SPYRUS®

WorkSafe™ e WorkSafe Pro™

Per Windows To Go 8.1 e Windows 10

WorkSafe & WorkSafe Pro

I drive WorkSafe di SPYRUS aggiungono un nuovo support Windows 8.1 e Windows 10 per il USB CCID su l'hardware criptato Rosetta® (validato FIPS 140-2 Level 3/ EAL 5+) alla lunga lista di caratteristiche già disponibili sui drive Windows To Go SecurePortable Workplace™ e Portable Workplace™. Sia WorkSafe (crittografia BitLocker) e WorkSafe Pro (crittografia hardware) includono una smart cart PKI reader-less integrata (FIPS 140-2 Livello 3) che consente l'autenticazione delle credenziali dell'utente. Gli utenti aziendali possono godere della mobilità di un drive Windows To Go certificato Microsoft con accesso autenticato a tutte le risorse della rete aziendale. L'IT dell'azienda può star certo che l'accesso remoto alle risorse di valore è ad opera di utenti autentici che operano sull'immagine Windows aziendale – anche quando essa viene avviata su computer non sicuri.

WorkSafe Pro fornisce crittografia hardware XTS-AES256 a livello militare per l'intero drive, garantendo protezione estrema al sistema operativo, alle applicazione ed all'archiviazione. Sia WorkSafe che WorkSafe Pro possono utilizzare BitLocker per la crittografia software aggiuntiva.

La serie di drive allo stato solido WorkSafe permette alte prestazioni con protezione dati sempre attiva.

Drive Avviabili che permettono il Lavoro Mobile

WorkSafe trasforma i personal computer, inclusi i Mac che permettono l'avvio di Windows, in computer Windows conformi alle direttive aziendali – in presenza ed anche in assenza di connettività. Questi dispositivi non hanno alcun impatto sul computer host e non lasciano tracce dietro a sé.

Migliora l'Endpoint Security

Assumi il controllo del BYOD e dei computer remoti. Dispositivi BYOD non aggiornati e non controllati creano un evidente pericolo quando viene loro permesso di accedere alla rete aziendale. I drive WorkSafe migliorano l'endpoint security trasformando i dispositive BYOD e i computer di casa in punti di accesso garantiti.

Smart Card Integrata FIPS 140-2 Livello 3 Anti-Manomissione Per l'Autenticazione Multifattore

WorkSafe e WorkSafe Pro sono drive certificate Microsoft-dotati delle ricche possibilità di autenticazione di una smart card readerless Rosetta integrata – niente di extra da portare o da perdere.

Supporto USB CCID (chip card interface device) significa che WorkSafe incorpora le funzionalità di una smart card integrata che protegge tutte le chiavi in un hardware anti-manomissione. Quando WorkSafe viene avviato, il tuo ID digitale viene reso automaticamente disponibile per le funzioni di certificazione digitale PKI quali crittografia delle email, autenticazione multifattore, logon di smart cars, BitLocker To Go e accesso VPN.

Quando non fa il boot, WorkSafe funziona come una smart card USB 3.0 readerless che ti abilita ad usare i tuoi certificate digitali su qualunque computer compatibile.

WorkSafe supporta gli standard crittografici PKCS #11 e CAPI/CNG. L'utility SPYRUS Minidriver Token è acclusa a WorkSafe per gestire la smart card, i certificate e le password.

Abilita l'Accesso Remoto Protetto e Senza Interruzione

Il personale remoto o viaggiante non trova alcuna differenza tra l'accedere dall'ufficio e quando usano VPN authenticate da smart card da postazioni remote. Con Microsoft DirectAccess VPN, gli utenti si connettono automaticamente ed accedono alla rete aziendale con la possibilità di archiviare chiavi e certificate sul controller integrato della smart card.

Consente più Livelli di Crittografia

La crittografia hardware anti-manomissione sempre attiva in WorkSafe Pro impedisce di accedere, distruggere o modificare i dati. Le chiavi crittofrafiche di WorkSafe Pro non vengono mai archiviate nella memoria flash. La crittografia software opzionale di BitLocker fornisce un secondo livello di sicurezza e le chiavi di BitLocker vengono archiviate nella partizione a crittografia hardware, inaccessibile agli hacker.

.

SPYRUS®

La Crittografia Hardware di WorkSafe Pro protegge l'Integrità di Windows 8.1 anche su PC Ostili

WorkSafe Pro difende l'integrità dell'ambiente operative anche se avviato su sistemi compromessi. Numerose verifiche ne convalidano l'integrità e rilevano alterazioni del loader SPYRUS Toughboot™, dell'hardware e del firmware prima di avviare il sistema operativo.

Il loader SPYRUS Toughboot è firmato da Microsoft ed è conforme a tutti i criteri di Secure Boot. Secure Boot è una specifica UEFI che verifica la presenza di una firma digitale approvata in tutti i driver e loader OS per evitare le infezioni da malware durante le operazioni di boot.

Windows 8.1
Windows 10

Dispositivo Mobile, Identità e Desktop Management

I drive WorkSafe possono essere gestiti a più livelli con l'ecosistema Microsoft e le soluziono SPYRUS:

- Servizi di ceertificazione di Microsoft o altri permettono ad un'organizzazione di gestire emission, rinnovo o revoca dei certificati
- Microsoft Certificate Services supporta Active Directory. La CA aziendale pubblica i certificate Utente e le liste di revoca dei certificate (CRL) in Active Directory.
- Microsoft Forefront Identity Manager permette agli amministratori di resettare, ripristinare, revocare e gestire I certificate utente sulla smart card integrata.
- Microsoft Direct Access per l'accesso remote permette di connettersi senza soluzione di continuità e in modo più sicuro alla rete aziendale senza la necessità di una VPN. Puoi archiviare le chiavi ed i certificati Direct Access sul chip smart card integrato
- Con la crittografia opzionale BitLocker, le aziende possono aggiungere un secondo livello di crittografia a quello hardware di SPYRUS WorkSafe Pro, assicurandosi una sicurezza profonda. BitLocker può anche essere usato per criptare i dati sui drive WorkSafe.
- Microsoft System Center abilita gli amministratori ad aggiornare ed inviare patch al SO ed alle applicazioni quando i dispositive WorkSafe sono collegati al dominio ed anche a configurarli remotamente..
- La smart card integrata SPYRUS Rosetta assieme al Minidriver, consente alle aziende di eseguire le funzioni di sicurezza standard delle smart card come crittografia delle email, autenticazione multifattore, logon di smart card e accesso VPN.

Protezione Read Only

L'opzione Read Only assicura una imagine non corrotta ad ogni boot del dispositivo. Tutte le modifiche del sistema operativo, delle applicazioni e dei file di dati vengono cancellate alla disconnessione. Le aziende possono così garantirsi che gli utenti lavorino SOLO sulla rete aziendale e non archivino dati localmente sul dispositivo.

Partizione Read/Write Data Vault

I drive WorkSafe possono essere dotati di una partizione read/write Data Vault dove possono essere archiviati file modificati dall'utente anche quando è abilitata la modalità Read-only. E' possibile accedere alla partizione Data Vault anche su un dispositivo WorkSafe che non abbia eseguito il boot, come ad un normale dispositivo di archiviazione USB esterno.

La partizione Data Vault può essere protetta con la sicurezza di Rosetta smart card security e/o con BitLocker To Go.

Gestione Centralizzata dei Dispositivi Aziendali

SPYRUS Enterprise Management System (SEMS™), console per la gestione dei dispositive, include, tra le alter, funzionalita di disabilitazione e cancellazione remote, reset delle password, rafforzamento delle policy, azioni di audit.