



Unparalleled Security for Virtual Call Centers

How Secure Pocket Drive Can Help Prevent Corporate and Customer Information Theft

Introduction

One of most rapidly expanding areas in Customer Relationship Management (CRM) revolves around the implementation of “Virtual Call Centers” which transcend the standard “bricks and mortar” business model. In particular, the virtual call center, with home-based agents, or “homeshoring” has shown extensive growth in the past decade, with an estimated workforce of over 500,000 at-home agents, with an projected CAGR of over 20%. Not only does this concept provide significant cost savings to corporations, with estimated \$\$ per agent/hr of 1/2 to 2/3 that of on-site employees, but either due to the flexibility of their scheduling, the maturity of the workforce, or just the overall personal comfort level, the typical home based agent provides significant independently evaluated customer satisfaction benefits over the on-site call center agent.

Of course, having a widely distributed workforce, handling sensitive information outside a traditional “brick and mortar” framework has significant challenges, not the least of which is security. From a corporate perspective, the enterprise creating a virtual call center must ensure compliance with mandatory regulations including PCI DSS, Federal regulations Sarbanes-Oxley, HIPAA, and state and regional standards.

Ensure control of the agent’s computer

There are a limited number of methods to ensure that the agent’s computer meets the security requirements imposed by the applicable regulations.

Having a widely distributed workforce, handling sensitive information outside a traditional “bricks and mortar” framework has significant challenges, not the least of which is security

The most obvious, but least desirable is to assign the task to the home based agent, e.g. have them perform his/her own security audit, monitor the desktop for virus and malware, and apply operating system and application patches as they are released and tested by the organization’s IT department.

Alternatively, the enterprise can directly manage the desktop, either by providing a complete, remotely administered computer, and/or creating a virtual machine environment where the capabilities are sharply limited by the enterprise managed application. Neither one of these options have proven particularly appealing, either due to overwhelming cost, service, and support (enterprise provided computer) or by issues with virtual machine incompatibility with existing platforms.

Mitigating Risk with Secure Pocket Drive

Secure Pocket Drive (SPD) from SPYRUS is the first licensed Windows® environment on an encrypting USB flash drive, designed for trusted mobile computing. SPD includes a hardware platform, a licensed version of Windows Embedded Standard or Linux that is cryptographically bound to the device, and a trusted ToughBoot boot loader that the host computer boots via the USB port.



Because all of the software, including the boot loader and the operating system, is integral to Secure Pocket Drive, no external drivers or middleware are required on the host PC. The goal is to provide a mobile computing environment in which users have a high degree of assurance that they are working in a known and trusted environment.

SPD provides three services that help prevent infection of the device and further mitigates the installation or concealment of rootkits should they gain entry into the device.

- ▲ **Data-at-Rest Protection**—When SPD is powered off or is inserted into a computer and powered on, its full disk encryption features provide strong data-at-rest protection to prevent infection of an inactive device. The OS partition is not decrypted until the user successfully authenticates to the device.
- ▲ **Resistance to Persistent Infection**—When active, the write filtering incorporated into the embedded Windows operating system blocks writes to the operating system and application files on SPD. This ensures that each time the SPD is booted, a known good operating environment is in place.
- ▲ **Integrity Verification**—A number of hardware-based and software-based integrity checks are performed during pre-boot, boot, and post-boot processing to ensure that the device has not been tampered with.

Data-at-Rest Protection

Before a user authenticates to SPD, the full disk encryption features of the device provide strong data-at-rest protection to prevent infection of an inactive drive.

SPD implements XTS-AES encryption, which uses two AES-256 keys for extremely strong sector-based encryption of its storage medium. Encryption of both the OS and boot loader partitions of SPD prevents modification of the storage area by using an external memory card reader, and it also defeats watermarking and related attacks that AES-CBC encryption cannot protect against. The integrity of

OS resources is therefore appropriately protected for the next power-up.

Resistance to Persistent Infection

Rootkits are designed to load and enable a software payload to operate undetected on a computing platform. This, obviously, requires loading that payload onto the SPD. This type of malware can be downloaded and installed by exploiting a web browser, email client, or OS bug without user detection.

The write filtering incorporated within the Windows Embedded Standard operating system blocks writes to the operating system and application files on SPD.

Ordinary computers can be infected outside of an organization's network then can bring their payload into the heart of the organization when they are used within the secure network.

Since the operating system and application files cannot be overwritten on SPD, a simple reboot clears the infection, preventing it from entering the organization's network.

To thoroughly protect sensitive user information and to further reduce the risk of bringing an infected data file into the network, you can couple SPD with a Hydra Privacy Card® (Hydra PC™) encrypting USB flash drive from SPYRUS. The optional Sentry A-V antivirus scanning engine built into Hydra PC will minimize the chance of you storing an infected file on the device and retrieving it either on SPD or on a different PC or network where it could cause damage.

Both SPD and Hydra PC implement full Suite B hardware-based cryptography that is designed, engineered, and manufactured in the USA. (Suite B algorithms include EC-DH key agreement and ECDSA digital signatures with high-strength P-384 keys, AES-256, and SHA-384).

Pre-Boot Integrity Verification

When SPD is inserted into the host computer, it goes through a power-up sequence before arriving at a fully operational state. This includes performing a

variety of integrity and security checks, as well as initializing the various hardware components and software/firmware states. If any of these tests fail, the device will not mount.

If the self-tests complete successfully, the boot loader partition is decrypted, the boot loader is read into memory, and control is passed to it. After more self-checks, the device prompts for the device unlock password, which is sent to SPD over a secure channel for evaluation.

If the password is correct, the encrypted partition is decrypted. In the WES 2009 version, the boot loader “walks the file system” before loading it into memory, validating specific OS files against pre-stored signatures (hashes). Depending on the outcome, the boot loader either terminates the boot process or loads the OS into memory.

Post-Boot Integrity Verification

After control is passed to the OS, additional SPYRUS software running within the OS environment validates the integrity of a larger set of files before allowing the user to authenticate (log in) to the OS.

As stated above, when the OS is running, write filtering incorporated in the Windows Embedded Standard operating system blocks writes to SPD. This ensures that each time SPD is booted by the user, a known good operating environment is in place.

Summary: The Perfect PC in a Pocket

Secure Pocket Drive is the ideal high-security solution for the travelling “road warrior,” teleworker, healthcare and financial sector workers or for pandemic and other disaster preparedness.

Secure Pocket Drive allows user to carry a complete, encrypted, high-assurance operating system in

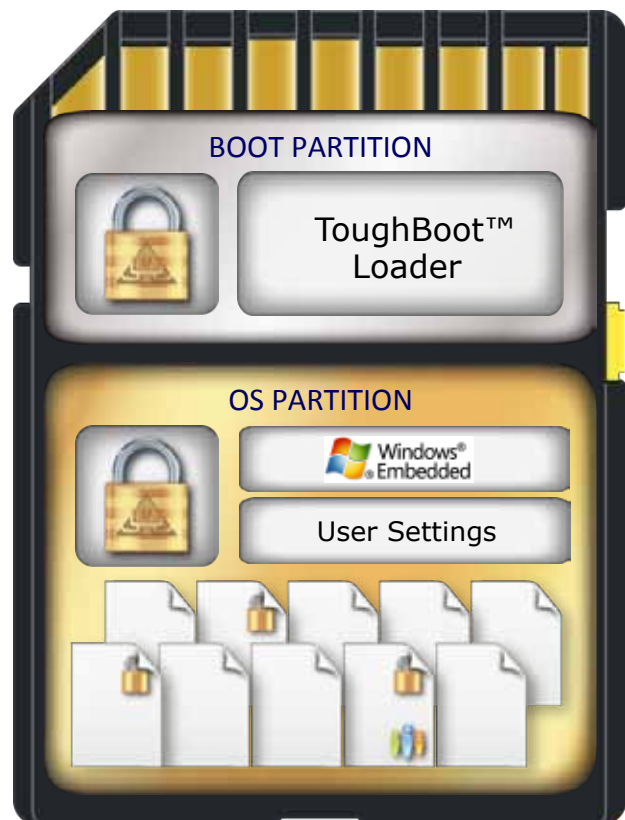
their pocket that can be booted on any available computer, completely bypassing the computer’s hard drive and any resident malware.

While not intended to replace a conventional desktop or laptop computer, it can serve as a trustworthy companion to a computer when security is particularly important.

Secure Pocket Drive gives everyone their own pristine operating system environment when used with a computer that may be used by others who engage in risky behavior from a computer security standpoint.

Hardware-level protection ensures that the ToughBoot loader has not been modified, and critical operating system files are hashed and verified against digital signatures to detect any modification.

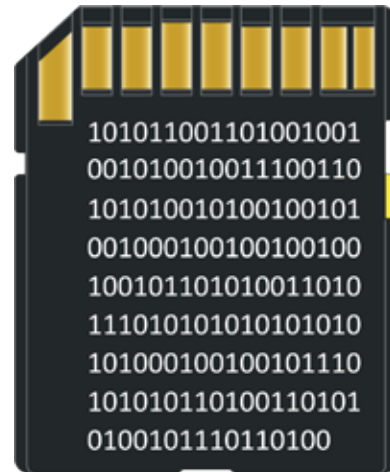
Any attempt to modify operating system files, for example, by a virus, modifies only the cached copy of those files in memory, and those modifications are lost when SPD is powered off.



SPD can be configured with a VPN and/or remote access “thin” client, such as Citrix XenApp, Citrix Receiver, Office 365, or other virtual desktop clients.

Neither users nor malware can save toolbars, plug-ins, Active-X controls, or files on the device. An external USB flash drive can be used for document storage (of course, a SPYRUS encrypting flash drive is recommended).

This makes it perfect for the enterprise, because employees can securely access the Internet, including web email, SAP, CRM, and other enterprise applications, without fear of user modification or infection by malware. Contact SPYRUS today to find out how SPD can make your employees more productive while reducing the malware threat.



When powered off, Secure Pocket Drive is protected by XTS-AES 256-bit encryption

Proudly designed, engineered,



and manufactured in the USA

ADDITIONAL INFORMATION

- Designed, engineered, and manufactured in USA
- FIPS 140-2 Level 3 compliant
- Secure pre-boot authentication
- No residue left on host PC—you were never there.
- Malware protection
- Sophisticated self-destruct mechanisms
- Works with government-issued CAC cards
- Computer BIOS must support booting from a USB drive
- Minimum 1GB RAM required, more is better
- Fixed or removable memory (8GB, 16GB)

CERTIFICATIONS

- FIPS 140-2 Level 3 certificate 1394 for the sector-based encryption module
- FIPS 140-2 Level 3 certificate 1302 for the SPYCOS® hardware security module
- Common Criteria EAL 5+ certificate BSI-DSZ-CC-0315-2005 for the Infineon SLE66CX642P cryptographic processor

For more information about SPYRUS products, visit www.spyrus.com or contact us by email or phone.

Corporate Headquarters

1860 Hartog Drive
San Jose, CA 95131-2203
+1 (408) 392-9131 phone
+1 (408) 392-0319 fax
info@spyrus.com

East Coast Office

+1 (732) 329-6006 phone
+1 (732) 329-6211 fax

Australia Office

Level 7, 333 Adelaide Street
Brisbane QLD 4000, Australia
+61 7 3220-1133 phc
+61 7 3220-2233 fax
www.spyrus.com.au
info@spyrus.com.au



© 2011 SPYRUS, Inc. All rights reserved. Secure Pocket Drive is protected by U.S. Patents 7,757,100, 7,380,140, 6,088,802, and 6,981,149, with other patents pending. Individual Hydra PC products may embody technology protected by one or more of the following patents or patent applications: U.S. Pat. Nos. 6,088,802; 6,003,135; 7,757,100; 7,380,140; 6,981,149; 5,761,305; 5,889,865; 5,896,455; 5,933,504; 5,999,626; 6,122,736; 6,141,420; 6,336,188; 6,487,661; 6,563,928; 6,618,483; U.S. Pat. Appl. Ser. Nos. 12/018,094; 61/300,772; 09/434,247; 09/558,256; 09/942,492; 10/185,735; Can. Pat. Appl. Ser. Nos. 2176972; 2176866; 2202566; 2174261; 2155038; 2174260; E.P. Pat. Appl. Ser. No. 96201322.3; 97106114.8; 96105920.1; 95926348.4; 96105921.9; PCT/US08/51729; Israeli Pat. App. No. 199983; India Pat. Appl. No. 1422/MUMNP/2009. SPYRUS, the SPYRUS logo, Secured by SPYRUS, Hydra Privacy Card, Hydra PC, PocketVault, Digital Attaché, Rosetta, Rosetta Micro, Secure Pocket Drive, SPYCOS, and Security to the Edge are either registered trademarks or trademarks of SPYRUS, Inc., in the U.S. and/or other jurisdictions. All other company, organization, and product names are trademarks of their respective organizations.