

# ► KASPERSKY ENDPOINT SECURITY PER LE AZIENDE

## Controlli Endpoint

Kaspersky offre un prezioso connubio tra potenti strumenti di controllo degli endpoint e avanzata tecnologia anti-malware per garantire alla tua azienda un livello superiore di prevenzione delle minacce emergenti.

### CONTROLLO APPLICAZIONI E WHITELISTING DINAMICO

La funzionalità **Controllo Applicazioni** (Application Control) di Kaspersky unita alla tecnologia Whitelisting Dinamico (Dynamic Whitelisting) ottimizza l'approccio di sicurezza delle aziende consentendo agli amministratori IT di impostare criteri tesi a consentire, bloccare o regolare applicazioni (o categorie di applicazioni).

Grazie all'uso di queste tecnologie, le organizzazioni possono implementare senza alcuna difficoltà un criterio di sicurezza "Nega Predefinito" (Default Deny). In un contesto di questo tipo, tutte le applicazioni vengono bloccate in maniera predefinita, ma l'amministratore ha la possibilità di definire un elenco di applicazioni di cui viene consentita l'esecuzione. Kaspersky semplifica l'attività dell'amministratore raggruppando in categorie centinaia di milioni di applicazioni al fine di agevolare la creazione di criteri. L'amministratore può quindi scegliere di creare il database delle applicazioni consentite a livello locale oppure avvalersi delle categorie predefinite da Kaspersky Lab.

Uno dei moduli di questa tecnologia è **Controllo Privilegi Applicazioni** (Application Privilege Control), che consente di analizzare e controllare costantemente il comportamento delle applicazioni. Kaspersky può definire delle limitazioni per un'applicazione, quali l'autorizzazione a scrivere nei registri, le risorse a cui può accedere (ad esempio, risorse di archiviazione), i dati degli utenti che può controllare e modificare e così via.

Infine, Kaspersky gestisce un database di **whitelist** dedicato contenente programmi sottoposti a regolari monitoraggi finalizzati a verificarne la legittimità. Di fatto, siamo l'unica azienda del settore delle soluzioni di sicurezza che dispone di un laboratorio di whitelist con un proprio team dedicato di esperti!

### CONTROLLO WEB

Esistono numerosi siti Web contenenti materiali non adatti al luogo di lavoro. Per questi e molti altri motivi, è fondamentale utilizzare controlli Web avanzati.

Kaspersky gestisce una directory costantemente aggiornata di siti Web raggruppati in categorie (per il gioco d'azzardo, per adulti, di ricerca e così via). Gli amministratori possono creare facilmente criteri per la navigazione sulla base di queste categorie oppure personalizzarle per creare elenchi personalizzati. L'accesso ai siti dannosi viene automaticamente negato.

È possibile impostare dei criteri in base ad una pianificazione per consentire la navigazione in determinate ore del giorno e, dal momento che la funzione Controllo Web (Web Control) di Kaspersky ti garantisce l'integrazione con la tua struttura Active Directory esistente, i criteri possono essere applicati in maniera semplice e rapida a livello dell'intera organizzazione.

L'innovativo approccio di Kaspersky consente di abilitare questa tecnologia direttamente presso l'endpoint, garantendo l'applicazione degli eventuali criteri creati anche se l'utente non si trova nella rete.

## CONTROLLO DISPOSITIVI

La disabilitazione di una porta USB non ti permette sempre di risolvere i problemi dei tuoi dispositivi rimovibili. Spesso è richiesto un livello di controllo più granulare per migliorare la produttività e la sicurezza degli utenti. Ad esempio, se un utente deve connettere un token VPN USB per accedere alla rete (ma non nel caso in cui connetta dispositivi di archiviazione rimovibili), un criterio di "disabilitazione della porta USB" non risulterà efficace.

Kaspersky consente all'amministratore di impostare criteri e di controllare i dispositivi collegati su qualsiasi bus di connessione (non solo USB) nel momento desiderato. Pertanto, l'amministratore può definire i dispositivi che possono essere collegati e autorizzati ad operazioni di lettura o scrittura, l'ora del giorno in cui verrà applicato un criterio e i tipi di dispositivi consentiti. Per garantire la massima sicurezza, questi controlli possono essere applicati anche al numero di serie specifico di un dispositivo.

## AMMINISTRAZIONE SEMPLIFICATA

Dal momento che Kaspersky offre soluzioni specifiche per gli amministratori, tutti i controlli risultano integrabili con Active Directory ed è possibile definire criteri di copertura con estrema semplicità e velocità. Tutti questi controlli degli endpoint vengono gestiti dalla stessa console e, di conseguenza, l'amministratore ha la possibilità di utilizzare un'unica interfaccia intuitiva senza l'esigenza di una formazione extra.

### Modalità di acquisto

Gli **strumenti di controllo** di Kaspersky non sono venduti separatamente, ma risultano abilitati per i seguenti livelli della soluzione **Kaspersky Security per le aziende**:

- Endpoint Security, Select
- 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](http://www.kaspersky.com)