kaspersky BRING ON THE FUTURE

Conforme al GDPR

Kaspersky Endpoint Security for Business

Efficace protezione delle risorse di maggior valore per il vostro business

Gli strumenti malevoli di cui fanno uso i cybercriminali sono ormai disponibili a basso costo: per tale motivo le aziende stanno sperimentando un drammatico incremento degli eventi legati alla sicurezza IT. In particolar modo, sta aumentando in modo considerevole la probabilità di subire attacchi di natura mirata. A tutto ciò si aggiungono ulteriori elementi: il lavoro in smart working, il proliferare dei metodi per lo scambio di informazioni, il fatto che la maggior parte di noi è cresciuta online, acquisendo determinate conoscenze in relazione alle best practice di Cybersecurity. In un ambiente così variegato e ricco di sfide come si può essere sicuri di avere il giusto prodotto per la sicurezza dell'azienda, ovvero una soluzione che protegga l'intera infrastruttura IT dalle minacce informatiche più avanzate e che garantisca la business continuity senza esaurire il budget?

Kaspersky Endpoint Security for Business offre un set completo di tecnologie all'avanguardia, assicurando difese flessibili e automatizzate contro le minacce, così come un efficace hardening dei sistemi; è perfettamente scalabile e in grado di salvaguardare il business e gli asset aziendali. 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. I nostri prodotti offrono una protezione altamente flessibile, che nessun altro vendor è in grado di fornire.

FORRESTER WAVE LEADER 2019 Endpoint Security Suites

KASPERSKY LAB NSS RECOMMENDED

Common Criteria

SE Labs AAA ENTERPRISE ENDPOINT PROTECTION OCT-DEC 2019

AV-TEST AWARD Best Performance Kaspersky Endpoint Security

AV-TEST AWARD Best Usability Kaspersky Endpoint Security

AV comparatives APPROVED Business Security DEC 2019

1 "The Forrester Wave™: Endpoint Security Suites, Q3 2019: The 15 Providers That Matter Most And How They Stack Up", a cura di Chris Sherman, con il contributo di Stephanie Balaouras, Merritt Maxim, Matthew Flug e Peggy Dostie.

2 "The Total Economic Impact™ Of Kaspersky Security Solutions", Forrester Research, Inc., Gennaio 2020.

3 Esistono alcune limitazioni riguardo alle funzionalità che si possono gestire attraverso la console cloud. Per informazioni più dettagliate consultare la guida online.

Cybersecurity all'avanguardia

Le tecnologie EDR altamente automatizzate, combinate con il nostro approccio multilivello, consentono di raggiungere un perfetto equilibrio tra performance e protezione efficace. Kaspersky è stata nominata azienda "Leader" nell'ambito del report Wave Endpoint Security Suites 2019 stilato da Forrester[1].

Protezione di endpoint, server e gateway

Le tecnologie di sicurezza più testate e premiate al mondo contribuiscono a migliorare il rilevamento delle minacce, grazie a un tasso di falsi positivi estremamente ridotto: proteggono con la massima efficacia endpoint, server, gateway e container.

Semplificazione in termini di gestione e delega della sicurezza

La console unificata, disponibile tramite un modello di deployment in cloud[3] oppure on-premise, supporta l'integrazione di Active Directory, così come la funzionalità Role-Based Access Control (RBAC) e dashboard personalizzabili: in tal modo si può semplificare l'accesso in base alle specifiche responsabilità dei membri del team.

Riduzione del costo totale di proprietà e del livello di complessità

Le interviste condotte da Forrester con i clienti riguardo al TEI (impatto economico totale) e il relativo report elaborato in seguito, confermano a pieno titolo come i nostri clienti, utilizzando questa soluzione di sicurezza, abbiano registrato un ROI medio del 441%[2]. Quest'anno, con la nostra nuova offerta SaaS, ci prendiamo ugualmente cura degli upgrade della console e di molto altro ancora, senza costi aggiuntivi, fornendo tutto il potenziale per conseguire un ROI ancor più elevato. La nostra console cloud di livello Enterprise[3] consente all'azienda di concentrarsi esclusivamente sugli eventi di sicurezza, non sulle attività di manutenzione.

Hardening dei sistemi e aumento della produttività

Il modulo Host Intrusion Prevention e l'impiego di strumenti cloud-enabled quali Application Control, Device Control e Web Control, unitamente all'implementazione dello scenario Default Deny, consentono di ridurre la superficie di attacco, salvaguardando le risorse aziendali anche all'esterno del perimetro IT.

Funzionalità EDR automatizzate, per rilevare un maggior numero di attacchi e intrusioni

I processi EDR automatizzati proteggono i dispositivi utente dagli attacchi mirati in grado di sfruttare le vulnerabilità non corrette da patch, presenti nel sistema operativo e nelle applicazioni più diffuse. Inoltre identificano modelli di comportamento anomali, rilevano e bloccano automaticamente attacchi ransomware mirati e minacce fileless.

Risparmio di tempo grazie all'automazione dei task di deployment del software e del sistema operativo

Il setup di nuove workstation nelle sedi e nelle filiali può essere eseguito automaticamente e da remoto. Inoltre, l'installazione automatica di nuove applicazioni può essere avviata e pianificata a distanza.

Semplificazione delle attività di migrazione

La migrazione intuitiva dalle soluzioni di protezione endpoint di terze parti garantisce una transizione semplice mentre il nostro efficace servizio di audit della qualità post-deployment verifica la correttezza della configurazione.

La tranquillità al centro della digital transformation

Il deployment automatizzato del software e i facili upgrade da una versione all'altra del prodotto riducono ai minimi termini il numero di eventi relativi allo stato dell'implementazione: ciò consente di risparmiare tempo e limitare al massimo i costi in relazione all'intervento degli esperti di sicurezza IT, che si potranno concentrare su task di maggiore importanza.

Le nostre competenze sono la vostra forza

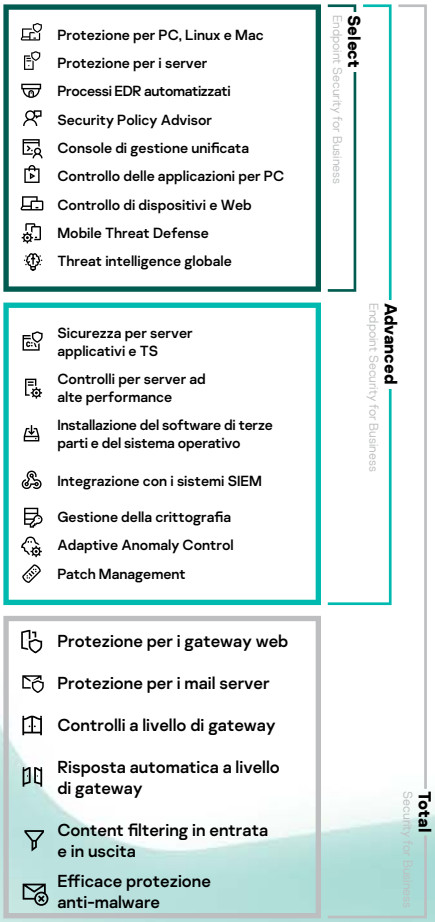
I tassi di rilevamento superiori e i processi EDR automatizzati integrati consentono di rispondere rapidamente a un notevole numero di attacchi, riducendo il TCO e minimizzando il numero di eventi che richiedono un intervento umano.

Un piccolo errore non deve tradursi in un serio problema

Le impostazioni di sicurezza predefinite sono ottimizzate: inoltre, il nostro security advisor monitora le eventuali modifiche apportate, avvisando in modo tempestivo gli amministratori riguardo a errori potenzialmente gravi.

Tre livelli di funzionalità di protezione progressivi

Gli strumenti e le tecnologie Next Generation presenti in Kaspersky Endpoint Security for Business sono studiati in modo intelligente, con livelli di licensing bilanciati per rispondere alle crescenti esigenze di sicurezza e IT. Per maggiori dettagli, consultare le nostre schede tecniche separate riguardo a ciascun livello: Select, Advanced e Total.



Assistenza e servizi

Fornendo assistenza in più di 200 paesi, da 35 uffici in tutto il mondo, il nostro servizio di Supporto tecnico soddisfa pienamente ogni eventuale richiesta del personale IT dell'azienda, 24 ore su 24, 7 giorni su 7, 365 giorni l'anno. I nostri servizi professionali includono, tra gli altri, la verifica della corretta configurazione delle soluzioni Kaspersky, relativamente alle implementazioni eseguite da partner e clienti. Ulteriori informazioni sono disponibili qui.

Oltre la protezione endpoint

Le nostre tecnologie sono in continua evoluzione e consentono di proteggere le risorse più importanti dell'azienda dalle minacce informatiche più recenti e complesse, grazie alla threat intelligence fornita in tempo reale e all'elevata efficacia del machine learning.

Un livello di efficacia pienamente riconosciuto dai decision-maker e dalle aziende leader

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, un singolo agente
- Perfetta integrazione dei componenti, acquisita con decenni di primi posti e verifiche indipendenti
- Tutto ciò che occorre in un singolo acquisto: licenze e costi trasparenti.

Gestione del prodotto
Settore Vari
Dimensione dell'azienda
<50M - 250M USD
Ultimo aggiornamento 2019
https://kas.pr/epp-ref5

> **I vostri dati sono la vostra vita. Kaspersky Endpoint Security proteggerà la vostra vita.**

Provatelo voi stessi

L'attenzione che rivolgiamo alla ricerca e sviluppo ci consente di individuare i task più importanti su cui concentrare le risorse, in modo da fornire tecnologie di protezione convenienti e aggiungere continue innovazioni tecnologiche. Provate voi stessi l'elevata flessibilità della protezione dalle minacce avanzate! Visitate questa pagina per una prova gratuita di 30 giorni della soluzione Kaspersky Endpoint Security for Business.

Prodotti Kaspersky per la sicurezza IT dell'azienda

La protezione degli endpoint, anche se critica, è solo l'inizio. Kaspersky offre prodotti per infrastrutture cloud ibride e per sistemi legacy Windows XP che collaborano tra loro o lavorano in maniera indipendente, così da poter scegliere in maniera autonoma la strategia di sicurezza più adatta (avanzata o basata su un'unica fonte di security), senza compromettere le performance. Ulteriori informazioni sono disponibili sul nostro sito web.

Per i requisiti di sistema fare riferimento alla Knowledge Base

www.kaspersky.it