SecureView: Government/Industry Collaboration Delivers Improved Levels of Security, Performance, and Cost Savings for Mission-Critical Applications

SecureView provides accredited cross-domain security, delivers the performance for advanced collaboration, and is estimated to reduce total cost of ownership (TCO) by up to 67 percent over single-domain architectures and 45 percent over an alternative thin-client, multi-domain architecture with results normalized to a four-year refresh cycle. The SecureView solution is the result of close collaboration among the US Air Force Research Laboratory, Intel and Citrix, and uses Citrix XenClient ™ XT [1] and Intel ® vPro™ technology. [2]

Authors:
Dr. Ryan J. Durante, DR-III, DAFC
Mr. John C. Woodruff, DR-III, DAFC
Cross-Domain Solutions and Innovation
Air Force Research Laboratory
Information Directorate
United States Air Force

Public Affairs Case Number: 88ABW-2012-6533 The material was assigned a clearance of CLEARED on 17 Dec 2012.

Table of Contents

Executive Summary

Data access and information-sharing strategies within the US Government must provide affordability without compromising the requirements for data security and operational efficiency. In a security environment marked by increasing sophistication and persistent threats, the US Air Force Research Laboratory (AFRL) led the development of a solution. AFRL engaged in a technical collaboration with Intel and Citrix resulting in SecureView, a government solution that expands on commercial off-the-shelf (COTS) capabilities in Citrix XenClient™ and Intel® Core™ i5 and i7 vPro™ processors.

SecureView has been deployed at more than one dozen federal agencies and has saved the government millions of dollars in development and TCO expenses. The solution is less vulnerable to modification or corruption than traditional software-based security solutions and provides unprecedented performance for mission-critical collaboration and media-intensive use cases than alternate hardware configurations.

As a hardened client-hosted virtualization (CHV) solution, SecureView enables independent, concurrent access to multiple 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 several Dell and HP desktop and numerous laptop models.

SecureView significantly improves all three vectors of security, performance, and cost as compared to both legacy and contemporary alternatives:

Security. Using hardware-assisted virtualization and security technologies built into select Intel® processors and chipsets, SecureView is less vulnerable to modification or corruption than traditional software-based security solutions. SecureView's advanced isolation provides the ability to run multiple securely isolated environments on a single PC. It includes a hardware-assisted trusted boot that verifies the integrity of the virtual desktop at launch, as well as hardware-assisted, accelerated disk encryption.

Performance and Responsiveness. SecureView can run on commercially available PCs, laptops or tablets with Intel® Core™ vPro™ technology-based processors with Intel® Integrated Graphics. This supports mission effectiveness by enabling analysts and other users the performance to run geographic information systems (GIS), multi-party High Definition, videoconferencing, and other performance-intensive applications that are essential to modern analysis and collaboration. SecureView's client-side intelligent virtualization and local execution avoid the performance degradations of network latency often encountered with server-side virtualization. SecureView not only provides a consistently responsive end-user experience but also offers flexibility for sites and users that need the flexibility of mobile computing; allowing users to work productively even when persistent network connectivity is lacking. The net result is demonstrable improvements to user productivity.

Costs. SecureView reduces the traditional need for each user to have separate workstations for each isolated domain. As a client-hosted virtualization (CHV) solution, it doesn't require the network and back-end build-out often necessary with server-hosted virtualization (SHV) approaches running on thin-clients. AFRL applied their direct experience in consultation with industry counterparts to conduct a detailed analysis of the TCO to deploy, manage, and support SecureView and three common deployment models. The data provided is verified by AFRL where available and based on conventional industry benchmark data otherwise. The concluding analysis estimates that SecureView reduces annual total (capital and operational) costs by up to 67 percent compared to single-domain architectures and up to 45 percent over a widely deployed thin-client, multi-domain architecture. The study shows that a site deploying SecureView to 10,000 users over a four-year period achieves cost savings of up to:

- $63.53 million compared to a traditional environment with independent security levels and three PCs per user (Environment 1)
- $73.79 million compared to a deployment with single-level security using two thin-clients and one PC (Environment 2)
- $29.85 million compared to a multi-level security solution with one thin-client (Environment 3)[3]

Developing SecureView

The 9/11 Commission highlighted the critical importance of collaboration to enable analysts to accurately and fully assess threats and share their findings across agencies to help prevent attacks. They must do this in a world where cyber-espionage, cyber-criminals, and cyber-terrorists pose an ever-increasing threat. A serious security breach to the government community can do serious harm to the nation's well-being, as well as confidence in the technology infrastructure.

Groups with responsibility for developing secure, cost-effective and powerful client environments for defense analysis have tried a number of approaches, but each presented problems that have become widely recognized.[4] Traditionally, analysts used a separate PC for each domain they needed access to. This approach was expensive to implement and support, as well as cumbersome and inconvenient for end-users. The emergence of thin-clients and desktop virtualization increased manageability and, in some cases, made it possible to provide users the convenience of a single-client system. However, with workloads running on back-end servers, deployment requires costly data center build-out for servers, networks, and storage. Even with these infrastructure investments performance has often been found to be inadequate for modern visually based applications. The result has been a poor user experience that reduces analysts' productivity and impacts their effectiveness in using modern, visually based applications.

AFRL developed SecureView in response to a direct request for the development of a secure, robust workstation that would support high-performance applications and provide independent and concurrent access to multiple security domains from a single-client system. The solution must prevent data exfiltration, be deployable with minimal impact to the host agency, and be capable of provisioning within four hours. The customer asked AFRL for a solution within 10 months, requiring rapid development and delivery of an innovative solution.

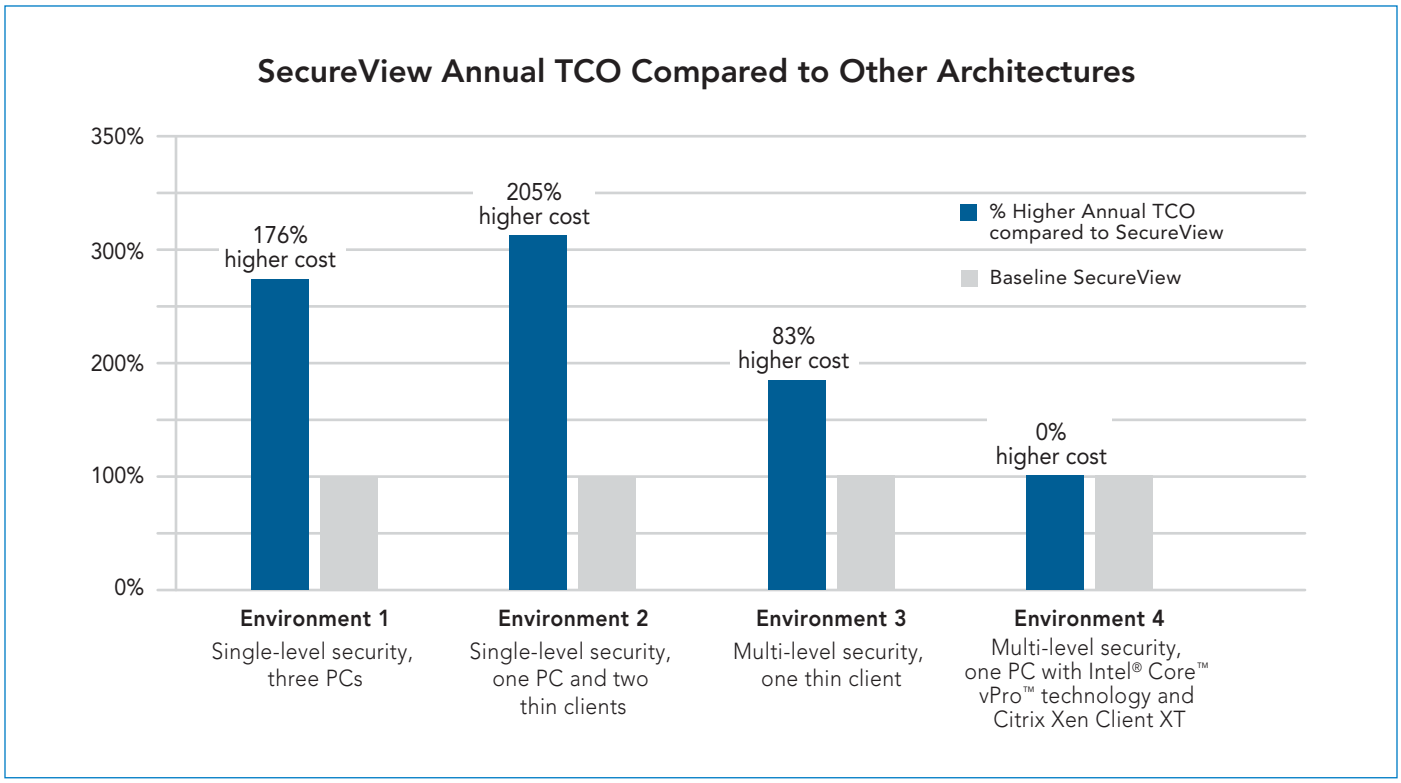

Figure 1. SecureView annual TCO. Other environments are 176 percent, 205 percent, and 83 percent higher, respectively, than the SecureView baseline (Environment 4). Results are derived from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts.

SecureView Technology Overview

SecureView's technology foundation is Intel vPro technology and Citrix XenClient XT—technologies that efficiently combine hardware and software to improve security, manageability, and performance of the client computing environment. SecureView is a flexible virtualization solution that runs on clients in either client-hosted or server-hosted modes of operation. Server-hosted modes use a thin virtual machine (VM), with a minimal operating system running on the client and applications executing on server infrastructure within the environment. In client-hosted modes, the end point operates a full operating system and applications execution within virtual containers. This TCO study assumes client-hosted operation for SecureView.

SecureView provides integrated, hardware-based functionality that supports multiple operating system environments and security domains on each end-user PC desktop or notebook via virtual containers. These capabilities are supported by Intel® Virtualization Technology (Intel® VT)[5] and provide safeguards, via Intel® Trusted Execution Technology (Intel® TXT)[6] to protect each virtual environment from malware contamination. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)[7] accelerates disk encryption. These hardware-aided security technologies render SecureView clients inherently less vulnerable than traditional software-only approaches. Additionally, new integrated graphics capabilities improve handling of high-resolution imagery and 3D graphics.

SecureView implements a true Type 1 "bare metal" client hypervisor to provide robust data and computer resource isolation by using Intel vPro technology and XenClient XT. SecureView provides hardware-assisted trusted boot, maintains isolation between multiple independent virtual machines (VMs), and verifies the integrity of the client at launch. The trusted computing base configuration state is measured, encrypted, and the measurements are sealed at installation. Upon subsequent system start, the computing base is re-measured and the encryption keys are unsealed only if they match the appropriate cryptographic response from a trusted platform module (TPM). XenClient XT Synchronizer™ enables SecureView to download centrally managed virtual desktops. Using Synchronizer, IT can centrally back up user data through a secure connection whenever the user connects to the network, define security policies for managed devices, disable XenClient PCs, and restore a user's virtual desktop on any XenClient-based device.

Comparing the Total Costs of Four Deployment Models

SecureView was developed to harden security within the government and increase analysts' effectiveness by improving their ability to use visually rich graphics, media, and collaboration tools. SecureView also delivers significant savings in both operational and capital expenses compared to prevalent alternative approaches. To assess these savings, AFRL compared SecureView's operational costs to those of three other client computing environments, reflecting the evolution of government agencies' approaches to providing access to multiple security levels.

To develop the analysis, AFRL worked closely with a business value analyst from Intel, and used a comprehensive client-compute TCO model that has been applied in a range of business and government environments.[8] The analysis uses data from actual deployments at AFRL where such data was available, and used respected sources of industry data, such as Principled Technologies' TCO Calculator, when it was not.[9] The study assumes that SecureView is deployed in a client-hosted mode.

The analysis calculates the costs to deploy and support 10,000 users for government environments which commonly use either desktop PCs over a life cycle of four years, and/or thin-client, server-hosted client environments with six-year life cycles. This comprehensive view includes the necessary build-out costs for client, server, network and other hardware over the entire life cycle. It considers power costs, the costs of pre-deployment preparation, deployment, and ongoing management costs over the upgrade cycle. The analysis also factors in user productivity impacts for each solution.

The analysis compared SecureView to two traditional, segregated architectures, where users have a separate client system for each security level, and a third, contemporary approach which provides comparable domain segregation. These architectures are more fully described on following pages.

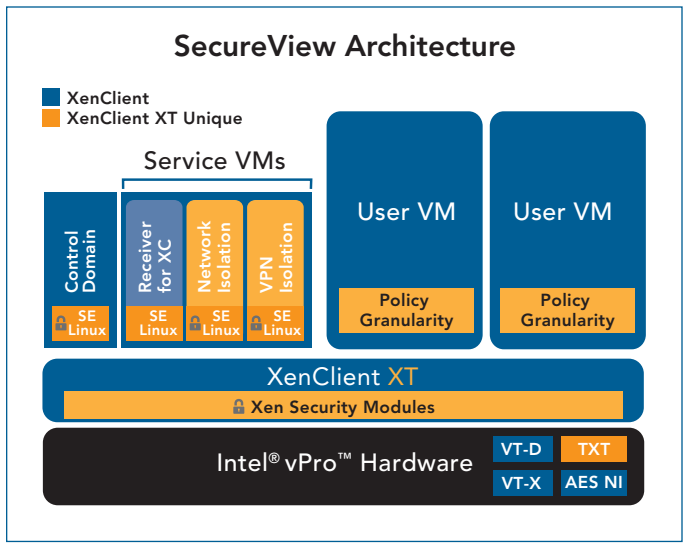

Figure 2. SecureView technology architecture.

Environment 1

Traditional single-level security environment with typically managed rich desktops. Each user has a separate PC, monitor, and network connection to back-end infrastructure for multiple security domains. The TCO analysis assumed a four-year upgrade cycle for this model.

Environment 2

Single-level environment, thick and thin-clients. Again, the user has a separate client system for each domain, but some domains are accessed via thin-clients, with access servers providing a portal to back-end infrastructure for each client. Applications on Domain A typically run on the PC, to facilitate performance-sensitive applications. Environment 2 has an assumed upgrade cycle of six years.

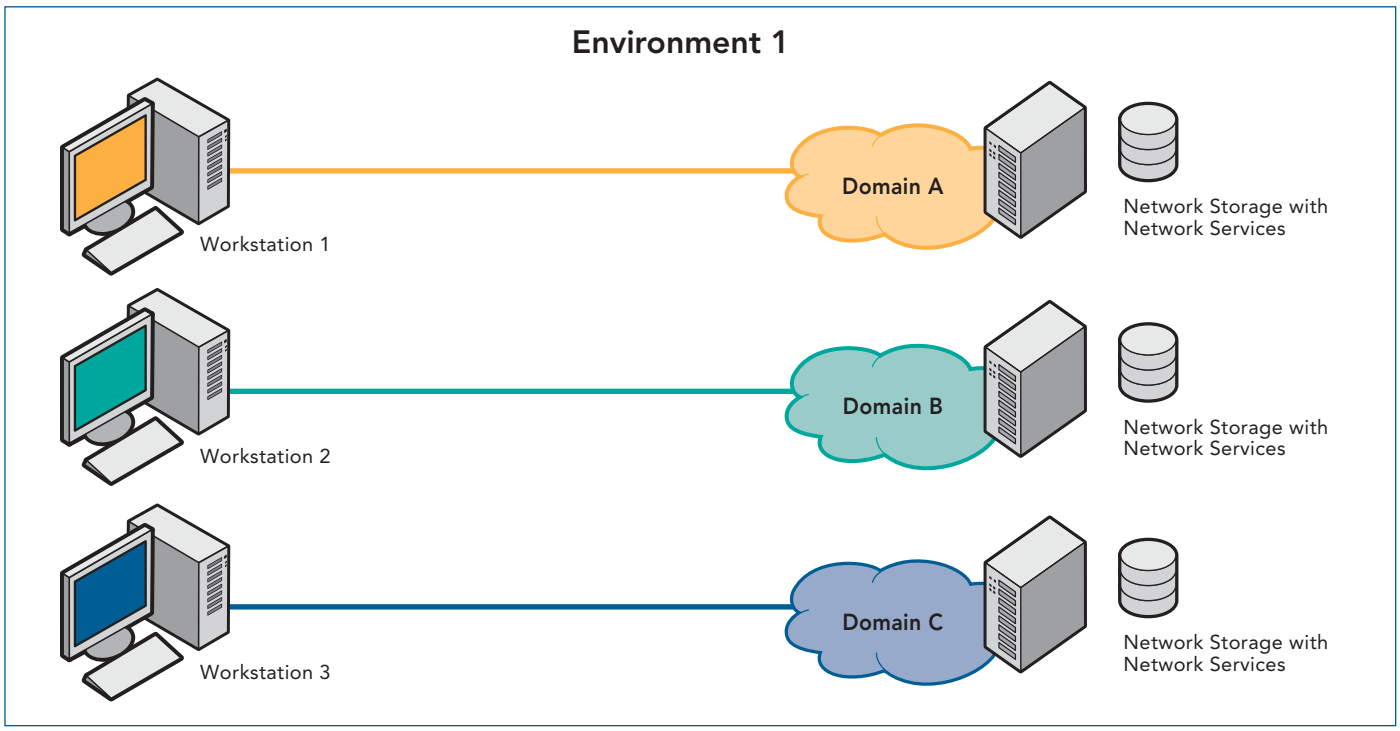

Figure 3. Environment 1. Single-level security, three PCs.

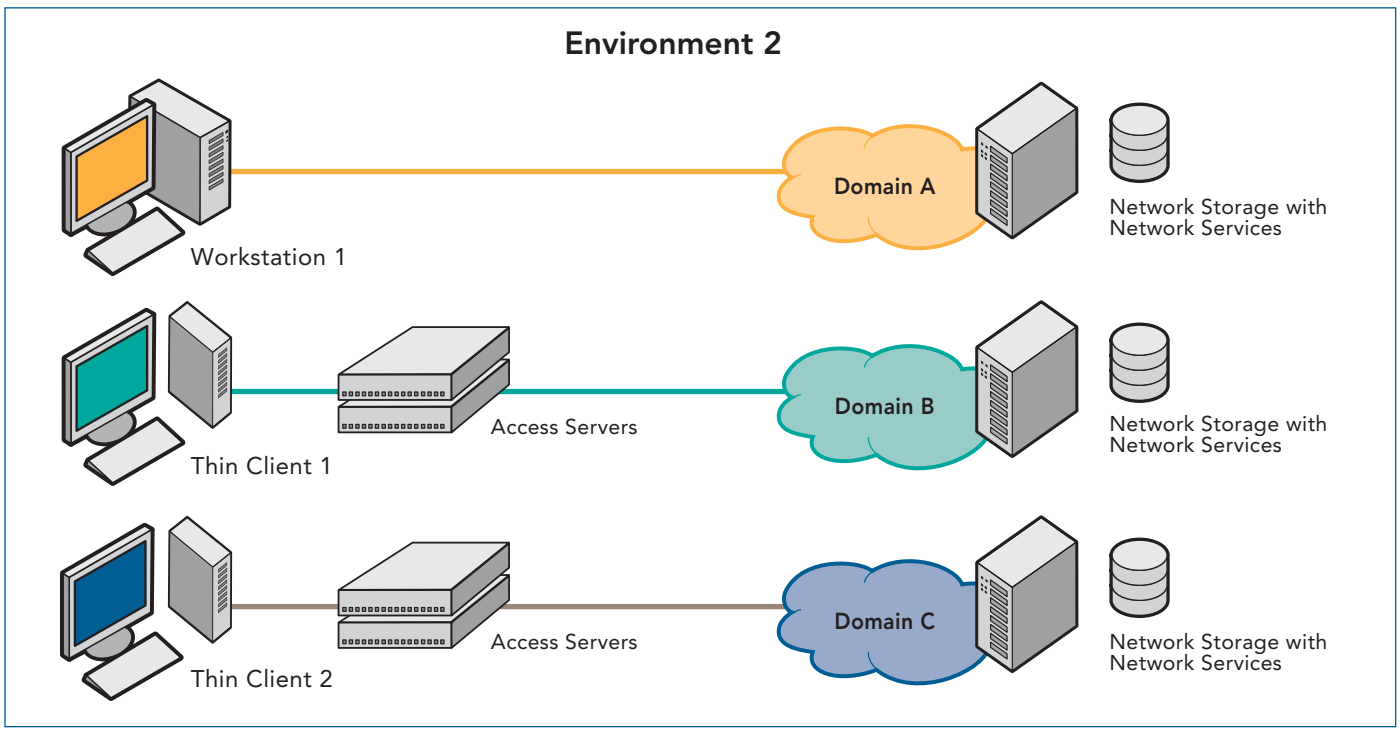

Figure 4. Environment 2. Single-level security, one PC and two thin clients.

Environment 3

Multi-level secure environment with a single thin-client and session (access servers) to provide concurrent connections to all three levels. The analysis uses data from a commonly deployed, multi-level thin-client environment for this model. The assumed upgrade cycle for Environment 3 is six years.

Environment 4

SecureView multi-level secure environment with a single intelligent, virtualized PC running Citrix XenClient XT and powered by Intel Core vPro processors providing concurrent, independent access to all three domains. The assumed upgrade cycle is four years.

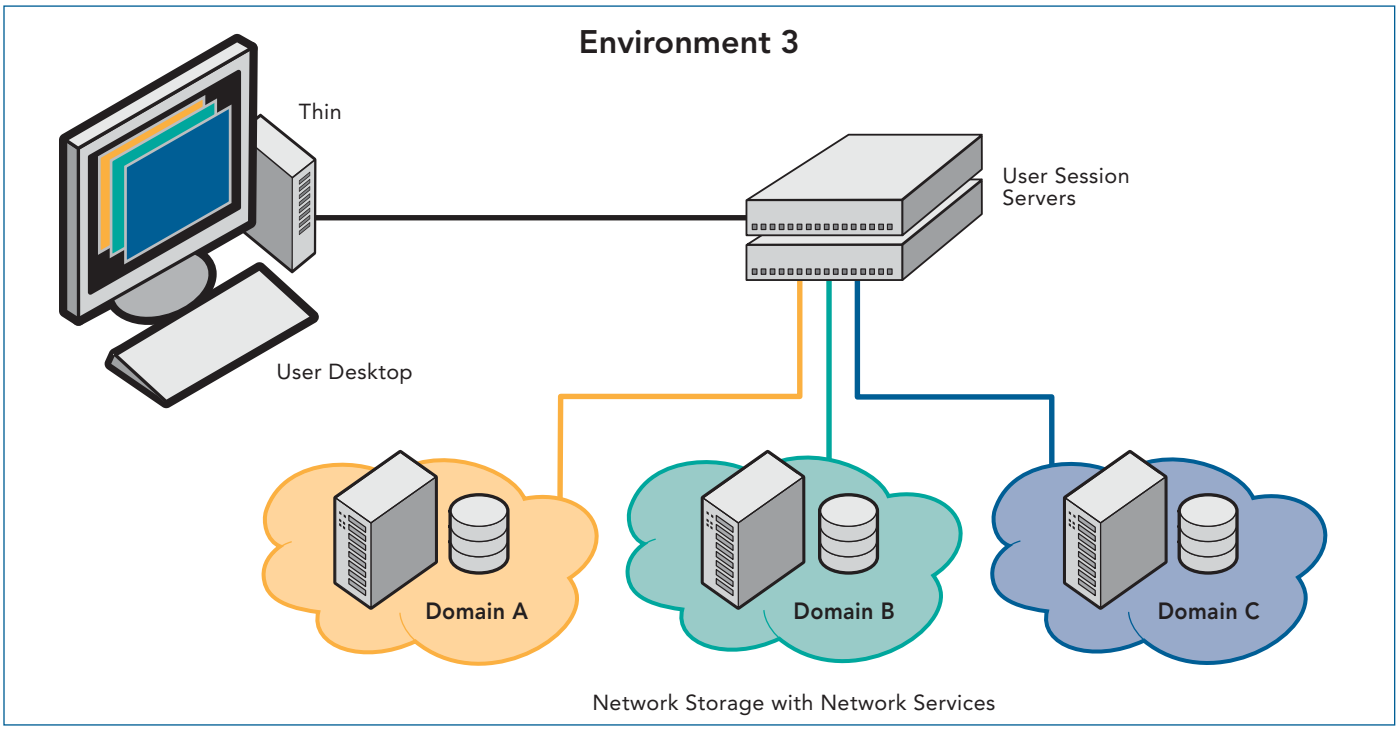

Figure 5. Environment 3. Multi-level security, one thin client.

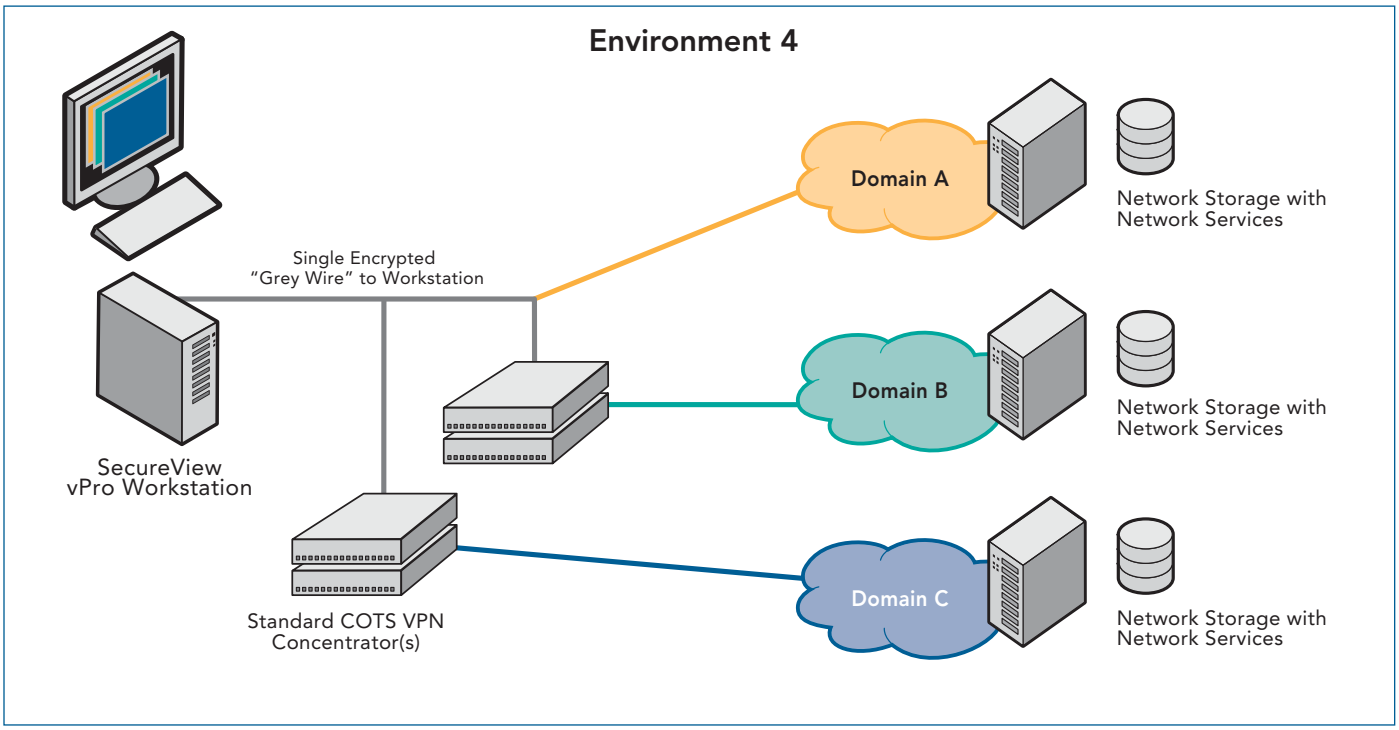

Figure 6. Environment 4. SecureView: Multi-level security, one PC with Intel® Core™ vPro™ technology and Citrix XenClient XT.

Cross-Domain Platform TCO Summary

Table 1 summarizes the cross-domain platform TCO for a deployment of 10,000 seats. It is followed by a brief discussion of the analysis and some of the major assumptions made. Figure 7 summarizes annual TCO including productivity savings.

Deployment Costs: Hardware

As expected, the acquisition cost for SecureView PCs is higher than that of thin-clients: $13.39 million for 10,000 PCs to $12.07 million for 10,000 thin-clients. However, these acquisition costs are more than offset by the added costs of server and network infrastructure build-out, among other issues.

Server and network infrastructure add significant costs to the deployment of thin-client models. Thin-clients require servers to provide access/presentation services, as well as, server infrastructure to run the server-hosted applications. The analysis calculates the clients supported per server based on AFRL's experiences, and lab tests funded by Intel and conducted by Principled Technologies. The analysis details the combined costs for access infrastructure servers for the two thin-client scenarios (Environments 2 and 3), session servers for the multi-security level thin-client scenario (Environment 3), and management servers for all four environments constitute the server deployment costs shown in Table 2.

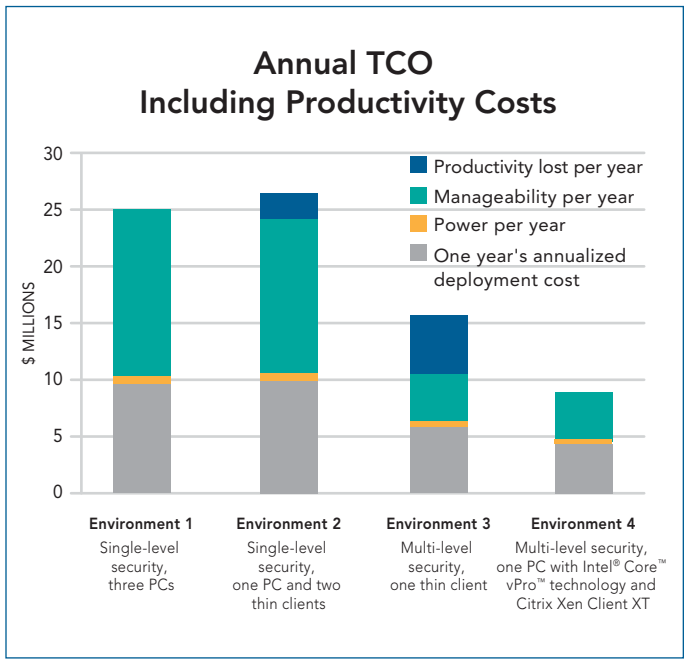

Figure 7. Annual TCO including productivity costs for 10,000 users.[11]

Table 1. Cross-Domain Platform TCO Summary for a 10,000 Seat Deployment**

	Siloed Domain Access, Single-Level		Concurrent Multi-Domain Access, Multi-Level	
Client Compute Platform	**Single-Domain, 3 Desktops Environment 1**	**Single-Domain, 2 Thin-clients + 1 Desktop Environment 2**	**Multi-Domain, 1 Thin-client Environment 3**	**SecureView: Multi-Domain, 1 vPro PC Environment 4**
TCO Summary Including Lost Productivity Costs				
Annual costs per client	$2,489	$2,745	$1,647	$901
TCO per client for the upgrade cycle	$9,956	$16,472	$9,881	$3,602
TCO for all clients for the upgrade cycle	$99,560,000	$164,720,000	$98,810,000	$36,023,000
TCO per year for all clients	$24,890,000	$27,450.000	$16,470,000	$9,006,000
TCO Summary Excluding Lost Productivity				
Annual costs per client	$2,489	$2,383	$1,103	$901
TCO per client for the upgrade cycle	$9,956	$14,297	$6,617	$3,602
TCO for all clients for the upgrade cycle	$99,560,000	$142,970,000	$66,174,000	$36,023,000
TCO per year for all clients	$24,890,000	$23,830,000	$11,029,000	$9,006,000
Annual Cost Breakdown				
One year annualized deployment cost	$9,466,000	$9,808,000	$6,644,000	$4,171,000
Power per year	$884,000	$951,000	$386,000	$295,000
Manageability per year	$14,538,000	$13,068,000	$3,999,000	$4,540,000
Productivity lost per year	$0	$3,626,000	$5,439,000	$0
Total	$24,888,000	$27,453,000	$16,468,000	$9,006,000
TCO Breakdown				
One-time deployment costs	$37,870,000	$58,850,000	$39,870,000	$16,690,000
Power for the entire upgrade cycle	$3,540,000	$5,710,000	$2,310,000	$1,180,000
Manageability for the entire upgrade cycle	$58,150,000	$78,410,000	$23,990,000	$18,160,000
Productivity lost for the entire upgrade cycle	$0	$21,760,000	$32,630,000	$0
Total	**$99,560,000**	**$164,730,000**	**$98,800,000**	**$36,030,000**

**Table is drawn from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts. Data for Environments 1 and 2 are largely based on industry data sources. Key assumptions for Environments 3 and 4 are drawn from common industry data sources, such as Principled Technologies' TCO Calculator, when actual data was not available. Key assumptions in the analysis include: SecureView deployment in a thick mode of operation; users wages are assumed to be $41 per hour, IT wages are assumed to be $63 per hour; client power state assumes 8 hours[10] on and 16 hours standby per workday; cooling power is assumed to be 1 W per system watt; power cost is assumed to be $0.1 per kWh; annual client management activities are assumed to consist of 12 asset inventories, 14 patch installations, and 5 helpdesk calls per client.

Data center build-out factors to support the server infrastructure for all four deployment environments are also factored into overall deployment costs, and shown in Table 3.

It should be noted that the analysis did not consider the fact that Environments 2 and 3 introduce the server as a single point of failure for multiple clients, since one server typically takes on the entire processing load of multiple clients. This risk can be mitigated through server and network redundancy, but this would further increase capital expenses and complexity of thin-client supporting infrastructure.

Deployment Costs: Implementation, Training and Application Porting/Replacement

In AFRL's experience, SecureView is a dramatically easier and faster approach to analyze, define, and validate requirements, and therefore, a superior implementation solution for access to multiple domains than either of the thin-client-based environments. At the same time, it is also the most cost-effective approach. The savings in Table 4 reflect roughly a tenfold difference in the costs of implementation and porting or replacing applications.

Annual Power Costs

The analysis factors in the costs of power consumption and cooling for PCs, thin-clients and monitors, as well as for servers required to support the client environments. The single-domain, three-PC environment modeled (Environment 1) had recently replaced its PCs. Environments with older PCs would see greater energy savings from refreshing their PCs and deploying SecureView, since new PCs consume significantly less power than older ones. The study assumed three monitors per user for the single-domain implementations (Environments 1 and 2), and two monitors each for the two multi-domain implementations (Environments 3 and 4). Table 5 shows that SecureView is the most energy-efficient of the four solutions with the lowest expenditures on power.

Annual Management Costs

Client management tasks are assumed to consist of 12 asset inventories, 14 patch installations, and 5 helpdesk calls per client per year.

Table 2. Hardware Deployment Costs Summary for 10,000 Users

	Single-Domain, 3 Desktops	Single-Domain, 2 Thin, 1 PC	Multi-Domain, 1 Thin	SecureView**
Server deployment costs	$3,240,000	$7,870,000	$12,210,000	$1,080,000
Desktop and thin-client costs	$31,880,000	$30,800,000	$12,070,000	$13,390,000
Network cost (client port, VPN)	$3,750,000	$3,750,000	$1,250,000	$1,280,000
Total hardware deployment costs	$38,870,000	$ 42,420,000	$25,530,000	$15,750,000

**Table is drawn from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts.

Table 3. Data Center Costs for the Entire Upgrade Cycle for 10,000 Users

	Single-Domain, 3 Desktops	Single-Domain, 2 Thin, 1 PC	Multi-Domain, 1 Thin	SecureView**
Construction costs	$40,000	$353,000	$600,000	$13,000
Port costs	$130,000	$1,145,000	$1,944,000	$43,000
Wiring costs	$7,000	$64,000	$108,000	$2,000
Total data center costs	$177,000	$1,562,000	$2,652,000	$58,000

**Table is drawn from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts.
Note that the cost of server power is a recurring cost and is included in the annual power cost shown in Table 5.

Productivity Losses

Productivity analysis is based on lab tests conducted by Principled Technologies, assuming a user wage is $41 per hour and an IT wage of $63 per hour. The analysis estimated conservatively that users in these multi-level, thin-client scenarios (Environments 2 and 3) would lose 3.25 minutes each day on each of their thin-clients due to server or network congestion. This results in a daily loss of $22,000 of user productivity across 10,000 users or $5.439 million annually for the multi-domain solution with a single thin-client (Environment 3). Environment 2, with a single PC and two thin-clients, results in annual lost productivity of $3.626 million. Note that the summary table reports the TCO results both with and without these productivity costs included.

The study assumed the cost and performance of common application or resource servers, such as those providing file, e-mail, database, Web services, and network services such as Active Directory and Domain Name System (DNS) hosting, would be uniform across all environments. Therefore, these were not included in the TCO analysis.

Security Benefits

SecureView's most important benefits did not lend themselves to inclusion in the analysis. Specifically, there is no quantification of the increase in information security provided by the SecureView technologies or any attempt to monetize the cost of a potential breach in information security. However, it is worth noting that Ponemon Institute estimates the organizational cost of a single data breach at $5.5 million.[12] Given that SecureView's landmark utilization of hardware-assisted security is intrinsically less vulnerable to modification or corruption than alternative, software-only solutions, there is additional, critical intrinsic value of risk reduction from data exfiltration and infiltration.

Table 4. Implementation, Training and Application Porting/Replacement Costs for 10,000 Users**

	Single-Domain, 3 Desktops	Single-Domain, 2 Thin, 1 PC	Multi-Domain, 1 Thin	SecureView**
Implementation costs	$34,000	$498,000	$464,000	$50,000
Training costs	$0	$1,550,000	$1,600,000	$1,211,000
Application porting and replacement costs	$38,000	$3,546,000	$3,508,000	$38,000

** Table is drawn from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts.

Table 5. Power Costs per Year for 10,000 Users**

	Single-Domain, 3 Desktops	Single-Domain, 2 Thin, 1 PC	Multi-Domain, 1 Thin	SecureView**
Total power consumed (kWh)	8,844,000	9,514,000	3,856,000	2,948,000
Cost of power	$884,400	$951,400	$385,600	$294,800

** Table is drawn from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts. Client power state assumes 8 hours on and 16 hours Standby per workday. Cooling power is assumed to be 1 W per system watt. Power cost is assumed to be $0.1 per kWh.

Table 6. Total Management Costs per Year**

	Single-Domain, 3 Desktops	Single-Domain, 2 Thin, 1 PC	Multi-Domain, 1 Thin	SecureView**
Total manageability costs	$14,538,000	$13,068,000	$3,999,000	$4,540,000

** Table is drawn from a detailed spreadsheet resulting from the TCO analysis conducted by AFRL in consultation with industry experts.

Conclusion

SecureView provides independent, concurrent access to multiple security domains from a single-client platform. The architecture establishes a new best-of-breed baseline in meeting the US Government's requirements for a secure data analysis and collaboration environment that is robust, affordable, easily deployable in multiple client configurations and supports mission effectiveness by enabling analysts to run the latest visually based software tools without sacrificing user experience.

With its flexible architecture and foundation in COTS technologies, SecureView is a readily deployable solution that enables agencies to achieve the cost and manageability benefits of modern desktop virtualization while increasing the security of the information infrastructure. It provides the flexibility of a server-hosted or a lower-cost client-hosted mode of operation, and offers straightforward ways for organizations to add security domains as project requirements change. In addition, SecureView is not a closed proprietary solution—it is based on Xen open source hypervisor and COTS hardware technologies that are easily accessible and affordable to acquire by government and private sector enterprises.

SecureView not only provides the convenience of multi-domain access from a single-client without performance compromises, but it is also distinguished from alternate approaches by setting a precedent in extending the secure multi-domain access boundary to mainstream mobile use environments. Its availability on Intel Core vPro processor-based notebook computers, along with an increasing variety of cutting-edge business Ultrabooks™ and tablets, enables security-sensitive users the flexibility to function in a wider range of settings, including those where a persistent network connection is unavailable.

The project execution of AFRL, Intel and Citrix is an excellent example of effective government/industry collaboration. The commitment and teamwork coupled with the use of robust COTS technologies enabled AFRL to meet the customer's request within months and deliver a solution that enhances the security of some of the nation's information infrastructure and assets. SecureView not only improves the productivity and effectiveness of analysts and other key users by enabling them to better support their organization mission, it does so with dramatic cost savings.

[1] For an overview of Citrix XenClient XT, see: http://www.citrix.com/products/xenclient/features/editions/xt.html.

[2] An overview of Intel vPro Technology is at: http://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html. Intel® vPro™ technology is sophisticated and requires setup and activation. Availability of features and results will depend upon the setup and configuration of your hardware, software, and IT environment. To learn more, visit http://www.intel.com/technology/vpro.

[3] Results are derived from a detailed spreadsheet which captured the TCO analysis conducted by AFRL in consultation with industry experts. All results were normalized to a four-year life cycle.

[4] For a discussion of the intelligence community's need for hardware-based information security, see, Michael Mestrovich, Implementing New Hardware-Based Information Security Capabilities, 26 October 2010: http://www.intel.com/Assets/PDF/whitepaper/itc-snb_hardware_security_capabilities.pdf.

[5] Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Consult your system manufacturer. For more information, visit http://www.intel.com/go/virtualization.

[6] Intel® Trusted Execution Technology (Intel® TXT). No computer system can provide absolute security under all conditions. Intel TXT requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1. For more information, visit http://www.intel.com/technology/security.

[7] Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

[8] Intel disclaims any responsibility or liability for any errors or inaccuracies that may appear in the model or which may have occurred in the underlying assumptions used to create the analysis discussed in this paper.

[9,10] For a whitepaper by Principled Technologies, see http://www.principledtechnologies.com/clients/reports/Intel/CompModelsTCO1107.pdf. The TCO Calculator is at http://www.principledtechnologies.com/Clients/Reports/Intel/ComputeModelTCOCalc1107.xls. The TCO Calculator was developed with funding support from Intel Corporation.

[11] Chart is derived from a detailed spreadsheet developed as part of the TCO analysis conducted by AFRL in consultation with industry experts.

[12] 2011 Cost of Data Breach Study: United States. Benchmark Research Conducted by Ponemon Institute, March 2012.

Printed in the USA 1112/WS/OCG/XX/PDF ♻ Please Recycle 328282-001US