KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Advanced

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

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

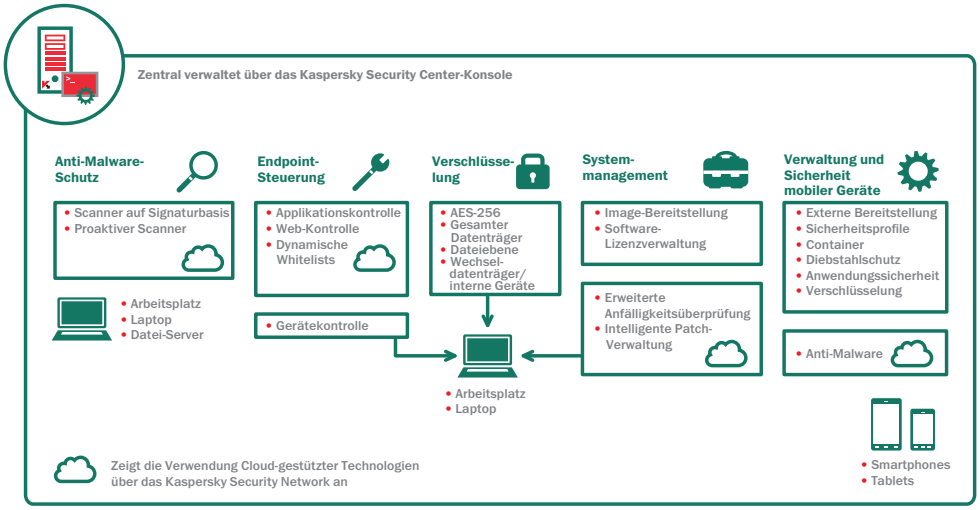
Alle Schutz- und Verwaltungsfunktionen, die Sie benötigen.

Wir bei Kaspersky Lab haben unsere gestufte Angebotspalette zunehmend um leistungsstarke Funktionen für Großunternehmen bereichert, während wir gleichzeitig den Zugang zur Technologie so unkompliziert machten, dass sie für Unternehmen jeder Größe nutzbar ist.

Welche Stufe ist die richtige für Sie?

- CORE
- SELECT
- **ADVANCED**
- TOTAL

ENTHALTENE FUNKTIONEN:
- ANTI-MALWARE
- FIREWALL
- CLOUD-UNTERSTÜTZTER SCHUTZ ÜBER KASPERSKY SECURITY NETWORK
- APPLIKATIONSKONTROLLE
- WHITELISTING
- WEB-KONTROLLE
- GERÄTEKONTROLLE
- DATEI-SERVER-SCHUTZ
- MOBILE DEVICE MANAGEMENT (MDM)
- MOBILE ENDPOINT SECURITY (FÜR TABLETS UND SMARTPHONES)
- VERSCHLÜSSELUNG
- SYSTEMKONFIGURATION UND -BEREITSTELLUNG
- NETZWERKZUGANGSKONTROLLE
- ERWEITERTE ANFÄLLIGKEITSÜBERPRÜFUNG
- PATCH-VERWALTUNG



DIE EINZIGE WAHRE SICHERHEITSPLATTFORM IN DER BRANCHE.

Eine Verwaltungskonsole
Über einen einzigen Bildschirm können Administratoren die gesamte Sicherheitslandschaft einsehen und verwalten: virtuelle, physische und mobile Geräte.

Eine Sicherheitsplattform
Kaspersky Lab entwickelte Konsole, Sicherheitsmodule und Tools selbst, anstatt die Komponenten von anderen Unternehmen zuzukaufen. Dies bedeutet, dass die gleichen Programmierer mit der gleichen Codebasis Technologien entwickelten, die miteinander kommunizieren und arbeiten. Das Resultat sind Stabilität, integrierte Richtlinien, sinnvolle Berichterstellung und intuitiv zugängliche Tools.

Eine Investition
Alle Tools sind aus einer Anbieterhand und werden in einer einzigen Installation geliefert. Auf diese Weise können Sie mit einem einzigen Budget-Posten und einer Zahlungsbewilligung Ihre Sicherheitsrisiken mit Ihren Unternehmenszielen in Einklang bringen.

VERSCHLÜSSELUNG UND DATENSCHUTZ:

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

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

FREIGABE SICHERER DATEN
Dies bedeutet, dass Benutzer sehr einfach verschlüsselte und selbst extrahierende Pakete erstellen können, um sicherzustellen, dass Daten, die über mobile Geräte, E-Mails, das Netzwerk oder das Internet weitergeleitet werden, geschützt sind.

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

ENDPOINT-STEUERUNG:

APPLIKATIONSKONTROLLE
Gestattet IT-Administratoren das Festlegen von Richtlinien, die Anwendungen (bzw. Anwendungs-Kategorien) gestatten, blockieren oder regulieren.

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

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

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

ENDPOINT-SCHUTZFUNKTIONEN:

OPTIMALE ENDPOINT-ANTI-MALWARE
Branchenbewährte herkömmliche Methoden – auf Signaturbasis, proaktiv und auf Cloud-Basis – zum Erkennen von Bedrohungen durch Malware.

CLOUD-UNTERSTÜTZTER SCHUTZ
Das Kaspersky Security Network (KSN) reagiert auf vermutete Bedrohungen deutlich schneller als herkömmliche Schutzmethoden. Die Reaktionszeit von KSN liegt für Malware-Bedrohungen teilweise bei 0,02 Sekunden!

MANCHE FUNKTIONEN WERDEN VON BESTIMMTEN PLATTFORMEN NICHT UNTERSTÜTZT. Nähere Informationen erhalten Sie unter **www.kaspersky.com.**

SYSTEMKONFIGURATION UND PATCH-VERWALTUNG:

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

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

NETWORK ADMISSION CONTROL (NAC)
«Mit der Netzwerkzugangskontrolle (NAC) können Sie Zugangsrichtlinien für Gastgeräte einrichten. Diese Gastgeräte werden automatisch erkannt (auch Mobilgeräte), und Ihre Benutzer werden zu einem Unternehmensportal weitergeleitet, wo sie mithilfe des richtigen Identifikationspassworts die von Ihnen genehmigten Ressourcen nutzen können.

BEREITSTELLUNG VON BETRIEBSSYSTEM UND ANWENDUNGS-IMAGE
Einfaches Erstellen, Speichern und Bereitstellen von System-Images von einem zentralen Standort aus. Perfekt für eine Migration zu Microsoft® Windows® 8.

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

MOBILE SICHERHEITSFUNKTIONEN:

INNOVATIVE ANTI-MALWARE-TECHNOLOGIEN
Kombination von signaturbasierter, proaktiver und Cloud-unterstützter Erkennung ermöglicht Echtzeitschutz. Sicherer Browser, Anti-Spam-Schutz und eine Anwendungs-Sandbox verbessern die Sicherheit.

BEREITSTELLUNG MIT OTA-PROVISIONING (OTA = OVER THE AIR)
So können Sie Anwendungen zentralisiert über SMS, E-Mails und PCs vorkonfigurieren und bereitstellen.

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

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

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

KASPERSKY LABS GMBH
DESPAG-STRASSE 3
85055 INGOLSTADT
DEUTSCHLAND
salesDACH@kaspersky.de
www.kaspersky.de

KESB-ADV/Version 0.2/Nov12/Global