

► KASPERSKY SECURITY FOR COLLABORATION

Datenschutz und Kontrolle für Collaboration-Plattformen, einschließlich SharePoint-Farms

Die von Ihnen eingesetzte Plattform zur Weitergabe von Dateien und Informationen stellt gleichzeitig ein ideales System zur schnellen Übermittlung gefährlicher Malware und anderer IT-Bedrohungen dar.

Im Hinblick auf eine sichere und reibungslose Umgebung für die Zusammenarbeit hat Kaspersky Lab eine Lösung entwickelt, die einfach zu verwalten ist und einen erstklassigen Echtzeitschutz vor Malware-Angriffen und dem Verlust vertraulicher Daten bietet.

- Vielfach ausgezeichnete Anti-Malware-Engine
- Suche und Schutz vertraulicher Daten
- Datenzugriffskontrolle
- Cloud-basierter Echtzeitschutz – Kaspersky Security Network
- Datei- und Inhaltsfilter
- Phishing-Schutz
- Backup und Speicher
- Zentrale, flexible Verwaltung
- Intuitive Verwaltungskonsole

WICHTIGSTE VORTEILE

UMFASSENDE SCHUTZ FÜR IHRE SHAREPOINT-PLATTFORM

Wenn Sie Microsoft SharePoint Server ausführen, wissen Sie, dass alle Inhalte in einer SQL-Datenbank gespeichert werden und herkömmliche Endpoint-Lösungen daher nicht geeignet sind. Kaspersky Security for Collaboration wendet in der gesamten SharePoint-Farm und auf alle Benutzer einen vielfach ausgezeichneten, fortschrittlichen Malware-Schutz an. Das Cloud-basierte Kaspersky Security Network bietet leistungsstarken Schutz vor bekannten, unbekanntem und erweiterten Bedrohungen, während die Anti-Phishing-Technologie vor Web-basierten Angriffen auf Unternehmensdaten schützt.

VERHINDERN DES VERLUSTS VERTRAULICHER DATEN

Um die Verbreitung vertraulicher Daten zu kontrollieren und diese Daten zu schützen, müssen sie zunächst identifiziert werden. Anhand von vorinstallierten oder angepassten Wörterbüchern und Datenkategorien überprüft Kaspersky Security for Collaboration jedes auf dem SharePoint-Server abgelegte Dokumente auf vertrauliche Informationen, Wort für Wort und Satz für Satz. Schutz und Kontrolle erstrecken sich insbesondere auf persönliche und Bankkartendaten, während Struktur-basierte Suchen vertrauliche Dokumente wie Kundendatenbanken aufspüren.

DURCHSETZEN VON KOMMUNIKATIONSRICHTLINIEN

Inhalts- und Filterfunktionen unterstützen Sie bei der Durchsetzung Ihrer Richtlinien und Standards zur Kommunikation, indem unerwünschte Inhalte identifiziert und blockiert und unnötiges Speichern unerwünschter Dateien und Dateiformate verhindert werden.

EINFACHES MANAGEMENT

Die Sicherheit der gesamten Serverfarm kann zentral von einem einzigen, intuitiven Dashboard aus verwaltet werden. Die Administration funktioniert schnell und unkompliziert und erfordert keine gesonderte Schulung.

VIRENSCHUTZ

- **Scans beim Zugriff:** Die Dateien werden beim Hoch- oder Herunterladen in Echtzeit gescannt.
- **Hintergrund-Scan:** Die auf dem Server gespeicherten Dateien werden regelmäßig anhand der neuesten Malware-Signaturen überprüft.
- **Integration mit Kaspersky Security Network:** Bereitstellen von Cloud-basiertem Echtzeitschutz selbst vor Zero-Day-Bedrohungen.

UNTERSTÜTZUNG DER KOMMUNIKATIONS- RICHTLINIEN IHRES UNTERNEHMENS

- **Datei-Filter:** Unterstützung bei der Durchsetzung von Richtlinien für die Ablage von Dokumenten sowie beim Reduzieren des Speicherbedarfs. Durch Analyse der eigentlichen Dateiformate unabhängig vom Erweiterungsnamen sorgt das Programm dafür, dass Benutzer nicht unter Umgehung der Sicherheitsrichtlinie einen verbotenen Dateityp verwenden können.
- **Schutz für Wikis/Blogs:** Schützt alle SharePoint-Quellen, einschließlich Wikis und Blogs.
- **Inhaltsfilter:** Verhindert unabhängig vom Dateityp das Speichern von Dateien, die unangemessene Inhalte enthalten. Der Inhalt aller Dateien wird anhand von Schlüsselwörtern analysiert. Kunden können zur Inhaltsfilterung auch ihre eigenen, benutzerdefinierten Wörterbücher erstellen.

VERHINDERN DES VERLUSTS VERTRAULICHER DATEN

- **Dokument-Scans für vertrauliche Daten:** Kaspersky Security for Collaboration scannt alle auf die SharePoint-Server heruntergeladenen Dokumente auf vertrauliche Daten.

In der Lösung sind Module integriert, die spezielle Datentypen identifizieren können. Dabei wird die Einhaltung der relevanten rechtlichen Standards gewährleistet, beispielsweise für persönliche Daten (definiert durch rechtliche Auflagen wie HIPAA oder EU-Richtlinie 95/46/EC) oder PCI DSS-Standarddaten (Datensicherungsstandard für Kreditkartentransaktionen).

Hinweise zum Kauf

Kaspersky Security for Collaboration kann als Teil von Kaspersky Total Security for Business oder als eigenständige Targeted Solution erworben werden.

Hinweis: Beim Kauf dieses Produkts muss die Option zum Verhindern des Verlusts vertraulicher Daten separat erworben werden.

Die Daten werden anhand integrierter und regelmäßig aktualisierter Themenwörterbücher gescannt, die Kategorien wie „Finanzen“, „Verwaltungsdokumente“ und „Erniedrigende und beleidigende Sprache“ umfassen, sowie anhand benutzerdefinierter Wörterbücher.

- **Suche nach strukturierten Daten:** Wenn bestimmte Informationsstrukturen in einer Nachricht gefunden werden, wird die Nachricht potentiell als vertraulich eingestuft. So erhalten Sie Kontrolle über vertrauliche Daten wie Kundendatenbanken, die in komplexen Arrays vorliegen.

FLEXIBLE VERWALTUNG

- **Einfaches Management:** Die gesamte Serverfarm kann zentral von einer einzigen Konsole aus verwaltet werden. Auf der intuitiven Oberfläche finden Sie alle häufig verwendeten Verwaltungsszenarien.
- **Ein einziges Dashboard:** Das übersichtliche Dashboard bietet eine Echtzeitanzeige des aktuellen Produktstatus, der Datenbankversion und des Lizenzstatus für alle geschützten Server.
- **Backup veränderter Dateien:** Bei einem Vorfall können die Ursprungsdateien auf Wunsch wiederhergestellt werden. Darüber hinaus sind für mögliche Untersuchungen detaillierte Sicherungsinformationen zu geänderten Dateien verfügbar.
- **Integration mit Active Directory®:** Ermöglicht die Authentifizierung von Active Directory-Benutzern.

SYSTEMANFORDERUNGEN

SharePoint-Server

- Microsoft SharePoint 2010
- Microsoft SharePoint 2013

Betriebssystem (zur Installation der Lösung)

Für SharePoint Server 2010:

- Windows Server 2008 x64/2008 R2/2012 R2

Für SharePoint Server 2013:

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

Eine umfassende Liste der Systemanforderungen ist verfügbar unter kaspersky.de