KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Select

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

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

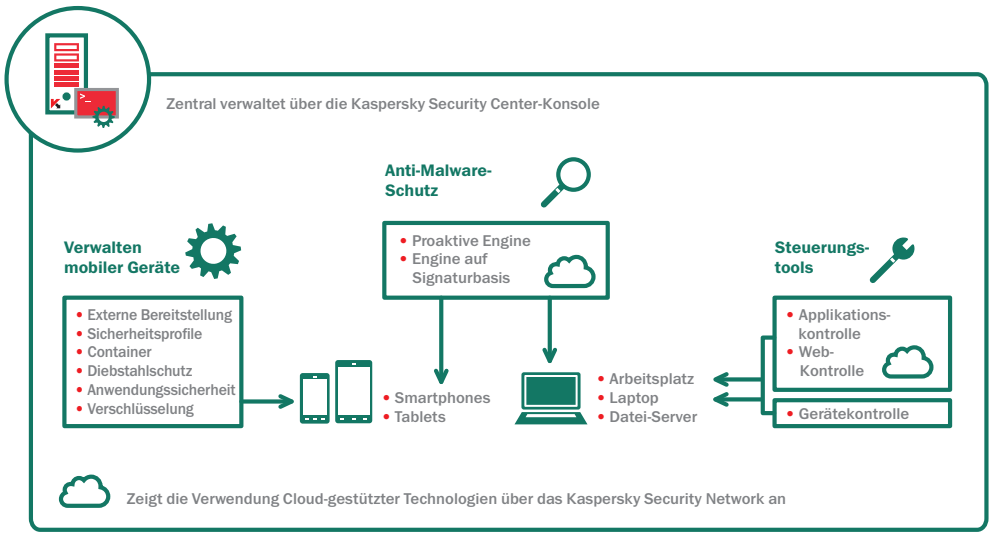
Alle Schutz- und Verwaltungs-funktionen, die Sie benötigen.

Wir bei Kaspersky Lab haben unsere gestufte Angebotspalette zunehmend um leistungsstarke Funktionen für Unternehmen 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-BASIERTER SCHUTZ ÜBER KASPERSKY SECURITY NETWORK
- PROGRAMMKONTROLLE
- WHITELISTING
- WEB-KONTROLLE
- GERÄTEKONTROLLE
- DATEI-SERVER-SCHUTZ
- MOBILE DEVICE MANAGEMENT (MDM)
- MOBILE ENDPOINT SECURITY (FÜR TABLETS UND SMARTPHONES)



HAUPTFUNKTIONEN:

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

FLEXIBLE, AUSGEARBEITETE STEUERUNGSTOOLS
Eine Datenbank auf Cloud-Basis, die Anwendungen nach «sicher» und «unsicher» kategorisiert, unterstützt den Administrator dabei, Richtlinien für den Umgang mit Anwendungen und Webseiten festzulegen, während Steuermechanismen im Detail bestimmen, welche Geräte sich mit Rechnern im Netzwerk verbinden können.

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

SCHWACHSTELLEN-SCANNER
Darauf ausgerichtet, Software-Schwachstellen aufzuzeigen, die anfällig für Angriffe sind.

ENDPOINT-SCHUTZFUNKTIONEN:

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

VERHALTENSANALYSE DURCH AKTIVITÄTSMONITOR
Liefert proaktiven Schutz vor Bedrohungen, die noch nicht in Signatur-Datenbanken erfasst wurden.

CLOUD-BASIERTER SCHUTZ
Das Kaspersky Security Network (KSN) reagiert auf vermutete Bedrohungen deutlich schneller als herkömmliche Schutzmethoden. Die Reaktionszeit von KSN liegt für Malware-Bedrohungen im Sekunden- oder Minutenbereich!

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

ENDPOINT-STEUERUNG:

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

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.

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.

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.

MOBILE SICHERHEITSFUNKTIONEN:

INNOVATIVE ANTI-MALWARE-TECHNOLOGIEN
Kombination von signaturbasierter, proaktiver und Cloud-basierter Erkennung ermöglicht Echtzeitschutz.

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.

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

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

IHR KOMPETENTER PARTNER FÜR DIE IT-SICHERHEIT.

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

Eine Sicherheitsplattform
Kaspersky Lab entwickelt Konsolen, Sicherheitsmodule und Tools selbst, anstatt die Komponenten von anderen Unternehmen zuzukaufen. Dies bedeutet, dass die gleichen Programmierer mit der gleichen Codebase Technologien entwickeln, die miteinander kommunizieren und arbeiten. Das Resultat sind Stabilität, integrierte Richtlinien, sinnvolles Reporting und intuitiv zugängliche Tools.

Eine Investition
Alle Tools sind aus einer Herstellerhand. Auf diese Weise können Sie mit nur einer Investition Ihre IT-Sicherheitslösung mit Ihren Unternehmenszielen in Einklang bringen.

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

Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | salesdach@kaspersky.de

4chya/Stand: Januar 2013