the system–a change that needs to survive a reboot the of the host system. Stop this access and the attack will not proceed.

PRIVILEGES:

Along with access, malware normally needs to escalate its rights or privileges before completing its task. Malware often positions itself to work around current operating system or third-party software defenses at the next boot cycle.

No matter the method of access, or the method of privilege escalation, the component most targeted by malware, in any system, is the system drive. Protect the system drive and you have drastically reduced your attack profile and increased the stability and uptime of your network.

$63,6 SECURE DRIVE

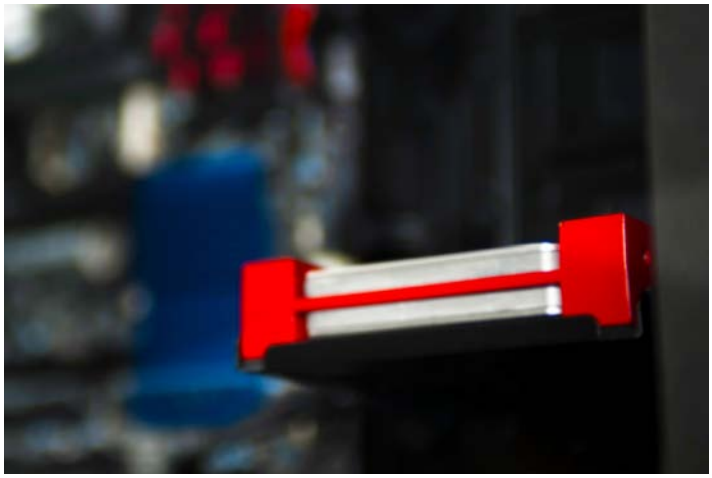
$63,6 is a unique, patent-pending secure drive that takes the place of a computer's hard drive. ASPIS provides an environment that shields the operating system, applications, and any other data you wish to protect from unauthorized changes. In operation, ASPIS is undetectable– ASPIS appears to the system and user as a standard drive. It requires no special drivers and leaves no signature that could be exploited. ASPIS uses no CPU or RAM resources from the host system and does not rely on signature files or other databases for operation–no updates are required.

The difference between ASPIS and a standard system drive is that ASPIS prevents unwanted changes to operating system and application resources. Thus, to the extent that malware relies on changes to those resources– that is to say, most strains of malware–your system is protected. For instance, malware that requires a system restart in order to run or to escalate privileges–many strains of malware fall into this category–will be disabled upon reboot, as any corrupted files and registry settings are returned to their trusted states. Indeed, any malware that requires changes to operating system resources will be disabled upon reboot.

ASPIS provides the ultimate "restore to last known good configuration". Literally, the 1,000th boot of a $63,6 protected system will be exactly the same as the 1st boot. Guaranteed!

$63,6 not only improves the stability and usability of your computer, it also provides you peace of mind that your network has not changed outside of your control and knowledge. Endpoint security is widely known as an effective method to secure a network: allow no changes to an endpoint (a computer, in other words) and malware cannot propagate into the network.

That's the power of ASPIS: hardware technology that protects your system resources from threats known and unknown. It's an elegant security tool in an industry where complexity has become its own enemy. ASPIS has achieved what software never could: physical protection of your system.



SECURITY WITH CONVENIENCE INCLUDED, NO CHARGE

For convenience and the utmost in security assurance, ASPIS provides two modes of operation: Secure Mode and Admin Mode. When in Secure Mode (the default mode), changes are not allowed on the system and application files that you have chosen to protect. When you want to update the system, you boot the computer into ASPIS Admin Mode. While in Admin Mode, changes to the system drive are allowed. Once these changes are

complete, the system is rebooted to Secure Mode and those authorized changes are protected.

Changing the mode of ASPIS requires a secure, hardware authorization key (dongle). The authorization path is independent of the data path used by ASPIS to connect to the system. This creates an impenetrable system drive–there is nothing the system can do, no command it can send, that will alter the mode of ASPIS. Without the authorization key, the system will remain the same, day in, and day out.

ASPIS eliminates the ability of malware, and other unauthorized changes, to become persistent within the system drive. This gives you control over when changes are made to your system.

WHAT ABOUT THE NEW OR UNKNOWN?

We are often asked, "but what about new malware strains we do not know about? Or those types of malware that attack other components within a system? How does ASPIS Secure Drive help there?"

New malware is being released routinely. As long as malware needs to live or become persistent within the system drive, ASPIS protects the system. Whether the malware is a well-known strain or a new zero day attack, ASPIS protects the system drive from unauthorized changes.

No one can claim 100% success defeating all malware types. However, a drastic reduction in the attack profile of your systems, blocking of 99-plus percent of malware currently harming networks, allows your other cyber defenses to focus on malware that targets components other than your system drive.

KEEP CALM AND REBOOT

ASPIS does not replace the software security you currently use. Proper system and network configuration, along with monitoring memory processes, protecting the network perimeter, and policing network traffic, will remain vital. ASPIS does protect your security programs from being altered or disabled by malware and assures the software defenses will properly launch during the next boot cycle.

When some type of cyber event occurs within your organization, how much time and manpower will you save if you can simply reboot a computer or the network and be back to your last known good computing environment? Think about that–in just a few minutes you can reboot to recovery every system on your network. Compare this to the days, weeks or months of time the typical network recovery takes.

ASPIS: THE CORNERSTONE OF SECURITY AND CYBER SAFETY

ASPIS is a unique, hardware-based solution to your cyber defense. By eliminating the possibility of malware making persistent and unauthorized changes to computers on your network, and giving you a way to quickly reboot to your golden image, ASPIS will become the cornerstone on which you build your cyber-safe computing environment.

For more information,
visit our web site.

www.tutelargroup.com

info@tutelargroup.com