kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Security for Business

La tecnologia è un motore di trasformazione per le imprese, di fronte alla quale o si rimane al passo o si rischia di rimanere bloccati. Ma la tecnologia apre anche le porte ai criminali, il cui obiettivo primario è rappresentato dagli endpoint. Dovete quindi essere più furbi dei cybercriminali che vi hanno preso di mira, implementando soluzioni efficaci e affidabili per proteggere ciò che la vostra azienda ha di più importante.

Sfide

Aumenta la pressione degli attacchi

Gli strumenti dei cybercriminali sono ormai così accessibili che assistiamo a un importante incremento degli incidenti e dei rischi per la security. Ransomware, spyware finanziario, phishing e altre minacce possono danneggiare gravemente la vostra organizzazione, soprattutto se siete impegnati nella trasformazione digitale.

Un'infrastruttura eterogenea da proteggere

Di fronte alla diffusione del lavoro a distanza, dei servizi cloud e dei processi agili, tutte le strategie di security devono coprire l'intera gamma degli endpoint, inclusi laptop, workstation, server e device mobili, anche quelli personali utilizzati per il lavoro. Bisogna anche pensare a tutti i sistemi operativi supportati.

Elevati livelli di complessità da affrontare

Un'infrastruttura IT complessa e le competenze necessarie per supportarla e proteggerla hanno un costo. Dovete investire in modo efficace nelle soluzioni giuste per soddisfare i requisiti aziendali di security in continua evoluzione in termini di tempo, budget, personale e competenze specifiche.

Soluzione

Sicurezza flessibile e adattiva

Dovete essere in grado di:

- Proteggere a 360 gradi dati, dipendenti e infrastruttura, senza impattare sulle prestazioni.
- Fare affidamento sulla threat intelligence più recente e affidabile per individuare e contrastare le minacce nuove ed emergenti in cui vi imbattete.
- Riconoscere i modelli di comportamento delle minacce, in modo da poter neutralizzare anche le minacce sconosciute.
- Ridurre la superficie di attacco controllando quali applicazioni, siti web e dispositivi possono interagire con i vostri endpoint e utenti.

Un'unica soluzione per qualsiasi piattaforma

Dovrete cercare:

- La migliore security possibile per ogni workstation, server e dispositivo mobile in cui transitano i vostri dati, ovunque si trovino e indipendentemente dal fatto che ne siate o meno proprietari. Pensate anche ai punti di ingresso delle minacce e a come proteggere i gateway web ed e-mail senza aumentare il carico di lavoro del vostro team.
- La certezza di poter coprire tutti i sistemi operativi nel vostro ambiente misto, inclusi Windows, Mac, Linux, iOS e Android, con un'unica soluzione, da un'unica console.

Gestione flessibile e automazione delle attività

È ideale ottimizzare le risorse con:

- Elevati livelli di automazione, in particolare per attività essenziali ma di routine come l'applicazione di patch e il deployment dei sistemi operativi. Il tempo e le competenze del vostro team sono troppo preziosi per essere sprecati.
- Funzionalità di gestione remota, sia che si tratti di configurare workstation negli home office o di proteggere i dati con opzioni di encryption.
- Centralizzazione. Non è necessario passare da una console all'altra: serve una gestione semplice e integrata tramite un'unica schermata, nel vostro perimetro o nel cloud.

Costo dei data breach

105.000 dollari
per le PMI

101.000 dollari (2020) ▲ 105.000 dollari (2021)

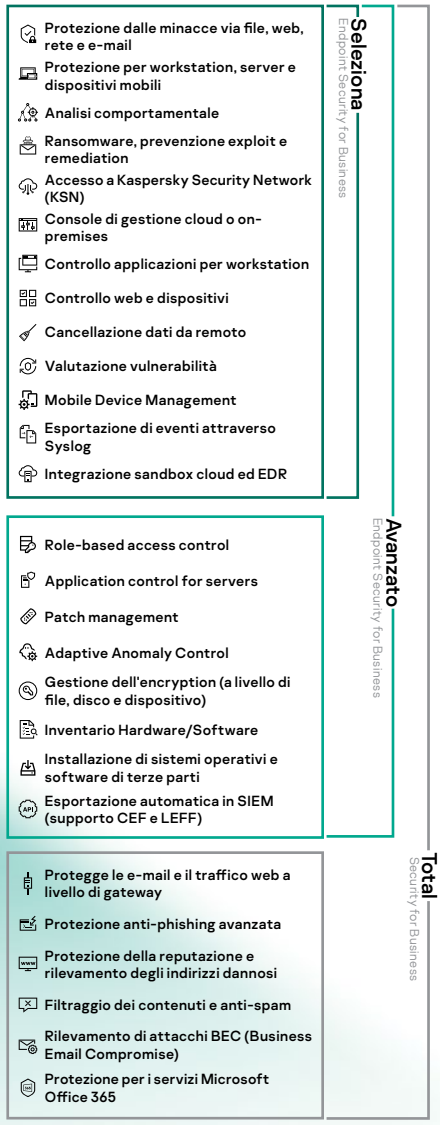
927.000 dollari
per le aziende

1,09 milioni di dollari (2020) ▼ 927.000 dollari (2021)

Fonte: Kaspersky IT security economics report 2021

Tre livelli di protezione progressivi

Gli strumenti e le tecnologie presenti in Kaspersky Endpoint Security for Business sono studiati e bilanciati in modo intelligente in più livelli progressivi per rispondere alle crescenti esigenze di sicurezza e IT.



La sicurezza più premiata e apprezzata dai nostri clienti.

Tra il 2013 e il 2021 i prodotti Kaspersky hanno partecipato a 741 test e recensioni indipendenti. I nostri prodotti sono arrivati primi 518 volte. Maggiori dettagli sono disponibili all'indirizzo www.kaspersky.it/top3

Minacce ransomware

Questi attacchi vengono perpetrati ai danni di individui o aziende, e negli ultimi anni alcuni degli attacchi più importanti hanno colpito brand rinomati.

L'88% dei top manager di aziende che sono state precedentemente colpite dal ransomware ha dichiarato di essere disposto a pagare in caso di nuovi attacchi.

Il ransomware è un problema in crescita per le aziende di tutto il mondo, e il numero di attacchi basati su ransomware è quasi raddoppiato nel 2021. Ciò può essere in parte attribuito alla pandemia, durante la quale sempre più persone hanno iniziato a lavorare da casa. Ma di fronte a un modello di lavoro ibrido destinato a non scomparire, la probabilità di attacchi ransomware rimane presente.

Cosa vi offriamo

- Sicurezza reale. Proteggiamo in modo completo tutti i vostri endpoint dalle minacce diffuse ed emergenti, grazie alle prestazioni imbattibili delle tecnologie Kaspersky come la **protezione dagli attacchi fileless**, l'analisi del comportamento **basata su machine learning** e la protezione specifica contro exploit, ransomware e spyware finanziario.
- Protezione proattiva. Blocchiamo gli attacchi sul nascere. La protezione pre-esecuzione tramite **Adoptive Anomaly Control** unisce la semplicità delle regole di blocco all'intelligenza dell'ottimizzazione automatica, basata sull'analisi comportamentale.
- Un ecosistema completo per le vostre crescenti competenze in materia di sicurezza IT. La risposta e l'analisi automatizzate sfruttano le **integrazioni** con le soluzioni EDR e **SIEM**.
- Risparmio economico. Il nostro approccio a più livelli vi consente di pagare solo per le funzionalità di cui avete bisogno al momento.
- Sempre al passo coi tempi. Upgrade semplificato: basta spostarsi tra i livelli. La nostra soluzione completamente scalabile è predisposta per supportare **migliaia di dispositivi gestiti** di pari passo con la crescita della vostra azienda.
- **Adozione del cloud semplificata.** Con protezione per i servizi **Microsoft Office 365**
- Flessibilità. **Scegliete la vostra opzione di deployment preferita**: in cloud, on-premises, air gap e in distribuzioni ibride. Allocate quindi i diversi livelli di accesso ai sistemi di sicurezza ai diversi membri del team con controllo dell'accesso granulare basato sui ruoli **(RBAC)**.
- Maggiore tranquillità. Tutti i vostri dati sensibili sono totalmente protetti con un **set di funzionalità per la protezione dei dati** che include gestione dell'encryption a livello di file e disco, nonché nei dispositivi esterni. La cancellazione dei dati da remoto elimina i dati in caso di furto o smarrimento di un dispositivo.
- Difese del perimetro **Impedite agli attacchi basati sul web e sull'e-mail** di raggiungere i loro obiettivi principali: dipendenti e relativi endpoint

Casi di successo

Proteggete automaticamente i vostri sistemi

La detection basata sui comportamenti del malware è un componente di fondamentale importanza nell'ambito della protezione multilivello Next Generation di Kaspersky. È uno dei metodi più efficienti per proteggersi da insidiose minacce avanzate, come malware fileless, ransomware e malware zero-day.

L'utilizzo dei dati di Kaspersky Security Network garantisce risposte più rapide alle nuove minacce, migliora le prestazioni dei componenti di protezione e riduce la probabilità di falsi positivi. In conclusione, tassi di detection superiori e sicurezza adattiva integrata si traducono in una risposta rapida agli attacchi con un tasso minimo di falsi positivi. Kaspersky è l'unico fornitore di sicurezza informatica a vantare un tasso di protezione dal ransomware del 100% in un recente studio AV-Test. AV-Test Advanced Endpoint Protection: Ransomware Protection test, AV-Test, 30 settembre 2021

Riducete la superficie di attacco

Allineate i dispositivi remoti con la sicurezza IT aziendale. I controlli relativi alle applicazioni riguardano sia la produttività (limitando ad esempio l'accesso ad app di gioco o social network) che la sicurezza. I dipendenti possono essere esposti a phishing e malware nelle app violate e nei siti web dubbi. Anche solo collegarsi a un modem USB o a una stampante di rete può comportare la fuga di dati sensibili. Tutti questi vettori di attacco, oltre al rischio di errore umano, possono essere notevolmente ridotti applicando controlli granulari di applicazioni, web e dispositivi.

L'Adaptive Anomaly Control consente di rafforzare i criteri comuni e di vedere come il sistema applicherà le regole, in base al comportamento dell'utente.

Riducete tempo, impegno e costi

Gestite Kaspersky Endpoint Security for Business dalla console cloud.

Questo approccio basato su SaaS non richiede investimenti hardware e vi consente di concentrarvi sulle iniziative di business piuttosto che dedicare tempo ad aggiornamenti, supporto e disponibilità, tutti aspetti di cui si occupa la nostra infrastruttura cloud.

E pensate al tempo che il vostro team dedica all'hardening degli endpoint, alla gestione remota dei dispositivi, al deployment dei sistemi operativi, alle patch e alla gestione dell'encryption. Kaspersky Endpoint Security ottimizza e automatizza tutte queste attività e altro ancora, offrendo un'unica soluzione e un'unica interfaccia web per gestire tutto. Niente più console separate o prodotti diversi per ogni attività o tipo di dispositivo.

Costruite una solida strategia di protezione dei dati

Gli attacchi odierni utilizzano strumenti e applicazioni legittimi che consentono agli attori delle minacce di trovare nuove vulnerabilità ed exploit zero-day nelle applicazioni di uso comune. La gestione automatizzata delle patch riduce significativamente il rischio per i vostri dati derivante da questi attacchi, mentre l'encryption garantisce che solo gli utenti legittimi possano accedere a specifici file sensibili o dispositivi esterni. L'encryption completo dell'hard drive protegge inoltre i dati in caso di furto o smarrimento di un dispositivo.

L'integrazione disponibile in Kaspersky Total Security for Business protegge anche la collaboration e il file sharing di Microsoft Office 365 e aiuta a prevenire la perdita delle PII (Personal Identification Information).

PROVATELO VOI STESSI

Perché non provate personalmente la nostra protezione adattiva? Visitate questa pagina per una versione di prova gratuita di 30 giorni di Kaspersky Endpoint Security for Business.

Un approccio step-by-step

Costruire solide security foundation per la propria azienda, scegliendo il prodotto o il servizio giusto, è solo il primo passo. La chiave per il successo a lungo termine è sviluppare una strategia lungimirante di cybersecurity aziendale.

Il nostro portfolio soddisfa le esigenze di security delle aziende odierne, rispondendo alle vostre esigenze aziendali indipendentemente dalle dimensioni dell'organizzazione o dal livello di maturità della sicurezza IT, attraverso un approccio graduale esclusivo.

Questo approccio unisce diversi livelli di protezione da tutti i tipi di cyberminacce e aiuta a prevenire automaticamente le minacce, consentendovi in modo metodico e sistematico di aggiungere funzionalità nuove e avanzate per contrastare minacce più sofisticate, di pari passo con la crescita del business. Noi abbiamo una visione globale che vi consente di concentrarvi serenamente sull'innovazione.

---

* (informazioni personali)

Kaspersky Security Foundations

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Embedded System Security
- Kaspersky Security for Storage
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Professional Services
- Kaspersky Premium Support and Professional Services

- Protezione per utenti aziendali e dispositivi mobili
- Sicurezza dei server per ambienti ibridi
- Protezione per VDI (Virtual Desktop Infrastructure)
- Protezione per endpoint tradizionali e PC legacy
- Protezione dal vettore di attacco più comune: l'e-mail
- Protezione all'avanguardia nei confronti delle minacce basate sul web
- Assistenza al deployment, alla configurazione e alla manutenzione

Sfruttate appieno il potenziale dell'ecosistema Kaspersky

Kaspersky Security Foundations

La nostra threat prevention gestita dal cloud consente a ogni organizzazione di bloccare automaticamente le più comuni minacce informatiche su qualsiasi dispositivo, VDI e infrastruttura server ibrida.

- Protegge ogni dispositivo, inclusi endpoint tradizionali e legacy
- Offre visibilità e controllo su ogni risorsa IT
- Aiuta a prevenire o mitigare gli errori degli utenti
- Consente l'automazione della gestione dei sistemi di cui avete bisogno, senza costi eccessivi

Kaspersky Optimum Security

Aiuta a proteggere le aziende dalle minacce nuove, sconosciute ed elusive. Efficace soluzione di threat detection and response, senza sprechi. Monitoraggio della sicurezza 24 ore su 24, 7 giorni su 7, ricerca automatizzata delle minacce e response guidate e gestite con il supporto degli esperti Kaspersky.

- Esegue l'upgrade della protezione degli endpoint da minacce elusive
- Supporta la creazione di processi di incident response essenziali
- Ottimizza l'utilizzo delle risorse di cybersecurity

Kaspersky Expert Security

Progettato per soddisfare le esigenze quotidiane di qualsiasi azienda con una IT security matura nell'affrontare le più sofisticate minacce attuali, comprese le APT (Advanced Persistent Threats) e gli attacchi mirati.

- Ottimizza i carichi di lavoro dei vostri esperti di sicurezza
- Aumenta le loro conoscenze e competenze
- Supporta i vostri esperti

News sulle minacce informatiche:
securelist.com
Notizie relative alla sicurezza IT:
business.kaspersky.it
Sicurezza IT per le PMI:
kaspersky.it/business
Sicurezza IT per le aziende Enterprise:
kaspersky.it/enterprise-security

kaspersky.it

We are proven. We are independent. We are transparent. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia possa migliorare le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Affidatevi alla cybersecurity per un futuro più sicuro.

Maggiori informazioni sono disponibili all'indirizzo kaspersky.it/transparency

Proven. Transparent. Independent.