver the best user experience by taking advantage of platform capabilities.

Centrally manage a layered Windows* image

Support evolving user computing environments by managing and delivering image layers as appropriate.

Use hardware-assisted management and security

Enhance security and control through capabilities embedded in the end point hardware.

Figure 1. Intelligent desktop virtualization (IDV) is a user-centric approach to managing consumerization

more granular control than traditional PC management models while supporting user productivity everywhere and cushioning the chaos that consumerization can introduce.

For example, with solutions that follow the second guideline—centrally manage Windows layers—you can easily replace a corrupt operating system layer over a network connection without affecting the applications or user settings. Some solutions even allow user self-service: users can revert the operating system layer themselves, without IT involvement. This capability minimizes work disruption for the user, even when a new operating system is needed—a scenario that requires hours or days under the traditional PC management model. Because the operating system and application layers are isolated from each other, the operating system can remain stateless even when users behave like consumers.

When necessary, users can access their Windows applications and settings on tablets and smart phones because IT administrators can deliver those layers as services:

- Application virtualization solutions decouple applications from the underlying operating system, giving you a range of deployment options.
- User-state virtualization solutions keep user settings consistent across devices, supporting a familiar user experience.

Some image management solutions inherently layer the Windows image in the back end and deliver those layers to Windows desktops as appropriate. Layering is a powerful way to mitigate IT complexity. When you divide the Windows image into layers and centrally manage each layer separately, you can manage just one copy of Windows and one copy of each application. Some user-state virtualization solutions take advantage of the divided Windows image to centrally track and manage personalization settings so that users have a consistent Windows experience when moving from device to device.

You can significantly strengthen device and data security on corporate-provided devices by following the third IDV principle: use hardware-based capabilities to manage and secure devices. Hardware-embedded Intel technologies in corporate-provided PCs can encrypt sensitive data and support solutions such as two-factor authentication.[4] And the remote management capabilities of Intel® vPro™ technology help you keep PCs secure while reducing desk-side visits.[5]

You can follow all three IDV principles when you deploy PCs that use client virtualization. These PCs provide a native user experience because Windows still executes on the local device, and the hypervisor allows you or your users to deliver or modify specific layers of the Windows image without affecting other layers. This approach also gives you extensive control of the device through management and security features enabled by the hypervisor and built into the hardware of PCs based on Intel Core vPro processors.

Simplify Management of User-Procured PCs or Apple Mac* Devices

These computers complicate your job because they do not provide a management framework that works easily with established enterprise IT practices. Retail PCs running Windows 7 Home edition can't be domain joined and don't support Group Policy controls. Additionally, these computers likely contain consumer-grade hardware such as NICs not designed for enterprise use, less robust chassis and interior parts, and lower-end processors. They also typically lack the hardware-assisted management and security capabilities now widely available with corporate-provided PCs that are based on Intel Core vPro processors. Any management framework you impose on these computers must be transparent to the user and must be easy to remove when employees leave the organization or stop using the computer for work.

The IDV guidelines provide hints for managing these computers so that you can make them secure, productive parts of the user computing environment. For example, you could run a layered corporate Windows image on a type-2 hypervisor on top of the original, manufacturer-installed operating system. The corporate image would run locally in isolation from users' potentially risky behavior on their personal images, and the hypervisor would be easy to remove when necessary. If a dual–operating system setup is not ideal for your organization, you could deliver corporate data or applications in a secure layer that remains isolated from users' personal operating systems. The same data and application layers could also be made available on tablets and smart phones to help users stay productive. Look to application virtualization solutions to deliver this capability. Some ISVs enhance this approach with workspace-management solutions. These solutions can strengthen security and user flexibility by delivering centrally managed applications to users in the most appropriate format based on user context such as device state, operating system, work location, and many other factors.

How to Support User-Procured Mobile Devices

Users' mobile devices are quickly becoming important productivity tools. However, they require a management approach that is completely different from what administrators are used to with PCs. That management approach is complicated, in part, because one size does not fit all—you must choose correct management tools and security policies to fit varied and dynamic user scenarios. For example, the policies enforced on a locally based sales person's phone will be different from those on the phone of the CEO while she travels abroad.

To further complicate the management picture, a wide range of mobile devices is available. While these many devices run only a handful of operating systems, each device and operating system combination offers varying management and security capabilities. Even different versions of the same operating system have different options. Fortunately, however, all of these many mobile platform combinations (device plus operating system version) offer some degree of manageability and security. These capabilities are most often found embedded in the hardware and/or through operating system support for Microsoft Exchange ActiveSync* policies.[6] MDM and MAM tools take advantage of these capabilities and let you support mobile devices as a secure component of users' computing environments.

What Is Exchange ActiveSync*?

Exchange ActiveSync is an XML-based protocol used to provide secure access to corporate information on mobile devices. It lets users access their e-mail, calendars, contacts, and notes, while you can use its policies to manage and secure mobile devices and the information that lives on them. Listed below are just a few of the features that these policies can support:

- Remote lockout
- Remote wipe in case of mobile device loss or theft
- Device password requirements (such as minimum number or variety of characters)
- Phone and removable-card encryption requirements
- Prevent camera use
- Restrict or block wireless networks

Each mobile device typically provides native support for only a subset of available Exchange ActiveSync policies. Even so, you can use that subset to establish a minimum configuration that mobile devices must meet to access corporate resources. Again, one size does not fit all—you will need to carefully evaluate devices and operating systems and determine which Exchange ActiveSync policies each platform supports and tune your management approach accordingly.

Extend Exchange ActiveSync Reach with Mobile Device Management and Mobile Application Management

The most efficient way to fine-tune your management approach to mobile devices is to deploy Mobile Device Management (MDM) and/or Mobile Application Management (MAM) programs. They can extend the native management functionality of devices, such as by adding audit and reporting capabilities. Vendors' offerings in this space vary significantly, but in general, MDM and MAM mean the following:

- **MDM software helps you manage mobile devices.** MDM solutions typically install an agent on the mobile device to communicate with a centralized MDM server. These solutions extend the capabilities of Exchange ActiveSync by taking advantage of device-native management APIs to control device resources. For example, on iOS, MDM solutions can control access to iTunes* and the Apple App Store*. MDM solutions can be used to provision and install corporate apps over the air and can also control which apps the user can install and launch. Some MDM solutions even provide an isolated container on the device for business apps and data. MDM solutions can also enable other capabilities that are not natively supported, such as the ability to detect a jailbroken device.
- **MAM software helps you manage the applications that run on mobile devices.** MAM solutions focus on application management and are typically used by enterprises to develop custom applications with built-in management code so that IT can deploy, provision, update, and manage the applications. MAM vendors are beginning to work with third-party application developers to support MAM solutions' management APIs in third-party applications. MAM vendors also wrap an application with a management container that communicates with a central server for management purposes.

The differences between MDM and MAM software are becoming less distinct as the software matures, and a complete mobile-management solution includes aspects of both. Together, MDM and MAM tools give you granular control over devices and applications with little impact on user experience and without a heavy-handed disregard of user privacy. You will need to carefully evaluate solutions to find the best fit for your environment, but with MDM and MAM solutions you can support users' mobile devices with confidence. The ecosystem is mature and the solutions offer fine-grained options that meet your needs for manageability and security and meet your users' need to be productive anywhere.

Learn more about the manageability and security benefits provided by hardware-embedded capabilities found on 3rd generation Intel® Core™ vPro™ processors.

Visit http://intel.ly/L1MYxG

The Shortest Path to Success

While users commonly go around IT with self-procured hardware and services, most users would prefer to work on corporate-provided devices that deliver an outstanding user experience and provide the tools and services they need to do their jobs efficiently. Users want the freedom to use the emerging technologies they encounter in their personal computing lives.

Because corporate-provided devices already give IT the most management options, the shortest path to user satisfaction and IT manageability and security is to deploy Ultrabook™ devices based on 3rd generation Intel Core vPro processors and Intel® architecture-based tablets. Trained by the agility and sleekness of the consumer computing environment, today's workforce expects a form factor that is thinner and lighter than traditional corporate-provided laptops. Ultrabook devices offer a full-featured computing experience along with the style that is sure to appeal to most end-users.

Just as important, Ultrabook devices also deliver the security, manageability, and compatibility IT administrators require—especially models based on 3rd generation Intel Core vPro processors. Future models of Ultrabook devices will be convertible and include a detachable tablet. These 2-in-1 devices can exceed your users' expectations while helping you manage your organization's costs and risks through hardware-based manageability and security capabilities.

Embrace Consumerization to Enhance User Productivity and Simplify Management

You have heard the warnings about consumerization and have already begun to see it in your organization. Intel believes that enterprises can achieve greater long-term benefits when they embrace this trend than when they fight it. Consumerization represents a rare opportunity to transform the way business users work. This transformation enables greater user productivity and job satisfaction while giving you the control and manageability you need to efficiently manage and secure corporate data and assets.

This paper has given guidance to help you embrace consumerization. To thrive, you need to:

- Provide a native experience and execute locally whenever possible
- Divide the Windows image into flexible layers and deliver them intelligently to devices
- Extend your management reach using hardware-assisted capabilities to manage and secure remote devices

You can begin to manage consumerization today. Enhanced user productivity and IT manageability might be closer than you think.

Check out the tips and resources at **www.intel.com/desktopvirtualization** to get started.

[1] Quotes from Intel Insights and Market Research (IMR) Position Paper, "Consumerization: What's In Store?" July, 2010. Available http://www.slideshare.net/dellenterprise/consumerisation-whats-in-store.

[2] See "Improving Security and Mobility for Personally Owned Devices." http://communities.intel.com/docs/DOC-19277.

[3] (vPro) Intel® vPro™ Technology is sophisticated and requires setup and configuration. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more about the breadth of security features, visit http://www.intel.com/technology/vpro.

[4] These technologies include Intel® Identity Protection Technology, Intel® Anti-Theft Technology, and Intel® AES-NI. (Intel ® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on Intel® Core™ i5-600 Desktop Processor Series, Intel® Core™ i7-600 Mobile Processor Series, and Intel® Core™ i5-500 Mobile Processor Series. 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/. (Identity Protection) No system can provide absolute security under all conditions. Requires an Intel® Identity Protection Technology-enabled system, including a 2nd or 3rd gen Intel® Core™ processor, enabled chipset, firmware, and software, and participating website. Consult your system manufacturer. Intel assumes no liability for lost or stolen data and/or systems or any resulting damages. For more information, visit http://www.intel.com/content/www/us/en/architecture-and-technology/identity-protection/identity-protection-technology-general.html.

[5] Requires activation and a system with a corporate network connection, an Intel® AMT-enabled chipset, network hardware and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating or powered off. Results dependent upon hardware, setup & configuration. For more information, visit http://www.intel.com/technology/platform-technology/intel-amt.

[6] RIM BlackBerry* devices are an exception to this general statement. They are managed through BlackBerry Enterprise Server* rather than through Exchange ActiveSync policies.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Printed in USA 1012/JG/PRW/PDF ♻ Please Recycle 328023-001US