



McAfee® Encrypted USB

(ehemals SafeBoot® for USB)

Sichern Sie USB-Speichergeräte

Im Unternehmensbereich werden sensible Daten heutzutage auf einer Vielzahl von Geräten gespeichert und verarbeitet, darunter USB-Laufwerke. Die Speicherkapazität dieser Geräte ist enorm gewachsen, ihre Abmessungen dagegen sind immer kompakter geworden. Dadurch sind sie leicht transportierbar und ermöglichen die Speicherung von verschiedensten wichtigen Informationen. Durch die kleine Größe gehen solche Geräte auch leichter verloren, und aufgrund der hohen Speicherkapazität steigt zugleich die Menge der Daten, die im Fall von Verlust oder Diebstahl dem Risiko eines unbefugten Zugriffs ausgesetzt sind. Dies wird noch dadurch verschlimmert, dass die überwältigende Mehrheit dieser Geräte von den IT-Abteilungen gar nicht kontrolliert wird.

HAUPTVORTEILE

Strenge Zugriffskontrolle und starke Verschlüsselung

- Mobile Speicherlösung für Anwender ohne Verstoß gegen Sicherheitsrichtlinien
- Datenverschlüsselung im laufenden Betrieb, ohne Zutun des Anwenders und ohne Erfordernis von Schulungen
- Datenschutz durch starke Verschlüsselung
- Unterstützung für tragbare Sicherheits-Tokens

Zentrale Verwaltung

- Einfacher Einsatz im gesamten Unternehmen
- Einfache Bereitstellung und Verfolgung von Geräten über eine zentrale Konsole
- Geringerer Zeit- und Kostenaufwand durch effizientere Arbeitsabläufe
- Nutzung von Active Directory für die Zuordnung von Anwendern zu Geräten

Einhaltung von Bestimmungen

- Nachweis der Einhaltung von Datenschutzgesetzen
- Durchsetzung unternehmensweiter obligatorischer Sicherheitsrichtlinien
- Nachweis, dass das Gerät zum Zeitpunkt des Verlustes verschlüsselt war

Schützen Sie Ihre Ressourcen und Ihre Marke

Jeden Tag verlassen Mitarbeiter ihre Büros und sind sich gar nicht bewusst, wie unsicher ihre tragbaren Laufwerke sind. USB-Sticks sind wegen ihrer geringen Größe und guten Tragbarkeit ein äußerst praktisches Speichermedium - aber sicherheitstechnisch ein Alptraum. Sie können leicht verloren gehen oder sogar für Wirtschaftsspionage missbraucht werden.

Mit McAfee® Encrypted USB-Speichergeräten dagegen können Sie sich darauf verlassen, dass die auf diese Geräte kopierten und damit transportierten Informationen sicher sind und nur von befugten Personen eingesehen werden können.

Schutz

McAfee Encrypted USB-Geräte sind sichere, tragbare Speichergeräte, in denen eine Zugriffskontrolle für Anwender und starke Datenverschlüsselung eingebaut sind, damit sensible Daten auch unterwegs stets sicher sind. Die Verschlüsselung der Daten geschieht im laufenden Betrieb, hat so gut wie keine Leistungseinbußen zur Folge und erfordert keine besondere Schulung für den Anwender. Sie schützt und validiert auch Personen- und Firmendaten, sodass die Sicherheit von Identitäten gewährleistet ist.

Zentrale Verwaltung

Der firmenweite Einsatz und die Verwaltung von tragbaren Speichergeräten kann für das Unternehmen eine extrem komplexe und kostspielige Angelegenheit sein. Mithilfe des zentralen Managements können Unternehmen diese Herausforderung dank einfacher Ausbringung sowie firmenweiter Verwaltung von McAfee Encrypted USB-Geräten meistern. Und das ohne Auswirkungen auf Ihre bestehende IT-Infrastruktur. Eine beliebige Zahl von Anwendern kann effektiv verwaltet, kontrolliert und mit einer Anwender-Identität aus Microsoft Active Directory verknüpft werden. Im Ergebnis erhalten Sie so bestmöglichen Schutz der Informationsbestände Ihres Unternehmens bei geringen Gesamtbetriebskosten.

Richtlinieneinhaltung und Passwort-Wiederherstellung

McAfee Encrypted USB unterstützt Sie bei der Richtlinieneinhaltung. Sicherheitsrichtlinien werden beim Endanwender durchgesetzt, wodurch sichergestellt wird, dass auf dem Gerät gespeicherte Daten bei Diebstahl oder Verlust geschützt sind. Darüber hinaus kann Ihr Unternehmen dank der umfassenden Prüffunktionen und den bestehenden Reporting-Tools nachweisen, dass das Gerät verschlüsselt war. Anwender, die ihre Passwörter vergessen oder nicht länger in der Lage sind, über biometrische Authentifizierungsverfahren auf Daten zuzugreifen, können per Challenge-Response-Verfahren ihren Zugang wiederherstellen und den Zugriff auf ihr Gerät zurückerlangen.

SYSTEMANFORDERUNGEN

Die Systemanforderungen variieren je nachdem, für welches Gerät Sie sich entscheiden:

Standard Secure USB-Flash-Speicher

Betriebssysteme

- Microsoft® Windows XP
- Microsoft® Windows Server 2003
- Microsoft® Windows 2000

Hardware-Daten

- Verfügbare Größen: 512 MB bis 4 GB

Zero-Footprint USB-Speicher

Betriebssysteme

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

Hardware-Daten

- Sticks: Kapazitäten von 512 MB bis über 8 GB
- Festplatte: Kapazitäten von 80 GB bis über 100 GB

Zentrale Verwaltung

Betriebssystem

- Microsoft® Windows 2000
- Microsoft® Windows Server 2003
- Microsoft® Windows XP

Server

- Microsoft® SQL Server 2000 SP4 oder höher

Browser

- Microsoft Internet Explorer 6.0 oder höher

Funktionen

McAfee Encrypted USB umfasst ein Sortiment an sicheren tragbaren Speichergeräten, die sich jeweils durch einzigartige Funktionen auszeichnen. In jedem Gerät ist eine Zugriffskontrolle für Anwender sowie Datenverschlüsselung eingebaut, damit sensible Daten auch unterwegs stets sicher sind. Es entstehen kaum Leistungseinbußen, und besondere Schulungen für die Mitarbeiter sind ebenfalls nicht erforderlich.

Standard Secure USB-Flash-Speicher

- Richten Sie strenge Zugriffskontrollen für USB-Wechseldatenträger ein und verschlüsseln Sie die Daten mit dem AES-256-Algorithmus, um sicherzustellen, dass Daten auch unterwegs stets sicher sind.
- Unterstützen Sie die Nutzung durch mehrere Anwender, die jeweils eine eigene sichere Partition erhalten; mit anwenderspezifischen Passwörtern wird das Gerät entsperrt, und jeder Anwender erhält Zugang zu seinen jeweiligen Daten.
- Legen Sie für noch höhere Sicherheit fest, wie oft Passwörter maximal eingegeben werden dürfen.
- Nutzen Sie Geräte gemeinsam mit anderen Anwendern, ohne dass nicht zur gemeinsamen Nutzung freigegebene Daten gefährdet werden.
- Richten Sie einen "öffentlichen Bereich" zur Speicherung von Informationen ein, die nicht verschlüsselt werden; dieser Bereich kann auch zum Transport unkritischer Informationen zu einem ungesicherten Computer verwendet werden.




Zero-Footprint-Technologie

- Erlangen Sie höchste Flexibilität mit einem Zero-Client-Footprint und Betriebssystemunabhängige Sicherheit; Software-Installationen oder Administrator-Rechte sind nicht erforderlich, sondern lediglich eine USB-Schnittstelle.
- Beugen Sie mit einer Zwei-Faktor-Authentifizierung per Passwort und/oder Fingerabdruck unbefugten Zugriffen auf Daten vor.
- Legen Sie zum Schutz vor Brute-Force-Angriffen eine zulässige Höchstzahl für Anmeldeversuche per Passwort oder biometrischer Authentifizierung fest.
- Erhalten Sie die Zertifizierung nach FIPS 140-2.

Zentrale Verwaltung

- Weisen Sie die Einhaltung von Datenschutzgesetzen nach. Sicherheitsrichtlinien werden beim Endanwender durchgesetzt. Somit wird sichergestellt, dass alle auf dem Gerät gespeicherten Daten bei Diebstahl oder Verlust geschützt sind.
- Schützen Sie Ihre Ressourcen und Ihre Marke, indem Sie durch umfassende Prüffunktionen den empirischen Beweis erbringen, dass ein Gerät zum Zeitpunkt des Verlustes verschlüsselt war.
- Stellen Sie Anwender-Passwörter mit einem Challenge-Response-Verfahren wieder her. Selbst wenn ein Anwender das Unternehmen verlässt, können Sie dank diesem Verfahren jederzeit auf die Daten zugreifen.
- Kontrollieren Sie, wie Ihr Unternehmen seine Anwendergeräte verwaltet – über eine zentrale Verwaltungsstelle oder über tausende von Kontrollrechnern an verschiedenen Orten in aller Welt.

McAfee Encrypted USB-Sortiment

Standard Secure USB-Flash-Speicher	
	<ul style="list-style-type: none"> • 512 MB-4 GB Flash-Speicher • Passwort-Authentifizierung • AES-256-Verschlüsselung
Zero-Footprint USB-Speicher	
	<ul style="list-style-type: none"> • 512 MB-8 GB Flash-Speicher • Authentifizierung per Passwort und/oder Fingerabdruck • AES-256-Verschlüsselung • "Zero-Footprint"-Technologie
	<ul style="list-style-type: none"> • 80 GB-100 GB Festplattenspeicher • Authentifizierung per Passwort und/oder Fingerabdruck • AES-256-Verschlüsselung • "Zero-Footprint"-Technologie

Weitere Informationen zum Thema Datenschutz finden Sie im Internet unter www.mcafee.com/data_protection.

McAfee GmbH

Ohmstraße 1, D-85716 Unterschleißheim, Telefon: 089-3707 0 | Sachsenfeld 2, D-20097 Hamburg, Telefon: 040-2531-0
www.mcafee.de