Kaspersky® Endpoint Security for Business

Proteggete le risorse di maggior valore per il vostro business

I budget per la sicurezza IT non rispecchiano sempre le crescenti esigenze aziendali e i livelli in ascesa delle minacce. Le risorse devono essere ottimizzate per soddisfare le sfide odierne e future. Ma come fare a identificare la soluzione di sicurezza più adatta, una che protegga l'intera infrastruttura IT dalle minacce informatiche più avanzate e che garantisca la business continuity, senza esaurire il budget?

Provate a chiedere ai nostri clienti. Kaspersky Endpoint Security for Business fornisce una soluzione di sicurezza completa e flessibile che che si adatta alle esigenze aziendali, grazie ad uno "stack" di tecnologie completo e all'avanguardia. E i risultati parlano da soli.

L'innovativo concetto di Threat Intelligence influenza tutte le attività che svolgiamo. Essendo un'azienda indipendente, possiamo muoverci con più flessibilità e rapidità per neutralizzare le minacce informatiche, indipendentemente dalla loro origine o dal loro obiettivo. Ecco come i nostri prodotti e le nostre soluzioni sono in grado di offrire livelli ineguagliabili di True Cybersecurity.

Common Criteria

Ready for GDPR

True Cybersecurity all'avanguardia

Le tecnologie presenti in Kaspersky Endpoint Security for Business forniscono un perfetto equilibrio tra performance e protezione efficace. Questo equilibrio potrebbe spiegare perché i nostri prodotti forniscono uno dei più alti tassi di rilevamento del settore, come dimostrato in modo continuativo da test indipendenti. Kaspersky Lab si è classificato tra i primi 3 vendor in ciascun Use Case del Gartner's 2018 Critical Capabilities for Endpoint Protection Platforms.

1. **Protezione** di server, gateway ed endpoint
2. **Semplificazione** della gestione mediante una console unificata
3. **Riduzione della complessità e del costo totale** di proprietà
4. **Supporto della delega** di responsabilità all'interno del team
5. **Incremento della produttività** tramite controlli cloud-enabled
6. **Protezione** delle vulnerabilità **24 ore su 24, 7 giorni su 7,** per ridurre i punti di ingresso agli attacchi
7. **Risparmio di tempo** automatizzando i task di deployment del software e del sistema operativo

Efficienza best-in-industry

Protezione flessibile pensata dagli esperti leader del settore, con un impatto minimo sulle risorse e sui sovraccarichi di gestione. La protezione e le tecnologie basate su machine learning identificano e bloccano le minacce agli endpoint, indipendentemente dall'origine o dall'obiettivo. Inoltre, in caso di attacco, le azioni nocive vengono annullate così gli utenti possono continuare a lavorare.

Su misura per l'ambiente di lavoro

Protezione di diversi ambienti e semplice scalabilità che non richiede una pianificazione estensiva nemmeno nelle infrastrutture IT eterogenee, fornendo la libertà di cambiare qualsiasi impostazione predefinita e di scegliere quando adottare nuove funzionalità.

Soddisfazione del cliente garantita

Un singolo prodotto contrasta le minacce ai dati in qualsiasi ambiente di installazione, con licenze e costi trasparenti. I nostri clienti esprimono costantemente enorme soddisfazione per i risultati ottenuti, come confermato nelle recensioni indipendenti, contribuendo alla nostra posizione di leadership nei test indipendenti degli ultimi 6 anni (Top 3).

Oltre la protezione endpoint

Le nostre tecnologie sono in continua evoluzione e consentono di proteggere le risorse più importanti dell'azienda dai cryptominer e dalle minacce informatiche più recenti e complesse, grazie alla nostra threat intelligence e machine learning.

Blocco di ransomware, attacchi fileless e acquisizioni di account

Protegge gli endpoint dagli exploit più recenti e salvaguarda i dati e le cartelle condivise da ransomware e minacce avanzate. **L'analisi comportamentale** implementa un meccanismo di **protezione della memoria** che preserva i processi fondamentali del sistema e impedisce il furto di credenziali utente e amministratore.

Riduzione dell'esposizione ad attacchi rivolti alle applicazioni

I controlli integrati riducono notevolmente l'esposizione a minacce sconosciute poiché consentono di gestire le azioni e i software che possono essere eseguiti sugli endpoint. **L'Adaptive Anomaly Control**, che adatta automaticamente la sicurezza al massimo livello appropriato a ciascun ruolo nell'organizzazione, è completato dal modulo Application Control di livello Enterprise e da un database di whitelisting sempre aggiornato.

Identificazione di un maggior numero di attacchi e intrusioni, anche i più avanzati

Gli utenti malintenzionati utilizzano rootkit e bootkit per nascondere le proprie attività alle soluzioni di protezione. La tecnologia anti-rootkit, parte della protezione multilivello di Kaspersky Lab, consente di rilevare e neutralizzare anche le infezioni più nascoste. I sensori incorporati e l'integrazione con **Kaspersky Endpoint Detection and Response** consentono l'acquisizione e l'analisi di grandi volumi di dati interni senza alcun impatto sulla produttività dell'utente.

Regolazione dell'accesso ai dati sensibili e dispositivi di registrazione

La nostra soluzione restringe i privilegi delle applicazioni in base ai livelli di affidabilità assegnati, limitando l'accesso a risorse come i dati crittografati. Lavorando con il reputation database locale e cloud (**Kaspersky Security Network** o KSN), **Host Intrusion Prevention System** (HIPS) controlla le applicazioni e l'accesso a risorse di sistema critiche, dispositivi di registrazione audio e video.

Blocco delle minacce web prima che possano raggiungere gli endpoint

Le nostre tecnologie di sicurezza filtrano il traffico dei gateway, bloccando automaticamente le minacce in entrata prima che raggiungano gli endpoint e i server. In questo modo si riduce notevolmente il rischio di exploit delle vulnerabilità e diminuiscono notevolmente i costi operativi per il personale di sicurezza IT.

Leggero ed efficace anche senza aggiornamenti regolari

Il nostro vasto knowledge system database include 50 TB di dati e oltre 4 miliardi di hash, ma questi enormi volumi di dati di intelligence non influiscono in alcun modo sulle risorse o sulle performance. Un'esclusiva modalità cloud per la protezione dei componenti garantisce una copertura ottimale con il minimo impatto sulle risorse del PC e sulla connessione a Internet.

Il nostro modello matematico analizza oltre 100.000 funzioni campione e utilizza 10 milioni di behavior log per "istruire" i modelli, in un pacchetto che lato client ha un peso di soli 2 MB.

Semplificazione dei task IT

Il deployment da remoto di software di terze parti è solo l'inizio. **Le funzionalità di patch management e vulnerability assessment automatizzate**, basate su una intelligence attiva 24 ore su 24, permettono di mantenere aggiornato il software potenzialmente vulnerabile consentendo agli amministratori IT di dedicarsi ad altre attività.

Prevenzione dei data breach

È possibile utilizzare la tecnologia di **gestione integrata Microsoft BitLocker** per abilitare la crittografia incorporata nel sistema operativo oppure è possibile proteggere i dati tramite la **crittografia** con certificazione Common Criteria: EAL2+ e FIPS 140-2. Il modulo **Device Control**, gestito centralmente, protegge dalle conseguenze dovute alla perdita di dati su dispositivi portatili non crittografati o non approvati e al caricamento di dati infetti sul dispositivo.

Supporto per l'accesso ai dati in mobilità e da remoto

La funzionalità integrata **Mobile Threat Protection** blocca gli attacchi che mirano a acquisire i dati e a sfruttare le vulnerabilità dei dispositivi mobili, per utilizzarli come punti di accesso all'infrastruttura IT. La **soluzione EMM già in uso** può essere utilizzata per installare e configurare la protezione per i dispositivi mobili, allineando il sistema di sicurezza ai processi aziendali esistenti.

Ottimizzazione dell'efficienza: gestione di tutte le piattaforme

Una singola console web offre visibilità e controllo completi su ogni workstation, server e dispositivo mobile, ovunque si trovi. Kaspersky Endpoint Security for Business è estremamente scalabile e fornisce funzionalità di accesso e controllo delle licenze, risoluzione dei problemi da remoto e controllo dell'utilizzo della rete. La gestione centralizzata è completata grazie all'integrazione con Active Directory, **Role-Based Access Control** (RBAC) e le dashboard integrate.

Aumento della produttività e riduzione delle minacce

L'**anti-spam assistito da cloud** di Kaspersky Lab rileva anche lo spam più sofisticato in qualsiasi lingua, riducendo al minimo la perdita di informazioni preziose a causa di falsi positivi. Il blocco tempestivo dello spam consente di **risparmiare risorse preziose**.

Processo di aggiornamento semplificato

Seamless upgrade per le major release di prodotto, incluse le macchine crittografate. Anche durante la migrazione tra versioni di Windows, la protezione resta costantemente attiva. Con criteri di sicurezza unificati e impostazioni predefinite, Kaspersky Endpoint Security for Business fornisce la libertà di adottare o cambiare qualsiasi impostazione e di scegliere quando effettuare la migrazione a nuove versioni preservando al contempo i criteri e le impostazioni.

La console di gestione che supporta il deployment negli ambienti cloud Amazon e Microsoft Azure consente di usufruire di una tolleranza d'errore migliorata e della garanzia di meno di 4 ore di inattività all'anno da parte di un vendor IaaS, pur preservando la completa flessibilità in termini di impostazioni di sicurezza e cicli di aggiornamento. La console web può essere utilizzata insieme a, o al posto di, una console tradizionale basata su MMC.

Le tecnologie e gli strumenti di **Kaspersky Endpoint Security for Business** sono studiati in maniera intelligente con livelli di licensing bilanciati per rispondere alle crescenti esigenze di sicurezza e IT.

Kaspersky® Total Security for Business

Le aziende con ambienti IT complessi, che combinano sistemi nuovi e legacy, devono regolare la propria sicurezza in base ai limiti e ai requisiti di ciascun sistema: ed è proprio questo che la nostra soluzione di sicurezza più completa per endpoint, gateway e server consente di fare, fornendo una protezione adattabile all'infrastruttura IT.

Kaspersky® Endpoint Security for Business
Advanced

Il nostro livello Advanced garantisce una soluzione efficace per la protezione dell'azienda. Oltre a garantire la copertura per tutti gli endpoint e server, offre livelli di sicurezza flessibili per proteggere i dati sensibili, eliminare le vulnerabilità e semplificare i task di gestione dei sistemi di sicurezza.

Kaspersky® Endpoint Security for Business
Select

In un mondo sempre più digitale, è necessario proteggere tutti i server Linux, i laptop Mac e i dispositivi mobili Android. Offriamo una sicurezza flessibile che permette di proteggere ogni endpoint aziendale, in un'unica soluzione con una console di gestione flessibile.

Aggiunta di tecnologie di sicurezza in base alle esigenze

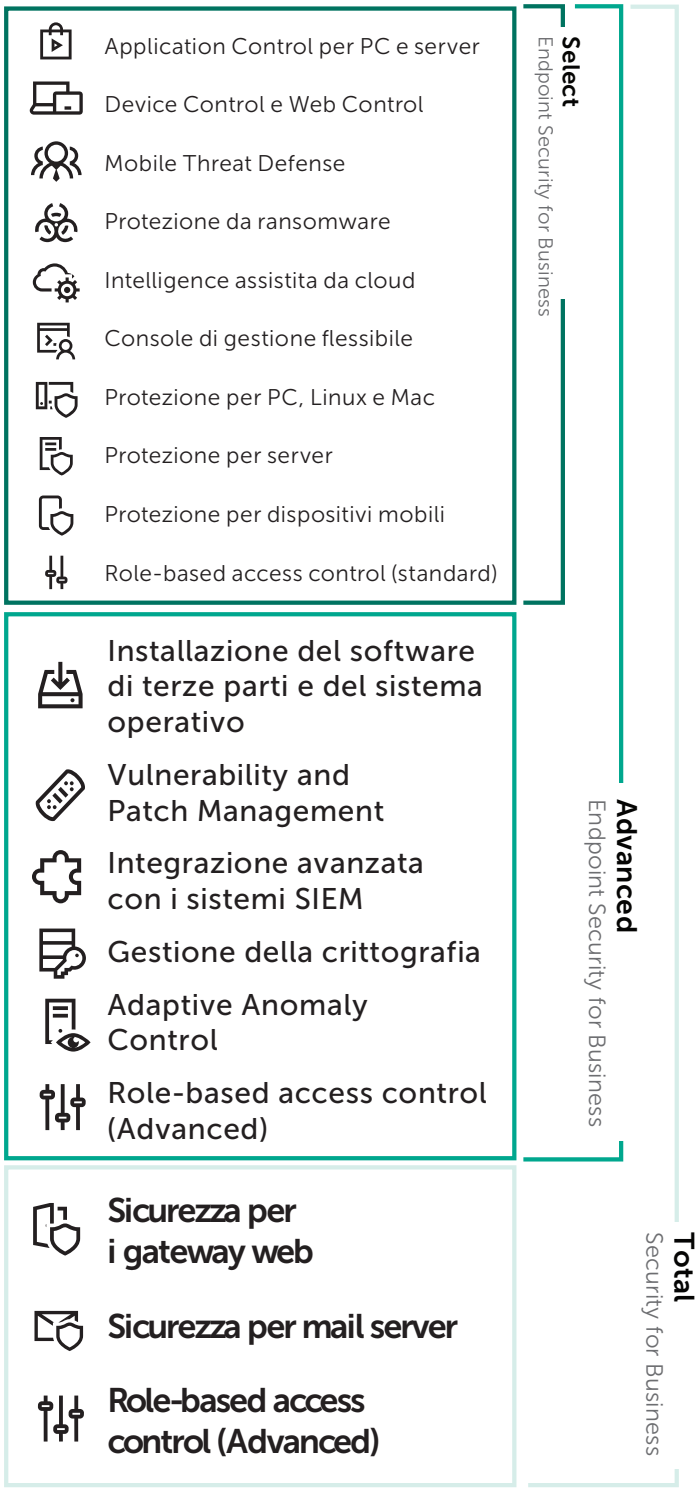
Per gli acquirenti di Kaspersky Endpoint Security for Business Select, i seguenti componenti già inclusi nei nostri livelli Advanced e Total sono disponibili come add-on separati:

- Kaspersky Vulnerability and Patch Management, automatizza e centralizza l'individuazione delle vulnerabilità del software ed unitamente al patch management aiuta a proteggere dalle minacce pericolose, incluso il ransomware.
- Kaspersky Encryption, che consente di gestire la full disk e file level encryption e supporta il Single Sign-On per l'accesso immediato ai file crittografati.

Dopo l'acquisto, basta attivare la funzionalità add-on dalla console di gestione unificata.

Qual è la versione più adatta a voi?

Vi aiutiamo a gestire e a proteggere il vostro mondo. Qualsiasi siano le esigenze IT e di sicurezza, **Kaspersky Endpoint Security for Business** è la soluzione giusta.



Assistenza e servizi

Fornendo supporto in più di 200 Paesi, da 35 uffici in tutto il mondo, il nostro impegno è 24 ore su 24, 7 giorni su 7 e viene incluso nei nostri pacchetti di assistenza Maintenance Service Agreement (MSA). I team Professional Services sono sempre pronti a garantire che l'utente possa utilizzare al meglio la soluzione, fornendo assistenza durante il setup iniziale e il supporto in caso di incidenti critici.

True Cybersecurity. Non dovete far altro che chiedere ai nostri clienti.

Kaspersky Lab è stato ancora una volta nominato per il **Gartner Peer Insights Customer Choice Awards 2018 per la soluzione Endpoint Protection**. Durante la prima edizione di questo premio per il segmento EPP nel 2017, solo Kaspersky Lab ha vinto il **platinum award**, il più alto riconoscimento in questa categoria. Siamo orgogliosi di ricevere un tale riconoscimento da coloro che rispettiamo maggiormente, i nostri clienti, e di vedere che la nostra valutazione complessiva si attesta costantemente su un valore **4,7 su 5** per le piattaforme di protezione endpoint.

Un livello impareggiabile di trasparenza e compliance

Le aziende richiedono neutralità e sovranità dei dati: il nostro prodotto esegue la scansione dei dati, ma non li raccoglie mai. I dati statistici vengono elaborati in Svizzera per garantire la neutralità geopolitica. L'apertura del primo Transparency Center nel nostro settore rappresenta uno step verso il nostro obiettivo: diventare completamente trasparenti. La nostra speranza è che altri vendor seguano il nostro esempio.

Riconosciuta dai decision-makercome voi

Fidatevi dei consigli di coloro che hanno già effettuato l'upgrade a Kaspersky Endpoint Security for Business e che ne stanno sfruttando i vantaggi:

- Protezione costante: gli upgrade facili e immediati vi garantiscono di essere sempre aggiornati e pronti a contrastare le minacce informatiche più recenti
- Gestione centralizzata e intuitiva: un server, una console web, un singolo agente
- Perfetta integrazione dei diversi componenti
- Tutto ciò che occorre in un singolo acquisto: licenze e costi trasparenti.

Quality Inspector
Settore Produzione
Ruolo Infrastruttura e operazioni
Dimensione dell'azienda < 50 milioni USD
Ultimo aggiornamento 25 ottobre 2018
https://kas.pr/epp-ref2

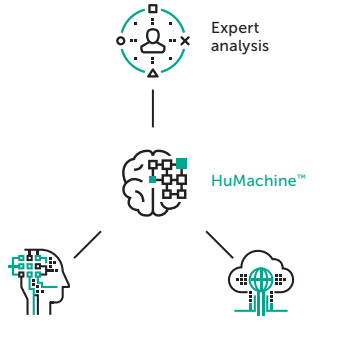
"Protezione completa con rapida implementazione".

Provate voi stessi

Scoprite la True Cybersecurity. Visitate questa pagina **per provare la versione completa** di Kaspersky Endpoint Security for Business.

Kaspersky IT Security Solutions for Business

La protezione endpoint, anche se critica, è solo l'inizio. Kaspersky Lab offre prodotti per infrastrutture cloud ibride e per sistemi legacy Windows XP che collaborano tra loro o lavorano indipendentemente, così da poter scegliere in maniera autonoma la strategia di sicurezza più adatta. Maggiori informazioni sul nostro sito web.



Kaspersky Lab
Trovate il partner più vicino: **www.kaspersky.com/buyoffline**
Kaspersky for Business: **www.kaspersky.com/business**
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Novità sulla sicurezza IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.it