Kaspersky endpoint security

Ultimo aggiornamento lunedì 16 novembre 2015

Â Kaspersky Endpoint Security for Business | AdvancedÂ Sicurezza di livello superiore â€“ gestione IT estesaFunzionalitÃ di gestione estesa dei sistemiValutazione delle vulnerabilitÃ e gestione delle patchSicurezza multilivello, inclusa crittografiaWeb Control, Application Control, Device ControlSicurezza mobile e gestioneGestione centralizzata di sicurezza e sistemiUna singola console di gestione unificata che offre tecnologie di sicurezza degli endpoint di livello superiore e funzionalitÃ di gestione dei sistemi estese.Protezione dei desktop e laptop Windows, Linux e Mac*Sicurezza multilivelloÂ

Il piÃ¹ recente motore anti-malware di Kaspersky unisce sicurezza basata su firma, analisi euristica e del comportamento e tecnologie assistite da cloud per proteggere le aziende contro minacce conosciute, nuove e avanzate. Ã^ infatti in grado di offrire protezione a qualsiasi combinazione di desktop e laptop Mac, Linux e Windows.Aggiornamento della sicurezza in modo piÃ¹ efficienteÂ

I cybercriminali creano e distribuiscono ogni giorno nuovi e sempre piÃ¹ complessi malware. Per questo motivo Kaspersky fornisce aggiornamenti del database in modo molto piÃ¹ frequente rispetto ad altri fornitori di prodotti di sicurezza. Inoltre, utilizza piÃ¹ tecnologie di sicurezza avanzate per assicurare percentuali di rilevamento migliorate in modo sostanziale, riducendo al contempo le dimensioni degli aggiornamentiâ€¦ per liberare e rendere disponibile alle aziende una maggiore larghezza di banda da dedicare ad altre attivitÃ .Protezione contro minacce sconosciute e avanzateÂ Â

Quando viene rilasciato e diffuso un nuovo malware, si verifica un periodo di rischio elevato. Per offrire una protezione "zero-hour" contro queste minacce, le tecnologie e la threat intelligence di Kaspersky Lab si evolvono continuamente, per assicurare la protezione delle aziende anche delle minacce piÃ¹ nuove e sofisticate.Rilevamento di comportamenti sospettiÂ Â

Ogni volta che viene eseguito l'avvio di un'applicazione sulla rete aziendale, il System Watcher di Kaspersky monitora il comportamento dell'applicazione. Se viene rilevato un comportamento sospetto, System Watcher blocca automaticamente l'applicazione. Inoltre, poichÃ© System Watcher conserva una registrazione dinamica di sistema operativo, Registro di sistema e altro, Ã¨ in grado di eseguire il rollback automatico delle azioni dannose implementate dal malware prima che venisse bloccato.Protezione dagli exploitÂ Â

L'innovativa tecnologia AEP (Automatic Exploit Prevention) di Kaspersky consente alle aziende di assicurarsi che il malware non sia in grado di sfruttare le vulnerabilitÃ del sistema operativo o le applicazioni eseguite sulla rete. AEP monitora in modo specifico le applicazioni piÃ¹ frequentemente sottoposte ad attacchi, tra cui Adobe Reader, Internet Explorer, Microsoft Office, Java e molte altre ancora, per fornire un ulteriore livello di monitoraggio della sicurezza e di protezione contro minacce sconosciute.Controllo delle applicazioni e della connettivitÃ Â

Le attivitÃ di alcune applicazioni possono essere considerate a rischio elevato, anche se le applicazioni in sÃ© possono non essere classificate come pericolose. In molti casi, Ã¨ preferibile limitare questo tipo di attivitÃ . Il sistema HIPS (Host-Based Intrusion Prevention System) di Kaspersky limita le attivitÃ dell'endpoint in base al livello di affidabilitÃ assegnato all'applicazione. HIPS lavora insieme al firewall personale a livello delle applicazioni per limitare l'attivitÃ di rete.Blocco degli attacchi alla reteÂ

La tecnologia Network Attack Blocker di Kaspersky rileva e monitora le attivitÃ sospette sulla rete aziendale e consente di preconfigurare la risposta dei sistemi al rilevamento di comportamenti sospetti.Tutta la potenza del cloud, per una sicurezza ancora miglioreÂ Â

Grazie anche ai milioni di utenti che consentono a Kaspersky Security Network (KSN) di ricevere dati sui comportamenti sospetti dei propri computer, le aziende possono sfruttare una protezione superiore contro i malware piÃ¹ recenti. Questo flusso di dati in tempo reale consente infatti ai clienti di adottare una rapida risposta ai nuovi attacchi e di ridurre al minimo l'incidenza dei "falsi positivi".*Queste funzionalitÃ non sono tutte disponibili su tutte le piattaforme.Protezione dei file serverProtezione di ambienti eterogeneiÂ

Il nostro pluripremiato software per la sicurezza protegge i file server che eseguono Windows, Linux o FreeBSD. I processi di scansione ottimizzata assicurano un impatto minimo sulle prestazioni dei server. Oltre a proteggere i server in cluster, Kaspersky garantisce anche la sicurezza dei server terminal Microsoft e Citrix.Garanzia di una protezione affidabileÂ

Se si verifica un problema o un guasto su uno dei file server in uso, le tecnologie di sicurezza di Kaspersky si riattiveranno automaticamente al riavvio del file server.Miglioramento della gestibilitÃ Â

Ogni minuto speso per attivitÃ amministrative e generazione di report Ã¨ tempo che potrebbe essere dedicato ad attivitÃ strategicamente importanti. Per questo motivo Kaspersky offre una console centralizzata che consente di gestire la sicurezza di tutti gli endpoint, file server, workstation e dispositivi mobili e semplifica la generazione di report dettagliati.Ottimizzazione della sicurezza ed estensione della gestione dei sistemiEliminazione delle vulnerabilitÃ noteÂ

Le tecnologie di Kaspersky eseguono la scansione dell'intera rete aziendale per individuare vulnerabilitÃ risultanti da applicazioni o sistemi operativi privi di patch. La prioritÃ delle vulnerabilitÃ rilevate puÃ² essere definita automaticamente ed Ã¨ quindi possibile distribuire automaticamente patch e aggiornamenti. Grazie alla rapiditÃ con la quale sono distribuite le soluzioni di patching di Kaspersky, sarÃ possibile eliminare le vulnerabilitÃ in tempi piÃ¹ brevi.Gestione di risorse hardware e softwareÂ

Tutto il software e i dispositivi presenti nella rete vengono rilevati e registrati automaticamente in un inventario hardware e in un inventario software. L'inventario hardware comprende informazioni dettagliate su ciascun dispositivo e l'inventario software consente di controllare l'utilizzo del software e di bloccare applicazioni non autorizzate. Ã^ possibile rilevare automaticamente persino i dispositivi guest che tentano di accedere alla rete e concedere a tali dispositivi privilegi di accesso, senza compromettere la sicurezza dei dati e dei sistemi aziendali.Ottimizzazione della distribuzione di

applicazioniÂ
Ã^ possibile implementare il software mediante comandi diretti o programmare l'implementazione dopo l'orario di ufficio. Per alcuni programmi di installazione Ã¨ possibile specificare parametri aggiuntivi, per personalizzare il pacchetto software installato. L'uso di connessioni remote protette a qualsiasi desktop o computer client consente di risolvere rapidamente i problemi e un meccanismo di autorizzazione impedisce l'accesso remoto non autorizzato. Tutte le attivitÃ eseguite durante una sessione di accesso remoto sono registrate per garantire la tracciabilitÃ .Automazione e ottimizzazione della distribuzione del sistema operativoÂ
Le tecnologie di Kaspersky automatizzano e centralizzano la creazione, l'archiviazione e la clonazione di immagini protette del sistema. Le immagini sono conservate in un inventario speciale, da cui sono facilmente accessibili durante la distribuzione. La distribuzione delle immagini di workstation client puÃ² essere eseguita con server PXE (Preboot eXecution Environment), giÃ utilizzati in rete, o mediante le funzionalitÃ di Kaspersky. L'uso di segnali Wake-on-LAN consente di distribuire automaticamente le immagini dopo l'orario di ufficio. Ã^ incluso inoltre il supporto per UEFI.Riduzione del traffico: distribuzione remotaÂ
Quando Ã¨ necessario distribuire software o patch a un ufficio remoto, un'unica workstation locale puÃ² svolgere il ruolo di agente di aggiornamento per l'intero ufficio remoto, per ridurre i livelli di traffico sulla rete.Integrazione con i sistemi SIEMÂ
PoichÃ© i sistemi SIEM (Security Information and Event Management) possono svolgere un ruolo cruciale nel consentire alle aziende di livello enterprise un monitoraggio in tempo reale, Kaspersky ha introdotto il supporto per l'integrazione con due dei sistemi SIEM piÃ¹ noti: HP ArcSight e IBM QRadar.Crittografia delle informazioni riservateCrittografia avanzataÂ
Per proteggere le informazioni riservate, Kaspersky offre una crittografia avanzata che utilizza un algoritmo di crittografia AES con chiave a 256 bit e con approvazione NIST (n. 2980). Se vengono smarriti o rubati file o sistemi, gli utenti non autorizzati non potranno accedere ai dati crittografati. La crittografia di Kaspersky Ã¨ inoltre stata progettata per essere compatibile con FIPS 140-2 (in attesa di convalida).Soluzioni integrate, per una migliore gestibilitÃ Â
A differenza dei prodotti di crittografia della maggior parte degli altri produttori, che non vengono distribuiti come parte di una soluzione di sicurezza IT integrata, le tecnologie di crittografia di Kaspersky sono integrate all'interno di una codebase unificata, sviluppata da esperti della sicurezza Kaspersky. In questo modo l'applicazione di impostazioni di crittografia risulta semplificata perchÃ© parte degli stessi criteri che coprono le difese anti-malware, i controlli degli endpoint e altre tecnologie di sicurezza degli endpoint.Crittografia dell'intero disco e crittografia a livello di fileÂ
Per una crittografia "vicina all'hardware" e per semplificare l'esecuzione di una strategia di crittografia completa in un'unica operazione, la crittografia dell'intero disco (FDE) agisce sui settori fisici del disco. La crittografia a livello di file (FLE) contribuisce a proteggere la condivisione dei dati sulla rete. Per maggiore sicurezza, quando un file Ã¨ crittografato, il file originale non crittografato viene cancellato dal disco rigido.Crittografia dei supporti rimovibiliÂ
Per proteggere i dati che devono essere trasferiti su dispositivi rimovibili, la funzionalitÃ di Crittografia dei supporti rimovibili puÃ² eseguire la crittografia dell'intero disco e la crittografia a livello di file.Crittografia in "modalitÃ portatile"Â
Per trasferire dati sensibili tramite e-mail, Internet o dispositivi rimovibili, Ã¨ possibile configurare facilmente pacchetti di file e cartelle autoestraenti crittografati, protetti da password. Una speciale "modalitÃ portatile" per la crittografia a livello di file sui supporti rimovibili consente il trasferimento sicuro dei dati, anche sui computer che non utilizzano Kaspersky Endpoint Security for Windows.Supporto di Single Sign-on e smartcard/tokenÂ
Quando un utente accende il PC e immette nome utente e password, la funzionalitÃ Single Sign-on consente all'utente l'accesso immediato ai dati crittografati presenti sul disco rigido del PC. CiÃ² consente di rendere i processi di crittografia e decrittografia virtualmente trasparenti all'utente, contribuendo ad aumentare efficienza e produttivitÃ . Ã^ inoltre supportata l'autenticazione a due fattori, via smartcard e token.Supporto di Intel AES-NI e altroÂ
Il supporto di Intel AES-NI consente una crittografia e decrittografia piÃ¹ rapide dei dati, per molti sistemi basati su processore Intel e su processore AMD*. La tecnologia di crittografia dell'intero disco supporta inoltre le piattaforme basate su UEFI. Ã^ inoltre disponibile il supporto per le tastiere non QWERTY.*Non Ã¨ disponibile il supporto per tutti i processori.Protezione dei dispositivi mobili*Solida sicurezza mobileÂ
Grazie alla combinazione delle tecnologie piÃ¹ avanzate del settore Kaspersky offre protezione contro le minacce mobili piÃ¹ recenti. Il software anti-phishing offre protezione dai siti Web che tentano di sottrarre informazioni o identitÃ e il software anti-spam consente di filtrare ed escludere le chiamate e i messaggi indesiderati. I flessibili strumenti di controllo consentono di bloccare l'avvio di applicazioni non autorizzate e di impedire l'accesso a siti Web pericolosi. Gli incidenti di rooting e jailbreaking vengono rilevati automaticamente e i dispositivi vengono bloccati.Separazione di dati aziendali e personaliÂ
La tecnologia di "isolamento delle app" di Kaspersky consente di configurare speciali contenitori su ciascun dispositivo. Le applicazioni aziendali vengono quindi archiviate nei contenitori, separate in tal modo completamente dai dati personali degli utenti. Ã^ possibile applicare la crittografia a tutti i dati inseriti nei contenitori e impedire che i dati vengano copiati e incollati al di fuori del contenitore; Ã¨ inoltre possibile richiedere una ulteriore autorizzazione dell'utente prima di consentire l'avvio delle applicazioni inserite nei contenitori. Se un dipendente lascia l'azienda, la funzionalitÃ di cancellazione selettiva controllata in remoto consente di eliminare il contenitore aziendale, senza eliminare i dati personali e le impostazioni del proprietario del dispositivo.Supporto di piattaforme MDM comuniÂ
Con funzionalitÃ MDM (Mobile Device Management) migliorate, Ã¨ facile applicare criteri MDM individuali o di gruppo ai dispositivi MDM Microsoft Exchange ActiveSync e iOS, grazie a una singola interfaccia. Il supporto per Samsung KNOX consente di gestire diverse impostazioni per i dispositivi Samsung.Blocco, cancellazione dei dati e localizzazione dei dispositivi smarriti o rubatiÂ
FunzionalitÃ di sicurezza attivabili da remoto consentono di proteggere i dati aziendali presenti su dispositivi smarriti o

rubati. Gli amministratori e gli utenti possono infatti bloccare il dispositivo, eliminare i dati aziendali e individuare la posizione del dispositivo. Qualora la scheda SIM venga cambiata da chi ha sottratto il dispositivo, la funzionalitÃ SIM Watch invierÃ all'utente il nuovo numero di telefono e consentirÃ quindi di eseguire comunque le funzionalitÃ di protezione dai furti. Il supporto per Google Cloud Messaging (GCM) consente di assicurare che i telefoni Android ricevano rapidamente i comandi per la protezione dai furti.Portale self-serviceÂ
Lo speciale Portale self-service di Kaspersky semplifica l'abilitazione dei dispositivi mobili personali all'interno della rete aziendale. Il portale offre inoltre agli utenti l'accesso remoto a funzionalitÃ di protezione dai furti per consentire loro di rispondere rapidamente alla perdita di un dispositivo e di ridurre i rischi di perdita dei dati senza aggiungere ulteriore carico di lavoro per gli amministratori.Riduzione del carico di lavoro degli amministratori ITÂ
Una singola console centralizzata consente di gestire i dispositivi mobili e la relativa sicurezza e semplifica l'applicazione di criteri coerenti su piattaforme mobili diverse. Inoltre, la console Web di Kaspersky consente di gestire i dispositivi mobili e la relativa sicurezza, piÃ¹ la sicurezza di altri endpoint, da qualsiasi postazione che abbia accesso online.*Determinate funzionalitÃ non sono disponibili su alcune delle piattaforme mobili supportate.Controllo di applicazioni, dispositivi e dell'accesso a InternetWhitelisting dinamico per completare la sicurezzaÂ
Application Control costituisce l'implementazione piÃ¹ completa del settore. Kaspersky Ã¨ l'unico fornitore di prodotti di sicurezza che ha investito nella creazione di un proprio Whitelist Lab che controlla la presenza di rischi per la sicurezza nelle applicazioni. Il nostro database di applicazioni inserite nella whitelist comprende piÃ¹ di 1,3 miliardi di file unici e cresce al ritmo di 1 milione di file al giorno. Application Control e Dynamic Whitelisting semplificano l'applicazione di un criterio Default Deny che blocchi tutte le applicazioni tranne quelle inserite nella whitelist. Se si desidera introdurre o aggiornare un criterio Default Deny, la nuova modalitÃ di test consente di configurare il criterio in un ambiente di test, in modo che sia possibile controllarne la configurazione prima di distribuirlo per l'implementazione.Protezione contro la connessione di dispositivi non autorizzatiÂ
Gli strumenti Device Control di Kaspersky Lab semplificano la gestione dei dispositivi autorizzati ad accedere alla rete aziendale. Ãˆ possibile configurare controlli basati sull'ora del giorno, la posizione geografica o il tipo di dispositivo. Ãˆ anche possibile allineare i controlli con Active Directory per una gestione e un'assegnazione dei criteri piÃ¹ granulari. Gli amministratori possono inoltre utilizzare delle maschere per la creazione delle regole di Device Control, per inserire facilmente piÃ¹ dispositivi nelle whitelist e autorizzarne l'uso.Monitoraggio e controllo dell'accesso a InternetÂ
Gli strumenti Web Control consentono di configurare i criteri per l'accesso a Internet e di monitorare l'uso di Internet. Ãˆ possibile vietare, limitare, consentire o controllare le attivitÃ degli utenti su singoli siti Web o categorie di siti Web, come i siti di giochi, social networking o giochi d'azzardo. I controlli geografici e sull'orario possono essere allineati con Active Directory per semplificare la gestione e la definizione di criteri..Centralizzazione delle attivitÃ di gestioneControllo di tutte le funzionalitÃ da un'unica consoleÂ
Kaspersky Endpoint Security for Business | Select include Kaspersky Security Center, una singola console di gestione unificata che assicura una visibilitÃ completa e un controllo totale su tutte le tecnologie di sicurezza degli endpoint Kaspersky Lab in esecuzione nell'ambiente aziendale. Kaspersky Security Center consente di gestire la sicurezza di dispositivi mobili, laptop, desktop, file server, macchine virtuali e altro, con la comoditÃ di una singola console come postazione di controllo.Assegnazione di responsabilitÃ diverse ad amministratori diversiÂ
Il controllo dell'accesso basato sui ruoli consente di suddividere le responsabilitÃ nell'ambito della gestione della sicurezza e della gestione dei sistemi tra piÃ¹ amministratori. Potrebbe essere necessario, ad esempio, che un amministratore si occupi della gestione della sicurezza degli endpoint, dei controlli degli endpoint e della sicurezza mobile e un altro amministratore si occupi della crittografia dei dati e di tutte le funzioni di gestione dei sistemi. La console Kaspersky Security Center puÃ² essere facilmente personalizzata in modo che ciascun amministratore possa accedere solo agli strumenti e alle informazioni pertinenti alle responsabilitÃ a lui assegnate.Elevato livello di integrazioneÂ PoichÃ© codice strettamente integrato ha come risultato prodotti che offrono una maggiore sicurezza, tutte le tecnologie di controllo degli endpoint sono state sviluppate dal team interno di Kaspersky Lab. L'intera funzionalitÃ di protezione degli endpoint Ã¨ contenuta nella stessa codebase per garantire l'assenza di problemi di incompatibilitÃ e offrire agli utenti tecnologie di sicurezza perfettamente integrate piÃ¹ efficaci nel proteggere gli ambienti IT e una gestione centralizzata che consente di risparmiare tempo.Informazioni tecniche

Â Â

Â