



▶ **KESB**
10 MOTIVI PER
ACQUISTARE

Kaspersky Endpoint

Security for Business

► 10 REASONS TO BUY

Kaspersky Endpoint Security for Business

La gestione della sicurezza dell'infrastruttura e degli endpoint si sta rivelando un'impresa sempre più ardua. Essendo costretto ad affrontare sfide di natura ampiamente diversificata, tra cui l'implementazione di soluzioni eterogenee e separate a fronte di un contesto caratterizzato da crescenti minacce di sicurezza, hai bisogno di un metodo innovativo e semplice per proteggere e gestire il tuo ambiente.

ECCO 10 MOTIVI PER I QUALI DOVRESTI SCEGLIERE LA SOLUZIONE KASPERSKY SECURITY FOR BUSINESS COME STANDARD DI SICUREZZA PER LA TUA AZIENDA:

1. **Un'unica piattaforma.** La piattaforma tecnologica di Kaspersky viene sviluppata internamente dai nostri ingegneri. Un singolo set di criteri permette di applicare protezione anti-malware, controlli degli endpoint, crittografia e altre funzioni di sicurezza.
2. **Un'unica console.** Attraverso un'intuitiva console centralizzata hai la possibilità di identificare, controllare e proteggere tutte le tue risorse endpoint (fisiche, virtuali, mobili), condurre valutazioni rapide e accurate delle vulnerabilità per assegnare la priorità alle patch di maggiore importanza, creare inventari hardware e software in tempo reale ed eseguire un reporting di informazioni precise e modificabili.
3. **Un unico costo.** Affidandoti a Kaspersky, non sarai costretto a valutare e reperire i fondi necessari per ordinare un nuovo strumento IT per ogni nuova area della rete che avrà bisogno di essere protetta. Abbiamo sviluppato un set completo di strumenti IT e di sicurezza integrati in un'unica piattaforma, mettendoti nelle condizioni di condurre un'unica valutazione e di presentare un'unica richiesta di budget!
4. **Controlli flessibili e granulari.** Scegliendo tra configurazioni predefinite o personalizzate, puoi impostare e applicare criteri di sicurezza per gestire il comportamento e le autorizzazioni relativi alle applicazioni, le periferiche collegate e l'utilizzo del Web, tanto in ufficio che durante gli spostamenti.
5. **Applicazione semplice e veloce della sicurezza mobile.** Il modulo centralizzato Mobile Device Management (MDM) ti permette di implementare in remoto la protezione degli endpoint mobili. Kaspersky ti offre la possibilità di proteggere i tuoi dati, anche sugli smartphone e i tablet personali dei dipendenti.
6. **Crittografia avanzata.** La crittografia del disco intero o dei file assicura la protezione dei dati aziendali in caso di furto o perdita del dispositivo. La tecnologia di Kaspersky consente di rendere illeggibili i dati per i cybercriminali, risultando al contempo trasparente per gli utenti e le applicazioni.
7. **Gestione efficiente delle patch.** Le avanzate funzionalità di Scansione delle Vulnerabilità (Vulnerability Scanning) e Gestione delle Patch (Patch Management) ti permettono di restare costantemente aggiornato e di ricevere immediata notifica di eventuali esposizioni al rischio di attacchi malware per la tua azienda.
8. **Potenti strumenti per la gestione dei sistemi.** È stato specificatamente progettato un potente toolkit per velocizzare e semplificare le attività IT che richiedono molto tempo, come installazione del sistema operativo, creazione dell'inventario di rete, provisioning dei sistemi, amministrazione remota, controllo degli accessi alla rete e gestione delle licenze.
9. **Protezione end-to-end.** Kaspersky vanta da tempo la fama di leader indiscusso del settore delle soluzioni di sicurezza dell'infrastruttura di rete. Assicura il supporto di numerosi sistemi operativi, tra cui Windows, Linux, Apple, Exchange, Netware, Notes/Domino, SharePoint, iOS, Android, Windows Mobile, Symbian e molti altri ancora. Kaspersky Lab ti offre la soluzione ideale per la protezione di tutti gli elementi del tuo ambiente, dall'endpoint al gateway Internet.
10. **Prestazioni comprovate e certificate.** Test indipendenti continuano a confermare regolarmente che i prodotti Kaspersky Lab sono sempre considerati i migliori. Scegli quindi di non mettere a repentaglio la tua sicurezza e non sprecare risorse preziose con altri fornitori che non sono in grado di contrastare l'escalation di minacce alla sicurezza!