Sicurezza dei dati semplice, completa e flessibile per l'intera organizzazione

Dell Encryption

Oggi, le organizzazioni devono proteggere sia gli endpoint sia i dati al loro interno, supportando al contempo la mobilità della forza lavoro. Le soluzioni per la crittografia di tipo tradizionale sono limitate e impongono delle restrizioni in termini di installazione, livello di copertura degli endpoint e prestazioni degli utenti. Le soluzioni di crittografia tradizionali cercano di soddisfare queste esigenze, ma la maggior parte è difficile da installare e gestire, non copre tutti gli endpoint e peggiora le prestazioni per gli utenti.

Con la flessibilità della sua tecnologia di crittografia, per proteggere i dati Dell Encryption Enterprise offre opzioni come la tecnologia Full Disk Encryption e un approccio basato su policy orientate ai dati. La soluzione è pensata per offrire:

- Deployment semplificato

- Trasparenza per gli utenti finali

- Conformità senza problemi

- Facilità di gestione con una singola console

Dell Encryption è una flessibile suite di soluzioni avanzate per la sicurezza che includono la crittografia basata su file, la tecnologia Full Disk Encryption, una migliore gestione centralizzata della crittografia nativa (Microsoft BitLocker e Mac FireVault) e la protezione dei dati memorizzati su supporti esterni, unità con crittografia automatica e dispositivi mobili.

Dell Encryption Enterprise

Con Dell Encryption Enterprise, il personale di IT può applicare facilmente le policy di crittografia per i dati presenti sia nell'unità di sistema che su supporti esterni, senza necessità di alcun intervento da parte degli utenti finali.

Soluzione perfetta per ambienti caratterizzati da prodotti di fornitori diversi, Encryption Enterprise assicura:

- Deployment e provisioning automatici quando preinstallato sui dispositivi commerciali di Dell;
- Installazione in meno di 30 minuti negli ambienti VMware, grazie alla procedura di installazione guidata e alla gestione di chiavi e database completamente integrata;
- Nessuna necessità di eseguire la deframmentazione prima della crittografia;
- Crittografia del disco di sistema e dei supporti esterni in un'unica soluzione;
- Possibilità di scegliere tra Full Disk Encryption e File Based Encryption;
- Facilità di gestione e controllo della conformità con modelli rapidi per la conformità delle policy, gestione remota e ripristino rapido del sistema;
- Integrazione con i processi esistenti per l'autenticazione, l'installazione delle patch e altro ancora;
- Centralizzazione della vendita e del supporto per l'hardware e le soluzioni di sicurezza;
- Crittografia di tutti i dati, eccetto i file essenziali all'avvio del sistema operativo, o crittografia del disco completo con Full Disk Encryption, a seconda delle preferenze;
- Sistema avanzato di controllo delle porte per prevenire la perdita di dati;
- Capacità di eseguire la crittografia in base a profili, dati e gruppi degli utenti finali all'interno dell'organizzazione;
- Gestione centralizzata di tutte le policy di crittografia, incluse self-encrypting drive, Full Disk Encryption e la crittografia Microsoft BitLocker;
- Migliore autenticazione per dispositivi conformi agli standard OPAL, tra cui single sign-on del sistema operativo con autenticazione in fase di preavvio tramite smart card e password.

Il vantaggio di Dell Encryption

Protezione completa con un livello di sicurezza elevato

- Protezione dei dati su qualsiasi dispositivo e supporto esterno
- Master Boot Record (MBR) e chiavi non sono mai esposti a rischi

Produttività e semplicità per il reparto di IT e gli utenti finali

- Installazione semplificata con Security Management Server Virtual o scalabilità per migliaia di utenti con Security Management Server
- Perfetta integrazione con i processi esistenti di gestione e autenticazione dei sistemi
- Crittografia trasparente per gli utenti finali, progettata per migliorare la loro produttività

Crittografia flessibile

- Basata su profilo dell'utente finale, riservatezza dei dati, prestazioni o esigenze di conformità
- Crittografia dei dati su supporti esterni o disattivazione delle porte, senza impedire il funzionamento dei dispositivi non di storage
- Gestione e controllo di Microsoft BitLocker e dei dischi a crittografia automatica per aiutare ad assicurare l'adempienza

Dell Security Management Server Virtual

Utilizzando un apposito server di gestione virtuale e un'app di console per VMware, Dell ha reso ancora più semplice e veloce rendere operativa la nostra soluzione di crittografia degli endpoint nella maggior parte degli ambienti aziendali di grandi dimensioni con fino a 3.500 endpoint.

Con Dell Security Management Server Virtual, la soluzione per la crittografia Dell Encryption è la scelta perfetta per le piccole e medie imprese che possiedono già soluzioni di VMware e sono alla ricerca di una piattaforma di gestione semplice e veloce da installare per le proprie policy di crittografia e autenticazione. Questo prodotto offre tutte le funzioni e i vantaggi di un server standard, incluso il supporto completo per la massima copertura di crittografia disponibile per notebook, desktop e supporti esterni.

Gestione delle unità con crittografia automatica con Dell Encryption Enterprise

Le organizzazioni che utilizzano i dischi a crittografia automatica necessitano anche di una gestione attenta per ridurre in modo efficace i rischi di perdita dei dati e per soddisfare gli obiettivi di controllo e di conformità.

Dell Encryption Enterprise consente di gestire in modo sicuro e centralizzato le unità con crittografia automatica di tutta l'organizzazione, sia in locale che da remoto. Tutte le attività riguardanti policy, autenticazione e gestione, archiviazione e recupero delle chiavi di crittografia sono disponibili da un'unica console. Ciò consente di ridurre il numero delle operazioni necessarie per proteggere i dati critici, insieme al rischio di mancata protezione dei sistemi in caso di smarrimento o di accesso non autorizzato. Soprattutto, la gestione dei dispositivi standard OPAL è completamente integrata nella stessa piattaforma di protezione dei dati, come la crittografia basata su file, Microsoft BitLocker e la crittografia dei supporti rimovibili.

Le funzioni di gestione remota permettono tra l'altro di:

- Disabilitare gli accessi e svuotare la cache dell'utente per proteggere i dati e garantire che solo gli amministratori autorizzati possano abilitare nuovamente l'accesso ai dati protetti;
- Disabilitare il dispositivo per evitare a qualsiasi utente di accedere al sistema finché non viene inviato un comando di sblocco;
- Abilitare il dispositivo in modo che gli utenti possano effettuare l'accesso per utilizzare l'unità SED;
- Eseguire un comando di sblocco del disco automatico e da remoto, permettendo agli amministratori di eseguire le attività essenziali, come l'applicazione di patch, senza dover lasciare il dispositivo sbloccato durante la notte;
- Impostare l'autenticazione preavvio completa, tra cui l'autenticazione tramite Active Directory;
- Impostare le policy di risposta automatica agli attacchi (compresi gli attacchi di forza bruta).

Gestione della crittografia Full Disk Encryption con Dell Encryption Enterprise

Le organizzazioni che utilizzano la crittografia Full-Disk Encryption possono assicurare la protezione continua dei dati sensibili memorizzati su PC e altri endpoint. Ultima novità di Dell Enterprise Encryption, la crittografia Full-Disk Encryption permette di soddisfare efficacemente ogni esigenza di protezione dei dati. Infatti, la crittografia Full Disk Encryption:

- Va a completare la nostra soluzione per la crittografia, che così si inserisce tra le più efficaci del settore;
- Fornisce un'autenticazione in fase di preavvio di livello enterprise per il deployment negli ambienti delle grandi imprese;
- Utilizza la tecnologia TPM per proteggere le chiavi, impedendo agli autori degli attacchi di rimuovere il disco rigido dalla piattaforma e di attaccare offline le chiavi offuscate memorizzate nell'unità;
- Esegue la crittografia di tutti i dischi rigidi locali in un framework semplificato di deployment e gestione remota;
- Full Disk Encryption offre anche una semplice tecnologia di crittografia che può essere abilitata e gestita con un impiego minimo di personale;
- Offre agli utenti un'esperienza trasparente e ad alte prestazioni;

- Con l'autenticazione in fase di preavvio di classe enterprise, Full Disk Encryption offre:
  - Single Sign-on per sistema operativo e rete
  - Client singolo, supporto multi-utente
  - Ripristino semplificato da parte dell'amministratore delle chiavi di crittografia e dell'accesso ai dati

Nota: La funzionalità Dell Full Disk Encryption è attualmente supportata sui PC commerciali Dell (X7 e successivi) in modalità di avvio UEFI con fattore di autenticazione della password. I PC non Dell e la modalità di avvio legacy con autenticazione tramite smart card saranno supportati nelle versioni successive.

Caratteristiche e vantaggi di Dell Encryption

Deployment e gestione semplificati

Poiché l'ideale è disporre di una soluzione facile da implementare e gestire senza interferire con i processi IT esistenti, Dell Encryption consente di:

- Eeseguire automaticamente il deployment e il provisioning quando la soluzione Dell Encryption è preinstallata su determinati dispositivi commerciali Dell;
- Installare la soluzione in meno di 30 minuti[1] negli ambienti VMware con gestione di chiavi e database completamente integrata, a differenza delle soluzioni dei concorrenti che in genere richiedono più server, un database distinto e più licenze;
- Eseguire l'installazione senza procedure dispendiose in termini di tempo, installazioni complete e deframmentazioni dell'intero disco;
- Eliminare ogni preoccupazione riguardo ai processi IT preesistenti, grazie a una soluzione pronta all'uso che non richiede operazioni di configurazione;
- Integrare la soluzione nei processi di autenticazione esistenti, tra cui password Windows, RSA, impronte digitali e smart card;
- Correggere, proteggere, controllare (rilevare rapidamente i dispositivi, applicare la crittografia e verificarla);
- Crittografare i file o i dati riservati degli utenti anche quando l'IT deve accedere all'endpoint;
- La gestione dei dispositivi standard OPAL è completamente integrata in un'unica console per tutti gli endpoint;
- proteggere gli endpoint negli ambienti eterogenei a prescindere da utente, dispositivo o posizione.

Conformità più semplice

Dell Encryption fornisce modelli di policy preimpostati per consentire ai clienti di adeguarsi alle normative in materia di conformità tra cui:

- Normative del settore: PCI DSS, Sarbanes Oxley (SOX)
- Normative federali e statali statunitensi: HIPAA e HITECH Act, Gramm Leach Bliley Act (California), SB1386 (Massachusetts), 201 CMR 17 (Nevada), NRS 603A (che richiede lo standard PCI DSS) e altre 45 leggi (e più) di competenza dei singoli Stati e del governo federale;
- Normative internazionali: come la certificazione “Safe Harbor” tra Stati Uniti ed Europa, la Direttiva 95/46/EC dell'Unione Europea in materia di tutela dei dati, il Data Protection Act (Regno Unito), la BDSG (Bundes-daten-schutz-gesetz, Germania) e leggi analoghe in vigore per tutti i Paesi dell'Unione Europea e il Canada - PIPEDA.

Specifiche tecniche

Dell Encryption Enterprise è disponibile per gli ambienti caratterizzati da prodotti di diversi fornitori che presentano le specifiche indicate di seguito.

Sistemi operativi client supportati:

- Microsoft Windows 7 Ultimate, Enterprise e Professional Edition
- Microsoft Windows 8 e 8.1 Enterprise e Professional Edition
- Microsoft Windows 10 Education, Enterprise e Pro Edition
- MacOS X El Capitan, Sierra

Dell Security Management Server è stato collaudato nei seguenti ambienti operativi:

- Windows Server 2008 R2 SP0-SP1 a 64 bit Standard ed Enterprise Edition
- Windows Server 2012 R2 Standard e Datacenter Edition
- Windows Server 2016 Standard e Datacenter Edition
- VMware ESXi 5.5, 6.0 e 6.5
- VMware Workstation 11 e 12.5

L'accesso alla console di gestione remota e a Compliance Reporter è supportato tramite i seguenti browser Internet:

- Internet Explorer 11.x o versione successiva
- Mozilla Firefox 41.x o versione successiva
- Google Chrome 46.x o versione successiva

Produttività dell'utente finale

Dell è cosciente dell'importanza di poter lavorare al massimo livello di capacità, senza interruzioni o ritardi. Ecco perché la soluzione viene installata in modo trasparente, contribuendo ad azzerare le interruzioni in fase di crittografia dei dispositivi. Addirittura, trattandosi di una tecnologia così discreta, gli utenti potrebbero non accorgersi nemmeno che i dispositivi sono stati crittografati.

Deployment Services

I nostri esperti si occuperanno dell'implementazione della soluzione. La nostra offerta include una linea completa di servizi per l'installazione di soluzioni di sicurezza nel tuo ambiente. Per prima cosa, il nostro team di esperti in materia di sicurezza informatica eseguirà una valutazione del tuo ambiente per individuare le aree in cui migliorare la sicurezza dei dati sugli endpoint, sui server, nel cloud e sui dispositivi mobili. Dopodiché, provvederemo a implementare, ottimizzare e gestire la soluzione che fa al caso tuo.

Ampia protezione crittografica

Affidati a Dell Encryption per salvaguardare i dati di valore memorizzati su qualsiasi dispositivo, supporto esterno e nel cloud pubblico, senza compromettere la produttività. Ancora una volta Dell offre la potenza per fare di più. Ulteriori informazioni sono disponibili all'indirizzo Dell.com/DataSecurity.