Kaspersky®
Security Center

Verwaltung und Schutz für alle Geräte – physisch, virtuell und mobil – von einer einzigen leistungsstarken und einheitlichen Konsole

Das Kaspersky Security Center bietet eine unkomplizierte Sicherheits- und IT-Systemverwaltung. Die vollständig skalierbare Konsole unterstützt Unternehmen, deren Sicherheitsanforderungen sich ständig verändern. Eine einzige Verwaltungskonsole vereinfacht das umfassende System- und Sicherheitsmanagement und ermöglicht die einfache Aufteilung von Administratoraufgaben.

Führend und anerkannt

Allein 2017 haben die Sicherheitsprodukte von Kaspersky Lab an 86 unabhängigen Tests und Bewertungen teilgenommen – mit 72 Siegen und 78 Top-3-Platzierungen. Unsere Endpoint-Lösung wird durch führende globale Analysten erkannt.

Kaspersky HuMachine™-Konzept

Funktionen für maschinelles Lernen, globale Big Data Threat Intelligence und zwei Jahrzehnte menschlicher Expertise sorgen gemeinsam für optimalen Schutz bei optimaler Effizienz.

Kaspersky Security Network

Das Kaspersky Security Network (KSN) ist eine komplexe verteilte Infrastruktur, die schneller als jemals zuvor auf neue Bedrohungen reagiert, die Leistung von Schutzkomponenten verbessert und das Risiko von Fehlalarmen (False-Positives) minimiert.

Eine Verwaltungskonsole

Da die Mehrheit unserer Sicherheitstechnologien über eine einzige Verwaltungskonsole, das Kaspersky Security Center, verwaltet werden kann, ist es schneller und einfacher für Ihr Sicherheitsteam, die Sicherheitsrichtlinien auf alle Endpoints anzuwenden. Die zentralisierte Verwaltung wird durch rollenbasierten Zugriff und integrierte Dashboards ergänzt, sodass jeder Administrator nur Zugriff auf die Werkzeuge und Daten hat, die für seine Aufgaben relevant sind.

Einfache Skalierbarkeit

Ermöglicht die Skalierung ohne Änderung der Ersteinrichtung – bis zu 100 000 physische, virtuelle und Cloud-basierte Endpoints können nun über eine einzige Serverinstallation des Kaspersky Security Center mit optimierten Backup-Funktionen verwaltet werden.

Erweiterbare Architektur

Die erweiterbare Architektur des Kaspersky Security Center beinhaltet Plug-ins für die Verwaltung von Sicherheitsprodukten für jede Plattform. Wenn ein neues Sicherheitsprogramm gekauft oder freigegeben wird, kann die entsprechende Erweiterung auf das Kaspersky Security Center installiert werden, ohne dass eine Neuinstallation oder ein Patching der Konsole notwendig ist.

Vorteile

Eine zentrale Sicherheitsverwaltung erhöht die Transparenz, optimiert die Kosten und steigert die Verwaltungseffizienz. Das Kaspersky Security Center umfasst Technologien und Tools, die zusammen eine integrierte und bewährte Sicherheitsplattform ergeben.

Beschleunigung von Routineaufgaben

Die Bereitstellung, Konfiguration und Verwaltung von Endpoint-Sicherheit sorgt für stets aktuelle Sicherheit für jeden Endpoint und jedes Gerät in Ihrem Netzwerk.

Mehr Schutz für alle Ihre Endpoints und Server

Windows, Linux, Mac, Android, iOS, Server und virtuelle Infrastrukturen werden alle über dieselbe Konsole geschützt und verwaltet.

Minimiert das Angriffsrisiko

Mit der zentralisierten Web-, Programm- und Gerätekontrolle können Sie die Nutzung ungeeigneter oder unsicherer Programme, Geräte und Websites einschränken.

Absicherung des mobilen Zugriffs

Unterstützt die zentrale Verwaltung des Schutzes für führende Plattformen von mobilen Geräten und erhöht die Sichtbarkeit und Kontrolle ohne zusätzliche Ressourcen oder Technologien.

Optimiert das Patching

Indem es über die bloße Remote-Bereitstellung von Drittanbietersoftware hinausgeht, hält das automatisierte Vulnerability Assessment und Patch Management mittels kontinuierlicher Suche nach ausgenutzten Schwachstellen potentiell verwundbare Software auf dem neuesten Stand, sodass Ihre IT-Administratoren mehr Zeit für andere Aufgaben haben.

Erleichtert die Bestands- und Programmbereitstellung

Erweiterte Client-Verwaltungstools automatisieren und zentralisieren Verwaltungsaufgaben, darunter Hardware- und Software-Bestandsaufnahme, Image-Erstellung sowie Softwareverteilung und Troubleshooting per Fernzugriff.

Mehr Möglichkeiten für Managed Services-Anbieter

Das Kaspersky Security Center unterstützt die B2B-Lizenzierung und Mehrmandantenfähigkeit auf Abonnementbasis. Unbegrenzte virtuelle Verwaltungsserver und das Remote-Management über die Webkonsole ermöglichen die flexible Verwaltung der IT-Infrastrukturen mehrerer Kunden.

Den Überblick behalten

Das Kaspersky Security Center überträgt Befehle, Nachrichten und Informationen zwischen dem Endpoint Detection & Response (EDR)-Server, der jeden Knoten in Echtzeit und den Endpoint-Agent auf Anzeichen eines Eindringens prüft und somit zur Erhöhung der Sichtbarkeit und Sicherheit beiträgt.

Trägt zur Einhaltung der DSGVO-Richtlinien bei

Die Konsole wird zur Verwaltung der Verschlüsselung eingesetzt – die in der Verordnung als zusätzliche Sicherheitsstufe angesichts der wachsenden Bedrohung von Datenverlust durch Gerätediebstahl bezeichnet wird – und erhöht die Sichtbarkeit über die ganze Infrastruktur hinweg.

Sichert die Systemintegrität

Mit dem Kaspersky Security Center können Sie alle Änderungen an wichtigen Komponenten Ihrer Anlagen, wie Webserver und Geldautomaten, überwachen und umgehend auf Verstöße gegen die Integrität dieser Systeme reagieren.

Direkte Integration von bewährtem Schutz in Cloud-Umgebungen

Die native Integration zwischen der Verwaltungskonsole und Amazon Web Services (AWS) Cloud-Umgebung bietet vollständige Transparenz und Kontrolle über Linux- und Windows Server-basierte Sicherheitsprogramme, die in der Cloud bereitgestellt werden.

Vereinfacht das Deployment

Verwaltungsassistenten für Enterprise Mobility Management (EMM) ermöglichen die Bereitstellung von Schutz mit OTA-Bereitstellungstechnologie, Drittanbieter-EMM-Systemen (z. B. VMWare AirWatch) und Anmeldungskonsolen (Samsung, KNOX).

Hauptfunktionen

Sofortige Installation, direkt einsetzbare Konfiguration

Folgen Sie bewährten Vorgehensweisen anhand vorkonfigurierter Richtlinien von Kaspersky Lab - oder erstellen Sie Ihre eigenen. Dies ist besonders hilfreich für kleinere Organisationen mit begrenzt verfügbaren IT-Administrationsressourcen für zusätzliche Konfigurationsaufgaben.

Über die Verwaltung des Schutzes vor Bedrohungen hinaus

Verwalten Sie physische, virtuelle und Cloud-basierte Endpoints zusammen mit nur einer Konsole, erhöhen Sie die Effizienz reduzieren Sie Ihre Betriebskosten und mehr:

- Verwalten und richten Sie Sicherheitsrichtlinien für Windows-, Linux- und Mac-Geräte ein.
- Verwalten Sie Cloud-basierten Schutz durch das Kaspersky Security Network (KSN).
- Verwalten Sie Programm-, Geräte- und Webkontrolle für einen besseren Schutz zentral.
- Hostbasierte Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) verwalten.
- Konfigurieren und verwalten Sie Firewall-Einstellungen unter Linux- und Windows-Betriebssystemen.
- Konfigurieren Sie Kaspersky-Verschlüsselung, Microsoft BitLocker und Filevault-Verschlüsselung zum Schutz von Daten, wenn Geräte verloren gehen oder gestohlen werden. Stimmen Sie Verschlüsselungsrichtlinien
- sowie Programm- und Gerätekontrolle aufeinander ab.

Praktische mobile Sicherheitsverwaltung

Verwalten Sie mobile Geräte, einschließlich Android, iOS, genauso wie Sie andere Endpoints verwalten. Administratoren haben die folgenden Optionen:

- Sie können kontrollieren, wie Mitarbeiter auf ihren mobilen Geräten auf das Internet zugreifen, indem Sie schädliche Webseiten blockieren und Benutzer vor Phishing-Webseiten schützen, die Informationen und personenbezogene Daten stehlen können.
- Sie können den Zugriff auf Unternehmensprogramme und -daten über gerootete Geräte verhindern.
- Sie können gestohlene mobile Geräte mithilfe von Anti-Theft-Funktionen, die von einem Administrator oder über das Selfservice-Portal vom Benutzer aktiviert werden können, sperren, löschen und orten.
- Sie können einheitliche Sicherheitsrichtlinien für mobile Geräte bereitstellen, indem sie den Zugriff auf MDM-Funktionen für verschiedene Plattformen über eine einzige Benutzeroberfläche ermöglichen.

Unterstützung für virtuelle Umgebungen

Vermeiden Sie leistungsbeeinträchtigende „Storms" durch Schutz vor Bedrohungen, indem Sie virtuelle Maschinen erkennen und das Load Balancing während intensiver Vorgänge vereinfachen – all das über eine einzige Verwaltungskonsole. Egal, ob Sie agentenlosen Schutz oder Light Agent für den Schutz Ihrer virtuellen Umgebungen nutzen – Sie können diese Sicherheitsprogramme vollständig über das Kaspersky Security Center verwalten.

Unterstützung von Cloud-Umgebungen

Genießen Sie vollständige Transparenz und Kontrolle über Kaspersky Endpoint Security for Linux- und Kaspersky Security for Windows Server-Instanzen, die in der Cloud bereitgestellt werden, Dies wird durch eine enge Integration der Verwaltungskonsole mit der AWS-Cloud-Umgebung ermöglicht.

Integration mit zielgerichteten Lösungen

Nutzen Sie die Integration mit verschiedenen Targeted Security-Lösungen, mit denen Sie die Sicherheit von Embedded System, Gateways, E-Mail-Systemen und Kollaborationsplattformen überwachen können. Sie können den Konnektivitäts- und den Systemstatus einsehen und haben Zugriff auf konsolidierte Statistiken für alle Server, zusammen mit den anderen Sicherheitskomponenten Ihrer Organisation- alles über eine einzige Konsole.

Erweitertes Reporting

Sie verfügen über eine breite Palette integrierter und anpassbarer Berichte, können dynamische Filter anwenden und Berichte nach beliebigen Feldern sortieren.

Web-Verwaltungskonsole

Sie können Remote-Management für Endpoints und mobile Geräte über die Webkonsole aktivieren.

Rollenbasiertes Modell

Weisen Sie über die rollenbasierte Zugriffssteuerung verschiedene Endpoint-Gruppen oder Verwaltungsaufgaben unterschiedlichen Administratoren zu, und passen Sie die Verwaltungskonsole so an, sodass jeder Administrator nur auf die Tools und Daten zugreifen kann, die für seine Aufgaben relevant sind.

Umfassendes Vulnerability und Patch Management

Identifizieren Sie mögliche Zugangspunkte für Schadprogramme zu Ihrem Netzwerk, indem Sie Schwachstellen in Ihren Programmen oder Betriebssystemen erkennen und diese beseitigen, bevor die Malware Schaden anrichten kann. Ermöglicht wird dies über die im Kaspersky Security Center enthaltenen Vulnerability and Patch Management-Funktionen. Hinzu kommt:

- Priorisieren Sie Schwachstellen und die automatische Verteilung von Patches und Updates für Software von Microsoft und anderen Anbietern.
- Beheben Sie Update-Probleme per Fernzugriff für jede physische, virtuelle oder Amazon EC2-Maschine.
- Reduzieren Sie Datenverkehr bei Updates zu Zweigstellen, indem Sie einen Remote-Endpoint als Update-Agent verwenden.
- Überwachen Sie den Patch-Installationsstatus durch Berichte über die erfolgreiche Patch-Anwendung.

Optimierte IT-Ressourcenverwaltung

Auf Basis einer breiten Palette von Funktionen zur IT-Systemverwaltung, die Verwaltungsaufgaben für IT-Ressourcen in heterogenen Netzwerken rationalisieren, haben Sie folgende Möglichkeiten:

- Automatische Ermittlung von Hardware und Software im Netzwerk für den vollständigen Überblick über alle Ressourcen, die verwaltet und geschützt werden müssen.
- Minimierung des erforderlichen Zeit- und Ressourcenaufwands für die Einrichtung neuer Geräte oder die Bereitstellung neuer Programme dank automatischer Softwarebereitstellung.
- Bereitstellung von Software per Befehl oder Planen der Bereitstellung außerhalb der Geschäftszeiten. Dabei können Sie zusätzliche Parameter angeben, um die Installation des Softwarepakets anzupassen.
- Nutzung von Remote-Troubleshooting, einschließlich eines Autorisierungsmechanismus und Remote-Sitzungsprotokollen.
- Kontrolle über das Erstellen, Speichern und Klonen von gesicherten System-Images, um eine optimale und schnellere Bereitstellung von Betriebssystemen zu ermöglichen. UEFI wird unterstützt.

Integration von Best Practices für Audits

Im Kaspersky Security Center werden alle Änderungen an Einstellungen, Richtlinien, Aufgaben und verwalteten Programmen für einen Versionsvergleich und gegebenenfalls ein mögliches Rollback protokolliert und gespeichert. Die Audit-Funktionen ermöglichen Administratoren den Vergleich zweier Richtlinien. Anschließend wird ein Bericht darüber erstellt, welche Einstellungen übereinstimmen und welche sich unterscheiden.

Systemanforderungen

Die vollständigen aktuellen Anforderungen finden Sie in der Wissensdatenbank.

Allgemeine Anforderungen

- CPU mit einer Betriebsfrequenz von mindestens 1,4 GHz
- 4 GB Arbeitsspeicher (RAM)
- 10 GB freier Festplattenspeicher

Betriebssysteme

- Microsoft Windows 10, 8.1, 8, 7
- Microsoft Windows Server 2016, 2012 R2, 2012
- Microsoft Small Business Server 2011
- Microsoft Windows Server 2008 R2, 2008 SP1, 2008

Systemanforderungen für ein Abonnement

Wenden Sie sich an Ihren Kaspersky-Partner vor Ort um die Verfügbarkeit von Monatsabonnements für Ihr Land zu prüfen. Die entsprechenden Systemanforderungen finden Sie hier.

Hinweise zum Kauf

Das Kaspersky Security Center ist in folgenden Produkten enthalten:

- Kaspersky Total Security for Business
- Kaspersky Endpoint Security for Business Advanced
- Kaspersky Endpoint Security for Business Select
- Kaspersky Vulnerability & Patch Management
- Kaspersky Hybrid Cloud Security
- Kaspersky Security for Storage
- Kaspersky Security for Mobile
- Kaspersky Security for Mail Server
- Kaspersky Security for File Server

Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners

#truecybersecurity
#HuMachine

www.kaspersky.de