

► KASPERSKY ENDPOINT SECURITY PER LE AZIENDE

Tecnologia di crittografia

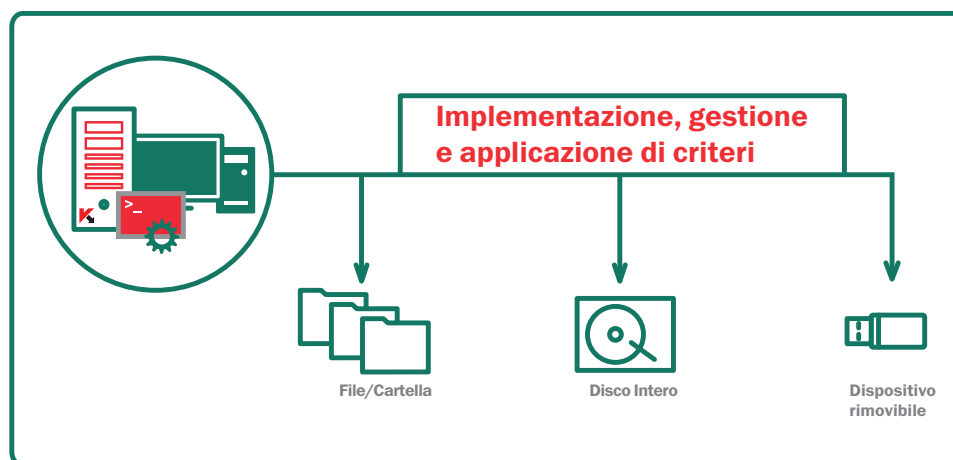
La crittografia previene l'accesso non autorizzato ai dati in caso di perdita accidentale di supporti o di un PC.

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. La soluzione coniuga una potente crittografia integrata con le tecnologie di protezione degli endpoint leader del settore di Kaspersky. Dal momento che si tratta di una soluzione Kaspersky, 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 per proteggere i tuoi dati in modo semplice:

- DISCO INTERO
- LIVELLO FILE E CARTELLE
- DISPOSITIVI RIMOVIBILI E INTERNI

AMMINISTRATI DA UN'UNICA CONSOLE DI GESTIONE.



CRITTOGRAFIA SICURA DI USO CONSOLIDATO NEL SETTORE

Kaspersky utilizza un algoritmo di crittografia AES con chiave a 256 bit.

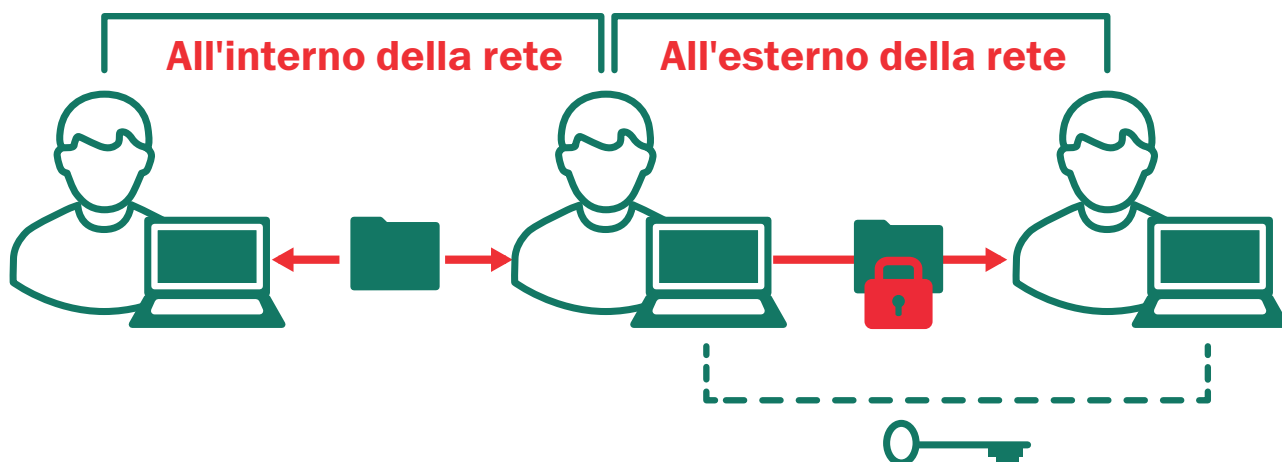
FLESSIBILITÀ NELLA SCELTA DEL METODO DI CRITTOGRAFIA

Per coprire tutti i possibili scenari di utilizzo, è disponibile qualsiasi combinazione di metodi di crittografia a livello di file e cartelle (FLE) e di disco intero (FDE) per la protezione dei dati presenti su dischi rigidi e dispositivi rimovibili.

TRASPARENZA PER GLI UTENTI FINALI

La tecnologia di crittografia di Kaspersky Lab garantisce una trasparenza costante per tutte le applicazioni, anche nella fase di configurazione. Offrendo una protezione immediata delle informazioni, non compromette minimamente la produttività degli utenti finali. Un punto di accesso singolo al sistema crittografato offre agli utenti un maggiore livello di trasparenza.

Durante un trasferimento di file, la crittografia di Kaspersky risulta intuitiva e trasparente per l'utente all'interno della rete. I dati destinati agli utenti esterni possono essere raccolti in speciali contenitori protetti tramite una password, che può essere inviata al destinatario per essere crittografata attraverso un canale separato.



FUNZIONALITÀ DI CRITTOGRAFIA:

CODEBASE INTEGRATA

Dal momento che tutte le funzioni che forniscono una protezione multilivello risultano integrate in un'unica applicazione software, non è necessario implementare e gestire molteplici soluzioni per applicare la protezione anti-malware, i controlli degli endpoint e la crittografia.

CRITERI INTEGRATI E INTERCONNESSI

La codebase integrata consente all'amministratore di creare criteri unici. Ad esempio: l'IT può definire che solo i supporti rimovibili approvati possano essere collegati ad un dispositivo e applicare anche un criterio di crittografia sullo stesso dispositivo (combinando criteri per il controllo dei dispositivi e tecnologie di crittografia).

IMPOSTAZIONI PRECONFIGURATE PERSONALIZZABILI

Le impostazioni di crittografia risultano predefinite (ma anche 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, archivi di messaggi e-mail).

CHIAVE CENTRALIZZATA DI EMERGENZA PER L'AMMINISTRATORE

L'amministratore della sicurezza può decrittografare i dati presenti sulle unità in caso di errore hardware o software.

RIPRISTINO DELLA PASSWORD UTENTE

Consente all'utente di ripristinare la password precedente all'avvio o di accedere a dati crittografati mediante un meccanismo di richiesta di verifica/risposta.

Modalità di acquisto

La tecnologia di crittografia di Kaspersky non è venduta separatamente, ma risulta abilitata per i seguenti livelli della soluzione **Kaspersky Security per le aziende**:

- Endpoint Security, Advanced
- Kaspersky Total Security per le aziende

QUESTE FUNZIONALITÀ NON SONO TUTTE DISPONIBILI SU TUTTE LE PIATTAFORME. Per informazioni dettagliate, consulta il sito Web www.kaspersky.com