KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Tecnologia di crittografia

La crittografia previene l'accesso non autorizzato ai dati in caso di perdita del dispositivo, furto o attacco malware finalizzato al furto di dati.

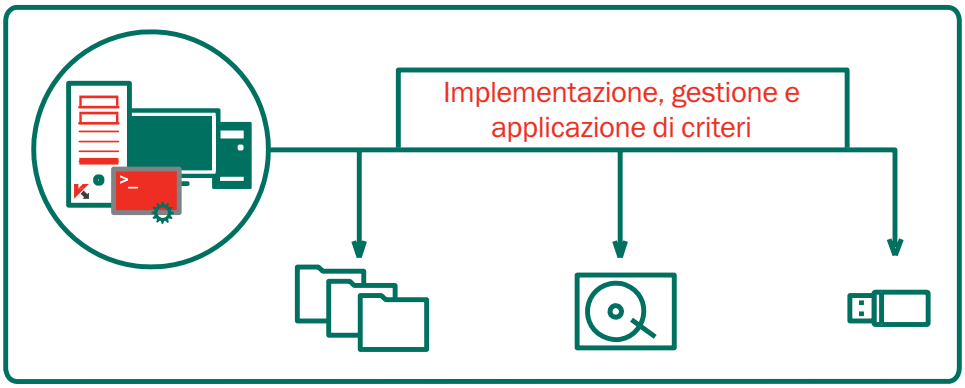
La protezione proattiva e la conformità dei dati sono imperativi assoluti. La tecnologia di crittografia di Kaspersky Lab consente di proteggere i dati importanti dal rischio di perdite accidentali dovute a smarrimento o furto dei dispositivi e ad attacchi malware mirati. La soluzione coniuga una potente tecnologia di crittografia con le tecnologie di protezione degli endpoint leader del settore di Kaspersky Lab; questa piattaforma integrata protegge i dati quando si è in movimento e non.

Dal momento che si tratta di una soluzione Kaspersky Lab, può essere facilmente implementata e amministrata da una console di gestione centralizzata tramite l'uso di un unico criterio.

Scegli la tecnologia di crittografia di Kaspersky Lab per prevenire la perdita di dati e l'accesso non autorizzato:

- Disco intero
- File e cartelle
- Dispositivi rimovibili e interni

AMMINISTRATIDAUN'UNICA CONSOLE DI GESTIONE



CRITTOGRAFIA SICURA DI USO CONSOLIDATO NEL SETTORE

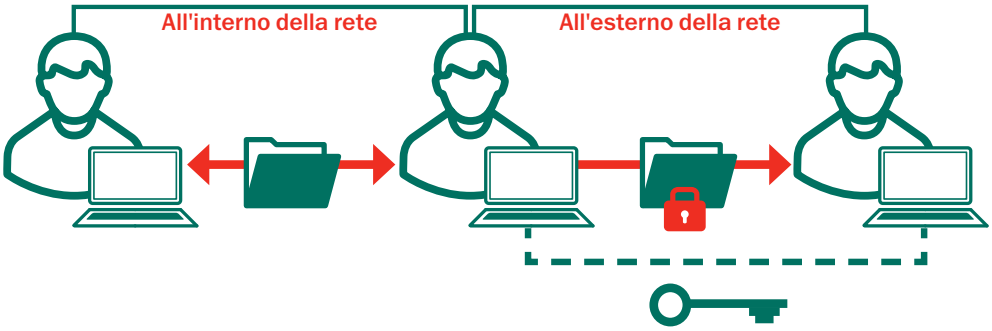
Kaspersky Lab utilizza lo standard AES con chiave a 256 bit, gestione semplificata delle chiavi. Supporta la tecnologia Intel® AES-NI, le piattaforme UEFI e GPT.

FLESSIBILITÀ TOTALE

Kaspersky Lab offre la crittografia di file e cartelle (FLE) e quella dell'intero disco (FDE), coprendo tutti i possibili scenari d'uso. I dati possono essere protetti sia su dischi rigidi sia su dispositivi rimovibili. La "modalità portatile" consente l'utilizzo e il trasferimento dei dati su supporti rimovibili crittografati, persino su computer privi di un software di crittografia, facilitando lo scambio di dati protetto "fuori perimetro".

SINGLE SIGN-ON, TRASPARENZA PER GLI UTENTI FINALI

Dall'impostazione all'uso quotidiano, la tecnologia di crittografia di Kaspersky Lab funziona in modo trasparente su tutte le applicazioni, senza compromettere la produttività degli utenti finali. La funzione Single sign-on garantisce la crittografia senza problemi: l'utente finale potrebbe non accorgersi del fatto che la tecnologia sia in esecuzione.



La crittografia di Kaspersky Lab consente di trasferire i file in modo agevole e trasparente tra gli utenti all'interno e all'esterno della rete.

FUNZIONALITÀ DI CRITTOGRAFIA

INTEGRAZIONE TOTALE CON LE TECNOLOGIE DI SICUREZZA DI KASPERSKY LAB

Integrazione completa con le tecnologie anti-malware, dei controlli e della gestione degli endpoint, per una autentica sicurezza multilivello costruita su una codebase comune. Ad esempio, un unico criterio potrebbe applicare la crittografia a particolari dispositivi rimovibili. È possibile applicare le impostazioni di crittografia secondo lo stesso criterio degli elementi anti-malware, di controllo dei dispositivi e di sicurezza degli endpoint. Non è necessario distribuire e gestire soluzioni separate. La compatibilità hardware di rete viene automaticamente verificata prima dell'implementazione della crittografia; il supporto per le piattaforme UEFI e GPT è standard.

CONTROLLO DELL'ACCESSO IN BASE AL RUOLO

Nelle organizzazioni più grandi, si può scegliere di delegare la gestione della crittografia usando la funzionalità di controllo degli accessi in base ai ruoli. Questo consente una gestione della crittografia meno complessa.

Modalità di acquisto

La tecnologia di crittografia di Kaspersky non viene venduta separatamente, ma risulta abilitata per i livelli "Advanced" e "Total" di Kaspersky Endpoint Security for Business come componente di una piattaforma per la sicurezza completa

AUTENTICAZIONE PRE-AVVIO (PBA)

Le credenziali utente sono richieste ancora prima dell'avvio del sistema operativo, fornendo un livello aggiuntivo di sicurezza con single sign-on opzionale. L'autenticazione pre-avvio della tecnologia di crittografia di Kaspersky Lab è disponibile anche per le tastiere non QWERTY.

AUTENTICAZIONE CON SMARTCARD E TOKEN

Supporta l'autenticazione a due fattori tramite marche popolari di smartcard e token, eliminando la necessità di nomi utente e password aggiuntive e migliorando l'esperienza dell'utente.

RIPRISTINO DI EMERGENZA

Gli amministratori possono decrittografare i dati nel caso di guasto hardware o software. Il recupero della password utente per autenticazione pre-avvio o accesso ai dati crittografati viene implementato tramite un semplice meccanismo di challenge e response.

IMPOSTAZIONI OTTIMIZZATE E PERSONALIZZABILI DI DISTRIBUZIONE

Per facilità di distribuzione, la funzionalità di crittografia di Kaspersky Lab è abilitata nei livelli "Advanced" e "Total" di Kaspersky Endpoint Security for Business e non necessita di installazione separata. Le impostazioni di crittografia sono predefinite ma personalizzabili per cartelle di uso comune quali Documenti e Desktop, nuove cartelle, estensioni di file e gruppi di estensioni di file (quali documenti Microsoft Office o archivi di messaggi e-mail).

Kaspersky Endpoint Security for Business/Encryption/

KASPERSKY lab