

McAfee Encrypted USB

Erweitern Sie Ihren Schutz auf mobile Datenspeicher mit McAfee® Encrypted USB-Geräten



In der heutigen Zeit speichern Unternehmen ihre Daten auf einer Vielzahl von Geräten, darunter auch auf kleinen, handlichen USB-Flash-Laufwerken, die nicht größer als eine Handfläche sind. Da diese Geräte immer kleiner werden, während ihre Speicherkapazität immer mehr zunimmt, können auf ihnen inzwischen große Mengen unternehmenswichtiger Daten gespeichert werden. Aus diesem Grund stellen sie ein Sicherheitsrisiko dar, zumal sie leicht verloren gehen oder gestohlen werden können. Darüber hinaus werden diese Geräte in den meisten Fällen nicht von der IT-Abteilung kontrolliert oder verwaltet oder sind in die Sicherheitsrichtlinien des Unternehmens eingebunden, so dass das Risiko eines unberechtigten Zugriffs, eines Datenverlusts und eines Verstoßes gegen die gesetzlichen Datenschutzbestimmungen erhöht ist. Daher ist es in heutigen mobilen Umgebungen wichtig, die zentralen Sicherheitsrichtlinien des Unternehmens auf die Kontrolle und Verwaltung von USB-Laufwerken auszuweiten.

Hauptvorteile

- Entsprechen Sie den Sicherheitsrichtlinien Ihres Unternehmens, den Datenschutzgesetzen und den Branchenrichtlinien durch den Einsatz von verschlüsselten USB-Geräten.
- Mobile Speicherlösung ohne Verstoß gegen Sicherheitsrichtlinien
- Übersicht und Verwaltung von verschlüsselten USB-Geräten im gesamten Unternehmen mit dem McAfee ePolicy Orchestrator (ePO), der die Erstellung automatischer Sicherheitsberichte sowie Prüfung, Überwachung und die Administration von Richtlinien ermöglicht.
- Zugriff auf die Steuerungsdaten mittels Zwei-Faktor-Authentifizierung
- Sichere Daten durch die Verwendung branchenweit führender Verschlüsselungsalgorithmen und -zertifikate wie AES-256 und FIPS 140-2, die starken Schutz bieten

Schützen Sie Ihre Ressourcen und Ihre Marke
USB-Laufwerke sind wegen ihrer geringen Größe und guten Tragbarkeit ein äußerst praktisches Speichermedium – aber sicherheitstechnisch ein Alptraum. Jeden Tag verlassen Mitarbeiter ihr Büros mit großen Mengen sensibler Unternehmensdaten auf tragbaren USB-Laufwerken, die sie in ihren Taschen oder Koffern mit sich führen, ohne dass ihnen bewusst ist, welches Sicherheitsrisiko dies für ihr Unternehmen darstellt, falls diese Datenträger verloren gehen oder gestohlen werden.

Wenn Sie Geräte mit McAfee Encrypted USB verwenden, werden die Informationen auf diesen Geräten verschlüsselt und können nur von berechtigten Personen gelesen werden. Dank der integrierten Zugriffskontrolle für Anwender und einer starken Datenverschlüsselung sorgt McAfee Encrypted USB dafür, dass sensible Daten auch unterwegs stets sicher sind. Außerdem ist der Nutzer vor neugierigen Blicken geschützt, da Personen- und Firmendaten durch die eingebauten Funktionen geschützt und validiert werden.

Zentrale Verwaltung dank des preisgekrönten ePolicy Orchestrator

Die firmenweite Ausbringung und Verwaltung von tragbaren Speichergeräten kann für das Unternehmen eine extrem komplexe und kostspielige Angelegenheit sein. Da USB-Laufwerke normalerweise nicht von der IT-Abteilung verwaltet werden, genießen Sie nicht den Schutz durch die unternehmensweiten Sicherheitsrichtlinien. Allzu oft kopieren einzelne Personen geistiges Eigentum oder andere interne Daten unverschlüsselt auf USB-Laufwerke –

Daten, die eigentlich verschlüsselt würden, wenn man sie als E-Mail-Anhang versenden oder auf einem Laptop speichern würde. Die zentrale Verwaltung mit McAfee ePolicy Orchestrator® (ePO™) ermöglicht es Unternehmen, diese Herausforderungen zu meistern, indem ein einfacher Weg zur gewünschten Verschlüsselung eröffnet wird. Sie können McAfee Encrypted USB-Laufwerke unternehmensweit ohne Auswirkungen auf Ihre bestehende IT-Infrastruktur einsetzen.

Der ePolicy Orchestrator und unsere verschlüsselten USB-Laufwerke können gemeinsam zentral mit Hilfe einer einzigen Konsole verwaltet und ausgebracht werden, so dass Sie die Unternehmenssicherheit verbessern und gleichzeitig Ihre Gesamtbetriebskosten senken. Mit der ePO-Managementschnittstelle können Sie jedes McAfee Encrypted USB-Gerät dank der kontaktlosen Initialisierungsfunktion einfach durch das Anschließen als ein durch ePO verwaltetes Gerät anmelden.

Sichern und schützen Sie Ihre Daten mit starker Verschlüsselung

Zur Nutzung von McAfee Encrypted USB-Geräten muss sich der Benutzer mit einem Passwort oder Fingerabdruck anmelden, damit ein unberechtigter Datenzugriff verhindert wird. Zur Erhöhung der Sicherheit kann eine Zwei-Faktor-Authentifizierung verwendet werden. Wenn der Benutzer das Passwort vergessen bzw. die biometrische Anmeldung nicht möglich ist, kann er dennoch Zugriff auf die Daten erhalten, indem er mit Hilfe von ePO das Passwort zentral zurücksetzen lässt oder es selbst über ePO zurücksetzt.

Spezifikationen

Treiberloses, verschlüsseltes USB-Standardlaufwerk

- Betriebssysteme
- Microsoft® Windows Vista
 - Microsoft® Windows XP
 - Microsoft® Windows 2000

- Hardware-Daten
- Verfügbare Größen: 1 GB und 2 GB

„Zero Footprint“-Ausführungen und Festplatte

- Betriebssysteme
- Microsoft® Windows Vista
 - Microsoft® Windows XP
 - Microsoft® Windows 2000
 - Mac OS X

- Hardware-Daten
- Sticks: Kapazitäten von 1 GB bis über 16 GB
 - Festplattenspeicher: Kapazitäten von 80 GB bis 320 GB

Daten zu McAfee ePolicy Orchestrator

- ePO 4.0 oder höher
- Encrypted USB-Erweiterung erforderlich

- Betriebssysteme
- Microsoft® Windows Vista
 - Microsoft® Windows XP
 - Microsoft® Windows 2003
 - Microsoft® Windows 2000

- Datenbank
- Microsoft® SQL Server 2000 oder 2005
 - Microsoft® SQL Express
 - Informix

- Browser
- Microsoft Internet Explorer 6.0 oder 7.0

- LDAP
- Microsoft® Windows 2003 Active Directory (oder höher)
 - Microsoft® ADAM

Dank der integrierten Verschlüsselung, Schlüsselerzeugung und Zertifikatsspeicherung können die Schlüssel nicht ausgelesen oder kopiert werden, da sie das USB-Laufwerk niemals verlassen. Es besteht sogar die Möglichkeit, andere Schlüssel und/oder Zertifikate für eine Public-Key-Infrastruktur (PKI) zu speichern. Alle Daten auf McAfee Encrypted USB-Geräten werden mit den stärksten in der Branche verfügbaren, hardwarebasierten Verschlüsselungsalgorithmen verschlüsselt. Dazu zählt AES-256 sowie Branchenstandards wie FIPS 140-2.

Compliance unter Beweis stellen





Durch die Integration in die ePO Management-Konsole unterstützt Sie McAfee Encrypted USB bei der Einhaltung aller Richtlinien, von unternehmensinternen Sicherheitsrichtlinien über branchenspezifische Regelungen bis zu Datenschutzgesetzen. So können Sie nachweisen, dass die Daten auf einem gestohlenen oder verlorenen USB-Gerät verschlüsselt sind. Außerdem können Sie zu Prüfzwecken Berichte erstellen, in denen Details zum Datenzugriff und zur Verwendung des USB-Gerätes angegeben sind.

Wichtige Merkmale

- **Implementierung strikter Zugriffssteuerungsmaßnahmen** für USB-Wechseldatenträger und Hardware-Verschlüsselung dem Advanced Encryption Standard (AES) 256-Algorithmus.
- **Stellen Sie ein, wie viele Anmeldeversuche mit Passwort oder biometrischer Authentifizierung erlaubt sind, um Brute-Force-Angriffe durch Maßnahmen wie der Zugangswiederherstellung oder der Zerstörung der Daten entgegenzuwirken.**
- **Erlangen Sie höchste Flexibilität mit einem Zero-Client-Footprint** sowie vom Betriebssystem unabhängige Sicherheit; Software-Installationen oder Administrator-Rechte sind nicht erforderlich, sondern lediglich eine USB-Schnittstelle.
- **Beugen Sie unbefugten Zugriffen auf Daten vor**, indem Sie für Benutzer eine Zwei-Faktor-Authentifizierung per Passwort und/oder Fingerabdruck vorsehen.
- **Installieren und nutzen Sie Anwendungen sicher und direkt vom USB-Laufwerk aus** (VPN, Internet-Browser, Thin Client usw.), so dass Anwendungen überall bequem und sicher laufen können.
- **Dank der integrierten Verschlüsselung, Schlüsselerzeugung und Zertifikatsspeicherung** können die Schlüssel nicht kopiert werden, da sie das USB-Laufwerk niemals verlassen. Es besteht sogar die Möglichkeit, andere Schlüssel und/oder Zertifikate für eine Public-Key-Infrastruktur (PKI) zu speichern.

McAfee Encrypted USB-Geräte

Die folgende Tabelle enthält die Leistungsmerkmale aller McAfee Encrypted USB-Geräte. Die USB-Sticks sind in Speicherkapazitäten von 1 GB bis 16 GB erhältlich, die USB-Festplatten haben eine Kapazität zwischen 80 GB bis 320 GB.

	Standard Driverless	Zero-Footprint Non-BIO	Zero-Footprint BIO	USB Hard Disk
				
Passwort-Authentifizierung	•	•	•	•
Biometrische Authentifizierung			•	•
Hardware-Verschlüsselung	•	•	•	•
Digitale Identität und Verschlüsselungsdienste		•	•	•
Verwaltung mit McAfee Encrypted USB Manager	•	•	•	•

Weitere Informationen über McAfee Encrypted USB erhalten Sie unter: www.mcafee.com/de.

