KASPERSKY lab

KASPERSKY SECURITY FOR BUSINESS-PORTFOLIO 2015

‚EFFEKTIVER SCHUTZ FÜR IHR UNTERNEHMEN‘

Jedes Unternehmen, egal welcher Größe, ist dem Risiko von Bedrohungen durch Malware ausgesetzt. Kaspersky Lab ist in der einmaligen Position, einen Großteil dieser Bedrohungen zu erkennen.

Und das Ausmaß der Bedrohung nimmt ständig zu. Es gibt täglich 325.000 neue Bedrohungen, die es auf Einzelbenutzer und Unternehmen wie das Ihre abgesehen haben.

Hier bei Kaspersky Lab nehmen wir diese Bedrohungen und die Risiken, die diese Unternehmen aussetzen, sehr ernst. Deshalb empfehlen wir Unternehmen wie Ihrem, eine IT-Sicherheitsstrategie zu implementieren, welche drei wichtige Kriterien erfüllt:

- **Erstens** benötigen Sie Informationen, die auf einer hochwertigen Bedrohungsanalyse beruhen. Diese setzt ein tiefgreifendes Verständnis dessen voraus, wie eine Malware-Bedrohung aussieht, wie sie programmiert und kompiliert wird. Es ist entscheidend, dass Ihr Sicherheitssystem laufend mit Experteninformationen gefüttert wird und Ihr Sicherheitsanbieter die weltweiten Malware-Hotspots durchkämmt, um auf kommende Entwicklungen vorbereitet zu sein.

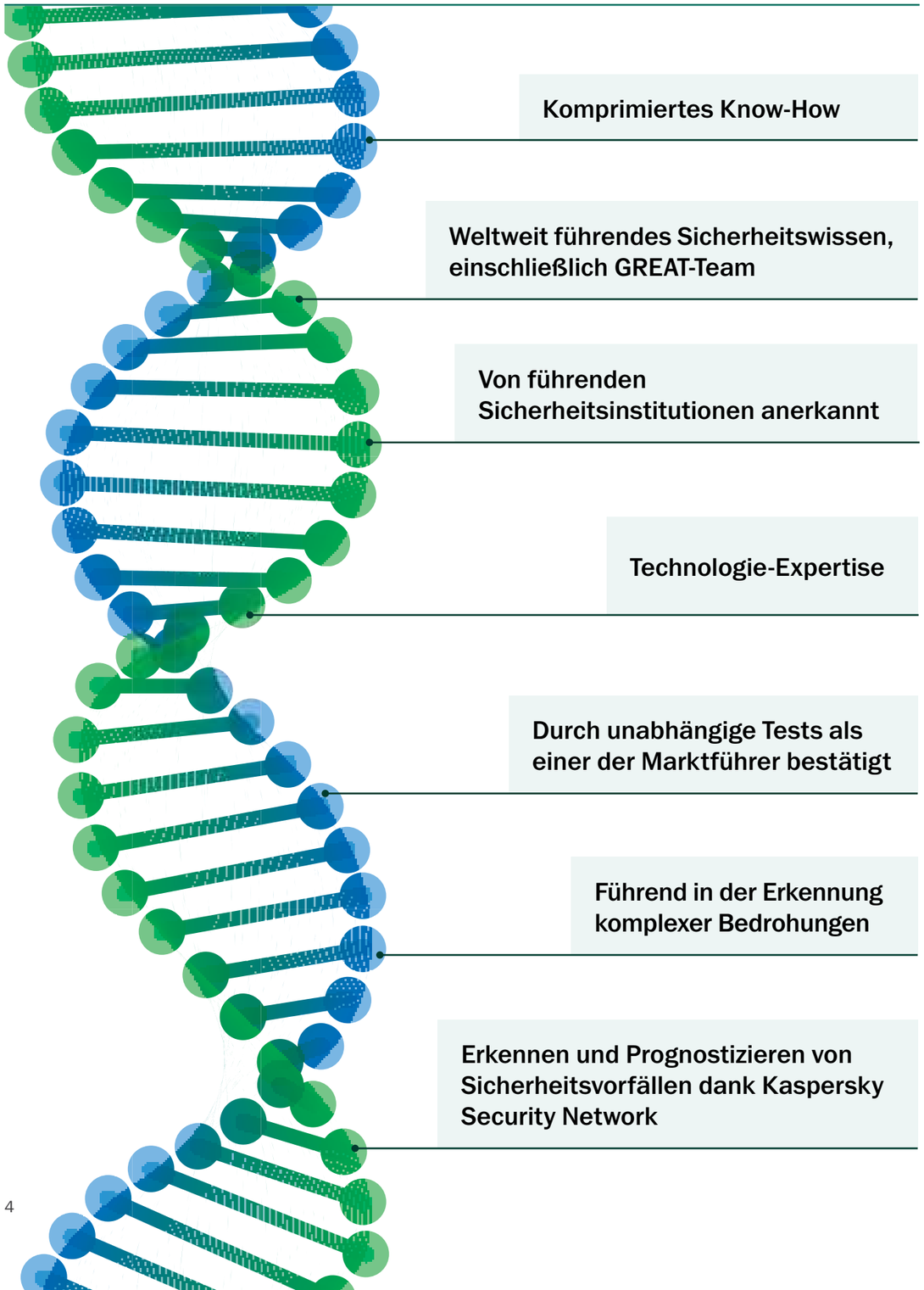
- **Zweitens** benötigen Sie Tools und Techniken, die in der Lage sind, bekannte, unbekannte und hoch entwickelte Malware zu erkennen und zu eliminieren. Gleichzeitig sollte Ihre Sicherheitssoftware jedoch auch keine zu große Belastung für Ihre Systeme darstellen und schnelle Scanzeiten ermöglichen, um den Geschäftsbetrieb nicht zu verlangsamen.

- **Drittens** muss diese Technologie aufgrund der zunehmenden Komplexität von IT-Umgebungen in Unternehmen physische, mobile und virtualisierte Endpoints nahtlos und effizient über eine einzige Plattform abdecken. Und das ohne irgendwelche Softwarekonflikte, unterschiedliche Bedienkonsolen und Sicherheitslücken.

Kaspersky Lab bietet eine weltweit führende Bedrohungsanalyse und die Technologie, die Ihr Unternehmen zur Umsetzung einer effizienten Sicherheitsstrategie benötigt - und das alles innerhalb einer umfassende Sicherheitsplattform.

Kaspersky-Lösungen bieten von sich aus die Flexibilität, an Ihre unternehmerischen Ziele angepasst zu werden. Dies bedeutet, dass wir immer in Bereitschaft sind, Ihr Unternehmen vor Bedrohungen Ihrer physischen und virtualisierten Endpoints, Ihrer mobilen Geräte, Ihre E-Mail-Systeme, Server, Gateways und SharePoint-Portale zu schützen. Wenden Sie sich noch heute an uns oder Ihren IT-Händler, wenn Sie Fragen zu einem der Produkte, Lösungen oder Services in diesem Dokument haben. Wir zeigen Ihnen gerne, auf welche Weise wir zusammenarbeiten können, um Ihr Unternehmen vor Cyberbedrohungen zu schützen.

IN UNSERER DNA STECKT DAS SICHERHEITS-GEN



Komprimiertes Know-How

Weltweit führendes Sicherheitswissen, einschließlich GREAT-Team

Von führenden Sicherheitsinstitutionen anerkannt

Technologie-Expertise

Durch unabhängige Tests als einer der Marktführer bestätigt

Führend in der Erkennung komplexer Bedrohungen

Erkennen und Prognostizieren von Sicherheitsvorfällen dank Kaspersky Security Network

SICHERHEIT MIT EINEM ENTSCHEIDENDEN UNTERSCHIED

Kaspersky Lab bietet die leistungsstärksten Anti-Malware-Technologien am Markt. Unser weltweit führendes Sicherheitswissen nutzen wir stets für alles was wir tun und wie wir es tun.

- Wir sind von Kopf bis Fuß ein technologiebasiertes Unternehmen, geführt von unserem CEO, Eugene Kaspersky.
- Unser Global Research & Analysis Team (GReAT) besteht aus einer erlesenen Gruppe von IT-Sicherheitsexperten, die einige der weltweit gefährlichsten Malware-Bedrohungen und gezielten Angriffe als erste erkannt hat.
- Viele der weltweit angesehensten Sicherheitsinstitutionen und Vollzugsbehörden haben uns bereits aktiv um Unterstützung gebeten.
- Die Kerntechnologien bei Kaspersky Lab werden intern entwickelt. Ein Grund, daß unsere Produkte sehr zuverlässig und leistungsfähig sind.
- Kaspersky Lab nimmt Jahr für Jahr an vielen unabhängigen Tests teil. Die Testergebnisse zeigen durchgängig überdurchschnittliche Resultate auf!
- Die renommiertesten Branchenanalysten, darunter Gartner, Forrester Research und International Data Corporation (IDC), setzen uns in vielen wichtigen IT-Sicherheitskategorien an die Spitzenposition.
- Mehr als 130 OEMs, darunter Microsoft®, Cisco® Meraki, Juniper Networks, Alcatel Lucent und weitere, nutzen unsere Technologien innerhalb ihrer eigenen Produkte und Services.

Und das alles macht den Unterschied aus!

INFORMATIONEN ZU UNSERER ANTI-MALWARE-TECHNOLOGIE

IT-Sicherheitssoftware ist nur so effektiv wie die zugrunde liegende Sicherheits-Engine. Patch Management, MDM, Verschlüsselung, Gerätekontrolle, Phishing-Schutz –all diese Technologien sorgen für wichtige zusätzliche Schutzschichten. Unternehmen sollten beim Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen keine Kompromisse eingehen.

Unsere Sicherheits-Engine wird kontinuierlich durch unser neuestes und dynamisches Sicherheitswissen aktualisiert und somit verbessert. Unser permanenter Fokus auf alle Sicherheitsthemen, zusammen mit unserer globalen Erfahrung, macht es möglich unseren Kunden beständig ein starker Partner zu sein.

Eine Vielzahl unabhängiger Tests beweisen, dass die Anti-Malware Engine, innerhalb des Security-Marktes eine herausragende Stellung einnimmt. Diese Engine ist integrativer Bestandteil der Kaspersky Endpoint Security for Business Plattform.

Malware-Schutz von Kaspersky Lab bietet eine Reihe von Vorteilen:

WICHTIGE PRODUKTFUNKTIONEN

- **Erkennung von bekannten, unbekannten und hoch entwickelten Bedrohungen**
- **Verhaltensanalyse & Heuristik**
- **Kaspersky Security Network für Cloud-basierten Schutz**
- **Active Disinfection**
- **Schutz vor Verschlüsselung und Ransomware**
- **Automatischer Exploit-Schutz**
- **HIPS & Persönliche Firewall**
- **Network Attack Blocker**
- **Einfache und übersichtliche Verwaltungskonsole**

WICHTIGSTE VORTEILE

MEHRSCHICHTIGER SICHERHEITSANSATZ

Der mehrschichtige Sicherheitsansatz von Kaspersky Lab ist einer der Gründe, warum wir zu den Marktführern im Markt zählen. Unsere Technologien werden intern bei Kaspersky Lab entwickelt. Aus diesen Grund greift jede unserer leistungsstarken und aufeinander abgestimmten Schutzschichten nahtlos ineinander und schont die Systemressourcen.

Jede dieser Schutzschichten geht die Cyberbedrohungen aus einer anderen Perspektive an. Dadurch ist es unseren IT-Experten möglich eng miteinander verzahnte Sicherheitstechnologien zu implementieren. Auf diese Weise entsteht ein Schutz, der sowohl in die Breite als auch in die Tiefe geht.

WELTWEIT FÜHRENDES SICHERHEITSWISSEN – IHR GARANT FÜR FORTLAUFENDEN SCHUTZ

Das globale Sicherheitswissen von Kaspersky Lab ist weltweit anerkannt und finden seine Anwendung in unseren Sicherheitslösungen, die darauf ausgelegt sind, sich einer ständig veränderten IT-Landschaft anzupassen.

FUNKTIONEN

HEURISTISCHE SICHERHEITSVERFAHREN SORGEN FÜR WENIGER BELASTUNG IHRER SYSTEME

Musterbasierte Malware-Identifizierungsverfahren garantieren höhere Erkennungsraten, ermöglichen kleinere Update-Dateien und sorgen für mehr Sicherheit.

VERHALTENSANALYSE

Anti-Malware von Kaspersky Lab arbeitet mit zwei bestimmten Komponenten für die Aktivitätsanalyse von Software:

- **Emulator** – Reproduziert und überprüft die beabsichtigten Aktivitäten eines Programms.
- **Aktivitätsmonitor** – Überwacht die Aktivitäten von bereits ausgeführten Programmen und erkennt und analysiert Verhaltensmuster, die charakteristisch für Malware sind.

CLOUD-BASIERTE MALWARE-ERKENNUNG DURCH DAS KASPERSKY SECURITY NETWORK (KSN)

Über 60 Millionen freiwillige Nutzer von Kaspersky-Software ermöglichen einen konstanten Strom von aktuellen Daten zu versuchten Malware-Angriffen und verdächtigem Verhalten. Diese Informationen ermöglichen Kaspersky Lab die umgehende Beurteilung verdächtiger Dateien. Auf diese diese Weise profitieren alle unsere Kunden von Echtzeitschutz und einer geringeren Anzahl von Fehlalarmen (False-Positives).

AUTOMATISCHER EXPLOIT-SCHUTZ

Der automatische Exploit-Schutz richtet sich insbesondere gegen Malware, die Schwachstellen in weit verbreiteten Programmen ausnutzt, indem typische oder verdächtige Verhaltensmuster analysiert werden. Einmal erkannt, erstickt die Technologie Exploits dann im Keim und hindert bereits heruntergeladenen Schadcode an der Ausführung.

SCHUTZ VOR VERSCHLÜSSELUNG DURCH RANSOMWARE

Für den Fall, dass verdächtige Prozesse versuchen sollten, auf wichtige Dateien zuzugreifen, hält der Aktivitätsmonitor Kopien davon im temporären Speicher vor. Sollte Ransomware den Versuch unternehmen, die Originale zu verschlüsseln, lassen sich die unverschlüsselten Kopien wiederherstellen.

ACTIVE DISINFECTION

Diese Technologie nutzt unterschiedliche Verfahren, um erkannte Infektionen zu „heilen“, z. B. durch die Verhinderung der Datei- und Prozessausführung inklusive Autostart, das Zerstören von Malware und das Zurücksetzen von gespeicherten Dateien in ihren Originalzustand.

HOSTBASIERTES SYSTEM ZUR ANGRIFFSÜBERWACHUNG (HOST-BASED INTRUSION PREVENTION SYSTEM, HIPS) UND PERSÖNLICHE FIREWALL

Einige Programmaktivitäten sind ausreichend risikobehaftet, um eine Einschränkung ratsam erscheinen zu lassen, auch wenn sie sich möglicherweise nicht als schädlich erweisen. Das hostbasierte System zur Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) von Kaspersky Lab schränkt Aktivitäten innerhalb eines Systems ein. Grundlage hierfür ist die dem jeweiligen Programm zugeordnete Vertrauensstufe. Unterstützt wird dieser Vorgang durch eine persönliche Firewall, welche die Netzwerkaktivität von Programmen einschränkt.

NETWORK ATTACK BLOCKER

Erkennt und überwacht verdächtige Aktivitäten in Ihrem Netzwerk und ermöglicht es Ihnen, die Reaktion Ihres Systems auf verdächtiges Verhalten festzulegen.

REGELMÄSSIGE UPDATES

Updates zum Schutz vor neuen Bedrohungen durch Malware werden durch den branchenweit schnellsten Aktualisierungszyklus in Ihre Sicherheitsdatenbank eingepflegt. Hinzu kommt die kontinuierliche Aktualisierung von Daten über neu entdeckte Malware aus der KSN-Cloud (Kaspersky Security Network).

PROFESSIONELLER SCHUTZ, MEHRFACH BEWIESEN – DIE FAKTEN

2014 haben die Produkte von Kaspersky Lab an **93 unabhängigen Tests und Bewertungen teilgenommen.** Unsere Produkte landeten **66 Mal unter den ersten Drei**, ein **TOP3-Ergebnis von 71 %**, und schnitten **51 Mal als Sieger** ab, also bei weitaus mehr als der Hälfte der Tests.

SICHERHEITSPRODUKTE, -LÖSUNGEN UND -SERVICES FÜR UNTERNEHMEN

Kaspersky Endpoint Security for Business

Wir nutzen unsere Expertise aus einer der besten Bedrohungsanalyse-Systeme der Welt und haben uns daher entschieden für Kaspersky Endpoint Security for Business einen mehrstufigen Sicherheitsansatz zu wählen. Dieser basiert auf einer einzigen, integrierten Plattform mit einer Vielzahl von Funktionen. Dazu gehören solide Tools für die Programm-, Geräte- und Web-Kontrolle, Datenverschlüsselung, Sicherheit für mobile Endpoints und Mobile Device Management (MDM) sowie Systems Management und Patch Management.

Alles wird über eine zentrale Konsole verwaltet – das Kaspersky Security Center.

Kaspersky Total Security for Business bietet zusätzlich Sicherheit für Mail-, Web- und Collaboration-Server, schützt Ihren Perimeter und sichert die gesamte IT-Infrastruktur Ihres Unternehmens ab.

Kaspersky Targeted Security-Lösungen

Eigenständige Lösungen, mit denen sich die Sicherheitstechnologien von Kaspersky Lab auf spezifische Bereiche Ihres IT-Systems anwenden lassen.

Einige dieser Lösungen, wie z. B. Kaspersky Security for Mobile sind im Lieferumfang von Kaspersky Endpoint Security for Business enthalten.

Andere wie Kaspersky Security for Virtualization sind ausschließlich als Targeted Solutions erhältlich.

Alle basieren jedoch auf denselben hochmodernen Technologien und profitieren von den Ergebnissen unserer Bedrohungsanalyse. Alle Sicherheitslösungen für physische, mobile und virtualisierte Endpoints werden zentral über das Kaspersky Security Center verwaltet.

Kaspersky Security Intelligence Services und Unternehmenslösungen

In diesem Bereich kommt unsere umfassende Bedrohungsanalyse, die technische Expertise und Schulungskompetenz von Kaspersky Lab zur Anwendung. All dies nutzen wir um Ihre Marke, Ihr Unternehmen und Ihre Mitarbeiter zu schützen.

Unternehmenslösungen gehen spezielle Probleme in bestimmten Branchen und Infrastrukturen an und schützen vor speziellen Angriffsarten wie z. B. DDoS-Attacken (Distributed Denial of Service).

KASPERSKY SMALL OFFICE SECURITY

Erstklassiger und einfacher Schutz für kleine Unternehmen.

MAINTENANCE-SERVICE-AGREEMENTS

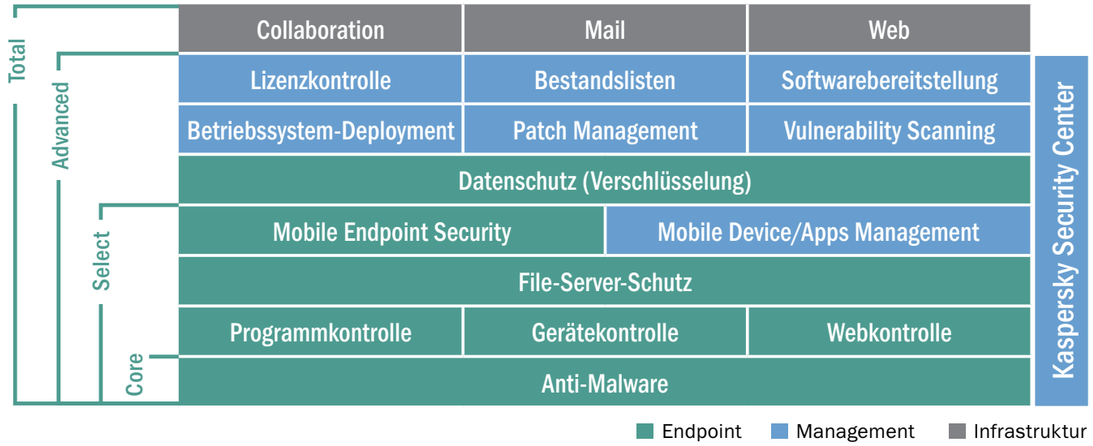
Eine Palette von Support-Optionen für Ihre Kaspersky-Sicherheitslösung.

ÜBER KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Endpoint Security for Business ist eine umfassende Sicherheitslösung, die von weltweit führenden Sicherheitsfachleuten entworfen wurde. Tiefgreifender, zukunftorientierter Schutz, hohe Effizienz und einfache Verwaltung bauen stufenweise aufeinander auf und bieten so umfassende Sicherheit für Ihr Unternehmen.

Sämtliche Komponenten wurden intern bei Kaspersky Lab entwickelt und zu einer einzigen Sicherheitsplattform integriert, die perfekt auf Ihre geschäftlichen Anforderungen zugeschnitten ist. Das Ergebnis ist eine stabile, integrierte Lösung ohne Lücken, ohne Kompatibilitätsprobleme und ohne zusätzlichen Workload, sollten Sie Ihre Sicherheitsanforderungen erweitern.

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 Lab kann Ihnen Ihre Arbeit erleichtern.

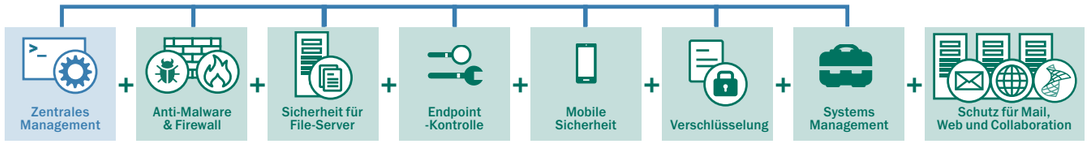


Kaspersky Lab kann mit einer umfassenden Liste von Technologien aufwarten, die alle auf der gleichen Codebasis fundieren und zusätzlich durch das cloud-basierte Kaspersky Security Network unterstützt werden, um Ihren Kunden den erstklassigen Schutz zu bieten, den sie benötigen.

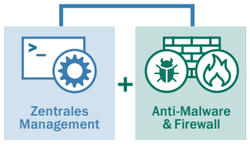
Fazit: Wir haben die erste Sicherheitsplattform der Branche bereitgestellt, die vom Kern aus aufgebaut wurde, sodass der Administrator Ihr Unternehmen sehen, kontrollieren und schützen kann.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Leistungsstarker, mehrstufiger Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen, entworfen und entwickelt von führenden IT-Sicherheitsexperten. Kaspersky Endpoint Security for Business und unsere weltweit anerkannte Bedrohungsanalyse sorgen zusammen für beispiellose IT-Sicherheit und -Kontrolle.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS – CORE



Erstklassiger Malware-Schutz, die Grundlage unserer Sicherheitsplattform

Die mehrstufigen Kaspersky-Schutztechnologien werden intern bei uns von Mitarbeitern entwickelt, denen das Thema Sicherheit sehr am Herzen liegt. Das in unabhängigen Tests immer wieder bestätigte Resultat ist die leistungsstärkste und effektivste Sicherheitslösung, die unsere Branche zu bieten hat – es gibt einfach keinen besseren Schutz für Ihr Unternehmen.

Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen – Ausgereifte Spezialtechnologien sorgen für die Identifizierung und Eliminierung von vorhandenen und neu aufkommenden Bedrohungen.

Automatischer Exploit-Schutz – Proaktive Identifizierung und Abwehr von unbekannten und hoch entwickelten Bedrohungen.

Cloud-basierter Schutz – Nutzt Echzeitinformationen aus dem weltweiten Kaspersky Security Network.

Aktivitätsmonitor – Bietet eine einzigartige Dateiwiederherstellungsfunktion, sollte das System einmal infiltriert werden.

Hostbasiertes System zur Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) mit persönlicher Firewall – HIPS schränkt die Aktivitäten je nach Vertrauensstufe eines Programms ein und arbeitet mit einer persönlichen Firewall zusammen, welche die Netzwerkaktivität einschränkt.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT

Wirkungsvolle, fein abgestufte Endpoint-Kontrollen in Kombination mit proaktiver Sicherheit und Verwaltung für mobile Geräte und die darauf gespeicherten Daten

Programm-, Web- und Gerätekontrollen inklusive dynamischem Whitelisting, die auf unserem einzigartigen internen Labor basieren, erweitern die umfassende Endpoint-Sicherheit von Kaspersky Lab um eine weitere Dimension. Unternehmenseigene und private Mobilgeräte der Mitarbeiter (BYOD) werden ebenfalls geschützt. Vorhandene Plattformen werden vereinheitlicht, damit sie zusammen mit allen geschützten Endpoints über eine zentrale Konsole, das Kaspersky Security Center, verwaltet werden können. Durch spezielle Schutzfunktionen für File-Server wird sichergestellt, dass Infektionen sich über gespeicherte Daten nicht auf die abgesicherten Endpoints ausbreiten können.

ENDPOINT-KONTROLLE

Programmkontrolle und dynamisches Whitelisting – Vom Kaspersky Security Network in Echtzeit bereitgestellte Dateireputationen ermöglichen es IT-Administratoren, die Ausführung von Programmen zuzulassen, zu blockieren oder einzuschränken. Hierzu gehören u. a. auch „Default Deny"-Whitelisting-Szenarien in Produktions- oder Testumgebungen. Application Privilege Control und Vulnerability Scanning überwachen Programme und schränken diejenigen ein, die auffälliges Verhalten zeigen.

Web-Kontrolle – Auf Grundlage vordefinierter oder anpassbarer Kategorien lassen sich Richtlinien für das Browsen festlegen, die einen umfassenden Überblick liefern und administrative Effizienz gewährleisten.

Gerätekontrolle – Es besteht die Möglichkeit, fein abgestufte Datenrichtlinien für den Anschluss von Wechseldatenträgern und anderen Peripheriegeräten festzulegen, zeitlich zu planen und durchzusetzen. Spezielle Masken ermöglichen das gleichzeitige Deployment auf einer Vielzahl von Geräten.

FILE-SERVER-SCHUTZ

Wird zusammen mit der Endpoint-Sicherheit über das Kaspersky Security Center verwaltet.

MOBILE SICHERHEIT

Wirkungsvoller Schutz für mobile Geräte – Hoch entwickelte, proaktive und Cloud-basierte Technologien ermöglichen zusammen einen mehrstufigen Echtzeitschutz für mobile Endpoints.

Web-Filter-, Spam-Schutz- und Phishing-Schutzkomponenten erhöhen die Gerätesicherheit zusätzlich.

Diebstahlschutz per Fernzugriff – Sperr-, Lösch-, Lokalisierungs- und Fahndungsfotofunktionen, SIM-Kontrolle sowie eine vollständige oder selektive Löschung verhindern im Zusammenspiel den unbefugten Zugriff auf Unternehmensdaten, falls ein Mobilgerät abhanden kommt oder gestohlen wird. Die Verfügbarkeit der Funktionen für Administratoren und Endbenutzer und die Unterstützung von Google Cloud Management ermöglichen bei Bedarf eine schnelle Aktivierung.

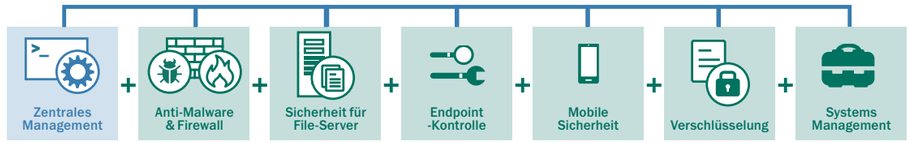
Mobile Application Management (MAM) – Es können nur freigegebene Programme von der Whitelist ausgeführt werden. Hierdurch wird der Einsatz unerwünschter oder unbekannter Software verhindert. Durch das so genannte „**Application Wrapping**" werden Unternehmensdaten auf den Privatgeräten von Mitarbeitern eingekapselt. Eine Verschlüsselung oder selektive Löschvorgänge lassen sich per Fernzugriff ausführen.

Mobile Device Management (MDM) – Eine einheitliche Benutzeroberfläche für **Microsoft®- Exchange ActiveSync-** und **iOS MDM**-Geräte mit OTA-Deployment (Over The Air) der Richtlinien. Geräte, die auf **Samsung KNOX** for Android™ basieren, werden ebenfalls unterstützt.

Self-Service-Portal – Erlaubt die eigenhändige Anmeldung von genehmigten Mitarbeitergeräten im Netzwerk bei gleichzeitiger Installation aller benötigten Zertifikate und Schlüssel sowie die Notfallaktivierung von Diebstahlschutz-Funktion durch den Benutzer/Eigentümer, wodurch sich der Verwaltungsaufwand für den IT-Administrator verringert.

Kaspersky Endpoint Security for Business – SELECT enthält außerdem alle Komponenten der Stufe „CORE".

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED



Systems-Management-Tools sorgen für optimale IT-Effizienz und -Sicherheit, während die integrierten Verschlüsselungsfunktionen vertrauliche Daten schützen

Automatisches Patch Management und die Verwaltung von Betriebssystem-Images, Remote-Softwarebereitstellung und SIEM-Integration tragen alle zu einer reibungslosen Administration bei, während Hard- und Softwarebestandslisten und Lizenzverwaltungsfunktionen für Transparenz und Kontrolle sorgen. Integrierte Verschlüsselungstechnologien sorgen für den effektiven Schutz Ihrer Daten.

SYSTEMS MANAGEMENT

Vulnerability Scanning und Patch Management – Automatische Erkennung und Einstufung von Schwachstellen in Betriebssystemen und Programmen in Kombination mit der raschen automatischen Verteilung von Patches und Updates.

Betriebssystem-Deployment – Einfaches Erstellen, Speichern und Deployment von so genannten „golden Images“ von Betriebssystemen sowie Funktionen für die Betriebssystem-Migration.

Softwarebereitstellung und Troubleshooting – Software-Deployment sowie bedarfs- oder zeitplangesteuerte Updates für Programme und Betriebssysteme inklusive Unterstützung von Wake-on-LAN-Technologie. Zeitsparendes Remote-Troubleshooting und effiziente Softwarebereitstellung durch Multicast-Technologie.

Hardware- und Software-Bestandslisten und Lizenzverwaltung – Identifizierung, Transparenz und Kontrolle (inklusive Blockierung) in Kombination mit Lizenznutzungsverwaltung ergibt vollständige Transparenz über sämtliche in Ihrer Umgebung eingesetzte Software und Hardware inklusive der Wechseldatenträger. Funktionen wie die Lizenzverwaltung für Software und Hardware, Erkennung von Gastgeräten, Kontrolle von Programmberechtigungen und Zugriffs-Provisioning sind ebenfalls verfügbar.

SIEM-Integration – Unterstützung von SIEM-Systemen wie IBM® QRadar- und HP ArcSight.

Rollenbasierte Zugriffskontrolle (RBAC) – In komplexen Netzwerken lassen sich die Aufgaben auf mehrere Administratoren verteilen, wobei die Konsolenansichten auf die verschiedenen Rollen und Berechtigungen zugeschnitten werden können

VERSCHLÜSSELUNG

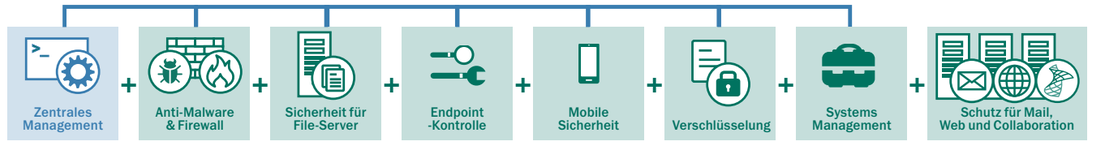
Effektiver Schutz von Daten – Auf Endpoints kann mit Datei-/Ordnerverschlüsselung (FLE) oder Full-Disk-Verschlüsselung (FDE) gearbeitet werden. Ein „portable Modus“ ermöglicht eine domänenübergreifende Verschlüsselungsverwaltung.

Flexible Benutzeranmeldung – Pre-Boot-Authentifizierung (PBA) für zusätzliche Sicherheit mit optionaler „einmalige Anmeldung“ für Benutzertransparenz. 2-Faktor- bzw. Token-basierte Authentifizierung sind ebenfalls möglich.

Erstellen integrierter Richtlinien – Einzigartige Integration der Verschlüsselung in Programm- und Gerätekontrollen sorgt für eine zusätzliche, hocheffektive Schutzschicht und vereinfacht die Verwaltung

Kaspersky Endpoint Security for Business – ADVANCED enthält außerdem alle Komponenten der Stufen „SELECT“ und „CORE“.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Unternehmen, die umfassenden Schutz für ihre gesamte IT-Umgebung benötigen, entscheiden sich für Kaspersky Total Security for Business

Kaspersky Total Security for Business stellt derzeit branchenweit die umfassendste Plattform für Endpoint-Schutz und -Verwaltung dar. Kaspersky Total Security for Business sichert jede Ebene des Netzwerks ab und umfasst leistungsstarke Konfigurationstools, welche die Produktivität der Benutzer und ihren Schutz vor Malware sicherstellen – egal mit welchem Gerät und an welchem Standort.

MAIL-SERVER-SCHUTZ

Effektiver Schutz vor E-Mail-basierten Malware-Bedrohungen, Phishing-Angriffen und Spam dank Echtzeit-Updates aus der Cloud – für unübertroffene Abfangraten und minimale Fehlalarme (False-Positives). Malware-Schutz für IBM® Domino® ist ebenfalls enthalten. DLP-Funktionen für Microsoft Exchange sind separat erhältlich.

INTERNET-GATEWAY-SCHUTZ

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

COLLABORATION-SICHERHEIT

Schützt SharePoint®-Server und -Serverfarmen vor allen Arten von Malware. Die separat erhältliche DLP-Funktion für Sharepoint bietet Inhalts- und Dateifilterfunktionen, um vertrauliche Daten automatisch zu identifizieren und Datenlecks zu verhindern.

Kaspersky Total Security for Business enthält außerdem alle Komponenten der Stufen „ADVANCED“, „SELECT“ und „CORE“.

PRODUKTMERKMALE

Welche Lösung ist die richtige für Sie?

	Core	Select	Advanced	Total	Verwaltung über Security Center	Als Targeted Solution verfügbar
Anti-Malware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Programmkontrolle		•	•	•	•	
Gerätekontrolle		•	•	•	•	
Webkontrolle		•	•	•	•	
File-Server-Schutz		•	•	•	•	•
Schutz für mobile Endpoints		•	•	•	•	•
Mobile Device Management/Apps Management		•	•	•	•	•
Verschlüsselung			•	•	•	
Vulnerability Scanning			•	•	•	•
Patch Management			•	•	•	•
Bestandslisten			•	•	•	•
Lizenzkontrolle			•	•	•	•
Softwarebereitstellung			•	•	•	•
Deployment von Betriebssystemen			•	•	•	•
Sicherheit für Collaboration-Server				•		•
Mail-Server-Schutz				•	•	•
Internet-Gateway-Sicherheit				•		•
Sicherheit der virtualisierten Infrastruktur					•	•
Sicherheit für Storage-Server					•	•

• Enthalten • Teilweise enthalten (genaue Angaben finden Sie in der Produktbeschreibung)

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server bietet kosteneffektiven, zuverlässigen und skalierbaren Schutz für freigegebenen Dateispeicher, der gleichzeitig die Systemressourcen schont.

WICHTIGSTE VORTEILE

LEISTUNGSSTARKER MALWARE-SCHUTZ
Die vielfach ausgezeichnete Anti-Malware-Engine von Kaspersky Lab bietet leistungsstarken Schutz auch vor neuester potentieller Malware, die über schädliche oder gefährliche Programme in das lokale Netzwerk eindringen kann.

HOHE LEISTUNG UND ZUVERLÄSSIGKEIT
Kaspersky Security for File Server führt auch bei hoher Netzwerklast nicht zur Beeinträchtigung der Systemleistung oder der normalen Geschäftsabläufe.

UMFASSENDE PLATTFORMUNTERSTÜTZUNG
Eine einzelne, effektive und umfassend kompatible Sicherheitslösung für heterogene Servernetzwerke mit Unterstützung der neuesten Plattformen und Server einschließlich Terminal-, Cluster- und virtualisierter Server.

EFFEKTIVES MANAGEMENT UND REPORTING
Effektive, benutzerfreundliche Management-Tools, Informationen über den Server-Schutzstatus, flexible Zeiteinstellungen für Scans und ein umfassendes Reporting-System bieten eine effiziente Kontrolle über die File-Server-Sicherheit und reduzieren damit letztlich die Gesamtbetriebskosten.

FUNKTIONEN

- **Echtzeit-Malware-Schutz** für File-Server mit den neuesten Versionen von Windows® (einschl. Windows Server® 2012/R2), Linux® und FreeBSD (jeweils mit Samba).
- **Schutz von Citrix- und Microsoft®-Terminalservern.**
- **Vollständige Unterstützung für Cluster-Server.**
- **Skalierbarkeit** – Problemlose Absicherung selbst für hochkomplexe, heterogene Infrastrukturen
- **Zuverlässigkeit, Stabilität und hohe Fehlertoleranz.**
- **Optimierte, intelligent Scan-Technologie**: inklusive bedarfsabhängigen Scans und Überprüfungen wichtiger Systembereiche
- **Vertrauenswürdige Bereiche**: erhöhen die Sicherheit und reduzieren die Ressourcenbelastung bei Scan-Vorgängen
- **Quarantäne und Backup** von Daten vor deren Desinfektion und Löschung
- **Isolierung** infizierter Workstations
- **Zentrale Installation, Verwaltung und Aktualisierung** mit flexiblen Konfigurationsoptionen.
- **Flexible Vorfallreaktionsszenarien.**
- **Umfassendes Reporting** zum Netzwerkschutzstatus.
- **Benachrichtigungssystem für Programmstatus.**
- **Unterstützung von Hierarchical-Storage-Management**-Systemen (HMS)
- **Unterstützung für Hyper-V und Xen Desktop.**
- **VMware-kompatibel.**
- **Unterstützung für ReFS.**

Kaspersky Security for File Server ist in Kaspersky Endpoint Security for Business – SELECT und ADVANCED sowie in Kaspersky Total Security for Business enthalten. Es ist auch separat als Targeted Solution erhältlich.

INFORMATIONEN ZU UNSERER ENDPOINT-KONTROLLTECHNOLOGIE

Leistungsstarke Endpoint-Kontroll-Tools, die nahtlos mit wegweisendem Malware-Schutz integriert sind, und das branchenweit einzige Whitelisting-Labor schützen Ihr Unternehmen vor der Dynamik der heutigen Bedrohungslage.

SCHUTZ, RICHTLINIENDURCHSETZUNG UND KONTROLLE

- Schwachstellen in vertrauenswürdigen Programmen, Web-basierte Malware und eine mangelnde Kontrolle über Peripheriegeräte sind nur einige Aspekte einer immer komplexer werdenden Bedrohungslage. Unsere Tools für die Programm-, Web- und Gerätekontrolle geben Ihnen die vollständige Kontrolle über Ihre Endpoints, ohne dabei die Produktivität zu beeinträchtigen.

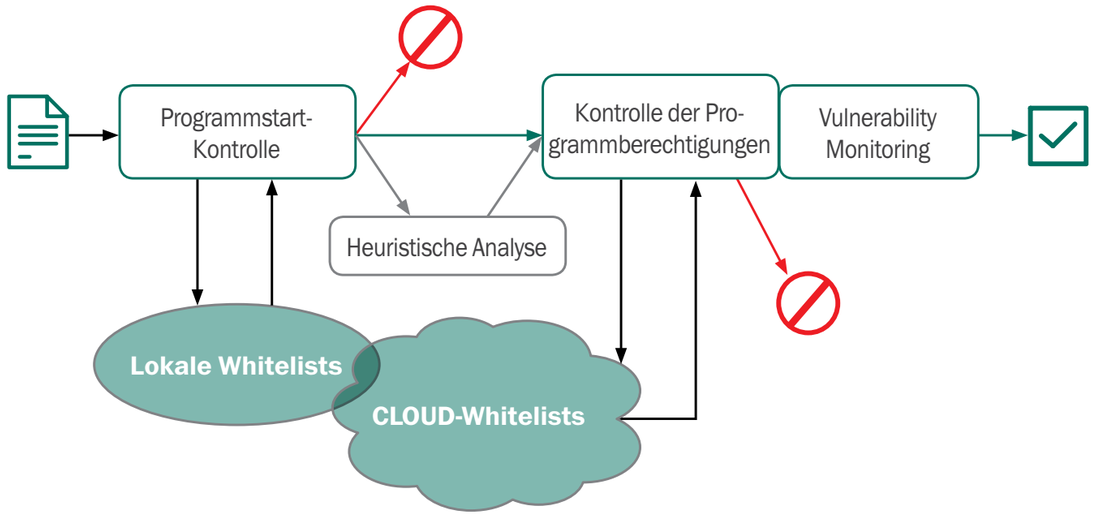
PROGRAMMKONTROLLE UND DYNAMISCHE WHITELISTS

Schützt Systeme vor bekannten und unbekannten Bedrohungen, da Administratoren unabhängig vom Verhalten der Endbenutzer die vollständige Kontrolle über die Programme haben, die auf den Endpoints ausgeführt werden können. Durch die Überwachung der Programmintegrität können Sie außerdem das Programmverhalten analysieren und die Ausführung unerwarteter Aktionen verhindern, durch die Endpoints oder das gesamte Netzwerk gefährdet werden könnten. Eine vereinfachte, individuell anpassbare oder automatische Erstellung und Durchsetzung von Richtlinien hat folgende Vorteile:

- **Kontrolle des Programmstarts**: Zum Zulassen, Blockieren und Prüfen von Programmstarts. Ermöglicht Produktivitätssteigerungen durch Zugriffsbeschränkungen für nicht unternehmensrelevante Programme.
- **Application Privilege Control**: Regulieren und kontrollieren Sie den Zugriff von Programmen auf Systemressourcen und Daten. Klassifizieren Sie Programme als vertrauenswürdig, eingeschränkt vertrauenswürdig oder nicht vertrauenswürdig. Regulieren Sie den Zugriff durch Programme auf verschlüsselte Daten auf Endpoints, z. B. Informationen, die über Webbrowser oder per Skype gepostet werden.
- **Vulnerability Scanning von Programmen**: Proaktive Verteidigung gegen Angriffe auf Schwachstellen in vertrauenswürdigen Programmen.

Die meisten Kontrolllösungen bieten lediglich einfache Funktionen für Blockierung und Zugriff. Die Kontroll-Tools von Kaspersky Lab sind die einzigen Tools, die auf Cloud-basierte Whitelisting-Datenbanken zugreifen und so Zugriff auf aktuelle Programminformationen praktisch in Echtzeit ermöglichen.

Unsere Programmkontroll-Technologien nutzen Cloud-basierte Whitelisting-Datenbanken zur Analyse und Überwachung von Programmen in allen Phasen: Download, Installation, Ausführung.



Dynamisches Whitelisting, das über eine lückenlose „Default Deny"-Richtlinie aktiviert werden kann, blockiert die Ausführung von Programmen auf allen Workstations außer ein Administrator gibt hierfür die explizite Erlaubnis. Kaspersky Lab ist der einzige IT-Sicherheitsanbieter mit einem eigenen Whitelisting-Labor, das eine laufend aktualisierte Datenbank mit mehr als 500 Millionen Programmen pflegt.

Unsere **Default Deny-Richtlinie kann in einer Testumgebung angewendet werden**, sodass der zuständige Administrator die Legitimität eines Programms überprüfen kann, bevor es blockiert wird. Außerdem lassen sich Programmkategorien auf Basis von digitalen Signaturen erstellen. Auf diese Weise wird der Benutzer daran gehindert, legitime Software zu nutzen, die von Malware modifiziert wurde oder aus einer verdächtigen Quelle stammt.

EINFACHE VERWALTUNG

Alle Kontroll-Tools von Kaspersky Lab lassen sich in Active Directory integrieren. Entsprechend einfach und schnell können globale Richtlinien konfiguriert und umgesetzt werden. Alle Endpoint-Kontrollen werden über dieselbe Konsole und Benutzeroberfläche verwaltet.

WEB-KONTROLLEN

Überwachen, filtern und kontrollieren Sie die Webseiten, auf die Endbenutzer am Arbeitsplatz Zugriff haben. Hierdurch steigern Sie die Produktivität und sorgen gleichzeitig für Schutz vor Web-basierter Malware und Attacken.

Unsere hochmodernen Web-Kontrollen basieren auf einem laufend aktualisierten Verzeichnis von Webseiten, das in verschiedene Kategorien unterteilt ist (z. B. Inhalte für Erwachsene, Gaming, Soziale Netzwerke, Glücksspiel). Dank einfach anzulegender Richtlinien können Administratoren den Zugriff von Endbenutzern auf einzelne Webseiten bzw. Webseitenkategorien untersagen, einschränken und überwachen und darüber hinaus eigene Listen erstellen. Schädliche Webseiten werden automatisch blockiert.

Durch Einschränkung ihrer Nutzung tragen unsere Web-Kontrollen dazu bei, die Weitergabe von Daten über Soziale Netzwerke und Instant-Messaging-Dienste zu verhindern. Flexible Richtlinien geben Administratoren die Möglichkeit, das Surfen im Internet auf bestimmte Tageszeiten zu beschränken. Die Integration mit Active Directory hat den Vorteil, dass sich die Richtlinien schnell und einfach im gesamten Unternehmen anwenden lassen.

Für noch mehr Sicherheit sorgt die Tatsache, dass die Web-Kontrollen direkt auf dem Endpoint aktiviert werden, d. h die Richtlinien werden durchgesetzt, selbst wenn der Benutzer nicht im Netzwerk angemeldet ist.

GERÄTEKONTROLLEN

Das Deaktivieren eines USB-Ports behebt nicht immer die Probleme mit Wechseldatenträgern. Wenn Sie z. B. einen USB-Port deaktivieren, verhindern Sie gleichzeitig den sicheren Zugang per VPN-Token über diesen Port.

Die Gerätekontrollen von Kaspersky Lab bieten eine noch feiner abgestufte Kontrolle auf Bus-, Typ- oder Geräteebene und erhalten so bei optimaler Sicherheit die Produktivität des Endbenutzers. Die Kontrollen lassen sich sogar auf einzelne Seriennummern von Geräten anwenden.

- Legen Sie Verbindungs-/Lese-/Schreibberechtigungen für einzelne Geräte fest, und erstellen Sie Zeitpläne.
- Erstellen Sie Gerätekontrollregeln auf Grundlage von Masken, damit Geräte nicht mehr angeschlossen werden müssen, um sie in die Whitelist aufzunehmen. Nehmen Sie mehrere Geräte gleichzeitig in die Whitelist auf.
- Kontrollieren Sie den Datenaustausch per Wechseldatenträger innerhalb und außerhalb des Unternehmens, und reduzieren Sie so das Risiko von Datenverlust und -diebstahl.
- Integrieren Sie die Kontroll-Tools mit unseren Verschlüsselungstechnologien, um Verschlüsselungsrichtlinien auf bestimmten Gerätetypen durchzusetzen.

Die Endpoint-Kontrolltechnologie ist in Kaspersky Endpoint Security for Business – SELECT und ADVANCED und in Kaspersky Total Security for Business enthalten.

KASPERSKY SECURITY FOR MOBILE

Mobile Geräte werden auch für Cyberkriminelle immer interessanter. Beruflich genutzte Mobilgeräte von Mitarbeitern (BYOD) sind der Grund für einen immer komplexer werdenden Gerätemix und schaffen so eine höchst anspruchsvolle Management- und Kontrollsituation für IT-Administratoren.

Mit Kaspersky Security for Mobile haben Sie die Gewissheit, dass Ihr Gerät gut geschützt ist, egal wo es sich gerade befindet. Sorgen Sie für Schutz vor sich ständig weiterentwickelnder mobiler Malware. Schaffen Sie sich schnell und problemlos einen Überblick über die Smartphones und Tablets innerhalb Ihrer Umgebung – von einer zentralen Konsole aus, bei minimaler Beeinträchtigung.

WICHTIGE PRODUKTFUNKTIONEN

- **Leistungsstarker Malware-Schutz**
- **Phishing- und Spam-Schutz**
- **Web-Schutz**
- **Programmkontrolle**
- **Erkennung von „Rooting“ und „Jailbreak“**
- **Containerisierung**
- **Diebstahlschutz**
- **Mobile Device Management**
- **Self-Service-Portal**
- **Zentralisierte Verwaltung**
- **Web Console**
- **Unterstützte Plattformen:**
  - **Android™**
  - **iOS**
  - **Windows® Phone**

WICHTIGSTE VORTEILE

WEGWEISENDER MALWARE-SCHUTZ FÜR MOBILGERÄTE UND DATEN
Allein im Jahr 2014 musste sich Kaspersky Lab mit fast 1,4 Millionen neuen Attacken durch mobile Malware auseinandersetzen. Kaspersky Security for Mobile kombiniert Malware-Schutz mit tiefgreifender Sicherheit, die Daten auf mobilen Geräten vor bekannten und unbekannten Bedrohungen schützt.

MOBILE DEVICE MANAGEMENT (MDM)
Integration mit allen führenden Mobile Device Management-Plattformen ermöglicht OTA-Deployments (Over the Air) und -Kontrolle per Fernzugriff und erleichtert so Bedienbarkeit und Verwaltung von Android-, iOS- und Windows Phone-Geräten.

MOBILE APPLICATION MANAGEMENT (MAM)
Containerisierung und selektive Löschung ermöglichen die Trennung von geschäftlichen und privaten Daten auf demselben Gerät und unterstützen so Ihre BYOD-Initiativen. Im Zusammenspiel mit unseren Verschlüsselungs- und Malware-Schutzfunktionen wird aus Kaspersky Security for Mobile so eine proaktive Lösung zum Schutz von Mobilgeräten – im Gegensatz zu anderen Ansätzen, die Geräte und Daten einfach nur isolieren.

ZENTRALISIERTE VERWALTUNG
Verwalten Sie eine Vielzahl von Plattformen und Geräten von derselben Konsole aus wie andere Endpoints, und erhöhen Sie so Transparenz und Kontrolle ohne zusätzlichen Aufwand oder Technologien.

SICHERHEIT UND VERWALTUNG MOBILER GERÄTE – FUNKTIONEN

LEISTUNGSSTARKER MALWARE-SCHUTZ
Proaktiver, Signatur- und Cloud-basierter Schutz (über das Kaspersky Security Network, KSN) vor bekannten und unbekannten Bedrohungen durch mobile Malware. Bedarfsabhängige oder zeitplangesteuerte Scans und automatische Updates sorgen für noch mehr Schutz.

PHISHING- UND SPAM-SCHUTZ
Leistungsstarke Technologien für Phishing- und Spam-Schutz schützen Geräte und Daten vor Phishing-Angriffen und ermöglichen die Blockierung unerwünschter Anrufe und SMS-Nachrichten.

WEB-KONTROLLE/FUNKTION „SICHERER BROWSER“
Unterstützt durch das Kaspersky Security Network (KSN) blockieren diese Technologien den Zugriff auf schädliche und nicht-autorisierte Webseiten. Die Funktion „Sicherer Browser“ bietet eine stets aktuelle Reputationsanalyse und sorgt so für eine sichere Internetnutzung auf mobilen Geräten.

PROGRAMMKONTROLLE
Die mit KSN integrierten Programmkontrollen beschränken die Programmnutzung auf genehmigte Anwendungen und verhindern so die Verwendung unsicherer oder nicht genehmigter Software. Machen Sie die Funktionalität des Geräts von den dort installierten Programmen abhängig. Durch die Überwachung des Inaktivitätszeitraums von Programmen kann eine erneute Anmeldung durch den Benutzer erzwungen werden, falls für einen vorgegebenen Zeitraum keine Benutzereingabe erfolgt ist. Auf diese Weise sind die Daten geschützt, selbst wenn ein Programm geöffnet ist und das Gerät abhanden kommt oder gestohlen wird.

ERKENNUNG VON „ROOTING“ UND „JAILBREAK“
Die automatische Erkennung von und das Reporting über „Rooting“- und „Jailbreak“-Versuche lässt sich mit einer automatischen Zugriffssperre für Container bzw. einer selektiven oder vollständigen Löschung der Gerätedaten kombinieren.

CONTAINERISIERUNG
Trennung von geschäftlichen und persönlichen Daten durch Kapselung von Programmen in Containern. Zusätzliche Richtlinien, z. B. für die Verschlüsselung, können zum Schutz vertraulicher Daten angewendet werden. Durch selektives Löschen können die Containerdaten auf einem Gerät gezielt gelöscht werden, ohne dabei die persönlichen Daten des Mitarbeiters zu beeinträchtigen.

DIEBSTAHLSCHUTZ
Per Fernzugriff steuerbare Diebstahlschutz-Funktionen wie Löschen, Gerätesperre, Ortung, SIM-Kontrolle, „Fahndungsfoto“ und Alarm können bei Verlust oder Diebstahl des Geräts ausgelöst werden. Die Diebstahlschutz-Befehle können äußerst flexibel eingesetzt werden. Durch die Integration mit Google Cloud Messaging (GCM) können die Funktionen beispielsweise fast umgehend eingesetzt werden, wodurch sich die Reaktionszeiten verkürzen und die Sicherheit steigern lässt, während die Nutzung des Self-Service-Portals zur Bedienung der Diebstahlschutz-Funktionen den Administrator entlastet.

MOBILE DEVICE MANAGEMENT (MDM)
Unterstützung von Microsoft® Exchange ActiveSync, Apple MDM und Samsung KNOX 2.0 ermöglicht die Nutzung unterschiedlichster Richtlinien über eine einzige, plattformunabhängige Benutzeroberfläche. Durchsetzen von Verschlüsselung und Kennwörtern oder Steuerung der Kameranutzung, Richtlinienanwendung für einzelne Benutzer oder Benutzergruppen, Verwalten von APN/VPN-Einstellungen, um nur einige Beispiele zu nennen.

SELF-SERVICE-PORTAL
Überlassen Sie routinemäßige Sicherheitsabläufe Ihren Mitarbeitern, und ermöglichen Sie eine eigenhändige Anmeldung von genehmigten Geräten. Während der Aktivierung neuer Geräte können alle erforderlichen Zertifikate automatisch über das Portal bereitgestellt werden, ohne dass sich ein Administrator damit befassen muss. Im Fall eines Geräteverlusts kann der Eigentümer alle verfügbaren Diebstahlschutz-Funktionen über das Portal aktivieren.

ZENTRALISIERTE VERWALTUNG
Zentrale Verwaltung aller Mobilgeräte von einer einzigen Konsole aus, über die auch die IT-Sicherheit aller anderen Endpoints kontrolliert wird. Unsere Webkonsole gibt Ihren Administratoren die Möglichkeit, Geräte per Fernzugriff von jedem beliebigen Computer aus zu kontrollieren und zu verwalten.

Kaspersky Security for Mobile ist in Kaspersky Endpoint Security for Business – SELECT und ADVANCED sowie in Kaspersky Total Security for Business enthalten. Es ist auch separat als Targeted Solution erhältlich.

INFORMATIONEN ZU UNSERER VERSCHLÜSSELUNGSTECHNOLOGIE

Verhindern Sie den unbefugten Zugriff auf Daten durch Geräteverlust, Diebstahl oder Daten entwendende Malware.

Proaktiver Schutz von Daten und Compliance sind eine zwingende Notwendigkeit. Die Verschlüsselungstechnologie von Kaspersky Lab schützt wertvolle Daten vor ungewolltem Verlust, bei Diebstahl oder gezielten Malware-Attacken. Durch die Kombination von leistungsstarken Verschlüsselungstechnologien mit unseren branchenführenden Technologien für die Sicherheit auf Endpoints, sorgt unsere integrierte Plattform für den Schutz von Daten, die gerade übertragen oder nicht genutzt werden.

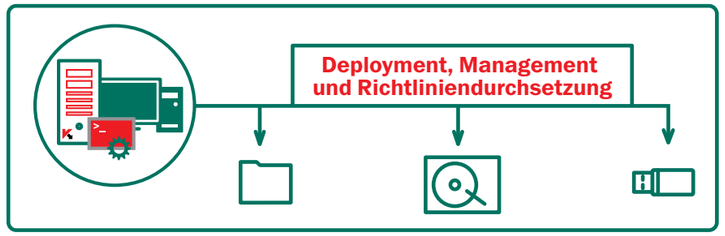
Da die Lösung von Kaspersky Lab stammt, kann sie leicht über eine zentralisierte Verwaltungskonsole mithilfe einer einzigen Richtlinie bereitgestellt und verwaltet werden.

Unsere Verschlüsselungstechnologien verhindern Datenverluste und unbefugten Zugriff auf Daten:
- **Full-Disk-Verschlüsselung (FDE)**
- **Folder-Level-Verschlüsselung (FLE)**
- **Wechseldatenträger/interne Geräte**

VERWALTUNG ÜBER EINE EINZIGE VERWALTUNGSKONSOLE

SICHERE KRYPTOGRAPHIE NACH BRANCHENSTANDARD
Kaspersky Lab nutzt den Advanced Encryption Standard (AES) mit 256-Bit-Schlüssellänge, vereinfachter Schlüsselverwaltung und sicherer Aufbewahrung. Unterstützt Intel® AES-NI-Technologie, UEFI- und GPT-Plattformen.

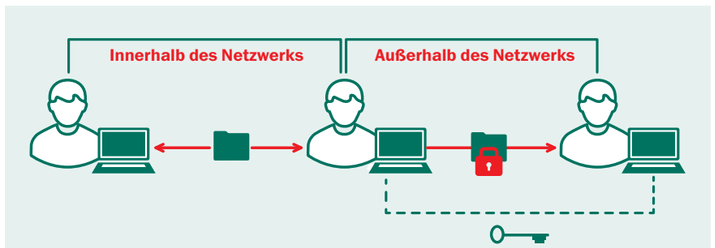
UMFASSENDE FLEXIBILITÄT
Kaspersky Lab bietet Datei- und Folder-Level-Verschlüsselung sowie vollständige Full-Disk-Verschlüsselung, um alle möglichen Anwendungsszenarien abzudecken. Es können sowohl Daten auf Festplatten als auch auf Wechseldatenträgern geschützt werden. Im „portablen Modus“ können die Daten auf verschlüsselten Wechseldatenträgern geschützt werden, selbst wenn auf dem Computer keine



Verschlüsselungssoftware installiert ist. Dies ermöglicht einen sicheren Datenaustausch auch außerhalb des „geschützten Perimeters“.

EINMALIGE ANMELDUNG, TRANSPARENZ FÜR ENDBENUTZER
Von der Konfiguration bis hin zur täglichen Nutzung lässt sich unsere Verschlüsselungstechnolgie transparent für alle Arten von Programmen einsetzen, ohne die Produktivität von Endbenutzern zu beeinträchtigen. Einmalige Anmeldung sorgt für nahtlose Verschlüsselung. Der Endbenutzer merkt möglicherweise gar nicht, dass die Technologie im Hintergrund läuft.

Verschlüsselungstechnologien von Kaspersky Lab ermöglichen einen nahtlosen, transparenten Datenaustausch zwischen Benutzern innerhalb und außerhalb des Netzwerks.



VERSCHLÜSSELUNGSFUNKTIONEN

NAHTLOSE INTEGRATION MIT SICHERHEITSTECHNOLOGIEN VON KASPERSKY LAB
Lückenlose Integration mit unserem Malware-Schutz und unseren Technologien für Endpoint-Kontrolle und -Schutz für echte mehrstufige Sicherheit, die auf einer gemeinsamen Codebasis aufbaut. Mit nur einer einzigen Richtlinie lässt sich beispielsweise die Verschlüsselung auf bestimmten Wechseldatenträgern durchsetzen. Wenden Sie Verschlüsselungseinstellungen im Rahmen derselben Richtlinie an, die auch für den Malware-Schutz, die Gerätekontrolle und andere Aspekte der Endpoint-Sicherheit eingesetzt wird. Keine Notwendigkeit, verschiedene Lösungen bereitzustellen und zu verwalten. Die Kompatibilität der Netzwerkhardware wird automatisch überprüft, bevor die Verschlüsselung eingesetzt wird; Unterstützung für UEFI- und GPT-Plattformen ist Standard.

ROLLENBASIERTE ZUGRIFFSKONTROLLE
In größeren Unternehmen kann die Verschlüsselungsverwaltung mithilfe der rollenbasierten Zugriffskontrolle delegiert werden. Auf diese Weise lässt sich die Verschlüsselungsverwaltung einfacher und weniger aufwendig gestalten.

PRE-BOOT-AUTHENTIFIZIERUNG (PBA)
Noch bevor das Betriebssystem hochfährt, müssen Anmeldeinformationen eingegeben werden. Dies bedeutet eine zusätzliche Sicherheitsstufe, wobei eine einmalige Anmeldung optional möglich ist. Unsere PBA-Verschlüsselungstechnologie ist für Nicht-QWERTY-Tastaturen erhältlich.

AUTHENTIFIZERUNG PER SMART-CARD UND TOKEN
Die Zwei-Faktor-Authentifizierung über gängige Smartcard-Modelle und Token erübrigt die Eingabe von Anmeldeinformationen und gestaltet die Benutzererfahrung so noch angenehmer.

NOTFALLWIEDERHERSTELLUNG
Der Administrator kann im Fall eines Hardware- oder Softwarefehlers Daten verschlüsseln. Die Wiederherstellung von Benutzerkennwörtern für PBA und der Zugriff auf verschlüsselte Daten sind über einen einfachen Challenge-/Response-Mechanismus möglich.

OPTIMIIERTES DEPLOYMENT, ANPASSBARE EINSTELLUNGEN
Für ein bequemes Deployment ist die Verschlüsselungsfunktion bei Kaspersky Endpoint Security for Business nur in den Stufen „Advanced“ und „Total“ aktiviert. Eine separate Installation ist nicht erforderlich. Verschlüsselungseinstellungen werden für häufig verwendete Ordner wie „Meine Dokumente“ und „Desktop“, neue Ordner, Dateinamenerweiterungen und Gruppen (z. B. Microsoft® Office-Dokumente oder Nachrichtenarchive) vordefiniert, können jedoch angepasst werden.

Die Verschlüsselung gehört bei Kaspersky Endpoint Security for Business – ADVANCED und Kaspersky Total Security for Business zum Funktionsumfang.

KASPERSKY SYSTEMS MANAGEMENT

Mehr Sicherheit, weniger Komplexität durch zentrale IT-Verwaltungstools.

Nicht gepatchte Schwachstellen in gängigen Programmen sind eine der größten Bedrohungen für die IT-Sicherheit in Unternehmen. Dieses Risiko wird durch die zunehmende Komplexität von IT-Umgebungen noch verschärft. Wenn Sie nicht wissen, welche Komponenten überhaupt vorhanden sind, wie sollen Sie diese dann schützen?

Durch Zentralisierung und Automatisierung von grundlegenden Sicherheits-, Konfigurations- und Verwaltungsabläufen, z. B. Vulnerability Assessment, Patch- und Update-Bereitstellung, Bestandsverwaltung und Anwendungs-Rollouts, sparen IT-Administration nicht nur Zeit, sie tragen auch zur Optimierung der Sicherheit bei.

Kaspersky Systems Management trägt zur Minimierung von IT-Sicherheitsrisiken bei und reduziert die Komplexität in der IT, da nun eine umfassende Echtzeit-Kontrolle und -Transparenz über mehrere Geräte, Programme und Benutzer über eine einzige Benutzeroberfläche möglich ist.

WICHTIGE PRODUKTFUNKTIONEN

- **Vulnerability Assessment und Patch Management**
- **Hardware- und Software-Bestandslisten**
- **Softwareinstallation und Troubleshooting per Fernzugriff auch in Zweigstellen**
- **Deployment von Betriebssystemen**
- **SIEM-Integration**
- **Rollenbasierte Zugriffskontrolle**
- **Zentralisierte Verwaltung**

VERBESSERTE SICHERHEIT
Verbesserte IT-Sicherheit und Reduzierung der Belastung durch Routineabläufe durch zeitnahe, automatisierte Patching- und Update-Funktionen. Automatische Erkennung und Priorisierung von Schwachstellen ermöglicht mehr Effizienz und reduziert die Ressourcenbelastung. Unabhängige Tests[1] beweisen, dass Kaspersky Lab die umfassendste und schnellste automatisierte Patch- und Update-Bereitstellung zu bieten hat.

KONTROLLE UND VOLLSTÄNDIGE TRANSPARENZ
Vollständige Netzwerktransparenz von einer einzigen Verwaltungskonsole beendet das Rätselraten für Administratoren: Alle Geräte und Programme (inklusive Gastgeräte), die sich im Netzwerk anmelden, werden erkannt. Dies ermöglicht eine zentrale Kontrolle des Benutzer- und Gerätezugriffs auf geschäftliche Daten und Programme auf Grundlage von IT-Richtlinien.

ZENTRALE VERWALTUNG
Kaspersky Systems Management ist eine verwaltete Komponente von Kaspersky Security Center. Zur Automatisierung von IT-Routineaufgaben wird jede Funktion über diese zentrale Konsole unter Verwendung einheitlicher, intuitiver Befehle und Benutzeroberflächen verwaltet.

1, 2 Von Kaspersky Lab in Auftrag gegebener und von der AV-TEST GmbH ausgeführter Test von Patch-Management-Lösungen (Juli 2013)

FUNKTIONEN

VULNERABILITY SCANNING UND PATCH MANAGEMENT
Automatisierte Software-Scans ermöglichen eine rasche Erkennung, Priorisierung und Behebung von Schwachstellen. Patches und Updates werden automatisch innerhalb kürzester Zeit[2] für Software von Microsoft® und anderen Herstellern bereitgestellt. Der Administrator wird über den Status der Patch-Installation informiert. Weniger wichtige Problemlösungen können auf Zeiten nach Geschäftsschluss verschoben werden. Durch Wake-on-LAN-Befehle funktioniert dies sogar bei ausgeschalteten Computern. Die Multicast-Übermittlungstechnik ermöglicht die lokale Bereitstellung von Patches und Updates in Zweigstellen und reduziert so die Bandbreitenanforderungen.

HARDWARE- UND SOFTWARE-BESTANDSLISTEN
Automatische Erkennung, Bestandsaufnahme, Benachrichtigung und Nachverfolgung von Hard- und Software, inklusive Wechseldatenträgern, geben Administratoren einen detaillierten Einblick in die im Unternehmensnetzwerk verwendeten Geräte und Ressourcen. Auch Gastgeräte werden erkannt und erhalten nach Wunsch Internetzugriff. Die Lizenzkontrolle liefert einen Überblick über die Anzahl der Netzwerk-Nodes und die Ablaufdaten.

FLEXIBLES PROVISIONING VON BETRIEBSSYSTEM UND PROGRAMMEN
Zentrales und einfaches Erstellen, Speichern, Klonen und Deployment von optimal geschützten System-Images. Deployment nach Büroschluss per Wake-on-LAN inklusive Bearbeitung nach der Installation für mehr Flexibilität. UEFI-Unterstützung

SOFTWAREBEREITSTELLUNG
Deployment/Updates über eine einzige Konsole. Über 100 weit verbreitete, vom Kaspersky Security Network identifizierte Programme können nach Wunsch nach Büroschluss installiert werden. Vollständige Unterstützung für Remote-Troubleshooting inklusive erweiterten Sicherheitsfunktionen mit Benutzerberechtigungen und Sitzungsprotokollen/Audits. Weniger Datenverkehr mit Zweigstellen dank Multicast-Technologie, die lokale Softwarebereitstellungen ermöglicht.

SIEM-INTEGRATION
Unmittelbare Meldung und Übermittlung von Ereignissen an führende SIEM-Systeme – IBM® QRadar und HP ArcSight. Erfassung von Protokollen und anderen sicherheitsrelevanten Daten für die Analyse bei geringerem Workload und weniger Tools für den Administrator und gleichzeitiger Vereinfachung des unternehmensweiten Reporting.

ROLLENBASIERTE ZUGRIFFSKONTROLLE
Unterscheidung von administrativen Rollen und Aufgaben in komplexen Netzwerken. Individuelle Anpassung der Konsolenansichten gemäß Rolle und Berechtigung.

ZENTRALISIERTE VERWALTUNG
Eine integrierte Verwaltungskonsole, Kaspersky Security Center, ermöglicht die Sicherheitsverwaltung für Desktops, Mobilgeräte und virtualisierte Endpoints im gesamten Netzwerk über eine einzige Benutzeroberfläche.

Kaspersky Systems Management ist in Kaspersky Endpoint Security for Business – ADVANCED und in Kaspersky Total Security for Business enthalten und kann auch separat als Targeted Solution erworben werden.

KASPERSKY SECURITY FOR MAIL-SERVER

Kaspersky Security for Mail Server bietet auch in komplexen heterogenen Infrastrukturen ausgezeichneten Schutz für den auf Mail-Servern anfallenden Datenverkehr, einschließlich Schutz vor Spam, Phishing sowie generischen und hochentwickelten Malware-Bedrohungen.

Schutz vor dem Verlust vertraulicher Daten in E-Mails und Anhängen wird auch für Microsoft® Exchange Server-Umgebungen gewährleistet.

WICHTIGSTE VORTEILE

SCHUTZ VOR MALWARE-BEDROHUNGEN
Leistungsstarker Malware-Schutz durch die vielfach ausgezeichnete Anti-Malware-Engine von Kaspersky Lab, einschließlich Echtzeit-Unterstützung durch das Cloud-basierte Kaspersky Security Network, proaktivem Schwachstellenschutz und Filterung schädlicher URLs.

SPAM-SCHUTZ
Für Microsoft Exchange- und Linux®-basierte E-Mail-Server blockiert die Cloud-basierte Anti-Spam-Engine von Kaspersky Lab nachweislich bis zu 99,96 % der Spam-Mail bei minimalen Fehlalarmen (False-Positives).

SCHUTZ VOR DATENVERLUST UND KONTROLLE (MICROSOFT EXCHANGE-SERVER)*
Durch Ermitteln von Geschäfts-, Finanz-, persönlichen und anderen vertraulichen Daten in ausgehenden E-Mails und Anhängen auf Microsoft Exchange-Servern und die Kontrolle dieses Informationsflusses sorgt Kaspersky Security for Mail Servers dafür, dass Ihre vertraulichen Daten und die Ihrer Mitarbeiter stets geschützt sind und Sie die gesetzlichen Datenschutzauflagen erfüllen. Dank ausgeklügelter Analysetechniken wie die Suche nach strukturierten Daten und unternehmensspezifische Glossare können verdächtige E-Mails identifiziert und somit blockiert werden. Das System kann sogar den Vorgesetzten des Absenders per E-Mail auf eine potentielle Datensicherheitsverletzung aufmerksam machen.

EINFACHE, FLEXIBLE ADMINISTRATION
Benutzerfreundliche Management- und Reporting-Tools und flexible Scan-Einstellungen verleihen Ihnen effiziente Kontrolle über die Sicherheit Ihrer E-Mails und Dokumente und tragen so zur Reduzierung der Gesamtbetriebskosten bei.

FUNKTIONEN

- Echtzeit-Malware-Schutz unterstützt durch das Cloud-basierte Kaspersky Security Network
- Umgehender Schutz vor unbekannten Exploits und sogar vor Zero-Day-Schwachstellen.
- Erweiterter Schutz vor Spam: Die Anti-Spam-Engine von Kaspersky Lab blockiert mehr als 99 % aller unerwünschten E-Mails.
- Schutz vor Datenlecks (Microsoft Exchange-Server)*. Identifizierung von vertraulichen Informationen in E-Mails und Anhängen auf Grundlage von Kategorien (inklusive persönlicher Angaben und Bankkartendaten), Glossaren und tiefgehender Analyse unter Verwendung strukturierter Daten.
- Cloud-basiertes Echtzeit-Scannen aller Nachrichten auf Microsoft® Exchange-Servern, einschließlich öffentlicher Ordner, mithilfe des Kaspersky Security Network.
- Zeitplangesteuertes Scannen von E-Mails und Lotus Domino-Datenbanken.
- Scannen von Nachrichten, Datenbanken und anderen Objekten auf IBM® Domino®-Servern.
- Filtern von Nachrichten durch Erkennung von Format, Größe und Name von Anhängen
- Einfacher und bequemer Update-Vorgang der Malware- und Spam-Datenbank
- Datensicherung vor der Desinfektion oder Löschung
- Skalierbarkeit und Fehlertoleranz.
- Einfache Installation und flexible integrierte Verwaltung.
- Leistungsstarkes Benachrichtigungssystem
- Umfassendes Reporting zum Netzwerkschutzstatus.

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

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway ist eine erstklassige Anti-Malware-Lösung, die den sicheren Internetzugang aller Mitarbeiter Ihres Unternehmens gewährleistet.

WICHTIGSTE VORTEILE

LEISTUNGSSTARKER SCHUTZ REDUZIERT AUSFALLZEITEN UND BETRIEBSUNTERBRECHUNGEN
Die vielfach ausgezeichnete Anti-Malware-Engine von Kaspersky Lab blockiert neueste bekannte sowie potentielle Malware-Bedrohungen und verhindert, dass diese über schädliche oder gefährliche Programme in das Netzwerk gelangen.

LEISTUNGSEFFIZIENZ DURCH OPTIMIERUNG
Optimierte, intelligente Scan-Technologie und Load Balancing reduzieren die Auslastung von Ressourcen und sparen so wertvolle Bandbreite, ohne dass Sie Abstriche bei der Sicherheit machen müssen.

UMFASSENDE PLATTFORMUNTERSTÜTZUNG
Die Unterstützung für die neuesten Plattformen und Server, darunter auch Proxyserver, ist ideal für hohe Netzwerklasten in heterogenen Umgebungen geeignet. Die Unterstützung für Microsoft® Forefront® TMG erweitert den Schutz auf den unternehmensinternen E-Mail-Verkehr und auf das Web-Gateway.

EINFACHES MANAGEMENT UND REPORTING
Einfache, benutzerfreundliche Management-Tools, flexible Einstellungen und Reporting-Systeme für den Schutzstatus.

FUNKTIONEN

- **Durchgehender proaktiver Schutz** vor aufkommenden und bekannten Malware-Bedrohungen
- **Ausgezeichnete Malware-Erkennungsraten** bei minimalen Fehlalarmen (False-Positives)
- **Optimierte, intelligente Scan-Technologie**
- **Echtzeit-Scannen** des HTTP-, HTTPS- und FTP-Datenverkehrs von veröffentlichten Servern.
- **Schutz für Squid,** den beliebtesten Linux-Proxy-Server
- **Benutzerfreundliche Tools** für Installation, Management und Updates
- **Flexible Scan-Tools und Vorfall-Reaktionsszenarien**.
- **Load Balancing** für Serverprozessoren
- **Skalierbarkeit und Fehlertoleranz.**
- **Umfassendes Reporting** zum Netzwerkschutzstatus

SPEZIFISCHE FUNKTIONEN FÜR MICROSOFT® FOREFRONT® TMG UND ISA-SERVER:

- Echtzeitüberprüfung des Programmstatus
- Scannen von VPN-Verbindungen.
- Scannen des HTTPS-Datenverkehrs in Echtzeit (nur TMG)
- Schutz von E-Mail-Datenverkehr (über POP3- und SMTP-Protokolle)
- Backup-Speicher (nur TMG)

Kaspersky Security for Mail Server und Kaspersky Security for Internet Gateway sind in Kaspersky Total Security for Business enthalten und können auch separat als Targeted Solutions erworben werden.

KASPERSKY SECURITY FÜR COLLABORATION

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

WICHTIGSTE VORTEILE

UMFASSENDER SCHUTZ FÜR IHRE SHAREPOINT-PLATTFORM
Das Cloud-basierte Kaspersky Security Network bietet leistungsstarken Schutz vor bekannten, unbekannten und erweiterten Bedrohungen, während die Anti-Phishing-Technologie vor Web-basierten Angriffen auf Unternehmensdaten schützt.

VERLUST VERTRAULICHER DATEN VERHINDERN*
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.

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.

FUNKTIONEN

MALWARE-SCHUTZ
- **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.

UNTERTÜTZT DIE KOMMUNIKATIONSRICHTLINIEN 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.
- **Inhaltsfilterung** – Das Programm kann verhindern, dass Dateien mit unangemessenen Inhalten gespeichert werden. Der Inhalt aller Dateien wird anhand von Schlüsselwörtern analysiert. Kunden können zur Inhaltsfilterung auch ihre eigenen, benutzerdefinierten Wörterbücher erstellen.

VERLUST VERTRAULICHER DATEN VERHINDERN*
- **Scannen von Dokumenten auf vertrauliche Informationen**. 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). Die Daten werden mit integrierten, regelmäßig aktualisierten Themenwörterbücher und benutzerdefinierten Wörterbüchern abgeglichen.
- **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.

Kaspersky Security for Collaboration ist in Kaspersky Total Security for Business enthalten und kann separat als Targeted Solution erworben werden.

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

KASPERSKY SECURITY FOR STORAGE

Hochwirksamer Schutz für Speichersysteme von EMC, NetApp, Hitachi und IBM®.

WICHTIGSTE VORTEILE

LEISTUNGSSTARKER MALWARE-SCHUTZ IN ECHTZEIT
Allzeit aktivierter, proaktiver Schutz für netzwerkgebundene Speicherlösungen (NAS). Die leistungsstarke Anti-Malware-Engine von Kaspersky Lab scannt jede aufgerufene oder geänderte Datei auf sämtliche Arten von Malware, einschließlich Viren, Würmer und Trojaner. Eine fortschrittliche, ganzheitliche Analyse erkennt selbst neue und bisher unbekannte Bedrohungen.

OPTIMIERTE SYSTEMLEISTUNG
Hochwirksame Scans auf der Grundlage optimierter Scan-Technologie und flexibler Ausschlusseinstellungen sorgen für maximalen Schutz und schonen gleichzeitig die Systemleistung.

ZUVERLÄSSIGKEIT
Eine unkomplizierte Architektur, deren einheitliche Komponenten auf ein reibungsloses Zusammenspiel ausgelegt sind, ermöglicht eine außergewöhnliche Fehlertoleranz. Dadurch ergibt sich eine stabile, widerstandsfähige Lösung, die bei erzwungenem Herunterfahren automatisch neu startet und dadurch zuverlässigen, durchgehenden Schutz gewährleistet.

EINFACHE VERWALTUNG
Die Server werden per Fernzugriff installiert und ohne Neustart sofort in den Schutz einbezogen. Verwaltet werden sie zusammen mit anderen Sicherheitslösungen von Kaspersky Lab über eine unkomplizierte, zentrale Konsole: Kaspersky Security Center.

FUNKTIONEN

ALLZEIT AKTIVIERTER, PROAKTIVER SCHUTZ
Die Scans der branchenführenden Anti-Malware-Engine von Kaspersky Lab, entwickelt von erfahrenen Fachleuten im Bereich der IT-Bedrohungen, bieten mit ihrer intelligenten Erkennungstechnologie proaktiven Schutz vor neu aufkommenden und potentiellen Bedrohungen.

AUTOMATISCHE UPDATES
Die Malware-Datenbanken aktualisieren sich automatisch ohne Unterbrechung der Scanvorgänge, sodass durchgängiger Schutz und minimale Belastung der Administratoren sichergestellt sind.

AUSGESCHLOSSENE PROZESSE UND VERTRAUENSWÜRDIGE BEREICHE
Feinjustieren lässt sich die Scan-Leistung durch die Einrichtung vertrauenswürdiger Bereiche, die von den Scans ausgenommen werden können. Das Gleiche gilt für festgelegte Dateiformate und Prozesse wie Datensicherungen.

SCANS VON OBJEKTEN MIT AUTORUN-FUNKTION
Zur Erhöhung des Serverschutzes lassen sich Scans von Autorun-Dateien und Betriebssystemen durchführen, um so die Aktivierung von Malware beim Hochfahren des Systems zu verhindern.

OPTIMALE LEISTUNG DURCH FLEXIBLE SCANS
Verringert die Scan- und Konfigurationsdauer und unterstützt Load Balancing zur Optimierung der Serverleistung. Der Administrator kann die Tiefe, Breite und Zeitplanung der Scanvorgänge bestimmen und festlegen, welche Dateitypen und Bereiche zu scannen sind. Scans nach Bedarf lassen sich für Zeiten mit geringerer Serveraktivität planen.

SCHUTZ FÜR HSM- UND DAS-LÖSUNGEN
Unterstützt Offline-Scanmodi zum wirksamen Schutz von Systemen mit Hierarchical Storage Management (HSM). Der Schutz von Direct Attached Storage (DAS) trägt ebenfalls dazu bei, die Nutzung von kostengünstigen Speichersystemen voranzutreiben.

UNTERSTÜTZUNG ALLER WICHTIGEN PROTOKOLLE
Kaspersky Security for Storage unterstützt die wichtigsten Protokolle, die von den unterschiedlichen Netzwerkspeichersystemen verwendet werden: CAVA Agent, RPC und ICAP.

SCHUTZ VON VIRTUALISIERTEN SYSTEMEN UND TERMINALSERVERN
Zur flexiblen Sicherheit gehört der Schutz von virtualisierten (Gast-) Betriebssystemen in virtualisierten Hyper-V- und VMware-Umgebungen sowie von Terminalinfrastrukturen von Microsoft® und Citrix.

VERWALTUNG

ZENTRALE INSTALLATION UND VERWALTUNG
Installation, Konfiguration und Verwaltung per Fernzugriff, einschließlich Benachrichtigungen, Updates und flexiblem Reporting, erfolgen über das intuitiv bedienbare Kaspersky Security Center. Alternativ lassen sich die Funktionen auch über die Befehlszeile verwalten.

KONTROLLE ÜBER ADMINISTRATORRECHTE
Jedem Administrator eines Servers können verschiedene Berechtigungsebenen zugewiesen werden, sodass sich spezielle IT-Sicherheitsrichtlinien des Unternehmens einhalten lassen.

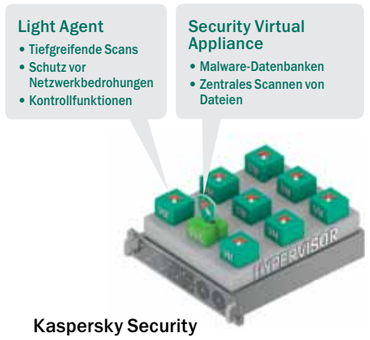
FLEXIBLE REPORTING-FUNKTIONEN
Zu Reporting-Zwecken können grafische Berichte bereitgestellt oder die Ereignisprotokolle von Microsoft Windows® oder dem Kaspersky Security Center überprüft werden. Such- und Filterfunktionen erleichtern den schnellen Datenzugriff in sehr umfangreichen Protokollen.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization ist eine flexible Lösung, die sowohl Schutz als auch Leistung für Ihre virtualisierte Umgebung garantiert.

LIGHT AGENT FÜR ERWEITERTEN SCHUTZ

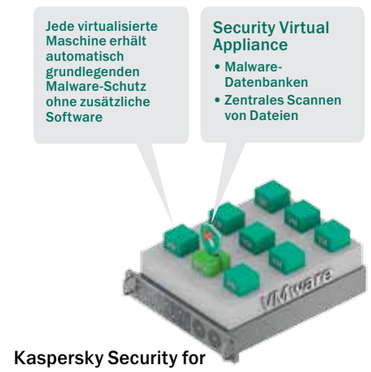
Kaspersky Security for Virtualization umfasst einen leistungsstarken Light Agent, der auf jeder virtualisierten Maschine bereitgestellt wird. Dies ermöglicht die Aktivierung erweiterter Endpoint-Sicherheitsfunktionen. Dazu zählen Vulnerability Monitoring, Programm-, Geräte- und Web-Kontrolle, Virenschutz des Instant-Messaging-, E-Mail- und Internet-Datenverkehrs sowie erweiterte Heuristik. Das Ergebnis ist ein leistungsstarker, mehrstufiger Sicherheitsansatz, der die Systemressourcen nicht unnötig belastet.



Kaspersky Security for Virtualization
Light-Agent-Konfiguration

OPTIONALE AGENTENLOSE KONFIGURATION FÜR VMWARE-UMGEBUNGEN

Tiefere Integration in VMware-Technologien bedeutet, dass Kaspersky Security for Virtualization auf dieser Plattform auch in einer agentenlosen Sicherheitskonfiguration sehr einfach bereitgestellt und verwaltet werden kann. Die gesamte Sicherheitsaktivität ist in der Security Virtual Appliance vereint und interagiert mit Schnittstellen von vShield – für sofortigen automatischen Schutz virtualisierter Maschinen – und vCloud für den Netzwerkschutz.



Kaspersky Security for Virtualization
Agentenlose Konfiguration*

WICHTIGE PRODUKTFUNKTIONEN

- **Zentralisierte Verwaltung über das Kaspersky Security Center**
- **Zentraler SVA-basierter VM-Schutz**
- **Verbesserter Malware-Schutz**
- **Host-basierte Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) und Firewall**
- **Endpoint-Kontrolle für Programme, Internetzugriff und Peripheriegeräte**
- **Cloud-basierte Sicherheit über das Kaspersky Security Network**
- **Network Attack Blocker**
- **Anti-Phishing**
- **Anti-Virus für IM-, Mail- und Internetdatenverkehr**
- **Keine zusätzliche Installation oder Neustarts für neue VMs****

FLEXIBLE LIZENZIERUNG

Kaspersky Security for Virtualization steht, abhängig von Ihren Anforderungen, mit folgenden Lizenzoptionen zur Verfügung:

- Maschinenbasierte Lizenzierung
  - Pro Desktop
  - Pro Server
- Ressourcenbasierte Lizenzierung
  - Pro Kern

VIELE PLATTFORMEN, EIN PREIS

Eine Einzellizenz von Kaspersky Security for Virtualization umfasst die Unterstützung für virtualisierte Citrix-, Microsoft®- und VMware-Umgebungen.

SECURITY VIRTUAL APPLIANCE (SVA)

Kaspersky Lab bietet in diesem Bereich zwei herausragende Lösungen, die beide auf einer Security Virtual Appliance basieren.

Die Security Virtual Appliance (SVA) von Kaspersky Lab scannt alle VMs in der Host-Umgebung zentral. Diese Architektur bietet effizienten VM-Schutz, schont gleichzeitig die Ressourcen des Endpoints, vermeidet AV-Scan- und Update-Storms sowie „Instant-on“-Lücken und verhilft Ihnen zu besseren Konsolidierungsraten.

INTEGRATION MIT DER PLATTFORMARCHITEKTUR

Kaspersky Security for Virtualization unterstützt VMware-, Microsoft® Hyper-V®- und Citrix Xen-Plattformen und ihre Kerntechnologien.

VMware	Microsoft Hyper-V	Citrix Xen
Hohe Verfügbarkeit	Dynamischer Arbeitsspeicher	Dynamische Speicherkontrolle
vCenter-Integration	Gemeinsame Cluster-Laufwerke	VM-Schutz und -Recovery (VM Protection and Recovery, VMPR)
vMotion – Host-DRS	Live-Backup	XenMotion (Live-Migration)
Horizon View (vollständige Clones und verknüpfte Clones)	Live-Migration	Multi-Stream ICA
		Citrix Receiver
		Personal vDisk

* Erweiterte Sicherheitsfunktionen wie Datei-Quarantäne, HIPS, Vulnerability Scanning und Endpoint-Kontrolle stehen bei dieser Konfiguration nicht zur Verfügung.
** Bei nicht-persistenten VMs ist ein sofortiger Schutz verfügbar, sobald der Light Agent im Image der VM integriert ist. Bei persistenten VMs muss der Administrator den Light Agent bei der Installation manuell einrichten.

KASPERSKY SECURITY INTELLIGENCE SERVICES

Als CISO/erfahrener Sicherheitsexperte liegt es in Ihrer Verantwortung, Ihr Unternehmen vor den heutigen Bedrohungen zu schützen und die Gefahren vorauszuahnen, die in den kommenden Jahren darauf zukommen. Hierfür ist ein Ausmaß an strategischem Sicherheitswissen erforderlich, das nur wenige Unternehmen intern selbst aufbauen können.

Kaspersky Lab ist ein wertvoller Partner, der durch die Bereitstellung topaktueller Sicherheitsinformationen über unterschiedliche Kanäle dafür Sorge trägt, dass Ihr SOC/IT-Sicherheitsteam über sämtliche Ressourcen verfügt, um Ihr Unternehmen erfolgreich vor allen Online-Bedrohungen zu schützen.

SCHULUNGSPROGRAMM FÜR CYBERSICHERHEIT

Das Schulungsprogramm zu Cybersicherheit von Kaspersky Lab wurde speziell für Unternehmen entwickelt, die die Rolle der Cybersicherheit stärken möchten, um die eigene Infrastruktur und geistiges Eigentum zu schützen.

Das Programm deckt alles von Sicherheitsgrundlagen bis zur fortgeschrittenen digitalen Forensik und Malware-Analyse ab. So helfen wir Kunden, ihr Wissen zu Cybersicherheit in drei Hauptbereichen zu erweitern:

- Grundwissen zum Thema
- Digitale Forensik und Vorfallsreaktion
- Malware-Analyse und Reverse Engineering

FEEDS MIT BEDROHUNGSINFORMATIONEN

Für zusätzlichen Schutz lassen sich über unsere Feeds mit Bedrohungsdaten die allerneuesten Sicherheitsinformationen in vorhandene SIEM-Systeme (Security Information and Event Management) integrieren.

MALWARE-ANALYSE DIGITALE FORENSIK VORFALLSREAKTION

Die Untersuchungsservices von Kaspersky Lab können Unternehmen durch eine umfassende Bedrohungsanalyse und eine Beratung zu den entsprechenden Schritten für die Behebung des Vorfalls bei der Formulierung ihrer Verteidigungsstrategien unterstützen.

Die Untersuchungsservices sind in drei Hauptbereiche unterteilt:

- Malware-Analyse: Erläutert Ihnen das Verhalten und die Ziele bestimmter Malware-Dateien, die es auf Ihr Unternehmen abgesehen haben.
- Digitale Forensik: Liefert Ihnen ein vollständiges Bild des Vorfalls und der Folgen für Ihr Unternehmen.
- Vorfallsreaktion: Ein vollständiger Vorfallsuntersuchungszyklus, der einen Besuch durch Experten von Kaspersky Lab vor Ort umfasst.

ÜBERWACHUNG VON BOTNET-BEDROHUNGEN

Die professionelle Lösung von Kaspersky Lab verfolgt die Aktivität von Botnets und bietet eine schnelle Benachrichtigung zu Bedrohungen (innerhalb von 20 Minuten), die mit den Benutzern einzelner Online-Zahlungs- und -Bankingsysteme zusammenhängen. Sie können dann auf Grundlage dieser Informationen entsprechende Benachrichtigungen zu bestehenden Risiken an Ihre Kunden, Sicherheitsdienstanbieter und an lokale Strafverfolgungsbehörden herausgeben.

INTELLIGENCE REPORTS

Unsere Intelligence Reports bieten Ihnen Zugang zu topaktuellen, relevanten Informationen auf Grundlage von über 80 Millionen Benutzerstatistiken aus 200 Ländern. Eine breitere Wissensgrundlage führt so zu einer Sensibilisierung für die Bedrohungen, mit denen sich Ihr Unternehmen auseinandersetzen muss.

Wissen, Erfahrung und tiefgreifende Erkenntnisse haben Kaspersky Lab zum vertrauenswürdigen Partner angesehener internationaler Strafverfolgungs- und Regierungsbehörden gemacht. Sie können dieses Wissen noch heute für Ihr Unternehmen nutzen.

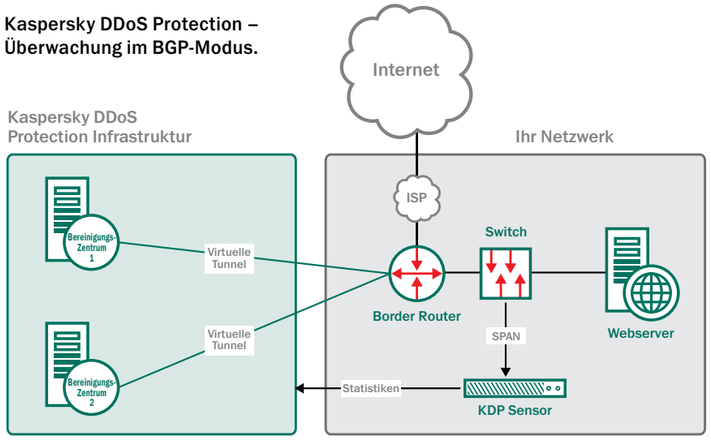
KASPERSKY-UNTERNEHMENSLÖSUNGEN

SCHUTZ VOR DDOS-ATTACKEN – OPTIMALE VERTEIDIGUNG UND RISIKOBEGRENZUNG

Wir haben an alles gedacht, um Ihr Unternehmen vor DDoS-Attacken (Distributed Denial of Service) zu schützen.

Kaspersky DDoS Protection bietet Ihnen alles, was Ihr Unternehmen benötigt, um sich vor allen Arten von DDoS-Attacken zu schützen und die Auswirkungen zu begrenzen. Hierzu gehören eine kontinuierliche Analyse Ihres gesamten Online-Datenverkehrs, die Benachrichtigung über einen vermuteten Angriff, das Umleiten des betroffenen Datenverkehrs, das Bereinigen der Daten und die Rückgabe des bereinigten Datenverkehrs an Sie.

Kaspersky DDoS Protection – Überwachung im BGP-Modus.



KASPERSKY FRAUD PREVENTION – FÜR BANKEN UND FINANZINSTITUTE

Eine umfassende Technologie-Plattform, die hochgradig anpassbar und einfach zu bedienen ist und Schutz vor Risiken bei Online- und mobilen Finanztransaktionen bietet.

Kaspersky Fraud Prevention schützt Kunden von Finanzinstituten unabhängig von der Art des Geräts, das sie für den Zugriff auf diese Dienste verwenden (PC, Laptop, Smartphone oder Tablet). Die Plattform verfügt zudem über eine bankseitige Softwarekomponente, die Malware entdeckt und abnormale Verhaltensmuster in einzelnen Kundentransaktionen automatisch erkennt. Die Clientless Engine kann sogar betrügerische Transaktionen verhindern, wenn Kaspersky Fraud Prevention for Endpoints nicht installiert ist.

SCHUTZ KRITISCHER INFRASTRUKTUREN

Schutz von industriellen Steuerungssystemen und Netzwerken

Kaspersky Endpoint Security for Business bietet im „industriellen Modus“ effektiven Schutz von ICS/SCADA-Endpoints vor Bedrohungen und Schwachstellen, die gern von Kriminellen für den Angriff auf kritische Systeme genutzt werden.

In Zusammenarbeit mit führenden Anbietern von Prozessautomatisierungslösungen wie Emerson, Rockwell Automation und Siemens hat Kaspersky Lab eine Reihe spezieller Verfahren entwickelt, um die Zulassung und Eignung für die Prozesstechnik unserer Kunden zu garantieren. Auf diese Weise können wir einen effektiven Schutz kritischer Infrastrukturen garantieren, ohne die betriebliche Kontinuität zu beeinträchtigen.

KASPERSKY LAB PROFESSIONAL SERVICES

Für Kunden mit komplexen IT-Installationen stellen die Kaspersky Professional Deployment and Upgrade, Training and Health Check-Services sicher, dass Kaspersky Security for Business-Lösungen einwandfrei konfiguriert, bereitgestellt und verwaltet werden.

KASPERSKY SMALL OFFICE SECURITY

Erstklassiger und einfacher Schutz für kleine Unternehmen.

Für Ihre Ihre speziellen Herausforderungen: eine spezielle Lösung. Leistungsstarker und erstklassiger Schutz, der schneller und einfacher zu verwenden ist als jemals zuvor.
- Speziell entwickelt für Unternehmen mit 25 Benutzern und weniger.
- Einfach zu installieren und auszuführen – keine Schulung erforderlich
- Webkonsole für internetbasierte Verwaltung von überall aus.

KEINE ERFAHRUNG NOTWENDIG
Kaspersky Small Office Security wurde so entwickelt, dass es auch von Personen, die nicht technikaffin sind, einfach installiert und ausgeführt werden kann. Es ist mit unkomplizierten „Assistenten" ausgestattet, die Sie automatisch durch folgende Schritte leiten:

- Einrichtung, einschließlich Entfernen eventuell vorhandener Anti-Malware
- Einrichten der Kontrollen und Auswählen der Richtlinien, die für Sie und Ihr Unternehmen am besten geeignet sind
- Automatisches Herunterladen dieser Änderungen auf mehrere Computer gleichzeitig

Alles wird über ein webbasiertes Dashboard verwaltet, sodass Sie oder jede andere Person, die Sie auswählen, Ihre IT-Sicherheit per Fernzugriff über das Internet verwalten kann.

Kaspersky Small Office Security bietet herausragende Sicherheit, aber wird so unauffällig und effizient im Hintergrund ausgeführt, dass praktisch gar nicht auffällt, dass es überhaupt da ist.

MEHRERE SCHUTZEBENEN
Kaspersky Small Office Security stattet Ihre PCs, Macs, Server, Tablets und Smartphones mit mehreren Schutzebenen aus. Alle Sicherheitstools, die Ihr wachsendes Unternehmen braucht, sind enthalten – und mehr. Vertrauen Sie Kaspersky Small Office Security Ihre IT-Sicherheit an, damit Sie sich ganz Ihrem Unternehmen widmen können.

- Cloud-basierter Echtzeitschutz vor neuen und aufkommenden Cyberbedrohungen.
- Schutz für Windows®- und Mac-Systeme, Windows-Server und Android™-Mobilgeräte.
- Schutz vor Hackern und Identitätsdieben bei Online-Finanztransaktionen durch die vielfach ausgezeichnete Technologie „Sicherer Zahlungsverkehr".
- Kontrolle der Aktivitäten von Mitarbeitern beim Surfen im Internet und in Sozialen Netzwerken.
- Verschlüsselung für den Schutz vertraulicher Unternehmens- und Kundendaten.
- Anti-Phishing-Technologien für den Schutz vor gefälschten und schädlichen Webseiten.
- Leistungsstarke Spam-Filterung.
- Sichere Passwort-Verwaltung.*
- Automatische Sicherung Ihrer Daten über Dropbox zum Schutz vor Datenverlust.

DADURCH SPAREN SIE GELD
Mit Kaspersky Small Office Security werden Sie nicht nur vor Hackerangriffen geschützt, die auf Ihr Geld abzielen, sondern es hilft Ihnen auch dabei, die Produktivität Ihrer Mitarbeiter zu steigern, indem Sie ihre Internetnutzung regulieren und die Zeiten begrenzen, in denen sie surfen oder Nachrichten versenden können. Mit leistungsstarken Sicherheitsfunktionen wie Verschlüsselung können Ihre Kunden davon ausgehen, dass ihre Daten bei Ihnen sicher sind, was Ihr Umsatzpotenzial und die Kundenzufriedenheit erhöht.

*Nur für 32-Bit-Anwendungen. Umfasst Android-und iOS-Geräte.

KASPERSKY MAINTENANCE- UND SUPPORT-AGREEMENTS

Ein hochwertiger Support für Vorfälle, Konfigurationsprobleme, Inkompatibilitäten und andere Problempunkte der IT-Sicherheit ist entscheidend für Unternehmen, für die ein beruhigendes Gefühl der Sicherheit und möglichst geringe Ausfallzeiten wichtig sind.

Unsere Maintenance- und Support-Agreements (MSAs) bieten garantierte Betriebszeiten und eine kontinuierliche Qualitätssicherung für die IT-Sicherheitsnetzwerke Ihres Unternehmens. Diese Vereinbarungen bieten hochwertigen Support bei unerwarteten Vorfällen, von fehlerhaften Konfigurationen bis hin zu Malware-Ausbrüchen, und tragen so zur Stabilität und Effizienz des gesamten Unternehmens bei.

Maintenance- und Support-Agreements von Kaspersky Lab decken die folgenden Bereiche ab:

- Unerwartete globale Virenausbrüche
- Beträchtliche Ausfallzeiten aufgrund komplexer Infrastrukturen
- Deployment-Optimierung und individuell angepasste Problemlösungen
- Probleme mit der Netzwerkinkompatibilität
- Produktaktualisierungsprozess von Kaspersky Lab
- Untersuchung von Malware-Vorfällen
- Support für Produktinstallation und -konfiguration*
- Deployment von Patches und anderen Updates*

Sollte Ihr Team Unterstützung benötigen, sind unsere Spezialisten über priorisierte Verbindungen in Ihrer Sprache für Sie da – mit Reaktionszeiten, die auf die Bedürfnisse Ihres Unternehmens abgestimmt sind. Die folgende Tabelle liefert einen Überblick über die verfügbaren Support-Optionen.

	Standard-Support		Erweiterter Support	
	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
Priorisierte Telefonleitung	Ja	Ja	Ja	Ja
Technical Account Manager	Nein	Nein	Ja	Ja (eigener)
Support in lokaler Sprache	8x5	8x5	8x5	24x7x365
Schweregrad-1-Support	8x5	8x5	24x7x365	24x7x365
Antwortzeit Schweregrad 1	8 Geschäftsstunden	6 Geschäftsstunden	4 Stunden	30 Minuten
Schweregrad-2-Support	8x5	8x5	8x5	24x7x365
Professional Services-Beratung	Nein	Nein	Zusätzliche Kosten	Health Check und angepasstes Reporting
Vorfallseingrenzung	6	12	36	Unbegrenzt

* Bezahloptionen für MSA Business nicht für MSA Starter und MSA Plus erhältlich.

KASPERSKY LAB WELTWEIT

Kaspersky Lab unterstützt lokal ansässige und globale Unternehmen durch weltweite Niederlassungen. Wenden Sie sich bitte an Ihren Händler vor Ort, wenn Sie weitere Informationen zum Erwerb der unterschiedlichen Kaspersky Security for Business-Lösungen wünschen.

www.kaspersky.de

APAC

1. Australien
2. China
3. Hongkong
4. Indien
5. Korea
6. Malaysia

Europa

7. Österreich
8. Frankreich
9. Deutschland
10. Italien
11. Niederlande
12. Portugal
13. Spanien
14. Norwegen
15. Schweiz
16. Großbritannien

Schwellenländer

17. Lettland
18. Polen
19. Rumänien
20. Slowenien
21. Südafrika
22. Türkei
23. Ukraine
24. Vereinigte Arabische Emirate

Japan

25. Japan (Tokio)

Nordamerika

26. Kanada
27. USA (Boston)
28. USA (Miami)

Russland und GUS

29. Russland
30. Kasachstan

Catalog_SP1/Feb15/Global