CASE STUDY
Intel® Core™ i5 and i7 vPro™ Processors
Government
Client Security

SecureView Improves Security, Costs, and Collaboration for Government Users

Air Force Research Laboratory (AFRL) teams with Intel and Citrix to increase client security while saving millions of dollars annually

"SecureView is vital to the nation's security. It improves the productivity and effectiveness of intelligence analysts and other key users while saving millions of dollars. The use of COTS technologies and the close teamwork and commitment from Intel and Citrix allowed us to deliver the solution within months."

– Dr. Ryan J. Durante, Chief of Cross Domain Solutions and Innovation, AFRL Information Directorate, United States Air Force

Client strategies for the U.S. Government must be affordable and readily deployable while meeting the most stringent requirements for data security and operational efficiency. At the request of a customer, AFRL engaged with Intel and Citrix to create SecureView, a solution that expands on capabilities in Citrix XenClient* and 2nd- and 3rd-generation Intel® Core™ i5 and i7 vPro™ processors to meet these requirements. SecureView, which has been deployed at more than a dozen federal agencies, is less vulnerable to modification or corruption than traditional software-based security solutions. It also provides high performance for mission-critical collaboration and saves the government tens of millions of dollars in total cost of ownership (TCO) for every 10,000 users to which it is deployed.

CHALLENGES

- **Visually-based applications.** Analysts demand higher client performance to improve the effectiveness of dynamic, multiparty collaboration without limitations on the use of visualization software, complex data set analysis, geographic information systems (GIS), and other performance-intensive applications that are essential to modern analysis and collaboration.
- **Costs and complexity of multiple security domains.** Many analysts work across numerous security domains simultaneously. Traditionally, analysts have used separate PCs or workstations for different data domains, which is costly and cumbersome, or used server-hosted virtualization with thin clients, which also raises costs and risks poor performance due to network latency or server contention.

SOLUTIONS

- **Government-industry collaboration.** AFRL engaged in a technical collaboration with Citrix and Intel to develop a hardened solution built on commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technologies.
- **Hardware-aided security.** SecureView uses the capabilities of PCs and laptops with 2nd- and 3rd-generation Intel Core i5 and i7 vPro processors with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), Intel® Trusted Execution Technology (Intel® TXT), and Intel® Virtualization Technology (Intel® VT).
- **Citrix XenClient XT.** Citrix XenClient XT implements client-hosted virtualization with a true bare-metal hypervisor, using the Intel® technologies to provide robust isolation between virtual environments and verify the integrity of the client at launch.

IMPACT

- **Mission effectiveness.** SecureView provides local application execution and concurrent access to multiple security domains. This supports mission requirements, giving analysts excellent performance to run leading-edge applications, assess potential threats, and share findings across agencies.

Annual TCO Including Productivity Costs

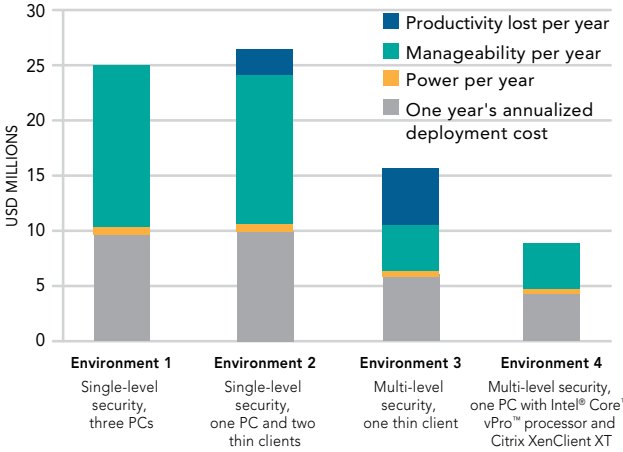

Figure 1. Annual TCO including productivity costs, drawn from TCO study conducted by AFRL and Intel[1]

	Siloed Domain Access, Single-Level		Concurrent Multi-Domain Access, Multi-Level	
Client Compute Platform	**Environment 1 Single Domain, 3 Desktops**	**Environment 2 Single Domain, 2 Thin Clients + 1 Desktop**	**Environment 3 Multi-Domain, 1 Thin Client**	**Environment 4 SecureView: Multi-Domain, 1 PC with Intel® Core™ vPro™ processor**
TCO Summary				
Annual costs per client	USD 2,489	USD 2,745	USD 1,647	USD 901
TCO per client for the upgrade cycle	USD 9,956	USD 16,472	USD 9,881	USD 3,602
TCO for all clients for the upgrade cycle	USD 99,560,000	USD 164,720,000	USD 98,810,000	USD 36,023,000
TCO per year for all clients	USD 24,890,000	USD 27,450,000	USD 16,470,000	USD 9,006,000
TCO Breakdown				
One-time deployment costs	USD 37,870,000	USD 58,850,000	USD 39,870,000	USD 16,690,000
Power for the entire upgrade cycle	USD 3,540,000	USD 5,710,000	USD 2,310,000	USD 1,180,000
Manageability for the entire upgrade cycle	USD 58,150,000	USD 78,410,000	USD 23,990,000	USD 18,160,000
Productivity lost for the entire upgrade cycle	USD 0	USD 21,760,000	USD 32,630,000	USD 0
Total	**USD 99,560,000**	**USD 164,730,000**	**USD 98,800,000**	**USD 36,030,000**

Table 1. Cross-domain platform TCO summary based on a 10,000-seat deployment[2]

SecureView's hardware-aided security helps agencies cut costs and protect sensitive information

- **Security.** Hardware-aided security helps make SecureView more difficult to breach than software-only solutions. SecureView is NIST 800-53–certified as High in Confidentiality and Integrity, and Medium in Availability.
- **Savings.** TCO analysis conducted by AFRL and Intel shows that SecureView is estimated to reduce TCO by up to 67 percent compared to single-domain architectures, and by up to 45 percent over a widely deployed solution that uses thin clients and server-hosted virtualization to provide concurrent, multi-domain access.
- **Flexibility.** With its COTS/GOTS foundation, SecureView is easy to deploy. It also enables agencies to add and remove new security domains quickly as project requirements change. It is supported on laptops, increasing agencies' ability to protect sensitive information in diverse environments.

Find the solution that's right for your organization. Contact your Intel representative, visit **Business Success Stories for IT Managers**, or explore the **Intel IT Center**.

[1,2] Results are a subset of those in a detailed spreadsheet based on TCO analysis conducted by AFRL and Intel with assumptions validated by AFRL, Intel, and 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. Results are normalized to a four-year refresh cycle. Key assumptions in the analysis include: SecureView deployment in a thick mode of operation; users wages are assumed to be USD 41 per hour, IT wages are assumed to be USD 63 per hour; client power state assumes 8 hours On and 16 hours standby per work day; cooling power is assumed to be 1 W per system watt; power cost is assumed to be USD 0.1 per kWh; annual client management activities are assumed to consist of 12 asset inventories, 14 patch installations, and 5 help desk calls per client. Intel disclaims any responsibility or liability for any errors or inaccuracies that may appear in the TCO model or which may have occurred in the underlying assumptions used to create the analysis discussed in this summary.

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/

No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (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. For more information, visit http://www.intel.com/technology/security.

The Intel® vPro™ platform 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.

Intel® Virtualization Technology 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. Software applications may not be compatible with all operating systems. Consult your system manufacturer. For more information, visit http://www.intel.com/go/virtualization.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. **For more information go to http://www.intel.com/performance**

Intel does not control or audit the design or implementation of third party benchmark data or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmark data are reported and confirm whether the referenced benchmark data are accurate and reflect performance of systems available for purchase.

Printed in USA Please Recycle 1112/LJ/TDA/XX/PDF 328247-001US