KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Verschlüsselungstechnologie

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

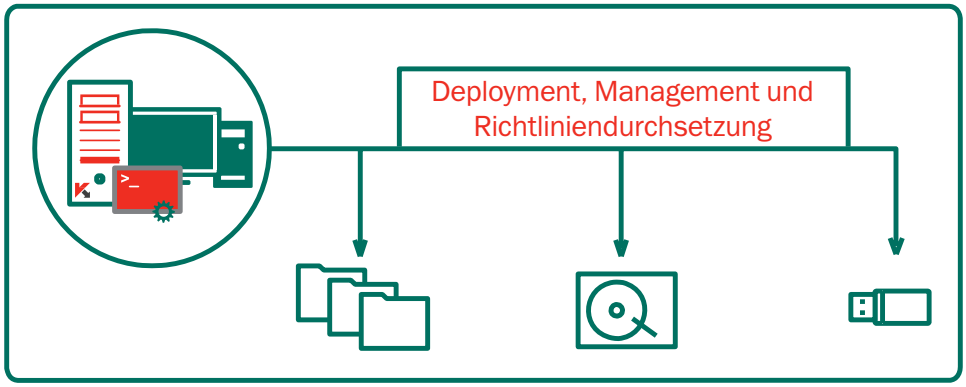
Proaktiver Schutz von Daten und Compliance ist eine zwingende Notwendigkeit. Die Verschlüsselungstechnologie von Kaspersky Lab schützt geschäftskritische Daten vor ungewolltem Verlust, bei Diebstahl oder gezielten Malware-Attacken. Egal ob stationär oder unterwegs, durch die Kombination von leistungsstarken Verschlüsselungsverfahren mit unseren zuverlässigen Technologien für die Sicherheit auf Endpoints sorgt unsere integrierte Plattform für den Schutz Ihrer Daten.

Die Verschlüsselungstechnologie von Kaspersky Lab kann mithilfe einer einzigen Richtline über eine zentrale Verwaltungskonsole bereitgestellt und verwaltet werden.

Unsere Verschlüsselungstechnologien verhindern Datenverluste und unbefugten Zugriff auf Daten:

- Full-Disk-Verschlüsselung (FDE)
- Verschlüsselung auf Datei-/Ordnerebene (FLE)
- Wechseldatenträger/ interne Geräte

VERWALTUNG ÜBER EINE ZENTRALE KONSOLE



BEWÄHRTE UND SICHERE KRYPTOGRAPHIE

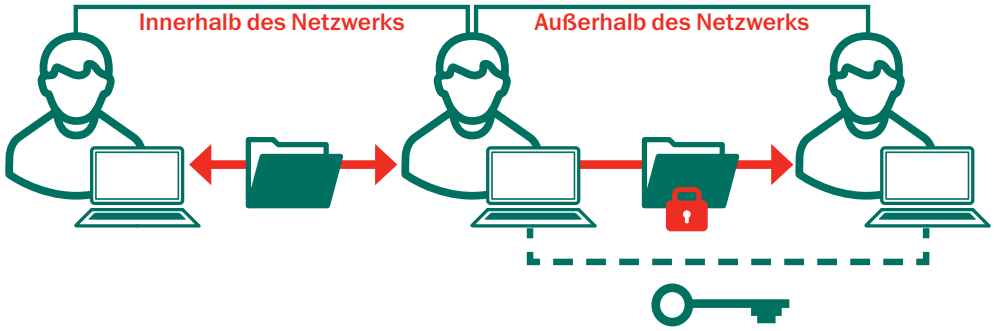
Kaspersky Lab nutzt den Advanced Encryption Standard (AES) mit 256-Bit-Schlüssellänge, vereinfachter Schlüsselverwaltung und sicherer Speicherung. Unterstützt Intel® AES-NI-Technologie, UEFI- und GPT-Plattformen.

UMFASSENDE FLEXIBILITÄT

Kaspersky Lab bietet Verschlüsselung auf Datei- und Ordnerebene (File-Level-Encrpytion, FLE) sowie vollständige Datenträgerverschlüsselung (Full Disk Encrpytion, FDE), um alle möglichen Anwendungsszenarien abzudecken. Es können sowohl Festplatten als auch Wechseldatenträger geschützt werden. Im „portablen Modus“ können die Daten auf Wechseldatenträgern selbst dann geschützt werden, wenn auf dem verbundenen Computer keine Verschlüsselungssoftware installiert ist. Dies ermöglicht einen sicheren Datenaustausch auch außerhalb des „geschützten Perimeters“.

EINMALIGE ANMELDUNG, KEINE BEEINTRÄCHTIGUNG VON ENDBENUTZERN

Von der Konfiguration bis hin zur täglichen Nutzung lässt sich unsere Verschlüsselungstechnologie transparent für alle Arten von Programmen einsetzen, ohne die Produktivität von Endbenutzern zu beeinträchtigen. Einmalige Anmeldung sorgt für lückenlose Verschlüsselung, und der Endbenutzer merkt möglicherweise gar nicht, dass die Technologie im Hintergrund läuft.



Verschlüsselungstechnologien von Kaspersky Lab ermöglichen einen reibungslosen, ungestörten 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 das Verschlüsselungs-Management mithilfe der rollenbasierten Zugriffskontrolle an verschiedene Personen delegiert werden. Auf diese Weise lässt sich das Verschlüsselungs-Management einfacher und weniger aufwändig gestalten.

Hinweise zum Kauf

Kaspersky-Verschlüsselungstechnologie ist nicht separat erhältlich. Sie ist nur bei den Stufen „Advanced“ und „Total“ von Kaspersky Endpoint Security for Business als eine der Komponenten einer vollwertigen und umfassenden Sicherheitsplattform aktiviert.

PRE-BOOT-AUTHENTIFIZIERUNG (PBA)

Noch bevor das Betriebssystem hochfährt, müssen Anmeldeinformationen eingegeben werden, wobei eine einmalige Anmeldung optional möglich ist. Unsere PBA-Verschlüsselungstechnologie wird auch bei Nicht-QWERTY-Tastaturen unterstützt.

AUTHENTIFIZIERUNG PER SMARTCARD UND TOKEN

Durch zwei-Faktoren-Authentifizierung über gängige Smartcard-Modelle und Token erübrigt sich die Eingabe von Anmeldeinformationen. Die Benutzererfahrung wird somit noch angenehmer gestaltet.

NOTFALLWIEDERHERSTELLUNG

Der Administrator kann im Fall eines Hardware- oder Softwarefehlers Daten auf Datenträgern 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 sind für allgemeine Ordner wie „Meine Dokumente“ und „Desktop“, neue Ordner, Dateinamenerweiterungen und Gruppen von Dateinamenerweiterungen (z. B. Microsoft Office-Dokumente, E-Mail-Nachrichtenarchive) vordefiniert, können aber auf Wunsch angepasst werden.

Kaspersky Endpoint Security for Business/Encryption/

KASPERSKY lab