KASPERSKY UNTERNEHMENS-PRODUKTE 2013

SEE IT. CONTROL IT. PROTECT IT.

KASPERSKY lab

INHALTSVERZEICHNIS

Über Kaspersky Lab	5
Die einzig wirklich integrierte Sicherheitsplattform der Branche	6
Die richtige Lösung für Sie	7
Kaspersky Security for Business	8
Kaspersky Endpoint Security for Business	9
Kaspersky Endpoint Security for Business Core	11
Kaspersky Endpoint Security for Business Select	13
Kaspersky Endpoint Security for Business Advanced	15
Kaspersky Total Security for Business	17
Kaspersky Security for Mobile	19
Kaspersky Systems Management	21
Kaspersky Security für File-Server	23
Kaspersky Security für Mail-Server	24
Kaspersky Security für Internet-Gateways	25
Kaspersky Security für Collaboration	26
Kaspersky Security for Virtualization	27
Kaspersky Anti-Virus für Storage-Lösungen	29
Notizen	30

ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltgrößte unabhängige Hersteller von Sicherheitssoftware. Wir bieten optimale IT-Sicherheit für Ihr Unternehmen durch eine Kombination aus leistungsstarkem Malware-Schutz, flexiblen Steuerungstools, Verschlüsselungstechnologie und Systemverwaltungstools. Kaspersky Lab schützt Ihr System von den Endpoints über die Server bis hin zu den Gateways, und dank unseres einzigartigen Designs können Sie all Ihre physischen, virtuellen und mobilen Geräte von einer einzigen zentralen Verwaltungskonsole aus schützen und kontrollieren, egal wie umfangreich die Infrastruktur auch sein mag. Technologien von Kaspersky Lab kommen darüber hinaus weltweit in Produkten und Services von führenden IT-Herstellern und -Anbietern zum Einsatz.

Weitere Informationen erhalten Sie unter: www.kaspersky.de.

Aktuelle Informationen zum Schutz gegen Viren, Spyware und Spam und weiteren Aspekten und Trends der IT-Sicherheit erhalten Sie hier: http://www.securelist.com/de.

DIE EINZIG WIRKLICH INTEGRIERTE SICHERHEITSPLATTFORM DER BRANCHE

EINE KONSOLE

Dank Kaspersky-Produkten können Administratoren über einen einzigen Bildschirm die gesamte Sicherheitslandschaft einsehen und verwalten: virtuelle, physische und mobile Geräte.

EINE PLATTFORM

Hier bei Kaspersky Lab haben wir eine eigene Konsole, eigene Sicherheitsmodule und Tools entwickelt, anstatt die Komponenten von anderen Unternehmen zuzukaufen. Dies bedeutet, dass die gleichen Programmierer mit der gleichen Codebase Technologien entwickeln, die miteinander kommunizieren und arbeiten. Das Resultat sind Stabilität, integrierte Richtlinien, sinnvolle Berichterstellung und intuitiv zugängliche Tools.

EINE INVESTITION

Alle Kaspersky-Produkte sind aus einer Herstellerhand. Auf diese Weise können Sie mit einer Investition Ihre Sicherheitsrisiken mit Ihren Unternehmenszielen in Einklang bringen.

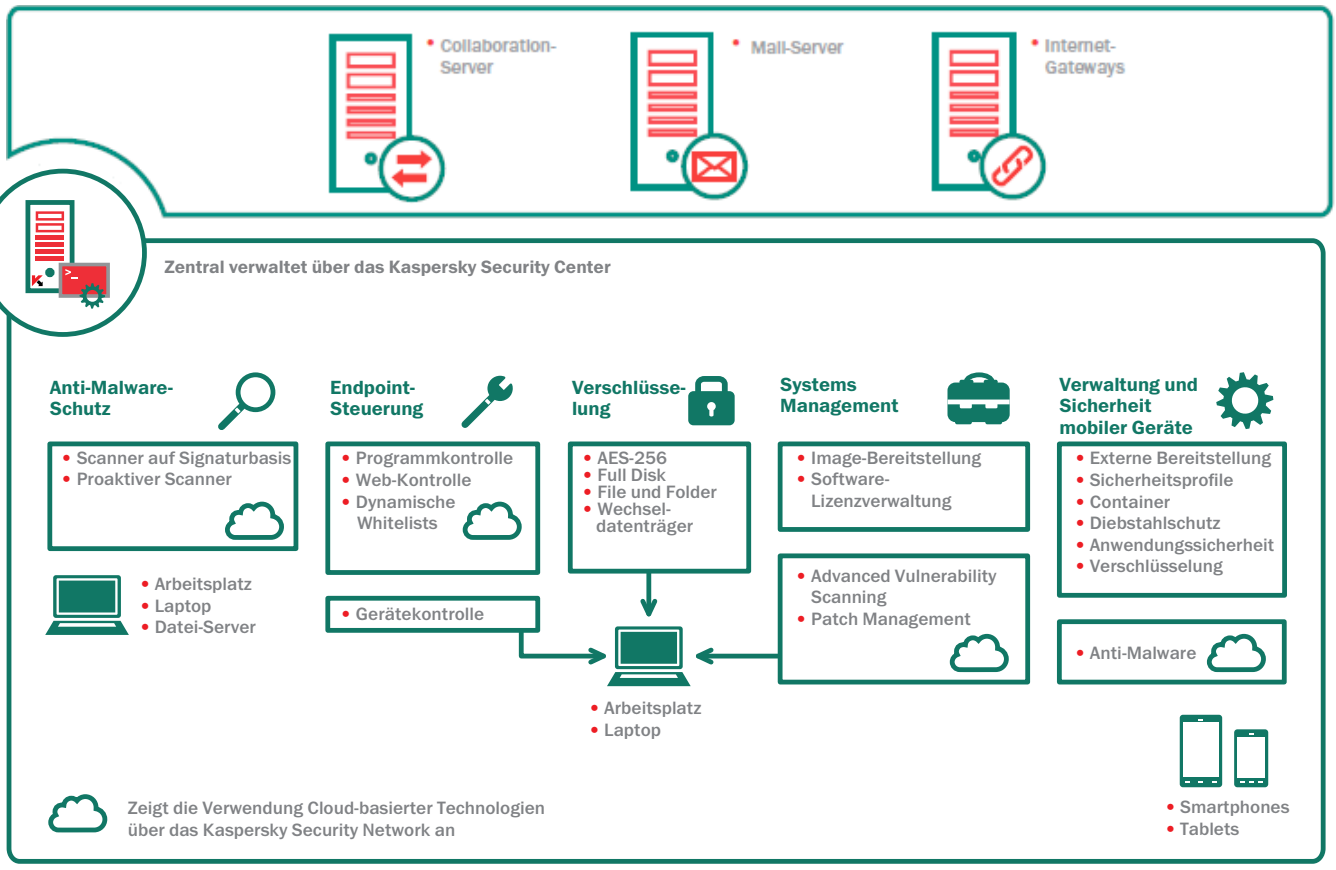
HINWEIS: Die aktuell unterstützten Betriebssysteme für die einzelnen Produkte und Lösungen finden Sie in den jeweiligen Release-Notes.

DIE RICHTIGE LÖSUNG FÜR SIE

Kaspersky Security for Business bietet die richtige Lösung für Ihr Unternehmen – egal, ob es Ihnen darum geht, Ihre Endpoints (von Workstations bis hin zu Smartphones und virtuellen Maschinen) zu schützen und zu kontrollieren, Ihre Server und Gateways abzusichern oder Ihre gesamte Sicherheitsinfrastruktur remote zu verwalten.

Kaspersky Lab kann mit einer umfangreichen Palette von Technologien aufwarten, angefangen bei Verschlüsselung und Mobile Device Management über Patch Management bis hin zur Inventarisierung von Lizenzen. Alle Technologien greifen nahtlos ineinander und werden vom cloudbasierten Kaspersky Security Network unterstützt, um unseren Kunden den erstklassigen Schutz zu bieten, den sie benötigen, um den immer ausgeklügelteren Bedrohungen aus dem Internet zu begegnen.

Fazit: Wir haben die erste Sicherheitsplattform in der Branche bereitgestellt, die von Grund auf neu entwickelt wurde, damit IT-Experten ihre Infrastruktur erkennen, kontrollieren und schützen können.

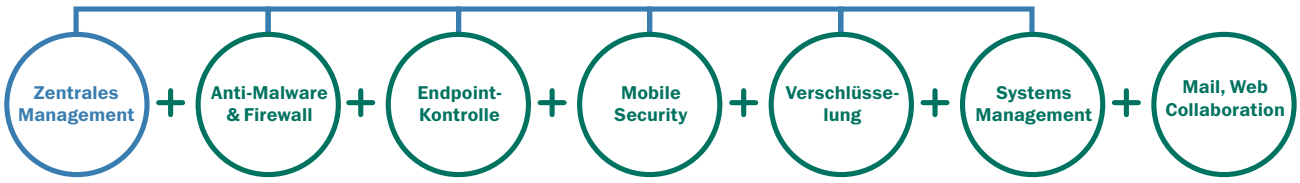


KASPERSKY SECURITY FOR BUSINESS

Unsere Technologien, und wie Sie sie einsetzen können

		Core	Select	Advanced	Total	Verwaltung über Security Center	Als Targeted Solution verfügbar
Hauptfunktionen	Anti-Malware	•	•	•	•	•	
	Firewall	•	•	•	•	•	
	Programmkontrolle		•	•	•	•	
	Gerätekontrolle		•	•	•	•	
	Web-Kontrolle		•	•	•	•	
	Mobile Device Management (MDM)		•	•	•	•	
	Verschlüsselungstechnologie			•	•	•	
Systems Management	Image Management			•	•	•	•
	Lizenzmanagement			•	•	•	•
	Advanced Vulnerability Scanning			•	•	•	•
	Patch Management			•	•	•	•
Targeted Solutions	Kaspersky Security for Mobile		•	•	•	•	•
	Kaspersky Security für File-Server		•	•	•	•	•
	Kaspersky Security für Mail-Server				•		•
	Kaspersky Security für Internet-Gateways				•		•
	Kaspersky Security für Collaboration				•		•
	Kaspersky Security for Virtualization					•	•
	Kaspersky Anti-Virus für Storage-Lösungen					•	•

KASPERSKY ENDPOINT SECURITY FOR BUSINESS



STUFE „CORE“

Ausgehend von der ausgezeichneten und leistungsstarken Anti-Mail-Technologie für Workstations von Kaspersky Lab und einer schützenden Firewall kommt bei dieser Stufe Kaspersky Security Center hinzu, unsere intuitive Verwaltungskonsole. Für Kunden, die nur Anti-Malware benötigen, ist dies die beste Lösung.

STUFE „SELECT“

Aufbauend auf „Core“ kommt bei dieser Stufe **File-Server-Sicherheit, Anwendungs-Whitelisting und -Kontrolle, Gerätesteuerung und Web-Kontrolle** zum Schutzangebot hinzu. Ebenfalls eingeschlossen ist eine **mobile Schutzlösung**, die aus einem **Endpoint-Sicherheitsagenten** und **Mobile Device Management (MDM)** besteht. Wenn Sie zusätzlich Ihre mobilen Mitarbeiter schützen und IT-Richtlinien durchsetzen müssen, ist SELECT ggf. die richtige Version für Sie.

STUFE „ADVANCED“

Auf der Stufe ADVANCED wird von Kaspersky Lab der **Datenschutz** in Form einer **Verschlüsselung** von Dateien oder des gesamten Datenträgers hinzugefügt. Bei **Kaspersky Systems Management**, einem weiteren neuen Angebot, wird Sicherheit mit IT-Effizienz kombiniert. In diesem breiten Funktionsangebot sind wichtige Tools enthalten, die dem Administrator Folgendes ermöglichen:

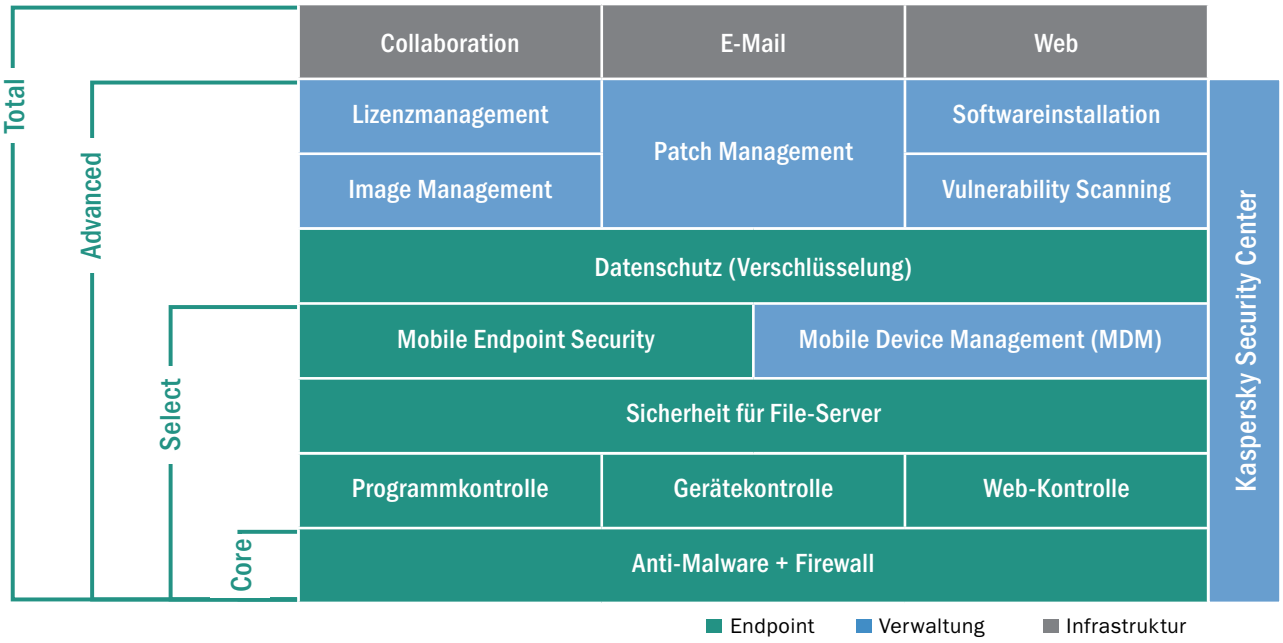
- Mit dem Image Management-Modul Images erstellen und Systeme bereitstellen.
- Die Behandlung von Schwachstellen in der Software mit einer leistungsstarken Kombination aus erweiterter Anfälligkeitsüberprüfung und intelligenter Patch Management priorisieren.
- Die Lizenzverwendung und die Einhaltung des Software-Lizenzmanagements verfolgen.
- Updates und neue Software für Benutzer von der zentralen Konsole aus der Ferne bereitstellen und installieren.

KASPERSKY TOTAL SECURITY FOR BUSINESS

Bei unserem Flaggschiffprodukt, Kaspersky Total Security for Business, werden alle vorigen Stufen zu einer Komplettversion kombiniert. Zusätzlich wird Ihre Sicherheitsposition mit dem Web-, E-Mail- und Collaboration-Serverschutz verbessert. Dies stellt die perfekte Lösung für Unternehmen mit breiten Sicherheitsanforderungen dar, die für jedes Netzwerk den besten Schutz verlangen.

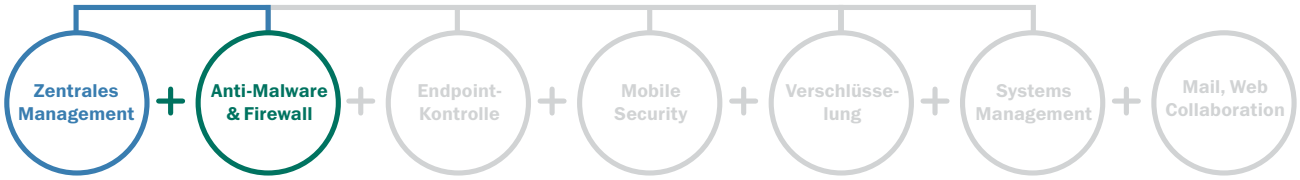
Administratoren können mit Kaspersky Endpoint Security for Business ihre IT-Umgebung beobachten, steuern und schützen. In den abgestuften Programmversionen sind die Tools und Technologien gezielt auf Ihre sich entwickelnden Sicherheits- und IT-Anforderungen ausgerichtet. Kaspersky Endpoint Security for Business kann Ihre Arbeit leichter machen.

ÜBERSICHT



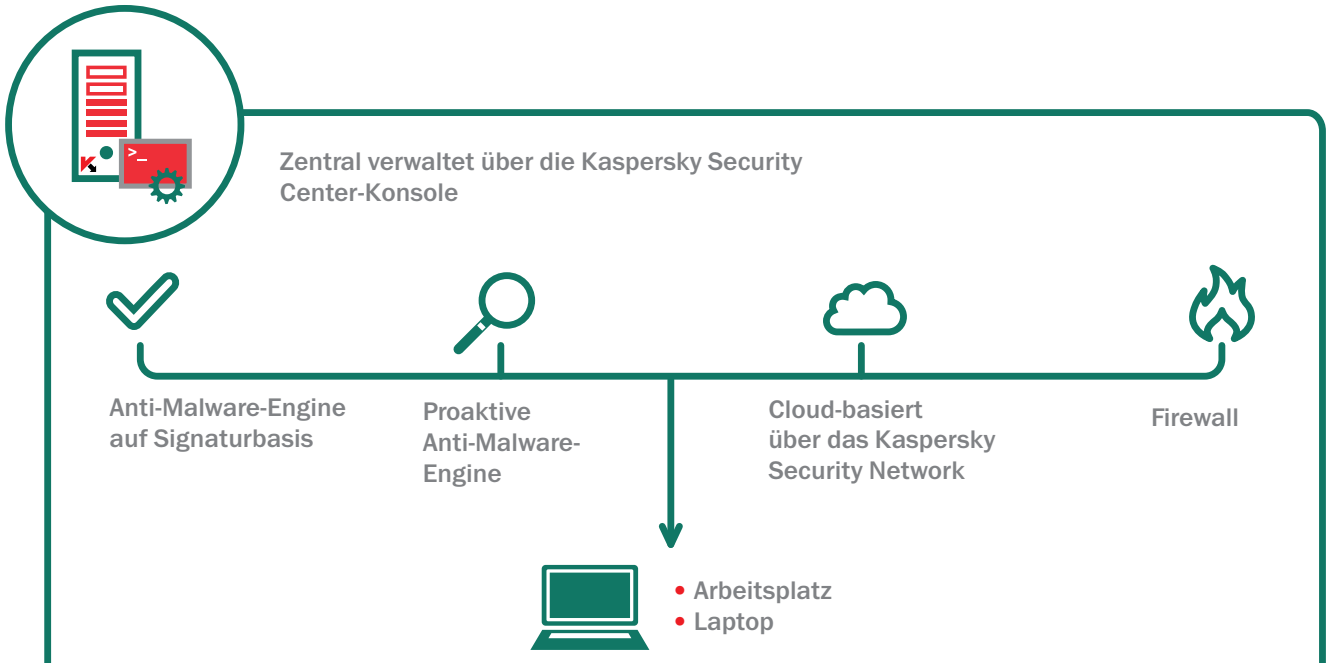
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Ausgezeichnete Anti-Malware mit zentralisierter Bereitstellung, Verwaltung und Berichterstellung.

Ein Sicherheitsmodell auf mehreren Ebenen mit branchenführender Anti-Malware. Kaspersky Lab gilt seit langem als Marktführer in der Erkennung und Beseitigung von schädlicher Software. Die Version „Core“ von Kaspersky Endpoint Security for Business wird über das Kaspersky Security Center zentral verwaltet und durch das Cloudbasierte Kaspersky Security Network unterstützt.



Version „Core“ von Kaspersky Endpoint Security for Business Kaspersky – Leistungsstarke Anti-Malware-Engine mit cloudbasiertem Schutz.

HAUPTFUNKTIONEN:

LEISTUNGSSTARKE ENDPOINT-ANTI-MALWARE
Die Scan-Engines von Kaspersky Lab werden auf mehreren Ebenen im Betriebssystem eingesetzt, um Malware umfassend zu bekämpfen.

CLOUD-BASIERTER SCHUTZ
Mit dem Cloudbasierten Kaspersky Security Network sind Benutzer in Echtzeit vor neuen Bedrohungen geschützt.

ZENTRALISIERTE VERWALTUNG
Administratoren können bestehende Antiviren-Software über eine einzige Konsole entfernen, Kaspersky Lab konfigurieren und bereitstellen und das Reporting ausführen.

FUNKTIONEN VON ENDPOINT-ANTI-MALWARE:

REGELMÄSSIGE UPDATES UND SCHUTZ AUF SIGNATURBASIS
Branchenbewährte herkömmliche signaturbasierte Methode zur Erkennung von Bedrohungen durch Malware.

VERHALTENSANALYSE DURCH AKTIVITÄTSMONITOR
Das Kaspersky Security Network (KSN) reagiert auf vermutete Bedrohungen deutlich schneller als herkömmliche Schutzmethoden. Die Reaktionszeit von KSN auf neue Bedrohungen liegt im Sekunden- oder Minutenbereich!

SYSTEM ZUR ANGRIFFSÜBERWACHUNG AUF HOST-BASIS (HOST-BASED INTRUSION PREVENTION SYSTEM = HIPS) MIT PERSONAL FIREWALL
Vordefinierte Regeln für Hunderte der häufigsten verwendeten Anwendungen verringern den Zeitaufwand für das Konfigurieren der Firewall.

UMFASSENDE PLATTFORMUNTERSTÜTZUNG
Kaspersky Lab bietet Endpoint Security für Windows®, Macintosh® und Linux® und verringert so die Arbeitslast von Administratoren, die verschiedene Netzwerke unterstützen.

WICHTIGE LEISTUNGSMERKMALE VON KASPERSKY SECURITY CENTER:

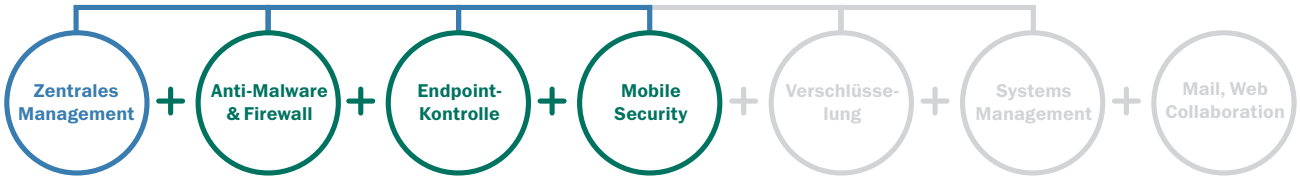
EINE ZENTRALE KONSOLE
Für die Remote-Verwaltung aller Ihrer mit Kaspersky Lab geschützten Endpoints.

INTUITIVE BENUTZEROBERFLÄCHE
Über klare, anschauliche Informationen in einem übersichtlichen Dashboard können Administratoren den Schutzstatus in Echtzeit anzeigen, Richtlinien einrichten, Systeme verwalten und Berichte erhalten.

WEB-OBERFLÄCHE
Überwacht den Schutzstatus aus der Ferne und berichtet von einer zugänglichen Oberfläche aus über die wichtigsten Ereignisse.

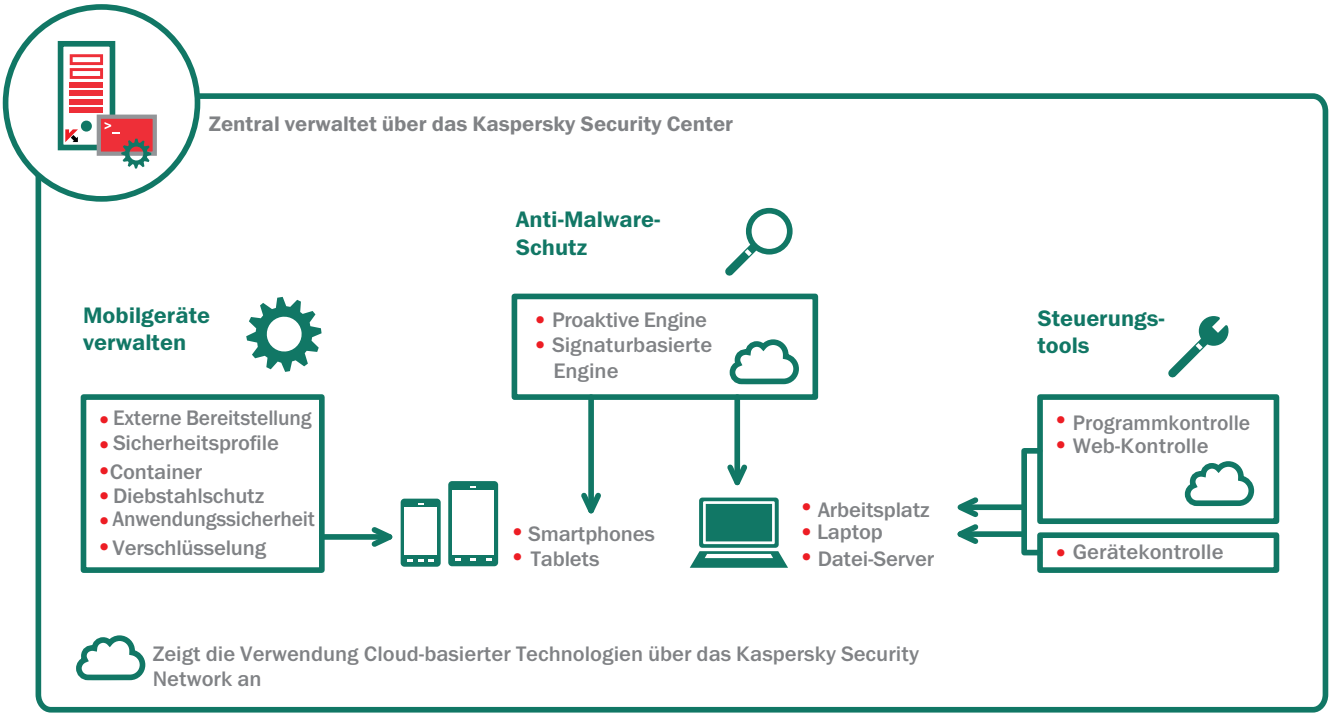
SKALIERBARER SUPPORT
Egal, wie groß Ihre Infrastruktur ist, das Kaspersky Security Center bietet Tools zur Bereitstellung und Verwaltung, flexible Optionen für Richtlinien und ein verlässliches Reporting, um Ihre wachsenden Anforderungen zu erfüllen.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Select



Tools, die mehr Mobilität bei den Mitarbeitern ermöglichen, die Einhaltung von IT-Sicherheitsrichtlinien sicherstellen und Malware blockieren.

Die Schutzstufe „Select“ von Kaspersky Lab umfasst Bereitstellung und Schutz mobiler Geräte über Mobile Device Management (MDM) und mobile Anti-Malware-Funktionalität. Endpoint-Steuerungstools für Web, Geräte und Programme unterstützen Ihr Unternehmen bei der Durchsetzung von IT-Richtlinien zum Schutz der zentralen Elemente der IT-Umgebung.



Kaspersky Endpoint Security for Business – Stufe „Select“. Mit Steuerungstools und mobiler Sicherheit.

HAUPTFUNKTIONEN:

LEISTUNGSSTARKE ENDPOINT-ANTI-MALWARE
Die branchenführende Scan-Engine von Kaspersky Lab entfernt Malware auf mehreren Ebenen des Betriebssystems. Das Kaspersky Security Network (KSN) auf Cloud-Basis schützt Benutzer in Echtzeit vor neuen Bedrohungen.

FLEXIBLE, AUSGEARBEITETE STEUERUNGSTOOLS
Eine kategorisierte Datenbank auf Cloud-Basis mit sicheren und unsicheren Anwendungen und Webseiten unterstützt den Administrator dabei, Richtlinien für Anwendungen und das Surfen im Internet festzulegen und durchzusetzen, während detaillierte Steuermechanismen sicherstellen, dass nur bestimmte Geräte sich mit Rechnern im Netzwerk verbinden können.

EFFEKTIVE MOBILE BEREITSTELLUNG UND SICHERHEIT FÜR SMARTPHONES UND TABLETS
Agentenbasierte mobile Sicherheit ist für Geräte mit den Betriebssystemen Android™, Blackberry®, Symbian und Windows® verfügbar. Richtlinien und Software für mobile Geräte können mit Kaspersky MDM über das Mobilfunknetz (Over-The-Air, OTA) sicher auf diese sowie auf iOS-Geräte übertragen werden.

IN DIESER STUFE KOMMEN HINZU:

ENDPOINT-STEUERUNG:

PROGRAMMKONTROLLE
Gestattet IT-Administratoren das Festlegen von Richtlinien, die Programme (bzw. Programmkategorien) gestatten, blockieren oder regulieren.

GERÄTEKONTROLLE
Dies gestattet es Administratoren, Datenrichtlinien zur Kontrolle von Wechseldatenträgern und sonstigen Peripheriegeräten festzulegen, zeitlich zu planen und durchzusetzen – egal, ob die Verbindung über USB oder sonstige Schnittstellen erfolgt.

WEB-KONTROLLE
Dies bedeutet, dass eine Kontrolle des Surf-Verhaltens von Benutzern auf Endpoint-Basis stattfindet – egal ob im Unternehmensnetzwerk oder beim Roaming gesurft wird.

DYNAMISCHE WHITELISTS
Von Kaspersky Security Network in Echtzeit bereitgestellte Dateireputationen stellen sicher, dass die von Ihnen bestätigten Anwendungen frei von Malware sind und zur Maximierung der Benutzerproduktivität beitragen.

KASPERSKY SECURITY FOR MOBILE:

INNOVATIVE ANTI-MALWARE-TECHNOLOGIEN
Kombination von signaturbasierter, proaktiver und Cloud-basierter Erkennung ermöglicht Echtzeitschutz. Sicherer Browser und Anti-Spam-Schutz bei SMS und MMS verbessern die Sicherheit.

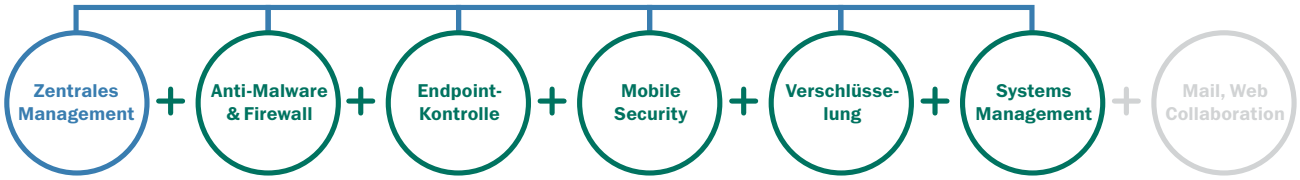
BEREITSTELLUNG MIT OTA-PROVISIONING (OTA = OVER THE AIR)
Möglichkeit, Anwendungen zentral über SMS, E-Mail und PC im Voraus zu konfigurieren und bereitzustellen

EXTERNE TOOLS ZUM DIEBSTAHLSCHUTZ
SIM-Überwachung, Fernsperrung, Löschung und Suche dienen dazu, nicht autorisierten Zugriff auf Unternehmensdaten zu verhindern, wenn ein mobiles Gerät verloren geht oder gestohlen wird.

PROGRAMMKONTROLLE FÜR MOBILE GERÄTE
Überwacht auf einem mobilen Gerät installierte Anwendungen gemäß vordefinierter Gruppenrichtlinien. Schließt eine Gruppe „Mandatory Application“ (zwingende Anwendung) ein.

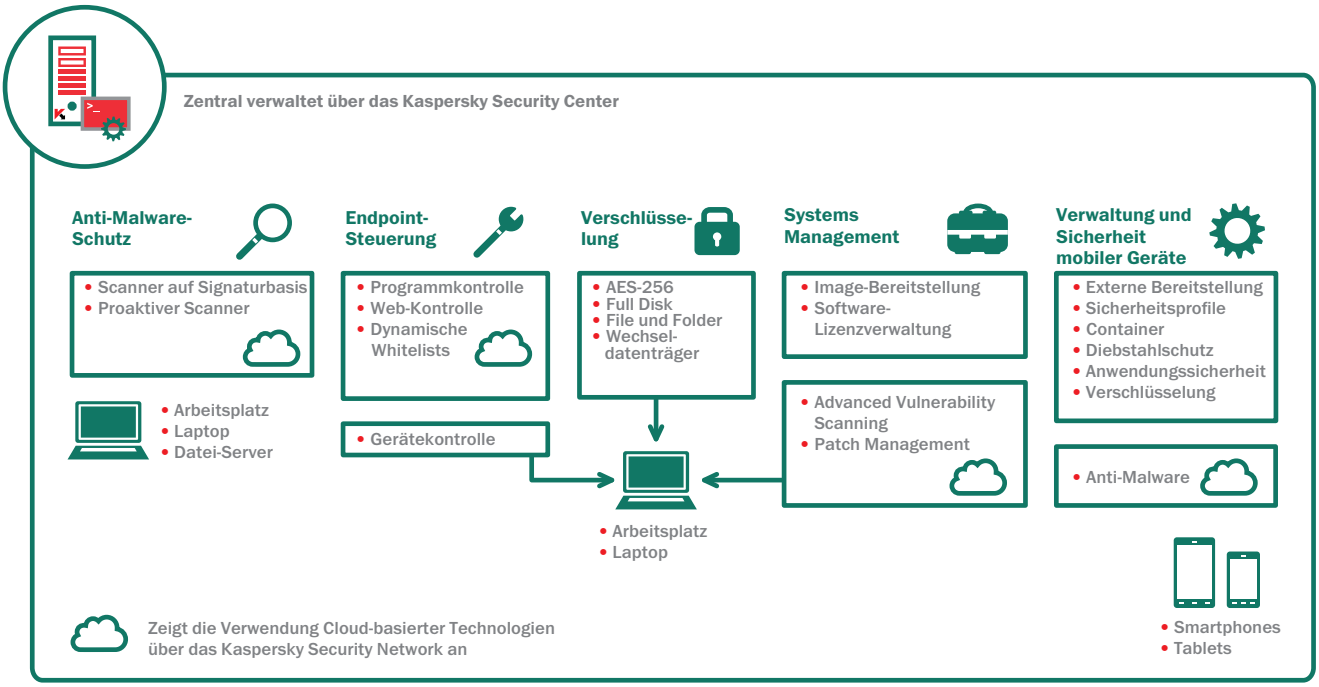
UNTERSTÜTZUNG VON MITARBEITEREIGENEN GERÄTEN
Unternehmensdaten und -anwendungen werden in verschlüsselten Containern isoliert, die für Benutzer transparent sind. Diese Daten können separat gelöscht werden.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Advanced



Die hochwertigen Lösungen von Kaspersky Lab umfassen eine große Zahl an Sicherheits-Tools und IT-Optimierungsfunktionen.

Die Schutzebene „Advanced“ von Kaspersky Lab bietet den Schutz und die Management-Lösung, die Ihr Unternehmen für IT-Richtliniendurchsetzung, Schutz der Benutzer vor Malware und Datenverlust und verbesserte IT-Effizienz benötigt.



Kaspersky Endpoint Security for Business – Stufe „Advanced“. Mit Verschlüsselungstechnologie und Security Systems Management.

HAUPTFUNKTIONEN:

HOCHWIRKSAME VERSCHLÜSSELUNGSTECHNOLOGIE
AES 256-Bit-Verschlüsselung auf Datenträger- oder File/Folder-Ebene sichert Daten, die verloren gegangen sind oder gestohlen wurden, und ermöglicht einen sicheren und transparenten Datenaustausch über Wechselmedien, per E-Mail, Netzwerk oder das Internet.

SYSTEMKONFIGURATION UND PATCH MANAGEMENT
Zusammen ergeben Funktionen zum Erstellen und Bereitstellen von Betriebssystem-Images, für die Prüfung auf Schwachstellen, ein automatisiertes Patch Management, Bestands- und Lizenzmanagement ein vollständig integriertes Toolkit, das über eine zentrale, benutzerfreundliche Verwaltungskonsole verwaltet wird.

MOBILE BEREITSTELLUNG UND SICHERHEIT FÜR SMARTPHONES UND TABLETS
Agentenbasierte Sicherheit für mobile Endpoints sowie Remoteverwaltung von mobilen Geräten und Softwarerichtlinien mithilfe von Kaspersky MDM.

LEISTUNGSSTARKE ANTI-MALWARE FÜR DEN ENDPOINT UND FLEXIBLE STEUERUNG
Cloud-basierte branchenweit führende Anti-Malware-Technologie sowie granulare Tools zur Kontrolle von Programmen, Web und Geräten.

IN DIESER STUFE KOMMEN HINZU:

VERSCHLÜSSELUNG UND DATENSCHUTZ:

UMFASSENDE VERSCHLÜSSELUNG
Gestützt auf Advanced Encryption Standard (AES) mit 256-Bit-Verschlüsselung können Sie entweder vollständige Datenträger oder auch Dateien verschlüsseln lassen, um erfolgserhebliche Geschäftsdaten bei Verlust oder Diebstahl eines Geräts abzusichern.

FREIGABE SICHERER DATEN
Erstellen Sie verschlüsselte und selbst extrahierende Pakete, um sicherzustellen, dass Daten, die über mobile Geräte, E-Mails, das Netzwerk oder das Internet weitergeleitet werden, geschützt sind.

UNTERSTÜTZUNG MOBILER GERÄTE
Verbessert Ihre Sicherheit über Richtlinien, die die Verschlüsselung von Daten auf mobilen Geräten erzwingen.

ENDBENUTZER-TRANSPARENZ
Die Verschlüsselungslösung von Kaspersky Lab ist nahtlos integriert, für Benutzer nicht erkennbar und beeinträchtigt die Produktivität nicht. Darüber hinaus gibt es keine Auswirkungen auf Anwendungseinstellungen oder Updates.

SYSTEMKONFIGURATION UND PATCH MANAGEMENT:

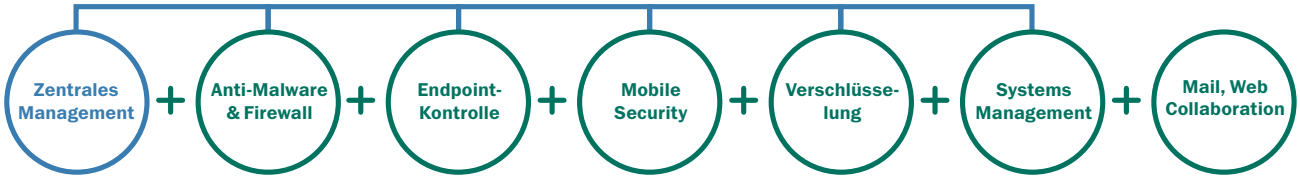
PATCH MANAGEMENT
Erweiterte umfassende Scans zu Schwachstellen in Kombination mit automatisierter Patch-Verteilung

BEREITSTELLUNG VON BETRIEBSSYSTEM UND ANWENDUNGS-IMAGE
Einfaches Erstellen, Speichern und Bereitstellen von System-Images von einem zentralen Standort aus.

EXTERNE BEREITSTELLUNG VON SOFTWARE
Zentrale Bereitstellung von Software auf Client-Rechnern, selbst in Zweigniederlassungen

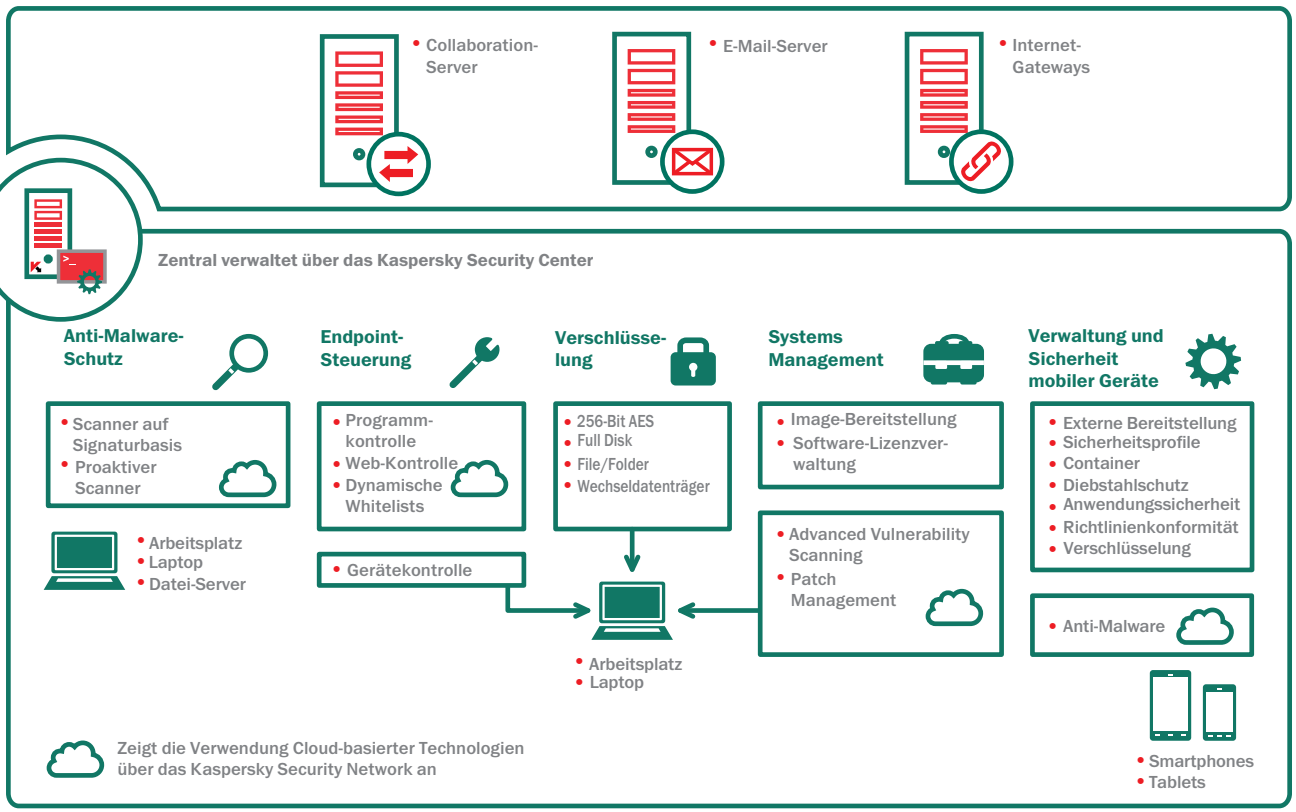
KONTROLLE ÜBER HARDWARE, SOFTWARE UND LIZENZEN
Hardware- und Software-Bestandsberichte unterstützen die Erfüllung von Software-Lizenzverpflichtungen. Entsprechend können Sie Kosten durch eine zentrale Bereitstellung von Software-Lizenzen sparen.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Durchgehender Schutz vor Malware, Verschlüsselung, umfassende IT-Effizienz und Tools zur Richtliniendurchsetzung.

Kaspersky Total Security for Business bietet eine umfangreiche Plattform für Schutz und Verwaltung. Total Security for Business sichert jede Ebene des Netzwerks ab und umfasst leistungsstarke Konfigurationstools, die die Produktivität der Benutzer und ihren Schutz vor Malware sicherstellen, egal mit welchem Gerät und an welchem Standort.



HAUPTFUNKTIONEN:

Alle Features der vorherigen drei Stufen plus:

MAIL-SERVER-SCHUTZ
Anti-Malware- und Anti-Spam-Schutz für E-Mail-Verkehr für alle gängigen E-Mail-Systeme

SICHERHEIT FÜR INTERNET-GATEWAYS
Gewährleisten Sie unternehmensweit sicheren Internetzugriff durch automatische Entfernung schädlicher und potenziell gefährlicher Programme im Datenverkehr über HTTP(S), FTP, SMTP und POP3.

COLLABORATION-SICHERHEIT
Kaspersky Lab schützt Ihre SharePoint®-Server vor Malware, während gleichzeitig Funktionen zur Inhalts- und Dateifilterung das Speichern unangebrachter Inhalte verhindern helfen.

IN DIESER STUFE KOMMEN HINZU:

MAIL-SERVER:

SCHUTZ DES E-MAIL-VERKEHRS
Schützt E-Mail der aktuellen Versionen aller führenden E-Mail- und Collaboration-Plattformen: Mail-Server auf Basis von Microsoft Exchange, IBM Lotus Domino und Linux.

KSN INTEGRATION FOR ANTI-SPAM
Erhöht die Spam-Erkennungsrate durch Integration in das Cloud-basierte Kaspersky Security Network (KSN).

REDUZIERUNG DER NETZWERKAUSLASTUNG
Cloud-basierte, intelligente Spam-Filter führen zu einer erheblichen Verringerung der Netzwerkauslastung.

OPTIMIERUNG DER SYSTEMRESSOURCEN
Eine neue Antiviren-Engine, Load Balancingverfahren für Serverressourcen und Scan-Ausnahmen reduzieren die Systembelastung.

INTERNET-GATEWAYS:

HOHE LEISTUNG UND ZUVERLÄSSIGKEIT
Eine neue Antiviren-Engine zusammen mit einer optimierten, intelligenten Scantechnologie und Load Balancing verbessern die Leistung und verringern den Bedarf an Computerressourcen während des Scans.

UNTERSTÜTZUNG MEHRERER PLATTFORMEN
Kaspersky Security für Internet-Gateways unterstützt die Gateways, die auf Windows- und Linux-Plattformen basieren.

COLLABORATION

ANTI-MALWARE-SCHUTZ FÜR SHAREPOINT-FARMEN
Nutzt innovative Erkennungstechnologien zur Identifizierung und Abwehr von Malware bei versuchten Uploads oder Downloads in Echtzeit.

INHALTSFILTERUNG
Verhindert externe Uploads unangemessener Inhalte, setzt interne Kommunikationsrichtlinien durch und blockiert die Speicherung von Dateien nach Dateityp oder Textinhalt.

KASPERSKY SECURITY FOR MOBILE

Komplette mobile Sicherheit durch Kombination von Mobile Device Management (MDM) und Endpoint Security for Mobile Devices.

Durch die Verwaltung mobiler Geräte ist die sichere Konfiguration von Mobilgeräten einfach und unkompliziert, während Kaspersky Endpoint Security for Mobile Devices den Schutz gewährt, den Sie vor heutigen Bedrohungen benötigen, und das sogar auf mitarbeitereigenen Geräten.

DETAILLIERTE FUNKTIONEN VON KASPERSKY SECURITY FOR MOBILE:

IT-EFFIZIENZ:

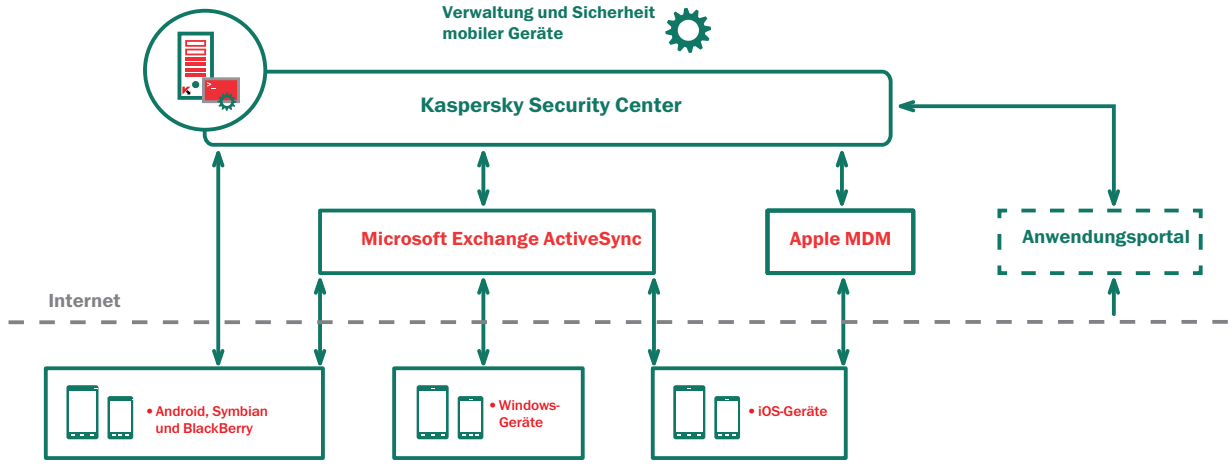
EINFACHE KONFIGURATION ÜBER EINE KONSOLE
Im Gegensatz zu anderen Lösungen brauchen Administratoren mit Kaspersky Lab nur eine Konsole zu verwenden, um die Sicherheit von mobilen Geräten, physischen Endpoints, virtuellen Systemen, Verschlüsselung und Tools zur Richtliniendurchsetzung zu verwalten.

PRIVATES ANWENDUNGSPORTAL
Administratoren veröffentlichen ein Unternehmensportal mit Links zu genehmigten Anwendungen. Die Benutzer können auf diese Anwendungen beschränkt werden.

„OVER THE AIR" PROVISIONING
Sichern Sie Telefone aus der Ferne, indem Sie entweder eine E-Mail oder eine SMS mit einem Link zum Unternehmensportal senden, von dem Benutzer das Profil und von Ihnen genehmigte Anwendungen herunterladen können. Der Zugriff auf Daten wird erst dann gestattet, wenn der Benutzer die Bedingungen akzeptiert hat.

SICHERE KONFIGURATION
Stellen Sie die Hardware- und Softwareintegrität sicher, indem Sie die Erkennung von Rooting und Jailbreaks aktivieren. Weitere Sicherheitseinstellungen sind „Camera disable", Kennwort erzwingen u. a.

EINHALTUNG UND RICHTLINIENDURCHSETZUNG
Über die Programmkontrolle können Sie die Anwendungsnutzung auf dem Gerät überwachen und steuern, einschließlich der Unterstützung für die Richtlinien „Default Deny" und „Default Allow".



SICHERHEITSRISIKOSTEUERUNG:

VERSCHLÜSSELUNG
Übertragene Daten werden durch eine transparente Datenverschlüsselung für den gesamten Datenträger oder auf Dateiebene geschützt, die auch auf einen Container angewendet werden kann.

DIEBSTAHLSCHUTZ
Administratoren können aus der Ferne eine vollständige oder selektive Gerätelöschung durchführen, den Standort eines vermissten Geräts mithilfe von GPS bestimmen und eine Benachrichtigung erhalten, wenn eine SIM-Karte entfernt oder ausgetauscht wird.

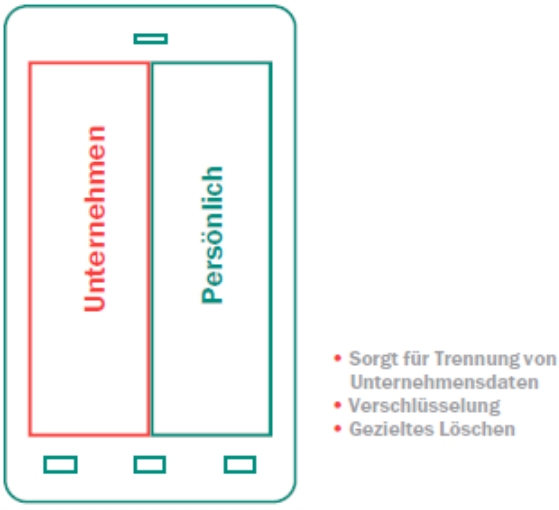
MOBILE ANTI-MALWARE
Die Anti-Malware-Engine von Kaspersky Lab weist mehrere Erkennungsebenen auf, einschließlich Cloud-basierten Schutz, und kombiniert einen sicheren Browser und leistungsstarken Anti-Spam-Schutz, um sicherzustellen, dass das Gerät nicht durch gefährliche Software manipuliert wird.

UNTERNEHMENS- UND PERSÖNLICHE DATENINTEGRITÄT:

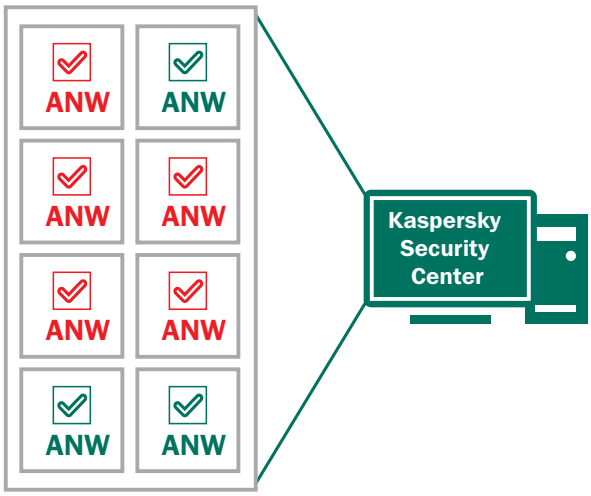
CONTAINER
Zur Unterstützung von mitarbeitereigenen Geräten können Unternehmensdaten und -anwendungen in isolierten „Containern“ platziert werden. Dadurch wird maximale Sicherheit für die Unternehmensdaten und optimale Integrität für persönliche Inhalte gewährleistet.

TOOLS FÜR DIE SICHERHEIT VON REMOTE-DATEN
Wenn ein Gerät verloren gegangen ist, kann die Remote-Sperre aktiviert werden. Die Unternehmensdaten in einem Container auf dem Gerät können unabhängig von den persönlichen Daten auf dem Gerät gesichert, verschlüsselt, aus der Ferne verwaltet und gelöscht werden.

Bildung von getrennten Containern



Privates „App“-Portal



PERFEKT FÜR BYOD-INITIATIVEN („BRING YOUR OWN DEVICE“)

Viele Mitarbeiter nutzen ihre eigenen Geräte für persönliche wie auch für geschäftliche Aufgaben. Manche Unternehmen ermutigen Ihre Mitarbeiter sogar, Ihr bevorzugtes Smartphone oder Tablet von einem Händler zu kaufen. Die IT-Abteilung fügt dann den E-Mail- und Unternehmenszugang zum mitarbeitereigenen Gerät hinzu.

Dadurch lassen sich Einsparungen und Produktivitätssteigerungen erzielen, doch die Nutzung mitarbeitereigener Geräte kann für das Unternehmen auch ein Sicherheitsrisiko bedeuten. Unternehmensdaten, die nicht korrekt gesichert und möglicherweise zusammen mit persönlichen Elementen vermischt sind, können leicht abhanden kommen oder in unbefugte Hände geraten. Diese Geräte werden häufig ohne Rücksicht auf Anwendungssicherheit von Familienmitgliedern genutzt. Manche werden sogar gerootet oder einem Jailbreak unterzogen.

Kaspersky Security for Mobile löst diese Probleme durch die Aktivierung der sicheren Konfiguration und Bereitstellung von Smartphones und Tablets über die gleiche Konsole, die auch für Ihre Netzwerksicherheit verwendet wird. IT-Administratoren können sich darauf verlassen, dass Benutzergeräte mit den korrekten Einstellungen konfiguriert sind und bei Verlust, Diebstahl oder Benutzermissbrauch abgesichert werden können.

KASPERSKY SYSTEMS MANAGEMENT

Das neue Kaspersky Systems Management. Diese Lösung bietet ein breites Funktionsangebot mit starken IT-Produktivitätstools, die im gleichen Code geschrieben sind und von einer Konsole aus verwaltet werden. Die so entstandene Plattform liefert die einfache Bedienung und Automatisierung, die Sie erwarten – sowie die Sicherheit und Kontrolle, die Sie benötigen.

UNEINHEITLICHE IT-TOOLS FÜHREN ZU KOMPLEXITÄT – UND KOMPLEXITÄT IST DER NATÜRLICHE FEIND VON SICHERHEIT.

Duplizierung vermeiden
Reduzieren Sie die Duplizierung des Aufwands bei der Einrichtung der individuellen Systeme für neue und vorhandene Benutzer. Mit der Systems-Management-Technologie können Disk-Images von einem zentralen Standort aus erstellt, verwaltet und bereitgestellt werden.

Sicherheit verbessern
Administratoren sagen, dass sie oft damit beschäftigt sind, sicherzustellen, dass Patches auf dem neuesten Stand sind. Kaspersky Lab reduziert diese Komplexität, indem es Schwachstellen identifiziert, die ausgenutzt werden könnten, und erkennt, welche Probleme später behoben werden können. Diese Priorisierung unterstützt Administratoren dabei, die IT-Sicherheit zu erhöhen.

Effizient arbeiten
Administratoren können per Fernzugriff Images, Updates, Patches und Anwendungen installieren. Wenn ein Benutzer ein Problem meldet, kann sich der IT-Mitarbeiter per Fernzugriff am Gerät anmelden und den Fehler im System beheben.

Diese und mehr Funktionen sind Teil von Kaspersky Systems Management, und der Zugriff erfolgt mithilfe der Kaspersky Security Center-Verwaltungskonsole. Da nicht jedes Tool eine eigene Konsole benötigt, sind die Befehle einheitlich und intuitiv.

FUNKTIONEN DES SYSTEMS MANAGEMENT:

BEREITSTELLUNG VON BETRIEBSSYSTEM UND ANWENDUNGEN
Einfaches Erstellen, Speichern, Klonen und Bereitstellen von System-Images von einem zentralen Standort aus. Stellen Sie sicher, dass Systeme dem Benutzer ohne Probleme und mit optimalen Sicherheitseinstellungen geliefert werden.

BEHALTEN SIE BEI SCHWACHSTELLEN DEN ÜBERBLICK
Mit nur einem Klick vergleicht die Hardware- und Softwareüberprüfung Ergebnisse mehrerer Datenbanken zu Schwachstellen, sodass Sie priorisieren können, welche Schwachstellen sofortige Aufmerksamkeit benötigen und welche Sie später beheben können.

FLEXIBLE SOFTWAREINSTALLATION PER FERNZUGRIFF
Verringern Sie die Arbeitslasten in Netzwerken, indem Sie manuelle oder planmäßige Bereitstellungen verwenden.

UPDATE-AGENTS
Legen Sie eine Workstation in einer Fern- oder Zweigniederlassung als zentralen Update-Agent fest. Sparen Sie Bandbreite, indem Sie ein Update an einen entfernten Standort senden – und die festgelegte lokale Workstation verwenden, um das Update für diesen Standort zu verteilen.

UNTERSTÜTZUNG VON WAKE-ON-LAN-TECHNOLOGIE
Für die Bereitstellung oder den Support außerhalb der Bürozeiten kann Kaspersky Systems Management eine Workstation per Fernzugriff hochfahren.

TOOLS ZUR FEHLERBEHEBUNG
Stellen Sie per Fernzugriff eine sichere Verbindung zu einem Client-System her, um Fehler zu beheben – über dieselbe Verwaltungskonsole.

UNTERSTÜTZUNG FÜR MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS)
Kaspersky Systems Management synchronisiert regelmäßig die verfügbaren Updates und Hotfixes mit Servern, einschließlich Microsoft Windows Update, lädt sie über Windows Update Services herunter und verteilt sie effizient.

HARDWARE- UND SOFTWARE-BESTANDSLISTEN
PCs, Festplatten und sogar Wechseldatenträger werden automatisch erkannt und inventarisiert. Beim Hinzufügen eines neuen Geräts wird eine Benachrichtigung an den Administrator gesendet. Diese Funktion ermöglicht es dem Administrator, den Status und die Nutzung der Hardware im Netzwerk zu verfolgen.

BEREITSTELLUNG UND STEUERUNG VON LIZENZEN
Kaspersky Systems Management berichtet genau, welche Software in Ihrer Umgebung verwendet wird. Dies ermöglicht Ihnen die Anpassung Ihrer Lizenzkosten und die Identifizierung von Benutzern, welche die Lizenzen nicht einhalten. In Kombination mit den Tools zur Endpoint-Steuerung von Kaspersky Lab können Sie die Nutzung auf genehmigte Anwendungen und Versionen begrenzen – und die Anzahl der gleichzeitig verwendeten Lizenzen einschränken.

KASPERSKY SECURITY FÜR FILE-SERVER

Kaspersky Security für File-Server schützt Server unter Microsoft® Windows®, Novell NetWare und Linux zuverlässig gegen alle Arten von Schadprogrammen.

Antiviren-Schutz für die Speicherung gemeinsam verwendeter Dateien ist unerlässlich, da eine einzige infizierte Datei auf einem Server, die Workstations aller Benutzer der Ressource infizieren könnte. Eine effektive Absicherung der Dateiserver sorgt nicht nur für den Schutz von Benutzern und ihren Daten, sondern verhindert auch, dass Schadprogramme in die Sicherungskopien der Dateien eindringen, was zu wiederholten Malware-Ausbrüchen und anderen Vorfällen führen könnte.

PRODUKT-HIGHLIGHTS*

- Unterstützung für aktuelle Versionen von Microsoft® Windows® und Linux-Plattformen
- Optimale Nutzung von Systemressourcen
- Unterstützung von HSM-Systemen (Hierarchical Storage Management)
- Schutz von Terminal- und Cluster-Servern
- „VMware-kompatibel“-Zertifizierung
- Unterstützung von NSS-Dateisystemen

FEATURES

- Schutz von File-Servern unter Windows®, Linux (einschließlich Samba) und Novell NetWare
- Verbesserter proaktiver Schutz vor neuer Malware
- Echtzeitschutz vor Viren
- Behandlung aktiver Infektionen
- Zeitplangesteuertes Scannen des Dateispeichers
- Scannen von kritischen Systembereichen
- Isolierung infizierter Workstations
- Skalierbarkeit
- Backup-Speicherung vor der Desinfektion und Löschung
- Zentralisierte Installation, Management und Updates
- Auswahl von Installations- und Verwaltungsmethoden
- Flexibles System aus Scanning- und Vorfallreaktionsszenarien
- Benachrichtigungssystem für Anwendungsstatus
- Umfassende Berichte zum Netzwerkschutzstatus

ANWENDUNGEN

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

KASPERSKY SECURITY FÜR MAIL-SERVER

Kaspersky Security für Mail-Server schützt Mail- und Groupware-Server vor Schadprogrammen und Spam.

Das Produkt enthält Anwendungen, die den E-Mail-Verkehr auf allen gängigen Mail-Servern absichern, darunter Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim und CommuniGate Pro. Außerdem lässt sich ein dediziertes E-Mail-Gateway einrichten.

PRODUKT-HIGHLIGHTS*

MAIL-SERVER-SCHUTZ
Anti-Malware- und Anti-Spam-Schutz für E-Mail-Verkehr für alle gängigen E-Mail-Systeme.

OPTIMIERUNG DER SYSTEMRESSOURCEN
Eine neue Antiviren-Engine, Load Balancingverfahren für Serverressourcen und Scan-Ausnahmen reduzieren die Systembelastung.

KSN-INTEGRATION FÜR ANTI-SPAM-SCHUTZ
Erhöht die Spam-Erkennungsrate durch Integration in das Cloud-basierte Kaspersky Security Network (KSN).

REDUZIERUNG DER NETZWERKAUSLASTUNG
Cloud-basierte, intelligente Spam-Filter führen zu einer erheblichen Verringerung der Netzwerkauslastung.

FEATURES

- Integrierter Schutz von Mail-Servern vor allen Arten von Schadprogrammen
- Effektiver Schutz vor Spam
- Echtzeitschutz vor Viren
- Zeitplangesteuertes Scannen von E-Mails und Datenbanken
- Schutz für verschiedene Mail-Server, darunter Sendmail, qmail, Postfix, Exim und CommuniGate Pro
- Scannen von Nachrichten, Datenbanken und anderen Objekten auf Lotus® Domino®-Servern
- Scannen aller Nachrichten auf einem Microsoft® Exchange-Server, darunter auch öffentliche Ordner
- Filtern von Nachrichten nach Anhangstyp
- Skalierbarkeit
- Unterstützung für Microsoft® Exchange Server, Microsoft ® Exchange Server-Cluster und -DAG
- Backup-Speicherung vor der Desinfektion und Löschung
- Isolierung infizierter Objekte
- Abbrechen sich wiederholender Mail-Prüfung
- Benutzerfreundliche Tools für Installation, Management und Updates
- Umfassende Berichte zum Schutzstatus
- Flexibles System aus Scanning- und Vorfallreaktionsszenarien
- Benachrichtigungssystem für Anwendungsstatus

ANWENDUNGEN

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

KASPERSKY SECURITY FÜR INTERNET-GATEWAYS

Kaspersky Security für Internet-Gateways garantiert für alle Mitarbeiter in einem Unternehmen den sicheren Internetzugriff.

Kaspersky Security für Internet-Gateways unterstützt die Gateways, die auf Windows- und Linux-Plattformen basieren. Bekannte Schadprogramme und potenziell gefährliche Programme, die über die Protokolle HTTP, HTTPS, FTP, POP3 und SMTP ausgeführt werden, werden automatisch aus dem Datenstrom gelöscht. Optimierungstechnologie, Skalierbarkeit und Unterstützung der aktuellen Plattformen machen es zum idealen Produkt für Unternehmen mit hohem Datenverkehrsaufkommen.

PRODUKT-HIGHLIGHTS*

- Schutz von Microsoft® Forefront® TMG
- Große Bandbreite von Tools für die Richtlinienverwaltung und -konfiguration
- Schutz von E-Mail-Schutz (über POP3- und SMTP-Protokolle)
- Scannen von HTTP- und FTP-Datenverkehr von veröffentlichten Servern
- „VMware-kompatibel“-Zertifizierung

FEATURES

- Echtzeit-Untersuchungen von Internetverkehr über HTTP, HTTPS, FTP, POP3 und SMTP
- Integrierter Schutz vor allen Arten von Schadprogrammen
- Backup-Sicherungen
- Load Balancing für Serverprozessoren
- Skalierbarkeit
- Benutzerfreundliche Tools für Installation, Management und Updates
- Flexibles System aus Scanning- und Vorfallreaktionsszenarien
- Umfassende Berichte zum Netzwerkschutzstatus

ANWENDUNGEN

- Kaspersky Anti-Virus für Microsoft® ISA Server und Forefront® TMG Standard Edition
- Kaspersky Anti-Virus für Microsoft® ISA Server Enterprise Edition
- Kaspersky Anti-Virus für Proxy Server

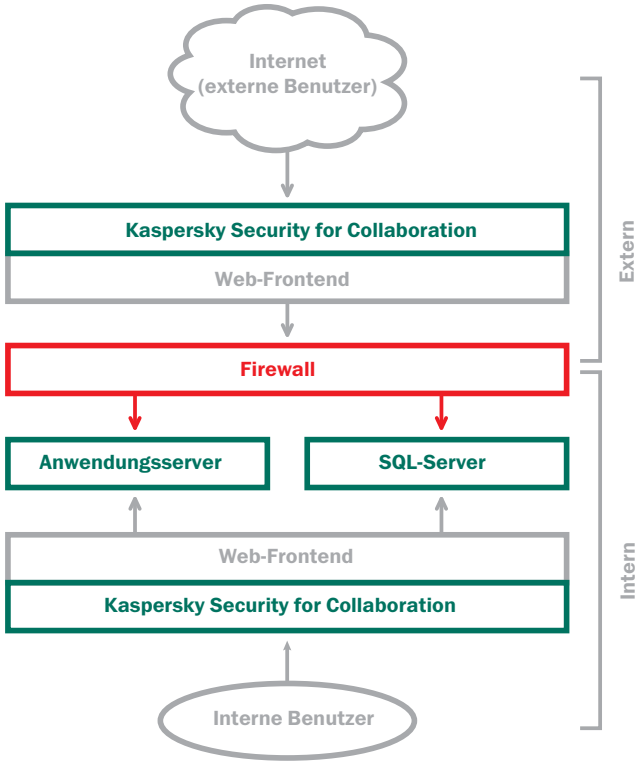
KASPERSKY SECURITY FÜR COLLABORATION

Kaspersky Security für Collaboration sichert Ihre Collaboration-Plattform mit hochmodernen, benutzerfreundlichen Schutztechnologien, die eine hohe Erkennungsrate bieten.

Kaspersky Security für Collaboration nutzt die preisgekrönte Antiviren-Engine von Kaspersky Lab, um Microsoft® SharePoint®-Umgebungen zu schützen. Dank seiner preisgekrönten Malware-Erkennungstechnologie schützt das Produkt einen einzelnen Server oder ganze SharePoint-Farms, während seine Inhalts- und Dateifilterfunktionen eine Speicherung von unangemessenen Inhalten verhindert.

FEATURES

- Innovative Erkennungstechnologien zur Identifizierung und Abwehr von Malware bei versuchten Uploads oder Downloads in Echtzeit.
- Hindert Benutzer an der Speicherung bestimmter Dateitypen (z. B. Musik, Video, Programmdateien) oder von Dateien mit unangemessenem Textinhalt
- Globale Verwaltungseinstellungen lassen sich über ein Dashboard auf allen geschützten Servern konfigurieren
- Einfache, intuitive Bedienung
- Interaktion mit Active Directory sorgt für optimierte Konfiguration und Benutzerauthentifizierung
- Detaillierte Protokolle und Sicherung von geänderten Dateien unterstützen Administratoren bei der Reaktion auf Sicherheitsverletzungen und -probleme
- Detaillierte, flexible Berichte



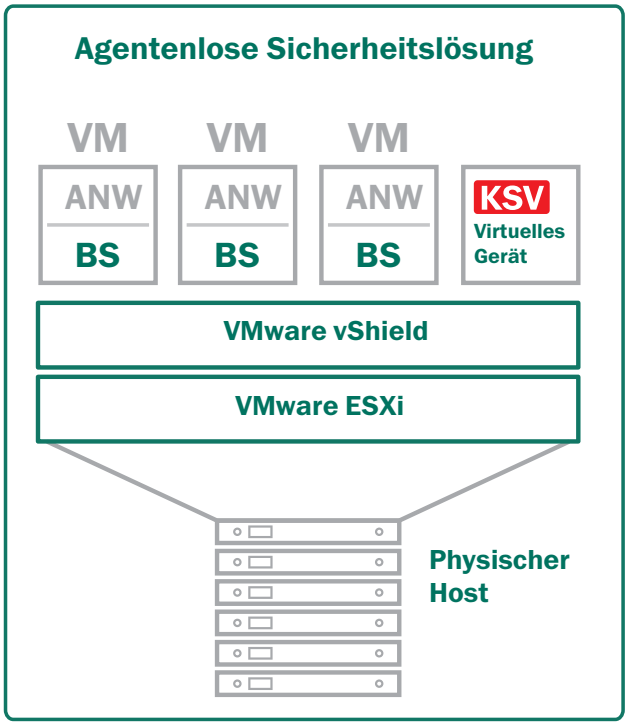
KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization ist genau auf die besonderen Anforderungen virtualisierter IT-Umgebungen zugeschnitten und bietet einen ausgezeichneten Anti-Malware-Schutz für virtualisierte Server, Desktops und Rechenzentren.

Kaspersky Security for Virtualization ist eine agentenlose Anti-Malware-Lösung für einen effizienteren Schutz Ihrer virtualisierten Infrastruktur, die für erhöhte Leistung sorgt und geringere Auswirkungen auf die Virtualisierungsdichte hat. Die Anwendung lässt sich auf einfache Weise bereitstellen und umfasst erweiterte Verwaltungsfunktionen zur Erleichterung einer Vielzahl von Sicherheitsaufgaben bei physischen und virtuellen Computern.

SCHUTZ- UND LEISTUNGSFUNKTIONEN

- Zentralisierte Sicherheit. Kaspersky Security for Virtualization ist ein virtuelles Gerät, das an vShield Endpoint von VMware angeschlossen werden kann und Anti-Malware-Scan-Funktionen bietet. Es stellt eine zentrale Anti-Malware-Engine und eine Datenbank für jeden physischen Host bereit.
- Erweiterte Antiviren-Engine. Die ausgezeichneten Anti-Malware-Technologien von Kaspersky Lab sowie die beispiellose Häufigkeit von Updates sorgen für einen optimalen Schutz vor neuen und entstehenden Bedrohungen. Polymorphe Malware wird durch ein heuristisches Analyseprogramm bekämpft.
- Automatischer Schutz. Neue virtuelle Maschinen werden automatisch mit Anti-Malware-Schutz versehen, um Sicherheitslücken und fehlerhafte Konfigurationen einzudämmen. Gast-VMs werden mithilfe der aktuellen Signaturdatenbank geschützt, unabhängig davon, ob eine VM zuvor offline war.
- Höhere Virtualisierungsdichte. Da Kaspersky Security for Virtualization eine agentenlose Lösung ist, werden „Update-Storms“ und „Scan-Storms“ vermieden, eine höhere Virtualisierungsdichte erzielt und die Auswirkungen auf die Leistung möglichst gering gehalten. Zudem werden die bei manchen agentenbasierten Produkten vorhandenen Sicherheitslücken beseitigt.
- Network Attack Blocker. Diese Applikation scannt den Netzwerk-Traffic virtueller Maschinen nach typischen Anzeichen von Netzwerk-Angriffen. Sobald eine Netzwerk-Angriff auf eine virtuelle Maschine erkannt wird, kann Kaspersky Security die IP-Adresse blockieren, von der der Angriff ausgeht. Kaspersky Security sendet Informationen aller Aktivitäten, die Netzwerk-Angriffe auf virtuelle Maschinen unterbinden, an den Administrator des Kaspersky Security Center.



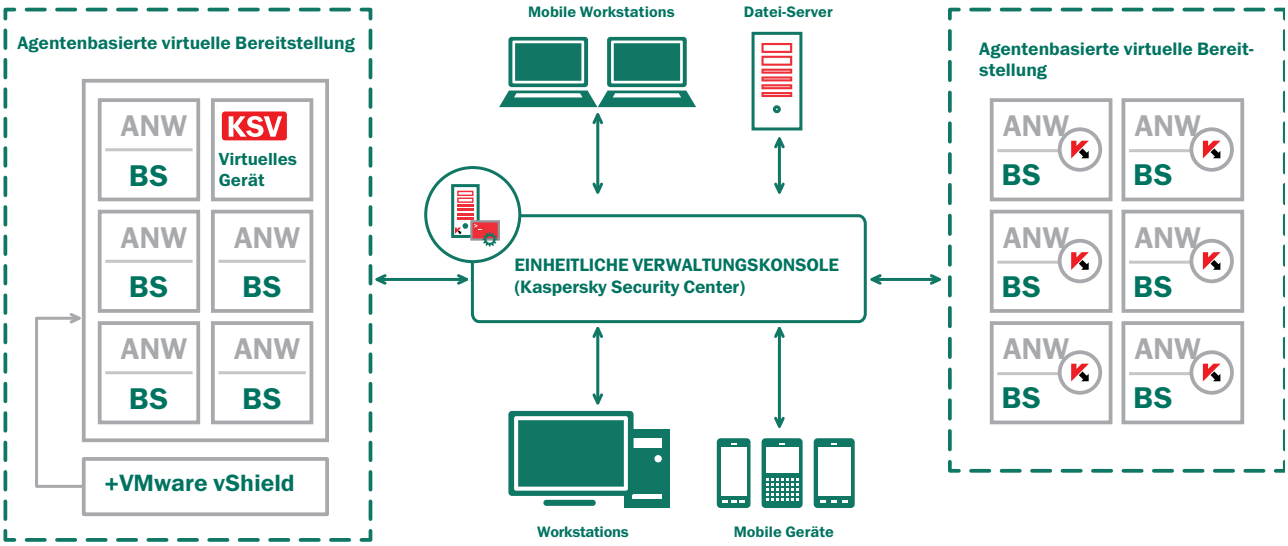
Kaspersky Security for Virtualization bietet agentenlosen Antiviren-Schutz für VMware-Bereitstellungen.

VERWALTUNGSFUNKTIONEN:

ZENTRALE VERWALTUNGSKONSOLE.
Mit Kaspersky Security Center – ohne zusätzliche Kosten verfügbar – erhalten Sie eine zentrale Verwaltungskonsole zur Überwachung der Sicherheit virtueller und physischer Maschinen sowie mobiler Geräte.

UNTERSTÜTZUNG VON VMWARE VMOTION
Dank der umfassenden Unterstützung von VMware vMotion sorgt Kaspersky Security for Virtualization dafür, dass der Schutz beim Übertragen von Arbeitslasten von einem ESXi-Host auf einen anderen nicht unterbrochen wird. Wenn der neue Host über die erforderlichen Lizenzen verfügt, wird der Schutz für die Arbeitslast unter Beibehaltung aller Sicherheitseinstellungen übernommen.

INTEGRATION MIT VMWARE VCENTER.
Kaspersky Security for Virtualization empfängt Informationen zu virtuellen Maschinen von vCenter, darunter eine Liste aller virtuellen Maschinen und relevanten Parameter. Neben der besseren Transparenz für das IT-Team bedeutet die Integration mit vCenter, dass bei jeder Konfiguration einer neuen virtuellen Maschine automatisch Schutz bereitgestellt wird.



KSV Kaspersky Security for Virtualization Sicherheitslösung von Kaspersky Lab

KASPERSKY ANTI-VIRUS FÜR STORAGE-LÖSUNGEN

Kaspersky Anti-Virus für Storage-Lösungen schützt EMC Celerra/VNX-Netzwerkspeicherprodukte vor allen Arten von Malware.

Daten-Storage-Systeme in einem Netzwerk bieten Mitarbeitern in Unternehmen aller Größenordnungen schnell und einfach Zugriff auf gemeinsam genutzte Daten. Ist ein Unternehmensnetzwerk jedoch nicht geschützt, kann der Zugriff auf gemeinsam genutzte Dateien wenig wünschenswerte Nebenwirkungen haben. Eine einzige infizierte Datei kann das gesamte Netzwerk gefährden und zu einem beträchtlichen Schaden für Unternehmen, Finanzen und Ansehen führen. Deshalb ist ein umfassender Schutz für Netzwerkspeichersysteme so essenziell.

Kaspersky Anti-Virus für Storage-Lösungen ist vollständig kompatibel mit der EMC Celerra/VNX-Produktpalette. Die Lösung ist auf größtmöglichen Schutz sowie eine effektive Erkennung und Neutralisierung von Malware in Dateien und Archiven in Celerra-Systemen optimiert. Scanvorgänge lassen sich in Echtzeit ausführen, wenn Objekte gespeichert und geändert werden, oder nach Bedarf.

FEATURES

- Schutz für EMC Celerra/VNX-Datenspeichersysteme
- Unterstützung für Windows Server®
- Unterstützung von HSM-Systemen (Hierarchical Storage Management)
- Verbesserter proaktiver Schutz vor neuer Malware
- Echtzeitschutz vor Viren
- Zeitplangesteuertes Scannen des Dateispeichers
- Scannen von kritischen Systembereichen
- Optimale Nutzung von Systemressourcen
- Backup-Speicherung vor der Desinfektion und Löschung
- Skalierbarkeit
- „VMware-kompatibel“-Zertifizierung
- Zentralisierte Installation, Management und Updates über Kaspersky Security Center
- Vollständige Integration mit Kaspersky Endpoint Security for Business Platform und anderen Kaspersky-Produkten
- Benachrichtigungssystem für Anwendungsstatus
- Umfassende Berichte zum Netzwerkschutzstatus

NOTIZEN

Kaspersky Labs GmbH
Despag-Straße 3
85055 Ingolstadt
Deutschland
salesDACH@kaspersky.de
www.kaspersky.de

Informationen zur Internetsicherheit:
www.viruslist.de

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

5bzfb/Stand: März 2013