SPYRUS®

Diventare GDPR Compliant

Panoramica dei prodotti SPYRUS

Il nuovo GDPR prevede pesanti sanzioni (fino a 20 milioni di euro o il 4% del fatturato globale annuo) qualora un'organizzazione non riesca a fornire un "ragionevole" livello di protezione dei dati personali, indipendentemente dalle sue intenzioni. Anche le compagnie internazionali con sede principale al di fuori dell'EU, sono ugualmente soggette alle sanzioni di GDPR per quanto riguarda le loro filiali europee.

Le organizzazioni non possono lasciare che il termine "ragionevole" venga definito a discrezione di chi effettua una verifica post-evento. E le spese legali per dimostrare lo "sforzo ragionevole" possono essere altrettanto dispendiose. Le trasparenti soluzioni di crittografia ad alta affidabilità di SPYRUS forniscono un valido rinforzo per conformarsi al GDPR, con particolare riferimento all'articolo 25 relativo a "protezione dei dati per design e per default". Le root of trust hardware di SPYRUS hardware, i prodotti di sicurezza abilitati Rosetta Hardware Security Module (HSM), sono l'unica soluzione in cui la ragionevolezza non può essere messa in discussione.

I dispositivi SPYRUS, protetti dall'HSM Rosetta, sono totalmente cifrati con chiari e algoritmi di livello militare, entrambi protetti dall'hardware, sono utilizzati anche per la protezione di informazioni classificate.

Windows To Go

I live drive SPYRUS Windows To Go (WTG) trasformano qualunque computer in desktop enterprise-compliant Windows 8, 8.1 o 10, in presenza o in assenza di connettività. I drive SPYRUS WTGsi avviano direttamento dalla propria partizione crittografata, bypassando completamente l'hard disk del sistema host. Non vi è alcun impatto sull'host e non viene lasciata alcuna traccia quando il drive viene disconnesso.

Principali caratteristiche:

- Built-in PKI smartcard
- Validato FIPS 140-2 Livello 3
- Crittografia hardware XTS-AEX 256
- Sola lettura opzionale
- Possibile partizione cifrata read/write
- Hardware rugged testato MIL-810

SPYRUS può aiutarti a diminuire i costi operativi, aggiungendo una significativa sicurezza ai tuoi end-point e rendendo più semplice supportare le policy BYOD sia per gli impiegati che per i collaboratori. I drive SPYRUS WTG possono anche venire impiegati per la sostituzione dei computer come modo per prolungare la vita e le prestazioni dei computer ad una frazione del costo.

Rosetta TrustedFlash™

La microSDHC Rosetta coon la configurazione TrustedFlash™ permette la cifratura hardware AES-256 per fornire la più robusta protezione dei dati commercialmente disponibile e le funzionalità PKI da utilizzare con le applicazioni a chiave pubblica. È progettata fin dalle basi per assicurare alta affidabilità nella protezione delle informazioni su dispositivi mobili,laptop e tablet per dati in transito e a riposo. Il suo conveniente formato permette lo storage sicuro per dispositivi con un numero limitato di porte USB o che hanno soltanto slot e microSD.

Organizzazioni nei settori Enterprise, Government, Critical Infrastructure, Sanità e altri saranno in grado di proteggere informazioni confidenziali e dati personali utilizzanto la sicurezza SPYRYS di livello militare, utilizzando nel contempo i certificati digitali conservati nell'HSM validato FIPS 140-2 Livello per autenticarsi sulla rete e nei servizi ed applicazioni cloud Microsoft.

Pocket Vault 3-X

PocketVault P-3X USB 3.0 è un dispositivo SSD a cifratura hardware, utilizzabile dappertutto, che protegge i tuoi dati come una cassaforte. La combinazione di USB 3.0 e storage SSD permette le più alte prestazioni. PocketVault P-3X cifra i dati con chiave XTS-AES 256-bit

Pocket Vault 3-X aggiunge ulteriori funzionalità di sicurezza provvedendo autenticazizone e servizi PKE per le applicazio-

SPYRUS®

ni utilizzate da imprese e organizzazioni governative per l'autenticazione a due fattori e le comunicazioni sicure nei servizi e applicazioni Microsoft Cloud.

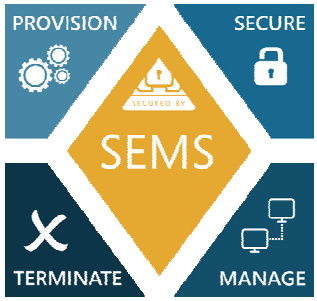
P-3X in modalità Courier è utilizzabile qualora le modifiche ai dati devono essere limitate ad utenti privilegiati mentre agli altri utenti devono essere consentite soltanto capacità di sola lettura. Per esempio, per archiviare su P-3X informazioni confidenziali, come previsioni di vendita, previsioni di bilancio, proprietà intellettuali o anche aggiornamenti dei data base, e limitare la possibilità dell'utente finale alla sola lettura senza poter effettuare alcuna modifica ai dati.

NcryptNshare

NcryptNshare in combinazione con i dispositivi descritti sopra supporta la collaborazione assicurando la cifratura end-to-end e la condivisione tra mittenti e destinatari per proteggere i dati in transito e a riposo. La linea di prodotti NcryptNshare™ offer crittografia, autenticazione e condivisione collaborativa delle informazioni per le applicazioni Microsoft Office, Office 365 e Microsoft Cloud Services. Le applicazioni NcryptNshare comprendono:

- **RES4Office**, un plug in di Office che abilita la cifratura e la condivisione sicura di file;
- **RES Disk**, che permette la creazione di partizioni virtuali protette per cifratura e condivision sicura;
- **RES Pro**, un'estensione di Windows Explorer che dà all'utente l'esperienza "testo destroy" per cifrare ogni tipo di file e permette la condivisione sicura con qualunque altro Utente autenticato RES Pro.

SPYRUS Enterprise Management System ("SEMS™")



SEMS offre una soluzione di robusta sicurezza e produttività per ogni organizzazione che adotti i dispositivi sicuri ed i live drive WTG di SPYRUS. Se da un lato questi dispositivi forniscono la più forte protezione per i dati a riposo quando utilizzati da utenti in mobilità, le organizzazioni devono dall'altro affrontare l'ulteriore sfida della gestione, dell'audit e dell'imposizione di policy per questi dispositivi piccoli ma di grande capacità di storage. SEMS risolve questo problema: progettato per operare nell'ecosistema Windows on premises o su Microsoft Azure con la possibilità di scalare da una POC a dispiegamenti di decine di migliaia di dispositivi da gestire.

SEMS estende un reale approccio di sicurezza end-to-end agli utenti mobile per proteggere i dati a riposo e in transito ed mettendo l'impresa in condizione di conformarsi con le più restrittive regolamentazioni. Grazie alla gestione dei dispositivi via SEMS, gli amministratori IT possono registrar, abilitare/disabilitare, revocare, settare policy, eseguire audit e "uccidere" centralmente i dispositivi a cifratura hardware SPYRUS.

Per maggiori informazioni sui prodotti SPYRUS, visita www.digitree.it o contattaci per email o telefono.

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

SUITE B ON BOARD

Distribuito da:
DIGITREE
www.digitree.it
sales@digitree.it
+39 366 8948545