SecureView Overview

Updated 8 July 2016

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

Due to growing collaboration demands within the Intelligence Community, 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 classified networks
4) Enable rapid provisioning & deployment of the solution across the IC and DoD
5) Ensure agility to meet future requirements
SecureView – What is it?

• SecureView is an Air Force developed Cross Domain Access solution that provides users with the ability to access Multiple Independent Levels of Security (MILS) on a single workstation.
  – A single computer to host multiple guest virtual machines (VMs) running at different classification levels.
  – Eliminates the need for NIAP approved KVM switches

• SecureView is a low-cost, non-proprietary MILS 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 any Intel vPro personal computer
  – Based on a “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
Why is SecureView needed?

Before SecureView

- Separate PC required for each security domain

After SecureView

- Access applications and data from multiple security domains on a single desktop
- Reduces footprint, power, and admin cost
- Increases security posture dramatically
SecureView Features

• SecureView Management Server
  – Enterprise Scalability

• Secure Seamless Windowing – 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 classified environments w/o expensive TACLANES
  – Data at Rest Protection
SecureView Management Server

Enterprise Management Capability
Site A Cost Savings from SecureView

- PDS
- SIPR-D PC
- SIPR PC
- NIPR PC

Traditional

- SIPR-D Tunnel
- Suite B Transport
- SecureView
- Single PC

SecureView
Typical Network Infrastructure

SecureView Workstation

Single wire to workstation

Network 1

Network 2

Network 3

Standard COTS VPN Concentrator(s)
SecureView 2.x 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 (NDVM)
- VPN Isolation
- ThinVMs

User VM 1
- Policy Granularity
  - Stub Dom

User VM 2
- Policy Granularity
  - Stub Dom

User VM n
- Policy Granularity
  - Stub Dom

XenClient XT / OpenXT
- Xen Security Modules

Hardware
- nVidia/ATI GPUs
- Intel Integrated GPU
User Interface
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/G510s
  - Colored keys and LCD screen
  - LCD shows security label (text) and VM name
- Corsair Strafe RGB
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.
# SecureView Historical Roadmap

<table>
<thead>
<tr>
<th>SecureView 2.0</th>
<th>SecureView 2.1</th>
<th>SecureView 2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Released:</strong></td>
<td><strong>Released:</strong></td>
<td><strong>Released:</strong></td>
</tr>
<tr>
<td>Nov 2013</td>
<td>DEC 2015</td>
<td>January 2016 (Deploying)</td>
</tr>
<tr>
<td><strong>vPro Processor(s):</strong></td>
<td><strong>vPro Processor(s):</strong></td>
<td><strong>vPro Processor(s):</strong></td>
</tr>
<tr>
<td>• Sandy Bridge</td>
<td>• Sandy Bridge</td>
<td>• Sandy Bridge</td>
</tr>
<tr>
<td>• Ivy Bridge (3rd Gen)</td>
<td>• Ivy Bridge</td>
<td>• Ivy Bridge</td>
</tr>
<tr>
<td>• Haswell (4th Gen)</td>
<td>• Haswell</td>
<td>• Haswell</td>
</tr>
<tr>
<td>• Broadwell (5th Gen)</td>
<td>• Broadwell</td>
<td>• Broadwell</td>
</tr>
<tr>
<td><strong>Type I Hypervisor</strong></td>
<td><strong>Type I Hypervisor</strong></td>
<td><strong>Type I Hypervisor</strong></td>
</tr>
<tr>
<td>• XenClient 3.1</td>
<td>• OpenXT (XenClient 4.0)</td>
<td>• OpenXT</td>
</tr>
<tr>
<td><strong>Features / Enhancements:</strong></td>
<td><strong>Hardware Platforms / OEMs</strong></td>
<td><strong>Features / Enhancements:</strong></td>
</tr>
<tr>
<td>• Dedicated 3D Graphics Support</td>
<td>• Desktop PCs – Dell, HP, NCS</td>
<td>• Display Handler</td>
</tr>
<tr>
<td>• MultiView™ Integrated Display</td>
<td>• Laptops – HP, Dell</td>
<td>• Power Management</td>
</tr>
<tr>
<td>• ConnectView™ VDI Support</td>
<td>• Convertible Laptops - HP</td>
<td><strong>Hardware Platforms / OEMs</strong></td>
</tr>
<tr>
<td>• SecureView Mgmt Server (SVMS)</td>
<td>• Tablets / 2-in-1s – Panasonic, HP</td>
<td>• Desktop PCs – Dell, HP, NCS</td>
</tr>
<tr>
<td>• Integrated NSA CSfC Capability</td>
<td></td>
<td>• Laptops – HP, Dell</td>
</tr>
<tr>
<td><strong>Hardware Platforms / OEMs</strong></td>
<td><strong>Hardware Platforms / OEMs</strong></td>
<td><strong>Hardware Platforms / OEMs</strong></td>
</tr>
<tr>
<td>• Desktop PCs – Dell, HP, NCS</td>
<td>• Desktop PCs – Dell, HP, NCS</td>
<td>• Desktop PCs – Dell, HP, NCS</td>
</tr>
<tr>
<td>• Laptops – HP, Dell</td>
<td>• Laptops – HP, Dell</td>
<td>• Laptops – HP, Dell</td>
</tr>
<tr>
<td>• Tablets - Panasonic</td>
<td>• Convertible Laptops – HP</td>
<td>• Convertible Laptops – HP</td>
</tr>
<tr>
<td></td>
<td>• Tablets / 2-in-1s – Dell, Panasonic, HP</td>
<td>• Tablets / 2-in-1s – Dell, Panasonic, HP</td>
</tr>
</tbody>
</table>
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 since 4 April 2013

- SV 2.1 Certification & Accreditation Status
  - ACC/A2S Top Secret SCI And Below Interoperability (TSABI) ATO: 23 December 2015
  - AF DAA – DIACAP ATO: 23 December 2015

- SV 2.2 Certification & Accreditation Status
  - ACC/A2S TSABI Certificate To Field (CTF): 19 May 2016
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/
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

SecureView Workstation

Guest VM (Red) → Vnic → Vif0 → Vnic → Vif0 → Vnic → Vif1 → Vnic → Eth0 → Green Network

Guest VM (Green) → Vnic → Vif2 → Vnic

Red Network

INNER IPSEC CONCENTRATOR → Single Suite-B Tunnel

OUTER IPSEC CONCENTRATOR → Double Suite-B Tunnel

NSA Commercial Solutions for Classified Program
SecureView Deployment Requirements

- As with any network deployed by the DoD, SecureView + CSfC deployments must be properly documented and accredited through the service/agency’s AO using its existing DIACAP or Risk Management Framework (RMF) process.

- For deployments where NSA Commercial Solutions for Classified are being leveraged to tunnel classified traffic over NIPRNET infrastructure, then a CSfC registration package has to be completed and approved by NSA.

- For deployments where SecureView workstations are going to provide access to multiple levels of security (i.e. NIPR + SIPR), then the proposed Cross-Domain deployment must be approved by DSAWG.
**SecureView Deployment Requirements**

- **Service DIACAP / RMF**
  - 60 – 180 Days

- **NSA CSfC Registration**
  - 90 – 120 Days

- **DSAWG CDS Pkg**
  - 180 – 270 Days

Note: As part of the Installation Support fee, AFRL will help customers prepare and submit the required documentation as well as leverage reciprocity from previous SecureView CSfC approvals and accreditations, but the Approval Processes and the associated timelines are completely outside of AFRL control.
Summary

• SecureView is an enterprise solution that meets DoD/IC growing requirements for secure networks
  – Reduces costs
  – Increases scalability
  – Enhances security
• SecureView enables classified 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