

## Sicurezza totale nella protezione dei dati

I metodi tradizionali di difesa perimetrale dei network aziendali – password, firewall, antivirus, etc. – offrono una protezione di base, ma non risolvono tutti i problemi legati alle minacce presenti nelle reti aziendali. Si fa sempre più forte l'esigenza di tutelare il patrimonio di dati sensibili personali, informazioni finanziarie, comunicazioni interne, codici sorgenti di applicazioni, progetti tecnici, contratti, ecc. Ad amplificare ulteriormente i rischi legati alla violazione delle informazioni è il crescente utilizzo di dispositivi "mobile" (portatili, smartphone, palmari etc), così come il frequente impiego di dispositivi removibili per la memorizzazione (cd, dvd, pen drive, memory card o dischi esterni). La sfida principale consiste nel trovare soluzioni specifiche che impediscano la fuga di informazioni e garantiscano la riservatezza dei dati.



## Le Soluzioni di SafeNet

L'utilizzo della crittografia, abbinata a strategie di autenticazione utente, è la soluzione più efficace ed economica per risolvere i problemi di sicurezza delle informazioni. Una volta cifrati, i dati saranno accessibili solo all'utente opportunamente autenticato e autorizzato. Le informazioni cifrate rimarranno così confidenziali e la loro integrità garantita. Symbolic propone la suite SafeNet per la cifratura dei dati abbinata all'utilizzo di token crittografici usb SafeNet iKey per l'autenticazione dell'utente a due fattori (password + token).

### • SafeNet Protect Drive

Risolve il problema della divulgazione non autorizzata di informazioni dovute a furto o smarrimento di un device hardware. Il software cifra l'intero contenuto dell'hard disk di pc, server, portatili o dispositivi di memorizzazione removibili, permettendone l'uso solamente a utenti autenticati e autorizzati. Protect Drive è anche in grado di impedire tentativi di lettura del disco tramite supporti esterni per il boot (es. cd live Linux). L'autenticazione impedisce il boot della macchina, possibile solo se si forniscono al sistema le credenziali di autorizzazione. Inoltre si possono creare regole per permettere l'utilizzo dei device removibili solo agli utenti autorizzati. Protect Drive si integra con Microsoft Active Directory e tramite esso è gestibile centralmente (deployment, configurazione, gestione, controllo). È possibile abbinare a Protect Drive i token Safenet iKey 1000 e 2032 per l'autenticazione a due fattori. È sviluppato per Windows (client e server) e ne supporta i meccanismi di single sign-on.

### • SafeNet Protect File

Permette la cifratura di file individuali, gruppi di file o intere cartelle memorizzati su server, workstation, portatili e dispositivi di memorizzazione removibili, proteggendo i dati anche dopo il boot della macchina. Protect File completa Protect Drive: quest'ultimo, infatti, una volta che l'utente si è autenticato, decifra l'intero disco mettendo a disposizione tutti i dati memorizzati. Solo dopo l'identificazione dell'utente da parte di Protect File sarà possibile accedere a quei dati per l'utilizzo. Protect File supporta meccanismi di single sign-on con Protect Drive, oppure richiede all'utente un ulteriore livello di autenticazione per accedere ai dati locali, a cartelle condivise su server di rete oppure a dati memorizzati su dispositivi removibili. Nel caso di dati condivisi su un server, Protect File gestisce la concorrenzialità degli accessi a file cifrati e protegge, cifrandola, la comunicazione tra i vari sistemi. Anche Protect File può utilizzare i token usb SafeNet iKey 2032 per un'autenticazione a due fattori. Protect File è sviluppato per l'ambiente Windows (client e server) e ne supporta i meccanismi di single sign-on.

Due sono le versioni disponibili: -Protect File Premium  
-Protect File Business

### L'Azienda

SafeNet è leader a livello globale nel settore della sicurezza informatica. Fondata più di 20 anni fa, l'azienda fornisce una sicurezza completa utilizzando proprie tecnologie di crittografia per proteggere le comunicazioni, la proprietà intellettuale e le identità digitali, e offre uno spettro completo di prodotti che includono hardware, software e chips.

- **SafeNet Protect Pack**

Consente la cifratura di quei file che vengono spediti via mail o copiati. Protect Pack si integra nell'ambiente Windows mettendo a disposizione le funzioni di cifratura e decifratura da riga di comando oppure tramite lo strumento di Esplora Risorse. L'operazione di cifratura dei file prevede anche la compressione e la possibilità di creare un package auto estraibile protetto da una password "robusta". Protect File è sviluppato per l'ambiente Windows (client e server).

## L'Identità Digitale: l'accesso sicuro alle risorse

Si costruisce definendo, per l'utente della rete, un profilo di autorizzazione all'accesso delle risorse. Non solo, proteggendo le credenziali che lo identificano con strumenti che superano lo schema della password segreta (fattore singolo di autenticazione) e introducendone uno più avanzato che implica un doppio fattore: conoscere il segreto (password o pin) e possedere lo strumento che protegge la credenziale.

## Le Soluzioni

Le smart card e i token USB SafeNet sono device che memorizzano in maniera sicura le credenziali utente, siano esse password, chiavi crittografiche, certificati o biometriche. Permettono operazioni di autenticazione e funzioni crittografiche, come la firma digitale, utilizzando le credenziali su di essi memorizzate. Sono integrabili sia in ambienti PKI oriented, sia in infrastrutture che non utilizzano certificati digitali come credenziali.

- **SafeNet Token USB iKey**

Tre sono i modelli:

**iKey 1000:** token non-PKI oriented. Non fa uso di certificati digitali, ma permette la memorizzazione di credenziali per l'autenticazione su applicazioni custom attraverso l'integrazione di queste ultime con l'SDK fornito con il device.

**iKey 2032:** token PKI based, compatibile con gli ambienti Windows e Mac OSX e certificato FIPS 140-1 Level 2. E'integrabile in operazioni di sign-on/smartcard logon, VPN authentication, e-mail encryption, firma digitale e applicazioni custom PKI based e non.

certificazioni FIPS 140-1 Level 3 e Common Criteria EAL 4+. Oltre a supportare le operazioni della iKey 2032, permette la creazione di piccole applicazioni custom (C/C++ e Java) eseguibili direttamente sul token, per impedire tentativi di reverse engineering del codice.

- **SafeNet Smart card 400**

È progettata per le certificazioni di sicurezza FIPS 201, 140-2 Level 2 e Common Criteria EAL 4+. Offre la protezione delle credenziali con 2 o 3 fattori di autenticazione, permettendo di abbinare alla conoscenza del segreto e possesso di un oggetto di autenticazione anche un terzo elemento: la credenziale biometrica.

In più gestisce tutte le funzionalità supportate dalle iKey 2032 e 4000.

