KASPERSKY SECURITY FOR COLLABORATION

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

La piattaforma utilizzata per condividere file e informazioni fornisce anche un sistema ideale per una rapida diffusione di malware pericoloso e altre minacce IT. Per offrire un ambiente di lavoro condiviso sicuro e senza problemi, Kaspersky Lab ha sviluppato una soluzione che combina facilità di gestione e protezione avanzata in tempo reale contro gli attacchi malware e le perdite dei dati sensibili.

- Pluripremiato motore anti-malware
- "Ricerca e protezione" dei dati riservati
- Controllo degli accessi ai dati
- Protezione in tempo reale basata su cloud - Kaspersky Security Network
- Filtro di file e contenuti
- Protezione anti-phishing
- Backup e archiviazione
- Gestione flessibile centralizzata
- Console di amministrazione intuitiva

CARATTERISTICHE PRINCIPALI

PROTEZIONE COMPLETA DELLA PIATTAFORMA SHAREPOINT.

Chi utilizza Microsoft SharePoint Server sa bene che, poiché tutto il contenuto è archiviato in un database SQL, le soluzioni tradizionali per la sicurezza degli endpoint non sono sufficienti. Kaspersky Security for Collaboration applica una pluripremiata protezione anti-malware avanzata in tutta la farm SharePoint e a tutti i suoi utenti. 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 condivisi dalle minacce basate sul Web.

DATA LOSS PREVENTION.

Per controllare e proteggere la condivisione dei dati sensibili, è innanzitutto necessario identificare tali dati. 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. I dati personali e delle carte di pagamento vengono specificamente sottoposti a protezione e controllo, mentre ricerche basate sulla struttura consentono di rintracciare documenti sensibili, ad esempio i database dei clienti.

APPLICAZIONE DEI CRITERI DI COMUNICAZIONE.

Le funzionalità di 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.

FACILITÀ DI GESTIONE.

La sicurezza dell'intera server farm può essere amministrata centralmente da una singola dashboard intuitiva. L'amministrazione è semplice e rapida, e non richiede alcuna formazione specifica.

PROTEZIONE ANTIVIRUS

- **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:** 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 assicura l'impossibilità da parte degli utenti di utilizzare un tipo di file proibito in violazione dei criteri di sicurezza.
- **Protezione di wiki/blog:** consente di proteggere tutti gli archivi di SharePoint, compresi wiki e blog.
- **Filtro dei contenuti:** impedisce l'archiviazione di file che includono contenuti inappropriati, indipendentemente dal tipo di file. Il contenuto di ogni file viene analizzato in base alle parole chiave. Gli utenti possono inoltre creare dizionari personalizzati per il filtro dei contenuti.

DATA LOSS PREVENTION

- **Scansione dei documenti per il rilevamento di informazioni sensibli:** Kaspersky Security for Collaboration esegue la scansione di tutti i documenti scaricati dai server SharePoint per rilevare la presenza di informazioni riservate.

  La soluzione integra moduli che identificano tipi di dati specifici, verificando che soddisfino le relative normative legali, ad esempio dati personali (definiti per conformità a normative quali HIPAA o la Direttiva UE 95/46/CE) o dati dello standard PCI DSS (Payment Card Industry Data Security Standard).

  I dati vengono sottoposti a scansione a fronte di dizionari tematici integrati, aggiornati regolarmente, che coprono categorie quali "Finanza", "Documenti amministrativi" e "Linguaggio umiliante e offensivo", e a fronte di dizionari personalizzati.
- **Ricerca di dati strutturati:** se in un messaggio vengono rilevate informazioni presentate in strutture specifiche, verranno trattate come informazioni potenzialmente riservate, garantendo quindi il controllo sui dati sensibili, ad esempio sui database degli utenti, contenuti in array complessi.

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, è possibile ripristinare i file originali se necessario e utilizzare le informazioni dettagliate di backup relative ai file modificati per scopi di analisi.
- **Integrazione con Active Directory®:** consente l'autenticazione degli utenti di Active Directory.

REQUISITI DI SISTEMA

Server SharePoint

- Microsoft SharePoint 2010;
- Microsoft SharePoint 2013.

Sistema operativo (per installare la soluzione)

Per SharePoint Server 2010:

- Windows Server 2008 x64/2008 R2/2012 R2.

Per SharePoint Server 2013:

- Windows Server 2008 R2 x64 SP1/2012 x64/ 2012 R2

L'elenco completo dei requisiti di sistema è disponibile sul sito www.kaspersky.it

Modalità di acquisto

Kaspersky Security for Collaboration può essere acquistato come parte di Kaspersky Total Security for Business o come soluzione mirata standalone.

Nota: quando si acquista questo prodotto, l'opzione per impedire la perdita di informazioni riservate è venduta separatamente.

Kaspersky Security for Collaboration/Version 0.3/Jan 15/Global

KASPERSKY lab