

# ► KASPERSKY ENDPOINT SECURITY PER LE AZIENDE Advanced

La ricca gamma di soluzioni di Kaspersky Lab offre un'ampia serie di strumenti di sicurezza e funzionalità per l'ottimizzazione dell'IT.

Il livello Advanced di Kaspersky garantisce la soluzione di protezione e gestione necessaria alla tua organizzazione per applicare criteri di sicurezza IT, proteggere gli utenti dalle minacce malware e dal rischio di perdita accidentale dei dati e migliorare l'efficienza delle risorse IT.

## Le funzionalità di protezione e gestione di cui hai bisogno.

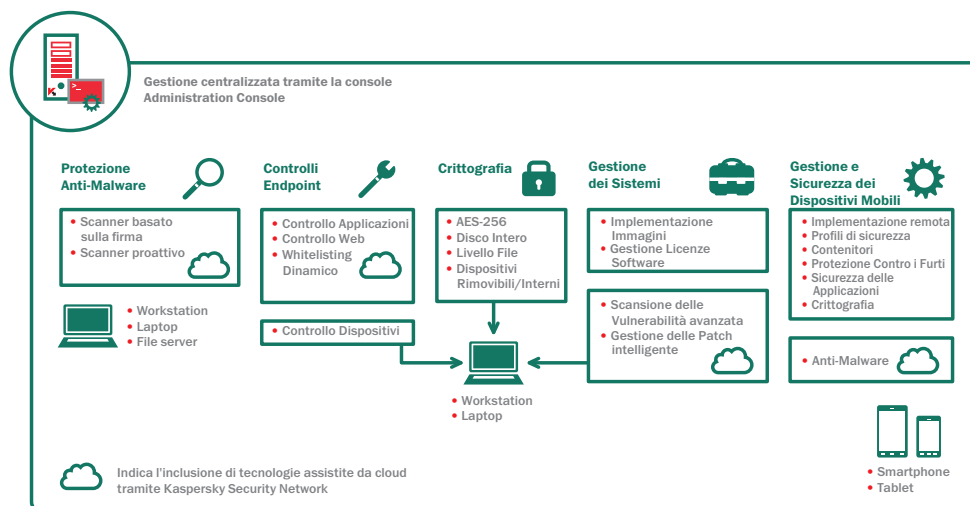
Kaspersky ha integrato avanzate funzionalità di classe enterprise nei livelli progressivi delle sue offerte, riuscendo al contempo a fornire una tecnologia estremamente semplice da utilizzare e pertanto adatta ad aziende di qualsiasi dimensione.

## Qual è il livello adatto a te?

- CORE
- SELECT
- **ADVANCED**
- TOTAL

### TRA QUESTE FUNZIONALITÀ SONO INCLUSE:

- ANTI-MALWARE
- FIREWALL
- PROTEZIONE ASSISTITA DA CLOUD TRAMITE KASPERSKY SECURITY NETWORK
- CONTROLLO APPLICAZIONI
- WHITELIST APPLICAZIONI
- CONTROLLO WEB
- CONTROLLO DISPOSITIVI
- PROTEZIONE FILE SERVER
- MOBILE DEVICE MANAGEMENT (MDM)
- SICUREZZA ENDPOINT MOBILI (PER TABLET E SMARTPHONE)
- CRITTOGRAFIA
- CONFIGURAZIONE E IMPLEMENTAZIONE SISTEMI
- CONTROLLO ACCESSI ALLA RETE
- SCANSIONE DELLE VULNERABILITÀ AVANZATA
- GESTIONE DELLE PATCH



## ► L'UNICA PIATTAFORMA DI SICUREZZA REALMENTE EFFICACE DEL SETTORE.

### Unica console di gestione

L'amministratore può avvalersi di una posizione centralizzata per visualizzare e gestire l'intero scenario di sicurezza: macchine virtuali e dispositivi fisici e mobili.

### Unica piattaforma di sicurezza

Kaspersky Lab ha scelto di sviluppare internamente console, moduli e strumenti di sicurezza anziché acquistarli da altre aziende. Ciò ha consentito ai programmatori di utilizzare la medesima codebase per sviluppare tecnologie perfettamente integrabili e interoperabili, in modo da poter garantire stabilità, criteri integrati, reporting efficiente e strumenti intuitivi.

### Unico costo

Tutti gli strumenti vengono offerti da un fornitore singolo in un'unica installazione, evitandoti l'onere di ripetere il processo di budgeting e giustificazione per garantire all'organizzazione un livello di protezione adeguato agli obiettivi aziendali.

## CRITTOGRAFIA E PROTEZIONE DEI DATI:

### CRITTOGRAFIA COMPLETA

Hai la possibilità di scegliere tra una crittografia del disco intero o a livello di file, con il supporto dell'algoritmo AES (Advanced Encryption Standard) a 256 bit, per garantire la protezione delle informazioni aziendali di importanza cruciale in caso di furto o perdita del dispositivo.

### SUPPORTO DI DISPOSITIVI RIMOVIBILI

Migliora la tua sicurezza tramite criteri che consentono l'applicazione della crittografia dei dati su dispositivi rimovibili.

### CONDIVISIONE SICURA DEI DATI

Gli utenti possono facilmente creare pacchetti crittografati e autoestraenti per garantire la protezione dei dati durante la condivisione tramite dispositivi rimovibili, e-mail, rete o Web.

### TRASPARENZA PER GLI UTENTI FINALI

La soluzione di crittografia di Kaspersky risulta intuitiva e invisibile per gli utenti e non genera ripercussioni né sulla produttività né sulle impostazioni o sugli aggiornamenti delle applicazioni.

## CONTROLLI DEGLI ENDPOINT:

### CONTROLLO APPLICAZIONI

Consente agli amministratori IT di impostare criteri tesi a consentire, bloccare o regolare applicazioni (o categorie di applicazioni).

### CONTROLLO DISPOSITIVI

Consente agli utenti di impostare, pianificare e applicare criteri per i dati con un dispositivo di archiviazione rimovibile e altri controlli dei dispositivi periferici, collegati all'USB o ad altri tipi di bus.

### CONTROLLO WEB

Consente di associare i controlli della navigazione basati su endpoint all'utente, sia all'interno della rete aziendale che durante gli spostamenti.

### WHITELISTING DINAMICO

Le reputazioni di file in tempo reale fornite da Kaspersky Security Network consentono di proteggere le tue applicazioni approvate dal rischio di minacce malware, ottimizzando al tempo stesso la produttività degli utenti.

## FUNZIONALITÀ DI PROTEZIONE DEGLI ENDPOINT:

### AVANZATA TECNOLOGIA ANTI-MALWARE DEGLI ENDPOINT

Metodi tradizionali basati sulla firma, proattivi e basati su cloud, di uso consolidato nel settore, per il rilevamento delle minacce malware.

### PROTEZIONE ASSISTITA DA CLOUD

Kaspersky Security Network (KSN) consente di rispondere alle minacce sospette in tempi estremamente più rapidi rispetto ai metodi di protezione tradizionali. KSN assicura tempi di risposta alle minacce malware di appena 0,02 secondi!

## CONFIGURAZIONE DEI SISTEMI E GESTIONE DELLE PATCH:

### GESTIONE DELLE PATCH

Un'avanzata funzionalità di scansione delle vulnerabilità si unisce alla distribuzione automatica delle patch.

### IMPLEMENTAZIONE REMOTA DEL SOFTWARE

Implementazione centralizzata del software su macchine client, anche presso gli uffici remoti.

### CONTROLLO DEGLI ACCESSI ALLA RETE (NAC)

Il Controllo Accessi alla Rete (NAC - Network Admission Control) consente di creare criteri per i dispositivi "ospiti" della rete. I dispositivi ospiti (compresi i dispositivi mobili) vengono riconosciuti automaticamente e inviati a un portale aziendale, nel quale, con la password corretta, possono utilizzare le risorse precedentemente approvate.

### IMPLEMENTAZIONE DELLE IMMAGINI DI SISTEMA OPERATIVO E APPLICAZIONI

Creazione, archiviazione e implementazione semplificate delle immagini del sistema da una posizione centralizzata. La soluzione ideale per la migrazione a Microsoft® Windows® 8.

### GESTIONE DI HARDWARE, SOFTWARE E LICENZE

I report degli inventari software e hardware consentono di controllare gli obblighi relativi alle licenze software, garantendoti risparmi attraverso un provisioning centralizzato dei diritti software.

## FUNZIONALITÀ DI SICUREZZA MOBILE:

### INNOVATIVE TECNOLOGIE ANTI-MALWARE

Combinazione dei risultati ottenuti con il rilevamento proattivo basato sulla firma e assistito da cloud in una funzionalità di protezione in tempo reale. Un browser protetto, una funzione anti-spam e una sandbox delle applicazioni migliorano la sicurezza dell'ambiente.

### IMPLEMENTAZIONE CON PROVISIONING IN MODALITÀ OTA (OVER-THE-AIR).

Preconfigurazione e implementazione delle applicazioni in maniera centralizzata tramite l'uso di SMS, e-mail e PC.

### STRUMENTI DI PROTEZIONE REMOTA CONTRO I FURTI

SIM Watch, Blocco Remoto (Remote Lock), Cancellazione (Wipe) e Localizzazione (Find) sono funzionalità in grado di impedire l'accesso non autorizzato ai dati aziendali in caso di perdita o furto di un dispositivo mobile.

### CONTROLLO DELLE APPLICAZIONI PER I DISPOSITIVI MOBILI

Garantisce il monitoraggio delle applicazioni installate su un dispositivo mobile in base ai criteri di gruppo predefiniti. Include un gruppo di "applicazioni obbligatorie".

### SUPPORTO DEI DISPOSITIVI PERSONALI DEI DIPENDENTI

Iniziativa BYOD? I dati e le applicazioni aziendali sono isolati in contenitori crittografati trasparenti per gli utenti. Tali dati possono essere eliminati separatamente.

**QUESTE FUNZIONALITÀ NON SONO TUTTE DISPONIBILI SU TUTTE LE PIATTAFORME.** Per informazioni dettagliate, consulta il sito Web [www.kaspersky.com](http://www.kaspersky.com)