SPYRUS®

Windows To Go & Storage Sicuri...

...nell'Ecosistema Microsoft

SYRUS è partner Microsoft dal 1994, offrendo a aziende pubbliche e private innovative soluzioni per la sicurezza e per il business. Tutti i prodotti SPYRUS sono progettati tenedo presente l'ecosistema Microsoft per accrescere ed estendere i servizi e le soluzioni di sicurezza offerti da Microsoft. I prodotti SPYRUS comprendono:

Windows To Go

I live drive SPYRUS Windows To Go (WTG) trasformano qualunque computer, compresi i tablet Surface Pro, in desktop conformi a Windows Enterprise 8, 8.1 o 10 – in presenza o assenza di connettività. I drive SPYRUS WTG avviano il proprio sistema operative direttamente dalla loro partizione hardware criptata e bypassano completamente il disco rigido del computer host: nessun impatto su quest'ultimo e nessuna traccia lasciata una volta che il drive viene disconnesso. Le caratteristiche includono:

- Built-in PKI smart card
- Validato FIPS 140-2 Level 3
- Crittografia hardware XTS-AEX 256
- Possibile modalità read-only
- Possibile data vault read/write (può venire utilizzata su Surface Pro 4 per la gestione sicura dei dati)
- Hardware testato MIL-810, caratteristiche rugged di livello militare

I drive SPYRUS possono far diminuire i tuoi costi operativi, aggiungere una significativa sicurezza ai tuoi end-point e rendere più agevole il supporto di policy BYOD sia per gli impiegati che per collaboratori e lavoratori in remoto. SPYRUS WTG è la scelta giusta anche al momento di sostituire un computer, come modo di estenderne vita e prestazioni, riducendo la spesa di 1/3.

Rosetta TrustedFlash™

La card Rosetta microSDHC nella configurazione TrustedFlash™ rende possibile la crittografia AES-256, offrendo la più forte protezione dei dati attualmente disponibile e le funzionalità PKI da utilizzare con le applicazioni abilitate a chiave pubblica. È progettata dall'inizio alla fine per garantire la più elevata protezione delle informazioni su dispositivi mobili, laptop e tablet, come Surface Pro, per i dati a riposo e in transito. Il suo conveniente formato consente l'archiviazione protetta dei dati su dispositivi con un numero limitato di porte USB o che hanno soltanto lo slot per la microSD, senza la scomodità di una chiave USB che sporge dal dispositivo.

Aziende nei settori dell'industria, della pubblica amministrazione, delle infrastrutture critiche, della sanità ed altri saranno abilitate a proteggere informazioni confidenziali o dati personali e sensibili utilizzando la sicurezza SPYRUS di livello militare assieme ai certificate digitali conservati nell' HSM validato FIPS 140-2 Level 3 integrato nella card per autenticarsi sulle reti e sui servizi ed applicazioni cloud di Microsoft.

Pocket Vault 3-X

Il dispositivo crittografico USB 3.0 PocketVault P-3X un dispositivo SSD ad alta sicurezza che, grazie alla crittografia hardware, protegge i tuoi dati come in una cassaforte. La combinazione di USB 3.0 e storage SSD raggiunge le più elevate prestazioni. PocketVault P-3X cifra con chiave XTS-AES 256-bit per proteggere dati sensibili e confidenziali. Perché affidare i dati di oggi alla sicurezza di ieri?

PocketVault P3-X somma in sé altre funzionalità di sicurezza come la possibilità di autenticazione e l'abilitazione PKE

SPYRUS®

ai servizi applicativi utilizzata da imprese e pubblica amministrazione per l'autenticazione a due fattori e la comunicazione protetta di dati tramite i servizi cloud e le applicazioni Microsoft.

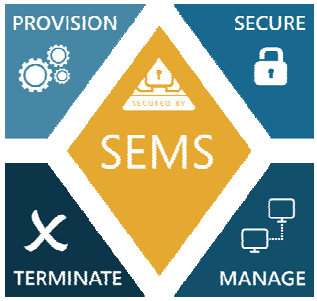
P-3X, nella modalità Courier, può essere impiegato in situazioni particolarmente critiche in cui la possibilità di modificare dati deve essere riservata ad utenti privilegiati, mentre agli altri può essere concessa solo la modalità read-only. La situazione tipica si ha quando un utente con più alti privilegi salva sul dispositivo P-3X informazioni confidenziali, come previsioni di vendita, previsioni finanziarie, brevetti, e così via e limita gli utenti alla sola possibilità di "leggere" i dati senza poterli modificare.

NcryptNshare

Le applicazioni NcryptNshare, assieme aidispositivi e le smart card descritti finora, permettono la collaborazione e lo scambio crittografato end-to-end tra mittenti e destinatari per proteggere i dati in transito e a riposo. La linea NcryptNshare™ offre crittografia, autenticazione, condivisione di informazioni tra le applicazioni di Office, Office 365 e Microsoft Cloud Services. La famiglia di prodotti NcryptNshare comprende:

- RES4Office, un plug-in di Office che abilita la cifratura e la condivisione di file Word, Excel, PowerPoint, Visio, Sharepoint e Outlook
- RES Disk, che permette di creare dei dischi virtuali protetti per la cifratura e la condivisione sicura;
- RES Pro, un'estensione di Windows Explorer che dà all'utente un'esperienza "tasto destro" per cifrare file di qualunque tipo e consente la condivisione sicura con altri utenti autenticati RES Pro.

SPYRUS Enterprise Management System ("SEMS™")



SEMS offre una soluzione forte a produttività e sicurezza per ogni organizzazione che impieghi i drive SPYRUS di storage crittografato e/o i live drive Windows To Go certificati Microsoft. Se da un lato questi dispositivi offrono la più forte protezione Data-at-Rest, quando vengono utilizzati da una forza lavoro mobile le organizzazioni si trovano ad affrontare un'altra sfida: la gestione, l'audit e l'imposizione delle policy per questi piccoli dispositivi ad elevate capacità. SEMS risolve questo problema: progettato per operare su server Windows on premises o su Microsoft Azure, ti offre la scalabilità da una soluzione con un piccolo numero di dispositivi (es., una POC) fino al dispiegamento di decine di migliaia di dispositivi da gestire.

SEMS estende l'approccio alla sicurezza del tipo end-to-end anche agli utenti mobili per proteggere i dati a riposo e in transito, e permette all'azienda di essere conforme alle più diverse e restrittive regolamentazioni sulla protezione dei dati. Grazie alla gestione dei dispositivi tramite SEMS, gli amministratori IT possono registrare, bloccare o sbloccare, revocare i permessi, settare policy, effettuare l'audit dei contenuti e persino "uccidere" i dispositivi crittografati SPYRUS da un'unica console centralizzata.

Per altre informazioni sui prodotti SPYRUS, visita www.digitree.it o contattaci via email o telefono.

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

SUITE B ON BOARD

Italy & Europe
Adriana Franca
Digitree
+39 366 8948545
adriana.franca@digitree.it

digitree