SecureView Overview

Updated 7 Oct 2013

Air Force Research Laboratory
AFRL/RIEB
afrl.rieb.secureview@us.af.mil
315-330-7658

SAF PA Case Number: 88ABW-2013-4408
The material was assigned a clearance of CLEARED on 17 OCT 2013

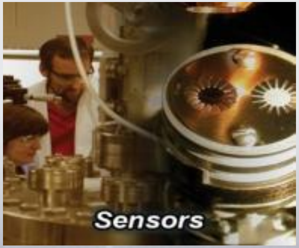
Powered by Citrix XenClient

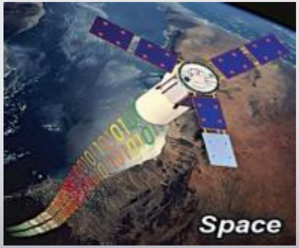
Overview

- About AFRL
- Background
- Architecture
- Features
- Hardware Support
- Programmatics
- MLS Comparison
- Summary
- POCs

AFRL Mission & Organization

Leading the discovery, development, and integration of affordable warfighting technologies for our air, space and cyberspace force





AFRL Rome Research Site in Upstate NY

750 on-site S&E team of scientists/ engineers

Dynamically formed research team ~3,700 collaborators

One of the world’s most diversified military research organizations, providing innovative technology for the nation

Distribution C. Distribution authorized to U.S. Government agencies and their contractors (Administrative or Operational Use) (01 Oct 2012). Other requests for this document shall be referred to (AFRL/RI, Rome NY)

AFRL/RIEB Background

Mission Partner Focused Technology Transition

Diverse – Direct – Respected

Mission Statement

Research, develop, transition and sustain leading-edge information technology solutions that deliver timely and secure intelligence information access, analysis, and dissemination capabilities to the Air Force and the Intelligence Community

- ***Intelligence Data Handling Systems* (IDHS) *Program***
  - Technology/products are used operationally throughout Department of Defense and Intelligence Community
- 40+ Year legacy of applying leading edge technologies to provide secure, affordable and sustainable IT solutions
- General Defense Intelligence Program (GDIP) resources represent the core of the IDHS manpower/program resources

A History Of Innovation…

- CATIS/IESS
- IPL
- XIDB/MIDB
- ISSE Guard
- CSE-SS
- JEDI
- CD-ROM
- MTIX
- Personalized Assistant that Learns (PAL)
- DTW
- WebTAS/CIDNE
- DRP
- JTT
- Collaboration Gateway
- Latex Paint

Current Focus Areas

Data Survivability

- AF JWICS Disaster Recovery

Cross Domain Collaboration

- Collaboration Gateway (CD Chat, V2CDS)

Multi-Level Security

- ISSE Guard
- SABER Multi-Level Thin Client
- SecureView Multi-Level Virtual Platform
- JEDI Security Lockdown
- DoDIIS Cross Domain Mgmt Office (DCDMO)

Data Access & Apps

- WebTAS Toolkit (incl CIDNE, CEP)
- Info for Op & Tactical Analysis (IOTA)
- Automated Virtual Intel Prod Spt Sys (AVIPSS)
- Databases for the 21st Century (DB-21)
- Modernized Integrated Database (MIDB)

Messaging

- Messaging Infrastructure Services & Tools for the IC (MISTIC)

Targeting Automation

- Joint Targeting Toolkit (JTT)

Solutions Globally Deployed – 100K+ users

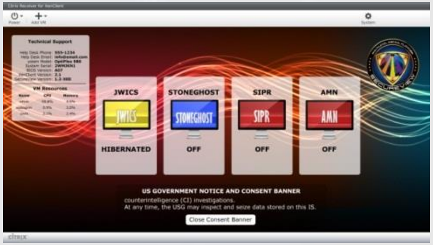
Certification Efforts

Product	TSABI	SABI	UCDMO Baseline
ISSE Guard 4.0	✓	✓	✓
SABER 4.3.1	✓		✓
Collaboration Gateway 2.0	✓	**ST&E Apr 13**	✓
MLDBR	✓		✓**1**
SAWES	✓	**~Fall 13**	✓
DTW 4.1.1	✓	✓	✓
Multi-Level Print Server (MLPS)	✓		✓**2**
SecureView 1.2	✓	**~Fall 13**	✓

1-As part of ISSE 2-as part of DTW

SecureView – What is it?

- **SecureView is a low-cost MILS (Multiple Independent Levels of Security) workstation based on COTS technology.**
  - **Runs on any Intel vPro personal computer**
  - **Based on a "Type 1" or bare metal client hypervisor (Citrix *XenClient* XT)**
  - **Single or multiple wires to desktop**
- **Allows a single computer to host multiple guest virtual machines (VMs) running at different classification levels.**
- **Supports Windows, Linux and Solaris guests**
- **Supports both rich and thin client computing models**



Technical Support

Help Desk Phone: 555-1234
Help Desk Email: info@email.com
System Model: OptiPlex 980
System Serial: [illegible]
BIOS Version: A07
XenClient Version: 2.1
SecureView Version: 1.2.000

VM Resources

Name	CPU	Memory
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]

US GOVERNMENT NOTICE AND CONSENT BANNER

counterintelligence (CI) investigations.
At any time, the USG may inspect and seize data stored on this IS.

vPro: Intel CPU technologies that enable management features such as monitoring, maintenance, and management independent of the state of the operating system.

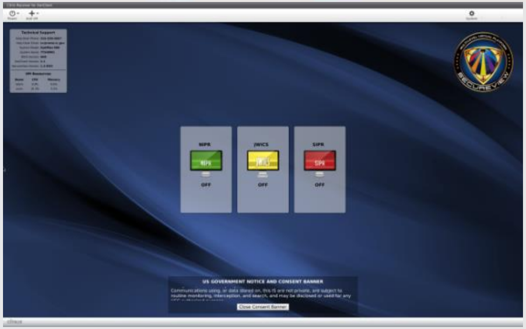
Type 1 hypervisor: A native, bare metal hypervisor which runs directly on the host's hardware to control the hardware and to manage the operating systems which run on a level above the hypervisor.

Background

- ODNI CIO requested AFRL/RI develop a secure & robust MLS workstation for the Intelligence Community and DoD
- Levied extraordinary security requirements
  - *Must handle highly-secure/sensitive data and information*
  - *Zero tolerance for data exfiltration*
- Minimal impact to host agency
- Support high-performance applications
- Rapid provisioning (4 hours)
- Required rapid delivery (<10 months)

The Solution

- Over a dozen solutions analysed over a 6-month period
- “Type 1” client hypervisor architecture selected
  - Based on Citrix’s XenClient
  - AFRL worked very closely with Citrix to modify and enhanced basic Xen architecture, resulting in XenClient XT
  - Added “GOTS” enhancements
- “SecureView” is the Government program that utilizes XenClient XT as the basis for a Multiple Independent Levels of Security (MILS) workstation
- XenClient XT is now a COTS product and commercially supported by Citrix.



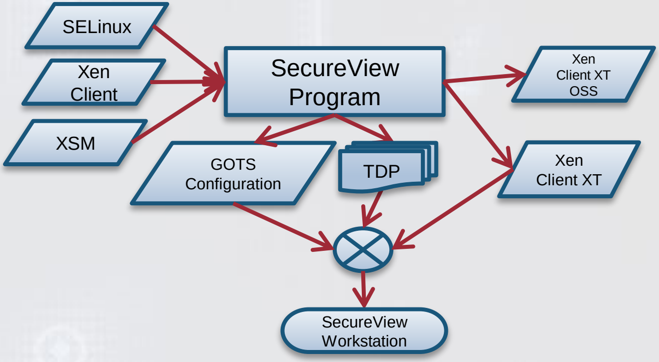
US GOVERNMENT NOTICE AND CONSENT BANNER

Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any

SecureView

Government – Industry Collaboration

- AFRL, Intel, and Citrix kicked off a partnership early 2010
- Intel & Citrix have provided the Government an unprecedented level of cooperation
- Collaborated with Intel on SMI Transfer Monitor (STM) specification
- NSA has provided guidance (HAP PMO) and testing (I733) resources
- Dell & HP have provided access to BIOS, firmware, and STM collaboration



SELinux

Xen Client

XSM

SecureView Program

Xen Client XT OSS

Xen Client XT

GOTS Configuration

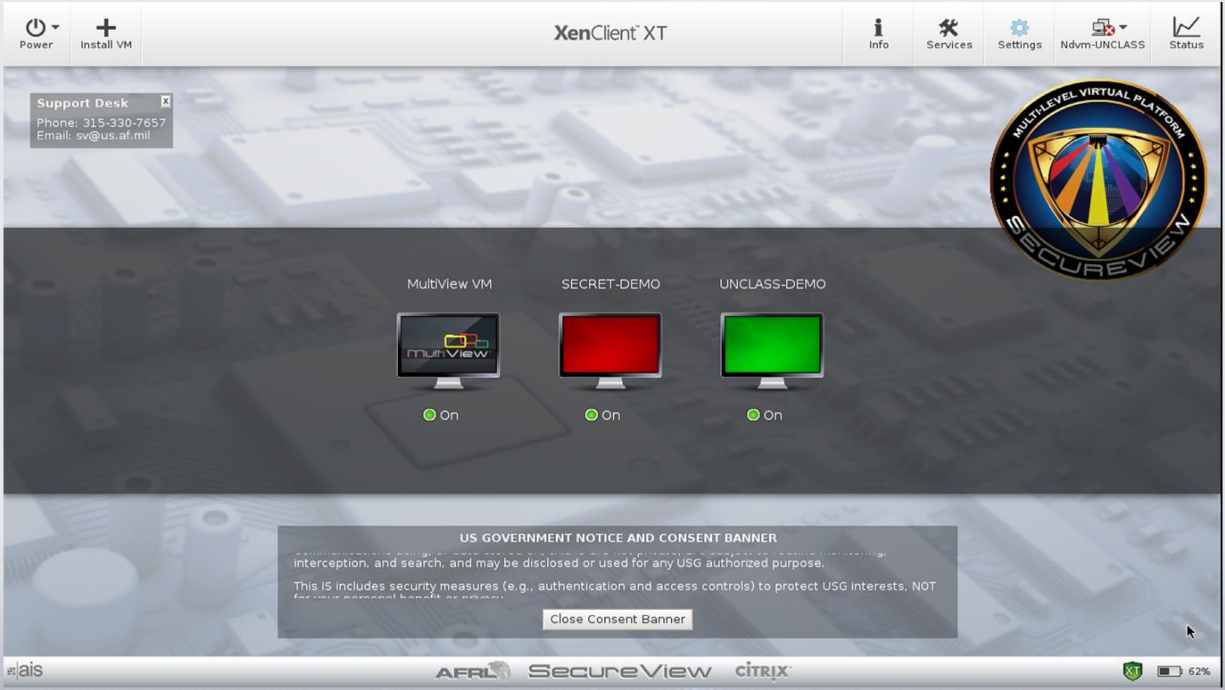
TDP

SecureView Workstation

Why Xen?

- The Xen.org Open Source Development Community
  - Hundreds of developers, many companies, universities and other organizations
  - More than 25,000 code submissions in Xen 4.0
- >85% of the Public Infrastructure Cloud runs on Xen
- Used in servers, desktops, laptops, storage appliances, network appliances, PDAs, and smart phones
- Runs multiple independent VMs *with policy controlled information flow*
  - Enables MILS systems
  - Enables out-of-band management & policy enforcement
  - Control removable media access, image update, backup, and attestation
  - “Thick” or “Thin” mode of operation

SecureView (Login Screen)



Support Desk
Phone: 315-330-7657
Email: sv@us.af.mil

MultiView VM	SECRET-DEMO	UNCLASS-DEMO
● On	● On	● On

US GOVERNMENT NOTICE AND CONSENT BANNER

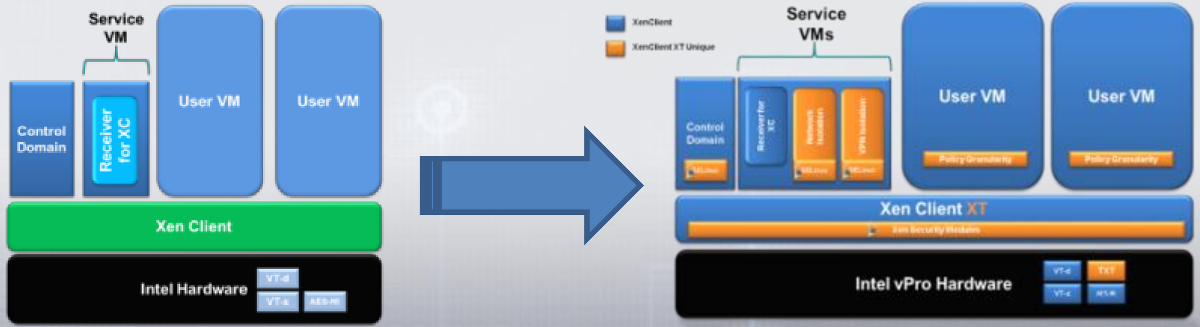
interception, and search, and may be disclosed or used for any USG authorized purpose.

This IS includes security measures (e.g., authentication and access controls) to protect USG interests, NOT

Close Consent Banner

Modifications from XenClient to XCXT

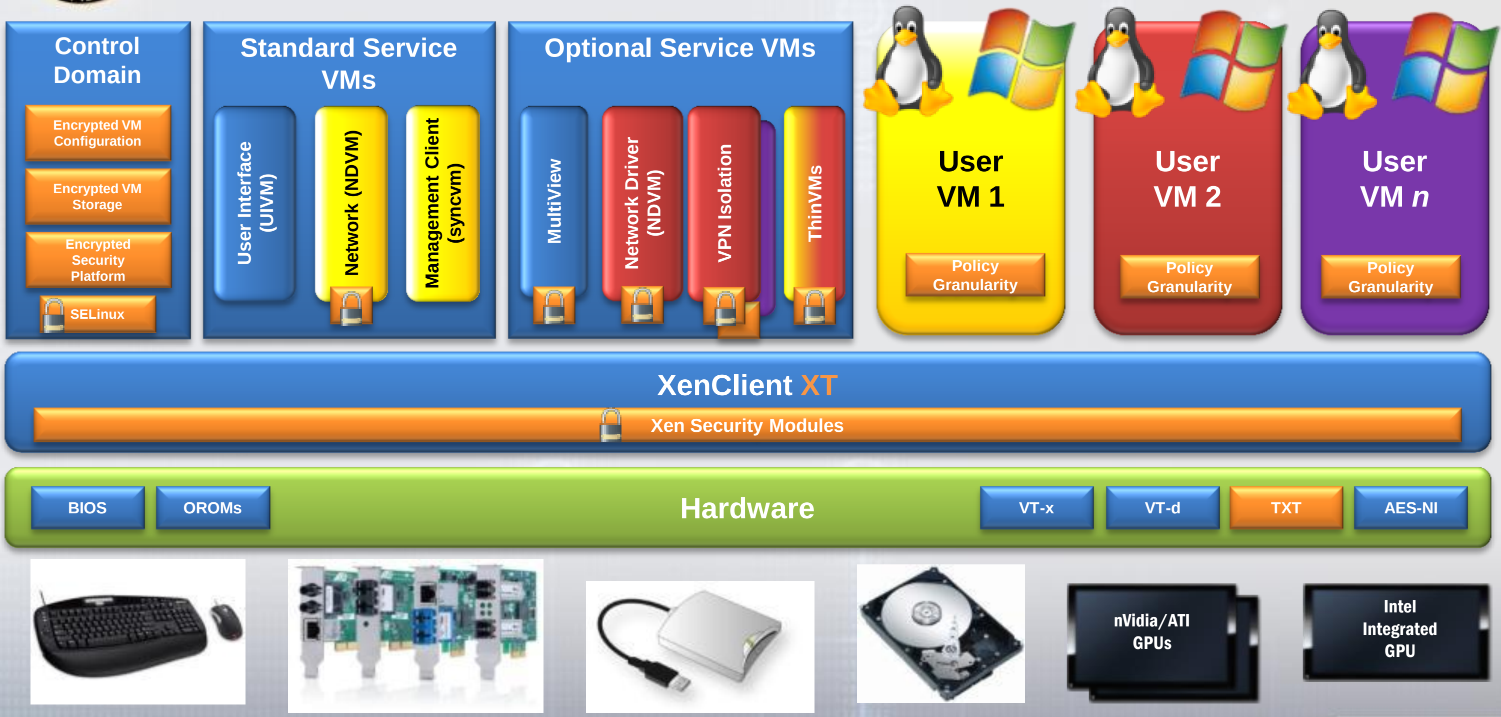
- DRTM of hypervisor and dom0 (measured launch)
- Platform hardening
- Disaggregate and de-privilege functionality into dedicated service VMs
- Moved network stack to a separate service VM
- Implemented SELinux in dom0 and service VMs with custom set of SELinux policies
- Narrow interfaces between components
- Cross-VM mouse control



XenClient

XenClient XT

SecureView 2.0 Architecture



Control Domain

- Encrypted VM Configuration
- Encrypted VM Storage
- Encrypted Security Platform
- SELinux

Standard Service VMs

- User Interface (UIVM)
- Network (NDVM)
- Management Client (syncvm)

Optional Service VMs

- MultiView
- Network Driver (NDVM)
- VPN Isolation
- ThinVMs

User VM 1 – Policy Granularity

User VM 2 – Policy Granularity

User VM *n* – Policy Granularity

XenClient XT

Xen Security Modules

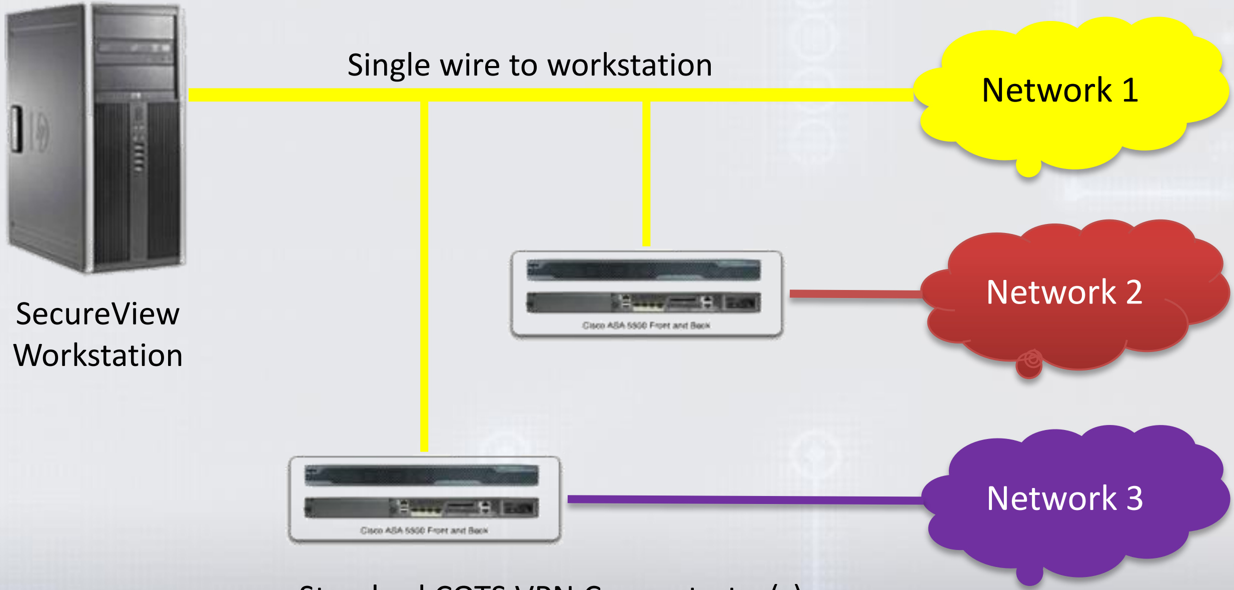
Hardware

BIOS | OROMs | VT-x | VT-d | TXT | AES-NI

nVidia/ATI GPUs

Intel Integrated GPU

Typical Network Architecture



Single wire to workstation

SecureView Workstation

Network 1

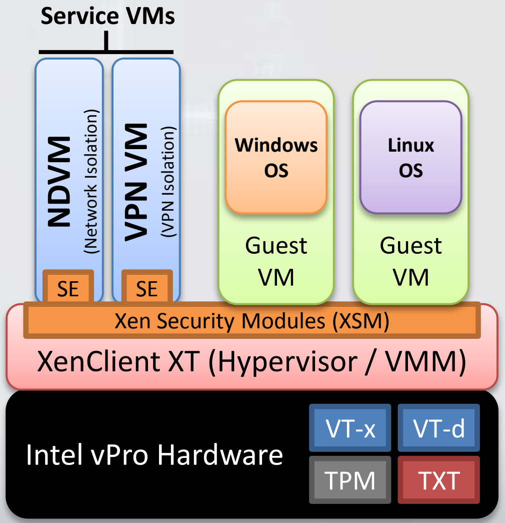
Network 2

Network 3

Standard COTS VPN Concentrator(s)

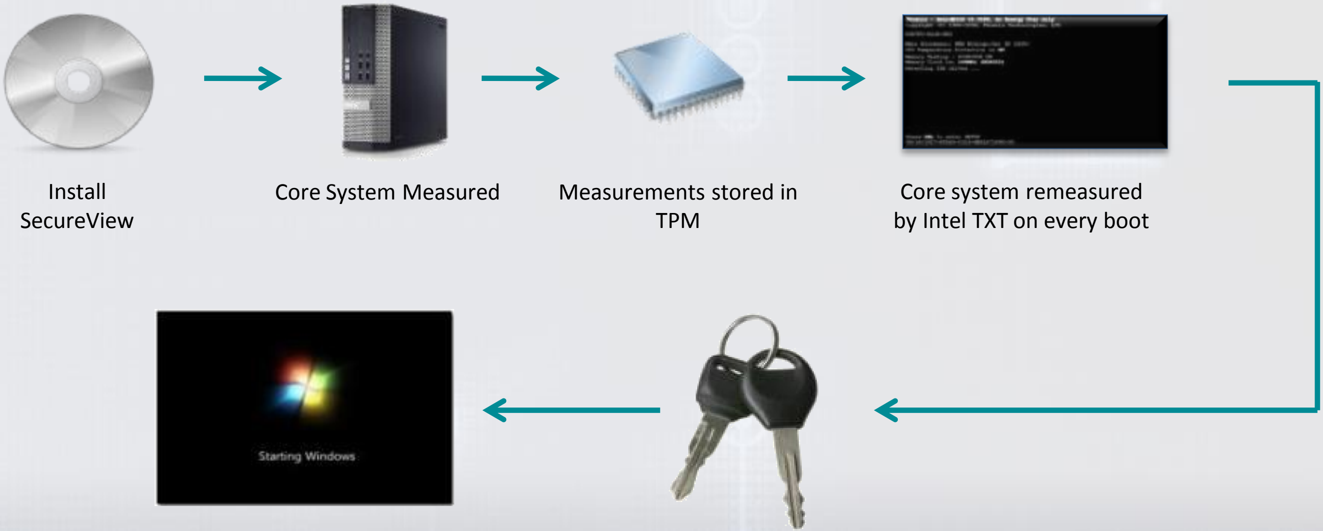
Security Foundation

- **Establish Secure Isolation in the hardware**
  - Intel Virtualization Technology Extensions (VT-x) : Hardware based X86 CPU virtualization
  - Intel Virtualization Technology for Directed I/O (VT-d): Hardware based Input & Output Memory Management Unit (IOMMU) that utilizes DMA mapping and direct PCI assignment
- **Utilize VM isolation to minimize attack surface and constrain exploits**
  - Assume attackers will compromise guest VMs, limit their mobility
- **Constrain Allowable Operations**
  - Use NSA Security Enhanced Linux (SELinux) to limit how Service VMs can use resources
  - NSA Xen Security Modules (XSM) to limit how hypervisor can use resources
  - Limit mobility of malware with policy constraints on capabilities (i.e USB)
- **Verify Integrity through Trusted Boot**
  - Measure and store initial system state in the Trusted Platform Module (TPM)
  - When booted, current core system re-measured and results verified
- **Protect Data at Rest and in Transit using encryption**
  - Trusted Boot mechanism locks core system components until verified
  - Encrypt all sensitive components including configuration, service VMs, and optionally guest VM images to protect from offline tampering
  - Encrypt network comms. within IPSEC VPN tunnels to protect data in transit



Hypervisor = Virtual Machine Manager (VMM)

SecureView: Trusted Boot with Intel TXT



Install SecureView

Core System Measured

Measurements stored in TPM

Core system remeasured by Intel TXT on every boot

Measurement used to unlock encryption keys and configuration

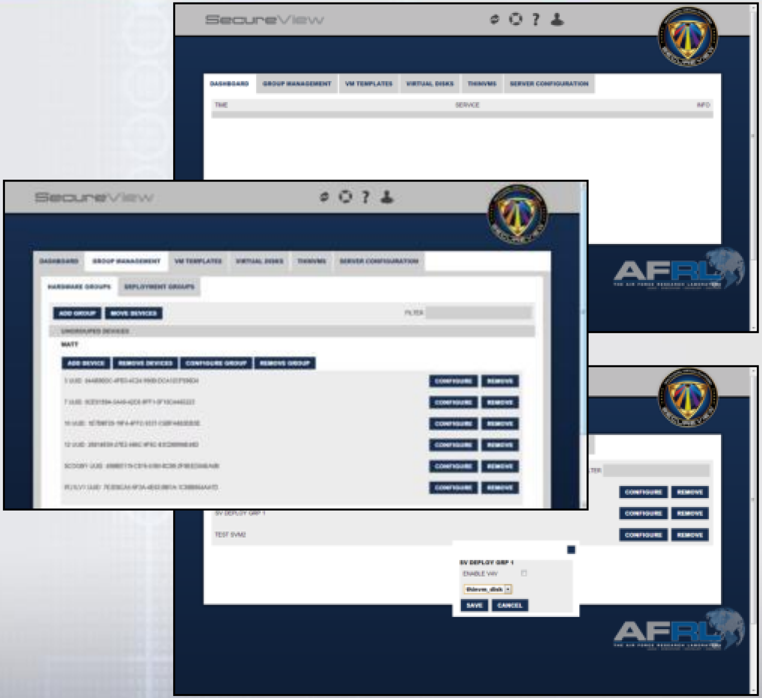
Only then can you boot ‘guest’ (Windows) VMs

SecureView 2.0 Enhancements

- SecureView Mgmt Server (Enterprise Scalability)
- Secure Seamless Windowing – MultiView
- ConnectView/Linux ThinVM
- Multi-Layer Suite B VPN Comms. (NSA/CSFC)
- NSA Certified Full Disk Encryption
- Expanded HW Compatibility List

SecureView Management Server

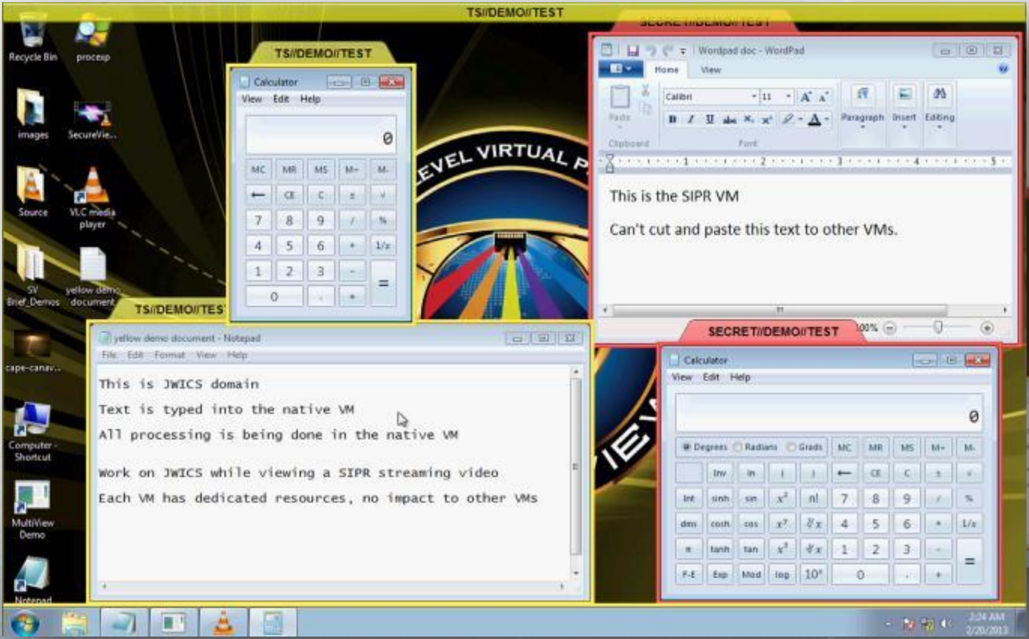
- **Enterprise Scalability**
  - Deploy new VMs
  - Delete managed VMs
  - Reconfigure existing VMs
  - Configure platform
  - Upgrade platform
  - Status monitor



Seamless Windowing - MultiView

- **Secure Seamless Windowing – MultiView**
  - Allows Windows applications from different security domains to be seen simultaneously on the same screen

Note: Images are Unclassified - Classified markings are for illustration purposes only



This is JWICS domain

Text is typed into the native VM

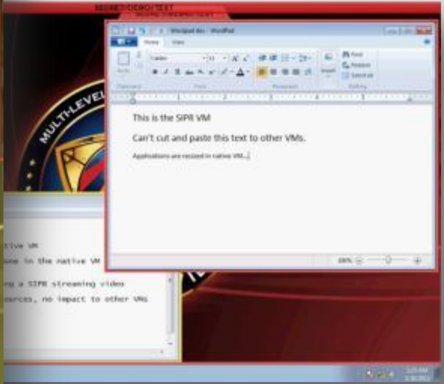
All processing is being done in the native VM

Work on JWICS while viewing a SIPR streaming video

Each VM has dedicated resources, no impact to other VMs

This is the SIPR VM

Can't cut and paste this text to other VMs.



This is the SIPR VM

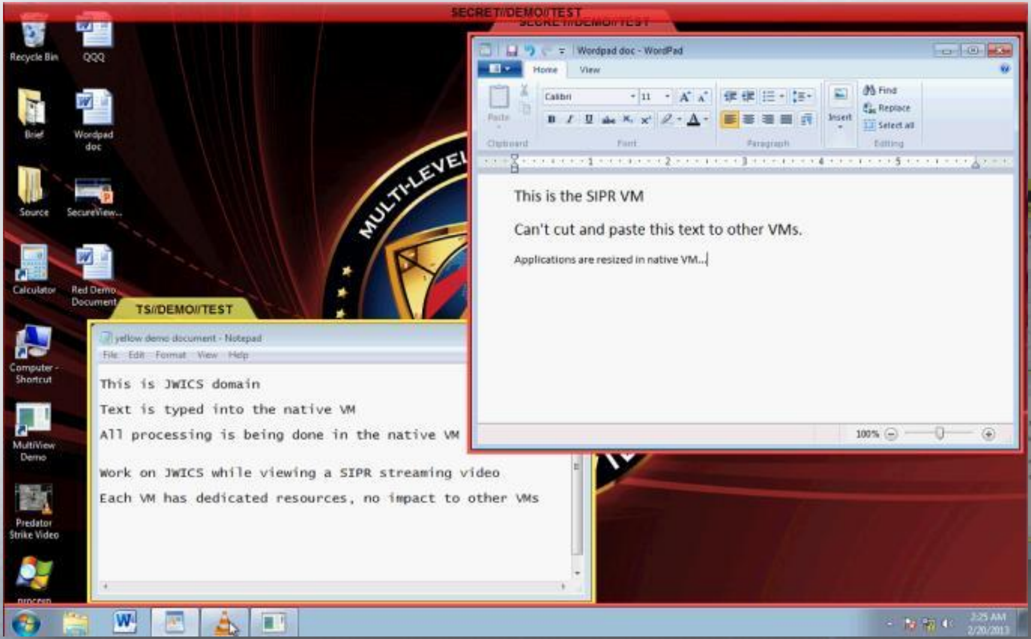
Can't cut and paste this text to other VMs.

Applications are resized in native VM...

Seamless Windowing - MultiView

- **Secure Seamless Windowing – MultiView**
  - Allows Windows applications from different security domains to be seen simultaneously on the same screen

Note: Images are Unclassified - Classified markings are for illustration purposes only



This is the SIPR VM

Can't cut and paste this text to other VMs.

Applications are resized in native VM...

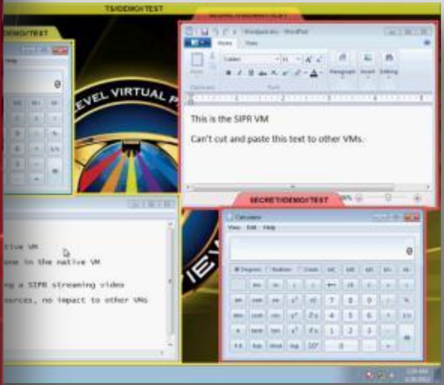
This is JWICS domain

Text is typed into the native VM

All processing is being done in the native VM

Work on JWICS while viewing a SIPR streaming video

Each VM has dedicated resources, no impact to other VMs



This is the SIPR VM

Can't cut and paste this text to other VMs.

tive VM

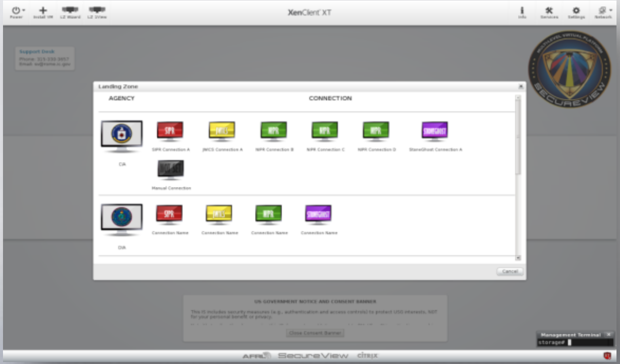
one in the native VM

ng a SIPR streaming video

ources, no impact to other VMs

ConnectView/Linux ThinVM

- ConnectView
  - Dynamically create ThinVM and paired VPNVM
  - Allows AD/Hoc connections to other networks (if allowed)



Support Desk
Phone: 315-330-3657
Email: sv@rome.ic.gov

US GOVERNMENT NOTICE AND CONSENT BANNER

This IS includes security measures (e.g., authentication and access controls) to protect USG interests, NOT for your personal benefit or privacy.

```
storage#
```

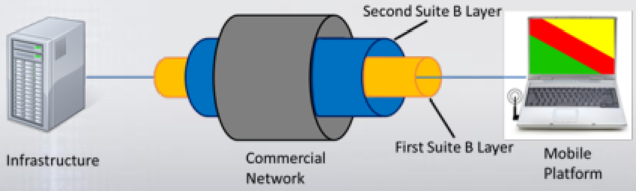
- Linux ThinVM
  - Virtual desktop access
    - Citrix ICA
    - Microsoft RDP
    - VMWare View
  - Isolated web browser
  - Seamless desktop
  - No data persistence
  - Read-only and measured
  - Shared image (saves storage)

GlowView

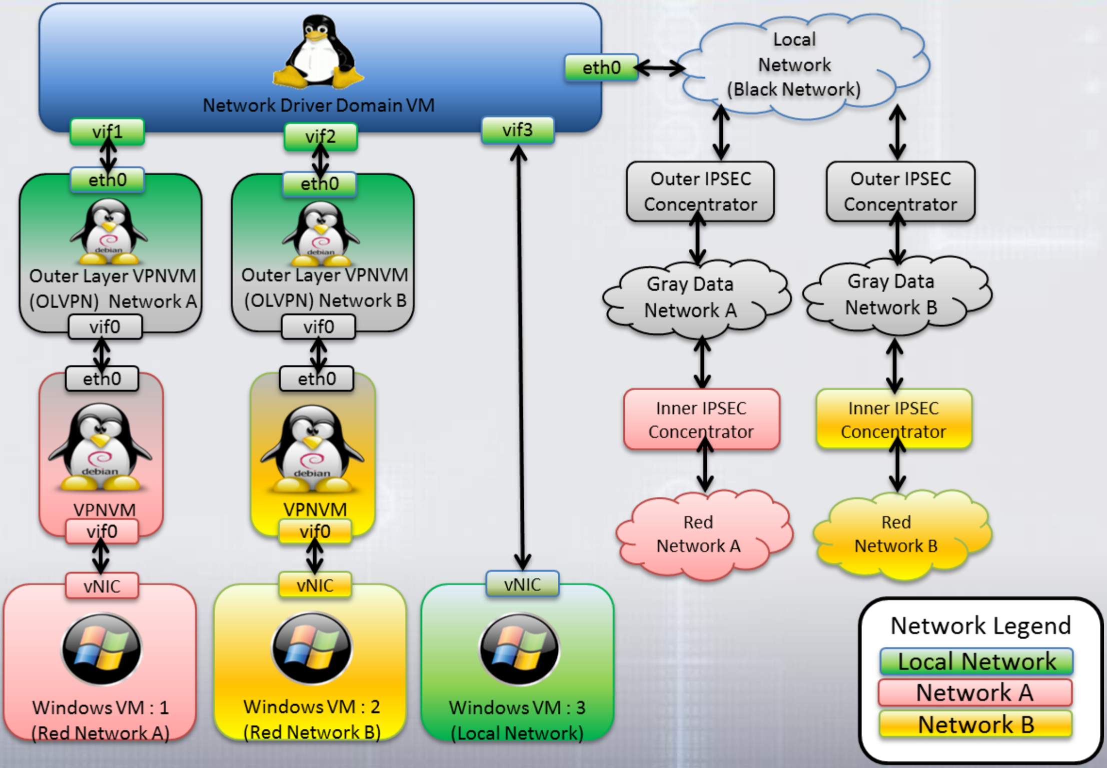
- Colored keyboards to identify security level of current action
- Security level color is associated with each Guest VM
  - Color changes based on where keyboard focus is given
- Logitech G510
  - Colored keys and LCD screen
  - LCD shows security label (text) and VM name
- Luxeed U7 Crossover
  - Colored keys only

SecureView 2.0 Features

- VPN Options
  - Single Low-over-High VPN
    - Example: Tunnel SIPR over JWICS
  - Double-nested Suite B VPN (NSA CSfC)
    - Example: Tunnel JWICS over SIPR or Internet
  - Expanded hardware
    - Cisco
    - Aruba



SecureView 2.0 VPN Data Flow



SecureView 2.0 Features

- Certified Full Disk Encryption
  - Hardware encryption of disks
  - Use TCG standard methods
  - Use COTS self-encrypting drives
  - Working with NSA to establish CSfC capability package

SIPRNET Token Support

- The approved SIPRNET token reader (OmniKey 3121) is currently supported on SecureView.
- The approved SIPR Token middleware by 90meter is also supported and fully functional.

Thin Client Support

- SecureView can be configured as a "Thin" Client
  - Minimal WinTPC or Linux OE installed locally
  - No local data
  - No local apps
  - Only locally installed app is a Citrix Receiver or other VDI client
- Variety of small and ultra small factor desktop appliances are supported
- Supports "Zero Touch" – small footprint updated remotely if/when required

SecureView 2.0 HW Compatibility List

- **Hardware Support**
  - Desktops
    - Dell OptiPlex 980, 990, 7010, 9010
    - HP Compaq Elite 8200, 8300
  - Laptops
    - Dell Latitude E6420 XFR and E6430
    - HP EliteBook 2760p and 9470 Folio
    - Lenovo T430s
  - Workstation
    - NCS Vortex A422

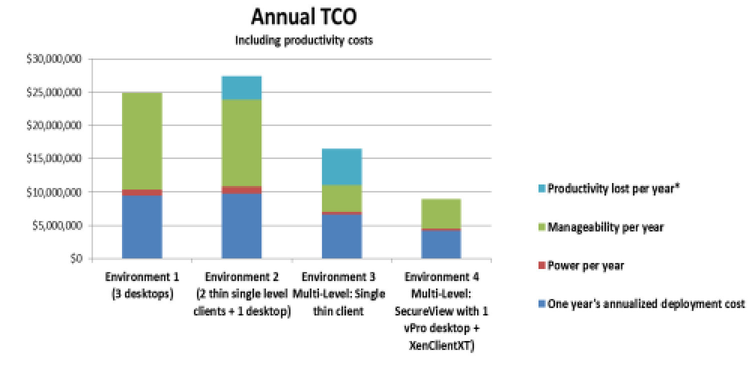
Almost any Intel-based platform with full vPro support and integrated Intel graphics can be supported.

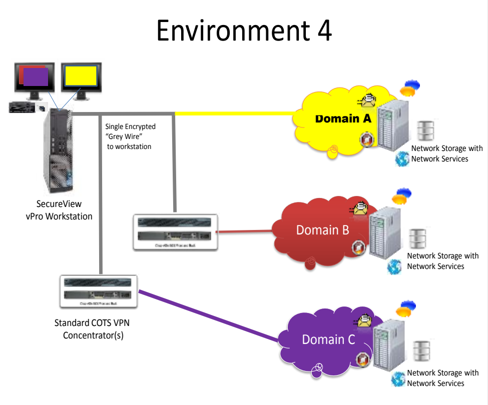
Cost

- Performance desktop computer $795 (AF QEB 2013A) + options
  - i.e. Dell Optiplex 980/990/9010, HP Compaq Elite 8200/8300, other desktops and laptops
- XenClient XT MSRP qty 1 = $610/license
  - AFRL ELA
    - $249 for any quantity includes year 1 software maintenance
  - Citrix has enterprise agreements with many agencies
    - Product may get bundled with other Citrix products
- AFRL Support
  - Installation – funding determined by level of support required
  - Sustainment – as low as $25 per seat at quantity

Total Cost of Ownership

Summary by Intel




Environment 4
Single Encrypted "Grey Wire" to workstation
SecureView vPro Workstation
Standard COTS VPN Concentrator(s)
Domain A
Domain B
Domain C
Network Storage with Network Services
Network Storage with Network Services
Network Storage with Network Services

- ***SecureView savings are significant compered to alternative architectures***
  - *SecureView is estimated to reduce TCO by up to 67% over single-domain architectures and 45% savings over a thin-client, multi-domain architecture.*

- **Analysis included:**
  - Cost to deploy and support 10,000 users
  - Necessary build-out costs for client, server, network and other hardware over entire upgrade cycle
  - Impact of lost productivity when analysts using a server-hosted virtualization solution must wait for slow systems or heavily-loaded networks
  - Power costs, costs of pre-deployment preparation, deployment, and ongoing management costs over upgrade cycle

Current Certification and ATOs

- **SecureView was favorably evaluated against the NIST 800-53 Security Controls Catalog for**
  - Confidentiality: **HIGH,** Integrity: **HIGH ,** Availability: **MEDIUM**
  - Original v1.0 ATO issued 10 August 2011
- **SV 1.2 Authority to Operate (ATO)**
  - **DIA – Top Secret SCI And Below Interoperability (TSABI) ATO: 2 April 2013**
  - **ODNI – IC3E ATO: 10 Dec 2012**
  - **AF DAA – DIACAP ATO: 4 June 2013**
  - **AFISRA/A6S – IATT: 23 Sep 2013**
- **Listed on UCDMO Baseline as CDS Access Solution - 4 April 2013**
- **SV 2.0 Certification, Test & Evaluation (CT&E) Status**
  - **Secret and Below Interoperability (SABI) CT&E started 26 September 2013**
  - **AFISRA TSABI CT&E completed 20 September 2013**
  - **DIA TSABI CT&E completed 19 September 2013**

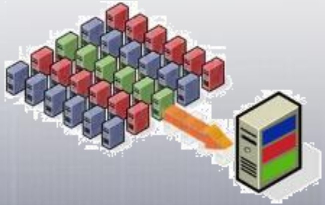
CERTIFIED & ACCREDITED

No Extensive Training Required

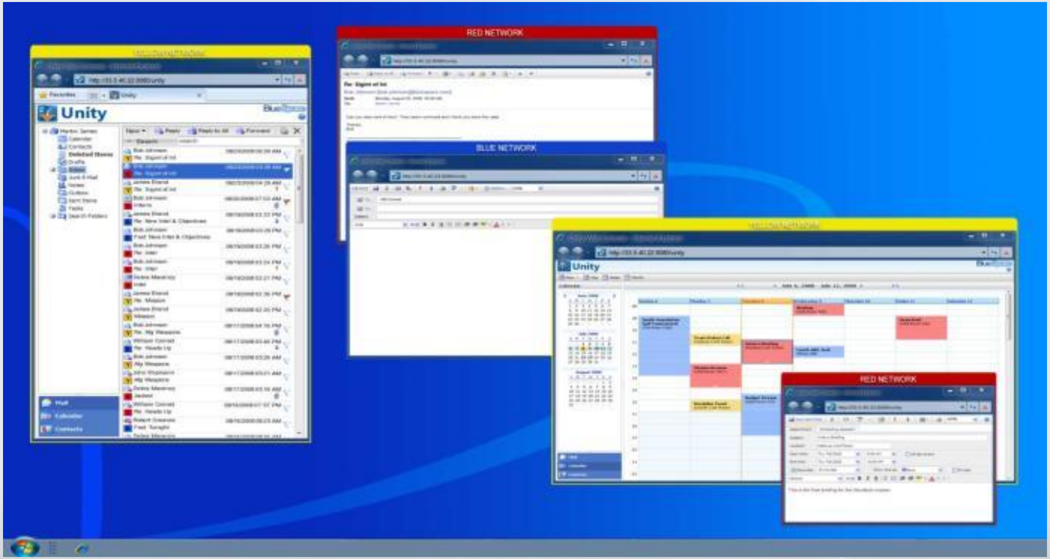
- Easy to setup, configure, and maintain
  - Qualified CSAs should have the skills
  - Even system admins cannot inadvertently create a cross-domain security breach
- Easy to use
  - Users adapt quickly to multi-domain features
  - Switching domains is somewhat similar to using a KVM switch
- Full documentation available
  - System Security Plan (SSP)
  - Security Test Plan & Procedures (STP)
  - Master Security Requirements Matrix (MSRTM)
  - Installation & Configuration Guide (ICG)
  - Administrator Guide (AG)
  - User's Guide (UG)
  - Integrated Support Plan (ISP)

Related Efforts - SecureServe

- March 2010 – ACC requested AFRL assist in virtualization solution for the Next Generation Air Operations Center (AOC)
- Start with SecureView (80% client/server code base common)
- Further security enhancements for both client and server
- Goal: “Citrix Xen Server XT” available as low cost COTS or Open Source
- Leveraging DARPA Detection and Response Embedded Device
- Network access control
- Availability: Secure Virtualization 2013 / Enhancement/Extensions 2014



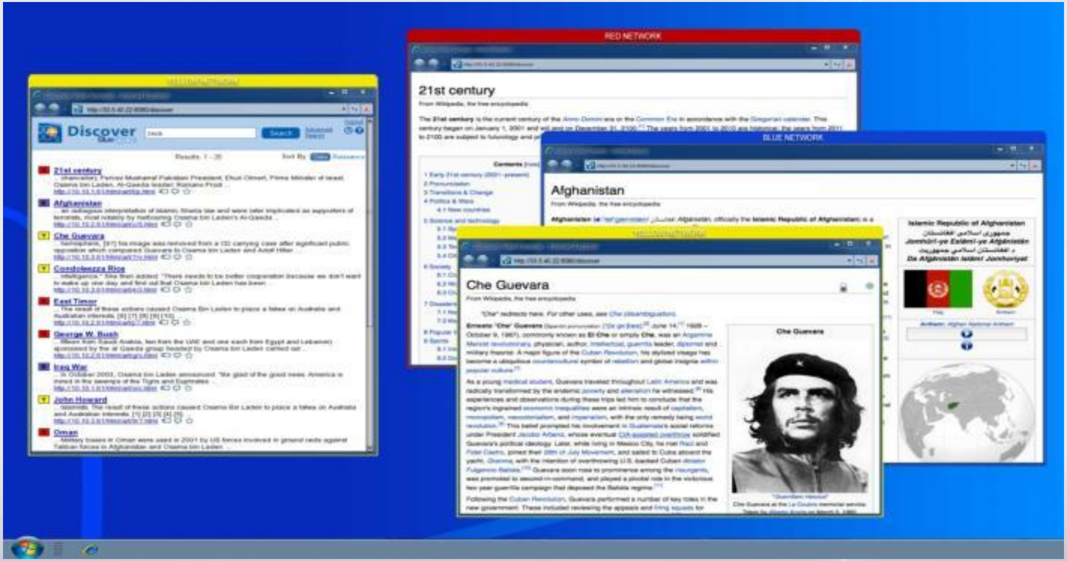
3rd Party Multi-Level Applications - Email



BlueSpace

- Single interface for email, calendar, contacts, tasks
- Only metadata transferred to create unified view
- Connects to existing Exchange servers
- Works in full screen and seamless desktop integration modes
- SecureView 2.0 adds colored borders to windows based on source VM classification

3rd Party Multi-Level Applications - Search



- Single interface for searching across multiple VMs
- View and interact with content at source security level
- Connects to existing search engines
- Works in full screen and seamless desktop integration modes
- SecureView 2.0 adds colored borders to windows based on source VM classification

Comparison to Other MLS Clients

- Unprecedented security via Intel's hardware-based security features
  - VT-d, VT-x, TPM, TXT, AESNI
- Relatively simple, robust and flexible architecture
  - Supports dedicated 3D graphics or shared display
  - Supports dedicated network I/Fs or One-wire Configuration
  - Guest VMs can be either "thick" or "thin"
  - Full SIPRNET Token Support
  - Does not require "specialized" sys admin support
- Extensive desktop server backend not required -- can be leveraged if available
- Low-cost commodity desktop hardware (or laptops)
- COTS software based on Open Source, no system integrator or "lock-in"
- Significantly cheaper than other MLS access solutions

Summary

- SecureView breaks new ground in client virtualization
- True type 1 hypervisor for robust isolation and very high performance
- COTS, open source based
- More affordable and capable – Total cost of ownership reduced by up to 67%
- Avoids integrator/hardware vendor "Lock-in"
- SecureView is available NOW
- NIST 800-53 certified

Questions

Points of Contact

Air Force Research Laboratory
AFRL/RIEB
afrl.rieb.secureview@us.af.mil
315-330-7658
NIPR: https://extranet.if.afrl.af.mil/sv
SIPR: http://sv.afmc.smil.mil
JWICS: http://web1.rome.ic.gov/sv

Powered by Citrix XenClient

AFRL

THE AIR FORCE RESEARCH LABORATORY

LEAD | DISCOVER | DEVELOP | DELIVER