

SecureView[®] Overview

Updated 30 Oct 2017

Air Force Research Laboratory
AFRL/RIEB
SecureView@us.af.mil
315-330-7657



Cleared for public release. Case Number: 88ABW-2017-5254

SecureView[®] is a registered trademark of AIS Inc., New York.





Overview

- **SecureView® Background**
- **Security & Architecture**
- **Features**
- **Hardware Support**
- **Programmatics**
- **Summary**
- **POCs**



SecureView® Genesis

Due to growing collaboration demands, ODNI tasked AFRL in 2010 with developing a secure workstation that would meet the following criteria:

- 1) *Provide the IC with unparalleled security and protection against data exfiltration*
- 2) *Support high-performance applications*
- 3) *Streamline IT infrastructure requirements for networks*
- 4) *Enable rapid provisioning & deployment*
- 5) *Ensure agility to meet future requirements*





SecureView® – What is it?

- **SecureView® is an Air Force developed multi-network access solution that provides users with the ability to access multiple environments on a single workstation.**
 - A single computer to host multiple guest virtual machines (VMs) on different isolated environments
 - Eliminates the need for NIAP approved KVM switches
- **SecureView® is a low-cost, non-proprietary solution that is based on commodity hardware and open source virtualization technology. Security and the chain-of-trust is established down to the processor and chipset of the PC.**
 - Runs on Intel vPro based clients
 - Based on OpenXT “Type 1” or bare metal client hypervisor
- **Flexible solution to address a wide variety of use cases**
 - Supports Windows, and Linux guests
 - Dynamic support for both thick and thin-client computing models
 - Single or multiple wires to desktop
 - Works on desktops, laptops, and tablets





SecureView® Desktop Consolidation

Before SecureView

- Separate PC or thin client for each security domain



With SecureView

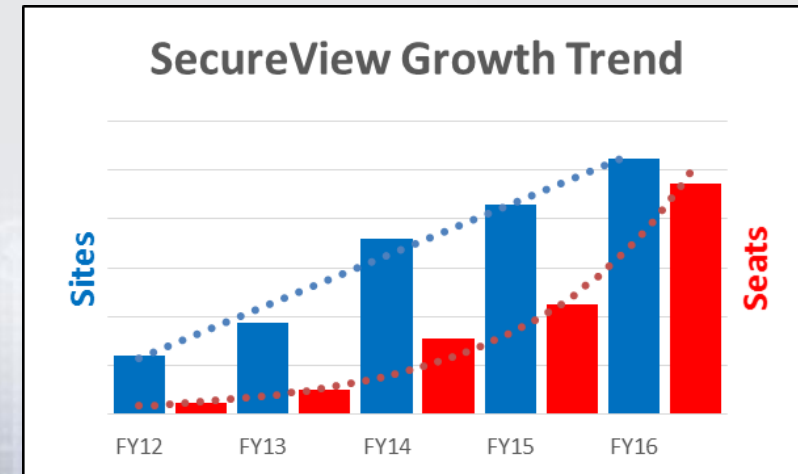


- Single desktop with concurrent access to multiple domains
- Reduces footprint, power, and cost
- Improves mission effectiveness



Who's Using It

- **SecureView is deployed widely across various agencies**
- **60+ active sites with thousands of clients**
- **Driving factors to more widespread deployments**
 - Implementation plan for Windows 10
 - Desire to collapse network connections to the desktop





Demonstration


Power ConnectView



Devices Info Services Settings NdvM-HIGH NdvM-LOW Status

SV Help ✕
Phone: 330-4561
Email: help@sv.desk

HIGH LOW

 Off  Off

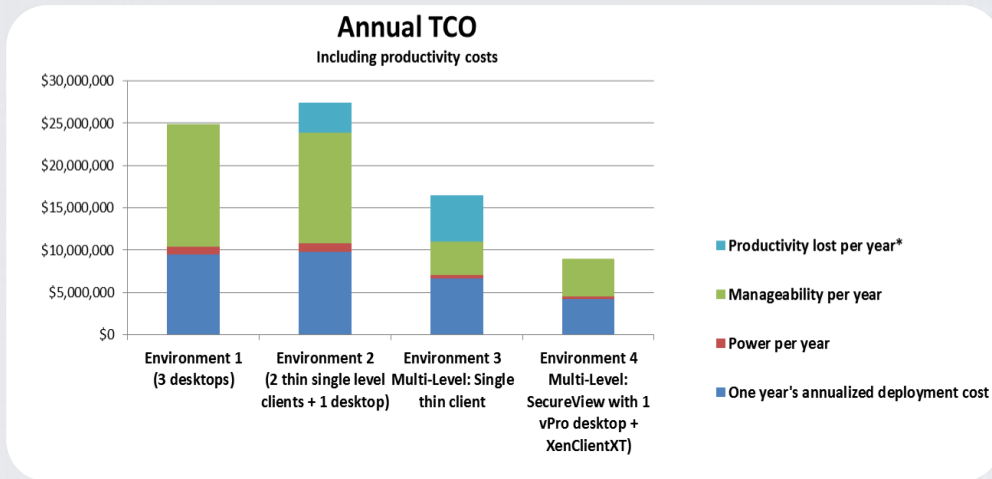
AFRL SecureView ais   83%





Total Cost of Ownership

Intel Corp. Total Cost of Ownership (TCO) Study



Analysis included:

- Cost to deploy and support 10,000 users on 3 networks
- Administration
- Impact of lost productivity
- Power cost

SecureView® is estimated to reduce TCO by up to 67% over single domain architectures and 45% over thin-client, multi-domain architectures



Fundamental SecureView® Components

- **OpenXT**
 - *Xen Type-1, Bare Metal Hypervisor*
 - *Minimized Dom0 and dedicated Service VMs*
- **Intel's vPro Processor & Chipset**
 - *VT-x: Virtualization Extensions*
 - *VT-d: Technology for Directed I/O*
 - *AES-NI: Hardware-based Encryption/Decryption*
 - *TXT: Trusted Execution Technology*
 - *TPM: Trusted Platform Module*



SV leverages vPro features to improve security and application performance.

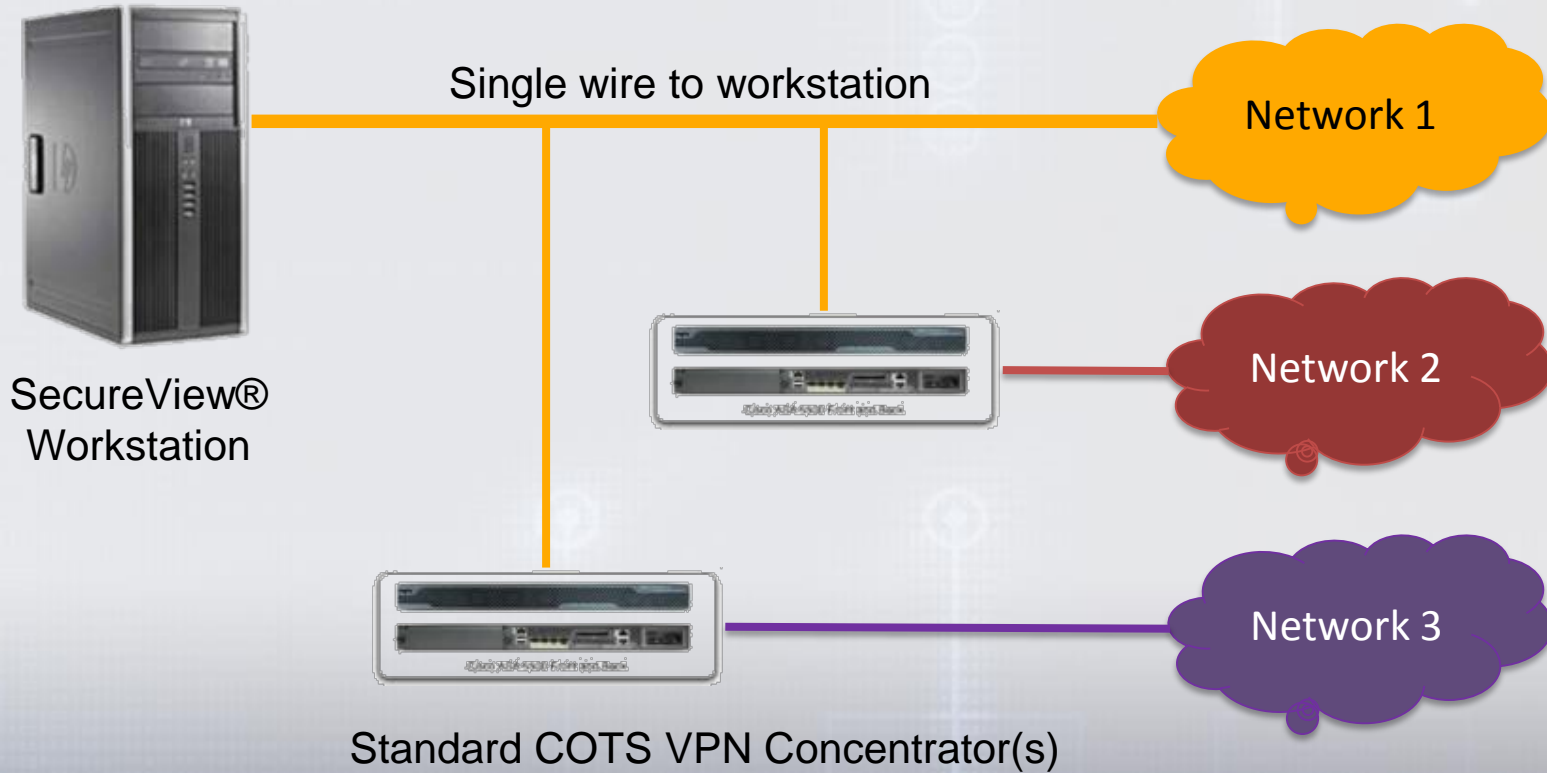


SecureView® Architecture





Typical Network Infrastructure





Current Certification and ATOs

- **SecureView® favorably evaluated against the NIST 800-53 Security Controls Catalog for**
 - Confidentiality: **HIGH**, Integrity: **HIGH** , Availability: **MEDIUM**
 - Original v1.0 Authority To Operate (ATO) issued 10 August 2011
- **Listed on UCDSMO Baseline as CDS Access Solution**
- **Multiple versions of SV have successfully completed Assessment & Authorization process for a variety of deployment scenarios**





SecureView® Features

- **SecureView® Management Server**
 - Enterprise Scalability
- **Secure Seamless Windowing – Mosaic (formerly MultiView)**
 - Consolidated view of multiple security domains
- **ConnectView/Linux ThinVM**
 - Seamless support for virtualized environments
- **GlowView**
 - Keyboard based awareness
- **NSA Commercial Solutions for Classified (CSfC)**
 - Multi-Layer Suite B VPN Communications
 - Connectivity to protected environments w/o expensive equipment
 - Data at Rest Protection



SecureView® Management Server (SVMS)



SecureView Management Server



Enterprise Management Capability





Mosaic Capability

- **Secure Seamless Windowing**

- Allows different security domains to be seen simultaneously on the same screen(s)
- Despite all appearing on the same physical screen(s), domain isolation is preserved and each VM is unaware of the existence of any other VM

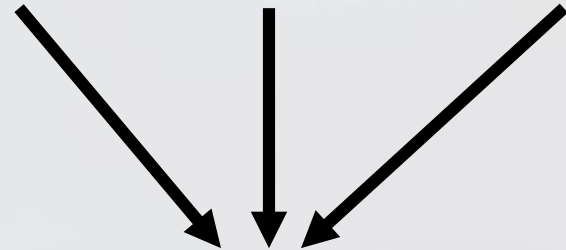




ConnectView

- ConnectView
 - ThinVM and paired VPNVM
 - Pre-Configured connections to VDI or Terminal Services backends
- Linux ThinVM
 - Virtual desktop access
 - Citrix ICA
 - Microsoft RDP
 - VMWare View
 - Isolated web browser
 - Seamless desktop
 - No data persistence
 - Read-only
 - Shared image (saves storage)

VMWare View *Microsoft RDP* *Citrix ICA*





GlowView

- **Colored keyboards to identify domain of current action**
- **Color and/or label is associated with each Guest VM**
 - Color changes based on where keyboard focus is given
- **Corsair Strafe RGB**
 - Colored keys and LCD screen
 - LCD shows label (text) and VM name





Commercial Solutions for Classified (CSfC)

- The National Security Agency / Central Security Services (NSA/CSS) Information Assurance Directorate (IAD) is developing new ways to leverage emerging technologies to deliver more timely IA solutions for rapidly evolving customer requirements.
- NSA/CSS' Commercial Solutions for Classified (CSfC) Program has been established to enable commercial products to be used in layered solutions protecting classified NSS information.
- This will provide the ability to securely communicate based on commercial standards in a solution that can be fielded in months, not years.

https://www.nsa.gov/ia/programs/csfc_program/

Commercial Solutions for Classified



*Layered Commercial Solutions
Enabling Assured Communications*



National Security Agency
Information Assurance Directorate
9800 Savage Road
Fort Meade, MD 20755

NSA/CSS INFORMATION ASSURANCE DIRECTORATE
COMMERCIAL SOLUTIONS FOR CLASSIFIED

Source: NSA/IAD Website

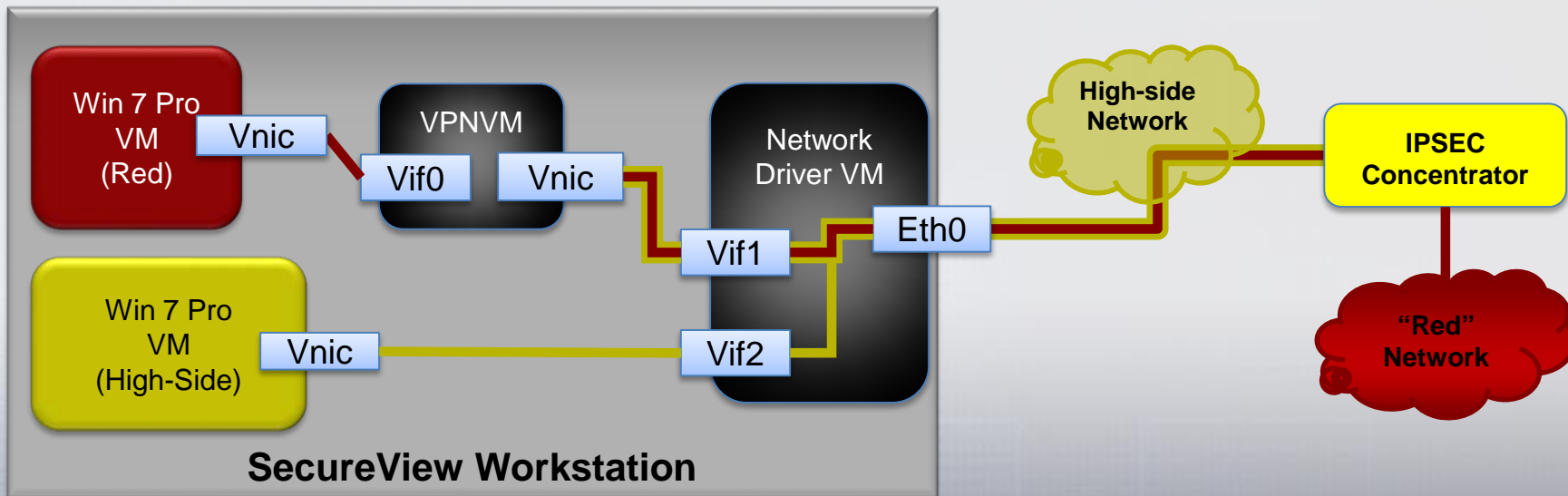


Protect Data-in-Transit

SecureView protects data in transit by encrypting the data and isolating the path of the network traffic from the guest VMs through dedicated and protected service VMs that communicate directly with the physical network interfaces.

Each physical network interface has a dedicated service VM (NDVM) to manage its' traffic exclusively. A guest VM can be configured to utilize single or multiple VPN service VMs in order to cryptographically separate data from other domains in single or double sleeve configuration.

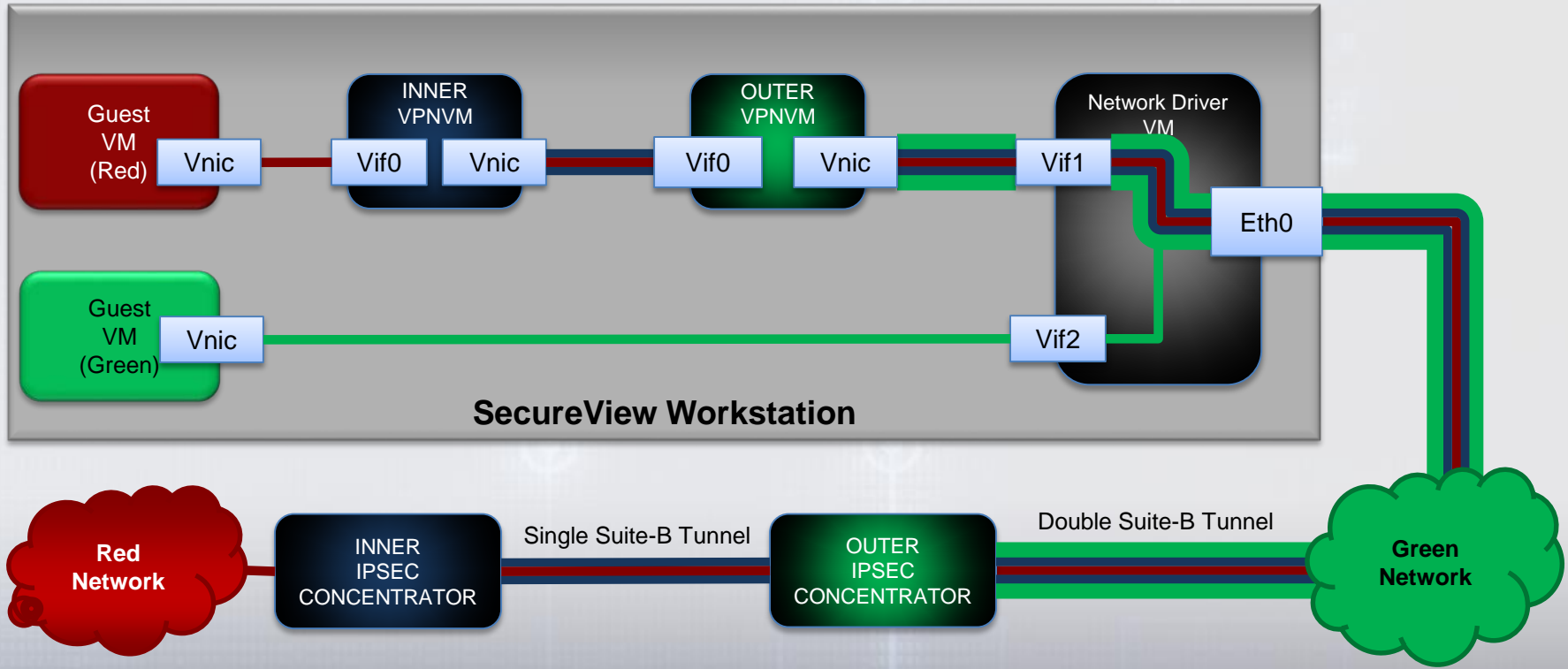
Low over High Configuration





Double Suite-B Tunnel

High over Low Configuration



NSA Commercial Solutions for Classified Program





DaR CP v3.0 support

- Hardware Full Disk Encryption (FDE) to be provided by Self Encrypting Drive (SED)
- Software FDE to be provided by Windows Bitlocker
 - Included with Windows 7 & 10
- Software File Encryption (FE) to be provided by Dell Data Protection Encryption (DDPE)
- DaR is accomplished by using any two of above
 - Data on device is fully protected when powered off





SecureView® 2.3 Hardware Compatibility List

Desktops

- Dell Optiplex 7040 MT, SFF & Micro, XE2 MT & SFF
- HP EliteDesk 800 G2 Tower, SFF, & Mini
- NCS Stratus 9480

Tablets

- HP Pro x2 612, Elite x2 1012 G1

Laptops

- Dell Latitude E5570, Precision 7710
- HP EliteBook Revolve 810 G2, G3
- HP EliteBook 850 G3

Workstations

- Dell Precision T3620, T7910, R7910
- HP Z240, Z840
- NCS Vortex MDT 5480
- HP Z840

+ Legacy Platforms



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

See SV website for updates.



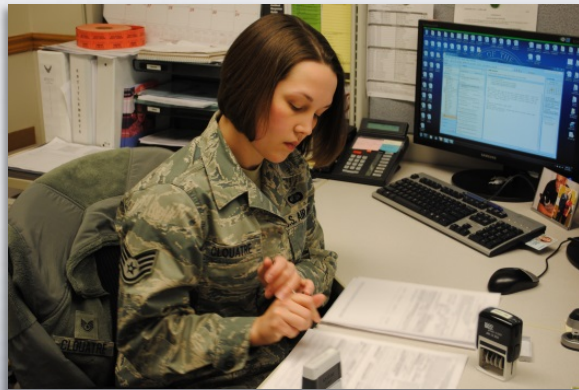
Thin Client Support

- SecureView can be configured as a “Thin” Client
 - Minimal WinTPC or Linux 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® Platform Evolution



Office / Workcenter



Mobile / Deployed



Tactical / Senior Leadership



SecureView® - Secure Mobility



- Tablet manufacturers are now integrating Intel vPro chipsets for enhanced security and virtualization that enable integration of SecureView
- SecureView® tablet supports senior leadership use cases as well as secure mobility applications
- Integration of NSA's Suite B Data-at-Rest and Data-in-Transit security will enable truly seamless enterprise mobility



Cost

- **Performance desktop computer \$700 + options**
 - i.e. Dell Optiplex 7050, HP Elitedesk 800, NCS Stratus, other desktops and laptops
- **Software: GOTS, no license required**
- **AFRL Support**
 - Installation – funding determined by level of support required
 - Sustainment* – \$30K per site plus
 - \$110 per seat up to 1000
 - \$80 per seat 1001-5000
 - \$55 per seat 5000+

* FY18 sustainment pricing; subject to annual adjustments



SecureView® Training Program

- SV Management Server (SVMS) Virtual Lab Environment
 - Allows SecureView admins to practice deploying SecureView Client machines in a lab environment
- SV User Computer Based Training (CBT)
- SVMS Administrator classroom training
 - Courses are regularly offered in Rome, NY or by special request locally through a mobile training program
- VPN Advanced classroom training
- See SV website for syllabus and current schedule for training courses
 - <https://intelshare.intelink.gov/sites/afrl-idhs/web/sv/training.html>



Comparison to Other CDS Clients

- **Unprecedented security via Intel's hardware-based security features**
 - VT-d, VT-x, TPM, TXT, EPT, AES-NI
- **Supports all modern Operating Systems**
- **Relatively simple, robust and flexible architecture**
 - Supports dedicated 3D graphics or shared display
 - Supports dedicated networks (multi-wire) or One-wire Configuration
 - Guest VMs can be either “thick” or “thin”
 - Does not require “specialized” sys admin support
- **Extensive desktop server backend not required – but can be leveraged if available**
- **Low-cost *commodity* desktop hardware (or laptops)**
- **GOTS software based on Open Source, no system integrator or “lock-in”**
- **Significantly cheaper than other CDS access solutions**



Summary

- SecureView® is an enterprise solution that meets USAF growing requirements for secure networks
 - Reduces costs
 - Increases scalability
 - Enhances security
- SecureView® enables secure information access to a globally agile force
- Delivers truly integrated user experience across security domains that
 - Increases personnel effectiveness
 - Enhances mission accomplishment
- More affordable and capable – TCO reduced by up to 67%
- Certified and available NOW



Points of Contact

Program Manager

John Woodruff, AFRL/RIEB
315.330.7657
john.woodruff.3@us.af.mil

Deputy PM

Capt Alex Gwin, AFRL/RIEB
315.330.3953
alexander.gwin.1@us.af.mil

Section Chief

Dr. Ryan Durante, AFRL/RIEB
315.330.4004
ryan.durante.1@us.af.mil

Technical Lead

Steve Scheiderich, MicroQuest
315.330.4635
stephen.scheiderich.ctr@us.af.mil

Chief Engineer

Kevin Pearson, AFRL/RIEB
315.330.3202
kevin.pearson.4@us.af.mil

Program Manager - Developer

Rich Turner, AIS
315.336.3306 x420
turnerr@ainfosec.com



NIPR Email: secureview@us.af.mil

NIPR Website: <https://intelshare.intelink.gov/sites/afrl-idhs/web/sv/index.html>

SIPR Website: <http://rie.afmc.af.smil.mil/sv>

JWICS Website: <http://www.rome.ic.gov/sv>



Questions





AFRL

THE AIR FORCE RESEARCH LABORATORY
LEAD | DISCOVER | DEVELOP | DELIVER