KASPERSKY lab

PORTFOLIO KASPERSKY FOR SECURITY BUSINESS 2015

"PROTEZIONE AVANZATA PER LE AZIENDE"

Ogni azienda, indipendentemente dalle dimensioni, è soggetta al rischio di minacce malware. Kaspersky Lab consente di individuare e rilevare da un punto di vista esclusivo molte di queste minacce.

Inoltre, Il numero delle minacce è in ascesa. Il malware diretto a singoli utenti e aziende ormai supera la soglia di 325.000 nuove minacce al giorno.

All'interno di Kaspersky Lab diamo la massima importanza a queste minacce e al rischio che comportano per le aziende. Per questo motivo consigliamo alle organizzazioni di assicurarsi che la strategia di sicurezza IT soddisfi tre criteri chiave:

- **In primo luogo**, è necessario avere accesso a un'intelligence avanzata dedicata alle minacce informatiche. Si tratta di conoscere approfonditamente come si presenta, come viene scritta e compilata una minaccia. È importante che il sistema di sicurezza riceva costantemente informazioni specifiche e che i fornitori siano sempre aggiornati grazie ad un costante monitoraggio delle aree di sviluppo del malware.

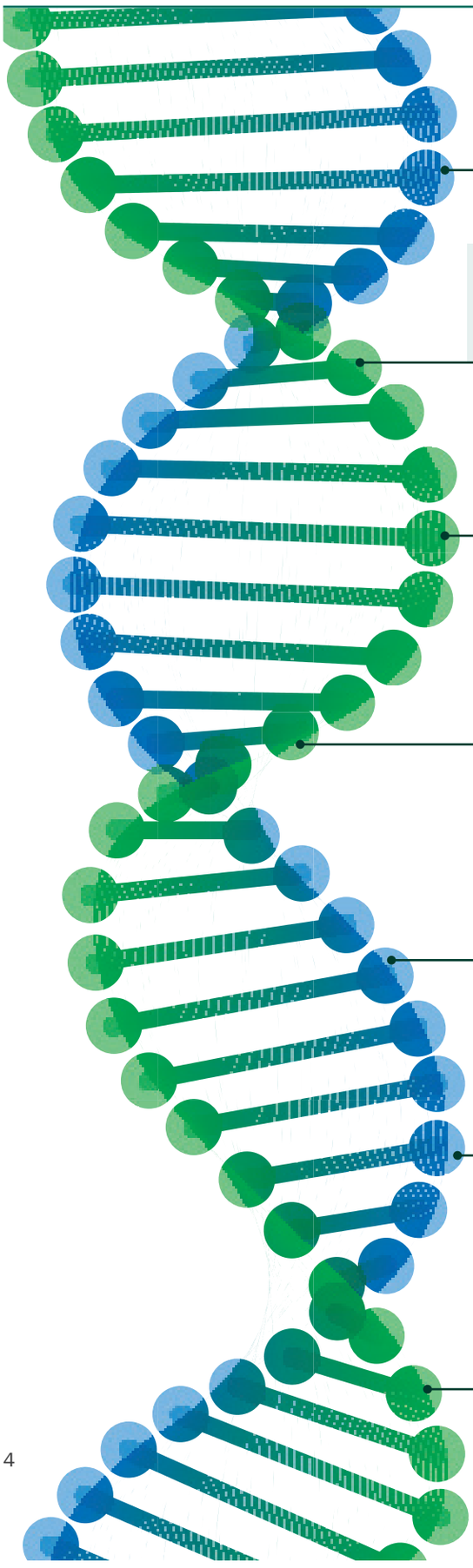
- **In secondo luogo,** è necessario disporre di strumenti e tecniche di sicurezza in grado di rilevare ed eliminare malware noto, sconosciuto e avanzato. Al contempo, il software di sicurezza deve ridurre al minimo il carico di lavoro dei sistemi e mantenere tempi di scansione rapidi per evitare interruzioni nelle attività aziendali.

- **In terzo luogo,** dal momento che gli ambienti IT aziendali diventano sempre più complessi, questa tecnologia va estesa in modo rapido ed efficace agli endpoint fisici, mobili e virtuali, ricorrendo a un'unica piattaforma per evitare conflitti tra i sofware, l'uso di più console o falle di sicurezza.

Solo Kaspersky è in grado di offrire un'intelligence per le minacce informatiche senza paragoni e la tecnologia necessaria per la relativa applicazione, integrata in una piattaforma di sicurezza completa.

Le soluzioni Kaspersky sono progettate con la flessibilità giusta per realizzare gli obiettivi aziendali. In altre parole, siamo sempre pronti a proteggere le aziende dalle minacce destinate a endpoint fisici e virtuali, dispositivi mobili, sistemi di posta, server, gateway e portali Sharepoint. Per avere informazioni sui prodotti, le soluzioni e i servizi illustrati nel presente documento, contattare Kaspersky o il proprio rivenditore IT. Presenteremo le modalità di collaborazione per proteggere le aziende dalle minacce informatiche.

LA TUTELA DELLA SICUREZZA È NEL NOSTRO DNA



Competenza a tutti i livelli

La migliore intelligence per le minacce a livello globale, a cui collabora anche il team GREAT

Una delle organizzazioni più accreditate per la sicurezza

Tecnologia al primo posto

Leader nei test indipendenti

Ricerca avanzata delle minacce complesse

Incidenti di sicurezza prevedibili grazie a Kaspersky Security Network

UNA SICUREZZA CHE FA LA DIFFERENZA

Kaspersky Lab offre la tecnologia anti-malware più potente sul mercato facendo leva sulla migliore intelligence dedicata alla sicurezza, insita nel nostro DNA e cardine delle nostre attività e del nostro modo di operare.

- Mettiamo la tecnologia al primo posto a tutti i livelli, già a partire dal nostro CEO, Eugene Kaspersky.
- Il team Ricerca globale e analisi (GReAT), uno dei gruppi di punta a livello di sicurezza IT, è stato il primo a scoprire molti degli attacchi mirati e minacce malware più pericolosi al mondo.
- Diverse organizzazioni di sicurezza di fama mondiale e forze dell'ordine si sono rivolte attivamente a noi.
- Dal momento che Kaspersky Lab sviluppa e perfeziona interamente tutte le principali tecnologie, i nostri prodotti sono più solidi ed efficaci.
- Ogni anno ci sottoponiamo a molti più test indipendenti di qualsiasi altro fornitore, classificandoci ai primi posti con una frequenza molto più alta di chiunque altro.
- Gli analisti più stimati del settore, tra cui Gartner, Inc, Forrester Research e International Data Corporation (IDC) riconoscono il nostro primato nell'ambito di diverse categorie chiave di sicurezza IT.
- Partner OEM, tra cui Microsoft®, Cisco® Meraki, Juniper Networks, Alcatel Lucent, si avvalgono delle nostre tecnologie nei loro prodotti e servizi.

Tutto questo fa la differenza.

INFORMAZIONI SULLA NOSTRA TECNOLOGIA ANTI-MALWARE

L'efficacia del software di sicurezza IT va di pari passo con quella della tecnologia su cui si basa. Le tecnologie relative a gestione delle patch, MDM, crittografia e controlli sui dispositivi, insieme a molte altre, offrono importanti livelli di sicurezza aggiuntivi. Le organizzazioni non devono scendere a compromessi quando si tratta di proteggersi da minacce note, sconosciute e avanzate.

La tecnologia di sicurezza di Kaspersky Lab viene costantemente alimentata e potenziata da un'intelligence dedicata alle minacce informatiche dinamica e senza paragoni. Ci distinguiamo perché la sicurezza è il nostro obiettivo esclusivo, che perseguiamo con un'esperienza globale e un'intelligence di livello elevato.

L'eccellenza delle prestazioni della tecnologia anti-malware integrata nella piattaforma Kaspersky Endpoint Security for Business è comprovata da continui e numerosi test indipendenti.

Ecco gli elementi che rendono la potente protezione anti-malware di Kaspersky Lab molto più efficace delle altre soluzioni.

CARATTERISTICHE PRINCIPALI DEL PRODOTTO

- **Rilevamento di minacce note, sconosciute e avanzate**
- **Analisi euristica e comportamentale**
- **Kaspersky Security Network per una protezione assistita da cloud**
- **Active Disinfection**
- **Protezione da ransomware e crittografia**
- **Prevenzione automatica degli exploit**
- **HIPS e firewall personale**
- **Network Attack Blocker**
- **Console di gestione semplice e chiara**

CARATTERISTICHE PRINCIPALI

UN APPROCCIO MULTILIVELLO

L'approccio multilivello di Kaspersky Lab è uno dei motivi per cui siamo in grado di offrire la migliore garanzia di sicurezza del settore. Le tecnologie Kaspersky Lab sono sviluppate internamente, rendendo possibile una protezione potente e immediata a più livelli che non compromette in alcun modo le prestazioni.

Ciascun livello di protezione mira a contrastare le minacce informatiche da una prospettiva diversa, consentendo ai professionisti IT di implementare tecnologie strettamente interconnesse fra loro e di garantire una sicurezza estesa e approfondita.

INTELLIGENCE PER LE MINACCE INFORMATICHE SENZA PARAGONI: PROTEZIONE COSTANTE GARANTITA

L'intelligence di Kaspersky Lab, nota a livello globale, applica nelle soluzioni di sicurezza tutte le competenze acquisite, in un'ottica di continua evoluzione per rispondere alle costanti trasformazioni del mondo IT.

FUNZIONALITÀ

SICUREZZA EURISTICA - RIDURRE IL CARICO SUI SISTEMI DEGLI UTENTI

L'identificazione malware basata sul modello offre una maggiore capacità di rilevamento delle minacce.

ANALISI DEL COMPORTAMENTO

Le soluzioni anti-malware di Kaspersky includono due componenti specifici per l'analisi delle attività del programma:

- **Emulatore:** verifica le attività dei programmi prima dell'esecuzione.
- **System Watcher** - monitora le attività dei programmi già in esecuzione, rilevando e analizzando i modelli di comportamento caratteristici del malware.

RILEVAMENTO DI MALWARE ASSISTITO DA CLOUD - KASPERSKY SECURITY NETWORK (KSN)
Una risposta in tempo reale alle minacce malware nuove e sconosciute. Grazie a un flusso costante di nuovi dati sui tentativi di attacchi malware e sui comportamenti sospetti, forniti da oltre 60 milioni di utenti volontari del software Kaspersky Lab, è possibile avere dei verdetti rapidissimi sui file analizzati, per offrire agli utenti una protezione in tempo reale con il minor numero di falsi positivi.

PREVENZIONE AUTOMATICA DEGLI EXPLOIT
La funzione di prevenzione automatica degli exploit si rivolge in modo specifico al malware che sfrutta le vulnerabilità software in applicazioni note, riconoscendo modelli di comportamento tipico o sospetto. Questa tecnologia blocca l'exploit e impedisce l'esecuzione del codice dannoso scaricato.

CONTROMISURE PER IL RANSOMWARE DI CRITTOGRAFIA
System Watcher salva le copie dei file importanti in archivi temporanei, nel caso in cui un processo sospetto tenti di accedervi. Se il ransomware tenta di crittografare gli originali, i file possono essere ripristinati in formato non crittografato.

ACTIVE DISINFECTION
Utilizza diverse tecniche per contrastare le infezioni rilevate, impedendo l'esecuzione di file e processi che prevedono l'avvio automatico, eliminando malware ed eseguendo il rollback dei file archiviati allo stato originario.

SISTEMA DI PREVENZIONE DELLE INTRUSIONI HOST-BASED (HIPS) E FIREWALL PERSONALE
Determinate attività presentano un rischio tale da renderne consigliabile la restrizione, anche se non classificate come dannose. Il sistema (HIPS) di Kaspersky Lab limita le attività all'interno del sistema in base al livello di affidabilità dell'applicazione grazie a un firewall personale a livello delle applicazioni per limitare l'attività di rete.

NETWORK ATTACK BLOCKER
Monitora le attività sospette sulla rete e consente di predefinire la risposta dei sistemi quando viene rilevato un comportamento sospetto.

AGGIORNAMENTI FREQUENTI
Gli aggiornamenti per la protezione dalle nuove minacce malware vengono distribuiti al database di sicurezza tramite il processo di aggiornamento più rapido del settore, unitamente all'aggiornamento costante dei dati sul nuovo malware rilevato del cloud Kaspersky Security Network (KSN).

PROTEZIONE LEADER DI SETTORE - UN DATO DI FATTO

Nel corso del 2014 i prodotti Kaspersky Lab hanno partecipato a **93 test e recensioni indipendenti**. Per **66 volte i nostri prodotti si sono classificati tra i primi tre posti**, ottenendo un **punteggio dei PRIMI 3 posti pari al 71%,** e hanno raggiunto **il 1° posto 51 volte** in oltre la metà dei test.

Nessun prodotto o soluzione concorrente riesce a sfiorare simili risultati.

PRODOTTI, SOLUZIONI E SERVIZI DI SICUREZZA PER LE AZIENDE

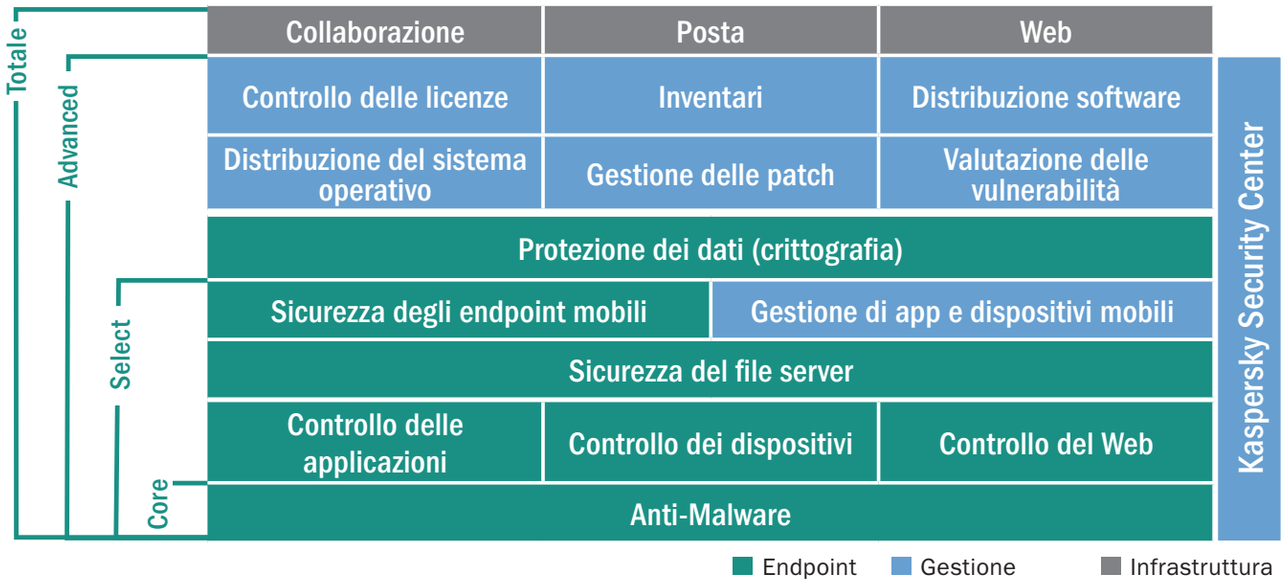
Kaspersky Endpoint Security for Business	Facendo leva sull'ecosistema di intelligence dedicato alle minacce informatiche migliore al mondo, Kaspersky Endpoint Security for Business offre un approccio alla sicurezza su livelli basato su un'unica piattaforma integrata con caratteristiche quali: una solida applicazione, strumenti per il controllo di Web e dispositivi, crittografia dei dati, sicurezza degli endpoint mobili, MDM e gestione di patch e sistemi. Il tutto gestito da un'unica console centralizzata: Kaspersky Security Center. Kaspersky Total Security for Business garantisce inoltre la sicurezza di server Web, di posta e di collaborazione, proteggendo i perimetri e l'intero ambiente IT aziendale.
Soluzioni mirate Kaspersky	Soluzioni standalone che consento l'applicazione della sicurezza Kaspersky Lab ad aree specifiche del sistema IT dell'utente. Alcune soluzioni, come Kaspersky Security for Mobile, sono disponibili anche in Kaspersky Endpoint Security for Business. Altre, come Kaspersky Security for Virtualization, sono disponibili esclusivamente come soluzioni mirate. Si basano tutte sulle stesse tecnologie all'avanguardia e sulla stessa intelligence leader di settore. Tutte le soluzioni di sicurezza per endpoint fisici, mobili e virtuali sono gestite a livello centralizzato tramite Kaspersky Security Center.
Treath Intelligence Services di Kaspersky e soluzioni aziendali	Intelligence dedicata alle minacce informatiche, competenze tecniche, dati e capacità di formazione per una maggiore sicurezza del vostro brand, della vostra organizzazione e dei vostri dipendenti. Le soluzioni aziendali consentono di risolvere i problemi relativi alla sicurezza per infrastrutture e settori specifici, nonché determinate forme di attacco, ad esempio attacchi DDoS (Distributed Denial of Service).
KASPERSKY SMALL OFFICE SECURITY	La protezione di livello mondiale a portata delle piccole aziende
CONTRATTI DI MANUTENZIONE E SUPPORTO	Un'ampia gamma di opzioni di supporto per la soluzione di sicurezza Kaspersky scelta.

INFORMAZIONI SU KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Endpoint Security for Business offre una soluzione di protezione completa, progettata dai massimi esperti di sicurezza al mondo. Garantisce la protezione più profonda e lungimirante, prestazioni efficienti e una gestione intuitiva, che si evolvono gradualmente tramite l'aggiunta di livelli progressivi, per garantire la sicurezza totale della vostra azienda.

Tutti i componenti sono stati testati e realizzati internamente, per dare vita a una singola piattaforma di sicurezza su misura per le esigenze dell'azienda. Il risultato è una soluzione integrata e stabile senza lacune, senza problemi di compatibilità e nessun carico di lavoro supplementare.

Gli amministratori possono optare per la soluzione Kaspersky Endpoint Security per le aziende per osservare, controllare e proteggere con la massima efficienza il loro ambiente IT. Numerosi strumenti e tecnologie vengono forniti in diverse combinazioni equilibrate nei livelli progressivi della soluzione per soddisfare le vostre esigenze IT e di sicurezza in costante evoluzione. Kaspersky può rendere il vostro lavoro molto più semplice.

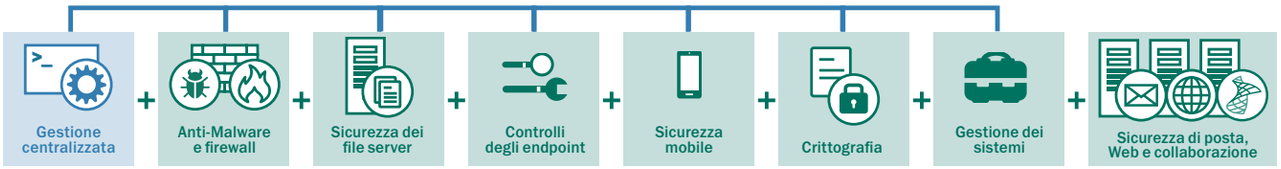


Kaspersky vanta di una gamma completa di tecnologie (interoperabili tra di loro, scritte a partire da una medesima codebase e supportate dal servizio basato su cloud Kaspersky Security Network), per offrire ai clienti l'avanzato livello di protezione di cui hanno bisogno.

In breve, forniamo la prima piattaforma di sicurezza del settore, senza rivali nel mercato, che consente agli amministratori di osservare, controllare e proteggere con la massima semplicità il proprio ambiente IT.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Una potente protezione multilivello da minacce note, sconosciute e avanzate, progettata e realizzata dai principali esperti di sicurezza. Kaspersky Endpoint Security for Business, supportata da un'intelligence dedicata alle minacce nota a livello mondiale, offre un controllo e una sicurezza IT senza paragoni.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS – CORE

Una protezione anti-malware senza confronti: la base della piattaforma di sicurezza Kaspersky Lab

Le tecnologie di protezione a più livelli di Kaspersky Lab vengono sviluppate internamente da veri e propri appassionati della sicurezza. Come confermato dai test indipendenti, il risultato è la soluzione di sicurezza più potente ed efficace del settore, per garantire all'organizzazione la protezione migliore in assoluto.

Protezione dalle minacce note, sconosciute e avanzate - tecnologie esclusive e sofisticate consentono di identificare ed eliminare le minacce esistenti ed emergenti.

Prevenzione automatica degli exploit - le minacce sconosciute e avanzate vengono individuate e mirate in modo proattivo.

Protezione assistita da cloud - vengono usate le informazioni in tempo reale di Kaspersky Security Network.

System Watcher - offre un'esclusiva funzionalità di ripristino dei file in caso di conseguenze sul sistema.

Sistema HIPS (Host-based Intrusion Prevention System) con firewall personale - questo sistema limita le attività in base al livello di affidabilità dell'applicazione, grazie a un firewall dedicato che riduce l'attività di rete.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS - SELECT

Controlli potenti e granulari degli endpoint uniti a una gestione e a una sicurezza proattiva per dispositivi mobili e dati

I controlli per applicazioni, Web e dispositivi, con whitelisting dinamico supportato dall'esclusivo laboratorio interno di Kaspersky, offrono un punto di vista aggiuntivo sulla sicurezza approfondita degli endpoint. È garantita la protezione anche dei dispositivi mobili aziendali o dei dipendenti (BYOD) e le piattaforme sono unificate per essere gestite tramite la console Kaspersky Security Center insieme a tutti gli endpoint protetti. La protezione dei file server impedisce alle infezioni di propagarsi agli endpoint protetti attraverso i dati archiviati.

CONTROLLI DEGLI ENDPOINT

Application Control con whitelisting dinamico - usando le informazioni relative alla reputazione dei file fornite in tempo reale da Kaspersky Security Network, gli amministratori IT possono autorizzare, bloccare o regolare applicazioni, anche in scenari di whitelisting "Default Deny" in ambienti reali o di test. Application Privilege Control e Scansione delle vulnerabilità consentono di monitorare e limitare le applicazioni con comportamenti sospetti.

Web Control - è possibile creare criteri di navigazione in base a categorie preimpostate o personalizzabili per garantire l'efficienza amministrativa e una panoramica globale.

Device Control - è possibile impostare, pianificare e applicare criteri per i dati granulari per controllare la connessione di dispositivi di archiviazione rimovibili e altre periferiche tramite maschere per l'implementazione simultanea in più dispositivi.

SICUREZZA DEL FILE SERVER

Gestita insieme alla sicurezza degli endpoint tramite Kaspersky Security Center.

SICUREZZA MOBILE:

Sicurezza rigorosa per i dispositivi mobili - le tecnologie avanzate, proattive e assistite da cloud si combinano per offrire una protezione degli endpoint mobili multilivello in tempo reale.

Protezione Web, i componenti anti-spam e anti-phishing aumentano ulteriormente la sicurezza dei dispositivi.

Tecnologia antifurto - i comandi Blocco, Cancellazione, Localizzazione GPS, SIM-Watch, Allarme, Scatta foto, Cancellazione selettiva o completa impediscono l'accesso non autorizzato ai dati aziendali in caso di furto o smarrimento di un dispositivo mobile. L'abilitazione per amministratori e utenti finali, insieme al supporto Google Cloud Management, consentono l'attivazione rapida in caso di necessità.

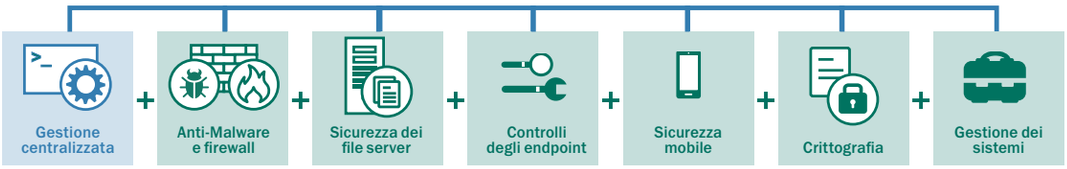
Mobile Application Management (MAM) - controlla e limita l'utente nell'esecuzione delle applicazioni inserite nella whitelist, impedendo l'implementazione di software sconosciuto o indesiderato. La tecnologia di **Application Wrapping** consente di isolare i dati aziendali nei dispositivi di proprietà dei dipendenti. È possibile effettuare da remoto la cancellazione selettiva dei dati o applicare un livello di crittografia aggiuntivo.

Mobile Device Management (MDM) - un'interfaccia unificata per i dispositivi **Microsoft® Exchange ActiveSync** e **iOS MDM** con implementazione dei criteri OTA (Over The Air). **È previsto anche il supporto per dispositivi basati su Samsung KNOX** for Android™.

Portale self-service - consente la registrazione automatica dei dispositivi approvati di proprietà dei dipendenti nella rete con l'installazione automatica di tutte le chiavi e di tutti i certificati necessari, nonché con l'attivazione di emergenza delle funzionalità di protezione contro i furti da parte dell'utente o del proprietario, riducendo il carico di lavoro amministrativo dell'IT.

Kaspersky Endpoint Security for Business - SELECT include anche tutti i componenti del livello CORE.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS - ADVANCED



Gli strumenti di gestione dei sistemi ottimizzano l'efficienza IT e la sicurezza, mentre la crittografia integrata protegge i dati sensibili

La gestione automatizzata delle patch e la gestione delle immagini del sistema operativo, la distribuzione del software da remoto e l'integrazione SIEM contribuiscono a semplificare l'amministrazione, mentre gli inventari hardware e software e la gestione delle licenze garantiscono controllo e stabilità. La tecnologia di crittografia integrata aggiunge un efficace livello di protezione dei dati.

GESTIONE DEI SISTEMI

Gestione di patch e vulnerabilità - rilevamento automatico e definizione delle priorità delle vulnerabilità di applicazioni e sistema operativo, uniti alla rapida distribuzione automatica di patch e aggiornamenti.

Implementazione del sistema operativo - implementazione, cattura e archiviazione centralizzata e semplificata delle "Golden Image", compreso il supporto ai sistemi UEFI.

Distribuzione del software e risoluzione dei problemi - implementazione del software da remoto e aggiornamento di applicazioni e sistema operativo disponibile on-demand o in base a una pianificazione, incluso il supporto Wake-on-LAN. Risoluzione dei problemi rapida e da remoto e distribuzione efficace del software supportate tramite la tecnologia Multicast.

Inventari hardware e software e gestione delle licenze - l'identificazione, la visibilità e il controllo (incluso il blocco), nonché la gestione dell'utilizzo delle licenze, offrono una panoramica più approfondita di tutto l'hardware e il software implementato nell'ambiente, compresi i dispositivi rimovibili. Sono inoltre disponibili la gestione delle licenze software e hardware, il rilevamento dei dispositivi ospiti, i controlli sui privilegi e il provisioning dell'accesso.

Integrazione SIEM - supporto per i sistemi IBM® QRadar e HP ArcSight SIEM.

Controllo dell'accesso basato sui ruoli (RBAC, Role-Based Access Control) - è possibile assegnare responsabilità amministrative in reti complesse tramite visualizzazioni console personalizzate in base ai diritti e ai ruoli assegnati.

CRITTOGRAFIA

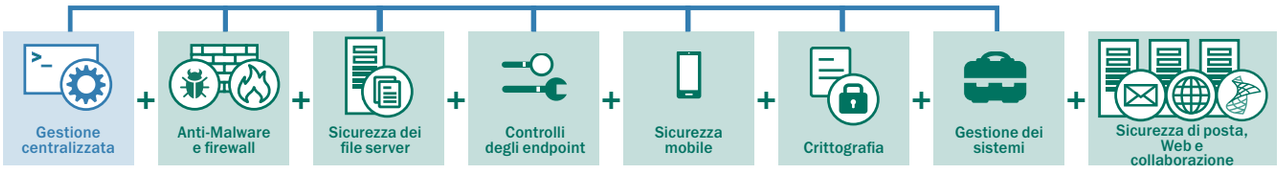
Protezione efficace dei dati - è possibile applicare agli endpoint la crittografia a livello di file e cartelle (FLE) o a livello di disco intero (FDE). Il supporto della "modalità portable" garantisce l'amministrazione della crittografia nei dispositivi esterni ai domini amministrativi.

Accesso utente flessibile - l'Autenticazione Pre-Avvio (Pre-Boot Authentication) per una maggiore sicurezza include la modalità opzionale "Single Sign-on", che garantisce trasparenza. È inoltre disponibile l'autenticazione a 2 fattori o l'autenticazione basata sul token.

Creazione dei criteri integrata - l'integrazione esclusiva della crittografia con i controlli per applicazioni e dispositivi offre un livello aggiuntivo di sicurezza avanzata e semplifica l'amministrazione.

Kaspersky Endpoint Security for Business - ADVANCED include anche tutti i componenti dei livelli SELECT e CORE.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Le organizzazioni che richiedono un sistema di sicurezza globale per il proprio ambiente IT scelgono Kaspersky Total Security for Business

Kaspersky Total Security for Business offre la piattaforma di protezione e gestione più completa attualmente disponibile nel settore. La soluzione Kaspersky Total Security for Business fornisce la protezione di tutti i livelli della rete e include avanzati strumenti di configurazione per migliorare la produttività degli utenti, garantendone la massima protezione contro le minacce malware, indipendentemente dalla loro posizione o dal dispositivo in uso.

SICUREZZA DEL SERVER DI POSTA

Blocca efficacemente le minacce malware basate sulla posta elettronica, gli attacchi di phishing e lo spam, avvalendosi di aggiornamenti in tempo reale basati su cloud per garantire tassi di rilevamento eccezionali e ridurre al minimo i falsi positivi. È inclusa anche la protezione anti-malware per IBM® Domino®. La funzionalità DLP per Microsoft Exchange è disponibile separatamente.

SICUREZZA PER I GATEWAY INTERNET

Garantisce un accesso Internet sicuro a livello dell'intera azienda, tramite la rimozione automatica dei programmi nocivi e potenzialmente ostili nel traffico HTTP(S)/FTP/SMTP e POP3.

SICUREZZA DELLA COLLABORAZIONE

Protegge le farm e i server SharePoint® da tutte le forme di malware. La funzionalità DLP per SharePoint, disponibile separatamente, offre funzionalità di filtro per file e contenuti al fine di identificare i dati riservati e impedirne la fuga.

Kaspersky Total Security for Business include anche tutti i componenti dei livelli ADVANCED, SELECT e CORE.

CARATTERISTICHE DEL PRODOTTO

Qual è la soluzione giusta per la vostra azienda?

	Core	Select	Advanced	Totale	Gestita tramite Security Center	Disponibile in una soluzione mirata
Anti-Malware	●	●	●	●	●	
Firewall	●	●	●	●	●	
Controllo delle applicazioni		●	●	●	●	
Controllo dei dispositivi		●	●	●	●	
Controllo del Web		●	●	●	●	
Sicurezza del file server		●	●	●	●	●
Protezione degli endpoint mobili		●	●	●	●	●
Gestione di app e dispositivi mobili		●	●	●	●	●
Crittografia			●	●	●	
Vulnerability Assesment			●	●	●	●
Gestione delle patch			●	●	●	●
Inventari			●	●	●	●
Controllo delle licenze			●	●	●	●
Distribuzione del software			●	●	●	●
Implementazione dei sistemi operativi			●	●	●	●
Sicurezza dei server di collaborazione				●		●
Sicurezza del server di posta				●	●	●
Sicurezza per i gateway Internet				●		●
Sicurezza dell'infrastruttura virtuale					●	●
Sicurezza dei server di archiviazione					●	●

● Incluso ● Parzialmente incluso (per i dettagli vedere le pagine dedicate ai prodotti)

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server assicura una protezione scalabile, affidabile ed economica per gli archivi di file condivisi, senza effetti rilevabili sulle prestazioni del sistema.

CARATTERISTICHE PRINCIPALI

POTENTE PROTEZIONE ANTI-MALWARE

Il pluripremiato motore anti-malware di Kaspersky garantisce una protezione avanzata dei server, impedendo anche alle più recenti minacce malware note e potenziali di accedere alla rete locale attraverso programmi nocivi o pericolosi.

ALTE PRESTAZIONI E AFFIDABILITÀ

Kaspersky Security for File Server non rallenta visibilmente il sistema, né interferisce con le attività aziendali, nemmeno in presenza di carichi di rete estremamente elevati.

SUPPORTO DI PIÙ PIATTAFORME

Una singola soluzione efficace per le reti di server eterogenee, capace di supportare le piattaforme e i server più recenti, inclusi server terminal, cluster e virtuali, senza alcun problema di compatibilità.

EFFICACIA DI GESTIONE E REPORTING

Strumenti di gestione efficaci e intuitivi, informazioni sullo stato di protezione dei server, impostazioni flessibili per l'orario delle scansioni e un sistema di reporting completo assicurano un controllo efficiente della sicurezza dei file server e al tempo stesso consentono di ridurre il costo di proprietà.

FUNZIONALITÀ

- **Protezione anti-malware in tempo reale** per file server che eseguono le versioni più recenti di Windows® (incluso Windows Server® 2012/R2), Linux® e FreeBSD (entrambi con Samba).
- **Protezione dei server terminal Citrix e Microsoft®.**
- **Supporto completo dei server cluster.**
- **Scalabilità** - supporta e protegge con facilità anche le infrastrutture eterogenee più complesse.
- **Affidabilità, stabilità ed elevata tolleranza di errore.**
- **Tecnologia di scansione intelligente ottimizzata,** che include la scansione on-demand e delle aree critiche del sistema.
- **Le aree affidabili** consentono di aumentare le prestazioni della protezione e al tempo stesso riducono la quantità di risorse necessaria per la scansione.
- **Backup e quarantena** dei dati prima della disinfezione o eliminazione.
- **Isolamento** delle workstation infette.
- **Installazione, gestione e aggiornamenti centralizzati** con opzioni di configurazione flessibili.
- **Scenari flessibili di risposta agli incidenti.**
- **Report esaustivi** sullo stato di protezione della rete.
- **Sistema di notifica sullo stato delle applicazioni.**
- **Supporto dei sistemi HSM** (Hierarchical Storage Management).
- **Supporto collaudato per desktop Hyper-V e Xen.**
- **Supporto per ambienti VMware**
- **Supporto di ReFS.**

Kaspersky Security for File Server è incluso in Kaspersky Endpoint Security for Business (SELECT e ADVANCED) e in Kaspersky Total Security for Business, ma risulta disponibile per l'acquisto anche separatamente come soluzione mirata.

INFORMAZIONI SULLA NOSTRA TECNOLOGIA DI CONTROLLO DEGLI ENDPOINT

Efficaci strumenti di controllo degli endpoint, strettamente integrati con soluzioni anti-malware all'avanguardia e l'unico laboratorio di whitelisting dedicato del settore, consentono di proteggere le aziende dalle minacce del contesto attuale, in continua evoluzione.

PROTEZIONE, APPLICAZIONE, CONTROLLO

- Le vulnerabilità nelle applicazioni attendibili, il malware basato sul Web e la mancanza di controllo sulle periferiche contribuiscono a un panorama sempre più complesso a livello di minacce. Gli strumenti per il controllo di applicazioni, Web e dispositivi di Kaspersky Lab consentono il controllo completo sugli endpoint senza compromettere la produttività.

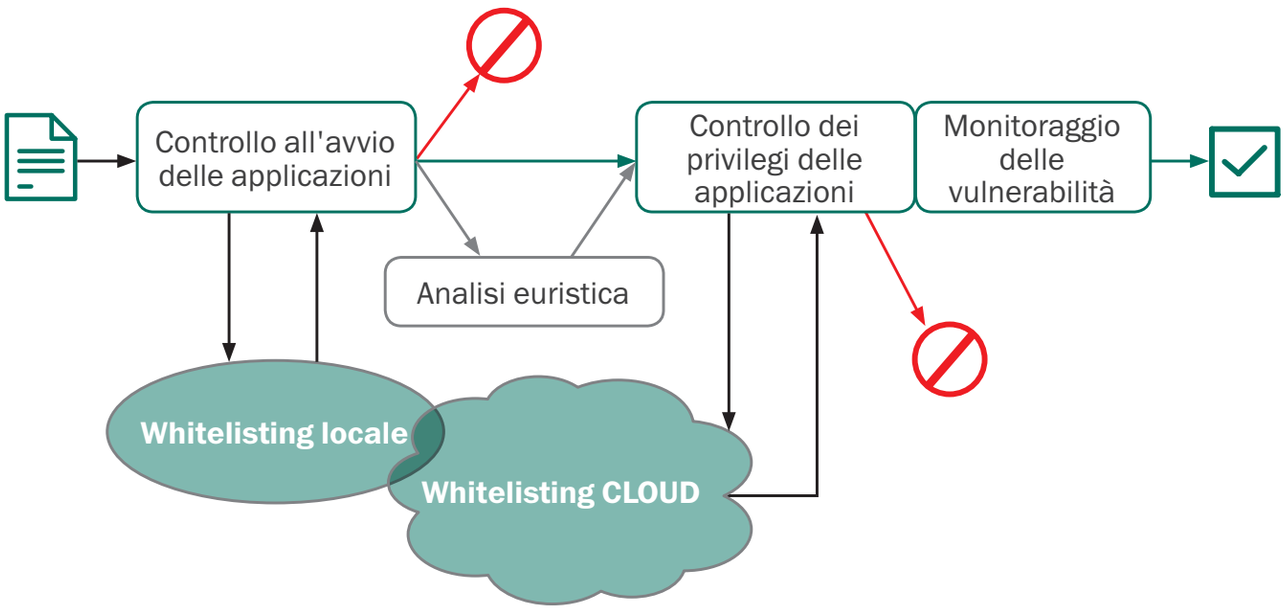
APPLICATION CONTROL E WHITELISITING DINAMICO

Proteggere i sistemi dalle minacce note e sconosciute è possibile affidando agli amministratori il controllo totale su applicazioni e programmi che possono essere eseguiti sugli endpoint, indipendentemente dal comportamento dell'utente finale. Inoltre, è possibile abilitare il monitoraggio dell'integrità delle applicazioni per valutarne il comportamento e impedire l'esecuzione di azioni impreviste che possono compromettere l'endpoint o la rete. Con la creazione e l'applicazione dei criteri di tipo semplificato, personalizzabile o automatico è possibile:

- **Controllo avvio applicazioni**: autorizzare, bloccare e controllare l'avvio delle applicazioni. Incrementare la produttività limitando l'accesso a quelle non correlate alle attività lavorative.
- **Controllo privilegi applicazioni**: regolare e controllare l'accesso delle applicazioni a dati e risorse di sistema. Classificare le applicazioni come attendibili, non attendibili o con restrizioni. Gestire l'accesso delle applicazioni ai dati crittografati sugli endpoint, ad esempio le informazioni pubblicate tramite browser Web o Skype.
- **Application Vulnerability Scanning**: difesa proattiva contro gli attacchi mirati a vulnerabilità presenti nelle applicazioni attendibili.

La maggior parte delle soluzioni di controllo offre esclusivamente la funzionalità di base relativa al blocco o all'accesso. Gli strumenti di Kaspersky Lab utilizzano in modo esclusivo i database per il whitelisting basati sul cloud, consentendo l'accesso quasi in tempo reale ai dati più recenti dell'applicazione.

Le tecnologie di controllo delle applicazioni di Kaspersky Lab utilizzano database per il whitelisting basati sul cloud per analizzare e monitorare le applicazioni in ogni fase: download, installazione, esecuzione.



Il whitelisting dinamico, che può essere abilitato tramite "Default Deny" globale, blocca tutte le applicazioni che tentano l'esecuzione in qualsiasi workstation, a meno che gli amministratori non abbiano dato il consenso esplicito.
Kaspersky Lab è l'unica azienda nel campo della sicurezza con un laboratorio dedicato per il whitelisting, in cui viene gestito un database costantemente monitorato e aggiornato di oltre 500 milioni di programmi.

Lo strumento Default Deny di Kaspersky Lab **può essere applicato in un ambiente di test**, consentendo agli amministratori di stabilire la legittimità delle applicazioni prima di bloccarle. Inoltre, è possibile creare categorie di applicazioni basate sulle firme digitali, impedendo agli utenti di avviare software legittimo modificato dal malware o proveniente da una fonte sospetta.

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 dalla stessa console tramite un'unica interfaccia.

CONTROLLI WEB
Monitorare, filtrare e controllare i siti Web a cui gli utenti finali possono accedere sul lavoro, aumentando la produttività e proteggendo da attacchi e malware web-based.

I controlli Web avanzati di Kaspersky Lab si basano su una directory sempre aggiornata di siti Web, raggruppati in categorie (ad esempio siti Web per adulti, giochi, social network, siti di gioco d'azzardo). Gli amministratori possono creare facilmente criteri per impedire, limitare o controllare l'utilizzo di singoli siti o categorie di siti da parte dell'utente finale, nonché creare elenchi personalizzati. L'accesso ai siti dannosi viene automaticamente bloccato.

Limitandone l'utilizzo, i controlli Web di Kaspersky Lab consentono di impedire la perdita dei dati tramite social network e servizi di messaggistica istantanea. I criteri flessibili consentono agli amministratori di autorizzare la navigazione in determinati orari della giornata. Grazie all'integrazione con Active Directory i criteri possono essere applicati in maniera semplice e rapida a livello dell'intera organizzazione.

Per una maggiore sicurezza, i controlli Web di Kaspersky Lab vengono abilitati direttamente nell'endpoint, quindi i criteri vengono applicati anche quando l'utente non è connesso alla rete aziendale.

CONTROLLO DISPOSITIVI
La disabilitazione di una porta USB non permette sempre di risolvere i problemi dei dispositivi rimovibili. Una porta USB disabilitata, ad esempio, ha conseguenze su altre misure di sicurezza, ad esempio l'accesso VPN basato sul token.

Il controllo dispositivi di Kaspersky Lab consente un livello di controllo più granulare, mantenendo la produttività dell'utente finale e ottimizzando la sicurezza. I controlli possono essere anche in base al numero di serie del dispositivo.

- Impostare le autorizzazioni di connessione/lettura/scrittura per i dispositivi, nonché la pianificazione temporale.
- Creare regole di controllo dei dispositivi basate su maschere, eliminando la necessità di una connessione fisica per l'inserimento nella whitelist. Inserire nella whitelist più dispositivi contemporaneamente.
- Controllare lo scambio di dati tramite dispositivi rimovibili all'interno e all'esterno dell'organizzazione, riducendo il rischio di furto o smarrimento dei dati.
- Eseguire l'integrazione con le tecnologie di crittografia di Kaspersky Lab per applicare i criteri di crittografia in determinati tipi di dispositivo.

La tecnologia di controllo degli endpoint è presente in Kaspersky Endpoint Security for Business (SELECT e ADVANCED) e in Kaspersky Total Security for Business.

KASPERSKY SECURITY FOR MOBILE

I dispositivi mobili stanno diventando sempre più allettanti per i cybercriminali. Al contempo, l'approccio "Bring Your Own Device" (BYOD) sta contribuendo ad arricchire la varietà dei dispositivi, comportando una gestione e un ambiente di controllo più impegnativi per gli amministratori IT.

Kaspersky Security for Mobile garantisce la protezione dei dispositivi ovunque, tutelandoli dal malware mobile in continua evoluzione. È possibile acquisire in modo semplice e rapido visibilità e controllo su smartphone e tablet del proprio ambiente, da un'unica posizione centralizzata e riducendo al minimo le interruzioni.

CARATTERISTICHE PRINCIPALI DEL PRODOTTO

- **Potente protezione anti-malware**
- **Anti-Phishing e Anti-Spam**
- **Protezione Web**
- **Controllo delle applicazioni**
- **Rilevamento dei tentativi di rooting e jailbreaking**
- **Containerization**
- **Protezione contro i furti**
- **Mobile Device Management**
- **Portale self-service**
- **Gestione centralizzata**
- **Console Web**
- **Piattaforme supportate:**
  - **Android™**
  - **iOS**
  - **Windows® Phone**

CARATTERISTICHE PRINCIPALI

ANTI-MALWARE AVANZATO PER LA SICUREZZA DI DATI E DISPOSITIVI MOBILI

Nel 2014 Kaspersky Lab ha fatto fronte a circa 1,4 milioni di attacchi diversi di malware mobile. Kaspersky Security for Mobile combina l'anti-malware con livelli profondi di tecnologie di protezione, che tutelano dalle minacce note e sconosciute rivolte ai dati archiviati nei dispositivi mobili.

MOBILE DEVICE MANAGEMENT (MDM)

L'integrazione con tutte le principali piattaforme di gestione dei dispositivi mobili consente il controllo e l'implementazione OTA (Over the Air) da remoto, per una maggiore semplicità di utilizzo e gestione dei dispositivi Android, iOS e Windows Phone.

MOBILE APPLICATION MANAGEMENT (MAM)

La tecnologia di Containerization e le funzionalità di cancellazione selettiva consentono la separazione dei dati aziendali e personali nello stesso dispositivo, a supporto degli approcci BYOD. La combinazione con la funzionalità di crittografia e la tecnologia anti-malware rende Kaspersky Security for Mobile una soluzione di protezione mobile proattiva anziché una semplice strategia di isolamento di un dispositivo e dei relativi dati.

GESTIONE CENTRALIZZATA

Consente di gestire più piattaforme e dispositivi dalla stessa console di altri endpoint, aumentando la visibilità e il controllo senza ulteriori tecnologie da gestire.

FUNZIONI DI SICUREZZA E GESTIONE MOBILI

POTENTE PROTEZIONE ANTI-MALWARE

Protezione basata sulla firma, proattiva e assistita da cloud (tramite Kaspersky Security Network - KSN) dalle minacce malware mobili note e sconosciute. Le scansioni programmate e on-demand si combinano agli aggiornamenti automatici per aumentare il livello di protezione.

ANTI-PHISHING E ANTI-SPAM

Efficaci tecnologie Anti-Phishing e Anti-Spam proteggono il dispositivo e i relativi dati dagli attacchi di phishing e consentono di filtrare le chiamate e i messaggi di testo indesiderati.

WEB CONTROL/SAFE BROWSER
Queste tecnologie, supportate da Kaspersky Security Network (KSN), operano in tempo reale per bloccare l'accesso a siti Web dannosi e non autorizzati. Safe Browser offre analisi di reputazione sempre aggiornate e garantisce una navigazione sicura da dispositivi mobili.

CONTROLLO DELLE APPLICAZIONI
Integrata con KSN, la funzionalità Application Control limita l'utilizzo delle applicazioni esclusivamente al software approvato, impedendo l'utilizzo del software non autorizzato o sconosciuto. È possibile fare in modo che la funzionalità del dispositivo dipenda dall'installazione delle applicazioni richieste. Il controllo dell'inattività delle applicazioni consente agli amministratori di richiedere all'utente di eseguire nuovamente l'accesso se un'applicazione è inattiva da un determinato periodo di tempo. In questo modo i dati vengono protetti anche se un'applicazione è aperta al momento del furto o dello smarrimento del dispositivo.

RILEVAMENTO DEI TENTATIVI DI ROOTING E JAILBREAKING
Il rilevamento e il reporting automatici dei tentativi di rooting e jailbreaking possono comportare il blocco automatico dell'accesso ai contenitori, la cancellazione selettiva o la cancellazione dell'intero dispositivo.

CONTAINERIZATION
Consente di separare i dati aziendali da quelli personali "isolando" le applicazioni in contenitori. È possibile applicare criteri aggiuntivi, ad esempio di crittografia, per proteggere i dati sensibili. La cancellazione selettiva consente di eliminare i dati nei contenitori presenti in un dispositivo quando un dipendente lascia l'organizzazione, senza conseguenze sui dati personali.

PROTEZIONE CONTRO I FURTI
Le funzionalità di protezione contro i furti da remoto, tra cui Cancellazione, Blocco Dispositivo, Localizzazione GPS, SIM-Watch, Scatta foto, Allarme e rilevamento del dispositivo, possono essere attivate in caso di furto o smarrimento del dispositivo. A seconda della situazione, i comandi di protezione contro i furti possono essere applicati in modo molto flessibile. L'integrazione con Google Cloud Messaging (GCM), ad esempio, permette di inviare i comandi quasi immediatamente, aumentando i tempi di reazione e migliorando la sicurezza, mentre l'invio dei comandi tramite il portale self-service non richiede l'intervento dell'amministratore.

MOBILE DEVICE MANAGEMENT (MDM)
Il supporto di Microsoft® Exchange ActiveSync, Apple MDM e Samsung KNOX 2.0 consente l'applicazione di un'ampia gamma di criteri tramite un'interfaccia unificata, indipendentemente dalla piattaforma. Alcuni esempi includono l'applicazione di crittografia e password o il controllo dell'utilizzo della fotocamera, l'applicazione dei criteri a singoli utenti o gruppi e la gestione delle impostazioni APN/VPN.

PORTALE SELF-SERVICE
Consente di delegare la gestione della sicurezza di routine ai dipendenti, nonché di abilitare la registrazione automatica dei dispositivi approvati. Durante il processo di abilitazione dei nuovi dispositivi, tutti i certificati necessari possono essere inviati automaticamente tramite il portale, senza l'intervento dell'amministratore. In caso di smarrimento del dispositivo, il dipendente può eseguire tutte le azioni di protezione contro i furti disponibili tramite il portale.

GESTIONE CENTRALIZZATA
È possibile gestire tutti i dispositivi mobili a livello centralizzato, da un'unica console, gestendo anche la sicurezza IT di tutti gli altri endpoint. Console Web consente agli amministratori di controllare e gestire i dispositivi da remoto, da qualsiasi computer.

Kaspersky Security for Mobile è incluso in Kaspersky Endpoint Security for Business (SELECT e ADVANCED) e in Kaspersky Total Security for Business, ma risulta disponibile per l'acquisto anche separatamente come soluzione mirata.

INFORMAZIONI SULLA NOSTRA TECNOLOGIA ENCRYPTION

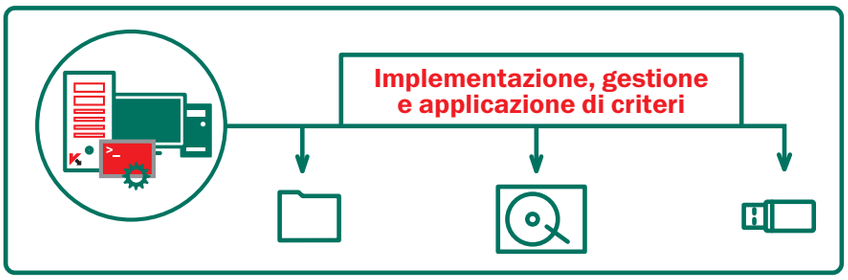
Impedire l'accesso non autorizzato ai dati in seguito a furto o smarrimento del dispositivo oppure ad attacchi malware mirati al furto dei dati.

La conformità e la protezione proattiva dei dati sono un imperativo globale. La tecnologia di crittografia di Kaspersky Lab protegge i dati importanti dalla perdita accidentale, dal furto del dispositivo e da attacchi malware mirati. Attraverso la combinazione di un'efficace tecnologia di crittografia con le tecnologie di protezione degli endpoint leader di settore di Kaspersky Lab, la nostra piattaforma integrata è in grado di proteggere i dati inattivi e in movimento.

Dal momento che si tratta di una soluzione Kaspersky Lab, può essere facilmente implementata e amministrata dalla console di gestione centralizzata tramite l'uso di un unico criterio.

Con la tecnologia di crittografia di Kaspersky Lab è possibile impedire la perdita dei dati e l'accesso non autorizzato alle informazioni:

- **Crittografia Disco Intero (FDE, Full Disk Encryption)**
- **Crittografia a livello di file e cartelle (FLE, File/Folder Level Encryption)**
- **Dispositivi rimovibili e interni**



AMMINISTRATI DA UN'UNICA CONSOLE DI GESTIONE

INDUSTRY STANDARD SECURE CRYPTOGRAPHY

Kaspersky Lab utilizza la crittografia AES (Advanced Encryption Standard) con chiave a 256 bit insieme alla gestione semplificata. Supporta la tecnologia Intel® AES-NI e le piattaforme UEFI e GPT.

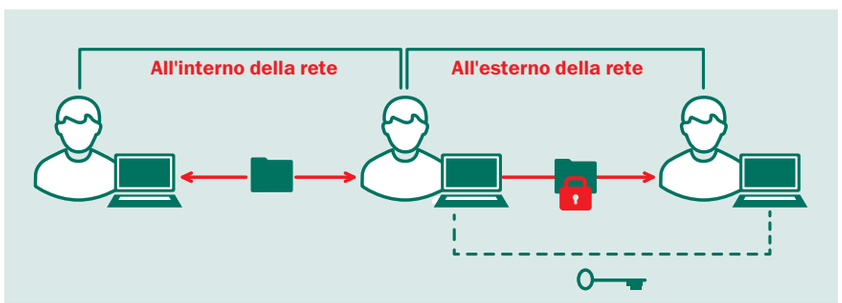
FLESSIBILITÀ TOTALE

Kaspersky Lab offre la crittografia a livello di file e cartelle (FLE) e di disco intero (FDE), per coprire tutti i possibili scenari di utilizzo. La protezione dei dati è garantita su dischi rigidi e dispositivi rimovibili. La "modalità portatile" consente l'utilizzo e il trasferimento dei dati su supporti rimovibili crittografati, persino su computer in cui non è installato nessun software di crittografia, agevolando uno scambio di dati sicuro all'esterno del perimetro.

SINGLE SIGN-ON, TRASPARENZA PER L'UTENTE FINALE

Dalla configurazione all'utilizzo quotidiano, la tecnologia di crittografia di Kaspersky Lab viene eseguita in modo trasparente in tutte le applicazioni, senza ostacolare la produttività dell'utente finale. Il metodo Single Sign-on garantisce una crittografia immediata, al punto che l'utente potrebbe non accorgersi che la tecnologia è in esecuzione.

La crittografia di Kaspersky Lab consente di trasferire i file in modo immediato e trasparente fra gli utenti all'interno e all'esterno della rete.



FUNZIONALITÀ DI CRITTOGRAFIA

INTEGRAZIONE IMMEDIATA CON LE TECNOLOGIE DI SICUREZZA KASPERSKY LAB

Integrazione completa con le tecnologie anti-malware e di gestione e con i controlli sugli endpoint di Kaspersky Lab per un'autentica sicurezza multilivello basata su una codebase comune. Un singolo criterio può ad esempio applicare la crittografia in determinati dispositivi rimovibili. È possibile applicare le impostazioni di crittografia con lo stesso criterio degli elementi di sicurezza degli endpoint, come gli elementi anti-malware o di controllo sui dispositivi. Non è necessario implementare e gestire soluzioni separate. La compatibilità dell'hardware di rete viene verificata automaticamente prima dell'implementazione della crittografia, mentre il supporto delle piattaforme UEFI e GPT è di tipo standard.

CONTROLLO DELL'ACCESSO BASATO SUI RUOLI

Nelle grandi organizzazioni, è consigliabile scegliere di delegare la gestione della crittografia tramite la funzionalità di controllo dell'accesso basato sui ruoli. In questo modo la gestione della crittografia risulta meno complessa.

AUTENTICAZIONE PRE-AVVIO (PBA, PRE-BOOT AUTHENTICATION)

Vengono richieste le credenziali dell'utente ancor prima dell'avvio del sistema operativo, offrendo una maggiore sicurezza con modalità Single Sign-on opzionale. La tecnologia di crittografia PBA di Kaspersky Lab è inoltre disponibile per i layout di tastiera non QWERTY.

AUTENTICAZIONE TRAMITE SMARTCARD E TOKEN

Supporta l'autenticazione a due fattori tramite comuni modelli di smartcard e token, eliminando la necessità di nomi utente e password aggiuntivi e potenziando l'esperienza dell'utente finale.

RIPRISTINO DI EMERGENZA

Gli amministratori possono decrittografare i dati in caso di errore hardware o software. Il ripristino della password dell'utente per l'autenticazione pre-avvio o per l'accesso ai dati crittografati viene implementato tramite un semplice meccanismo di challenge/response.

IMPLEMENTAZIONE OTTIMIZZATA, IMPOSTAZIONI PERSONALIZZABILI

Per semplificare l'implementazione, la funzionalità di crittografia di Kaspersky Lab è abilitata soltanto per i livelli Advanced e Total di Kaspersky Endpoint Security for Business e non è richiesta l'installazione separata. Le impostazioni di crittografia sono predefinite ma personalizzabili per cartelle comuni come Documenti, Desktop, nuove cartelle, estensioni file e gruppi, ad esempio gli archivi di messaggi o i documenti Microsoft® Office.

La tecnologia di crittografia è presente in Kaspersky Endpoint Security for Business (ADVANCED) e in Kaspersky Total Security for Business.

KASPERSKY SYSTEMS MANAGEMENT

Gli strumenti per la gestione IT centralizzata consentono di ottimizzare la sicurezza e ridurre la complessità.

Le vulnerabilità non corrette presenti nelle comuni applicazioni rappresentano una delle minacce più incombenti per la sicurezza IT aziendale. A questo rischio si aggiunge la crescente complessità IT: infatti non è facile applicare una protezione efficace senza sapere di preciso di cosa si dispone.

Attraverso la centralizzazione e l'automazione delle attività fondamentali di sicurezza, configurazione e gestione, ad esempio la valutazione delle vulnerabilità, la distribuzione di patch e aggiornamenti, la gestione dell'inventario e le distribuzioni delle applicazioni, gli amministratori IT possono non solo risparmiare tempo, ma anche ottimizzare la sicurezza.

Kaspersky Systems Management consente di ridurre al minimo i rischi per la sicurezza IT e semplificarne la complessità, offrendo ai responsabili il controllo totale e in tempo reale e la visibilità rispetto a più dispositivi, applicazioni e utenti da un'unica schermata.

CARATTERISTICHE PRINCIPALI DEL PRODOTTO

- **Valutazione delle vulnerabilità e gestione delle patch**
- **Inventari hardware e software**
- **Installazione del software e risoluzione dei problemi da remoto con estensione agli uffici remoti**
- **Implementazione dei sistemi operativi**
- **Integrazione SIEM**
- **Controllo dell'accesso basato sui ruoli**
- **Gestione centralizzata**

OTTIMIZZAZIONE DELLA SICUREZZA

È possibile aumentare la sicurezza IT e ridurre i carichi delle attività di routine con l'applicazione puntuale e automatica di patch e aggiornamenti. Il rilevamento automatico delle vulnerabilità e l'assegnazione delle priorità consentono una maggiore efficienza e riducono il carico sulle risorse. I test indipendenti[1] dimostrano che Kaspersky Lab offre un'elevata capacità di applicazione completa e automatica di patch e aggiornamenti nel più breve tempo possibile.

CONTROLLO CON VISIBILITÀ COMPLETA

Grazie alla visibilità completa della rete da una singola console, gli amministratori possono essere a conoscenza di ogni dispositivo e applicazione che accede alla rete, inclusi i dispositivi ospiti. Questa visibilità permette il controllo centralizzato dell'accesso di utenti e dispositivi ai dati e alle applicazioni dell'organizzazione, in linea con i criteri IT.

GESTIONE CENTRALIZZATA

Kaspersky Lab Systems Management è un componente gestito di Kaspersky Security Center. Ogni funzionalità è accessibile e gestibile tramite questa console centralizzata, con l'utilizzo di interfacce e comandi coerenti e intuitivi per automatizzare le attività IT di routine.

FUNZIONALITÀ

VALUTAZIONE DELLE VULNERABILITÀ E GESTIONE DELLE PATCH

La scansione software automatica consente il rilevamento rapido delle vulnerabilità, l'assegnazione delle relative priorità e la correzione. Patch e aggiornamenti possono essere distribuiti automaticamente, nel più breve intervallo di tempo possibile[2], per software Microsoft® e non Microsoft. L'amministratore viene informato sullo stato di installazione delle patch. Le correzioni non critiche possono essere eseguite dopo l'orario di ufficio, anche a computer spenti, tramite Wake-on-LAN. La

1, 2 Test sulle soluzioni di gestione delle patch commissionato da Kaspersky Lab ed eseguito da AV-TEST GmbH (luglio 2013)

trasmissione Multicast consente la distribuzione locale di patch e aggiornamenti agli uffici remoti, riducendo i requisiti di larghezza di banda.

INVENTARI HARDWARE E SOFTWARE
Individuazione automatica, inventario, notifica e monitoraggio di hardware e software, anche dei dispositivi rimovibili, offrono agli amministratori una visione dettagliata su dispositivi e risorse utilizzati nella rete aziendale. I dispositivi ospiti possono essere individuati e dotati di accesso a Internet. Il controllo delle licenze garantisce visibilità rispetto al numero di nodi e alla data di scadenza.

PROVISIONING FLESSIBILE DI SISTEMI OPERATIVI E APPLICAZIONI
Creazione centralizzata e semplificata, archiviazione, clonazione e implementazione di immagini di sistema con livelli ottimali di sicurezza. Implementazione dopo l'orario di ufficio tramite Wake-On-LAN con modifica successiva all'installazione per una maggiore flessibilità. Supporto UEFI.

DISTRIBUZIONE DEL SOFTWARE
Implementazione e aggiornamento da remoto da un'unica console. È possibile installare automaticamente oltre 100 applicazioni note individuate da Kaspersky Security Network, anche dopo l'orario di lavoro. Supporto completo della risoluzione dei problemi da remoto, con sicurezza ottimizzata tramite autorizzazioni utente e registri o verifiche delle sessioni. Con la tecnologia Multicast per la distribuzione software locale è possibile ottimizzare il traffico relativo agli uffici remoti.

INTEGRAZIONE SIEM
Consente di eseguire direttamente il reporting ed effettuare trasferimenti di eventi in importanti sistemi SIEM, come IBM® QRadar e HP ArcSight. È possibile raccogliere log e altri dati relativi alla sicurezza a scopi di analisi, riducendo al minimo gli strumenti e il carico di lavoro dell'amministratore e semplificando il reporting di livello enterprise.

CONTROLLO DELL'ACCESSO BASATO SUI RUOLI
Consente di distinguere responsabilità e ruoli amministrativi in reti complesse. In base a ruoli e diritti è possibile personalizzare la visualizzazione della console.

GESTIONE CENTRALIZZATA
Una console di amministrazione integrata, Kaspersky Security Center, supporta l'amministrazione della sicurezza di sistema per desktop, dispositivi mobili ed endpoint virtuali della rete tramite un'unica interfaccia.

Kaspersky Systems Management è presente in Kaspersky Endpoint Security for Business (ADVANCED) e in Kaspersky Total Security for Business, ma risulta disponibile per l'acquisto anche separatamente come soluzione mirata.

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server assicura una protezione eccezionale del traffico che attraversa i server di posta, da spam, phishing e minacce malware sia generiche che avanzate, anche nelle infrastrutture eterogenee più complesse.

La protezione dalla perdita di dati riservati in messaggi e-mail e allegati è disponibile anche per ambienti Microsoft® Exchange Server.

CARATTERISTICHE PRINCIPALI

PROTEZIONE DALLE MINACCE MALWARE

Avvalendosi del supporto in tempo reale del modulo basato su cloud Kaspersky Security Network, il pluripremiato motore anti-malware di Kaspersky garantisce una potente protezione dal malware, la protezione proattiva dagli exploit e il filtraggio degli URL nocivi.

PROTEZIONE ANTI-SPAM

Per i server di posta basati su Microsoft Exchange e Linux®, il motore anti-spam assistito da cloud di Kaspersky ha dimostrato di riuscire a bloccare il 99,96% dello spam, che comporta un inutile spreco di tempo e risorse, con un numero minimo di falsi positivi.

CONTROLLO E PROTEZIONE DALLA PERDITA DI DATI (SERVER MICROSOFT EXCHANGE)*

Rilevando l'inserimento di dati aziendali, finanziari, personali e di altri dati sensibili negli allegati e nei messaggi e-mail in uscita sui server Microsoft Exchange e controllando il flusso di tali informazioni, Kaspersky Security for Mail Server protegge i dati riservati di aziende e dipendenti, in conformità con le leggi in materia di protezione dei dati. Elaborate tecniche analitiche, fra cui ricerche di dati strutturati e glossari specifici di settore, consentono di individuare i messaggi e-mail sospetti da bloccare. Il sistema è addirittura in grado di avvisare il responsabile di linea del mittente della potenziale violazione in materia di sicurezza dei dati.

AMMINISTRAZIONE SEMPLICE E FLESSIBILE

Gli intuitivi strumenti di gestione e reporting, insieme alle impostazioni di scansione flessibili, garantiscono un controllo efficiente della sicurezza di posta e documenti, permettendo di ridurre il costo totale.

FUNZIONALITÀ

- Protezione anti-malware in tempo reale, supportata dal modulo basato su cloud Kaspersky Security Network.
- Protezione immediata dagli exploit sconosciuti e persino dalle vulnerabilità zero-day.
- Protezione avanzata contro lo spam: il motore anti-spam di Kaspersky Lab blocca più del 99% del traffico e-mail indesiderato.
- Protezione dalla fuoriuscita di dati (server Microsoft Exchange)*. Rilevamento di informazioni riservate in messaggi e-mail e allegati tramite categorie (tra cui dati personali e dettagli delle carte di credito), glossari e analisi approfondite utilizzando i dati strutturati.
- Scansione anti-spam in tempo reale assistita da cloud di tutti i messaggi sui server Microsoft® Exchange, incluse le cartelle pubbliche, tramite Kaspersky Security Network.
- Scansione programmata di e-mail e database Lotus Domino.
- Scansione di messaggi, database e altri oggetti su server IBM® Domino®.
- Filtraggio dei messaggi in base al riconoscimento del formato, delle dimensioni e del nome degli allegati.
- Processo semplice e pratico di aggiornamento dei database anti-malware e anti-spam.
- Archiviazione dei backup dei dati prima della disinfezione o della rimozione.
- Scalabilità e tolleranza di errore.
- Installazione semplificata e amministrazione integrata flessibile.
- Avanzato sistema di notifica.
- Report esaustivi sullo stato di protezione della rete.

*Durante l'acquisto del prodotto, l'opzione per impedire la perdita o la fuga di dati riservati è in vendita separatamente.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway è una soluzione anti-malware di altissimo livello, che garantisce un accesso a Internet sicuro e costante all'intera forza lavoro.

CARATTERISTICHE PRINCIPALI

UNA PROTEZIONE EFFICACE, CHE RIDUCE DISSERVIZI E TEMPI DI INATTIVITÀ

Il pluripremiato motore anti-malware di Kaspersky Lab impedisce alle più recenti minacce malware note e potenziali di accedere alla rete locale attraverso programmi nocivi o pericolosi.

PRESTAZIONI EFFICIENTI GRAZIE ALL'OTTIMIZZAZIONE

L'intelligente tecnologia di scansione ottimizzata e il bilanciamento del carico, permettendo di risparmiare preziosa larghezza di banda senza accettare compromessi in termini di prestazioni di sicurezza.

SUPPORTO DI PIÙ PIATTAFORME

Grazie al supporto dei server e delle piattaforme più recenti, inclusi i server proxy, è l'ideale per gli ambienti eterogenei con volumi di traffico di rete estremamente elevati. Il supporto di Microsoft® Forefront® TMG si estende all'e-mail aziendale e alla protezione dei gateway Web.

GESTIONE E REPORTING SEMPLIFICATI

Strumenti di gestione semplici e intuitivi, impostazioni di scansione flessibili e sistemi di reporting sullo stato della protezione.

FUNZIONALITÀ

- **Protezione proattiva e costante** per minacce sconosciute ed emergenti.
- **Percentuali di rilevamento malware eccezionali** e numero minimo di falsi positivi.
- **Tecnologia di scansione intelligente ottimizzata.**
- **Scansione in tempo reale** del traffico HTTP, HTTPS e FTP dai server pubblicati.
- **Protezione per Squid,** il più diffuso server proxy per Linux.
- **Strumenti facili da usare** per l'installazione, la gestione e gli aggiornamenti.
- **Flessibili strumenti di scansione e scenari di risposta agli incidenti**.
- **Bilanciamento del carico** dei processori server.
- **Scalabilità e tolleranza di errore.**
- **Reporting esaustivo** sullo stato di protezione della rete.

FUNZIONI SPECIFICHE DI MICROSOFT® FOREFRONT® TMG E ISA SERVER:

- Monitoraggio in tempo reale dello stato delle applicazioni.
- Scansione delle connessioni VPN.
- Scansione in tempo reale del traffico HTTPS (solo TMG).
- Protezione del traffico e-mail (tramite i protocolli POP3 e SMTP).
- Archiviazione dei backup (solo TMG).

Kaspersky Security for Mail Server e Kaspersky Security for Internet Gateway sono presenti in Kaspersky Total Security for Business, ma risultano disponibili per l'acquisto anche separatamente come soluzioni mirate.

KASPERSKY SECURITY FOR COLLABORATION

Protezione dei dati e controllo per le piattaforme di collaborazione, incluse le farm SharePoint.

CARATTERISTICHE PRINCIPALI

PROTEZIONE TOTALE DELLA PIATTAFORMA SHAREPOINT
L'efficace protezione contro le minacce note, sconosciute e avanzate viene garantita dal modulo basato su cloud Kaspersky Security Network, mentre la tecnologia anti-phishing protegge i dati di collaborazione dalle minacce basate sul Web.

IMPEDIRE LA FUGA DEI DATI RISERVATI*
Tramite l'utilizzo di categorie di dati e dizionari preinstallati o personalizzati, Kaspersky Security for Collaboration verifica la presenza di informazioni sensibili in tutti i documenti presenti sui server SharePoint, parola per parola e frase per frase.

APPLICAZIONE DEI CRITERI DI COMUNICAZIONE
Le funzionalità per il filtro dei contenuti consentono di applicare gli standard e i criteri di comunicazione aziendali, identificando e bloccando i contenuti inappropriati e al tempo stesso evitando di archiviare inutilmente file e formati di file inappropriati.

FUNZIONALITÀ

PROTEZIONE ANTI-MALWARE
- **SCANSIONE ALL'ACCESSO** - i file vengono esaminati in tempo reale, durante il caricamento o il download.
- **SCANSIONE IN BACKGROUND** - i file archiviati nel server vengono controllati regolarmente, utilizzando le firme malware più recenti.
- **INTEGRAZIONE CON KASPERSKY SECURITY NETWORK** - offre protezione in tempo reale assistita da cloud perfino contro le minacce zero-day.

SUPPORTO DEI CRITERI DI COMUNICAZIONE DELL'ORGANIZZAZIONE
- **Filtro dei file** - consente di applicare i criteri di archiviazione dei documenti e ridurre le richieste indirizzate ai dispositivi di archiviazione. Analizzando i formati di file reali, indipendentemente dall'estensione, l'applicazione impedisce la violazione dei criteri di sicurezza proibendo agli utenti di utilizzare un tipo di file vietato.
- **Protezione di wiki/blog** - consente di proteggere tutti gli archivi di SharePoint, compresi wiki e blog.
- **Filtro dei contenuti** - impedisce l'archiviazione di file con contenuti inappropriati. Il contenuto di ogni file viene analizzato in base alle parole chiave. Gli utenti possono inoltre creare dizionari personalizzati per il filtro dei contenuti.

PREVENZIONE DELLA PERDITA DI DATI RISERVATI*
- **Scansione dei documenti per rilevare la presenza di informazioni riservate.**
  La soluzione integra moduli per l'identificazione di determinati tipi di dati, confermando che questi soddisfano gli standard legali di riferimento, ad esempio dati personali (definiti dalla conformità alle normative in vigore, tra cui HIPAA o la Direttiva UE 95/46/CE++) o dati standard PCI DSS (Payment Card Industry Data Security Standard).
  I dati vengono esaminati in base a dizionari tematici integrati aggiornati regolarmente e a dizionari personalizzati.
- **Ricerca di dati strutturati** - se le informazioni presentate in strutture specifiche vengono rilevate in un messaggio, verranno trattate come informazioni potenzialmente riservate, e verrà applicato il controllo sui dati sensibili contenuti in array complessi, ad esempio database di utenti.

GESTIONE FLESSIBILE
- **Facilità di gestione** - è possibile gestire un'intera server farm centralmente da una singola console. In un'interfaccia intuitiva sono inclusi tutti gli scenari amministrativi più comuni.
- **Dashboard singola** - una dashboard altamente intuitiva consente di accedere in tempo reale a informazioni aggiornate sullo stato del prodotto, sulla versione del database e sullo stato delle licenze di tutti i server protetti.
- **Backup dei file modificati** - in caso di incidenti, i file originali possono essere ripristinati se necessario e le informazioni dettagliate di backup sui file modificati possono essere utilizzate per scopi di analisi.
- **Integrazione con Active Directory®** - consente l'autenticazione degli utenti di Active Directory.

Kaspersky Security for Collaboration è presente in Kaspersky Total Security for Business, ma risulta disponibile per l'acquisto anche separatamente come soluzione mirata.

*Durante l'acquisto del prodotto, l'opzione per impedire la perdita o la fuga di dati riservati è in vendita separatamente.

KASPERSKY SECURITY FOR STORAGE

Protezione ad alte prestazioni per soluzioni di archiviazione EMC, NetApp, Hitachi e IBM®.

CARATTERISTICHE PRINCIPALI

POTENTE PROTEZIONE ANTI-MALWARE IN TEMPO REALE
Protezione proattiva e costante per soluzioni NAS (Network Attached Storage). Il potente motore anti-malware di Kaspersky esegue la scansione di ogni singolo file avviato o modificato per rilevare qualunque tipo di malware, inclusi virus, worm e trojan. L'analisi euristica avanzata identifica anche le minacce nuove e sconosciute.

PRESTAZIONI OTTIMIZZATE
La scansione ad alte prestazioni, caratterizzata da una tecnologia di scansione ottimizzata e da impostazioni di esclusione flessibili, consente di potenziare al massimo la protezione e al tempo stesso ridurre l'impatto sulle prestazioni del sistema.

AFFIDABILITÀ
L'architettura lineare, basata su componenti unificati progettati e costruiti per integrarsi perfettamente, garantisce una tolleranza di errore eccezionale. Questo consente di ottenere una soluzione stabile e resistente che, in caso di arresto forzato, si riavvia automaticamente per assicurare una protezione affidabile e continua.

AMMINISTRAZIONE SEMPLIFICATA
I server vengono installati da remoto, sono dotati di una protezione preconfigurata che non richiede alcun riavvio e vengono amministrati contemporaneamente tramite una console centrale semplice e intuitiva, Kaspersky Security Center, insieme alle altre soluzioni di sicurezza Kaspersky in uso.

FUNZIONALITÀ

PROTEZIONE PROATTIVA E COSTANTE
Il motore di scansione anti-malware leader di settore Kaspersky, realizzato dai massimi esperti mondiali nell'analisi delle minacce, assicura una protezione proattiva contro le minacce emergenti e potenziali, avvalendosi di tecnologie intelligenti per il rilevamento avanzato.

AGGIORNAMENTI AUTOMATICI
I database anti-malware vengono aggiornati automaticamente senza interrompere la scansione, assicurando una protezione continua e minimizzando il carico di lavoro per l'amministratore.

PROCESSI ESCLUSI E AREE AFFIDABILI
Le prestazioni di scansione possono essere ottimizzate creando aree affidabili che possono essere escluse dalla scansione, insieme ai processi e ai formati di file specificati, come i backup dei dati.

SCANSIONE DEGLI OGGETTI A ESECUZIONE AUTOMATICA
Per aumentare la protezione dei server, è possibile eseguire automaticamente la scansione di file e sistemi operativi in modo da evitare il lancio del malware durante l'avvio del sistema operativo.

SCANSIONE FLESSIBILE E PRESTAZIONI OTTIMIZZATE
Il prodotto riduce i tempi di scansione e configurazione, oltre a favorire il bilanciamento del carico, permettendo di ottimizzare le prestazioni dei server. L'amministratore può specificare e controllare il livello, la portata e le tempistiche dell'attività di scansione, specificando i tipi di file e le aree da analizzare. È possibile programmare la scansione on-demand in modo che venga eseguita nei periodi di minore attività dei server.

PROTEZIONE DELLE SOLUZIONI HSM E DAS
Supporta le modalità di scansione offline per una protezione efficace dei sistemi HSM (Hierarchical Storage Management). La protezione DAS (Direct Attached Storage) promuove inoltre l'uso delle soluzioni di archiviazione a basso costo.

SUPPORTO DI TUTTI I PRINCIPALI PROTOCOLLI
Kaspersky Security for Storage supporta i principali protocolli utilizzati da diversi sistemi di archiviazione: CAVA agent, RPC e ICAP.

PROTEZIONE DI SISTEMI VIRTUALI E SERVER TERMINAL
La sicurezza flessibile include la protezione dei sistemi operativi virtuali (guest) negli ambienti virtuali Hyper-V e VMware e nelle infrastrutture di terminali Microsoft® e Citrix.

AMMINISTRAZIONE

INSTALLAZIONE E GESTIONE CENTRALIZZATE
L'installazione, la configurazione e l'amministrazione da remoto, inclusi aggiornamenti, notifiche e reporting flessibile, vengono gestite tramite l'intuitiva console Kaspersky Security Center. Per chi la preferisce, è disponibile anche la gestione dalla riga di comando.

CONTROLLO SUI PRIVILEGI DI AMMINISTRAZIONE
È possibile assegnare livelli di privilegi diversi agli amministratori dei singoli server, per garantire la conformità a specifici criteri di sicurezza IT aziendali.

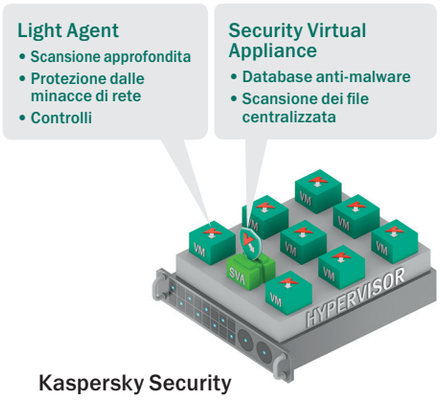
REPORTING FLESSIBILE
Il reporting è disponibile sotto forma di report grafici o tramite l'analisi dei registri eventi di Microsoft Windows® o Kaspersky Security Center. Gli strumenti di ricerca e filtraggio consentono di accedere rapidamente ai dati nei registri di grandi dimensioni.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization è una soluzione flessibile che garantisce un elevato livello di protezione e prestazioni per il vostro ambiente.

PROTEZIONE AVANZATA MEDIANTE LIGHT AGENT

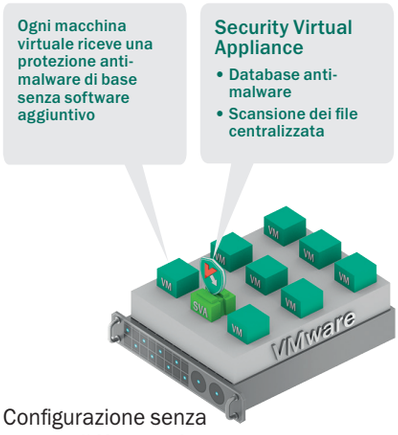
Kaspersky Security for Virtualization include un light agent ma potente che viene implementato su ogni singola macchina virtuale e abilita varie funzioni di sicurezza avanzate per gli endpoint: monitoraggio delle vulnerabilità; controllo di applicazioni, dispositivi e Web; protezione antivirus per messaggistica istantanea, posta e Web; euristica avanzata. Il risultato complessivo è un sistema di sicurezza potente e multilivello, abbinato a un'elevata efficienza prestazionale.



Kaspersky Security for Virtualization
Configurazione Light Agent

CONFIGURAZIONE OPZIONALE SENZA AGENTE PER AMBIENTI VMWARE

Grazie alla stretta integrazione con le tecnologie VMware, Kaspersky Security for Virtualization può anche essere implementato e gestito facilmente su questa piattaforma in una configurazione di sicurezza agentless. Tutte le attività di sicurezza sono concentrate nella Security Virtual Appliance, che si interfaccia con vShield per garantire una protezione automatica delle macchine virtuali e con vCloud per la protezione della rete.



Configurazione senza agente di **Kaspersky Security for Virtualization***

CARATTERISTICHE PRINCIPALI DEL PRODOTTO

- **Gestione centralizzata tramite Kaspersky Security Center**
- **Protezione centralizzata delle macchine virtuali tramite SVA**
- **Anti-malware avanzato**
- **Sistema di prevenzione delle intrusioni basato su host (HIPS) e firewall**
- **Controlli degli endpoint per applicazioni, accesso Web e periferiche**
- **Sicurezza assistita da cloud tramite Kaspersky Security Network**
- **Network Attack Blocker**
- **Protezione anti-phishing**
- **Antivirus per IM, posta e traffico Internet**
- **Non richiede ulteriori installazioni o riavvio per le nuove macchine virtuali****

LICENZE FLESSIBILI

A seconda delle esigenze specifiche, Kaspersky Security for Virtualization è disponibile nelle seguenti opzioni di licenza:

- Licenze basate sul numero di macchine:
  - Per desktop
  - Per server
- Licenze basate su risorse:
  - Per core.

PIATTAFORME MULTIPLE, COSTO SINGOLO

Una singola licenza di Kaspersky Security for Virtualization include il supporto per gli ambienti virtuali basati su Citrix, Microsoft® e VMware.

SECURITY VIRTUAL APPLIANCE (SVA)

Kaspersky Lab offre due soluzioni efficaci in questo settore, entrambe basate su una Security Virtual Appliance.

Security Virtual Appliance (SVA) di Kaspersky Lab analizza a livello centrale tutte le VM dell'ambiente host. Questo tipo di architettura garantisce una protezione efficiente delle macchine virtuali, senza sacrificare le risorse degli endpoint, eliminando scansioni antivirus, update storms e falle instant-on, e permettendo tassi di consolidamento superiori.

INTEGRAZIONE CON L'ARCHITETTURA DELLA PIATTAFORMA

Kaspersky Security for Virtualization supporta le piattaforme VMware, Microsoft® Hyper-V® e Citrix Xen e le relative tecnologie di base.

VMware	Microsoft Hyper-V	Citrix Xen
High Availability	Dynamic Memory	Dynamic Memory Control
Integrazione con vCenter	Cluster Shared Volumes	Virtual Machine Protection and Recovery (VMPR)
vMotion – DRS host	Live backup	Xenmotion (Live Migration)
Horizon View (Full clone e Linked Clone)	Live Migration	Multi-stream ICA
		Citrix receiver
		Personal vdisk

* Le funzioni di sicurezza avanzate, quali quarantena dei file, HIPS, scansione delle vulnerabilità e controlli degli endpoint, non sono disponibili in questo tipo di configurazione.

** Per le macchine virtuali non persistenti, la protezione istantanea è disponibile dopo l'inclusione del Light Agent nell'immagine della macchina virtuale. Per le VM persistenti, l'amministratore deve implementare il Light Agent sulle VM durante l'installazione.

SERVIZI DI INTELLIGENCE PER LA SICUREZZA KASPERSKY

È responsabilità dei professionisti della sicurezza di livello avanzato tutelare le proprie organizzazioni dalle minacce dei nostri giorni e anticipare i pericoli previsti per gli anni a venire. A tal scopo è necessario un livello di intelligence per la sicurezza strategica che poche aziende possono sviluppare con le risorse interne.

Kaspersky Lab è un importante partner aziendale, sempre pronto a condividere l'intelligence più aggiornata tramite diversi canali, garantendo al team SOC/IT tutte le risorse necessarie per proteggere l'organizzazione da qualsiasi minaccia online.

FORMAZIONE SULLA SICUREZZA INFORMATICA
Il programma di formazione sulla sicurezza informatica di Kaspersky Lab è stato sviluppato appositamente per tutte le organizzazioni che intendono promuovere il ruolo della sicurezza informatica per proteggere meglio l'infrastruttura e la proprietà intellettuale.

Il programma tratta svariati aspetti, dai principi di base della sicurezza all'analisi del malware e all'analisi digitale avanzata, consentendo agli utenti di migliorare le proprie competenze in ambito di sicurezza informatica in tre aree principali:

- Competenze fondamentali sull'argomento
- Analisi digitale e risposta agli incidenti
- Analisi del malware e reverse engineering

FEED DI DATI SULLE MINACCE
I feed di dati sulle minacce di Kaspersky Lab sono progettati per l'integrazione costante dell'intelligence sulla sicurezza nei sistemi SIEM (Security Information and Event Management) esistenti, offrendo un ulteriore livello di protezione.

ANALISI DEL MALWARE; ANALISI DIGITALE; RISPOSTA AGLI INCIDENTI
I servizi di analisi di Kaspersky Lab aiutano le organizzazioni a formulare le proprie strategie di difesa fornendo un'analisi delle minacce approfondita e consulenza sulle operazioni da eseguire per la risoluzione dell'incidente.

Sono disponibili tre livelli di analisi:

- Analisi del malware - consente di individuare il comportamento e gli obiettivi di determinati file malware che attaccano l'organizzazione.
- Analisi digitale - offre un quadro completo dell'incidente e degli effetti sull'organizzazione.
- Risposta agli incidenti - un'analisi a ciclo completo dell'incidente che comprende una visita sul posto di un esperto di Kaspersky Lab.

MONITORAGGIO DELLE MINACCE BOTNET
La soluzione avanzata di Kaspersky Lab tiene traccia delle attività delle botnet e fornisce notifiche rapide (entro 20 minuti) delle minacce associate agli utenti di singoli sistemi bancari e di pagamento online. Queste informazioni possono essere utilizzate per avvertire e informare i clienti, fornitori di servizi di sicurezza e forze dell'ordine locali delle minacce in corso.

REPORT DI INTELLIGENCE
I report di intelligence di Kaspersky Lab consentono di accedere a informazioni sempre aggiornate basate sulle statistiche raccolte da oltre 80 milioni di utenti in 200 paesi, per aumentare la consapevolezza e la conoscenza delle minacce a cui deve far fronte l'organizzazione.

Le conoscenze, l'esperienza e le informazioni approfondite di Kaspersky Lab ne hanno fatto il partner di fiducia delle più importanti agenzie governative e forze dell'ordine. Potete sfruttare queste informazioni nella vostra organizzazione oggi stesso.

SOLUZIONI AZIENDALI KASPERSKY

DDOS PROTECTION - DIFESA TOTALE E MITIGAZIONE DEGLI EFFETTI

Una strategia completa per difendere l'azienda dagli attacchi DDoS (Distributed Denial of Service).

Kaspersky DDoS Protection offre all'azienda gli strumenti necessari per difendersi da tutti i tipi di attacchi DDoS e mitigarne gli effetti. Questo comprende: analisi costante del traffico online, avviso della possibile presenza di un attacco e ricezione del traffico reindirizzato, pulizia e reinvio del traffico "pulito".

KASPERSKY FRAUD PREVENTION - PER BANCHE E ISTITUTI FINANZIARI

Una piattaforma tecnologica completa, personalizzata e di facile utilizzo orientata ai rischi legati alle frodi durante le transazioni finanziarie online e da dispositivi mobili.

Kaspersky Fraud Prevention protegge gli utenti delle organizzazioni finanziarie indipendentemente dal tipo di dispositivo utilizzato per accedere a questi servizi: PC, laptop, smartphone o tablet. La piattaforma comprende inoltre un componente software bancario in grado di rilevare il malware e di identificare automaticamente modelli di comportamento anomali nelle singole transazioni degli utenti. Anche se Kaspersky Fraud Prevention for Endpoints non è installato, il Clientless Engine è in grado di impedire le transazioni fraudolente.

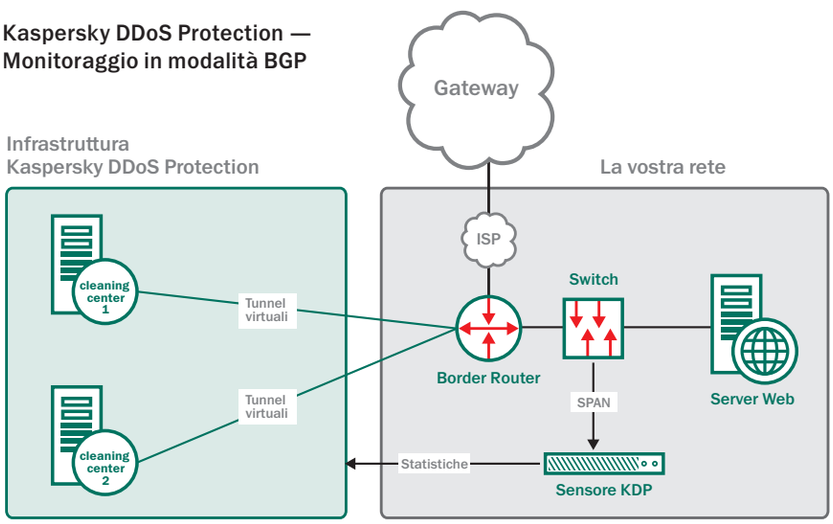
LA PROTEZIONE DELLE INFRASTRUTTURE DI IMPORTANZA CRITICA

Protezione di reti e sistemi di controllo industriali

Kaspersky Endpoint Security for Business offre un'autentica protezione di tipo industriale, che tutela gli endpoint ICS/SCADA da minacce e vulnerabilità usate come backdoor da molti criminali per attaccare i sistemi critici.

Collaborando con i principali fornitori di automazione industriale, del calibro di Emerson, Rockwell Automation e Siemens, Kaspersky Lab ha stabilito molte procedure specializzate per garantire approvazione e compatibilità con la tecnologia operativa dei clienti. Questo ci consente di garantire una protezione efficace per le infrastrutture critiche, senza compromettere la coerenza e la continuità operativa.

Kaspersky DDoS Protection — Monitoraggio in modalità BGP



SERVIZI PROFESSIONALI KASPERSKY LAB

Per i clienti con installazioni IT complesse, i servizi professionali Kaspersky di implementazione e aggiornamento, formazione e Health Check mirano a fare in modo che le soluzioni Kaspersky Security for Business vengano configurate, implementate e gestite correttamente per garantire prestazioni ottimali.

KASPERSKY SMALL OFFICE SECURITY

La protezione di livello mondiale a portata delle piccole aziende.

Una sfida unica richiede una soluzione unica. Un'efficace protezione di livello mondiale più semplice e rapida che mai da utilizzare.

- Appositamente progettata per aziende con massimo 25 utenti.
- Facile da installare ed eseguire, non richiede formazione.
- Console Web per l'amministrazione basata su Internet da qualsiasi posizione.

L'ESPERIENZA NON SERVE
La progettazione di Kaspersky Small Office Security consente anche all'utente meno esperto di effettuare senza problemi l'installazione e l'esecuzione. È dotato infatti di esplicite procedure guidate per accompagnare l'utente in processi quali:

- Configurazione, previa rimozione di qualsiasi anti-malware esistente.
- Impostazione dei controlli e scelta dei criteri più adatti per l'utente e la relativa azienda.
- Download automatico delle modifiche in più computer contemporaneamente.

Il tutto viene gestito tramite una dashboard basata sul Web che consente all'utente o a una persona da lui scelta di gestire la sicurezza IT da remoto via Internet.

Kaspersky Small Office Security assicura un livello di protezione imbattibile ma, poiché viene eseguito in background, non interferisce minimamente con il vostro lavoro.

MOLTEPLICI LIVELLI DI PROTEZIONE
Kaspersky Small Office Security applica tutti i livelli di protezione a PC, Mac, server, tablet e smartphone. Sono inclusi tutti gli strumenti di sicurezza necessari all'evoluzione aziendale e molto altro ancora. Affidando a Kaspersky Small Office Security la sicurezza IT sarà possibile dedicarsi completamente alla gestione della propria azienda.

- Protezione in tempo reale basata sul cloud dalle minacce informatiche nuove ed emergenti.
- Consente di proteggere i computer Windows® e Mac, server Windows e dispositivi mobili Android™.
- La pluripremiata tecnologia Safe Money protegge le transazioni finanziarie online da hacker online e ladri di identità.
- I controlli consentono di gestire la navigazione sul Web dei dipendenti e le attività nei social network.
- Crittografia per proteggere i dati riservati dei clienti e dell'azienda.
- Tecnologie anti-phishing per la protezione da siti Web dannosi e contraffatti.
- Potente filtro anti-spam.
- Gestione sicura delle password.*
- Backup automatico dei dati tramite Dropbox per impedire la perdita dei dati.

PIÙ RISPARMIO
Oltre a proteggere dagli attacchi degli hacker mirati a sottrarre denaro, Kaspersky Small Office Security contribuisce a rendere i dipendenti più produttivi controllandone l'accesso al Web e impostando controlli per stabilire quando possono navigare o inviare messaggi. Funzioni di sicurezza avanzate come la crittografia convincono i clienti ad affidare i propri dati all'azienda, che vedrà aumentare il proprio potenziale di vendita e la soddisfazione dei clienti.

* Applicabile solo ad applicazioni a 32 bit. Comprende dispositivi Android e iOS.

CONTRATTI DI MANUTENZIONE E SUPPORTO KASPERSKY

Un supporto di qualità elevata in caso di incidenti, problemi di configurazione, incompatibilità e altri inconvenienti legati alla sicurezza IT è fondamentale per le organizzazioni.

I contratti di manutenzione e supporto di Kaspersky Lab offrono un supporto eccellente in caso di incidenti imprevisti, da un'errata configurazione ad attacchi malware, e contribuiscono alla stabilità e all'efficienza dell'intera organizzazione.

Nei contratti di manutenzione e supporto di Kaspersky Lab sono contemplati i seguenti argomenti:

- Epidemie inaspettate di virus globali
- Tempi di inattività considerevoli dovuti alla complessità dell'infrastruttura
- Ottimizzazione dell'implementazione e correzioni personalizzate
- Problemi di incompatibilità di rete
- Processo di aggiornamento dei prodotti Kaspersky Lab
- Analisi degli attacchi malware
- Supporto per l'installazione e la configurazione dei prodotti*
- Implementazione di patch altri aggiornamenti*

Se è necessario ottenere assistenza, gli specialisti di Kaspersky Lab sono disponibili tramite linee prioritarie dedicate nelle lingue locali, in orari che si adattano alle esigenze dell'organizzazione. La matrice di seguito illustra le opzioni di supporto disponibili.

	Supporto standard		Supporto esteso	
	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
Linea telefonica prioritaria	Sì	Sì	Sì	Sì
Technical Account Manager	No	No	Sì	Sì, dedicato
Supporto nella lingua locale	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Supporto livello di gravità 1	8 x 5	8 x 5	24 x 7 x 365	24 x 7 x 365
Tempo di risposta livello di gravità 1	8 Orario di lavoro	6 Orario di lavoro	4 Ore	30 Minuti
Supporto livello di gravità 2	8 x 5	8 x 5	8 x 5	24 x 7 x 365
Consulenza professionale	No	No	Costi aggiuntivi	Controllo di integrità e reporting personalizzato
Limitazione degli incidenti	6	12	36	Illimitato

* Opzioni a pagamento per MSA Business non disponibili per MSA Starter e MSA Plus.

KASPERSKY LAB A LIVELLO GLOBALE

Kaspersky offre supporto alle aziende locali e globali da uffici dislocati in tutto il mondo. Per ulteriori informazioni sull'acquisto delle soluzioni Kaspersky Security for Business, contattate il rivenditore locale.

www.kaspersky.com

APAC

1. Australia
2. Cina
3. Hong Kong
4. India
5. Corea
6. Malesia

Europa

7. Austria
8. Francia
9. Germania
10. Italia
11. Paesi Bassi
12. Portogallo
13. Spagna
14. Norvegia
15. Svizzera
16. Regno Unito

Mercati emergenti

17. Lettonia
18. Polonia
19. Romania
20. Slovenia
21. Sudafrica
22. Turchia
23. Ucraina
24. Emirati Arabi Uniti

Giappone

25. Giappone (Tokyo)

Nord America

26. Canada
27. Stati Uniti d'America (Boston)
28. Stati Uniti d'America (Miami)

Russia e CSI

29. Russia
30. Kazakistan

Kaspersky Lab Italia
www.kaspersky.it

Tutto sulla sicurezza in Internet:
www.securelist.com

Trovate il partner più vicino:
www.kaspersky.it/buyoffline

Catalog_SP1/Feb15/Global

KASPERSKY lab