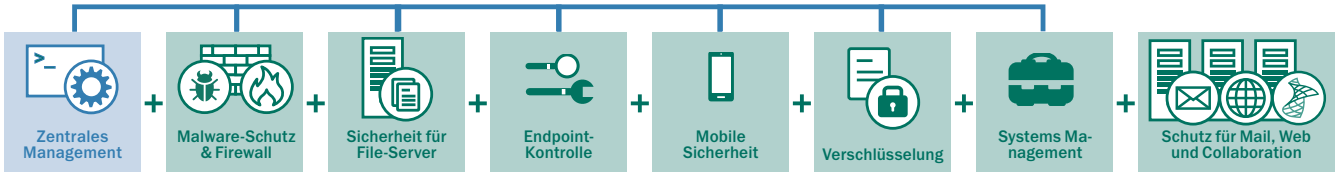
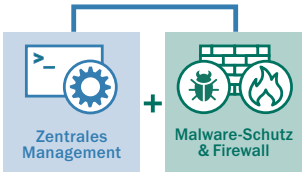
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Leistungsstarker, Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen, von erfahrenen Sicherheitsexperten konzipiert und entwickelt. Kaspersky Endpoint Security for Business bietet mithilfe der international anerkannten Bedrohungsanalyse höchstmöglichen IT-Schutz und komfortable IT-Kontrolle.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS – CORE



Malware-Schutz als Fundament der Sicherheitsplattform von Kaspersky Lab

Die mehrschichtigen Schutztechnologien von Kaspersky Lab werden intern von Mitarbeitern entwickelt, die großen Wert auf Sicherheit legen. Unabhängige Tests bestätigen das Ergebnis: Es handelt sich um einer der vier führenden Anbieter von Sicherheitslösungen für Endpoint-Nutzer.

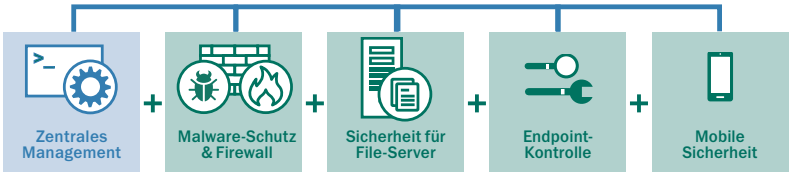
Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen – Hoch entwickelte Technologien erkennen und beseitigen bestehende sowie neu aufkommende Bedrohungen.

Automatischer Exploit-Schutz entdeckt gezielt unbekannte und hoch entwickelte Bedrohungen. **Cloudbasierter Schutz** durch Echtzeitinformationen aus dem Kaspersky Security Network.

Aktivitätsmonitor bietet eine komfortable Funktion zur Dateiwiederherstellung im Falle einer Systembeeinträchtigung.

System zur Angriffsüberwachung auf Host-Basis (Host-based Intrusion Prevention System (HIPS)) mit persönlicher Firewall – HIPS schränkt Aktivitäten je nach der Vertrauensstufe eines Programms ein und wird dabei von einer persönlichen Firewall auf Programmebene unterstützt, die die Netzwerkaktivität einschränkt.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT



Leistungsstarke, fein abgestufte Endpoint-Kontrolle mit aktivem Schutz und aktiver Verwaltung für mobile Geräte und Daten

Programm-, Web- und Gerätekontrolle, einschließlich dynamischen Whitelists mit dem internen Labor von Kaspersky Lab, vertiefen den Endpoint-Schutz noch weiter. Mobilgeräte, die vom Unternehmen oder vom Mitarbeiter selbst (BYOD) bereitgestellt werden, werden ebenfalls geschützt, und Plattformen werden über das Kaspersky Security Center zur gemeinsamen Verwaltung mit allen geschützten Endpoints zusammengeführt. Durch spezielle Schutzfunktionen für File-Server wird sichergestellt, dass Infektionen sich über gespeicherte Daten nicht auf die abgesicherten Endpoints ausbreiten können.

ENDPOINT-KONTROLLE

Programmkontrolle mit dynamischen Whitelists – Von Kaspersky Security Network in Echtzeit bereitgestellte Dateireputationen ermöglichen IT-Administratoren, Programme zuzulassen, zu blockieren oder zu regulieren, einschließlich eines „Default Deny"-Whitelist-Szenarios in einer Live- oder Test-Umgebung. Durch Steuerung von Programmberechtigungen und Vulnerability Scanning werden Programme, die sich verdächtig verhalten, überwacht und beschränkt.

Web-Kontrolle – Richtlinien für das Browsen können im Zusammenhang mit vorgegebenen oder eigenen Kategorien erstellt werden. Dadurch erlangen Sie einen umfassenden Überblick und eine effiziente Verwaltung.

Gerätekontrolle – Mithilfe von Masken für gleichzeitige Einrichtung auf mehreren Geräten können fein abgestufte Datenrichtlinien festgelegt, geplant und durchgesetzt werden, die die Verbindung von Wechseldatenträgern und anderen Peripheriegeräten kontrollieren.

FILE-SERVER-SCHUTZ

Wird gemeinsam mit dem Endpoint-Schutz über das Kaspersky Security Center verwaltet.

MOBILE SICHERHEIT

Leistungsstarker Schutz für mobile Geräte – Hoch entwickelte, aktive, cloudbasierte Technologien kommen zu einem mehrschichtigen Echtzeitschutz für mobile Endpoints zusammen.

Web-Filter, Spam- und Phishing-Schutz sorgen für einen noch umfangreicheren Schutz Ihrer Geräte.

Remote-Diebstahlschutz – Sperrung, Ortung, SIM-Überwachung, Warnung, Fahndungsfoto und vollständige oder selektive Löschung sind Funktionen, die einen nicht autorisierten Zugriff auf Unternehmensdaten verhindern, wenn ein mobiles Gerät verloren geht oder gestohlen wird. Die Administrator- und Endbenutzeraktivierung sowie die Unterstützung für Google Cloud Management ermöglichen bei Bedarf eine schnelle Aktivierung.

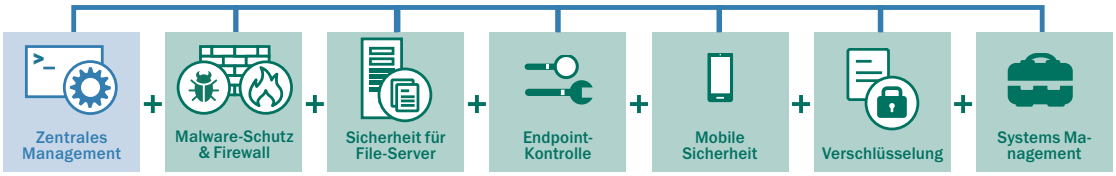
Mobile Programmverwaltung (Mobile Application Management, MAM) – Kontrollen beschränken den Benutzer darauf, unbedenkliche Programme auszuführen, und beugen dem Deployment unerwünschter oder unbekannter Software vor. Durch die **Containerisierung von Programmen** werden Unternehmensdaten auf Privatgeräten von Mitarbeitern isoliert. Zusätzliche Verschlüsselung und selektive Löschung sind per Fernzugriff möglich.

Mobile Device Management (MDM) – Eine gemeinsame Oberfläche für **Microsoft® Exchange ActiveSync**- und **iOS MDM**-Geräte mit OTA (Over The Air)-Richtlinien-Deployment. **Samsung KNOX** für Android™-basierte Geräte wird ebenfalls unterstützt.

Self-Service-Portal – Selbstständige Registrierung genehmigter Privatgeräte von Mitarbeitern im Netzwerk mit automatischer Installation aller erforderlichen Zertifikate und Schlüssel sowie Notfallaktivierung von Diebstahlschutz-Funktionen durch Benutzer/Besitzer. Dies verringert den administrativen Arbeitsaufwand für die IT.

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

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED



Systems-Management-Tools optimieren die Effizienz und Sicherheit der IT, und die integrierte Verschlüsselung schützt gleichzeitig vertrauliche Daten.

Das automatisierte Patch Management und die Verwaltung von Betriebssystem-Images, Remote-Softwarebereitstellung und SIEM-Integration optimieren die Verwaltung, während Hardware- und Software-Bestandslisten sowie die Lizenzverwaltung für Transparenz und Kontrolle sorgen. Die integrierte Verschlüsselungstechnologie erweitert den Datenschutz um eine leistungsstarke Komponente.

SYSTEMS MANAGEMENT

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

Betriebssystem-Deployment – Einfaches Erstellen, Speichern und Bereitstellen von „Golden Images“ des Betriebssystems, einschließlich UEFI-Unterstützung.

Software-Distribution und Troubleshooting – Remote-Softwarebereitstellung sowie Programm- und Betriebssystem-Updates nach Bedarf oder zeitplangesteuert, einschließlich Wake-on-LAN-Unterstützung. Das zeitsparende Remote-Troubleshooting und die effiziente Softwarebereitstellung werden durch die Multicast-Technologie unterstützt.

Hardware- und Software-Bestandslisten und Lizenzverwaltung – Dank Erkennung, Überblick und Kontrolle (einschließlich Blockierung) sowie verwalteter Lizenznutzung erhalten Sie einen Einblick in die gesamte in der Umgebung bereitgestellte Software und Hardware, inklusive Wechseldatenträger. Hardware- und Software-Lizenzverwaltung, Erkennung von Gastgeräten, Steuerung von Berechtigungen und Zugriffs-Provisioning sind ebenfalls verfügbar.

SIEM-Integration – Unterstützung für die SIEM-Systeme IBM® QRadar und HP ArcSight

Rollenbasierte Zugriffskontrolle (Role Based Access Control, RBAC) – Administrative Zuständigkeiten können netzwerkübergreifend zugewiesen werden, mit Konsolenansichten, die an die zugewiesenen Rollen und Rechte angepasst werden.

VERSCHLÜSSELUNG

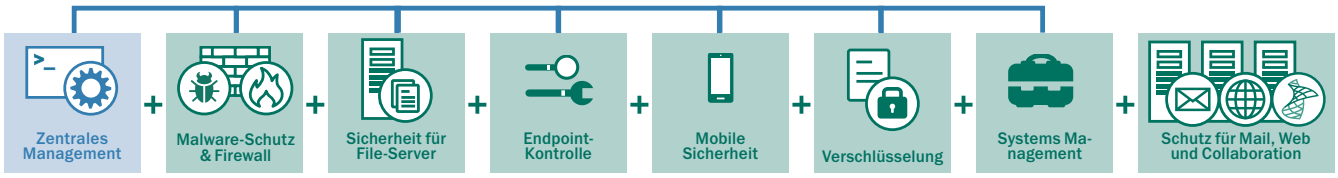
Leistungsstarker Datenschutz – File-/Folder-Level-Verschlüsselung (FLE) und Full-Disk-Verschlüsselung (FDE) können auf Endpoints angewendet werden. Der Support für den „portablen Modus“ ermöglicht eine geräteübergreifende Verschlüsselungsverwaltung, weg von administrativen Domänen.

Flexible Benutzeranmeldung – Die Authentifizierung vor dem Start (Pre-boot authentication, PBA) bietet zusätzlichen Schutz und Benutzertransparenz durch die Option zum „einmaligen Anmelden“. Zweistufige oder tokenbasierte Authentifizierung sind ebenfalls verfügbar.

Erstellung integrierter Richtlinien – Die einzigartige Integration der Verschlüsselung mit der Programm- und Gerätesteuerung trägt zusätzlich zur erweiterten Sicherheit und einfachen Verwaltung bei.

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

KASPERSKY TOTAL SECURITY FOR BUSINESS



Kaspersky Total Security for Business bietet einen umfassenden Schutz der gesamten IT-Umgebung in Ihrem Unternehmen.

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 sehr gute Abfangraten und minimale Fehlalarme (False-Positives). Malware-Schutz für IBM® Domino® ist ebenfalls enthalten. Die DLP-Funktion für Microsoft Exchange ist 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 -Farms vor allen Arten von Malware. Die separat erhältliche DLP-Funktion für SharePoint bietet Inhalts- und Dateifilter-Funktionen, erkennt vertrauliche Daten und schützt vor Datenverlusten.

AUSGEZEICHNETER SCHUTZ

- **In unserem Unternehmen steht Technologie auf allen Ebenen im Mittelpunkt** und bei unserem CEO Eugene Kaspersky an allererster Stelle.
- **Unser internationales Forschungs- und Analyseteam (Global Research & Analysis Team, GReAT)**, ein Team aus führenden IT-Sicherheitsexperten, hat viele der gefährlichsten Malware-Bedrohungen und gezielten Angriffe als Erstes entdeckt.
- **Viele der weltweit angesehensten Sicherheitsinstitutionen** und Strafverfolgungsbehörden haben sich schon aktiv an uns um Hilfe gewandt.
- **Jedes Jahr nimmt Kaspersky Lab an unabhängigen Tests teil** und geht dabei sehr häufig als Sieger hervor!
- **Die renommiertesten Branchenanalysten**, darunter Gartner, Inc, Forrester Research und International Data Corporation (IDC), sehen uns in vielen Kategorien der IT-Sicherheit als führend an.
- **Über 130 OEMs**, einschließlich Microsoft, Cisco Meraki, Juniper Networks, Alcatel Lucent u.v.m., verwenden unsere Technologien in ihren eigenen Produkten und Diensten.

Das macht den Unterschied!

Weitere Informationen zu Kaspersky Endpoint Security for Business erhalten Sie bei Ihrem Vertriebspartner.

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

Kaspersky Endpoint Security for Business/Okt 15/Global

KASPERSKY lab