SHARED PC'S - WTG

SPYRUS Windows To Go Live Drives provide a powerful and enforceable solution for supporting multiple users on a limited amount of computers

Enforce strong separation of personal and company information from one sharing employee to another, and ensure that terminated employees do not pass confidential information on to their new employers.

Sharing PC's between employees makes a lot of economic sense, especially in health care, public service and law enforcement, where ruggedized laptops can be priced in thousands of Euros. One work station shared by different employees and different work shifts. Sounds great and saves money. One big problem – they use different email accounts, different data files and based on roles, different programs. All of the sudden, sharing PC's and workstations comes with a lot of trade-offs.

Another major issue arises when the employee takes the laptop or PC home for use in telecommuting or other work related functions. The platform is now in an unsecured location and the inadvertent access by a friend or family member may inject malware or create another compromise.

SPYRUS WINDOWS TO GO LIVE DRIVES

SPYRUS Windows To Go drives provide a strong hardware-enforced cryptographic separation and a physical separation between individual computing environments that makes data leakage or attacks all but impossible between the two or more shared user configurations, even when sharing the same host platform.

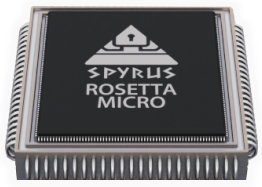
A full disk encrypted partition containing an approved user's image of the corporate operating system, user privileges, and their specific data storage and application functionality resides on each physical WTG device assigned to a user, replacing resources resident on the host platform. The SPYRUS WTG device now functions as a specific user-assigned secure managed endpoint extension of the corporation's IT infrastructure. With cryptographic separation of the devices, no electronic history or footprint is left behind when physically unplugged from the shared host platform, which for further isolation, may be a diskless system without the WTG device.

Documented business cases have shown that an IT organization can save up to 75% in per-employee IT costs by issuing a hardware-encrypting drive such as the SPYRUS Worksafe Pro, with repurposed older PC's and Macs, eliminating the need to purchase new laptops.

SECURITY TO THE EDGE

SPYCOS is the firmware operating system incorporated into SPYRUS hardware devices. It supports more cryptographic algorithms than any other commercial product and dynamically allocates nonvolatile memory.

- FIPS 140-2 Level 3 physical protection
- FIPS 140-2 Level 3 Security Controller
- Complete Suite B Crypto Services
- HSM for MFA and smartcard services
- Multi-Factor authentication
- CSFC Approved for Classified Data
- Tamper resistant and tamper evident
- MILSTD 810 tested with no device failure



THE SPYRUS ADVANTAGE

Spyrus hardware is designed, engineered and manufactured in the USA, under strict regulations, using the strongest cryptographic algorithms available.

Spyrus has over 26 years' experience developing hardware-based encryption, authentication and digital content security products.

ABOUT 3825 | 3825 Technology provides end-to-end security solutions for access control and management, encrypted storage and secure file sharing with embedded SPYRUS HSM's.

info@3825technology.com