Today's users expect consistent, simple access to their applications and data to work productively from any device, anywhere, at any time. With the broad range of employer-provided and employee-owned mobile devices now in use, IT organizations are faced with the daunting challenge of ensuring that all company data and applications are fully protected and managed across each and every device and network.

IT organizations are expected to take a leadership role in enabling enterprise users with a secure and managed set of devices across any network. Citrix helps IT organizations meet these security challenges while enabling stronger user productivity with Citrix* XenClient*. Citrix XenClient extends the performance, flexibility, and security of desktop virtualization to mobile users on laptops, tablets, Ultrabook™ devices, and 2 in 1 devices by utilizing Intel® vPro™ technology to improve security and simplify IT management.

Citrix XenClient utilizes Intel vPro technology to provide highly secure client virtualization solutions that are optimized on Intel vPro processor-based devices.

Delivering a High-Definition User Experience with Intel® vPro™ Technology

Citrix XenClient delivers true bare-metal performance with secure isolation to run multiple local virtual desktops simultaneously. Together with Intel VMCS Shadowing, XenClient sits at the root hypervisor level and provides a secure platform for any other type of hypervisor to sit on. The result is a highly secure client virtualization environment that enables full productivity for users.

With XenClient, IT organizations can:

• Gain new levels of security, reliability, and control, as well as simplified desktop management.
• Increase security and control of the company environment with Advanced Encryption Standard, AES-256 full disk encryption with Intel vPro technology acceleration, USB filtering, remote kill, expiration, and time-based lockout on a secure client hypervisor.
• Extend the central management benefits of desktop virtualization with local execution so employees gain unlimited mobility with exceptional flexibility and productivity—even when disconnected from the network.

Citrix works extensively with Intel to optimize powerful technologies such as Intel Virtual Machine Control Structure (Intel VMCS) to deliver near-native performance and powerful security on 4th generation Intel Core™ vPro processors.

For example, Citrix and Intel are working together to improve nested virtualization with Intel VMCS Shadowing technology. XenClient delivers true bare-metal performance with secure isolation to run multiple local virtual desktops simultaneously. Together with Intel VMCS Shadowing, XenClient sits at the root hypervisor level and provides a secure platform for any other type of hypervisor to sit on. The result is a highly secure client virtualization environment that enables full productivity for users.

While this capability is available on any Intel vPro processor-based device, VMCS Shadowing technology is available on any 4th generation Intel Core vPro processor-based device.
Meeting Regulatory Requirements with XenClient XT

Citrix XenClient XT is an advanced client virtualization solution that leverages Intel technology by providing high assurance isolation and protection for sensitive computing environments that are subject to strict regulatory compliance laws, such as those found in government, finance, and energy industries. XenClient XT uses Intel Trusted Execution Technology (Intel TXT) to create a secure launch environment that protects against unauthorized changes to the hypervisor. When XenClient XT is installed, Intel TXT essentially measures the XenClient hypervisor and stores the known good value as a hash in the Trusted Platform Module (TPM). At each system boot, this technology measures the hypervisor and compares the result with the known good value. If the values are different, the system is not allowed to boot.

Extending Mobile Device Management to Intel Architecture-Based Mobile Devices

Citrix is now working closely with Intel to extend the key benefits of mobile management, including security and manageability of enterprise applications and data, to any Intel architecture–based mobile device with Citrix XenMobile*, one of the industry's most comprehensive enterprise mobile management solutions. With Citrix solutions such as XenMobile and XenClient, IT can secure data on Intel architecture–based devices running the Windows* 8.1 operating system, fully manage those devices, and certify that device users are trusted. Citrix XenMobile container technology separates business and personal applications and data into discrete mobile containers to protect both the enterprise and the individual user. This strategic segregation ensures all corporate applications and data are managed while also protecting any personal information residing on the user's device. XenMobile offers compliance for IT while giving users the confidence that everything on their Intel architecture–based mobile device is secure.

Citrix is delivering on the promise of a highly secure client virtualization solution and continuing to integrate Intel's technologies across its broad product portfolio. Our ongoing goal is to optimize security while ensuring a consistently rich and productive user experience on Intel vPro processor-based devices.

Additional Resources

To find out more about mobile devices based on the Intel® architecture, visit intel.com/mobileproductivity.

To learn more about Citrix® XenClient®, go to citrix.com/xenclient.

Share with Colleagues

Legal

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

Copyright © 2013 Intel Corporation. All rights reserved. Intel, the Intel logo, Intel Core, Intel vPro, and Ultrabook are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

1 Intel vPro technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit Intel.com/technology/vpro.

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

3 No computer system can provide absolute security. Requires an enabled Intel processor and software optimized for use of the technology. Consult your system manufacturer and/or software vendor for more information.

4 No computer system can provide absolute security. Requires an enabled Intel processor, enabled chipset, firmware, and software, and may require a subscription with a capable service provider [may not be available in all countries]. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your service provider for availability and functionality. For more information, visit Intel.com/antitheft. Consult your system manufacturer and/or software vendor for more information.