Portable Workplace

Bootable USB 3.0 Windows To Go Drives

MICROSOFT-CERTIFIED WINDOWS TO GO DRIVES

Hardware-encrypted Secure Portable Workplace and unencrypted Portable Workplace from PNY are Microsoft-certified Windows To Go drives that securely boot your custom Windows 8, 8.1, and 10.

PNY Windows To Go drives are not slow virtual machines. They boot a native operating system using your computer hardware but never access or alter the host computer's hard drive.

Enterprise users can enjoy the mobility of a pocket-sized Windows To Go drive with access to all their enterprise network resources. Enterprise IT can rest assured that remote access to valuable resources is by authentic users running the corporate Windows image—even when booted from untrusted computers.

SECURE HARDWARE ENCRYPTION

Secure Portable Workplace provides military-grade XTS-AES 256 hardware encryption over the entire drive, providing the ultimate protection of the operating system, applications, and data storage. Always-on, tamper-proof hardware encryption prevents data at rest on SecurePortable Workplace from being accessed, deleted, or modified. Encryption keys are never stored in flash memory.

The Secure Portable Workplace/Portable Workplace family of solid state drives delivers ultra-fast SSD performance with always-on data protection.

LAYERED ENCRYPTION WITH BITLOCKER OPTION

Both Secure Portable Workplace and unencrypted Portable Workplace drives can be configured with BitLocker software encryption on the operating system and data storage compartments. The BitLocker keys are stored in the hardware-encrypted

Available Options

SECURE PORTABLE WORKPLACE

256 GB:	P-FDWS256SCE-FS
128 GB:	P-FDWS128SCE-FS
64 GB:	P-FDWS64GSCE-FS
32 GB:	P-FDWS32GSCE-FS

PORTABLE WORKPLACE

256 GB:	P-FDW256SC-FS
128 GB:	P-FDW128SC-FS
64 GB:	P-FDW64GSC-FS
32 GB:	P-FDW32GSC-FS

SPECIFICATIONS

Secure Portable Workplace	
Usable Capacities (IDEMA)	**32 GB, 64 GB, 128 GB, 256 GB**
Dimensions (L × W × H)	**95.3 × 24.5 × 9.8 mm**
PERFORMANCE	
USB	**USB 3.0 Super Speed**
Sequential Max Read	**Up to 240 MB/s (100 GB)**
Sequential Max Write	**Up to 240 MB/s (100 GB)**
ELECTRICAL	
Operating Voltage	**Vcc=3.3 to 5 VDC**
Power Consumption	**~300mA @ 3.3 VDC**
Humidity	**90%, noncondensing**
ENVIRONMENTAL	
Operating Temperature	**0° C ~ 70° C**
Storage Temperature	**-20° C ~ 85° C**
Operating Humidity	**5 to 98%**
RELIABILITY / SECURITY	
Certifications	▸ **Microsoft Windows To Go certified drives** ▸ **FIPS 140-2 Level 3 Certified PKI device, #1302** ▸ **EAL 5+ validated hardware security core** ▸ **CE, FCC 47 Part 15, Class B** ▸ **EN55022, EN55024, EN61000**
Data Retention	**10 Years**
Data Encryption	**XTS-AES 256** **All cryptographic functions performed in hardware** **Tamper-evident epoxy**
Cryptographic Standards	**Suite B, a set of cryptographic algorithms promoted by the DoD for cryptographic modernization, including:** ▸ **Elliptic curve cryptography (P-256, P-384, P-521)** ▸ **ECDH per SP 800-56A** ▸ **ECDSA digital signature algorithm** ▸ **Concatenation KDF** ▸ **RSA 1024 and 2048 digital signature algorithm** ▸ **RSA-1024/2048 key exchange** ▸ **DES, two- & three-key triple DES with ECB, CBC** ▸ **XTS-AES 256** ▸ **AES 128/192/256 with ECB, CBC** ▸ **SHA-1 and SHA-224/256/384/512 secure hash algorithms with HMAC support**

PNY®
Make Life Simple™

PNY Technologies, Inc. 100 Jefferson Road, Parsippany, NJ 07054 | Tel 973 515 9700 | Fax 973 560 5590

Features and specifications subject to change without notice. The PNY logo is a registered trademark of PNY Technologies, Inc.

Covered by Spyrus U.S. Pat. Nos. 7,380,140; 6,088,802; 7,757,100.

compartment, inaccessible to hackers. Used in combination with the HW encryption of Secure Portable Workplace, BitLocker software encryption provides a second layer of security.

BOOTABLE LIVE DRIVES ENABLE MOBILE WORK

Secure Portable Workplace and Portable Workplace drives transform personal computers, including many Macs (Mac support provided by SPYRUS), into compliant enterprise Windows computers—with or without connectivity. These drives have no impact on the host computer or its hard drive and leave no footprint behind. Access legacy Windows XP and Windows 7 computers with dual booting from hard disk or SPYRUS Windows To Go drive.

TAKE CONTROL OF ENDPOINT SECURITY

Unpatched, uncontrolled BYOD and remote computers create a clear danger when permitted access to enterprise networks. Secure Portable Workplace and Portable Workplace drives improve endpoint security by transforming BYOD and home computers into trustworthy network access points.

ENABLES SEAMLESS, SECURE REMOTE ACCESS

Remote or traveling workers see no difference in network experience between on-premises access or when using smart card authenticated VPNs from remote locations. With Microsoft DirectAccess VPN, users automatically connect and access the corporate network.

PROTECT WINDOWS 8, 8.1, AND 10 INTEGRITY

Secure Portable Workplace defends the integrity of the operating environment even when booted on compromised systems. Numerous health checks validate the integrity and detect tampering of the SPYRUS ToughbootTM loader, the hardware, and the firmware prior to booting the OS.

The SPYRUS Toughboot loader is signed by Microsoft and meets all Secure Boot criteria. Secure Boot is a UEFI specification that checks for an approved digital signature in all drivers or OS loaders to prevent malware infections during the boot sequence.

MOBILE DEVICE AND DESKTOP MANAGEMENT

Secure Portable Workplace and Portable Workplace drives can be managed at multiple levels with Microsoft and PNY solutions.

CENTRAL ENTERPRISE DEVICE MANAGEMENT

The SPYRUS Enterprise Management System (SEMS)* for device management includes features to remotely disable and destroy enterprise USB devices, remotely reset passwords, enforce policy, audit transactions, and more.

MICROSOFT SECURITY FEATURES

Microsoft Direct Access for remote access allows seamless and secure connectivity to the corporate network without the need for a VPN.

Microsoft System Center allows administrators to update and patch the OS and applications when Secure Portable Workplace and Portable Workplace drives are joined to the domain.

Secure Portable Workplace and Portable Workplace drives make an ideal configuration for remote access/VDI/Cloud, and Office 365, providing a true secure trusted endpoint. Your enterprise can enforce access to only your network and prevent local access or data storage.

ENTERPRISE USERS INSIST ON MOBILITY

Secure Portable Workplace and Portable Workplace drives provide continuity and security for mobile workers:

- BYOD computers at the office
- Road Warrior traveling light
- Telework from home computer
- Temporary or contract workers
- Continuity of Operations for disaster recovery

As a cost-effective teleworker solution, use PNY 32 GB Windows To Go drives with the Read Only option to boot PNY drives securely from untrusted home computers. Your organization can enforce work and data saving to the enterprise network, or if required, modified files can be saved on a Data Vault read/write partition.

*Available as an add-on service

Make Life Simple™

PNY Technologies, Inc. 100 Jefferson Road, Parsippany, NJ 07054 | Tel 973 515 9700 | Fax 973 560 5590