Kaspersky®
Endpoint Security
for Business

Verschlüsselungstechnologie

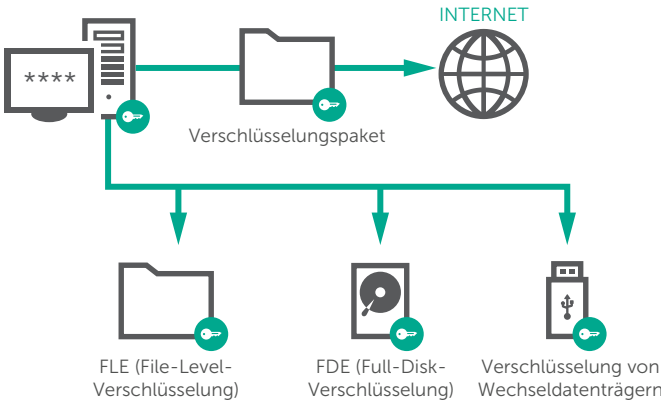
Verhindern Sie den unbefugten Zugriff auf Daten durch Geräteverlust, Diebstahl oder Malware.

Proaktiver Schutz von Daten und Compliance sind zwingend notwendig. 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 führenden Lösungen für die Sicherheit auf Endpoints, sorgt unsere integrierte Plattform für den Schutz von Daten, die gerade übertragen oder nicht genutzt werden.

Unsere Verschlüsselungstechnologien verhindern Datenverluste und unbefugten Zugriff auf Daten:

- Vollständige Datenträgerverschlüsselung (FDE)
- Folder-Level-Verschlüsselung (FLE)
- Verschlüsselung von Wechseldatenträgern

VERWALTUNG ÜBER EINE EINZIGE KONSOLE



Sichere Kryptographie nach Branchenstandard

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

Umfassende Flexibilität

Kaspersky Lab bietet File- und Folder-Level-Verschlüsselung sowie Full-Disk-Verschlüsselung, um alle möglichen Anwendungsszenarien abzudecken. Es können sowohl Daten auf Festplatten als auch auf Wechseldatenträgern geschützt werden. Im „portablen Mode" 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".

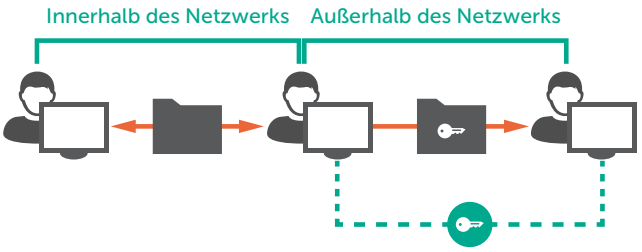
„Forrester Research, Inc. hat Kaspersky Lab in seiner Bewertung von Endpoint-Verschlüsselungslösungen als starken „Strong Performer" bewertet. Laut Forrester Wave™-Endpoint-Verschlüsselung, 2015, Kaspersky Lab."

Von Branchenexperten bestätigte Qualität.

Einmalige Anmeldung, Transparenz für Endbenutzer

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 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 mehrschichtige Sicherheit, die auf einer gemeinsamen Codebasis aufbaut. Das bedeutet, dass die Verschlüsselungseinstellung auf die ganze Umgebung oder auf bestimmte Geräte unter derselben Richtlinie wie Anti-Malware, Gerätekontrolle und andere Endpoint-Sicherheitselemente angewendet werden kann. Es müssen keine separaten Richtlinien erstellt oder separate Lösungen verwaltet werden. Die Hardware-Kompatibilität 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. PBA ist auch für Nicht-QWERTY-Tastaturen erhältlich.

Authentifizierung per Smartcard und Token

Die unterstützte Zwei-Faktor-Authentifizierung über gängige Smartcard-Modelle und Token macht die Eingabe von Anmeldeinformationen überflüssig und gestaltet die Benutzererfahrung so noch angenehmer.

Microsoft BitLocker-Verwaltung

Die Festplattenverschlüsselung auf Microsoft Windows-Geräten kann mithilfe der Microsoft BitLocker-Technologie verwaltet werden. Die Microsoft BitLocker-Verwaltung ermöglicht die Verwendung der nativen Verschlüsselungstechnologie, um die Hardware-Kompatibilität zu verbessern, ohne den Benutzer einzuschränken.

Notfallwiederherstellung

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

Optimiertes Deployment, anpassbare Einstellungen

Zur Erleichterung des Deployments sind Verschlüsselungseinstellungen für allgemeine Ordner wie „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 Lab
Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners
Kaspersky for Business: **www.kaspersky.de/business-security**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**
Unser einzigartiges Konzept:
https://www.kaspersky.de/true-cybersecurity

#truecybersecurity
#HuMachine

www.kaspersky.de