SPYRUS®

SPYRUS Windows To Go Products (Technology)

The World's Most Secure Windows To Go Solution

Table of Contents

Windows To Go Introduction

Today, we live in an IT world comprised of what appear to be opposing corporate forces. On one hand, we have enormous demands to increase worker productivity and support an ever-changing, distributed and mobile workforce. On the other hand, we are being asked to secure our corporate network access and our underlying corporate data … and all of this, while managing our overall spending.

The BIG question: Is it really possible to manage a distributed and mobile workforce, secure corporate data and maintain network integrity while at the same time managing costs?

The simple answer: YES. In this white paper we will cover the basic SPYRUS Windows To Go offering as well as a full in-depth discussion of our family of products and services that offer your organization not just the mobility and cost savings inherent with WTG, but also provide enhanced levels of data and network security for those users.

Why Windows To Go? You have already done your research so we will not spend much time on this area. Simply stated, Windows To Go makes a lot of sense for certain key business applications such as contractors, travelling executives, work from home employees and those employees/contractors that bring their own device to work (BYOD). The Microsoft website summarizes these benefits quite nicely: WTG is included with Enterprise Software Assurance, you can be productive from virtually any location without

lugging around your more expensive laptops or other devices, and you essentially have your Windows 8.1 or Windows 10 enterprise in your pocket.

So Why SPYRUS? At the most basic level, the answer is experience and reliability. We were the visionary for and have the history with Windows To Go. Our products operate at the highest performance levels and are built to last. SPYRUS pioneered the first bootable Windows on a USB 2.0 hardware-encrypting drive in

2008 to become the first Windows™ licensee for USB and followed this innovation by receiving the first Microsoft certifications for both hardware-encrypting and non-hardware-encrypting Windows To Go products in 2012.

Our entry point to Windows To Go is the Portable Workplace (Basic). Although this product does not include all the robust security features of our other WTG solutions, it highlights many of our core foundational product differences between SPYRUS and other certified Windows To Go solutions, including:

- **Speed:** SSD and High Performance Random Read/Random Write Speeds Critical to Boot an OS.

- **Physical Device Integrity:** At SPYRUS, we understand that people rely on their WTG device for mission critical functions. In essence, it is their computer SSD drive. So unlike a traditional USB that is used less regularly and is much easier to replace, we realized early-on in our customer deployments that the device must withstand punishment from a physical design perspective. To that end we designed our Windows To Go devices to meet the highest physical standards in design and component materials. The combination of stringent environmental testing and additional testing for magnetic fields, X-Ray and long term immersion demonstrate the usability of this high security configuration of the SPYRUS WTG devices in the challenging financial services, healthcare, and critical infrastructure environments as well.

- **MAC Boot:** Supports booting from most Macintosh computers.

- **Made In America:** Significantly reduces supply chain issues.

Beyond the feature set of this foundational product, SPYRUS offers a complete line of products with varying levels of design and security enhancements to meet all potential corporate requirements for Windows To Go applications. The remainder of this white paper provides details about all of our products and underlying technologies.

The Threat is Real

With this ever increasing use of portable computing and storage capability comes a liability. Information exploitation in the world today is at an all-time high. In our modern computing environment, classified government data, sensitive corporate data, personal identity & financial information, and other personal data are all under attack from a variety of assailants. There exists a wide variety of threats to your sensitive information from both casual and sophisticated adversaries. Since 2005, at least 931,326,448 records containing Personally Identifiable Information (PII) have been reported as breached in the United States

alone[1]. But there is no single cause for this loss of data. 25% of these data compromises are attributed to lost or stolen media, 25% to external hacking from outside a device or network, and a full 50% are attributed to a trusted user's negligence or malicious activity. Add to this compromise of PII information data breaches from the likes of WikiLeaks and Eric Snowden, and the most recent attacks on Sony, and it becomes clear that security must be central in the planning of any mobility solution. And the problems are not confined to the loss of sensitive data. Mobile devices are being exploited more and more as a means for malware infiltration into host computers and ultimately into enterprise networks.

The recently publicized hijacking attack at the 2014 Black Hat conference, referred to as "the bad USB attack", clearly illustrates the need for mobile devices to be aware of and have countermeasures in place to defend against subtle and sophisticated attacks as well as the more obvious brute force attacks. The "bad USB attack" exploited a very common vulnerability in USB devices, allowing modification of the device firmware, to covertly take-over a device and make it do what the attacker wanted rather than what the user expected.

The SPYRUS Windows To Go (WTG) drives have been designed with this kind of threat environment in mind. In particular, the secure WTG drives – the WorkSafe Pro and the Secure Portable Workplace – have built in safeguards and countermeasures for a wide variety of attacks including:

- Exploitation of weak key generation
- Password Guessing Attacks (a vulnerability increased with weak passwords)
    - Offline password attack
    - Online password attack
- Identity Masquerade & Spoofing attacks
- Cryptographic Side Channel attacks
- Fault induction attacks
- Physical penetration attacks
- Unauthorized access to critical security parameters
- Replay attacks
- Hijacking attacks (BadUSB Exploit)

So, the threat is real; and it is naive to think that any particular person or organization is not vulnerable. In fact, there is a whole new industry of "Data Brokers" that has arisen in the last few years, collecting any and all information they can squeeze out of the digital world. And all this information is for sale. Some of these are legitimate activities and others are malicious. But at present there is little or no regulation on these activities. And the fact that these activities can and do take place from almost anywhere in the world makes monitoring and controlling them virtually impossible. Hence the need to determine if and how you want to protect your sensitive information.

This White Paper is intended to provide a technical overview that will allow you to see how the SPYRUS Windows To Go products help you address this threat environment.

[1] From: http://www.PrivacyRights.org (as of 15 November 2014)

SPYRUS = Reliability & Security

SPYRUS, Inc. has been in business since 1992 and has a long and extensive history producing reliable, high assurance security devices. As a forerunner with mobility solutions, SPYRUS pioneered Windows on a USB in 2008 becoming the first Windows licensee and followed this path by receiving the first Microsoft certification for a hardware-encrypted Windows To Go product in 2012. Continuing the company's broad based innovation, SPYRUS developed and produced the first certified Windows To Go products with embedded onboard FIPS HSM/smartcard in 2013. SPYRUS Windows to Go products are members of an extensive family of high assurance data storage and authentication devices developed over decades of experience in government and enterprise.

While other companies may claim to have the "most secure flash drive" available, SPYRUS' USB 3.0 Windows To Go drives have been evaluated by a variety of independent third parties who's business is to determine the reliability and security of devices and solutions in the market today. In September 2014, The SSD Review released its evaluation titled, "SPYRUS WorkSafe Pro WTG Secure Flash Drive Review – Worlds Most Secure Flash Drive"[2]. In that review, Les Tokar, the Founder of The SSD Review, said,

> "Our review of the SPYRUS WorkSafe Pro Windows To Go Secure Flash Drive marks the world's first independent report of the SPYRUS encrypted flash drive, a flash drive that would most definitely suit the likes of James Bond. It brings to end a period of over two years of discussions and final agreement on exactly what could (or could not be) shown and discussed with respect to this drive. As much as our report of the SPYRUS cannot zone in on such things as component closeups, hardware specifics, or even some of the information that might normally be discussed in such a hardware build, we trust you will be as amazed as we were at what is easily the worlds most advanced and secure flash drive."

While security is a critical aspect of a portable computing solution, so is reliability. All WTG drives receive a very limited amount of this testing when they are being certified by Microsoft. However, this is not very extensive, nor does it consider anything beyond a benign office environment. Most users of WTG drives will be carrying them around in a pocket or purse (with a variety of other things clattering around) and will be using them in less than optimal conditions. As a result, SPYRUS has submitted its WTG drives to MIL 810 environmental testing. The section below, titled "Operational Environment", identifies the specific tests that were performed.

As you continue reading this White Paper you will receive a technical overview of the operational and security features built in to the SPYRUS Windows To Go products.

[2] http://www.thessdreview.com/our-reviews/spyrus-worksafe-pro-wtg-secure-flash-drive-review-worlds-secure-flash-drive/

SPYRUS Windows To Go Products

To meet the wide range of requirements being faced in today's mobile computing environment, SPYRUS provides four different models of its Microsoft certified Windows To Go (WTG) drives. Each of these models is built on the same robust hardware platform and is available in a variety of memory sizes including 32 Gbytes, 64 Gbytes, 128 Gbytes, 256 Gbytes, and 512 Gbytes; and they all take advantage of SSD memory to provide high performance over a USB 3.0 interface. The four different models are:

- Portable Workplace (PW) – This is the entry level WTG drive that supports Windows 8.0, Windows 8.1, and Windows 10 operating systems. It can be protected with software based full-disk encryption using the Microsoft BitLocker FDE product. All of the technologies you use with Windows 8.0, 8.1, and 10 Enterprise work with Windows To Go: Group Policy, BitLocker, BranchCache, AppLocker, App-V, UE-V, and DirectAccess.
- Secure Portable Workplace (SPW) – This model of the SPYRUS WTG drives adds a layer of high assurance, hardware-based, full-disk encryption to the feature set of the PW drive. In addition, it provides enhanced user authentication and integrity checking fully integrated into the boot up process.
- WorkSafe (WS) – The WorkSafe model enhances the PW by providing full access to the identity and rooted authentication capabilities of a full smart card. With WorkSafe, the FIPS 140-2 Level 3 / EAL 5+ validated Rosetta Micro crypto smart card chip embedded in all SPYRUS Windows To Go drives can be used as a traditional smart card in your enterprise environment.
- WorkSafe Pro (WSP) – This model provides the best of all worlds. It provides all of the hardware based FDE protection and the enhanced user authentication and integrity checking available on the SPW. It also provides the same access to the embedded Rosetta Micro crypto smart card chip that you have with the WS drive.

As you can tell from the brief descriptions above, the drives vary from each other in terms of the available security features on each drive. In particular, two of the drives provide hardware based full disk encryption (FDE) – the WSP and SPW drives – and two of the drives provide access to the built in smart card capabilities – the WS and WSP drives. The following table summarizes the main features available on each drive.

	XTS-AES 256 Full Disk Encryption	BitLocker full disk encryption	Layered Security w/ BitLocker	Built-in PKI Smart Card	Read-Only Windows Volume	Up to 2 Data Vault Volumes	BitLocker FDE for Data Vault	SEMS Enabled
PW		✓			✓	✓	✓	✓
SPW	✓	✓	✓		✓	✓	✓	✓
WS		✓		✓	✓	✓	✓	✓
WSP	✓	✓	✓	✓	✓	✓	✓	✓

Each of these features is described in a little more detail below.

- Hardware Based XTS-AES 256 Full Disk Encryption – This feature provides a fully integrated, hardware enforced level of full disk encryption (FDE) utilizing the strongest commercially available data encryption technology.
- Software Based BitLocker Full Disk Encryption – All SPYRUS Windows To Go drives can be configured with BitLocker software encryption to protect some or all of the volumes that have been provisioned on the drive.
- Layered Security for Higher Assurance Data-At-Rest Protection – On the SPW and the WSP drives, adding BitLocker FDE enables a second layer of encryption for Defense-In-Depth protection. On these drives BitLocker keys are protected by the hardware layer of protection built into those drives, further enhancing the security profile presented.
- Built-in PKI Smart Card – WorkSafe and WorkSafe Pro are the only Microsoft-certified Windows To Go drives that deliver the identity and rooted authentication capabilities of a full smart card. With these drives, the FIPS 140-2 Level 3 / EAL 5+ validated Rosetta Micro crypto smart card chip embedded in all SPYRUS Windows To Go drives can be used as a traditional smart card in your enterprise environment. This is available whether you are booted off the WTG drive or you simply insert the drive into an already booted Windows system. In either case, the Rosetta processor is presented as a reader-less USB 3.0 smart card (CCID) that enables you to use your RSA and/or elliptic curve ECDSA digital certificates with any compatible computer. It has full Microsoft certified mini-driver support that will be automatically downloaded from the Microsoft update site. It is also supported with a PKCS#11 interface library separately available from SPYRUS. To ensure the highest level of security available in a smart card, keys can be generated and maintained completely within the Rosetta hardware and will never be exported. The user keys and certificates embedded on the Rosetta smart card can be easily managed with standard smart card management systems such as Microsoft Forefront Identity Manager and with the included SPYRUS Mini-driver Token Utility.
- Read-Only Windows System Volume – This feature provides additional Data-In-Use protection for the Windows system volume (the C: drive) when you are booted off any of the SPYRUS WTG drives. The Read Only option prevents retention of malware and other unauthorized downloads by redirecting all write operations to the Windows volume to a separate overlay partition on the drive. Then, when the user shuts down and/or reboots the drive, all the overlay data is lost and the system restarts with the unaltered contents of the Windows volume. In Read Only mode, your operating system, applications, and data files on the Windows volume are completely protected against alteration or infection from outside sources.
- Data Vault Storage Volumes – Up to two Data Vault volumes (read/write partitions) can be configured on any of the SPYRUS WTG drives, allowing a user to save and access files even when the Read-Only mode is enabled on the Windows volume. In addition, these volumes can be accessed from an already booted Windows system by simply inserting the drive and, for the SPW and WSP drives, running a log on application that is included with those drives. In this way the SPYRUS WTG drive can double as a removable storage drive.
- Additional, Independent BitLocker Protection of Data Vaults – You can also configure separate BitLocker FDE protection for any Data Vault volume that has been provisioned on a WTG drive,

using separate passwords for each instance of BitLocker if desired. This allows the WTG drives to have tailored access control and protection in order to support a wide variety of operational scenarios.

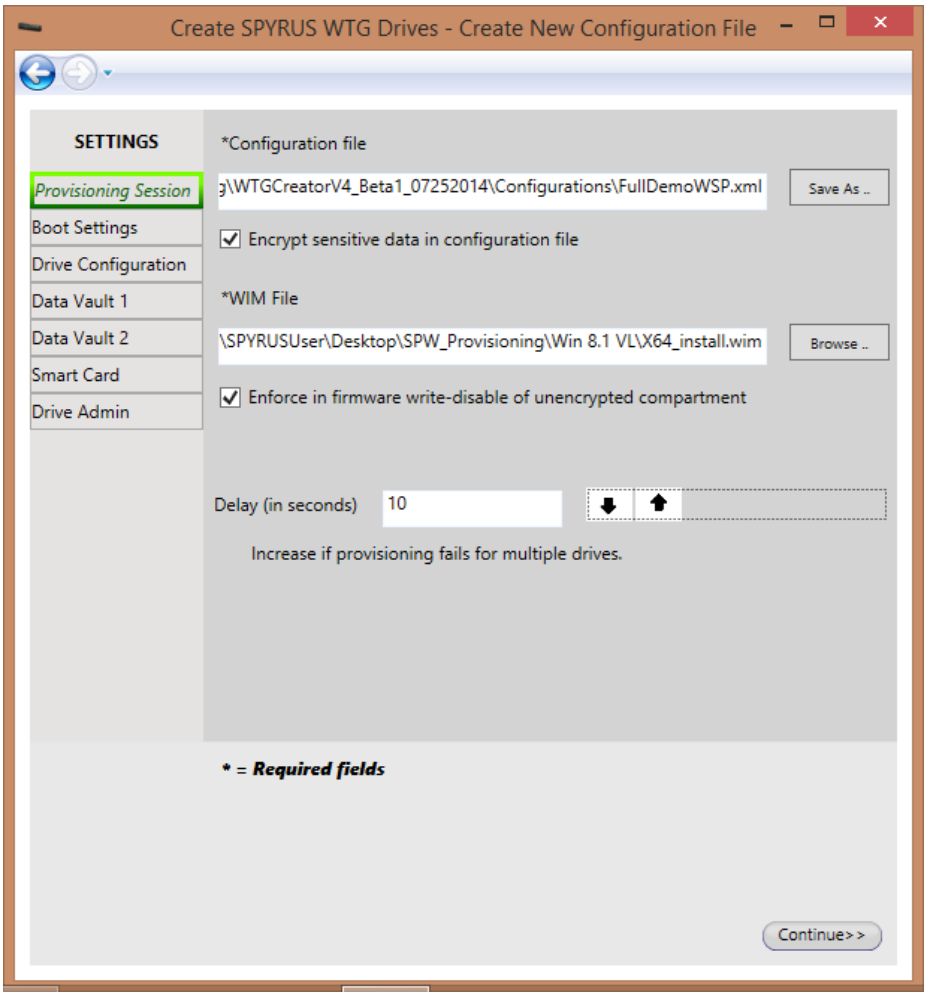
- SPYRUS Enterprise Management Enabled for Additional Data-In-Use Protection – The SPYRUS Enterprise Management System (SEMS) provides secure lifecycle management on enterprise domains for USB devices. SEMS-managed drives must have the SEMS client software (separate order, requires licensed server software) installed and be joined to a SEMS domain. All SPYRUS Windows To Go drives can be managed over an enterprise domain with the SPYRUS Enterprise Management System (SEMS) for mobile device management (MDM). SEMS features include remote device disable and destroy functions, remote password reset, policy enforcement, transaction auditing, and more.

Flexible and Easy to Configure

SPYRUS provides a suite of deployment software with all WTG drives. The heart of this package is the SPYRUS WTG Creator utility which allows an administrator to easily provision one or more drives with their own custom enterprise Windows image (WIM) to create a SPYRUS Windows To Go drive exactly tailored to their organization's requirements. When you provision your own drives, you have full control over all operating system configurations, applications, settings, Data Vault configuration, and options such as Read Only or SEMS.

The SPYRUS WTG Creator allows an administrator to set a variety of provisioning parameters that will control the configuration and security settings on the drives. These are all accessible from a single page which is displayed to the administrator as shown in the figure below.

(Note: The specific settings available will depend on the type of SPYRUS WTG drive that is being provisioned. The discussion below refers to the WSP which has all of the provisioning settings that can be configured for any of the SPYRUS WTG drives.)



For each of the categories of settings (identified by tabs on the left of the display) the following configuration items can be set:

- Provisioning Session:
  - Configuration File: This is the file where all the configuration settings being created by the utility will be saved. This configuration file can be reused in the future to provision identical drives without having to re-enter all of the settings.
  - Encrypt sensitive data: If this option is selected, the Creator will encrypt all of the sensitive information (such as passwords) in the configuration file.
  - WIM File: This is the Windows operating system Image File.
  - Enforce write-disable: If this option is selected, the Creator will set the boot compartment to the hardware protected, read-only state after provisioning completes.
  - Delay: When the drive goes off the USB bus during provisioning, this is the time that the utility will wait for the drive to come back on-line.
- Boot Settings:
  - Boot Type: This selection determines whether UEFI Secure Boot will be enforced or whether the drive will be allowed to boot on any UEFI or BIOS machine.
  - Boot Password: The default user boot password to be used.
  - Password Attempt Limit: This is the number of consecutive logon failures that will be allowed before a remedial action is taken.
  - Password Limit Action: This selection determines the specific remedial action that will be taken by the drive when the Password Attempt Limit has been reached. The actions are to “block” the user’s password or to zeroize the password and keys on the drive.
  - Warning Level: This identifies the point at which a warning message is displayed to a user of how many remaining logon attempts the user has before the remedial action is taken.
  - Allow Password Change: If this option is selected the user will be able to change the password manually during the boot process.
  - Min Password Length: The user boot password must be at least this long.
  - Required Char Groups: The number of different categories of characters that must be present in an acceptable password.
  - Upper Case The number of Upper Case characters required if this class is included in the password.
  - Lower Case: The number of Lower Case characters required if this class is included in the password.
  - Numeric: The number of Numeral characters required if this class is included in the password.
  - Special: The number of Special characters required if this class is included in the password.
  - Char Repeat Count: The number of times an individual character can be repeated in the password.
- Drive Configuration:
  - OS BitLocker Password: If BitLocker protection is to be applied to the Windows volume on the drive, the default password should be set here. If this field is blank, BitLocker will NOT be applied.
  - Domain: If the drive is to be remotely joined to a domain during provisioning, this should identify the domain.

- User account: If remote domain join is being performed, this option will still allow the user to create a local account on the drive during the OOBE process.
- Enable Read-Only: This option identifies if Read-Only is to be used on the Windows volume of the drive.
- Enable SEMS: This option identifies if the drive is to be SEMS managed.

- Data Vault 1:
  - Size (in MB): If this Data Vault volume is to be partitioned on the drive, this should specify the size of the volume. If this is left blank, this Data Vault will NOT be created.
  - File System: If this Data Vault volume is being created, this selection identifies which file system the volume should be formatted with.
  - Label: If this Data Vault volume is being created, this is the volume label that will be assigned to it.
  - BitLocker Password: If BitLocker protection is to be applied to this Data Vault volume, the default password should be set here. If this field is blank, BitLocker will NOT be applied.
- Data Vault 2:
  - Size (in MB): If this Data Vault volume is to be partitioned on the drive, this should specify the size of the volume. If this is left blank, this Data Vault will NOT be created.
  - File System: If this Data Vault volume is being created, this selection identifies which file system the volume should be formatted with.
  - Label: If this Data Vault volume is being created, this is the volume label that will be assigned to it.
  - BitLocker Password: If BitLocker protection is to be applied to this Data Vault volume, the default password should be set here. If this field is blank, BitLocker will NOT be applied.
- Smart Card:
  - User PIN: This is the default user PIN for PKI access to the smart card.
  - Admin PIN: This is the default administrator PIN for PKI access.
  - Admin Key: This is the Admin Key to be used by the Microsoft mini-driver when it needs to perform admin functions on the smart card.
  - Force Re-initialize: If the Rosetta processor is already initialized for PKI operations, the Creator will normally NOT re-initialize it. This will preserve all of the keys and certificates that have been programmed on the smart card. If this option is selected, the Creator will always re-initialize the Rosetta processor for PKI operations.
- Drive Admin:
  - Admin Password: The default Admin password to be used.
  - Password Attempt Limit: This is the number of consecutive Admin logon failures that will be allowed before a remedial action is taken.
  - Password Limit Action: This selection determines the specific remedial action that will be taken by the drive when the Admin Password Attempt Limit has been reached. The actions are to “block” the user’s password or to zeroize the password and keys on the drive.
  - Warning Level: This identifies the point at which a warning message is displayed to a user of how many remaining logon attempts the Admin has before the remedial action is taken.

- Min Password Length: The Admin password must be at least this long.
- Required Char Groups: The number of different categories of characters that must be present in an acceptable Admin password.
- Upper Case The number of Upper Case characters required if this class is included in the password.
- Lower Case: The number of Lower Case characters required if this class is included in the password.
- Numeric: The number of Numeral characters required if this class is included in the password.
- Special: The number of Special characters required if this class is included in the password.
- Char Repeat Count: The number of times an individual character can be repeated in the password.

SPYRUS Windows To Go Security Features

Because SPYRUS is first and foremost a security company, the SPYRUS WTG drives have been designed and architected with security in mind. They provide some of the strongest military-grade hardware encryption commercially available. The on-board hardware security infrastructure includes AES-256, ECDH, ECDSA, ECC P-384, and SHA-384, which together make up the US Government's Suite B cryptography, part of its cryptographic modernization program. But strong crypto is only one part of a high assurance solution. To be effective, cryptography needs to be implemented and applied in a manner that effectively addresses the threat environment described earlier in this paper. The SPYRUS WTG drives start this with a strong hardware trust anchor and build on this to not only protect your data-at-rest but also to provide you a high assurance processing environment while your data is in use.

Trust Anchor

Enforcement within any strong security solution must be anchored in some point of trust. There must be something you trust to hold up to the threat environment within which you are trying to establish a secure solution. Within every Microsoft certified SPYRUS WTG drive there is a Rosetta micro security controller to which all security is anchored. As a hardware trust anchor it provides superior protection to any software trust anchor that can be provided. The computer industry has finally come to grips with this and most modern machines are being manufactured with a built in "Trusted Platform Module" (or TPM). On UEFI based machines, this hardware trust anchor is utilized by the machine during its boot process as the starting point from which all trust proceeds. That's why the UEFI Secure Boot process in most modern machines allows a public authentication key to be stored within the TPM.

However, with a portable platform like a WTG drive that can boot on many different machines, a single host machine's TPM cannot be used as the trust anchor for the drive. But an anchor is still needed and in the SPYRUS WTG drives it is the Rosetta security processor. The Rosetta microprocessor has been independently certified to FIPS-140 level 3 and has been through extensive evaluations by other independent government agencies. It contains a large number of hardware defense mechanisms and countermeasures designed to make it a strong security processor. It contains a very high entropy, strong random number source that is used for all key generation on the drive. This is where all keys and other critical security parameters are stored as encrypted values to provide the maximum available protection. It is also within the Rosetta module that user authentication and credential management takes place.

Strong Data-At-Rest Protection

While mobility increases convenience and productivity, the use of small portable devices brings with it the increased risk that these devices can be easily lost or stolen. The skyrocketing theft rate of first laptops and then cell phones only proves the point. But as USB devices become physically smaller, they also become much easier to misplace or lose. And with the increasing memory sizes available on these drives, the amount of data at risk is also increasing. As a result, there has been an increasing demand, in both government and enterprise markets, for high assurance data-at-rest solutions.

To provide strong data-at-rest protection, all the operational memory on the WorkSafe Pro (WSP) and the Secure Portable Workplace (SPW) drives is protected directly by the hardware using sector-based full disk

encryption, based on XTS-AES 256 encryption (NIST SP800-38E). This is the strongest approved mode of AES encryption available for sector based media and is resistant to most modern cryptographic attacks.

When evaluating the security provided by a product it is important to realize that the length of keys used by the encryption algorithm is NOT enough for a secure solution. First of all, those keys need to be truly random (i.e. contain a high amount of entropy) and they (along with all other critical security parameters) need to be strongly protected against exposure. Even then, while these keys are in use they need to be protected by appropriate countermeasures against attacks such as various side-channel and snooping exploits. This is accomplished within the SPYRUS WTG drives by taking full advantage of the built-in Rosetta security controller that was described earlier in this paper as the trust anchor on the drive.

All data encryption is performed within the tamper-resistant, epoxy-coated cryptographic hardware. The access password is never stored on the device, in software, or on a host computer, even in encrypted or hashed form. This safeguards the keys, passwords, and encrypted data from physical attack at all times, whether or not the WorkSafe Pro or Secure Portable Workplace is connected to a host computer.

User Authentication and Access Control

No matter how strongly the data encryption is implemented, the data-at-rest protection provided by a drive is only as strong as the user authentication and access control that are used to grant access to authorized users of that data. For example, it is common knowledge that a user's password must be complex enough that it cannot be easily guessed, but even then there are password guessing/searching programs available that are very effective if a sufficient number of attempts are allowed.

To help strengthen this aspect of the SPYRUS WTG drive's security, the hardware has built in enforcement of password complexity and it limits the number of consecutive failed authentication attempts that are allowed. In addition, all user passwords (and any other critical security parameter) can only be sent to the drive over an encrypted secure channel.

User authentication on the secure SPYRUS WTG drives is performed inside the onboard Rosetta security controller that acts as the trust anchor for the drive as described earlier in this paper. This authentication is performed using a multi-factor authentication algorithm and is not based on a stored copy of the user's password. This algorithm simultaneously authenticates the user and verifies the integrity of the firmware performing this authentication. In addition, the actual access to the protected data on the drive is tightly controlled. Until user authentication is successfully completed, none of the hardware encrypted memory is even mapped to the USB port on the drive. This blocks all access to the data (even encrypted) by an unauthorized user.

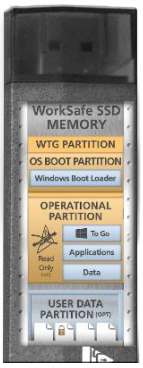
High Assurance Boot Authentication

When booting up your Microsoft processing environment, it is always good to have a high degree of confidence that the environment being booted has not been tampered with. When booting from a SPYRUS secure WTG drive – the SPW or the WSP – this is exactly what you get. The boot process is controlled by the SPYRUS ToughBoot boot loader which assures that each step of the boot process performs the required integrity and authentication checks necessary to give a high level of assurance. These checks start at the time the drive is powered on and continue until control is passed over to the Windows operating system.

The steps involved in this process include the following:

Power-On Self-Test – This step performs integrity checks on the hardware and its operation. The firmware on all processors included in the drive are tested for integrity and all of the crypto operations are tested to make sure they are performing correctly. If and tampering is detected in the firmware, if any hardware malfunctions are detected, or if any of the crypto operations are not performing correctly, the power-on self-test will fail and the boot process will not continue.

Boot Process Initiation – After the power-on self-test succeeds, the drive enumerates itself on the USB bus, identifying itself as a mass storage drive (in the case of the PW and the SPW) or as composite drive consisting of both a mass storage and a CCID component (in the case of the WS and the WSP). However, with the secure WTG drives (the SPW and WSP) at this point in the boot process, only a small portion of the drive memory is mapped to the USB port. This memory contains the ToughBoot loader and is typically protected by the hardware as read-only. If the host machine is in the process of booting, it will recognize the drive as a bootable device and, if correctly configured, the machine's BIOS will take the appropriate steps to load the ToughBoot loader into memory for execution. If the machine is running a legacy BIOS subsystem it simply loads ToughBoot into RAM and starts it running. In the case of a UEFI subsystem, however, the host machine may also be configured to run a "secure-boot" integrity check on the ToughBoot loader. ToughBoot has been digitally signed and the UEFI Secure-Boot process will perform a full digital signature verification on the ToughBoot executable to make sure of its integrity before loading it into RAM and beginning its execution.



User Authentication – Once the ToughBoot loader begins execution, it first sets up a secure communication channel with the hardware processor on board the SPYRUS WTG drive. It then prompts the user for their authentication password which it securely passes to the drive. The actual user authentication is performed within the hardware of the drive, inside the onboard Rosetta security controller. This authentication is performed using a multi-factor authentication algorithm and is not based on a stored copy of the user's password. If this authentication is successful, the FDE encryption keys are recovered and the crypto processing is set up to recover and save (decrypt and encrypt) data off and onto the drive. It is after this is successively done that the drive's FDE protected memory is mapped to the USB port, replacing the boot compartment which contains the ToughBoot loader. This memory is now accessible to the ToughBoot image that is running in the host computer's RAM; however, the Windows operating system is not yet booted. One step remains before this can be done.

Windows Verification – Prior to initiating the actual boot of the Windows operating system, an integrity check is performed on the Windows Boot Loader. Just like the ToughBoot loader, it has been digitally signed. To make sure no one has tampered with it, a full digital signature verification is run on it by the ToughBoot loader. If this is successful, the Windows operating system on the WTG drive is booted and ToughBoot is removed from the host machine's RAM. At this point, all of the security settings and policies configured into the Windows 8, 8.1, or 10 image are now in effect. If the drive was configured with Read-Only protection of the Windows volume, the mass storage filter driver that blocks all writes to the Windows volume will be activated.

Protections While In Use

When evaluating the security provided by any device it is important to keep in mind that the data-at-rest protection provided by full disk encryption (FDE) is only a partial solution. Once a user has been authenticated, all the data on an FDE drive is completely available. Not only is it available to the authorized user but it is also available to any malware that might find its way onto the drive or any external intrusion attacks that may occur. It is at this point that data-in-use protection mechanisms become critical.

The SPYRUS WTG drives have a number of available controls and defensive mechanisms that can be utilized to significantly improve the drive's drives security profile while it is in use.

- Isolation from the Host Machines Disk Drives – SPYRUS Windows To Go drives boot the Windows operating system and, by default, set a policy to completely bypass the host computer's hard drive. This will prevent infection of the WTG drive by any malware that may be on that host machine. In addition, there will be no impact on the host computer and no footprints left behind once the WTG drive is shut down. While this policy can be changed by a Windows Administrator or during provisioning, it is "best practice" to leave it in place.
- Independent Administrative Settings and Controls – There are a number of hardware enforced security policies and controls on the secure SPYRUS WTG drives that a regular user does NOT have access to change. This includes things like the user password complexity, logon access limitations, tamper response mechanism, and read-only protection of the boot volume. Even though the authorized user can log on to the drive and have full use of its functionality, they will not be allowed to make changes to the underlying security settings of the drive.
- Windows Volume Read-Only protection – This feature provides additional Data-In-Use protection for the Windows operating system volume (the C: drive) when you are booted off any of the SPYRUS WTG drives. The Read Only option prevents retention of malware and other unauthorized downloads by redirecting all write operations to the Windows volume to a separate overlay partition on the drive. Then, when the user shuts down and/or reboots the drive, all the overlay data is lost and the system restarts with the unaltered contents of the Windows volume. In Read Only mode, your operating system, applications, and data files on the Windows volume are completely protected against alteration or infection from outside sources.

- Configurable Data Vault Volumes – Up to two Data Vault volumes (read/write partitions) can be configured on any of the SPYRUS WTG drives, allowing a user to save and access files even when the Read-Only mode is enabled on the Windows volume. In addition, these volumes can be accessed from an already booted Windows system by simply inserting the drive and, for the SPW and WSP drives, running a log on application that is included with those drives. In this way the SPYRUS WTG drive can double as a removable storage drive. You can also configure separate BitLocker FDE protection for any Data Vault volume that has been provisioned on a WTG drive, using separate passwords for each instance of BitLocker if desired. This allows the WTG drives to have tailored access control and protection even when the drive is in use and on-line.
- SPYRUS Enterprise Management System – Centralized management is a critical component for Data-in-Use protection of drives being used remotely. If a drive is compromised for any reason, an administrator still has the ability to control its use. The SPYRUS Enterprise Management System (SEMS) provides secure lifecycle management on enterprise domains for the SPYRUS WTG drives. SEMS features include remote device disable, enable and destroy functions, remote password reset, dynamic policy management and enforcement, transaction auditing, and more.
- Built-in Smart Card Access – Many enterprises have a PKI infrastructure in place to be able to enforce strong authentication and access control throughout their network and other systems. The SPYRUS WS and WSP drives provide full access to the built-in Rosetta smart card capabilities, allowing the operations of these WTG drives to be seamlessly integrated into enterprise operations.

Built-in Hardware Security Module (HSM) and/or Smart Card

The SPYRUS WorkSafe and WorkSafe Pro drives are the only Microsoft-certified Windows To Go drives that deliver the identity and rooted authentication capabilities of a full smart card. These drives provide full access to the FIPS 140-2 Level 3 / EAL 5+ validated Rosetta Micro crypto security controller embedded in all SPYRUS Windows To Go drives. This feature allows the built-in Rosetta smart card to be used as a traditional smart card in your enterprise environment. This is true whether a user is booted from their WTG drive or not. When not booted, if the user just inserts the drive into an already booted Windows machine, it serves as a reader-less USB 3.0 smart card (CCID) that enables them to use their RSA and/or elliptic curve ECDSA digital certificates with any compatible computer application that uses either the PKCS#11 or the Microsoft Mini-driver crypto standards. The Microsoft certified SPYRUS Minidriver for the Rosetta smart card is automatically downloaded from Windows Update when the drive is first booted. The PKCS#11 library must be obtained separately from SPYRUS.

This embedded Rosetta Micro security controller supports both RSA and ECC suites of cryptographic operations and can be managed and programmed with keys and certificates using standard smart card management systems such as Microsoft Forefront Identity Manager. It is a fully enabled smartcard and can be used for most PKI digital certificate functions such as:

- Smart card logon
- File signature and/or encryption
- Signed/encrypted e-mail
- VPN authentication
- Web authentication

Physical Protection

Each of the SPYRUS WTG drives is contained within an epoxy filled, molded aluminum case. This provides the first level of protection against adversaries who may acquire a drive and try to break into it to gain access to the memory contents. The case has passed physical penetration testing as specified by FIPS 140-2, at level 3.

Depending on the memory size of the drive two different case sizes are available:

- 32,64,128,256 GB Drive Case dimensions 87.2 x 24.3 x 10.7 mm
- 512 GB Drive Case dimensions 101.6 x 24.3 x 10.7 mm

Operational Environment

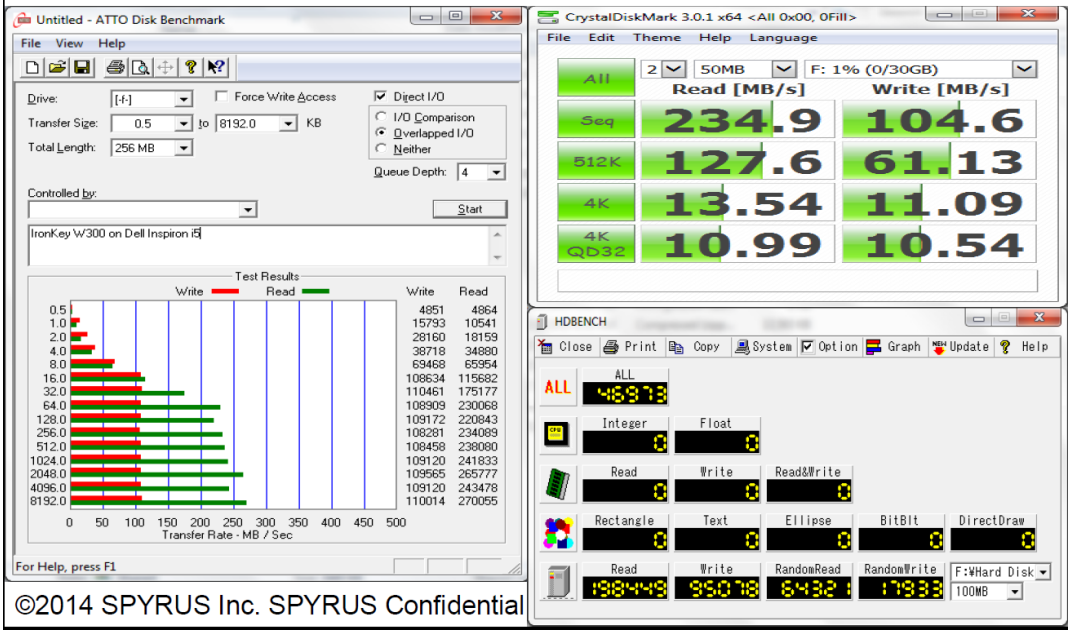
SPYRUS Windows To Go drives have been built to provide robust performance under a wide variety of environmental conditions. To evaluate and confirm this, the drives have been put through extensive MIL 810 testing as well as FCC/CE and Physical testing. The results are summarized in the following table.

#	Test	Reference Spec.	Condition	Criteria
1	Operating High Humid / High Temperature	MIL-STD-202, METH 103B	40ºC; 90% RH (non-condensing); 96 hours	No functional failures
2	Operating Temperature Cycling (RDT)	MIL-STD-810, METH 503	0ºC - 70ºC; Ramp rate 3ºC/min; 30 min dwell at each temp; 10 cycles	No functional failures
3	Non-Operating Temperature Cycling	MIL-STD-810, METH 503	-40ºC - 85ºC; Ramp rate 3ºC/min; 30 min dwell at each temp; 10 cycles	No functional failures
4	High Temperature Storage	MIL-STD-810, METH 501	85ºC; 96 hours	No functional failures
5	Low Temperature Storage	MIL-STD-810, METH 502	-40ºC; 96 hours	No functional failures
6	Thermal Shock	MIL-STD-202, METH 107	-25ºC ~ 85ºC; per test condition A (5 cycles0	No functional failures
7	Operating Shock	MIL-STD 883J, Method 2002.5, Cond. B	1500g, 0.5ms, 1/2 sine wave, 5 shocks - 6 directions	No functional failures
8	Non-Operating Vibration	MIL-STD-202, METH 204	(20Hz - 80Hz/1.52mm)/(80Hz to 2KHz/20G)/3 axis 30 minutes each	No functional failures
9	Drop Test	Drop Tube	Drop Tube - 1.5 meters - 12 axis - 1 drop per axis	No functional failures or housing damage
10	Data Retention	PNY Memory Test Script	100ºC; 5 hours	No functional failures
11	EMI	FCC/CE	FCC Part 15, Class B/EN55022 - EN55024/etc.	Pass
12	ESD	EN61000-4-2	Enclosure Discharge - Contact & Air	No functional failures
13	Bend Test	PNY connector to body bend test	Force = 20 N, X and Y axis	No functional failures
14	Torque Test	PNY connector to body torque test	Torque = 30Nm, CW, CCW	No functional failures
15	Tumble Test	Tumbler	Media=Typical pocket content (coins, keys, etc.)	No functional failures
16	USB Connector Mating cycles	PNY Connector cycle mechanism	Cycles+2000	No functional failures
17	End Cap Separation Test	Pull Test	Test to failure	Test to failure
18	Dust test	IEC 60529, IP6	As per defined	Pass
19	Waterproof test	IEC 60529, IPX7	As per defined	Pass
20	Magnet Test	ISO764: 2002 (4800A/M 3 orientations)	As per defined	Pass
21	X-ray Test	ISO7816-1 (1Gy relative to medium energy 40 to 100Kv	As per defined	Pass

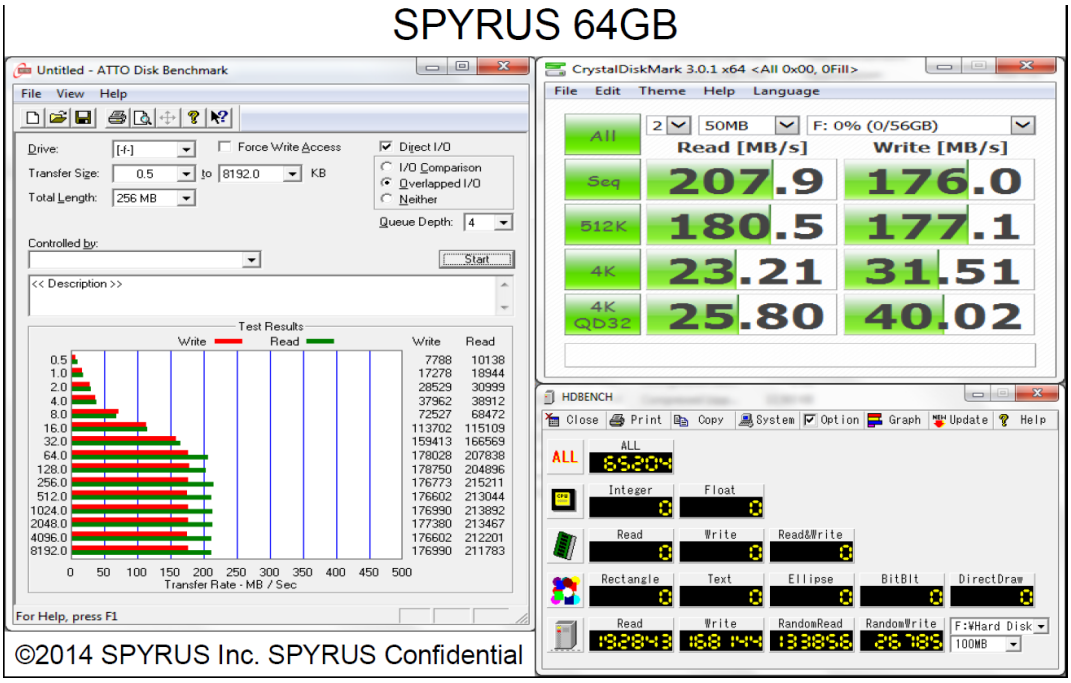
At the same time, these drives take full advantage of the SSD memory performance that is integral to each device. The following figures show the performance of the 32, 64, 128, 256 and 512 GB SPYRUS WTG drives.

(Note: Performance testing was conducted on a DELL Inspiron i5 core laptop, running Windows 7, and using three separate benchmark programs: ATTO, HDBENCH, and CrystalDiskMark 3.0.1 X64.)

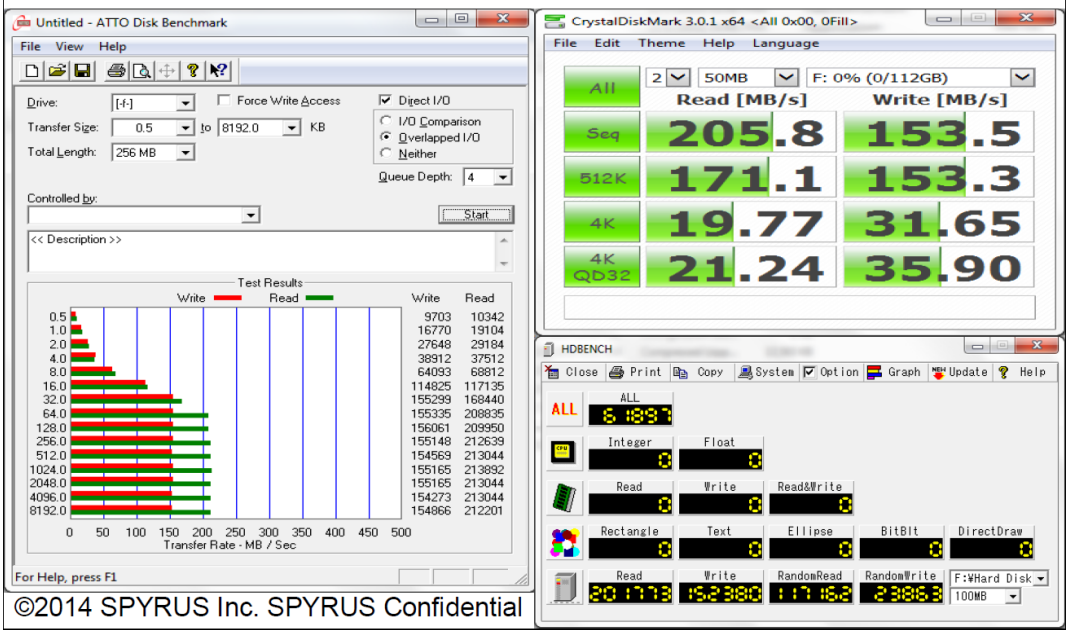
SPYRUS 32GB



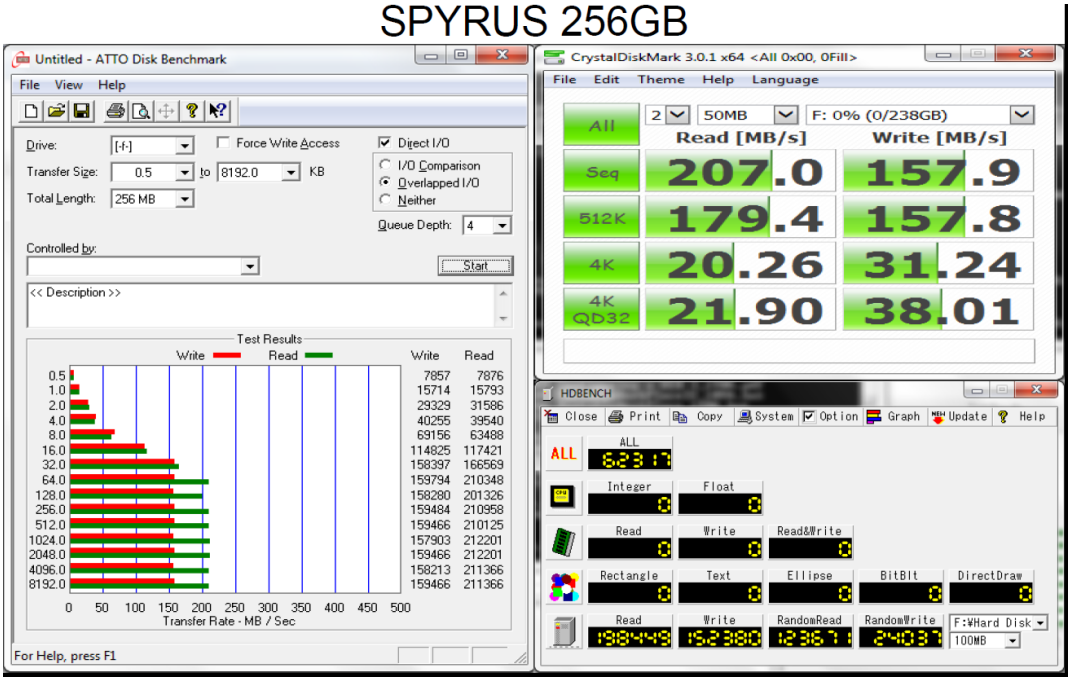
SPYRUS 64GB



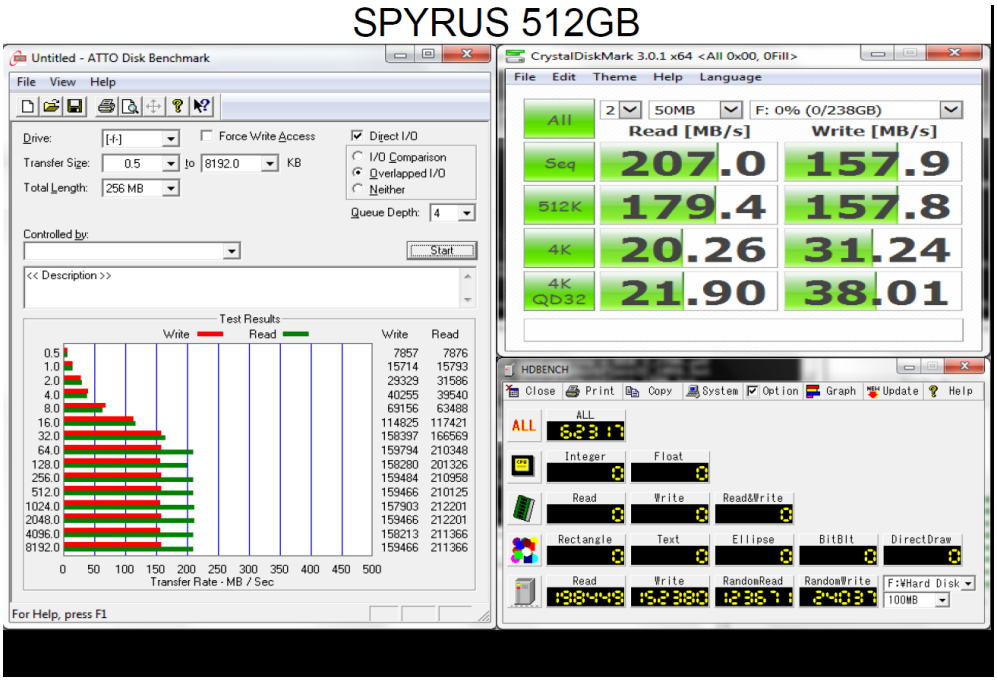
SPYRUS 128GB



SPYRUS 256GB



SPYRUS 512GB



Operational Use Cases

With the flexibility, configurability, reliability, and security built into the SPYRUS WTG drives, they are finding use in a wide variety of operational scenarios. Some of the use cases where these drives have found a home include the following:

- Personal PC In Your Pocket – For those users who want to always have ready access to their own personal processing environment and the comfort of knowing that everything is set up just right, the SPYRUS WSP drives are a cost effective way of keeping that processing environment with you.
- BYOC/BYOD
- Road Warriors/Travel – SPYRUS Windows To Go drives are great for remote or traveling workers, who can enjoy the same networking experience at the office or at remote locations using smart card authenticated VPNs.
- Working from home/Telework – As a cost-effective teleworker solution, use a 32 GB SPYRUS Windows To Go drive with the Read Only option to boot SPYRUS drives securely from untrusted home computers. Your organization can enforce work and data saving to the enterprise network, or if required, changed files can be saved on a Data Vault read/write partition. The employee can travel light and still be productive from home.
- Temporary/Contract Workers – Most enterprises incur significant overhead and expense when provisioning contract workers with the computing resources they need to do the work they are contracted to do without compromising corporate network security. SPYRUS Windows To Go drives provide a cost effective way to deploy the required processing environment with all the policies and settings in place. And what's more, the contractor doesn't have to carry around multiple laptops.
- Shared PCs – In office environments where there are fixed computing resources yet every employee needs their own processing environment, SPYRUS WTG drives are the ideal solution. Environments such as help desks, customer support, or sales and marketing contact are just a few examples of where this condition may exist.
- Continuity of Operations/Disaster Recovery Scenarios – For disaster recovery, SPYRUS Windows To Go drives configured with your enterprise image can quickly restore Continuity of Operations on rental hardware. You can be up and running in hours instead of days, saving the time it could take to configure each new computer.
- Secure Access to Cloud Systems – SPYRUS Windows To Go 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.
- Application Development with On-Board Code Signing Certificates Stored in the HSM/smartcard

Summary

SPYRUS's family of high-capacity Windows to Go USB 3.0 drives and secure storage devices provide contractors, remote workers, and telecommuters with a complete operating environment that includes extensive storage capacity for development tools and large datasets that create "personal cloud-like" data analytics. The drives retain all their capabilities from 32 GB through 512 GB versions and feature superior security defense of the operating system, documents, and identity credentials from tampering and theft with layered hardware and software encryption depending on the particular model.

Technical leadership, hardware security, optional onboard FIPS 140-2 Level 3 PKI capabilities, ultra-high performance, and the new features of Windows 8.1 and Windows 10 make SPYRUS Windows to Go drives the choice for high-capacity Windows To Go platforms. In addition, by utilizing the wide range of unique capabilities in the SPYRUS products, corporations may finally realize significant cost savings by repurposing employee-owned or corporate legacy computers. In particular, the 256 GB and 512 GB high capacity live drives for Windows To Go are ideal for Disaster Recovery and Continuity of Operations scenarios, customers in the entertainment industry and government agencies with high data volume requirements.

The entire family of new drives also maintains compatibility with the optional SPYRUS Enterprise Management System (SEMS). Combining a Microsoft public key with a smart card-enabled ecosystem and SPYRUS security applications extends a true end-to-end security approach for enterprise smart card and PKI infrastructure to mobile users for authentication to applications and networks. With SEMS device management, enterprise administrators can centrally register, block/unblock, revoke, set policies, audit, and "kill" SPYRUS Windows To Go drives.

Appendices

A link to the data sheet for each of the SPYRUS Windows To Go products has been included with this paper for easy reference and comparison. In addition, a link for the SPYRUS Enterprise Management System datasheet is included to provide a more comprehensive overview of how the drives would operate within a managed enterprise environment. Altogether, datasheets for the following products are included:

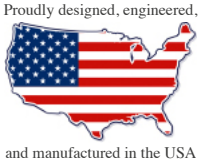
- WorkSafe
  http://www.spyrus.com/company/literature/SPYRUSdatasheets/DSWorkSafe-WorkSafePro.pdf
- WorkSafe Pro
  http://www.spyrus.com/company/literature/SPYRUSdatasheets/DSWorkSafe-WorkSafePro.pdf
- Portable Workplace
  http://www.spyrus.com/company/literature/SPYRUSdatasheets/DSPW-SPW.pdf
- Secure Portable Workplace
  http://www.spyrus.com/company/literature/SPYRUSdatasheets/DSPW-SPW.pdf
  http://www.spyrus.com/company/literature/SPYRUSmarketlit/415-450001.pdf
- SPYRUS Enterprise Management System
  http://www.spyrus.com/products/sems.html

Additional information and technical details for these products can be obtained from SPYRUS, Inc. following the execution of an appropriate Non-Disclosure Agreement.

SPYRUS®

Microsoft Partner
Gold OEM Hardware
Silver Independent Software Vendor (ISV)

Proudly designed, engineered,



and manufactured in the USA

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) 832-0123 fax

UK Office
+44 (0) 113 8800494

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