Solution Brief

Intel® vPro™ Technology

Trusted Platform Management

GENERAL DYNAMICS
C4 Systems

Department of Defense Creates a Secure, Virtualized Environment

Challenges	Government workers and warfighters need to: ▪ Access information from multiple networked security classifications from a single client PC. ▪ View classified information on mobile clients in a variety of secure locations. ▪ Help prevent information leaks from PCs while increasing their assured information sharing. ▪ Reduce the number of PCs they have been using from three—or more—to one.
Solutions	▪ **General Dynamics Trusted Virtual Environment (TVE) Desktop*** allows the end user to simultaneously use different OSs, such as Microsoft Windows*, Linux*, and Solaris*, in different networked security classifications—such as Top Secret, Secret, and Unclassified. ▪ **Intel® Trusted Execution Technology (Intel® TXT)**, included in Intel® vPro™ technology, provides a hardware-based security foundation that enables high levels of protection for information stored, processed, and exchanged on PCs. ▪ **Intel® Virtualization Technology (Intel® VT)**, also included in Intel vPro technology, provides hardware isolation, allowing several virtual environments to run securely on a single PC, increasing flexibility, performance, and system utilization. This solution operates within a virtual environment, reducing IT costs while improving security. From a single PC, it gives workers and warfighters access to information critical to fulfilling the Department of Defense's strategic and tactical missions.

GHOST TVE™
General Dynamics High Assurance Open Scalable Technology

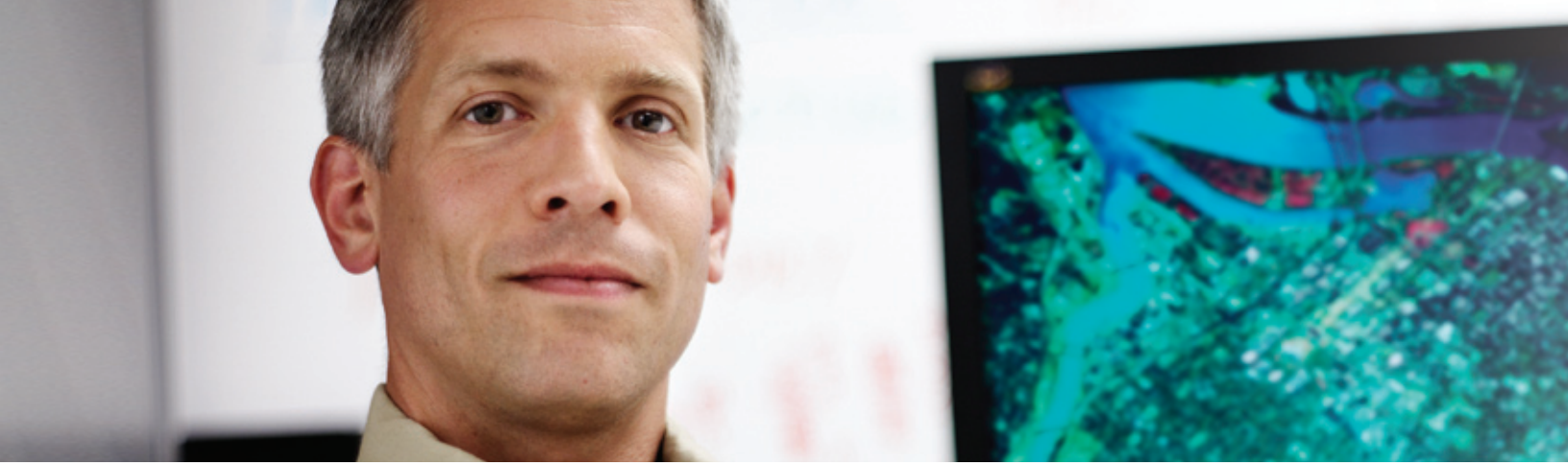
Executive Summary

The Department of Defense's (DoD's) necessarily complex security requirements traditionally resulted in the physical separation of classified information onto different networks and computer systems. This created strong security, yet also created higher total costs and impeded access to necessary information. The DoD is addressing these issues with the TVE Desktop, a General Dynamics High Assurance Open Scalable Technology (G.H.O.S.T.)*, which features Intel TXT and Intel VT.

This solution offers:

- Access to more information using fewer computers and less power in less space, and saving weight on military platforms
- The ability to use one computer to securely access information and applications in several networked security domains at the same time, such as Secret, Secret/Releasable, and Unclassified
- National Security Agency (NSA)-evaluated trusted computing capabilities within the DoD environment
- Use of commercial-off-the-shelf (COTS) OSs and hardware to support both legacy and future applications

This new, secure virtualization technology gives government workers and warfighters access to more information when they need it, enabling them to be more effective in their jobs. By using one computer instead of three or more to access different networked security classifications, the DoD can drive down total costs for their mission, enterprise, and business systems.



Case Study 1: Internet Connection into Government and Commercial Networks

Problem: By only firewalling the Internet into protected networks, client and server computers once infected can easily spread malicious code within the protected networks. End-user mistakes, zero-day operating system bugs, and extensive and continual necessary patching create an environment where even the protected network has to be perceived as actively hostile.

Solution: Isolate the Internet. "Safe browsing" is a concept developed by Industry and offered by TVE Desktop. The Internet is "crypto-tunneled" to each client and server into an Internet virtual machine (VM). If the OS in that Internet VM gets corrupted, the malicious code cannot "see" any other computers on the protected network to infect, except the Internet gateway router and one or two network servers (DHCP, print server, e-mail POP server). The Internet VM can be made non-persistent such that it gets created as a new VM each time the user logs in. This eliminates the need for any recovery activities if the VM gets corrupted in any way.

The Challenge: Secure Access to Information

To protect our nation, the DoD requires several highly secure, independent, and closed IT infrastructures. However, many government workers and warfighters need simultaneous access to two or more of these infrastructures. Older technologies led to many approaches to physical separation: duplicated infrastructures, different rooms for different information, KVM switches, and more.

This complexity caused several problems, including:

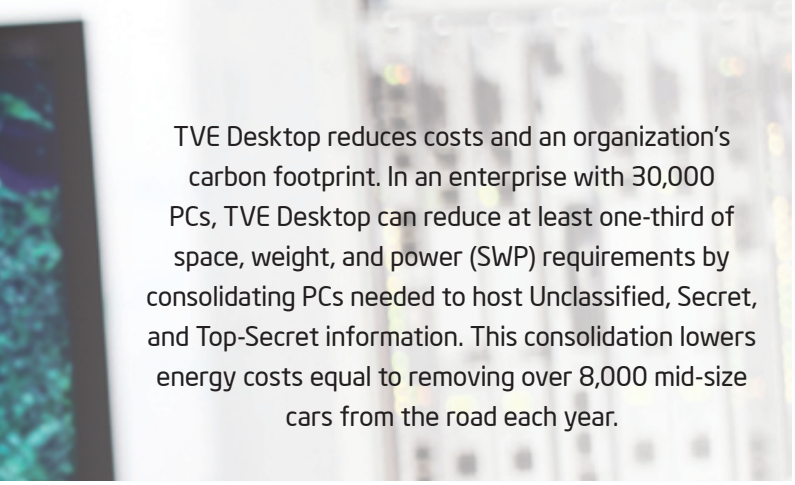
- Multiple systems for each government worker and warfighter to access the information they needed
- Difficulty in accessing and sharing information, which inhibited effective operations
- Large rooms to handle redundant equipment
- Increased purchasing and maintenance costs

Some workers had three or more workstations in their work areas, and they still could not access all the information they needed because they had run out of space.

The DoD's Vision

- A single client computer in each user's workspace
- Simultaneous access to information from different networked security classification IT infrastructures
- An agile and adaptable technology that can be used for desktops, laptops, and other mobile computers, or even for specialized mission systems

Figure 1. General Dynamics Trusted Virtual Environment (TVE) Desktop* lets workers access networks with different security classifications.



TVE Desktop reduces costs and an organization's carbon footprint. In an enterprise with 30,000 PCs, TVE Desktop can reduce at least one-third of space, weight, and power (SWP) requirements by consolidating PCs needed to host Unclassified, Secret, and Top-Secret information. This consolidation lowers energy costs equal to removing over 8,000 mid-size cars from the road each year.

The Solution: General Dynamics Trusted Virtual Environment (TVE) Desktop*

TVE Desktop (a part of the G.H.O.S.T. suite) offers multi-level and cross-domain capabilities in a desktop PC. Its advanced security features are provided by hardware assistance using Intel TXT and by high-robustness virtual machine monitor (VMM) software from General Dynamics. By adding high-robustness security only at critical points in the security architecture, the TVE Desktop can keep pace with most technology advancements with minimal recertification effort. The result is a useful, cost-effective, and evolvable NSA-evaluated PC, allowing the end user to simultaneously access and process information from multiple security domains on the same physical machine.

General Dynamics developed the TVE Desktop taking advantage of Intel vPro technology. This single desktop solution offers multi-domain capabilities and can even host cross-domain solutions within its virtual machines (see Figure 1). By using Intel vPro technology, the DoD can be sure the trusted components of the TVE Desktop have not been tampered with. Table 1 describes features and benefits.

Trusted Platform Management Features

Intel vPro technology includes Intel TXT and Intel VT. Two components of Intel VT—Intel® VT-x and Intel® Virtualization Technology for Directed I/O (Intel® VT-d)—are implemented in the TVE Desktop. Intel VT-x enables a new privilege space where the VMM software can operate and reduces the size and complexity of the VMM software, improving its efficiency and enabling greater functionality. Intel VT-d is a hardware enhancement for I/O virtualization that is part of core logic chipset. It defines an architecture for direct memory access (DMA) remapping that improves system reliability, enhances security, and enables direct assignment of I/O devices to unmodified or paravirtualized virtual machines (VMs).

These technologies enable developers and the security community to deliver higher levels of system security and information assurance in PC computing solutions. A key aspect of that protection is the provision of an isolated execution environment, along with associated sections of memory, where operations can be conducted on sensitive data, strongly segregated from other parts of the computer. Additionally, a sealed portion of storage, where sensitive data such as encryption keys can be kept, helps shield sensitive data from being compromised if attacked by malicious code. Attestation mechanisms work with Intel TXT to help ensure the integrity of code that is creating and maintaining this protected environment.

Table 1. Trusted Platform Management Features and Benefits

Feature	Benefits
Secure memory protection area	Safeguards applications in isolated, protected execution environments; unauthorized software on the platform can not observe or compromise the information being operated upon.
Authenticated code execution area	Protects the authenticated code module, which verifies the hardware configuration, enables memory protection for the domain manager, and records the identity of the domain manager before transferring control to it.
Memory access policy enforcement	Shields hardened (trusted) software running in memory pages from viewing or modification by unauthorized applications; erases all traces of measured launch environments from memory once it terminates.
Policy storage	Prevents unwanted execution environments from running, and protects the virtual machine monitor (VMM) from compromise by allowing the user to set policy regarding the execution environments allowed to run on the platform.
Software attestation hashes	Helps ensure that the protected execution environment is correctly invoked and enables measurement of the software running in the protected space, which is essential for determining if an execution environment has been tampered with.
Crypto key storage	Helps prevent loss of sensitive data from attacks that can occur when encrypted data has been transferred to other platforms; allows the release (decryption) of data only to an executing environment that matches the one where the sensitive data was encrypted.
I/O virtualization support	Enables greater reliability, availability, and trust in virtual environments with isolation from Intel® Virtualization Technology for Directed I/O (Intel® VT-d) hardware assistance; Intel VT-d provides remapping capability for controlling and monitoring direct memory access (DMA) and also performing direct I/O assignment under the control of the system software.
Trusted boot	Builds more secure platforms, with controlled launch and registration of the measured launch environment and system software components.

Intel® Trusted Execution Technology

Designed to help protect against software-based attacks, Intel TXT integrates security features and capabilities into the processor, chipset, and other platform components. This hardware-rooted security:

- Isolates and limits the effects of software-based attacks.
- Allows the usability advantages of COTS hardware, OS, and software while providing a secure foundation for TVE Desktop.
- Delivers increased security in platform-level solutions through measurement and protection capabilities.

When used in conjunction with Intel VT, the protected execution environments provided by Intel TXT are capable of running a wide variety of OSs and applications.[1]

Intel® Virtualization Technology (Intel® VT)

Virtualization solutions enhanced by Intel® Virtualization Technology (Intel® VT) allow a single platform to run multiple OSs and applications as independent virtual machines (VMs); one physical computer functions as multiple "virtual systems." In secure environments like military networks, virtualization eliminates the need for physical hardware separation between secure applications and non-secure applications. Fewer physical platforms translate into substantial capital and operating cost savings.

Virtualization involves a software program called a virtual machine monitor (VMM) or hypervisor that abstracts hardware to different partitions—VMs. It also coordinates shared hardware between multiple partitions. Hardware emulation allows guest OSs to run in a hardware environment different from their original environment.

Case Study 2: Interagency Mission Planning and Coordination

Problem: Mission planning and real-time coordination in today's environments require collaboration from a variety of sources: coalition forces, foreign agencies, federal agencies, and state governments and agencies. Those plans require review and need to be shared amongst all stakeholders. Planning occurs all the time: pre-mission in operation centers, en route on transports, and on-mission in the theater of operation. There are few tools and mission components to make this process efficient.

Solution: TVE Desktop with integrated cross-domain applications. Integrated cross-domain applications and collaboration tools, such as chat with TVE Desktop, allow warfighters to collaborate with planners. Planners now have simultaneous access to relevant information from the separate networks and can easily combine information from the various security domains and interagency networks. With simple drag-and-drop, those plans can be checked and sent for review by stakeholders. Information from these fully coordinated plans can then be sent, again with simple drag-and-drop, to those with need to know in all security domains.

Benefits

By creating the TVE Desktop, the DoD will begin to:

- Drive down networking, desktop, and maintenance costs.
- Reduce size, weight, and power requirements.
- Increase government worker and warfighter effectiveness.
- Increase the manageability of their IT infrastructures.

They can now replace the two, three, or even more PCs presently in their work spaces with one PC. Importantly, this one PC will provide simultaneous access to information from multiple networked security classifications. The DoD also increases their use of COTS hardware and OSs, further reducing costs and complexity.

The TVE Desktop has obtained necessary government security evaluations. It has also been accredited through both the Top Secret and Below Interoperability (TSABI) process, and the Secret and Below Interoperability (SABI) process. It is a listed technology by the U.S. Unified Cross-Domain Management Office (UCDMO).

Conclusion

Implementing the new solution enabled by Intel and developed by General Dynamics, the DoD can now operate within a virtual environment and save IT costs while maintaining required levels of security. Government workers and warfighters can securely access the information they need to do their jobs effectively, supporting the DoD's strategic and tactical missions.

TVE Desktop is scalable and is being developed for other platforms such as servers and handheld devices. In addition, its security capabilities will be expanded to allow simultaneous access to all security levels and to allow mobile PCs access to classified information.

For information on implementing this solution, visit General Dynamics at www.gdc4s.com/tve and Intel at www.intel.com/go/military.

GENERAL DYNAMICS
C4 Systems

1 For more information on Intel TXT, refer to http://softwarecommunity.intel.com/articles/eng/3702.htm.

Printed in USA 0608/NSB/KC/LT/1K Please Recycle 320070-001US