KASPERSKY SOLUZIONI PER AZIENDE 2013

Guarda. Controlla. Proteggi.

KASPERSKY lab

INFORMAZIONI SU KASPERSKY LAB

Kaspersky Lab è la più grande azienda del mondo che produce soluzioni software di sicurezza. Garantiamo i migliori prodotti per la sicurezza IT destinati alle aziende che combinano funzionalità di protezione anti-malware, strumenti di controllo flessibili, tecnologia di crittografia e strumenti per la gestione dei sistemi. Kaspersky è in grado di garantire la sicurezza dell'intero ambiente, dagli endpoint fino ai server e gateway e, in virtù del design integrato che abbiamo scelto per i nostri prodotti, vi permettiamo di proteggere e controllare tutti i vostri dispositivi fisici, virtuali e mobili da una console di gestione centralizzata, indipendentemente dalla portata dell'infrastruttura in uso. La tecnologia di Kaspersky è diffusa in tutto il mondo, all'interno di prodotti e servizi dei più importanti sviluppatori di utilità anti-malware e produttori IT.

Ulteriori informazioni sul sito Web: www.kaspersky.com.

Per ottenere informazioni sulle tecnologie antivirus, anti-spyware e anti-spam più recenti e conoscere altre problematiche e tendenze correlate alla sicurezza IT, visitate il sito Web: www.securelist.com.

L'UNICA PIATTAFORMA DI SICUREZZA REALMENTE INTEGRATA DEL SETTORE

UN'UNICA CONSOLE

I prodotti di Kaspersky sono progettati affinché l'amministratore possa avvalersi di una posizione centralizzata per visualizzare e gestire l'intero scenario di sicurezza: macchine virtuali e dispositivi fisici e mobili.

UN'UNICA PIATTAFORMA

Kaspersky Lab ha scelto di sviluppare internamente console, moduli e strumenti di sicurezza anziché acquistarli da altre aziende. Ciò ha consentito a dei programmatori di utilizzare la medesima codebase per sviluppare tecnologie perfettamente integrabili e interoperabili, in modo da poter garantire stabilità, criteri integrati, reporting efficiente e strumenti intuitivi.

UNICO COSTO

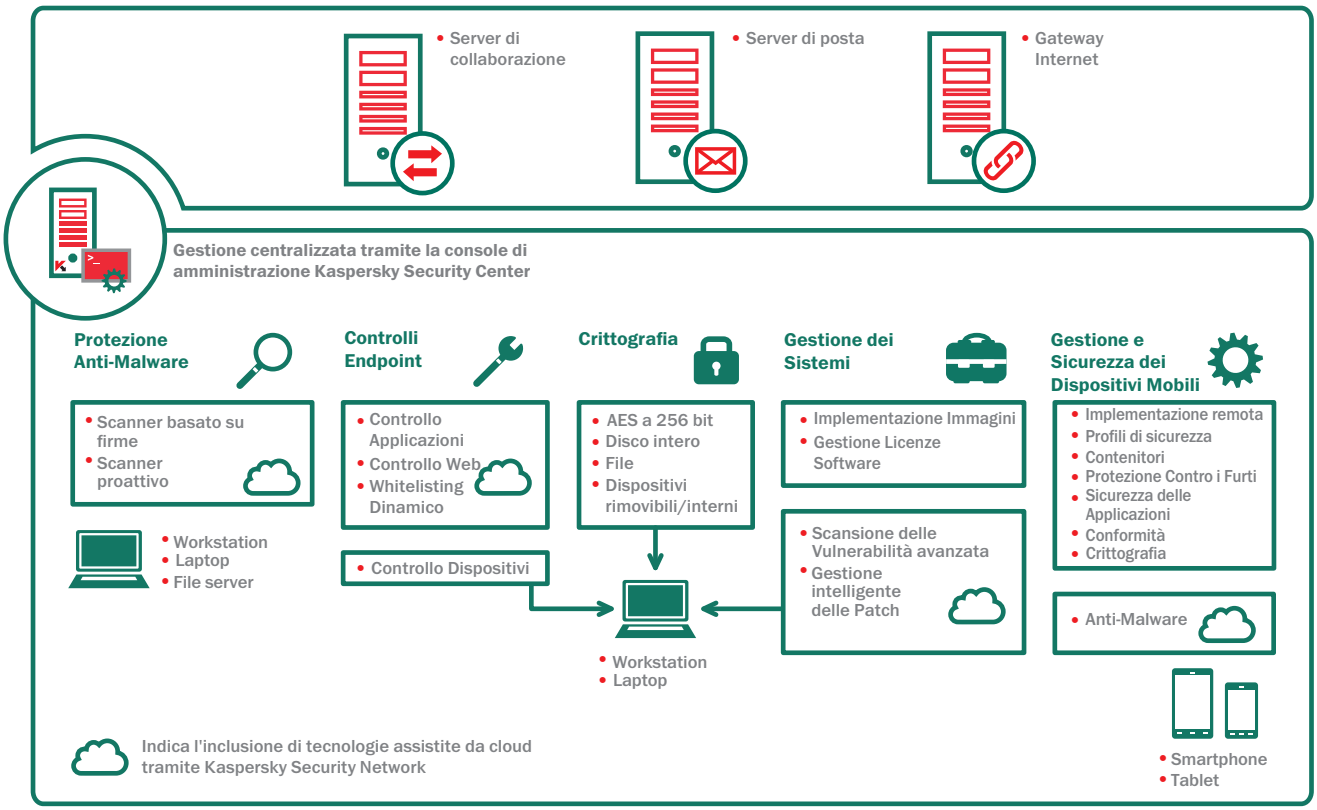
Tutti gli strumenti vengono offerti da un fornitore singolo in un'unica installazione, evitandovi l'onere di ripetere il processo di budgeting e giustificazione per garantire all'organizzazione un livello di protezione adeguato agli obiettivi aziendali.

LA SOLUZIONE GIUSTA PER VOI

Kaspersky Security for Business rappresenta la soluzione ideale per la vostra organizzazione poiché consente di progettare e controllare gli endpoint (inclusi workstation, smartphone e macchine virtuali), garantire la protezione di server e gateway o gestire in modalità remota l'intero ambiente di sicurezza.

Kaspersky vanta di una gamma completa di tecnologie (dagli strumenti di crittografia e gestione dei dispositivi mobili, alla gestione delle patch e inventari di licenze) perfettamente interoperabili e supportate dal servizio basato su cloud Kaspersky Security Network, per offrire ai clienti l'avanzato livello di protezione di cui hanno bisogno per contrastare al meglio le più sofisticate e diversificate minacce informatiche.

In breve, forniamo la prima piattaforma di sicurezza del settore, senza rivali nel mercato, che consente agli amministratori di osservare, controllare e proteggere in modo semplice il loro ambiente IT.

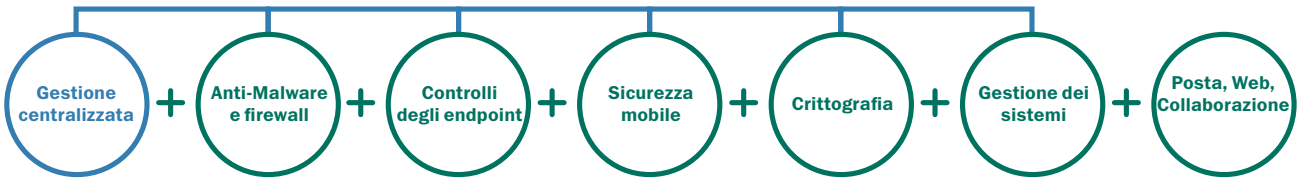


KASPERSKY SECURITY FOR BUSINESS

Le nostre tecnologie perfettamente interoperabili

	Core	Select	Advanced	Total	Gestita tramite Security Center	Disponibile in una soluzione mirata
Anti-Malware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Controllo Applicazioni		•	•	•	•	
Controllo Dispositivi		•	•	•	•	
Controllo Web		•	•	•	•	
File Server		•	•	•	•	•
Agente per gli endpoint mobili		•	•	•	•	•
Mobile Device Management		•	•	•	•	•
Tecnologia di crittografia			•	•	•	
Gestione delle immagini del sistema operativo			•	•	•	•
Gestione Licenze			•	•	•	•
Gestione delle vulnerabilità			•	•	•	•
Gestione delle Patch			•	•	•	•
Controllo Accessi alla Rete			•	•	•	•
Collaborazione				•		•
Server di posta				•		•
Gateway Internet				•		•
Virtualizzazione					•	•
Archiviazione					•	•

KASPERSKY ENDPOINT SECURITY FOR BUSINESS



LIVELLO CORE

Alla combinazione base costituita da una potente e pluripremiata tecnologia anti-malware e dal firewall Kaspersky, abbiamo aggiunto la nostra intuitiva console di amministrazione Kaspersky Security Center. Questa rappresenta la soluzione ideale per i clienti che richiedono esclusivamente una protezione anti-malware.

LIVELLO SELECT

Potenziando il livello CORE, abbiamo aggiunto le funzionalità di protezione **Sicurezza File Server (File Server Security), Whitelist delle Applicazioni (Application Whitelisting), Controllo Applicazioni (Application Control), Controllo Dispositivi (Device Control) e Controllo Web (Web Control)**. Il livello include inoltre una **soluzione di protezione mobile** costituita da un **agente per la sicurezza degli endpoint** e da **Mobile Device Management (o MDM)**. Se avete bisogno di proteggere una forza lavoro mobile e di applicare i criteri IT, il livello SELECT potrebbe essere la soluzione più adatta a voi.

LIVELLO ADVANCED

Con il livello ADVANCED, Kaspersky garantisce la **protezione dei dati** attraverso la **crittografia** del disco intero o dei file. Un'altra nuova offerta, **Kaspersky Systems Management**, combina sicurezza con efficienza dell'IT. Questo ampio set di funzionalità comprende strumenti essenziali che consentono all'amministratore di:

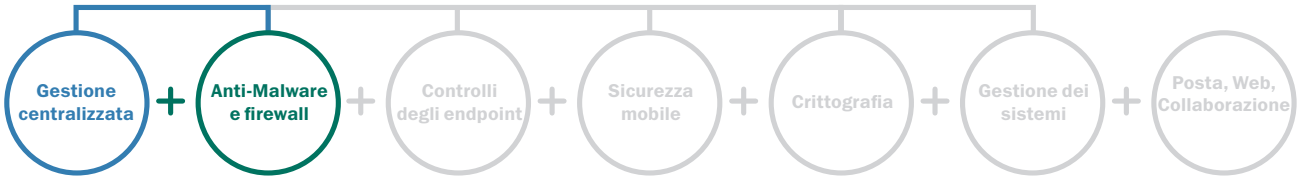
- Creare immagini e implementare sistemi con il modulo Image Management.
- Definire le priorità per la gestione delle vulnerabilità hardware e software con le avanzate funzionalità Scansione delle Vulnerabilità (Vulnerability Scanning) e Gestione delle Patch (Patch Management).
- Monitorare l'utilizzo delle licenze e la conformità con la funzionalità Gestione Licenze Software (Software License Management).
- Impostare criteri per l'accesso ai dati e all'infrastruttura per utenti e guest con la funzionalità Controllo Accessi alla Rete (Network Admission Control).
- Implementare e installare aggiornamenti e nuovo software per gli utenti remoti tramite la console centralizzata.

KASPERSKY TOTAL SECURITY FOR BUSINESS

Soluzione di punta della nostra gamma di prodotti, Kaspersky Total Security for Business combina tutti i livelli precedenti migliorando ulteriormente l'approccio di sicurezza grazie all'integrazione di funzionalità di protezione del Web, della posta e dei server di collaborazione. Rappresenta la soluzione ideale per organizzazioni con requisiti di sicurezza particolarmente impegnativi che necessitano di una protezione ottimale ad ogni singolo livello della rete.

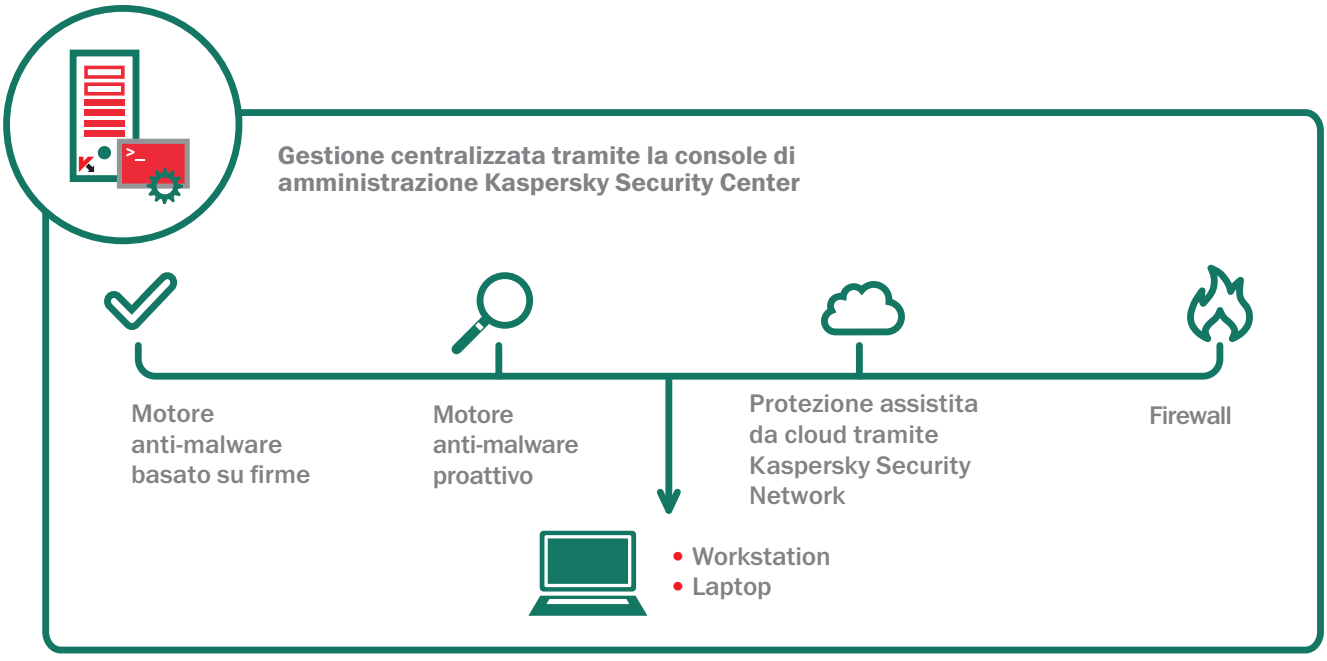
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Pluripremiata tecnologia anti-malware con implementazione, gestione e reporting centralizzati.

Un approccio di sicurezza a più livelli può essere creato solo a partire da un'avanzata tecnologia anti-malware. Dal momento che Kaspersky vanta da tempo la fama di fornitore leader del settore di soluzioni per il rilevamento e la rimozione del software nocivo, le sue soluzioni non potrebbero essere una premessa migliore. Il livello "Core" della soluzione Kaspersky Endpoint Security for Business è gestito in maniera centralizzata da Kaspersky Security Center, con il supporto del servizio basato su cloud Kaspersky Security Network.



Kaspersky Endpoint Security for Business - Livello Core. Potente motore anti-malware con protezione assistita tramite cloud.

FUNZIONALITÀ CHIAVE:

POTENTE TECNOLOGIA ANTI-MALWARE DEGLI ENDPOINT
I motori di scansione di Kaspersky consentono di individuare ed eliminare il malware agendo a molteplici livelli del sistema operativo.

PROTEZIONE ABILITATA PER IL CLOUD
Grazie al servizio basato su cloud Kaspersky Security Network, gli utenti ottengono una protezione in tempo reale contro le nuove minacce.

GESTIONE CENTRALIZZATA
Gli amministratori possono rimuovere il software antivirus esistente, configurare e implementare la soluzione Kaspersky ed eseguire il reporting da un'unica console.

FUNZIONALITÀ ANTI-MALWARE DEGLI ENDPOINT:

AGGIORNAMENTI FREQUENTI E PROTEZIONE BASATA SULLA FIRMA
Metodo tradizionale basato sulla firma, di uso consolidato nel settore, per il rilevamento delle minacce.

ANALISI DEL COMPORTAMENTO CON LA FUNZIONALITÀ CONTROLLO DEL SISTEMA (SYSTEM WATCHER)
Kaspersky Security Network (KSN) consente di rispondere alle minacce sospette in tempi estremamente più rapidi rispetto ai metodi di protezione tradizionali. KSN assicura tempi di risposta di appena 0,02 secondi!

SISTEMA DI PREVENZIONE DELLE INTRUSIONI BASATO SU HOST (HIPS, HOST-INTRUSION PREVENTION SYSTEM) CON FIREWALL PERSONALE
Regole predefinite per centinaia delle applicazioni più comunemente utilizzate riducono i tempi impiegati per la configurazione del firewall.

AMPIA GAMMA DI PIATTAFORME SUPPORTATE
Kaspersky offre funzionalità di sicurezza degli endpoint per Windows®, Macintosh® e Linux®, semplificando il carico di lavoro dell'amministratore impegnato nella gestione di più reti.

CARATTERISTICHE DI KASPERSKY SECURITY CENTER:

CONSOLE CENTRALIZZATA
Per la gestione remota di tutti i vostri endpoint protetti con una soluzione Kaspersky.

INTERFACCIA UTENTE INTUITIVA
Informazioni chiare e modificabili in un cruscotto intuitivo offrono agli amministratori la possibilità di visualizzare lo stato della protezione, impostare criteri, gestire sistemi e ottenere report in tempo reale.

INTERFACCIA WEB
Monitora in remoto lo stato della protezione e fornisce report sugli eventi chiave da un'interfaccia flessibile e accessibile.

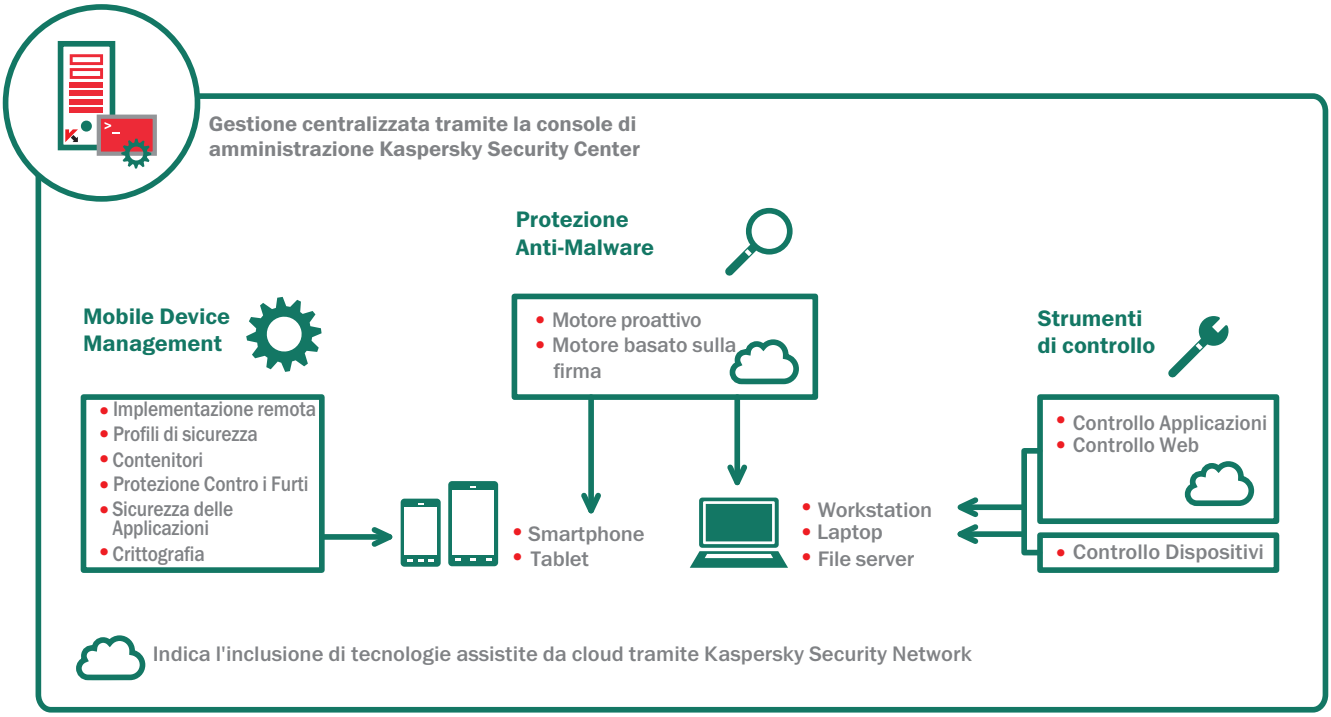
SUPPORTO SCALABILE
A prescindere dalle dimensioni dell'infrastruttura, Kaspersky Security Center fornisce tutti gli strumenti necessari per l'installazione e la gestione, opzioni flessibili per i criteri e solide capacità di reporting per soddisfare ogni vostra nuova esigenza.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Select

Strumenti per dispiegare una forza lavoro mobile, garantire la conformità ai criteri di sicurezza IT e bloccare le minacce malware.

Il livello "Select" di Kaspersky include l'implementazione e la protezione dei dispositivi mobili tramite Mobile Device Management (MDM) e anti-malware. Strumenti per il controllo degli endpoint (Web, dei dispositivi e delle applicazioni) permettono alla vostra organizzazione di applicare criteri IT in grado di proteggere gli elementi fondamentali del vostro ambiente IT.



Kaspersky Endpoint Security for Business - Livello Select. Strumenti di controllo e funzionalità di sicurezza mobile.

FUNZIONALITÀ CHIAVE:

POTENTE TECNOLOGIA ANTI-MALWARE DEGLI ENDPOINT
Il motore di scansione all'avanguardia di Kaspersky consente di individuare ed eliminare il malware agendo a molteplici livelli del sistema operativo. Il servizio basato su cloud Kaspersky Security Network (KSN) assicura una protezione in tempo reale degli utenti contro le nuove minacce.

FLESSIBILI STRUMENTI DI CONTROLLO GRANULARE
Un database basato su cloud di categorie di applicazioni e siti Web sicuri e non sicuri permette all'amministratore di impostare e applicare criteri per le applicazioni e la navigazione nel Web, mentre dei controlli granulari limitano l'accesso alle macchine della rete solo a specifici dispositivi.

EFFICIENTE FUNZIONALITÀ DI IMPLEMENTAZIONE E SICUREZZA MOBILE PER SMARTPHONE E TABLET
La sicurezza mobile con agente è disponibile per i dispositivi Android™, BlackBerry®, Symbian e Windows® Mobile. Kaspersky MDM permette di implementare il software e i criteri per i dispositivi mobili in modalità OTA (Over-The-Air) sia su tali dispositivi che su dispositivi iOS.

TECNOLOGIE INTRODOTTE IN QUESTO LIVELLO:

CONTROLLI DEGLI ENDPOINT:

CONTROLLO DELLE APPLICAZIONI
Consente agli amministratori IT di impostare criteri tesi a consentire, bloccare o regolare applicazioni (o categorie di applicazioni).

CONTROLLO DISPOSITIVI
Consente all'amministratore di impostare, pianificare e applicare criteri circa l'uso dei dispositivi rimovibili collegati all'USB o ad altri tipi di bus

CONTROLLO WEB
Consente di associare i controlli della navigazione basati su endpoint all'utente, sia all'interno della rete aziendale che durante gli spostamenti.

WHITELISTING DINAMICO
Le reputazioni di file in tempo reale fornite da Kaspersky Security Network consentono di proteggere le applicazioni approvate dal rischio di minacce malware, ottimizzando al tempo stesso la produttività degli utenti.

KASPERSKY SECURITY FOR MOBILE:

INNOVATIVE TECNOLOGIE ANTI-MALWARE
Combinazione dei risultati ottenuti con il rilevamento proattivo basato sulla firma e assistito da cloud in una funzionalità di protezione in tempo reale. Un browser protetto e una potente funzionalità anti-spam migliorano la sicurezza dell'ambiente.

IMPLEMENTAZIONE CON PROVISIONING IN MODALITÀ OTA (OVER-THE-AIR).
Possibilità di preconfigurare e implementare le applicazioni in maniera centralizzata tramite l'uso di SMS, e-mail e PC.

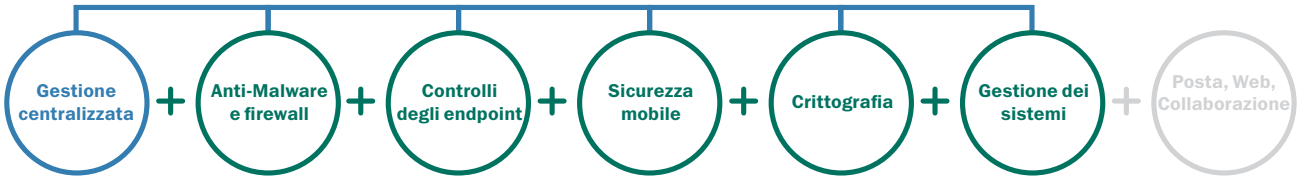
STRUMENTI DI PROTEZIONE REMOTA CONTRO I FURTI
SIM Watch, Blocco Remoto (Remote Lock), Cancellazione (Wipe) e Localizzazione (Find) sono funzionalità in grado di impedire l'accesso non autorizzato ai dati aziendali in caso di perdita o furto di un dispositivo mobile.

CONTROLLO DELLE APPLICAZIONI PER I DISPOSITIVI MOBILI
Garantisce il monitoraggio delle applicazioni installate su un dispositivo mobile in base ai criteri di gruppo predefiniti. Include un gruppo di "applicazioni obbligatorie".

SUPPORTO DEI DISPOSITIVI PERSONALI DEI DIPENDENTI
I dati e le applicazioni aziendali sono isolati in contenitori crittografati trasparenti per gli utenti. Tali dati possono essere eliminati separatamente.

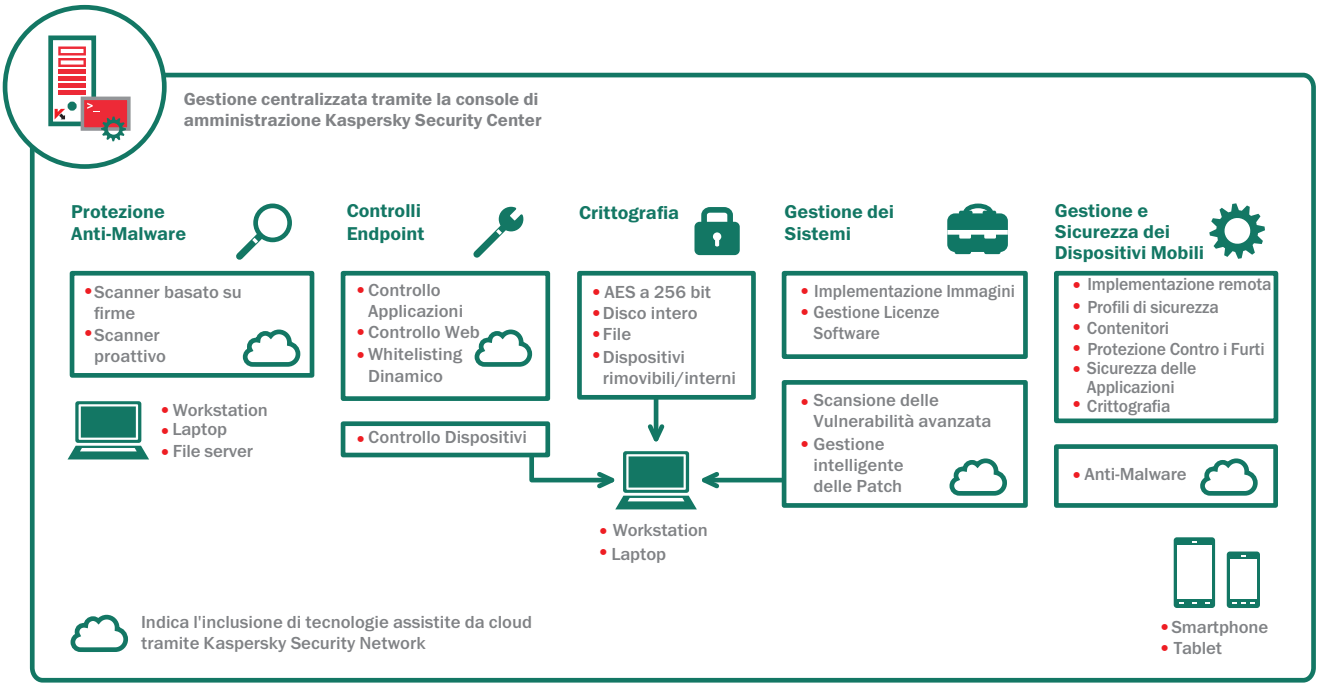
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Advanced



La ricca gamma di soluzioni di Kaspersky Lab offre un'ampia serie di strumenti di sicurezza e funzionalità per l'ottimizzazione dell'IT.

Il livello Advanced di Kaspersky garantisce la soluzione di protezione e gestione necessaria alla vostra organizzazione per applicare criteri di sicurezza IT, proteggere gli utenti dalle minacce malware e dal rischio di perdita dei dati e migliorare l'efficienza delle risorse IT.



Kaspersky Endpoint Security for Business - Livello Advanced. Tecnologia di crittografia e strumenti per la gestione dei sistemi di sicurezza.

FUNZIONALITÀ CHIAVE:

TECNOLOGIA DI CRITTOGRAFIA AVANZATA
La crittografia del disco intero o a livello di cartelle, con il supporto dell'algoritmo AES (Advanced Encryption Standard) a 256 bit, garantisce una protezione dei dati in caso di perdita o furto dei dispositivi e consente la condivisione sicura dei dati tramite dispositivi rimovibili, e-mail, rete o Web, offrendo la massima trasparenza agli utenti.

CONFIGURAZIONE DEI SISTEMI E GESTIONE DELLE PATCH
Creazione e implementazione delle immagini del sistema operativo, scansione delle vulnerabilità, gestione automatizzata delle patch, Controllo Accessi alla Rete (Network Admission Control), inventari e gestione delle patch creano un toolkit completamente integrato amministrato in maniera centralizzata mediante un'unica console intuiva.

FUNZIONALITÀ DI IMPLEMENTAZIONE E SICUREZZA MOBILE PER SMARTPHONE E TABLET
Sicurezza degli endpoint mobili basata su agente e gestione in modalità remota dei criteri per dispositivi e software mediante Kaspersky MDM.

POTENTE TECNOLOGIA ANTI-MALWARE DEGLI ENDPOINT E CONTROLLI FLESSIBILI
Avanzata tecnologia anti-malware assistita da cloud e strumenti per il controllo granulare di applicazioni, dispositivi e Web di Kaspersky.

TECNOLOGIE INTRODOTTE IN QUESTO LIVELLO:

CRITTOGRAFIA E PROTEZIONE DEI DATI:

CRITTOGRAFIA COMPLETA
Avete la possibilità di scegliere tra una crittografia del disco intero o a livello di file, con il supporto dell'algoritmo AES (Advanced Encryption Standard) a 256 bit, per garantire la protezione delle informazioni aziendali di importanza cruciale in caso di furto o perdita del dispositivo.

CONDIVISIONE SICURA DEI DATI
Create pacchetti crittografati e autoestraenti per garantire la protezione dei dati durante la condivisione tramite dispositivi rimovibili, e-mail, rete o Web.

SUPPORTO DI DISPOSITIVI RIMOVIBILI
Migliorate la sicurezza tramite criteri che consentono l'applicazione della crittografia dei dati su dispositivi rimovibili.

TRASPARENZA PER GLI UTENTI FINALI
La soluzione di crittografia di Kaspersky risulta intuitiva e invisibile per gli utenti e non genera ripercussioni né sulla produttività né sulle impostazioni o sugli aggiornamenti delle applicazioni.

CONFIGURAZIONE DEI SISTEMI E GESTIONE DELLE PATCH:

GESTIONE DELLE PATCH
Un'avanzata funzionalità di scansione delle vulnerabilità si unisce alla distribuzione automatica delle patch.

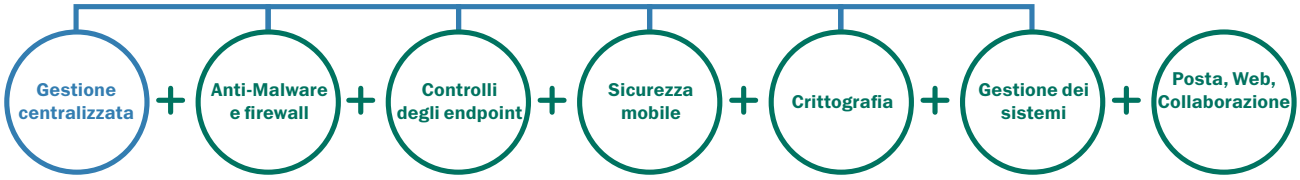
IMPLEMENTAZIONE DELLE IMMAGINI DI SISTEMA OPERATIVO E APPLICAZIONI
Creazione, archiviazione e implementazione semplificate delle immagini del sistema da una posizione centralizzata. La soluzione ideale per la migrazione a Microsoft® Windows® 8.

IMPLEMENTAZIONE REMOTA DEL SOFTWARE
Implementazione centralizzata del software su macchine client, anche presso gli uffici remoti.

CONTROLLO ACCESSI ALLA RETE (NAC)
Il Controllo Accessi alla Rete (NAC - Network Admission Control) consente di creare criteri per i dispositivi "guest" della rete. I dispositivi guest (compresi i dispositivi mobili) vengono riconosciuti automaticamente e inviati a un portale aziendale, nel quale, con la password corretta, possono utilizzare le risorse precedentemente approvate.

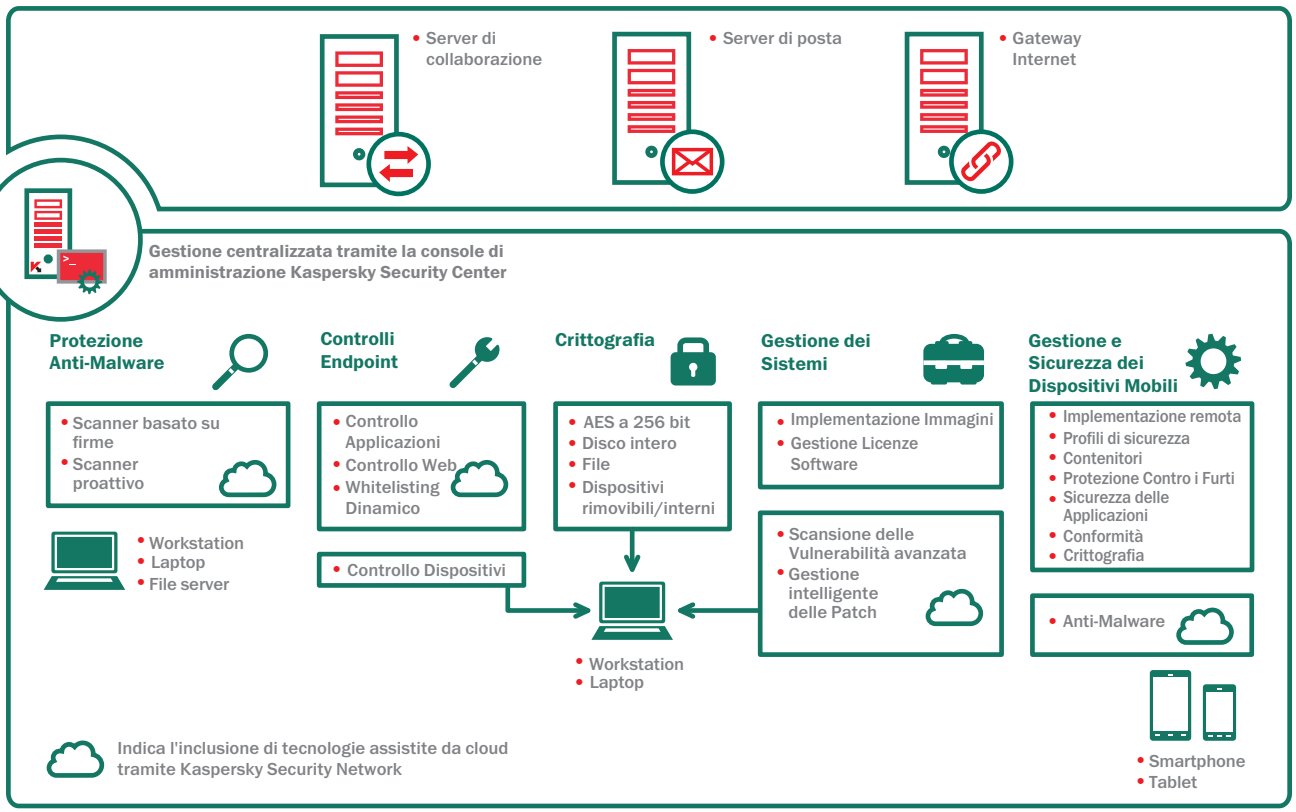
INVENTARIO HARDWARE E SOFTWARE E CONTROLLO DELLE LICENZE
I report degli inventari software e hardware consentono di controllare gli obblighi relativi alle licenze software, garantendo risparmi attraverso un provisioning centralizzato dei diritti software.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Protezione end-to-end contro le minacce malware, crittografia, efficienza delle risorse IT e strumenti per l'applicazione di criteri.

Kaspersky Total Security for Business offre la piattaforma di protezione e gestione più completa attualmente in uso nel settore. La soluzione 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.



FUNZIONALITÀ CHIAVE:

Tutte le funzionalità dei tre livelli precedenti, oltre a:

PROTEZIONE DEI SERVER DI POSTA
Protezione anti-malware e anti-spam del traffico di posta elettronica per tutti i sistemi di posta più diffusi

SICUREZZA PER I GATEWAY INTERNET
Garantisce un accesso sicuro a Internet a livello dell'intera azienda tramite la rimozione automatica dei programmi dannosi e potenzialmente ostili nel traffico HTTP(S)/FTP/ SMTP e POP3.

SICUREZZA DELLA COLLABORAZIONE
Kaspersky consente di proteggere i server SharePoint® contro le minacce malware, mentre le funzionalità per il filtro di file e contenuti aiutano a prevenire l'archiviazione di contenuti inappropriati.

TECNOLOGIE INTRODOTTE IN QUESTO LIVELLO:

SERVER DI POSTA:

PROTEZIONE DEL TRAFFICO DI POSTA ELETTRONICA
Consente di proteggere la posta sulle versioni più recenti delle principali piattaforme di posta e collaborazione: server di posta Microsoft Exchange, IBM Lotus Domino e Linux.

INTEGRAZIONE CON KSN PER LA PROTEZIONE ANTI-SPAM
Migliora il tasso di rilevamento dello spam grazie all'integrazione con il motore di identificazione delle minacce basato su cloud di Kaspersky Lab (KSN).

RIDUZIONE DEL CARICO DEL TRAFFICO
Una tecnologia di filtraggio anti-spam avanzata basata su cloud consente di ridurre considerevolmente il carico del traffico.

OTTIMIZZAZIONE DELLE RISORSE DI SISTEMA
Un nuovo motore antivirus, il bilanciamento del carico delle risorse server e le esclusioni di scansione riducono il carico sul sistema.

GATEWAY INTERNET:

ALTE PRESTAZIONI
Potente motore antivirus, tecnologia di scansione intelligente e ottimizzata e bilanciamento del carico migliorano le prestazioni e riducono il numero di risorse necessarie per la scansione antivirus.

SUPPORTO MULTIPIATTAFORMA
Kaspersky Security for Internet Gateway supporta gran parte dei gateway più diffusi basati sulle piattaforme Windows e Linux.

COLLABORAZIONE:

SICUREZZA ANTI-MALWARE PER LE FARM SHAREPOINT
Un'innovativa tecnologia di rilevamento consente di identificare e bloccare il malware in tempo reale, nel momento stesso in cui i file vengono caricati o scaricati.

FILTRAGGIO DEI CONTENUTI
Consente di prevenire il rischio di upload esterni inappropriati mediante l'applicazione di criteri per le comunicazioni interne e il blocco dell'archiviazione dei file inappropriati per tipo di file e contenuto.

KASPERSKY SECURITY FOR MOBILE

Soluzione di sicurezza completa per i dispositivi mobili che combina Mobile Device Management (MDM) ed Endpoint Security for Mobile Devices.

Kaspersky MDM semplifica e velocizza la configurazione sicura dei dispositivi mobili, mentre Kaspersky Endpoint Security for Mobile Devices assicura la protezione necessaria per contrastare le minacce di oggi persino sui dispositivi personali degli utenti.

FUNZIONALITÀ DI KASPERSKY SECURITY FOR MOBILE NEI DETTAGLI:

FUNZIONALITÀ PER L'EFFICIENZA IT:

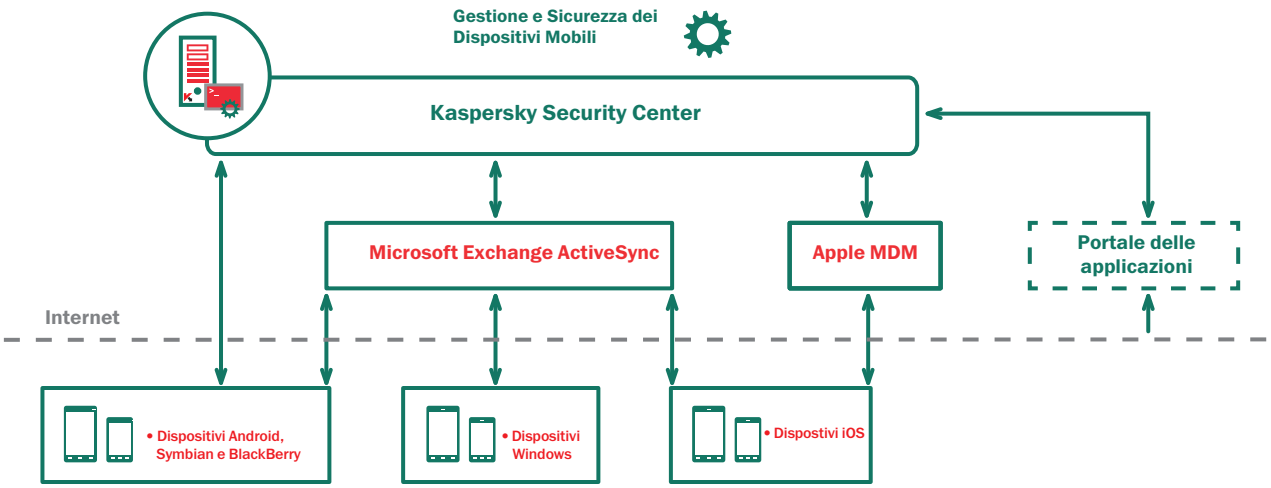
CONFIGURAZIONE SEMPLIFICATA TRAMITE UN'UNICA CONSOLE
Diversamente da altre soluzioni, la soluzione Kaspersky Lab consente agli amministratori di utilizzare un'unica console per gestire dispositivi mobili, endpoint fisici, sistemi virtuali, crittografia e strumenti per l'applicazione di criteri.

PORTALE DELLE APPLICAZIONI PRIVATE
Gli amministratori pubblicano un portale aziendale contenente collegamenti ad applicazioni approvate. È possibile limitare gli utenti ad utilizzare solo tali applicazioni.

PROVISIONING IN MODALITÀ OTA (OVER-THE-AIR)
Consente di proteggere i telefoni in modalità remota con l'invio di un'e-mail o di un SMS contenente un collegamento al portale aziendale da dove gli utenti possono scaricare il profilo e le applicazioni approvate. L'accesso ai dati non verrà concesso fino all'accettazione dell'utente.

CONFIGURAZIONE DI SICUREZZA
Garantisce l'integrità di hardware e software tramite l'abilitazione della funzionalità Rilevamento Rooting e Jailbreaking (Rooting and Jailbreak Detection). Tra le altre impostazioni di sicurezza figurano le impostazioni relative alla "disabilitazione della videocamera", alla password forzata e molte altre ancora.

CONFORMITÀ E APPLICAZIONE DI CRITERI
Controllo Applicazioni (Application Control) consente il monitoraggio e il controllo dell'utilizzo delle applicazioni, incluso il supporto delle funzionalità "Nega Predefinito" (Default Deny) e "Consenti Predefinito" (Default Allow).



CONTROLLO DEI RISCHI LEGATI ALLA SICUREZZA:

CRITTOGRAFIA
I dati in movimento vengono protetti tramite una crittografia trasparente dei dati a livello di intero disco o di file, applicabile anche a un contenitore.

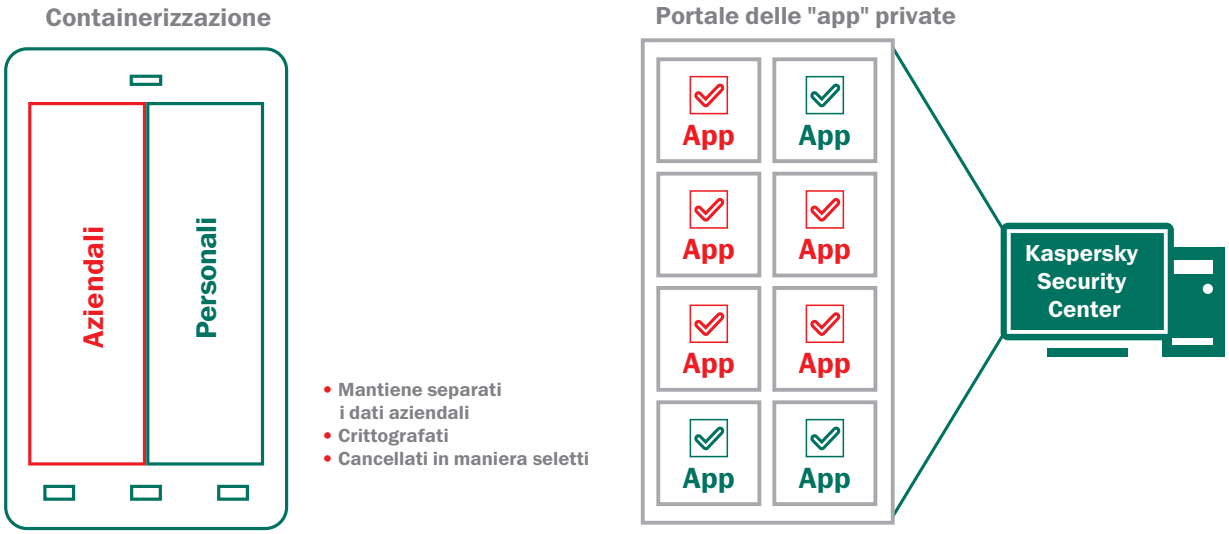
PROTEZIONE CONTRO I FURTI
Gli amministratori possono eseguire la cancellazione remota parziale o completa dei dati di un dispositivo, identificare la posizione di un dispositivo smarrito tramite la funzionalità GPS "Localizzazione" (Find) e ricevere notifica in caso di rimozione o sostituzione di una scheda SIM.

PROTEZIONE ANTI-MALWARE PER I DISPOSITIVI MOBILI
Il motore anti-malware di Kaspersky Lab fornisce molteplici livelli di rilevamento che includono una protezione assistita da cloud e si combina con un browser protetto e con una potente funzionalità anti-spam per garantire una protezione efficace del dispositivo contro il software dannoso.

INTEGRITÀ DEI DATI AZIENDALI E PERSONALI:

CONTENITORI
A fronte di uno scenario dominato dall'uso dei dispositivi personali dei dipendenti, i dati e le applicazioni aziendali possono essere inseriti in "contenitori" isolati. Ciò garantisce il massimo livello di sicurezza dei dati aziendali e un'integrità ottimale dei contenuti personali.

STRUMENTI PER LA SICUREZZA DEI DATI IN REMOTO
In caso di smarrimento di un dispositivo, è possibile attivare un blocco in remoto. I dati aziendali inclusi in un contenitore possono essere protetti, crittografati, gestiti in remoto e cancellati indipendentemente dai dati personali presenti sul dispositivo.



SOLUZIONE IDEALE PER LE INIZIATIVE "BYOD" (BRING YOUR OWN DEVICE)

Molti dipendenti utilizzano i propri dispositivi per svolgere attività sia di carattere personale che relative al lavoro aziendale. Di fatto, alcune organizzazioni incoraggiano i dipendenti a scegliere lo smartphone o il tablet che preferiscono da un rivenditore, mentre l'IT integra gli strumenti per l'accesso alla posta e ai dati aziendali sui dispositivi di proprietà dei dipendenti.

Un approccio BYOD garantisce una riduzione dei costi e un miglioramento della produttività, ma espone l'organizzazione a rischi legati alla sicurezza. I dati aziendali, protetti in maniera inadeguata e potenzialmente mescolati con dati personali, possono essere facilmente sfruttati da terzi non autorizzati. Spesso questi dispositivi vengono utilizzati anche dai familiari dei dipendenti che non prestano la dovuta cautela alla sicurezza delle applicazioni. Alcuni dispositivi vengono compromessi persino tramite attività di rooting o jailbreaking.

Kaspersky Security for Mobile consente di risolvere questo tipo di problemi garantendo la configurazione e l'implementazione sicura di smartphone e tablet tramite la stessa console utilizzata per la sicurezza della rete aziendale. Gli amministratori IT possono avere la certezza che i dispositivi degli utenti vengano configurati con le impostazioni necessarie e che risultino protetti in caso di perdita, furto o uso improprio da parte dell'utente.

KASPERSKY SYSTEMS MANAGEMENT

Ecco Kaspersky Systems Management, una soluzione che offre una vasta gamma di efficaci strumenti IT per la produttività scritti con lo stesso codice e gestiti da un'unica console, riuniti in una piattaforma che assicura semplicità e automazione, con tutta la sicurezza e il controllo necessari.

STRUMENTI IT ETEROGENEI CREANO COMPLESSITÀ, CHE È IL PRINCIPALE NEMICO DELLA SICUREZZA.

Mai più fare le cose due volte
Non c'è più bisogno di configurare sistemi individuali per utenti nuovi e già attivi: utilizzando la tecnologia di provisioning dei sistemi, è possibile creare, gestire e implementare le immagini disco da una posizione centralizzata.

Ottimizzazione della sicurezza
Sappiamo che gli amministratori trascorrono spesso gran parte delle loro giornate ad aggiornare le patch. Kaspersky consente di eliminare la complessità identificando le vulnerabilità presenti e le correzioni che si possono rimandare al termine dell'orario di ufficio. Tale definizione delle priorità permette agli amministratori di programmare le attività giornaliere e migliorare il loro approccio alla sicurezza.

Maggiore efficienza nel lavoro
Gli amministratori hanno la possibilità di installare in modalità remota immagini, aggiornamenti, patch e applicazioni. In caso di malfunzionamenti, il personale IT può accedere in modalità remota alla macchina dell'utente e intervenire sul sistema per risolvere il problema. Ciò si traduce in un risparmio di tempo per l'amministratore, che non deve passare da una postazione all'altra o trascorrere ore improduttive e frustranti a offrire assistenza telefonica.

Queste e altre funzionalità fanno parte di Kaspersky Systems Management e sono accessibili tramite la console di amministrazione Kaspersky Security Center. Poiché ogni strumento non richiede una propria console, i comandi sono coerenti e intuitivi e non richiedono formazione extra.

FUNZIONALITÀ DI KASPERSKY SYSTEMS MANAGEMENT:

PROVISIONING DI SISTEMI OPERATIVI E APPLICAZIONI
Creazione, archiviazione, clonazione e implementazione semplificate delle immagini del sistema da una posizione centralizzata. Garantisce che i sistemi siano forniti all'utente senza problemi e con le configurazioni di sicurezza ottimali. Questo strumento è particolarmente adatto per la migrazione a Microsoft Windows 8.

CONTROLLO TOTALE DELLE VULNERABILITÀ
Una scansione hardware e software, lanciata con un solo clic, confronta i risultati di diversi database e permette così di stabilire quali vulnerabilità hanno bisogno di attenzione immediata e quali invece si possono rimandare al termine dell'orario di ufficio.

INSTALLAZIONE SOFTWARE REMOTA E FLESSIBILE
È possibile ridurre al minimo il carico di lavoro della rete utilizzando le implementazioni manuali o quelle programmate.

AGENTI REMOTI
È possibile assegnare una workstation in un ufficio periferico in qualità di agenti di agente a livello centrale. Inviando un aggiornamento ad un altro ufficio e utilizzando la workstation locale assegnata per distribuire l'aggiornamento al resto della sede si ottiene una riduzione dell'impiego di banda.

SUPPORTO DELLA TECNOLOGIA WAKE-ON-LAN
Kaspersky Systems Management consente di avviare una workstation in modalità remota per l'implementazione negli orari di chiusura o per assistenza.

STRUMENTI PER LA RISOLUZIONE DEI PROBLEMI
È possibile collegarsi in remoto a un sistema client per la risoluzione dei problemi da un'unica console amministrativa.

SUPPORTO DI MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS)
Kaspersky Systems Management sincronizza regolarmente i dati sugli aggiornamenti e gli hotfix disponibili con i server, compreso Microsoft Windows Update, li scarica tramite Windows Update Services e li distribuisce in maniera efficiente.

CONTROLLO ACCESSI ALLA RETE (NAC)
Il Controllo Accessi alla Rete (NAC - Network Admission Control) consente di creare criteri per i dispositivi "guest" della rete. I dispositivi guest (compresi i dispositivi mobili) vengono riconosciuti automaticamente e inviati a un portale aziendale, nel quale, con le credenziali corrette, possono utilizzare le risorse precedentemente approvate.

INVENTARI HARDWARE E SOFTWARE
I PC, i dischi rigidi e persino i dispositivi rimovibili vengono automaticamente rilevati e inseriti negli inventari. L'introduzione di un nuovo dispositivo genera una notifica per l'amministratore. Questa funzionalità consente all'amministratore di tenere traccia dello stato e dell'utilizzo dell'hardware nella rete.

PROVISIONING E CONTROLLO DELLE LICENZE
Kaspersky Systems Management fornisce un report preciso sui software in uso all'interno dell'ambiente, con il quale è possibile regolare i costi delle licenze e identificare gli utenti non in regola. Grazie all'integrazione con gli strumenti di controllo degli endpoint di Kaspersky Lab, è possibile restringere l'uso alle sole applicazioni e versioni autorizzate e limitare il numero delle licenze in uso.

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server offre una protezione affidabile da tutti i tipi di programmi dannosi per i server in esecuzione su Microsoft® Windows®, Novell NetWare e Linux.

Una protezione antivirus per i server è essenziale poiché la presenza anche di un solo file infetto su un server può compromettere le workstation di tutti gli utenti della risorsa. Una protezione adeguata del file server non solo garantisce la piena sicurezza degli utenti e dei loro dati, ma elimina anche il rischio che programmi dannosi accedano a copie di backup dei file, causando ripetuti attacchi malware e altri pericolosi incidenti.

CARATTERISTICHE PRINCIPALI DEL PRODOTTO*

- Supporto delle ultime versioni delle piattaforme Microsoft® Windows® e Linux
- Uso ottimizzato delle risorse di sistema
- Supporto dei sistemi HSM (Hierarchical Storage Management)
- Protezione di server terminal e server cluster
- Predisposizione VMware certificata
- Supporto dei file system NSS
- Supporto di FreeBSD

FUNZIONALITÀ

- Protezione di file server in esecuzione su Windows® (compreso Windows Server® 2008 R2), Linux (compreso Samba) e Novell NetWare
- Protezione proattiva ottimizzata contro nuovi programmi dannosi
- Protezione antivirus in tempo reale
- Trattamento delle infezioni attive
- Scansione pianificata degli archivi di file
- Scansione delle aree critiche del sistema
- Isolamento delle workstation infette
- Scalabilità
- Archiviazione di backup dei dati prima della disinfezione o della rimozione
- Installazione, gestione e aggiornamenti centralizzati
- Scelta dei metodi di installazione e gestione
- Sistema di scansione flessibile e scenari di risposta agli incidenti
- Sistema di notifica sullo stato delle applicazioni
- Report esaustivi sullo stato di protezione della rete

APPLICAZIONI

- Kaspersky Anti-Virus for Windows® Servers Enterprise Edition
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Endpoint Security per Windows®
- Kaspersky Anti-Virus for Novell NetWare
- Kaspersky Security Center

*Le funzionalità dei prodotti possono variare a seconda della combinazione di componenti utilizzata. Per ulteriori informazioni sulle funzionalità dei singoli componenti, fate riferimento alle descrizioni dei prodotti disponibili sul sito Web: www.kaspersky.com.

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server è una soluzione che protegge i server di posta e groupware da programmi dannosi e spam.

Il prodotto comprende applicazioni in grado di proteggere tutti i server di posta più diffusi, inclusi Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim e CommuniGate Pro. Può essere utilizzato anche per configurare un gateway di posta dedicato.

CARATTERISTICHE PRINCIPALI DEL PRODOTTO*

PROTEZIONE DEI SERVER DI POSTA
Protezione anti-malware e anti-spam del traffico di posta elettronica per tutti i sistemi di posta più diffusi.

OTTIMIZZAZIONE DELLE RISORSE DI SISTEMA
Un nuovo motore antivirus, il bilanciamento del carico delle risorse server e le esclusioni di scansione riducono il carico sul sistema.

INTEGRAZIONE CON KSN PER LA PROTEZIONE ANTI-SPAM
Migliora il tasso di rilevamento dello spam grazie all'integrazione con il motore di identificazione delle minacce basato su cloud di Kaspersky Lab (KSN).

RIDUZIONE DEL CARICO DEL TRAFFICO
Una tecnologia di filtraggio anti-spam avanzata basata su cloud consente di ridurre considerevolmente il carico del traffico.

FUNZIONALITÀ

- Protezione integrata dei server di posta da tutti i tipi di programmi dannosi
- Efficiente protezione contro lo spam
- Protezione antivirus in tempo reale
- Scansione pianificata di e-mail e database
- Protezione per i server di posta Sendmail, qmail, Postfix, Exim e CommuniGate Pro
- Scansione di messaggi, database e altri oggetti su server Lotus® Domino®
- Scansione di tutti i messaggi su server Microsoft® Exchange, comprese le cartelle pubbliche
- Filtro dei messaggi in base al tipo di allegato
- Scalabilità
- Supporto di cluster Microsoft® Exchange Server 2007 e DAG per Microsoft® Exchange Server 2010
- Archiviazione di backup dei dati prima della disinfezione o della rimozione
- Isolamento degli oggetti infetti
- Annullamento della scansione ripetuta della posta
- Strumenti di facile utilizzo per l'installazione, la gestione e gli aggiornamenti
- Report esaustivi sullo stato della protezione
- Sistema di scansione flessibile e scenari di risposta agli incidenti
- Sistema di notifica sullo stato delle applicazioni

APPLICAZIONI

- Kaspersky Security for Microsoft® Exchange Servers
- Kaspersky Anti-Virus for Lotus® Domino®
- Kaspersky Security for Microsoft® Exchange Server 2003
- Kaspersky Security for Linux Mail Server

*Le funzionalità dei prodotti possono variare a seconda della combinazione di componenti utilizzata. Per ulteriori informazioni sulle funzionalità dei singoli componenti, fate riferimento alle descrizioni dei prodotti disponibili sul sito Web: www.kaspersky.com.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway garantisce un accesso sicuro a Internet a tutti i dipendenti di un'azienda.

Kaspersky Security for Internet Gateway supporta gran parte dei gateway più diffusi basati sulle piattaforme Windows e Linux. Rimuove automaticamente dal flusso di dati i programmi dannosi conosciuti e quelli potenzialmente pericolosi in esecuzione tramite i protocolli HTT P, HTT PS, FT P, POP3 e SMTP. La tecnologia di ottimizzazione, la scalabilità e il supporto delle piattaforme più recenti lo rendono il prodotto ideale per grandi aziende con volumi di traffico particolarmente elevati.

CARATTERISTICHE PRINCIPALI DEL PRODOTTO*

- Protezione di Microsoft® Forefront® TMG
- Ampia gamma di strumenti per la configurazione e la gestione dei criteri
- Scansione delle connessioni VPN
- Protezione del traffico e-mail (tramite i protocolli POP3 e SMTP)
- Scansione del traffico HTTP e FTP dai server pubblicati
- Predisposizione VMware certificata

FUNZIONALITÀ

- Scansione in tempo reale del traffico Internet che utilizza i protocolli HTTP, HTTPS, FTP, POP3 e SMTP
- Protezione integrata da tutti i tipi di programmi dannosi
- Supporto dei server proxy Squid, Blue Coat e Cisco®
- Archiviazione di backup
- Bilanciamento del carico dei processi server
- Scalabilità
- Strumenti di facile utilizzo per l'installazione, la gestione e gli aggiornamenti
- Sistema di scansione flessibile e scenari di risposta agli incidenti
- Report esaustivi sullo stato di protezione della rete

APPLICAZIONI

- Kaspersky Anti-Virus for Microsoft® ISA Server and Forefront® TMG Standard Edition
- Kaspersky Anti-Virus for Microsoft® ISA Server Enterprise Edition
- Kaspersky Anti-Virus for Proxy Server

*Le funzionalità dei prodotti possono variare a seconda della combinazione di componenti utilizzata. Per ulteriori informazioni sulle funzionalità dei singoli componenti, fate riferimento alle descrizioni dei prodotti disponibili sul sito Web: www.kaspersky.com.

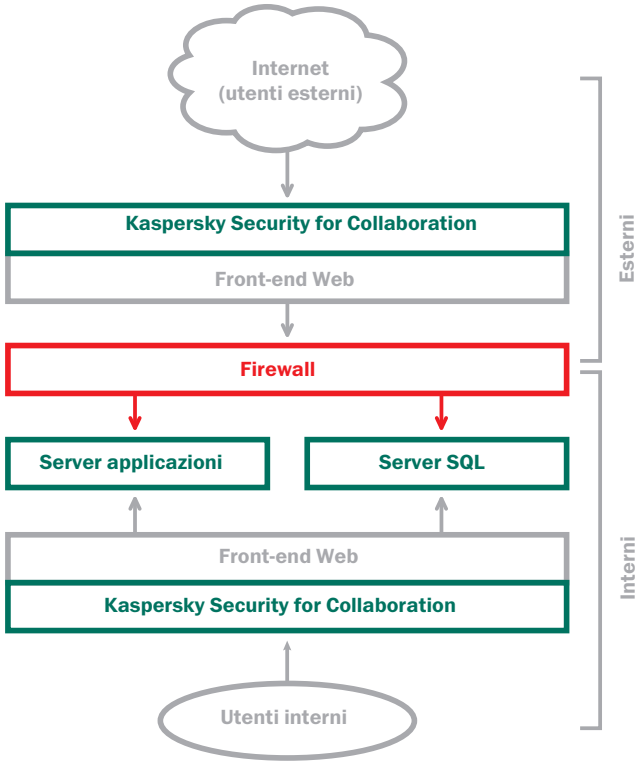
KASPERSKY SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration fornisce le più recenti tecnologie in materia di protezione per la vostra piattaforma di collaborazione, combinando facilità di gestione ed elevati tassi di rilevamento malware.

Kaspersky Security for Collaboration utilizza il motore antivirus pluripremiato di Kaspersky per garantire la protezione degli ambienti Microsoft® SharePoint®. Grazie alla pluripremiata tecnologia di rilevamento malware su cui si basa, il prodotto è in grado di tutelare la sicurezza di un singolo server o di intere farm SharePoint, mentre le sue funzionalità per il filtro di file e contenuti aiutano a prevenire l'archiviazione di contenuti inappropriati.

FUNZIONALITÀ

- Tecnologia innovativa di rilevamento malware progettata per identificare e bloccare qualsiasi minaccia in tempo reale, ovvero nel momento stesso in cui i file vengono caricati o scaricati
- Impedisce agli utenti finali di archiviare tipi di file specifici (ad esempio, musica, video, file eseguibili)
  o file con contenuti inappropriati
- Possibilità di configurare le impostazioni di gestione globali su tutti i server protetti da un'unica dashboard
- Gestione semplice e intuitiva, che non necessita di formazione specifica
- Integrazione con Active Directory, che semplifica la configurazione e l'autenticazione degli utenti
- Registri dettagliati e backup dei file modificati per aiutare gli amministratori ad affrontare al meglio violazioni o problemi di sicurezza
- Report flessibili e accurati



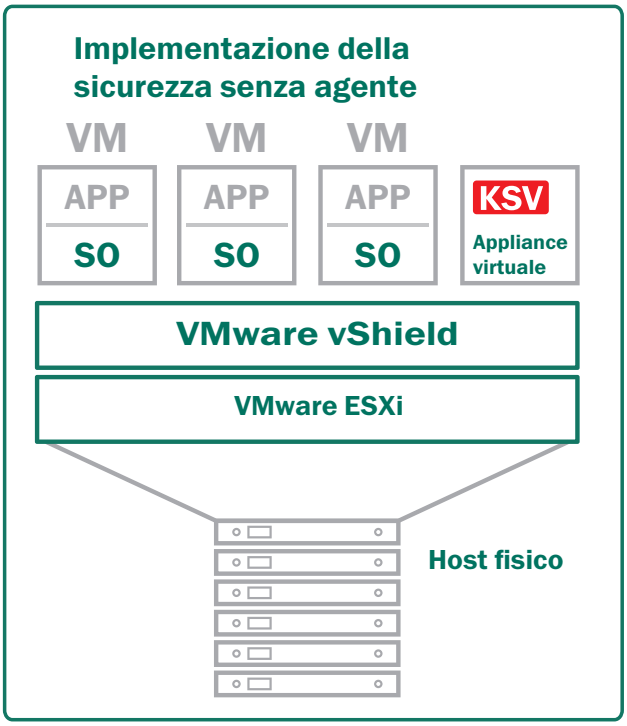
KASPERSKY SECURITY FOR VIRTUALIZATION

La soluzione Kaspersky Security for Virtualization, appositamente ideata per gli specifici requisiti degli ambienti IT virtualizzati, offre una pluripremiata funzionalità di protezione anti-malware per server, desktop e data center virtualizzati.

Kaspersky Security for Virtualization è una soluzione anti-malware senza agente che vi permette di proteggere con maggiore efficienza la vostra infrastruttura virtualizzata, garantendovi prestazioni migliori e un impatto ridotto sulla densità della virtualizzazione. L'applicazione è facile da implementare e le sue avanzate funzionalità di gestione permettono di semplificare una vasta gamma di attività di sicurezza solitamente svolte sulle risorse informatiche, sia fisiche che virtuali.

FUNZIONALITÀ PER PROTEZIONE E PRESTAZIONI

- Sicurezza centralizzata. Kaspersky Security for Virtualization è un'appliance virtuale che si collega a vShield Endpoint di VMware, per garantire funzionalità di scansione anti-malware. Offre un unico motore anti-malware centralizzato e un unico database per ogni host fisico.
- Motore antivirus avanzato. Le pluripremiate tecnologie anti-malware di Kaspersky, combinate con l'impareggiabile frequenza degli aggiornamenti garantita da Kaspersky, vi aiutano a contrastare le minacce nuove ed emergenti. Un analizzatore euristico assicura la massima protezione contro il malware polimorfo.
- Protezione automatica. Sulle nuove macchine virtuali viene automaticamente installata la protezione anti-malware, per eliminare falle di sicurezza ed errori di configurazione. Il database delle firme, costantemente aggiornato con le firme più recenti, garantisce la protezione delle VM guest, anche di quelle appena riattivate.
- Maggiore densità della virtualizzazione. Dal momento che Kaspersky Security for Virtualization è una soluzione senza agente, aiuta a prevenire picchi di aggiornamento e picchi di scansione, consentendo di ottenere una maggiore densità della virtualizzazione, di ridurre l'impatto sulle prestazioni e di eliminare le falle di sicurezza che possono crearsi con l'uso di alcuni prodotti con agente.



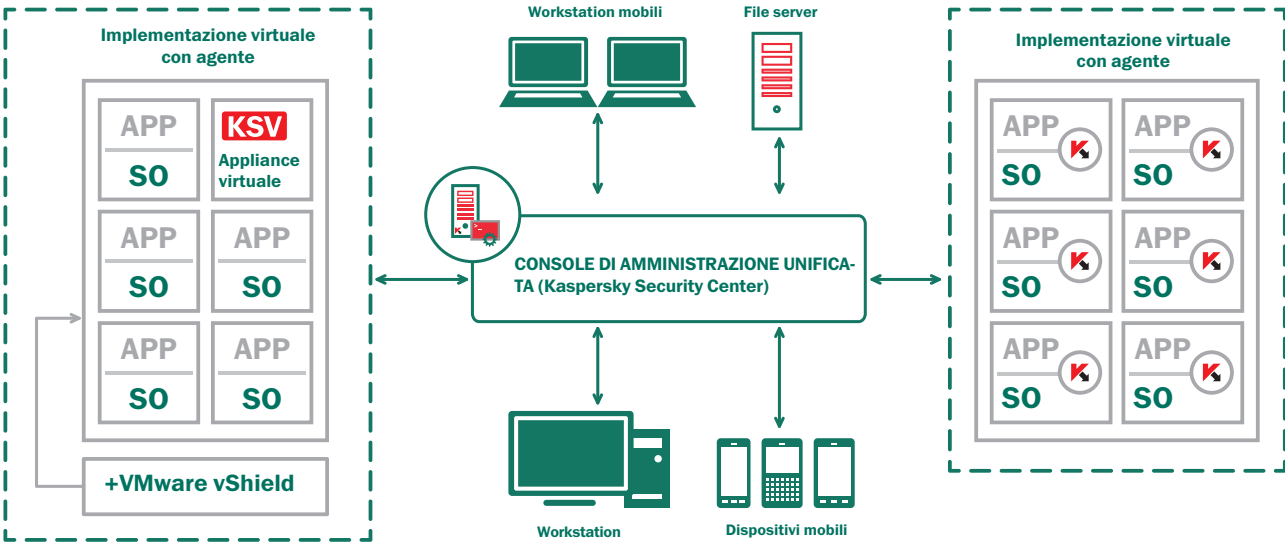
Kaspersky Security for Virtualization offre la protezione antivirus senza agente per le implementazioni di piattaforme VMware.

FUNZIONALITÀ DI GESTIONE:

UNICA CONSOLE DI GESTIONE.
Kaspersky Security Center, disponibile senza costi aggiuntivi, è una console di gestione unificata che permette di gestire la sicurezza di macchine virtuali, macchine fisiche e dispositivi mobili.

SUPPORTO DI VMWARE VMOTION.
Grazie al supporto di VMware vMotion, Kaspersky Security for Virtualization garantisce una continuità della protezione anche al momento del trasferimento di un carico di lavoro da un host ESXi all'altro. Purché il nuovo host disponga delle licenze richieste, la protezione seguirà il carico di lavoro e tutte le impostazioni di sicurezza resteranno invariate.

INTEGRAZIONE CON VMWARE VCENTER.
Kaspersky Security for Virtualization riceve i dati sulle macchine virtuali da vCenter, incluso un elenco di tutte le macchine virtuali e dei relativi parametri. Oltre a offrire al team IT una maggiore visibilità, questa integrazione con vCenter assicura la protezione automatica di ogni nuova macchina virtuale configurata.



KSV Kaspersky Security for Virtualization Kaspersky Lab Security Solution

KASPERSKY ANTI-VIRUS FOR STORAGE

Kaspersky Anti-Virus for Storage protegge la famiglia EMC Celerra di prodotti per l'archiviazione di rete da tutti i tipi di malware.

I sistemi di archiviazione dati all'interno di una rete aziendale forniscono ai dipendenti di organizzazioni di qualsiasi dimensione un accesso condiviso alle informazioni rapido e agevole. Se la rete non è protetta, tuttavia, l'accesso a file condivisi può portare a conseguenze decisamente sgradevoli. Anche un singolo file infetto archiviato in un sistema può compromettere l'intera rete, causando potenzialmente danni di considerevole entità sul piano finanziario, della reputazione e della produttività. Questo è il motivo per cui una protezione completa dei sistemi di archiviazione di rete è assolutamente indispensabile.

Kaspersky Anti-Virus for Storage è perfettamente compatibile con l'intera gamma di prodotti EMC Celerra, ai quali fornisce una protezione di altissimo livello, rilevando e rimuovendo malware da file e archivi memorizzati nei sistemi Celerra. La soluzione consente agli amministratori di configurare il sistema in modo che venga eseguito un accurato processo di scansione in tempo reale di tutti gli oggetti al momento del loro salvataggio o della loro modifica oppure on-demand, se necessario.

FUNZIONALITÀ

- Protezione per i sistemi di archiviazione dati EMC Celerra
- Supporto di Windows Server® 2008 R2
- Supporto dei sistemi HSM (Hierarchical Storage Management)
- Protezione proattiva ottimizzata contro nuovi programmi dannosi
- Protezione antivirus in tempo reale
- Scansione pianificata degli archivi di file
- Scansione delle aree critiche del sistema
- Uso ottimizzato delle risorse di sistema
- Archiviazione di backup dei dati prima della disinfezione o della rimozione
- Scalabilità
- Predisposizione VMware certificata
- Installazione, gestione e aggiornamenti centralizzati tramite Kaspersky Security Center
- Integrazione completa con la piattaforma Kaspersky Endpoint Security for Business e con altri prodotti Kaspersky
- Sistema di notifica sullo stato delle applicazioni
- Report esaustivi sullo stato di protezione della rete

Kaspersky Lab Italia
sales.corporate@kaspersky.it
www.kaspersky.it

Tutto sulla sicurezza in Internet:
www.securelist.com

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

KASPERSKY lab