Mobile-Secure Client with INTEGRITY Foundation (M-SCIF)

MILTOPE
A company of ST Engineering North America

Reliable in the Extreme

Contents:

Introduction:

Introduction:

The critical infrastructure of our world is now networked and exposed to attack on a daily basis. We have created the Internet of “Dangerous” Things by connecting power grids, planes, trains, automobiles, medical devices, and ourselves together on an insecure and vulnerable network we are all at risk constantly. Miltope, in partnership with INTEGRITY Global Security, has a solutions that can separate, isolate, and protect your people, your devices, your critical networks, and your data centers. As the work-from-anywhere mentality continues to flourish, cybersecurity policies must adapt to protect people wherever they are. But policy can only take us so far, and we have reached that point. It is time to change the main link to vulnerability in any network, the Machine to Network interface.

1.0 Security Problem

Current Situation: Widespread use of the Internet and the proliferation of mobile devices have created a Future Operating Environment (FOE) in which individuals, units, and forces are more connected than ever before. The Internet of Things (IoT), backed by edge computing, machine learning, data analytics, and cloud technology, is accelerating and amplifying those connections. Currently, the number of IoT-connected devices worldwide is expected to reach 41.6 billion by 2025, which additional security challenges as these commercial devices are integrated into Defense networks.

As the world becomes more connected, however, it also becomes less secure. With each new connected device, vulnerabilities multiply, resulting in a rapid increase in the number of successful cyberattacks and serious data breaches worldwide. Globally, malicious hackers, cyberterrorists, peer-competitors, and non-nation state actors are a growing threat to information security. According to the January 2019 edition of the U.S. National Intelligence Strategy Report, “Cyber threats will pose an increasing risk to public health, safety, and prosperity as information technologies are integrated into critical infrastructure, vital national networks, and consumer devices.”

Today’s cyberattacks are moving down the computing stack, from software to hardware, making it increasingly difficult for the legacy model of software protecting the system to cope and keep pace with rapidly advancing threats to digital security, safety and privacy. Now security must be hardware-enabled directly into silicon level to help protect every layer of the compute stack, including hardware, firmware, operating systems, applications, networks, and the Cloud.

U.S. government organizations and individuals who routinely handle classified information and safeguard national security, including military and intelligence services, require highly secure access to mobile resources in diverse locations. Unfortunately, many high-security or encryption solutions are expensive, complex, inflexible, difficult to scale, and hard to manage and maintain.

2.0 M-SCIF Solution

Security in the Extreme: Designed by Miltope, the Mobile-Secure Client with INTEGRITY Foundation (M-SCIF) is a hardware and software solution that demonstrates zero vulnerabilities and is one of the world’s most secure laptop computers. The M-SCIF client is built on a high-performance hardware set, which provides both an excellent end-user experience and sufficient performance to operate efficiently in diverse locations and under often challenging conditions. The complete MSCIF appliance allows an organization to reduce their stand-alone, office-bound, IT systems that have been set up specifically to meet cyber security requirements. This also lowers the percentage of users exposed to "public" keyboards etc. that open pathways of vulnerability.

The physical hardware is exceptionally operationalized by the INTEGRITY Separation Kernel, INTEGRITY-178B. The INTEGRITY Separation Kernel is the first and only separation kernel to be evaluated by the NSA and certified by National Information Assurance Partnership (NIAP) to EAL6+ High Robustness under the International Common Criteria standard (ISO/IEC 15408). This security rating certifies that the product is suitable for the protection of classified information and other high-value resources against well-funded, sophisticated attackers. INTEGRITY-178B is the only software product ever to achieve the EAL6+ High Robustness rating.

Commercial Solution for Classified (CSfC): M-SCIF is the first-ever turnkey mobility solution that meets CSfC program requirements. Developed by the National Security Agency (NSA), the CSfC program is an important part of the U.S. government's strategy to more quickly deliver layered cybersecurity solutions by leveraging emerging technologies and commercial products to meet rapidly evolving customer requirements.

Foundational Security: In addition to providing hardware-enhanced security features, the platform is optimized for managed IT environments and enables the enforcement of regional/command policies. The INTEGRITY Real Time Operating System (RTOS), makes extensive use of Intel hardware-assisted virtualization and security technologies to build a secure and trusted virtualized environment. The foundational technology building blocks are Intel® Virtualization Technology (Intel® VT including VT-x & VT-d) and Intel® Trusted Execution Technology (Intel® TXT), all part of the Intel® Hardware Shield suite of technologies. Intel VT and Intel TXT enable the hypervisor to secure operating systems, applications, and data by keeping them isolated on their own Virtual Machines (VM), running in their own virtual hardware environment. Each VM is prevented from accessing another VM's OS, applications, data and input/output (I/O). Intel TXT enables a dynamic root of trust to ensure VMs are running on trusted hardware with trusted software, by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. This creates the ability to verify the security of installation, launch, and use of the hypervisor and operating systems. These technologies provide a highly scalable architecture that is specifically designed to harden platforms against hypervisor and BIOS attacks, malicious root kit installations, and other firmware- or software-based attacks. Miltope's M-SCIF appliance uses this technology on the platform for the multilevel, integrated software- and hardware-security separation capabilities they provide. This technology helps to ensure more secure platforms and greater application, data, or virtual-machine isolation while providing a foundation for more advanced solutions as security needs continue to evolve.

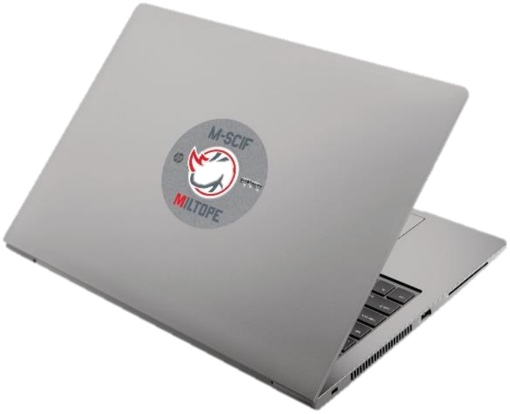


Figure 1 – M-SCIF Hardware

3.0 Miltope Capabilities

Complete Lifecycle Product Management:

In August 2020, Miltope will celebrate 45 years of continuous product development. From full-scale development to non-development programs, Miltope has earned the preferred recognition and distinguished reputation for producing high-quality ultra-rugged products that reliably perform over a wide range of environmental, Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC), and High Altitude Electromagnetic Pulse (HEMP) to meet requirements per MIL-STD-810, MIL-STD-461, and MIL-STD-464. Miltope is most proud of its ability to rapidly incorporate state of the art technologies consistent with leading edge commercial trends into our products. Miltope consistently designs and delivers ultra-rugged products incorporating high technology COTS components and modules to military customers. Our true added benefit is that these products are performance proven and fielded designs that are totally capable of withstanding the harsh battlefield environment at a fraction of the time and cost of producing traditional military systems – providing a best value investment for the U.S. Government.

An outstanding example of this capability has been demonstrated in the SRNC 17 offered on the CHS catalog where Miltope has incorporated COTS LCD and computer board assemblies in a rugged chassis for a CHS compliant product with many thousands of the products serving CHS customers reliably for years.

Miltope, in cooperation with its parent company and strategic partners, continues to expand its complete life-cycle support in areas such as communications, advanced electronics, intelligent transportation systems as well as supporting a strong global customer base from over 25 countries. The Miltope brand is recognized as a rugged reliable product and a leader in the commercial, government, defense, and homeland security sectors worldwide.

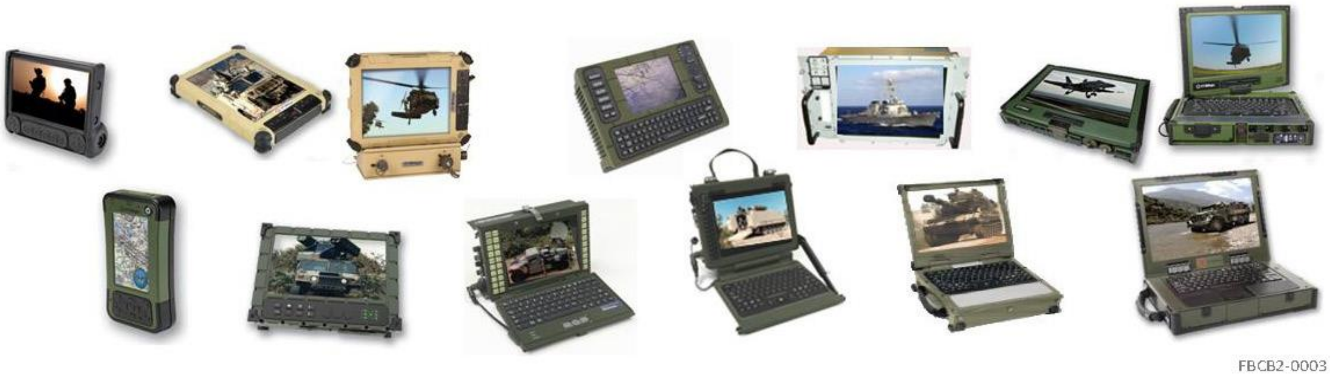


Figure 2- Miltope's Product Line

4.0 Conclusion

Cyber Security Redefined: Through commercial and military supply chains Miltope provides reliable, secure, and mature products to the most remote and isolated expeditionary warriors today. Battle-proven through the most demanding and hostile environments, Miltope continues to support its customers today, and will for years to come, through a continuous and ongoing development and sustainment roadmap. Through its inherent un-hackable design, the M-SCIF will be the future bridge to not only carry forward Miltope's legacy of Reliable to the Extreme, but now we can add Security in the Extreme.

5.0 Company Information

Reliable in the Extreme: Miltope is categorized as a Large Business. Within Other Transaction Agreements (OTAs), Miltope is consider to be a Non-Traditional Defense Contractor (NTDC). Miltope is headquartered in Huntsville, AL and has manufacturing operations in Hope Hull, AL. See complete SAM and Point of Contact Information in **Error! Reference source not found..**

Company Information	
Legal Company Name	Miltope Corporation DBA: VT Miltope
Size	Large Business
Average Employees	100
DUNS	07-750-8810
Address	3800 Richardson Rd
City	Hope Hull
State / Zip Code	AL / 36043
URL	www.mymiltope.com
Program Point of Contract	
Name	David Worthy
Title	VP Mission Systems
Street Address	7037 Old Madison Pike Suite 410
City	Huntsville
State / Zip Code	AL / 35806
Phone	256.772.9940 x7106
Email	dworthy@miltope.com
Technical Point of Contract	
Name	Brian Bostick
Title	Engineering Director
Street Address	7037 Old Madison Pike Suite 410
City	Huntsville
State / Zip Code	AL / 35806
Phone	256.772.9940x7103
Email	bbostick@miltope.com
Contracts Point of Contract	
Name	Alora Fisher Byrd
Title	VP Contracts
Street Address	3800 Richardson Rd
City	Hope Hull
State / Zip Code	AL / 36043
Phone	(334) 613-6500
Email	afisher@miltope.com

Authors:

Jason ‘Nic’ Nicholas
Director BD
+1 (256) 772 9940 x7113
jnicholas@Miltope.com
SOF, Cyber Security, Boats,
Rotary Wing, UXV

Markus Gilges
Director BD
+44 7793 758755
mgilges@Miltope.com
Europe, Middle East, Africa
(EMEA)

References:

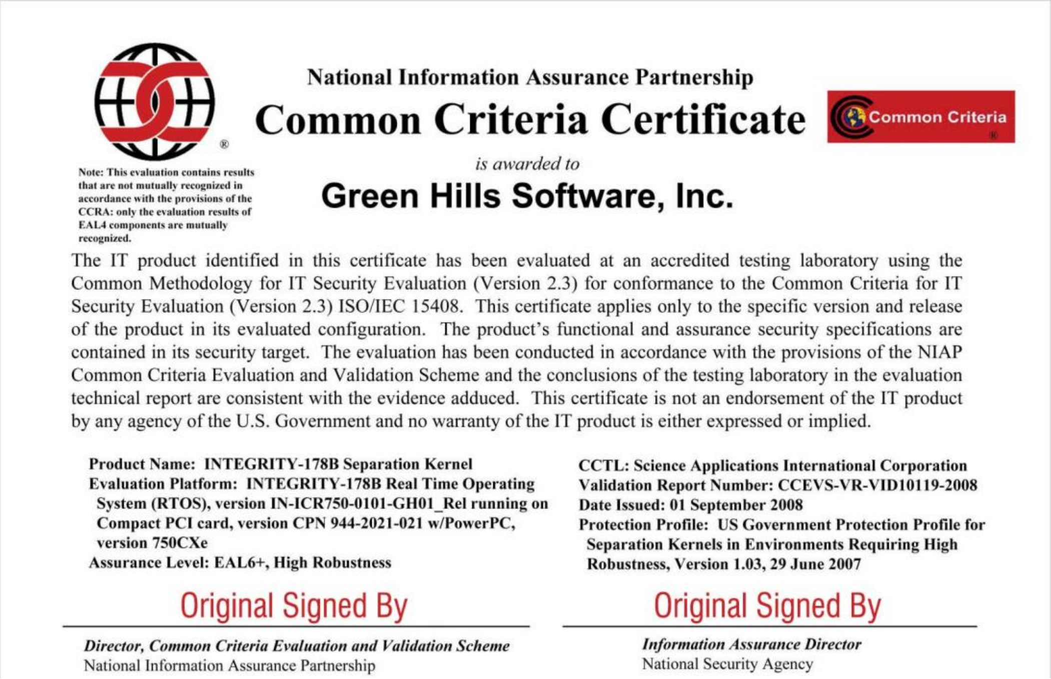
https://www.integrityglobalsecurity.com/learning-center.html

INTEGRITY is the first and only operating system technology to be certified by NIAP, a U.S. government initiative operated by the National Security Agency (NSA), to EAL 6+ High Robustness.

Other common enterprise operating systems are certified to EAL 4+ or lower. EAL 4+ means that there is no assurance of security UNLESS the attack threat is non-hostile, with “casual or inadvertent attempts to breach the system security”. With worldwide access, anywhere and anytime, the Internet is the ultimate hostile environment against which current IT security solutions are unable to adequately defend. The world has become accustomed to a fail-first, patch-later mentality that is expensive and will never provide the security the world deserves.

EAL6+ High Robustness is the gold standard of security certification. INTEGRITY was designed from the ground up to meet EAL7 and therefore was able to meet the U.S. Government’s EAL6+ High Robustness requirements.

INTEGRITY is in a class by itself.



National Information Assurance Partnership

Common Criteria Certificate

Common Criteria

is awarded to

Green Hills Software, Inc.

Note: This evaluation contains results that are not mutually recognized in accordance with the provisions of the CCRA: only the evaluation results of EAL4 components are mutually recognized.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.3) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3) ISO/IEC 15408. This certificate applies only to the specific version and release of the product in its evaluated configuration. The product’s functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: INTEGRITY-178B Separation Kernel
Evaluation Platform: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0101-GH01_Rel running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXe
Assurance Level: EAL6+, High Robustness

CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10119-2008
Date Issued: 01 September 2008
Protection Profile: US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007

Original Signed By

Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By

Information Assurance Director
National Security Agency