

# ► KASPERSKY ENDPOINT SECURITY FOR BUSINESS

## Controlli degli endpoint

I potenti strumenti di controllo degli endpoint, strettamente integrati con una avanzata tecnologia anti-malware e con l'unico laboratorio di creazione di whitelist dedicato del settore, aiutano a proteggere dall'ambiente dinamico delle minacce IT del nostro tempo.

### PROTEZIONE, APPLICAZIONE, CONTROLLO

Le vulnerabilità delle applicazioni attendibili, il malware del Web e la mancanza di controllo sui dispositivi periferici sono gli elementi di un panorama delle minacce informatiche sempre più complesso. Gli strumenti di Application, Web e Device Control di Kaspersky Lab permettono il totale controllo degli endpoint senza compromettere la produttività.

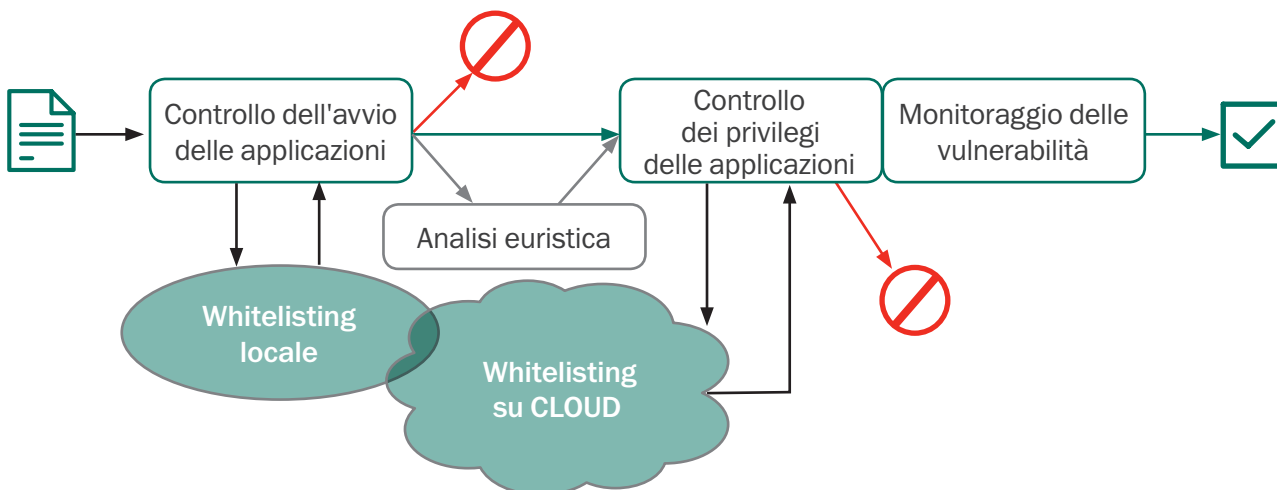
### CONTROLLO APPLICAZIONI E WHITELISTING DINAMICO

I sistemi vengono protetti dalle minacce conosciute e sconosciute offrendo agli amministratori il controllo totale delle applicazioni e dei programmi dei quali è autorizzata l'esecuzione sugli endpoint, indipendentemente dal comportamento dell'utente finale. Inoltre, viene monitorata l'integrità delle applicazioni per valutare il comportamento delle applicazioni ed impedire che eseguano azioni impreviste che potrebbero mettere in pericolo l'endpoint o la rete. La creazione e l'applicazione di criteri semplificati, personalizzabili o automatizzati consentono:

- **Controllo dell'avvio delle applicazioni:** consente, blocca, verifica l'avvio delle applicazioni. La produttività viene ottimizzata limitando l'accesso alle applicazioni non correlate all'attività aziendale.
- **Controllo dei privilegi delle applicazioni:** regola e controlla l'accesso delle applicazioni a risorse e dati del sistema. Le applicazioni vengono classificate come attendibili, non attendibili o con restrizioni. Viene gestito l'accesso delle applicazioni ai dati crittografati sugli endpoint, come le informazioni postate tramite browser Web o da Skype.
- **Scansione delle vulnerabilità delle applicazioni:** difesa proattiva dagli attacchi mirati alle vulnerabilità delle applicazioni attendibili.

Molte soluzioni di controllo si limitano a offrire funzionalità di blocco/accesso di base. Gli strumenti di controllo di Kaspersky Lab sono gli unici ad usare database di whitelist basati su cloud, consentendo l'accesso quasi in tempo reale agli ultimi dati sulle applicazioni.

Le tecnologie di controllo delle applicazioni di Kaspersky Lab si avvalgono di database di whitelist basati su cloud per analizzare e monitorare l'applicazione in ogni fase: download, installazione, esecuzione.



**Whitelisting dinamico**, che può essere abilitato tramite "Default Deny" completo: blocca tutte le applicazioni che tentano l'esecuzione su qualsiasi workstation se non esplicitamente autorizzate dagli amministratori. Kaspersky Lab è l'unica società di sicurezza IT con un laboratorio dedicato per il whitelisting che gestisce un database costantemente monitorato e aggiornato di oltre 500 milioni di programmi.

Il **Default Deny di Kaspersky Lab può essere applicato in un ambiente di prova**, permettendo agli amministratori di stabilire la legittimità delle applicazioni prima di bloccarle. Inoltre, si possono creare categorie di applicazioni in base alle firme digitali, impedendo agli utenti di avviare software legittimo che è stato però modificato da malware o proviene da una fonte sospetta.

## CONTROLLI WEB

Monitoraggio, filtro e controllo dei siti a cui l'utente finale può accedere sul posto di lavoro, aumentando la produttività e proteggendo da malware e attacchi basati su Web.

I controlli Web avanzati di Kaspersky Lab si basano su un elenco costantemente aggiornato di siti Web, raggruppati in categorie (ad es. adulti, giochi, social network, gioco d'azzardo). Gli amministratori possono creare facilmente criteri per proibire, limitare o controllare l'utilizzo da parte dell'utente finale di siti o categorie di siti, e per creare le proprie liste. L'accesso ai siti dannosi viene automaticamente bloccato.

Ponendo restrizioni al loro utilizzo, i controlli Web di Kaspersky Lab aiutano a prevenire la perdita di dati tramite social network e servizi di messaggistica istantanea. I criteri flessibili permettono agli amministratori di consentire la navigazione in orari della giornata determinati. L'integrazione con Active Directory consente l'applicazione di criteri in tutta l'organizzazione in modo rapido e facile.

Per maggiore sicurezza, i controlli Web di Kaspersky Lab vengono abilitati direttamente sull'endpoint, quindi i criteri vengono applicati anche se l'utente non è in rete.

## CONTROLLI DEI DISPOSITIVI

Non sempre la disabilitazione di una porta USB permette di risolvere i problemi dei dispositivi rimovibili. Ad esempio, una porta USB disattivata ha effetto su altre misure di sicurezza, come l'accesso VPN basato su token.

I controlli dei dispositivi di Kaspersky Lab consentono un livello più granulare di controllo a livello di bus, tipo e dispositivo, mantenendo la produttività dell'utente e al contempo ottimizzando la sicurezza. I controlli possono essere applicati con un dettaglio che arriva allo specifico numero di serie del dispositivo.

- Impostazione delle autorizzazioni di connessione/ lettura/scrittura dei dispositivi, oltre che della pianificazione temporale.
- Creazione di regole di controllo dei dispositivi basate su maschere, eliminando l'esigenza di connessione fisica dei dispositivi per inserirli nella whitelist. Whitelist contemporanea di più dispositivi.
- Controllo dello scambio di dati tramite dispositivi rimovibili all'interno e all'esterno dell'organizzazione, riducendo il rischio di perdita o furto di dati.
- Integrazione con le tecnologie di crittografia di Kaspersky Lab per applicare criteri di crittografia su specifici tipi di dispositivi.

## AMMINISTRAZIONE SEMPLIFICATA

Tutti gli strumenti di controllo di Kaspersky Lab risultano integrabili con Active Directory ed è possibile definire criteri di copertura con estrema semplicità e velocità. Tutti i controlli degli endpoint vengono gestiti da un'unica console, attraverso una sola interfaccia.

## Modalità di acquisto

**Gli strumenti di controllo degli endpoint di Kaspersky Lab non vengono venduti separatamente, ma risultano abilitati per i livelli "Select", "Advanced" e "Total" di Kaspersky Endpoint Security for Business.**