SOLUTION BRIEF
Federal Government
Citrix XenClient XT
2nd Generation Intel® Core™ vPro™ Processors

Secure, High-Performance Client Virtualization with Citrix XenClient XT* and 2nd Generation Intel® Core™ vPro™ Processors

A new high-performance virtualization solution for mobile and desktop PCs, jointly developed by Citrix and Intel, provides the highest levels of security, isolation, and auditability for federal agencies.

Together, Citrix XenClient XT* and PCs based on Intel® Core™ vPro™ processors provide:

- The ability to run multiple securely isolated environments on a single mobile or desktop PC
- Hardware-enforced security, including trusted boot and accelerated disk encryption
- Faster virtualization performance enabling a richer user experience, including high-performance 3-D graphics
- Simpler PC management
- Support for teleworking and COOP
- More secure information sharing within and across agencies

Today, federal agencies face an array of IT challenges, including the need to drive operational efficiencies in an increasingly complex environment. At the same time, they must secure their IT environments while supporting an increased emphasis on teleworking and continuity of operations (COOP).

Citrix XenClient XT* is a secure, high-performance client-hosted virtualization (CHV) solution designed specifically to meet agency requirements. The result of a strategic collaboration between Citrix and Intel, XenClient XT enables agencies to run multiple securely isolated environments on a single mobile or desktop PC.

Optimized for 2nd generation Intel® Core™ vPro™ processors, XenClient XT delivers new levels of virtualization performance and security by taking advantage of Intel®-based PC hardware capabilities.

Comparing Client Virtualization Models

Agency interest in virtualization for client computing is rapidly increasing due to compelling benefits made possible through emerging microprocessor technology and software that takes advantage of a new portfolio of hardware capabilities.

With all virtualization models, client applications and the OS run on a virtualization hypervisor and are abstracted from the underlying hardware. This helps make the agency workspace and data more accessible, portable, manageable, and ultimately less vulnerable to exfiltration and leakage.

Virtualization models include server-hosted virtualization (SHV), in which the client software runs on servers in a data center and is accessed by the user over the network, and CHV, in which the client software runs on the user's mobile or desktop PC.

Server-hosted Virtualization

With SHV, applications and data are stored and managed centrally, and delivered over the network to a broad range of computing devices. Because computing occurs in the data center, traditional SHV approaches have typically required additional IT infrastructure. However, even with this additional investment, users have been unable to run many graphical applications to their satisfaction. Newer technologies such as Citrix HDX* have mitigated this limitation, identifying and taking advantage of complementary PC hardware capabilities. For example, multimedia processing can be offloaded to PCs with 2nd generation Intel Core vPro processors, enhancing the user experience and reducing the burden on IT infrastructure. Despite advances, the operating model of SHV has not changed; it does not support offline computing, which can affect an entire agency if major network or data center failure occurs, or if the workforce is highly mobile. Because of these characteristics, SHV is most suited to agency employees with task-oriented roles who do not need to run mission-critical applications.

Client-hosted Virtualization

High-performance CHV technologies offer many of the same benefits that federal agencies expect from SHV, while offering additional capabilities to support multiple demanding applications and environments in a secure manner. Because client software executes locally on users' mobile or desktop PCs, users can run multiple CPU-intensive and graphical applications in separate, securely isolated virtual machines (VMs) on the same system. This meets the requirements of agency knowledge workers who handle sensitive information, run multiple graphical applications or may need to

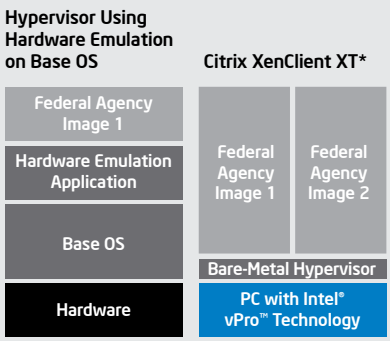
Citrix XenClient XT*: Secure Hypervisor Technology

Citrix XenClient XT* is a hardened bare-metal (Type 1) hypervisor. It runs directly on PC hardware using hardware-assisted virtualization, as shown in the figure below. This contrasts with previous Type 2 PC hypervisors, which used hardware emulation on top of a base OS.

With the Type 1 approach, XenClient XT can provide increased performance, a richer user experience, and greater security. XenClient XT lets local virtual machines (VMs) run at maximum performance and gives users a richer desktop experience.

XenClient XT provides the highest levels of VM isolation: Performance and security issues that occur within one VM do not affect the rest of the system. In contrast, with emulation-based virtualization solutions, if the base OS is compromised, the VMs running on top of it are subject to compromise.

Citrix XenClient XT* runs directly on PC hardware, optimizing performance and security.



do so in future, or work in a secure and/or mobile environment. The combination of XenClient XT and PCs based on 2nd generation Intel Core vPro processors also provides simplified management and hardware-enforced security.

Introducing Citrix XenClient XT

Citrix XenClient XT is a CHV solution that brings secure, high-performance virtualization to mobile and desktop PCs. With XenClient XT, government IT administrators can deliver multiple agency desktop environments to secure, isolated VMs that run directly on the XenClient XT hypervisor on employees' computers. (See the sidebar "Citrix XenClient XT*: Secure Hypervisor Technology.")

XenClient XT is specifically designed to address the challenges of agencies that require the highest levels of security, isolation, and auditability. To date, agency employees have often been forced to use multiple physical clients or customized systems to access multiple agency environments. With XenClient XT, employees can access multiple environments with differing security levels from a single mobile or desktop PC.

Together with PCs based on 2nd generation Intel Core vPro processors, XenClient XT provides the performance to support increasing demand for graphical and CPU-intensive workloads such as 3-D mapping, visualization of complex datasets, and multiple high-definition video streams.

XenClient XT simplifies deployment of new PCs, as well as hardware and software upgrades, because IT administrators can quickly deliver a new desktop environment or move an existing one to any new system running XenClient XT. Because the desktop and applications execute locally, employees are free to work online or offline with all the rich performance and user experience of a traditional computing environment.

Faster Performance and a Richer User Experience

The combination of XenClient XT with PCs based on 2nd generation Intel Core vPro processors provides unparalleled performance, resulting in a richer user experience.

At the heart of XenClient XT is a hardened bare-metal (Type 1) hypervisor, based on proven technology, that accelerates virtualization performance by running directly on the PC hardware.

XenClient XT delivers additional performance benefits by taking advantage of features in laptops with Intel® Core™ i5 vPro™ processors and Intel® Core™ i7 vPro™ processors, such as Intel® Virtualization Technology for Directed I/O (Intel® VT-d).

With XenClient XT and Intel VT-d, applications in VMs have dedicated access to Intel® HD graphics hardware, enabling near-native performance with hardware-enforced isolation for greater security. This eliminates the performance limitations experienced with some previous virtualization technologies, which prevented the use of some graphics-intensive applications or forced agencies to use multiple physical systems, each dedicated to a different application.

Now, agencies can securely run multiple 3-D graphics, analytical, or interactive applications on a single PC with excellent performance.

Simpler PC Management

PCs with Intel Core vPro processors dramatically reduce management effort by enabling consistent, remote management of PCs across the agency IT environment—even when users' PCs are powered off.[1]

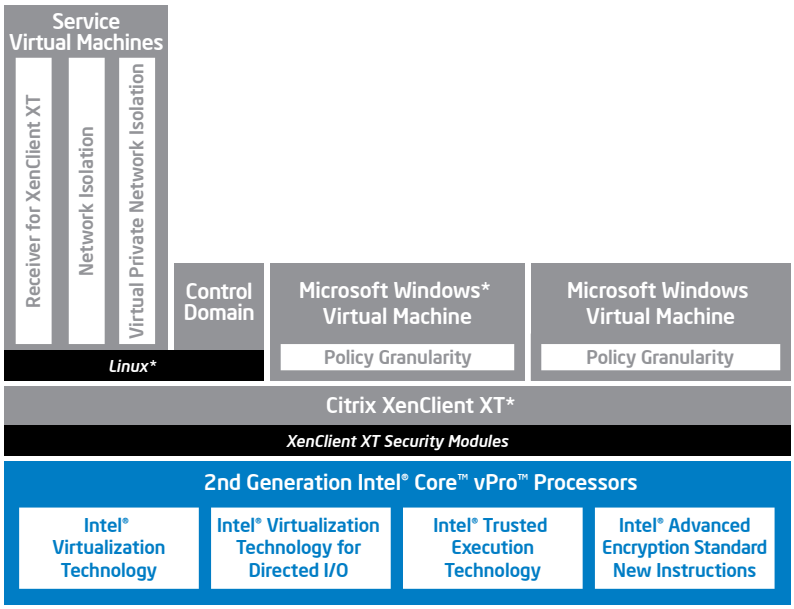
Additionally, agencies can seamlessly incorporate PCs with XenClient XT into their existing IT environments. With XenClient XT and PCs based on Intel Core vPro processors, a single image can be used across different PC generations or even across compatible PCs from different suppliers. This makes it much easier to manage an agency environment that includes PCs from multiple suppliers, to upgrade users to new systems, and to get users up and running again if they experience a laptop failure.

Enhanced Security

With XenClient XT, each VM running on a PC is completely isolated from the rest of the PC environment—preventing performance and security issues occurring within one VM from spreading to the rest of the system.

With this high level of VM isolation, XenClient XT can support multiple environments on one machine, as shown in Figure 1. This reduces

Figure 1. Citrix XenClient XT* enhances security by providing isolation between virtual machines and taking advantage of hardware-based capabilities of Intel® Core™ vPro™ processors.



management complexity for federal IT groups and makes it much easier for federal users to access multiple agency networks. For example, it can enable users to access networks with different security classifications from different VMs running on a single system. VM isolation can also be used to separate agency and personal data.

To deliver this enhanced security, XenClient XT takes advantage of hardware-assisted security features in PCs with 2nd generation Intel Core vPro processors. Key capabilities include trusted boot with Intel® Trusted Execution Technology (Intel® TXT), which verifies at boot time that the hypervisor has not been compromised—and blocks launch of the hypervisor and VMs if a compromise is detected. This helps to forge a chain of trust from the hardware up to the virtualization software.

XenClient XT includes a powerful disk encryption system that takes advantage of Intel encryption acceleration hardware to protect sensitive agency data without compromising performance. The software detects when it is running on an Intel Core i5 vPro processor or Intel Core i7 vPro processor and automatically enables acceleration of encryption and decryption operations by offloading them to Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI).

XenClient XT delivers additional protection by isolating network traffic into separate VMs, by providing enhanced policy granularity including the ability to lock down VM configurations, and by using access control technologies including Xen Security Modules.

Support for Teleworking and COOP

Local desktop virtualization with mobile PCs facilitates teleworking and COOP by enabling users to work more securely from home or while traveling.

Recent legislative initiatives (detailed at www.telework.gov) are helping to increase teleworking among federal agencies. Teleworking provides the flexibility

2nd Generation Intel® Core™ vPro™ Processor Family

Citrix XenClient XT* takes advantage of a collection of powerful manageability solutions powered by the 2nd generation Intel® Core™ vPro™ processor family, as shown in the figure below. Laptops with Intel® Core™ i5 vPro™ processors and Intel® Core™ i7 vPro™ processors deliver benefits to federal users and IT administrators including greater manageability, security, and performance.

Key features of laptops with the 2nd generation Intel Core vPro processor family can include:

Intel® Active Management Technology (Intel® AMT). This enhances PC manageability with hardware-based capabilities that let federal IT administrators better discover, heal, and secure PCs. Intel AMT provides dramatic cost and energy savings through out-of-band management, enabling functions such as remote troubleshooting and asset tracking even if PCs are powered off.

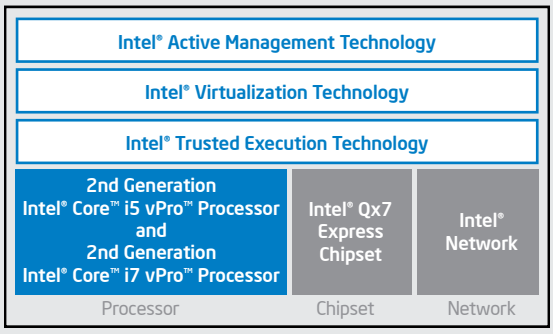
Intel® Turbo Boost Technology[2] and 4-Way or Greater Multitask Processing. These features increase performance. Intel Turbo Boost Technology allows processor cores to run faster when necessary. 4-way or greater multitask processing accelerates throughput when running a greater number of applications or threads.

Intel® Virtualization Technology (Intel® VT) hardware virtualization support.[3] OS virtualization is enabled by hardware support within the processor (Intel® VT-x). Additionally, support for Intel® Virtualization Technology for Directed I/O (Intel® VT-d) within the chipset accelerates graphics performance by enabling a virtual machine (VM) to gain dedicated access to the Intel® HD Graphics hardware. This enriches the user experience by allowing users to run highly graphical applications.

Intel® Trusted Execution Technology (Intel® TXT). This enhances security by helping to detect attempts to compromise the system. Intel TXT lets the hardware verify the integrity of the hypervisor on every boot.

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)[4]. This set of processor instructions implements complex and performance-intensive encryption and decryption steps in hardware. This provides significant performance gains over software-only encryption, enabling agencies to protect data using disk encryption with minimum impact to users.

Intel® Anti-Theft Technology (Intel® AT)[5]. This intelligent laptop security technology is included in PCs with selected Intel® Core™ processors. If a laptop is lost or stolen, a poison pill can be activated that renders the PC inoperable and useless to thieves.



U.S. Defense Intelligence Agency to Secure PCs with Intel® vPro™ Technology and Citrix XenClient XT*

The U.S. Department of Defense (DoD) Defense Intelligence Agency (DIA) has embarked on a multiyear program to deploy and use Intel® vPro™ technology to support multi-level security (MLS) capabilities on end-user PCs. Going forward, DIA looks to build on this by implementing a Type 1, bare-metal hypervisor client virtualization solution using Citrix XenClient XT*.

The DIA effort is motivated by the need to deliver a secure, cost-effective client environment for defense analysts. The DIA environment currently includes a disparate mix of devices, including thin clients, and supporting network infrastructures. This environment is inflexible and difficult to manage, and the client systems currently used by DIA intelligence analysts have limitations displaying computationally and graphically intensive applications at an acceptable resolution.

DIA initiated a search for newer off-the-shelf technologies that could enable analysts to better perform their work, and provide lower operations and maintenance costs compared to proprietary or customized solutions. The agency identified a need for new client technologies—specifically Intel® Virtualization Technology and Intel® Trusted Execution Technology—that can support virtualization in a trusted computing environment.

The initiative is designed to provide a single client device that eliminates the need for many distinct network infrastructures and provides a flexible, relatively low-cost solution that can help the agency fulfill its mission and more quickly respond to new threats.

for employees to work more effectively and achieve a better work-life balance while reducing impact on the environment. Teleworkers can perform officially assigned duties from wherever they can set up a virtual office—at home, a coffee shop, hotel, airport, or satellite office.

The U.S. General Services Administration found that the benefits of investing in telework far outweigh the costs. The return on investment (ROI) in the first year alone can reach 1,500 percent, and the cost of mobile technology is a small fraction of a typical IT budget. Agencies can also avoid costs for real estate and reduce existing facilities costs such as maintenance, heating, and cooling.

Implementing a teleworking program with mobile PCs is also an excellent way to implement and improve COOP, helping agencies prepare for faster response to natural or manmade disasters.

Improved Information Sharing Across Agencies

Information sharing between federal agencies is sometimes difficult due to incompatibilities or other differences between the networks or systems used at each agency. With XenClient XT, users can run multiple agency environments on a single system, enabling authorized users to more easily access information stored within different agencies.

Summary

The combination of XenClient XT and systems with 2nd generation Intel Core vPro processors addresses key IT challenges federal agencies face, including the need to efficiently increase support for telework and COOP. By delivering new levels of virtualization performance, security, and manageability, XenClient XT provides an ideal platform for transitioning from desktop to mobile computing.

Check out more solutions for government at: http://premierit.intel.com/community/ipip/fedgov

CITRIX®

intel®

1 Intel® vPro™ technology includes powerful Intel® Active Management Technology (Intel® AMT). Intel AMT requires the computer system to have an Intel AMT-enabled chipset, network hardware, and software, as well as connection with a power source and a corporate network. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to laptops, Intel AMT may not be available or certain capabilities may be limited over a host OS-based virtual private network or when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. For more information, see www.intel.com/technology/platform-technology/intel-amt/.

2 Requires a system with Intel® Turbo Boost Technology capability. Intel Turbo Boost Technology 2.0 is the next generation of Turbo Boost Technology and is only available on 2nd gen Intel® CoreTM processors. Consult your PC manufacturer. Performance varies depending on hardware, software and system configuration. For more information, visit http://www.intel.com/technology/turboboost

3 Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM). Functionality, performance or other benefits will vary depending on hardware and software configu- rations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/go/virtualization.

4 Intel® Advanced Encryption Standard-New Instructions (AES-NI) requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. 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/.

5 Intel® Anti-Theft Technology (Intel® AT). No system can provide absolute security under all conditions. Requires an enabled chipset, BIOS, firmware and software and a subscription with a capable Service Provider. Consult your system manufacturer and Service Provider for availability and functionality. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/ anti-theft.

Printed in USA 0611/RJ/KC/PDF ♻ Please Recycle 325339-001US