Intel IT Center

MAY 2012

Vendor Spotlight

Citrix* XenClient* Brings the Best of Desktop Virtualization to Mobile Users

Peter Blum, *Director of Product Management and Marketing, Citrix XenClient*

Peter Blum explains how Citrix XenClient extends the performance, flexibility, and security of desktop virtualization to mobile laptop users.

For our customers, it's all about mobility. The number of corporate employees using laptops continues to grow, and more importantly, the overall mobility of these users is increasing dramatically. Employees are taking sensitive corporate data off of the corporate network: They're on the road, on an airplane, working from home, or working from a customer location. Unfortunately for some, this leads to lost or stolen devices. Companies must make sure that data is backed up and protected, and they need to be able to disable these devices if someone is trying to break into them. They also need quick recovery from these events with minimum impact to user productivity.

Citrix set out to address these challenges with a flexible solution that meets the needs of these mobile users who are working both online and offline—and gives IT maximum control over security.

Delivering Flexibility and Security with Intel® vPro™ Technology

Citrix* XenClient* extends the performance, flexibility, and security of desktop virtualization to mobile laptop users by leveraging Intel® vPro™ technology[1] to help improve security and simplify IT management. This robust solution:

- Protects corporate data and applications with Intel Advanced Encryption Standard New Instructions[2] (Intel AES-NI), which encrypts data up to four times faster
- Enforces robust policy controls to block unauthorized movement of data from the laptop, such as copying data to a USB flash or optical drive
- Backs up user data unobtrusively and securely from any location

XenClient also gives users maximum flexibility by allowing them to run multiple copies of Microsoft* Windows* on the same laptop. One common scenario is a user running a corporate and a personal computing environment, where both are kept completely separate. IT is able to maintain full security control, and users get the freedom and flexibility of their personal computing environment without posing risks to the business.

This is made possible with two Intel vPro technologies. With Intel Virtualization Technology[3] for CPU (Intel VT-x), XenClient can efficiently virtualize Windows-based workloads with hardware-based support.

XenClient also leverages Intel Virtualization Technology for Directed I/O (Intel VT-d), which makes a virtual experience feel like a regular Windows-based laptop experience. Intel VT-d allows the virtual machine to have secure, direct access to the Intel graphics subsystem on the laptop so that users gain all the performance and 3-D graphics capabilities of modern operating systems like Microsoft Windows 7.

Finally, XenClient allows for image management, which is part of Intel's vision of Intelligent Desktop Virtualization. IT managers can use a single image of their corporate desktop to deploy, update, and roll back their distributed computing environments.

New releases of XenClient will definitely leverage the additional layer of security and performance of the 3rd Generation Intel® Core™ vPro™ processor.*

Protecting Classified Data: Citrix XenClient XT and Intel TXT

Citrix also offers an extreme security version of XenClient called Citrix XenClient XT, which was developed in cooperation with the U.S. Air Force Research Lab, and is specifically designed for high-security environments, such as those managing top-secret and classified data. XenClient XT leverages Intel Trusted Execution Technology[4] (Intel TXT) to create a measured, protected launch environment that guards against viruses, malware, and unauthorized changes. When XenClient XT is installed, Intel TXT essentially captures a snapshop of exactly what the software looks like. At each system boot, this technology verifies that XenClient XT has not been modified in any way.

Collaborating on the Roadmap to Hardware and Security Virtualization

We have an ongoing, collaborative partnership with Intel around our XenClient and XenClient XT technologies. Citrix has worked closely with Intel to develop and optimize XenClient based on Intel vPro technology, and we plan to continue that going forward. New releases of XenClient will definitely leverage the additional layer of security and performance of the 3rd Generation Intel Core™ vPro processor. Furthermore, Citrix will continue actively working with Intel on the future roadmap for hardware and security virtualization.

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

To download a free trial of Citrix XenClient, go to citrix.com/xenclient/tryit.

1 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, visit intel.com/technology/vpro/.

2 Intel AES-NI requires a computer system with an Intel AES-NI–enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. Intel AES-NI is available on select Intel Core processors. For availability, consult your system manufacturer. For more information, visit http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni.

3 Intel VT requires a computer system with an enabled Intel processor and 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/go/virtualization.

4 No computer system can provide absolute security under all conditions. Intel TXT requires a computer with Intel VT, an Intel TXT–enabled processor and BIOS, a chipset, Authenticated Code Modules, and an Intel TXT–compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit intel.com/technology/security.

Share with Colleagues

0512/JM/ME/PDF-USA 327294-001

Sponsors of Tomorrow.™