SPYRUS

# Windows To Go Live Drives

## Introducing the highest possible level of assurance for Windows To Go


Per far fronte all'ampia gamma di richieste degli attuali ambienti di mobile computing, SPYRUS fornisce quattro diversi modelli dei suoi drive Windows To Go (WTG) certificati Microsoft. Ciascuno di questi modelli è implementato sulla stessa robusta piattaforma hardware ed è disponibile in una varieta di dimensioni, da 32 GB fino a 512 GB, e sfrutta la memoria SSD per garantire alte prestazioni tramite l'interfaccia USB 3.0.

Un riepilogo dei prodotti e delle caratteristiche è delineato nella seguente tabella per Worksafe Pro™, WorkSafe™, Secure Portable Workplace™ e Portable WorkPlace™:

| | XTS-AES 256 Hardware Encryption | Layered Data Security | Built in PKI Smart Card | Data Vault Read/Write | Read Only Configuration | SEMS Device Management Option | Bit Locker full disk and/or Data Vault |
|---|---|---|---|---|---|---|---|
| WorkSafe Pro | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| WorkSafe | | | ✓ | ✓ | Upgrade | ✓ | ✓ |
| Secure Portable Workplace | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ |
| Portable Workplace | | | | ✓ | Upgrade | ✓ | ✓ |

**XTS-AES 256 Hardware Encryption**

SPYRUS WorkSafe Pro e Secure Portable Workplace garantiscono la più alta sicurezza a livello militare attualmente disponibile sul mercato grazie alla crittografia hardware per una complete cifratura del drive e la protezione dei dati a riposo. La cifratura è basata sull'algoritmo XTS-AES 256 (NIST SP800-38E). L'infrastruttura di sicurezza integrata include gli algoritmi AES CBC, ECDH, ECDSA, ECC P-384, e SHA-384 (Suite B del governo US). Tutta la crittografia è eseguita in un hardware anti-manomissione, fissato con resine epossidiche. La password di accesso non è mai archiviata sul dispositivo, in un software o su un computer host, neppure in forma criptata o hashed. Ciò salvaguarda le chiavi, le password e i dati criptati dagli attacchi, sia che il dispositivo sia connesso o meno ad un computer host.

**Layered Data Security**

Tutti i dispositivi SPYRUS Windows To Go drives possono essere configurati con la crittografia software BitLocker per proteggere alcune o tutte le partizioni del drive ed abilitare un secondo livello di Defense-In-Depth encryption. Le password di BitLocker sono protette nella partizione di memoria a crittografia hardware antimanomissione (FIPS 140-2 Livello 3).

I dispositive criptati SPYRUS Windows To Go difendono l'integrità dell'ambiente operative anche se il boot viene eseguito su sistemi compromessi. La tecnologia brevettata SPYRUS rafforza la validazione pre-boot dell'hardware per garantire un avvio sicuro pur mantenendo una delle più alte velocità di boot della produzione attuale.

WorkSafe Pro e Secure Portable Workplace eseguono esaurienti validazioni della sequenza di boot:

Power-on self-tests validano l'integrità dell'hardware, del firmware e delle operazioni crittografiche. Ogni sospetta manomissione impedisce l'avvio del dispositive.

L'UEFI può validare il loader SPYRUS Toughboot™ per garantire immediatamente l'autenticazione protetta pre-boot. Il loader SPYRUS Toughboot è firmato da Microsoft ed è conforme a tutti i criteri di firma digitale per dispositive e loader di SO. Toughboot richiede una password ed autentica l'utente prima di eseguire la sequenza di caricamento. Quindi decripta la partizione Windows To Go ed esegue una verifica dell'integrità crittografica sul loader del boot di Windows. Dopo tutti questi test, il sistema si avvia. Infine Windows autentica l'account dell'utente, permettendogli l'accesso.

**Built In PKI Smart Card**

WorkSafe e WorkSafe Pro sono i soli dispositive certificati Microsoft Windows To Go dotati delle complete funzionalità di una smart card per l'identificazione e l'autenticazione. Con WorkSafe, il modulo hardware crittografato di sicurezza Rosetta Micro – validato FIPS 140-2 Livello 3/EAL 5+ - può essere utilizzato come un tradizionale smartcard token per l'autenticazione a due fattori ed altri servizi di sicurezza PKI basati su smart card nel tuo ambiente aziendale. Quando non è booted, WorkSafe serve come una smart card readerless USB 3.0 (CCID) che ti abilita ad utilizzare i tuoi cerfiticati RSA e/o elliptic curve ECDSA su qualunqeu computer compatibile.

WorkSafe supporta gli standard crittografici PKCS #11 e Microsoft Minidriver crypto. L'utility SPYRUS Minidriver Token per la gestione della smart card, dei certificate e delle password viene scaricata automaticamente da Windows Update al primo boot.

Le chiavi sono sempre generate a livello hardware nel controller Rosetta Micro e, per assicurare il più alto livello di sicurezza, non sono mai esportate. Gli amministratori possono resettare, ripristinare, revocare e gestire i certificati utente sulla smart card integrata Rosetta con i sistemi di gestione standard come Microsoft Forefront Identity Manager e con SPYRUS Minidriver Token Utility.

Quando WorkSafe viene avviato, il tuo ID digitale diviene automaticamente disponibile per le funzioni PKI di certificazione digitale come: smart card logon, firma o crittografia dei file e delle email, autenticazione VPN, autenticazione web.

**Data Vault Read/Write**

La partizione read/write Data Vault può archiviare file modificati dall'utente anche quando è abilitata la modalità Read-Only di protezone scrittura. E' possibile anche configurare una crittografia BitLocker separate per la partizione Data Vault ed usare password separate per ciascuna istanza di BitLocker o la stessa password BitLocker sia per il drive che per la partizione Data Vault. Tutti i dispositivi SPYRUS Windows To Go possono essere configurati con una partizione Data Vault durante il provisioning.

**Opzione Read Only**

L'opzione Read Only Evita la ritenzione di malware o altri download non autorizzati resettando tutte le modifiche intervenute su dati, SO ed applicazioni (eccetto i file archiviati nella partizione Data Vault) quando l'utente disconnette il dispositivo. In modalità Read Only il tuo sistema operativo, le tue applicazioni ed i tuoi file di dati sono completamente protetti contro alterazioni o infezioni da fonti esterne: puoi utilizzare un drive Read Only Windows To Go ad un chiosco dell'aeroporto, su WiFi pubblico o su un computer domestic senza alcuna preoccupazione.

**SPYRUS Enterprise Management System – Device Management**

Tutti i dispositivi SPYRUS Windows To Go possono essere gestiti tramite la console SPYRUS Enterprise Management System (SEMS™) per il mobile device management (MDM). Le funzionalità di SEMS includono: la disabilitazione e la cancellazione remote dei dispositivi, il password reset remoto, il rafforzamento delle policy, l'audit delle attività.

SPYRUS Enterprise Management System (SEMS) consente la gestione sicura dell'intera attività dei dispositivi USB aziendali. I drive gestiti da SEMS devono avere installato un software client (richiede l'acquisto di una licenza separata) e possono essere collegati ad un dominio SEMS. Drive disabilitati in remoto possono successivamente essere riconfigurati e reimpiegati..

**Bit Locker**

Tutti i dispositivi SPYRUS Windows To Go possono essere configurati con la crittografia software BitLocker per proteggere alcune o tutte le partizioni ed abilitare un secondo livello di sicurezza - Defense-In-Depth – aggiuntivo rispetto alla crittografia hardware. Le password BitLocker sono protette nella partizione hardware criptata ed antimanomissione validata FIPS140-2 Livello 3.




Rivenditore Autorizzato per l'Italia:
digiTree – via di Romagna 9/1, Trieste
sales@digitree.it – www.digitree.it
mob. +39 366 89 48 545