

Secure Virtualization: Today's Reality

Secure virtualization is an exciting new technology that allows you to secure your computing systems, networks, and data while simultaneously remaining connected to trusted and untrusted networks. Secure virtualization delivers security along with the key benefits of virtualization, which include reduced total cost of ownership, reduction in space, weight, power and cooling, and simplified maintenance.

Therefore, secure virtual environments shrink your IT footprint, decreasing your administration and maintenance costs while expanding your ability to securely access information from both trusted and untrusted sources.

Over the past decade, both small and large organizations have grappled with dramatic growth on three fronts: 1. the amount of information needed that exists external to the organization, 2. the need to securely transfer information to and from other organizations, and 3. the number of threats to both the data and the IT systems on which the data resides. When addressing information sharing needs, organizations have been faced with:

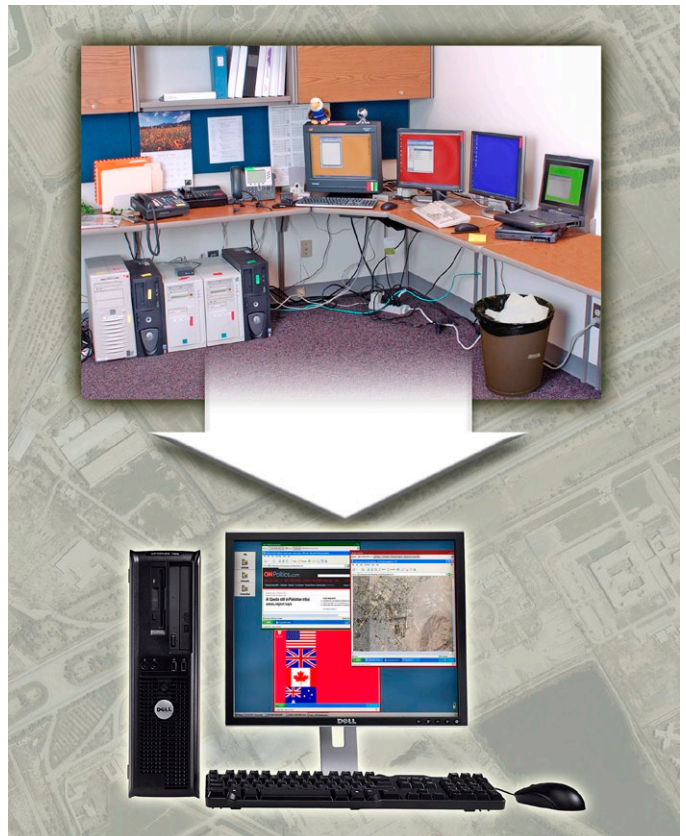
- Increasing implementation costs
- Increasing complexity of the systems they have to manage
- Inability to share information and/or share information securely

Today, however, we see a shift toward enabling technologies that can help isolate and protect the information and the IT system on which it resides. One of the key technologies it brings is the processing capacity of multiple PCs onto a single desktop or laptop machine so that multiple virtual machines can be utilized within a "secure virtual environment." This secure virtual environment means one computer that can securely isolate multiple networks or domains into independent virtual machines.

By using secure virtualization, multiple virtual machines are created within a single computer. Each virtual machine can run different operating systems or security levels and appear in separate "windows" on a shared computer and monitor. The separation between each virtual machine is trusted — ensuring that the data in each virtual machine is encapsulated and cannot pass through to another virtual machine. A secure virtual environment solution provides both a root of trust in hardware and independent health assessment checks to enable the end solution security to be certified by the DoD.

Secure virtualization provides:

- A full-performance multi-domain client solution for all virtual machines to include graphics and bandwidth intensive applications such as streaming video



Note: security classification labels shown on this equipment are for example purposes and do not reflect any actual classification; all information shown is unclassified. CNN web image courtesy CNN.

- Network consolidation and ease of technology transition
- No increase in bandwidth requirements
- Multi-level enablement without changes to the backend infrastructure
- Redundancy/reliability in software versus costly hardware redundancy

In this paper, we will discuss how these technologies can provide secure access to information from multiple networks, including multiple security levels on a single mission platform.

Your challenge: Accessing multiple networks at once

The hurdle preventing most intelligence and defense organizations from secure and effective assured-information sharing is a profound gap (in most cases, literally a physical gap) between partitioned security networks. This divide has sometimes prevented operators from easily connecting to the information they need. At the same time, on the back end, IT groups have struggled to provide this access cost effectively while, more importantly, insulating the information across domains and within specific compartments. In another instance, the threat of cyber attacks has led organizations to remove open internet access or strictly prohibit its use. While this may help to prevent the attack, it has the unfortunate side effect of limiting the ability of the organization to gather needed information that exists on the internet.

Overcoming these challenges requires a dynamic, cost-effective technology solution that taps into mainstream enterprise management services, is able to connect, without modifications, to existing physical and virtual private networks, and supports standard images on those networks.

Secure virtual environments provide the high-performance foundation for multi-domain and cross-domain functionality while dramatically reducing the total cost of system administration and maintenance.

A leading approach: a Trusted Virtual Environment

General Dynamics C4 Systems' Trusted Virtual Environment (TVE), utilizing High Assurance Platform® (HAP) technology, provides multiple independent levels of security (MILS)-based technology within a single computer. Using integrity mechanisms built into the platform, the PC can run multiple operating systems — Linux®, Windows®, Trusted Solaris™ — simultaneously in different security domains, including Unclassified, Secret and Top Secret. The stability and security of the system are further managed by industry standard, client health assessment protocols.

A Hypothetical Case Study

The Mission. A new mission has been defined for law enforcement activities in human trafficking. Liaisons have been established between the agency and various foreign interests and non-government organizations (NGO). Though each of these organizations maintains database and web services on suspected offenders to which the agency has been provided access, they also maintain different security standards. For example, some are state-sponsored and are subject to foreign monitoring operations. Also, some NGOs are operating in unstable political landscapes and are subject to the shifting attitudes of their host country. Other partners are well-meaning, but do not have the resources and expertise to protect their networks from infiltration.

Results. Using a secure virtual environment, the mission was carried out effectively by providing access to multiple levels of security simultaneously, but also by restricting access to domains and compartments across the agencies, NGOs and the foreign entities. Not only was the data and information secure, the environment promoted increased system-wide mobility for operators. And, the mission benefited from reduced cost associated with running multiple platforms while requiring fewer network-support personnel.

Today's leading Trusted Virtual Environments are built on next-generation Intel® vPro™ and, with other upcoming chipsets including emerging broad industry standards from the Trusted Computing Group™. The Trusted Virtual Environment features:

- Hardened, industry-standard compliant, government-evaluated hypervisor software;
- Next-generation commercial, off-the-shelf hardware designed for increased security;
- Safe-browsing functionality to limit the effects of malicious content; and,
- Co-hosting capabilities of legacy and transformed mission systems.

The Trusted Virtual Environment applies virtual machine technology on a government-certified security foundation.

Benefits of the Trusted Virtual Environment

The capabilities in today's General Dynamics' Trusted Virtual Environments provide an unprecedented blend of power and flexibility to strategic and secure tactical settings as well as in tactical field scenarios. In other words, security administrators can simply access auditable controls to tailor the system for the specific mission. Other advantages to the TVE solution include:

- TVE supports both thin and thick-client applications — TVE is the only Multi-level solution that supports the flexibility to support both thin and thick client infrastructures — you're not restricted to one or the other
- Use of a single computer delivers lower total cost of ownership (TCO)
 - Reduction of costs for maintenance, logistics and upgrades
 - Reduction in size, weight, power and cooling
- Utilization of existing infrastructure — unlike other solutions that require infrastructure modifications to support; e.g., "distribution" consoles
- Optimized workstation agility and flexibility
- Improved joint-operations functionality through trusted methods for accessing disparate networks simultaneously
- Support for legacy applications on multiple operating systems – a capability only provided in a TVE-like solution
- Improved operational workload and streamlined workflow for data access
- Minimized the potential for data leakage
- Single display view increases operational efficiencies (eliminates "Swivel Seat")
- Allows for multiple user access types and privileges

General Dynamics' Trusted Virtual Environment is built with flexibility and scalability in mind, and future enhancements will focus on increased collaboration and ways to improve end users' operational efficiency.

Taking the first step

As much as the landscape has changed in the past 10 years, the pace of change for organizations to include government and non-government — and a need to adapt to the change quickly — will only accel-

erate. New threats will emerge and more sophisticated technologies will be developed to respond. General Dynamics' Trusted Virtual Environment should be a core component in any strategy for providing operators with tools and technology to address current and future strategic and tactical demands. General Dynamics currently offers TVE in a desktop solution with plans to implement the technology into laptops, servers and handhelds giving users the maximum flexibility needed to execute their mission in an efficient, cost-effective manner.

GENERAL DYNAMICS
C4 Systems

8220 E. Roosevelt St., M/D R7229 • Scottsdale, Arizona 85257 • Website: www.gdc4s.com/tve
General Dynamics contact: INFOSEC 77 A Street • Needham, MA 02494
Phone: 781-455-2800 • Toll-free: 888-Type1-4-U (888-897-3148) • Fax: 781-455-5555 • Email: infosec@gdc4s.com