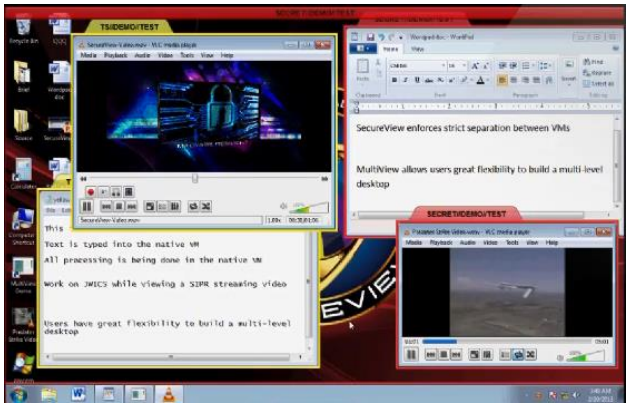
SecureView - Secure Multi-Level Virtual Platform

devastating capability, revolutionary advantage



- ***Run multiple environments securely isolated on a single mobile or desktop PC***
- ***Secure compositing of multiple domain application windows into a single desktop display***
- ***Hardware enforced security and isolation (Trusted boot and accelerated disk encryption)***
- ***Rich user experience including high performance 3D graphics***
- ***Simpler, more flexible, and more affordable than traditional Multi-level security solutions***

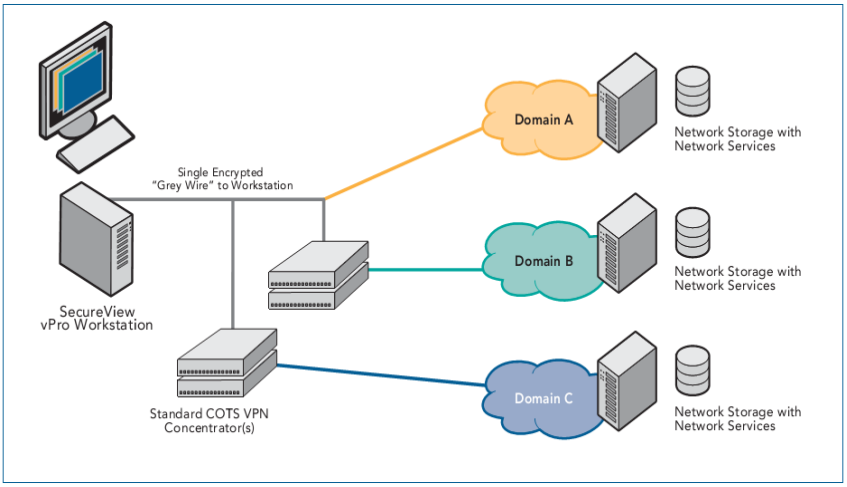
SecureView was developed for the Air Force Research Lab (AFRL) to affordably meet the stringent information sharing needs of the US Government without compromising data security and operational efficiency. As a hardened client-hosted virtualization solution, SecureView enables independent and concurrent access to multiple security domains. It provides performance that is independent of network bandwidth and server contention issues, providing analysts with consistent responsiveness for visually intensive analysis and collaboration. SecureView is NIST 800-53 certified as High in both Confidentiality and Integrity, and Medium in availability. It has been deployed to users at more than one dozen federal agencies as of November 2012, and is supported on numerous Dell and HP desktop and laptop models.

Benefits for Users

SecureView users have constant access to multiple domains, all with smooth performance, high-quality video and graphics. Each domain uses its original operating system environment, so migrating to SecureView is easy with minimal training needed. Productivity can be increased with secure window compositing, where multiple applications from multiple domains can be used from a single desktop view.

Benefits for Administrators

SecureView provides the flexibility of a server-hosted or client-hosted Virtual Desktop Integration (VDI). New security domains can be added as requirements change. In addition, SecureView is not a closed proprietary solution, since it is based on the Xen open source hypervisor and COTS hardware technologies. SecureView deployments can start small and grow enterprise-wide with the addition of central management via a synchronizer server.



A single SecureView workstation can securely connect to, and isolate, multiple backend environments.

Benefits for Information Assurance

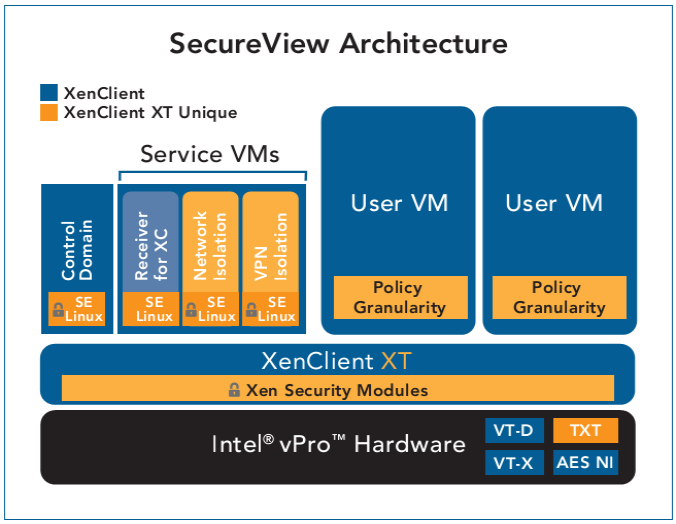
An encrypted, locked-down and measured desktop environment protects data, eliminates the instabilities and risks caused by user changes, and guards the system against malware intrusion. SecureView provides a trusted boot upon each start-up of the workstation, ensuring the hardware and software has not been tampered with or altered.

Benefits for CIOs

SecureView's lifecycle costs are lower than any other multi-level system on the market today. By allowing access to multiple enclaves from a single workstation, this significantly decreases each site's equipment footprint from desktop to data storage. SecureView provides a safe and secure environment for accessing the most secure of data, while remaining easy to use and straight forward to manage.

Architecture and Technologies

SecureView's foundation is based on Intel vPro and Citrix XenClient XT. These efficiently combine hardware and software to improve security, manageability, and performance of the client computing environment. The result is the ability to run standard desktop operating systems (Microsoft Windows and Linux) and standard desktop applications (Microsoft Office, etc.) from multiple security domain on a single desktop or laptop.



Hardware isolated VMs ensure security

Maintaining secure isolation is the #1 priority, and the following technologies are used to achieve this:

- Hardware assisted CPU and memory virtualization (Intel VT-x)
  - Eliminates need for complex, and error prone, software techniques in the hypervisor
  - Simpler and smaller hypervisor resulting in a smaller trusted-computing base
- Hardware assisted IO device virtualization (Intel VT-d)
  - Improved security and device isolation via hardware assisted DMA remapping
- Trusted boot of hypervisor and measured launch of guest VMs to ensure no software tampering
  - Trusted Computing Module (TPM)
  - Intel Trusted Execution Technology (TXT) enables a Dynamic Root of Trust

In addition, the platform has been hardened using custom software technologies and security best practices:

- Thin hypervisor to minimize code running with privilege (~150K SLOC) based on 64-bit open source Xen technology used in 85% of public infrastructure cloud environments
- NSA's Xen Security Modules for Mandatory Access Control
- Disaggregate and de-privilege functionality into dedicated Service VMs (Network stack, VPN, etc.)
- SELinux enabled and policy enforced in Service VMs
- Constrained communication interfaces between isolated virtualized components and no communications between users VMs
- All hypervisor device configuration state is encrypted (keys in TPM)
- Keyboard and mouse always securely routed only to current guest VM with focus
- NSA Suite B encryption for VPN and dual-sleeve VPNs via the NSA Commercial Solutions for Classified program architecture

Summary

SecureView has been architected, designed and carefully implemented to provide the state-of-the-art in security while maintaining cost effectiveness and ease of use. The system can handle a wide variety of applications from general office needs to performance intensive 3D graphics, each in different security environments, all running on a single virtualized COTS PC platform. Please contact AIS for more details on SecureView or to arrange a demonstration.

Hardware Requirements[1]
- Intel vPro (VT-x, VT-d and TXT) enabled desktops or laptops

Supported Guest VM OSes[1]
- Windows XP, Windows 7, Debian, and Ubuntu

Supported Peripherals[1]
- Most USB peripherals including SmartCard readers

Supported Remote VDI Clients[1]
- Citrix ICA, Microsoft RDP, and VMWare PCoIP

[1] – Support is continually changing. Please contact AIS for the latest information

The SecureView project is sponsored by the Air Force Research Laboratory (AFRL)

All information presented within this document was obtained from public sources (AFRL SecureView TCO Whitepaper and NSA Trusted Computing Conference Brief).