



Sentinel Computer Security System

Secured Processing Inc. (SPI) developed the “Sentinel” Computer Security System based on a technology that has 3 existing U.S. patents and one pending U.S. patent. Sentinel has also been Validated by the National Information Assurance Partnership (NIAP) at an EAL4 Level as listed on their webpage at <http://www.niap-ccevs.org/st/vid1000>. This level is sufficient for the secure processing of multiple levels of classified data in minimally protected physical environments. The Sentinel is a low cost Multi-Domain Security (MDS) System that is easily installed in a desktop computer and is transparent to the processing hardware/software. It eliminates multiple separate computers or specialized processing hardware/software used in other MDS technologies thus providing cost, space, and energy savings in excess of 60%. Sentinel also implements a sophisticated access control to selectively control user access to data; computer interfaces such as network/USB ports; and portable media such as DVDs/CDs. This allows Sentinel to counter Insider Threats and external malware and hacker attacks. Sentinel is the only validated technology that can address the growing market for secure MDS systems at a fraction of the cost of other existing MDS technologies while also providing major energy savings.

The Sentinel NIAP Validation was performed under ISO 15408, which grants it recognition and acceptance as an approved security product for the entire U.S. Government and over 15 countries including the UK, Australia, Canada, France, Germany, Greece, Italy, Japan, New Zealand, Spain, and South Korea. The U.S. will be the initial and primary focus since it is the largest MDS market and the SPI management has over 30 years of experience in this sector. SPI has performed a market survey and estimates that the U.S. market for MDS solutions is approximately 1.5 million users within Government and Industry world-wide of which 2/3 are in the U.S. This does not include potential commercial applications in the financial, medical, legal, and technology sectors. The U.S. MDS market has more than tripled in the last 10 years since 9/11 with the growth in the number of secure intelligence, DoD, and law enforcement networks being used world-wide.

The most popular MDS solution by far is the use of separate computers dedicated to each domain with a KVM Switch to switch a user’s (K)eyboard, (V)ideo monitor, and (M)ouse between each computer. Since each security domain needs a separate computer with its own operating system, software, and data the costs, space, and energy usage increase with each domain required. It is not uncommon to see DoD users operating with 3 or more computers on their desktop. Another MDS solution that is in use in some agencies relies on software virtualization within an external server that users connect to via a Thin Client. The Server software sets up virtualized simultaneous domains with their connected networks and user software for access from the Thin Client Terminal. All processing is done within the server, which uses increased power as more domains are created. Heavy usage by a large number of users can also slow down processing times dramatically. This solution also requires a heavy and expensive investment in a new infrastructure of servers, specialized server operating systems and software, and thin client hardware. User acceptance of this solution has been a difficult hurdle since Thin Clients are “dumb terminals” that will not support processing if the server fails or is disabled.

Sentinel differs from other MDS solutions in that it uses an automated secure domain switching technology that allows only one domain to be active at any time. This is enabled and controlled by the Sentinel Security Module that is installed in a desktop computer’s 3 ½” or 5 ¼” bay. Security domains require a separate removable drive that hosts the domain’s operating system, software, and data. The host computer’s internal hard drive is usually designated as an unrestricted domain, although it can also be controlled in the same manner as the removable drives. Removable drives are locked in the computer via standard 3 ½” or 5 ¼” commercially available Removable Hard Disk Drive Bays that can house one or more drives. Each authorized domain has access to a designated host network port and USB ports based on a combination of user rights programmed on their User Smart Card and access permissions setup within the Sentinel. This allows a Sentinel Security Administrator to setup the Smart Cards and Security Module to enable the methodology of “Minimum Privilege”, which allows a user to only get access to the data and resources that their security clearance allows and are safely permitted within the host computer. Access to domains and resources can also be individually controlled based on Time of Day (TOD) in increments as small as 1 minute.

The access rights of each system user is tied to their Smart Card and the Sentinel via an electronic keying mechanism that determines if the Smart Card key matches the key within the host security module and the domain being accessed. If there is a discrepancy, access is immediately denied. If the Smart Card is recognized the user proceeds with the Identification and Authorization (I&A) process by entering their PIN and Password from the keyboard or biometric data that is compared with the values on their Smart Card and within the Security Module. Once a user implements a successful login they can use the computer in a normal manner. Transitioning to another domain simply requires logging off and selecting the new domain to be accessed. As long as the Smart Card is not removed, the session remains enabled and the I&A process does not have to be repeated. Removal of the user's Smart Card during a session immediately shuts off the computer.

The recent availability of low cost Solid State Drives (SSDs) has reduced the domain switching time to seconds, which is a small fraction of the time required for electromechanical drives. The fast domain boot-up speed provided by SSDs along with their increased availability at a relatively low cost has made this Sentinel option very attractive to the subset of users that need frequent access to multiple domains. All security related events during any session are recorded as audit data within the security module and can only be accessed and processed by an Administrator using the Windows-based SPI Audit-X software that is also used to program User Smart Cards. Another recent option added to the Sentinel is a user command to disable USB and/or Network ports if an Intrusion Detection System indicates the computer or network is under attack.

As compared to other MDS technologies listed in the Table below, Sentinel has the following competitive advantages:

1. Lowest acquisition/support cost of any MDS solution and the lack of expensive infrastructure support requirements allows for cost-efficient scalability to large and small user populations.
2. Only MDS solution that is energy efficient and can lower energy usage within large Federal Government facilities such as Fort Meade (currently restricted from any energy increases for the next 18 months).
3. Only MDS solution that qualifies for procurement preferences under FAR Parts 7 and 23 and Presidential Executive Order 13423.
4. Only MDS solution that controls access to vulnerable resources (USB and portable media) that have been used for malware attacks and unauthorized data removal as documented by CBS News 60 Minutes on November 8, 2009.
5. Only MDS solution that has Validated Access Control capability to address the "Insider Threat".
6. Only MDS solution Validated for processing classified data without specialized expensive physical security.
7. Only MDS solution that accesses multiple classified domains without multiple computers or special software and/or infrastructure.
8. Only MDS solution with security audit capability and a countermeasure against external attacks.
9. Only MDS solution that can be implemented in mobile environments.
10. Cannot be disabled by external attacks since there is no direct processing interface with host computers.
11. A patented technology that is not dependent on hardware, software, operating systems, or infrastructure that are likely to become obsolete or incompatible.
12. Multiple Patents on both the processes and product combined with trade secrets and a NIAP Validation.

Multi-Domain Security System Comparison

	Sentinel	Multiple Workstations & KVM	Secutor Data Vault	Sun DTW Server	Tenix Interactive Link	Microsoft Trusted Multi-Net	Cryptek DiamondTek 2.4
Domains	Up to 5	Dependent on Number of Workstations	2 Simultaneous	Dependent on Number of Servers	2 Network Domains	4 Simultaneous	1 Network Domain with multiple security levels
Domain Access Speed	Requires seconds to switch between domains using SSDs	Requires seconds to switch between domains using KVM	Depends on login speed	Depends on login speed	Depends on login speed	Depends on login speed	Requires seconds to switch between domains
Infrastructure Requirements	None	None	Windows Server	Unix Servers with Ultra-Thin Client	None	Citrix Servers with Thin Client	Network Security Controller
OS Dependency	None	None	Requires Windows	Requires Trusted Solaris	None	Requires Citrix version of Unix	None
Software Dependency	None	None	Can only support Windows Applications	Must run on Trusted Solaris version of Unix	None	Requires VM Ware with a hardened Windows OS	None
Hardware Dependency	Any PC or workstation	Any PC or workstation	Requires Proprietary PC Hardware	Requires Sun Ray Ultra-Thin Client	Requires Thin Client	Requires Thin Client	Any PC or Workstation
Domain Isolation	Complete Host & Network Domain Isolation	Complete Host & Network Domain Isolation	Complete Domain Isolation	Uses TCS Relabeler Guard to share domain data	Access to unclassified Domain from classified	Complete Network Domain Separation	Complete Separation of Security Levels within domain
Access Control	To data, I/O, networks, and media + TOD capability	To hard drives and networks	To hard drives and networks	To Server Software and Networks	From classified to unclassified domain	To multiple Network Domains	To Security Levels within network domain
User Token	Smart Card	None	Three Mechanical Keys	None Specified	None Specified	4 Smart Cards (1 for each domain)	Smart Card
Green Product	Yes	No	No	No	No	No	No
Defensive Capability	Yes	No	No	No	No	No	No
Biometrics	Optional	Optional	No	No	No	Optional	No
Portability	Capable of Laptop & PDA	No	No	No	No	No	No
Current Validation Status	EAL 4 on all 29 security functions	None	EAL 4 on 9 security functions	Not NIAP but accredited under DCID 6-3 at PL4	EAL 5	Not NIAP but accredited under DCID 6-3 at PL2	EAL 4
Cost	\$1.5 K per user (without workstation)	Depends on cost of workstations & KVM	Over \$12K per Secutor	Estimated at over \$6K per user	\$2K per user (without workstation)	Depends on number of users	\$2.5K per user (without workstation)