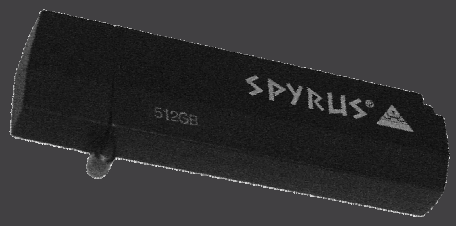
SPYRUS®

Windows To Go Xtreme Drives



Ambienti operativi Windows To Go multipli su un unico dispositivo

Windows To Go - Xtreme (WTGXtreme™)

I drive SPYRUS WTGXtreme aggiungono una nuova dimensione al mondo Windows To Go. Questi drive sono costruiti sulla base delle caratteristiche della famiglia SPYRUS Windows To Go, ed incorporano le più avanzate tecnologie di cifratura e sicurezza con la più grande versatilità in dimensioni e prestazioni disponibili attualmente sul mercato. WTGXtreme permette un enorme balzo in avanti, abilitando ambienti computazionali multipli, ciascuno con il proprio profilo operativo indipendente, sullo stesso dispositivo. Una forte separazione dovuta alla crittografia assicura un ambiente ad elevata garanzia per ciascun profilo.

Secure Portable Workplace Xtreme & WorkSafe Pro Xtreme

Sono disponibili due modelli di drive SPYRUS WTGXtreme: Secure Portable Workplace Xtreme (SPWXtreme™) e WorkSafe Pro Xtreme (WSPXtreme™). Entrambi coniugano le tecnologie SPYRUS™ per cifratura e sicurezza con i drive USB 3.0 certificati per Windows To Go (WTG). WSPXtreme integra inoltre la smart card PKI Rosetta® Micro, security controller certificato FIPS 140-2 Livello 3/EAL5+, se utilizzato con il Mini Driver SPYRUS o software PKCS#11 software. Tutti i drive WTGXtreme possono essere configurati con profili multipli indipendenti, ciascuno con il suo sistema operativo Windows 8, 8.1, or 10 e cifrati indipendentemente con il proprio unico insieme di chiavi crittografiche. Ciò permette alle organizzazioni di avere diversi ambienti operative, o profile, per un massimo di quattro utenti indipendenti, amministratori o applicazioni, pur mantenendo una forte separazione crittografica tra ciascun ambiente.

Stesso profilo a sicurezza di alto livello disponibile su tutti i drive SPYRUS Secure Windows To Go

I drive SPYRUS WTGXtreme assicurano lo stesso insieme di robuste caratteristiche di sicurezza di tuttti i drive SPYRUS Secure Windows To Go. Alcune di queste caratteristiche si applicano al drive nel suo complesso, ma molte possono essere configurate separatamente per ciascun profilo di un drive particolare.

Caratteristiche di Sicurezza del Drive WTGXtreme

Boot Protetto – I drive WTGXtreme difendono l'integrità dell'ambiente operative tramite il processo di boot di ciascun profile, anche quando il drive viene avviato su sistemi compromessi. Numerose verifiche validano l'integrità e rilevano manomissioni dell'hardware e del firmware del dispositivo, oltre al loader SPYRUS ToughBoot™ ed al loader di Windows, prima di avviare il sistema operativo. Il loader SPYRUS ToughBoot è firmato Microsoft ed è conforme a tutti criteri UEFI Secure Boot, consentendo una verifica addizionale di integrità durante il processo di boot, per prevenire che le infezioni da malware possano corrompere la sequenza di boot.

Hardware Read-Only sul Settore di Boot – Per accrescere la protezione dell'ambiente di boot dei drive WTGXtreme, l'intera sezione di boot può venire protetta con la modalità read-only, in modo da bloccare ogni tentative di modifica sulle component di boot del dispositivo. Inoltre, prima della autenticazione utente in uno dei profili configurati, non è possibile accedeere a nessuna delle memorie cifrate del drive tramite l'interfaccia USB.
In questo modo, quando il drive è "a riposo" soltanto il settore di boot read-only è esposto a eventuali attacchi informatici.

Controllo dei Privilegi di Accesso – Tutti i drive WTGXtreme possono essere configurati con una policy che controlli le condizioni di accesso della memoria cifrata. Queste condizioni includono:

- Boot Only – E' possibile accedere alla memoria del dispositivo solo da un drive autenticato ed avviato con successo.
- Accesso Limitato – Si può effettuare il login ed accedere al dispositivo da una macchina differente, ma viene imposta la modalità read-only.
- Accesso Completo – Viene consentito l'accesso complete al dispositivo su una differente macchina una volta che si è effettuato il login.

Built-in PKI Smart Card – Nella versione WSPXtreme dei dispositivi WTGXtreme, la smart card integrata_SPYRUS Rosetta, assieme al Minidriver certificato Microsoft, consente alle imprese di eseguire funzioni di sicurezza standard come la cifratura e la firma di file di Office, la firma e cifratura delle email, l'autenticazione multifattore, lo smart card logon, e l'accesso VPN, utilizzando le robuste credenziali PKI di un HSM certificato FIPS 140-2 Livello 3/EAL5. Inoltre è disponibile una libreria PKCS#11 per supportare le applicazioni che utilizzano questa interfaccia standard.

SPYRUS®

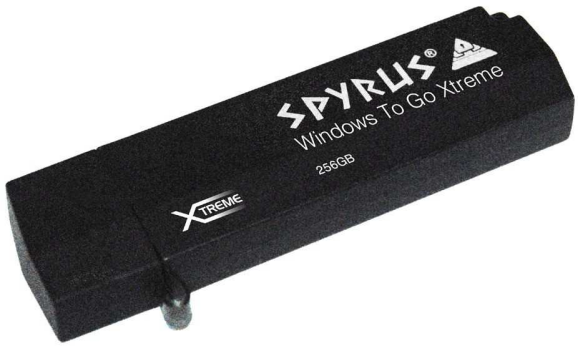
Caratteristiche di Sicurezza del Profilo Individuale

Hardware Full Disk Encryption – La protezione anti-manomissione sempre attiva dovuta alla crittografia hardware complete di tutti I dispositivi WTGXtreme fornisce estrema protezione per sistema operative, applicazioni e archiviazione dati, evitando che i dati a riposo possano essere visualizzati, cancellati o modificati. Ciò avviene in un modo che consente a tutta la memoria configurata per ciascun profilo sul drive WTGXtreme possa essere cifrata utilizzando le proprie uniche chiavi crittografiche ad entropia totale. Queste chiavi non vengono mai archiviate nella memoria flash e sono rese disponibili soltato dopo l'autenticazione per uno specifico profilo. Ciò fornisce una forte separazione crittografica tra profili, abilitando così l'indipendenza e l'isolamento delle attività di ciascun ambiente operative e prevenendo la sottrazione di dati tra profili differenti.

Protezione Read Only Opzionale per i volume di Sistema La modalità Read Only assicura l'utilizzo di un'immagine di sistema non corrotta ogni volta che si avvia un particolare profilo sui drive WTGXtreme. Ogni profilo può essere configurato con la modalità SPYRUS Read Only e, quando essa è abilitata, tutte le modifiche della partizione Windows di quel profilo vengono resettate quanto l'utente espelle il dispositivo, ritornando allo stato originale. Dal momento che impedisce la costante e non autorizzata archiviazione dei dati, la modalità Read Only è il modo ideale per indurre gli utenti a lavorare soltanto sulla rete, tramite VDI o in cloud, e per prevenire ulteriormente l'archiviazione locale di dati. Ciò aiuta a prevenire la sottrazione di dati aziendali importanti o critici.

Data Vault Read/Write– Ciascun profilo WTGXtreme può essere configurato con uno o due volume Data Vault read/write opzionali e di capacità variabile per l'archiviazione di file. I volumi Data Vault hanno capacità di lettura/scrittura persino quando la modalità Read Only è attivata, in modo che l'utente possa archiviare file di dati senza perderli. Gli amministratori possono avere il sistema operativo Windows e le applicazioni settate in modalità Read Only il che aiuta a prevenire il trasferimento di malware sulla rete aziendale, mantenendo nel contempo la possibilità per gli utenti di archiviare dati sul dispositivo. Si può accedere ai volumi Data Vault, se la policy lo permette (vedi paragrafo precedente) da un ambiente Windows To Go già avviato senza aver eseguito il boot dal drive. Questo consente all'utente di trasferire file a e da i suoi volumi Data Vault da un altro ambiente operativo desktop.

Sicurezza dei Dati a più Livelli – Utilizzando il software opzionale BitLocker di Microsoft, le aziende possono aggiungere un secondo livello di cifratura alla partizione Windows oppure alle partizioni Data Vault per ciascun profilo del drive WTGXtreme. Ciò permette un ulteriore difesa profonda da configurare quando se ne riscontra la necessità. E, ogni volta che vengono utilizzate, le chiavi BitLocker sono archiviate nel settore a crittografia hardware, rendendole così inaccessibili agli hackers quando i dati sono a riposo.



Esigenze Versatili

Permettendo di avere più ambienti operative su un unico dispositivo, ciascuno dei quali con il proprio profilo operativo indipendente, i drive WTGXtreme consentono di ottemperare ad un numero ancora maggiore di esigenze d'uso, come descritto di seguito.

Bring Your Own Device (BYOD)

Se un impiegato dell'azienda ha intenzione di utilizzare un dispositioo per uso sia aziendale che personale (es. fare transazioni bancarie nella pausa pranzo), entrambe le parti vogliono assicurarsi che ci sia una forte separazione tra questi due ambienti operativi per essere certi che non ci siano compromissioni tra dati sensibili di entrambi gli ambienti.

I driver SPYRUS WTGXtreme soddisfano questa esigenza in un unico conveniente pacchetto. L'autenticazione indipendente e la cifratura del drive in entrambi i profili fornisce un firewall molto potente tra ambienti operativi.

Accesso Internet Protetto

Alcune organizzazioni non permettono di accedere ad internet dalle proprie piattaforme o da specifiche immagini del proprio sistema operativo, il che talvolta può causare delle inefficienze sul lavoro. WTGXtreme risolve questa difficoltà avendo la possibilità di avviare soltanto l'immagine aziendale sicura o, al contrario, quando è necessario accedere ad internet, di avviare un'immagine alternative che permetta l'accesso alla rete quando si opera al di fuori degli obblighi aziendali.

SPYRUS®

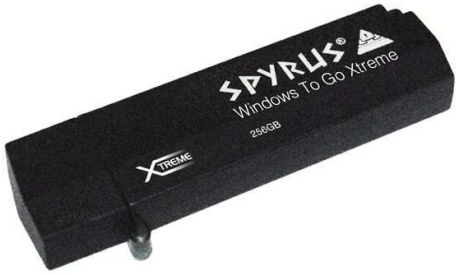
PC Condivisi

Molte organizzazioni offrono un servizio di assistenza 24/7. In questo caso WTGXtreme provvisto di profili multipli può permettere a quattro operatori di operare sul medesimo dispositivo per fornire l'assistenza necessaria nel corso di tutta la giornata. Similmente in campo sanitario, più di un operatore può accedere al proprio profilo da un unico dispositivo, per esempio, nelle postazioni critiche di un pronto soccorso.

Migrazione Aziendale

Se un'azienda passa da Windows 7 a Windows 8.1 e poi a Windows 10, è praticamente impossibile effettuare la transizione ad un nuovo ambiente operativo in modo istantaneo. Ci saranno vecchie applicazioni che risultano ancora essenziali all'attività aziendale che non sono ancora passate al nuovo sistema operativo.
A ciò si aggiunga il tempo necessario alla formazione del personale perché apprenda il nuovo sistema, e quindi molto probabilmente si cercherà di estendere l'intervallo di transizione. Per minimizzare le inefficienze ed la generale perturbazione delle attività dell'azienda, è utile che gli impiegati possano avere accesso sia al vecchio che al nuovo ambiente operativo.

I drive SPYRUS WTGXtreme costituiscono una soluzione ideale per facilitare questa transizione. Con un drive WTGXtreme l'utente può avviare entrambi gli ambienti, avere piena operatività in ciascuno di essi ed accedervi da un'unica postazione.



Amministrazione di Dominio

Molti amministratori di sistema gestiscono molteplici reti che si espandono su differenti domini amministrativi. Per sicurezza aggiuntiva nell'accesso a ciascun dominio, gli amministratori possono usare differenti profili per gestire ciascuna rete. Inoltre, utilizzando la modalità read-only su ogni profilo o su uno in particolare, il trasferimento del malware tra domini viene grandemente diminuito..

I drive WTGXtreme sono anche ideali per implementare la Privileged Access Workstation (PAW) di Microsoft, il che, per operazioni che richiedano un'aumentata cautele, fornisce un sistema operative dedicato che è protetto dagli attacchi di internet e vettori di minacce. Separare questi compiti e questi account dall'utilizzo quotidiano di workstation e dispositivi assicura una protezione fortissima contro un'ampia varietà di attacchi o vulnerabilità di sistema.

Utilizzo Cross Domain

Molte organizzazioni limitano l'accesso a differenti tipi di dati in base alle necessità individuali degli utenti di vedere i dati archiviati sulle reti. Gli utenti potrebbero potenzialmente utilizzare uno specifico profilo per un tipo di accesso multi-dominio a differenti livelli di classificazione dati. Utilizzando la smart card integrata in WSPXtreme, certificati diversi possono venire archiviati per differenti profili, aggiungendo un altro strato di autenticazione sicura per quelle specifiche informazioni archiviate sulla rete.

Molte organizzazioni governative restringono l'accesso agli utenti in base a livelli di classificazione dei dati presenti sulle reti. Gli Stati Uniti, per esempio, distinguono le informazioni in Sensitive But Unclassified (SBU), SECRET e TOP SECRET, e ciascun tipo richiede delle credenziali utente diverse. Usando i profili multipli del drive WTGXtreme, con credenziali diverse archiviate nel rispettivo profilo per avere accesso a domini con differenti livelli di classificazione dei dati, un unico dispositivo può venire utilizzato per accedere a più domini con una forte separazione crittografica tra profili, fornendo così una piattaforma cross-dominio super affidabile.

Chi è SPYRUS

SPYRUS fornisce soluzioni crittografiche innovative che offrono la più forte protezione per il trasferimento, l'archiviazione e l'elaborazione dei dati. Da oltre 20 anni, SPYRUS ha fornito prodotti del massimo livello per quanto riguarda la crittografia hardware, l'autenticazione e la sicurezza dei contenuti digitali a enti pubblici, organizzazioni finanziarie e strutture sanitarie. Per evitare l'introduzione di componenti non sicure, la tecnologia brevettata "Secured by SPYRUS™" è progettata, ingegnerizzata e prodotta negli Stati Uniti per conformarsi agli standard FIPS 140-2 Livello 3. SPYRUS collabora fianco a fianco con Microsoft per fornire piattaforme portabili certificate Windows 7, Windows 8, Windows 8.1. e Windows 10. La sede principale di SPYRUS è a San Jose, California.

SPYRUS®

Specifiche Tecniche

Capacità & Dimensioni (LxPxH)

128 GB, 256 GB
86.1 mm x 24.2 mm x 10.8 mm (+/- 0.20)

512 GB capacities (1 TB coming soon)
101.6 mm x 24.2 mm x 10.8 mm (+/- 0.20)

Prestazioni (basate su un drive 512 GB)

USB 3.0 Super Speed; USB 2.0 Compatible

Nota: le prestazioni Random Read e Random Write sono la metrica più importante per i Live Drive avviabili.

Lettura Sequenziale: fino a 249 MB/sec

Scrittura Sequenziale: fino a 238 MB/sec

Affidabilità

Data Retention: 10 anni

Altre Certificazioni

Microsoft Windows To Go

FIPS 140-2 Algorithm Certificates

FIPS 140-2 Level 3

Consumo Elettrico

Voltaggio Operativo	Vcc = 3.3 to 5 VDC
Consumi	275mA @ 3.3VDC

Altro

Umidità	90%, noncondensing

Integrità Fisica dei Dispositivi:

SPYRUS sa che le persone spesso si affidano ai loro dispositivi USB per missioni critiche. Essenzialmente, essi costituiscono i loro computer SSD. Così, diversamente dai drive USB tradizionali, che sono meno utilizzati e più facilmente rimpiazzabili, comprendiamo che i dispositivi devono resistere anche per quanto riguarda le caratteristiche fisiche. A tal fine abbiamo progettato i nostri drive seguendo gli standard più elevati per componenti e materiali. Stringenti test ambientali unitamente ad ulteriori test su campi magnetici, radiazioni e immersioni prolungate dimostrano l'usabilità di questa configurazione ad alta sicurezza dei dispositivi USB di SPYRUS persino nelle strutture più critiche, come possono essere quelle sanitarie.

Configurabilità

I drive SPYRUS WTGXtreme possono essere configurati con un massimo di 4 indipendenti ambienti operativi Windows isolati crittograficamente, per supportare la multi-utenza, il cross-domain, la migrazione aziendale, il BYOD ed altri scenari operative. È consigliabile che ciascun profilo abbia almeno 64GB di capacità.

Test ambientali

Temperatura Operativa (MIL-STD-202, METH 503) 0ºC - 70ºC

Ciclyng della Temperatura non operativa (MIL-STD-810, METH 503)
-40ºC - 85ºC

Alte temperature archiviazione (MIL-STD-810, METH 501) 85ºC; 96 ore EMI (FCC/CE) FCC Part 15, Class B/EN55022 - EN55024/etc

ESD (EN61000-4-2)
Enclosure Discharge - Contact & Air. Dust Test (IEC 60529, IP6) As per defined

Waterproof Test (IEC 60529, IPX7) As per defined

Operating Shock, MIL-STD 883J, Method 2002.5, Cond. B, 1500g, 0.5ms, 1/2 sinusoide

Alte Temperature Archiviazione/Data Retention, MIL-STD-810, METH 501, 100ºC; 96 ore

Waterproof test,MIL-STD-810, METH 512.6,1 metro prof., 30 minuti

Hardware Security & Cryptographic Standards

Gli algoritmi utilizzati da SPYRUS comprendono la Suite B (insieme di algoritmi di cifratura impiegati per la modernizzazione della crittografia) e crittografia RSA.

XTS - AES 256 Full Disk Encryption^

AES 128, 196, and 256 ECB, CBC, CTR, and Key Wrap Modes

SP800 - 90 DRBG (Hash DRBG)

Elliptic Curve Cryptography (P-256, P-384, P-521)

ECDSA Digital Signature Algorithm

CVL (ECC CDH) [ECDH per SP 800-56A]

Concantenation KDF (SP800-56A)

RSA 1024 and 2048 Signature
RSA 1024 and 2048 Key Exchange

PBKDF - 2 (per PKCS#5 versione 2)

DES, two-& three-key triple DES with ECB, CBC Mode (Note DES has been deprecated by NIST.)

SHA-1 and SHA-224/256/384/512 hash algorithms with HMAC Support

Il supporto per la crittografia può variare a seconda della versione.

Il case opaco riempito di resine epossidiche FIPS 140-2 Livello può essere modificato per ordini speciali.

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

Venduto in Italia da:
DigiTree
Via di Romagna 9/134134
Trieste (Italy)
+39 366 8948545
sales@digitree.it
www.digitree.it