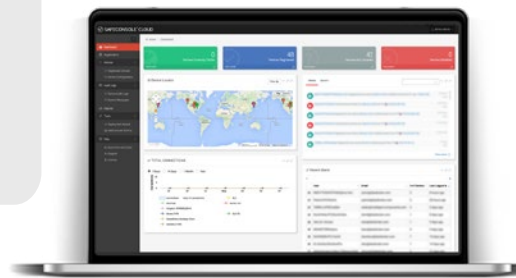


SAFECONSOLE[®]

DIE ZENTRALE VERWALTUNGSLÖSUNG FÜR SICHERE USB-LAUFWERKE



VERWALTEN SIE ALLE
SAFECONSOLEReady[®]
LAUFWERKE VON EINER SICHEREN
KOMMANDOZENTRALE AUS



DAMIT SIE STETS WISSEN WO SICH IHRE SENSIBLEN DATEN BEFINDEN

Durch DataLockers Verschlüsselungslösungen können vertrauliche Daten bei Transport, Speicherung und Austausch zuverlässig geschützt werden. Zusätzlich ermöglicht die SafeConsole die zentrale Verwaltung der verschlüsselten Laufwerke, ganz gleich wo sie sich gerade befinden.

SafeConsole ist die sichere Kommandozone für verschlüsselte Laufwerke, wie die externen verschlüsselten Festplatten DL3 und DL3FE, die verschlüsselten USB-Flashlaufwerke Sentry[®] ONE und Sentry[®] K300, sowie das virtuelle verschlüsselte Laufwerk SafeCrypt[®]. Auch PortBlocker, DataLockers DLP-Ansatz um USB-Ports zu sperren und ausschließlich autorisierte Laufwerke zur Nutzung freizugeben, kann durch SafeConsole verwaltet werden. Weitere SafeConsoleReady[®] Laufwerke sind von unseren Partnern Kingston[®] Technology und Origin Storage erhältlich.*

SafeConsole[®] ist die ideale Lösung für mobile Mitarbeiter, die an unterschiedlichen Standorten auf vertrauliche Daten oder geistiges Eigentum Zugriff haben müssen. SafeConsole erlaubt dabei sowohl kleineren Unternehmen, als auch sehr großen Organisationen die effiziente und transparente Administration und Kontrolle ihrer verschlüsselten Laufwerke.

LEISTUNGSMERKMALE



Inventarisierung. Überwachen Sie weltweit alle verschlüsselten Laufwerke inklusive ihres Aufenthaltsortes. Die Einbindung von Active Directory wird zur einfachen Nachverfolgung der Benutzer, sowie der zugeordneten Laufwerke und Computer, unterstützt.



Audit. Falls gewünscht, können Sie jederzeit sehen, welche Dateien auf Ihren verschlüsselten Laufwerken gespeichert oder gelöscht wurden. Sie haben bei Bedarf Zugriff auf ein komplettes Audit-Protokoll zur Beobachtung von Nutzeraktivitäten inklusive Verbindungen, fehlgeschlagenen Anmeldungen, wiederhergestellten Passwörtern und Verlustberichten.



Kontrolle. Setzen Sie Ihre Sicherheitsrichtlinien, wie Passwortregeln, Dateityp- oder geographische Einschränkungen durch. Passwörter können zurückgesetzt, der Schreibschutz-Modus kann aktiviert und bei Verlust oder Diebstahl kann das Gerät sogar aus der Ferne gelöscht werden.



Berichte. Erhalten Sie einen kompletten Überblick Ihrer weltweit genutzten verschlüsselten Laufwerke. Erstellen Sie Berichte nach Konfiguration, geographischem Standort, Status, Aktualisierungen, letzter Aktivität und mehr.

WEITERE LEISTUNGSMERKMALE

GEOLOCATION AND GEOFENCING

Durch die Nutzung von IP-basierter Ortsbestimmung kann der Aufenthaltsort Ihrer verschlüsselten Laufwerke weltweit ermittelt werden. Zudem kann SafeConsole Ihre Endgeräte per „Geofencing“ nur in einem vordefinierten geographischen Raum zur Nutzung freigeben.

EINFACHE UND SCHNELLE BEREITSTELLUNG

SafeConsole erlaubt eine einfache Bereitstellung für kleine und große Organisationen mit einer Verbindung zu Active Directory (AD). Administratoren können sich mit Ihren AD Benutzerdaten anmelden. Nach der Einrichtung von SafeConsole werden den Anwendern dann USB-Laufwerke zugeordnet. Jedes Laufwerk ist dabei mit einem eindeutigen Nutzer in der SafeConsole, basierend auf den Nutzerdaten aus dem Unternehmensverzeichnis (falls vorhanden) verbunden.

ZONE-BUILDER

Zone Builder erlaubt die Definition einer vertrauenswürdigen Zone wodurch zusätzliche Funktionen in Bezug auf Sicherheit und Benutzerfreundlichkeit zur Verfügung stehen:

🔒 BESCHRÄNKEN Sie die Verwendung der USB-Laufwerke auf die vertrauenswürdige Zone.

🔑 AUTO-UNLOCK ermöglicht ein automatisches Login ohne das Passwort eingeben zu müssen.

ANTI-MALWARE

DataLocker bietet in Partnerschaft mit McAfee einen optionalen Anti-Malware Schutz an, der im Hintergrund der verwalteten USB-Laufwerke agiert. Der Anti-Malware Scanner prüft das Laufwerk bei jeder Nutzung, erkennt und beseitigt Malware und meldet dies der SafeConsole, so dass stets überprüfbar ist, welche Laufwerke infiziert und bereinigt wurden.

Mit der nahtlosen McAfee Integration in alle USB-Laufwerke erreicht eine Organisation höchste Compliance und verhindert Vorfälle, die zu hohen Kosten und Datenverlusten führen können.

Powered by  **McAfee**[®]

* Die Verwaltung für SafeCrypt und EncryptDisc ist in Kürze verfügbar.

SAFECONSOLE[®]

DIE ZENTRALE VERWALTUNGSLÖSUNG FÜR SICHERE USB-LAUFWERKE

UNTERSTÜTZTE SAFECONSOLEREADY[®] LAUFWERKE



DataLocker Sentry ONE Managed*

Sentry ONE ist FIPS-140-2 Level 3-validiert und nutzt eine Hardware-basierte 256bit AES-Verschlüsselung. Dieses USB 3.2 Gen 1 Flash-Laufwerk neuester Generation steht für höchste Portabilität und Sicherheit.



DataLocker H300 und H350 Enterprise*

Die Kombination aus der Hardware-basierten 256bit AES-Verschlüsselung, der Validierung nach FIPS 140-2 Level 3 Standard (H350) und den USB 3.2 Gen 1 Datentransferraten sorgt für ein attraktives Preis-Leistungs-Verhältnis dieser sicheren externen USB-Festplatten.



DataLocker Sentry K300

Die microSATA SSD im Formfaktor eines USB-Sticks bietet Hardware-basierte 256bit AES-Verschlüsselung, ein alphanumerisches Tastaturfeld und ein integriertes OLED Display zur Konfiguration der umfangreichen Sicherheitsfunktionen.



DataLocker DL3 und DL3 FE

Die Kombination aus der Hardware-basierten 256bit AES-Verschlüsselung, der Validierung nach FIPS 140-2 Standard (DL3 FE), den USB 3.2 Gen 1 Datentransferraten und dem Touchscreen mit zufälliger Ziffernreihenfolge, lässt in Bezug auf Geschwindigkeit, Kapazität und Sicherheit keine Wünsche offen.



Kingston DataTraveler 4000 G2 (managebar)

Dieses Flash-Laufwerk mit USB 3.2 Gen 1 Schnittstelle und FIPS 140-2 Level 3 Validierung bietet durch die AES 256bit Hardware-Verschlüsselung ein hohes Maß an Sicherheit.



IronKey S1000 Enterprise* und D300 SM* - Serialized Managed

Kingstons Ironkey[™] S1000 und D300 Flash-Laufwerke stehen für höchste Sicherheit, so wie ihre Vorläufer aus der Ironkey Familie. Sie sind FIPS 140-2 Level 3 zertifiziert und verschlüsseln mit AES 256bit Hardware-Verschlüsselung im XTS-Modus.



Origin SC100

Das sichere und kostengünstige Flash-Laufwerk bietet neben AES 256bit Hardware-Verschlüsselung auch USB 3.2 Gen 1 Geschwindigkeit und sorgt damit für einen permanenten Schutz sensibler Unternehmensdaten.



DataLocker SafeCrypt

Das virtuelle Laufwerk kombiniert FIPS-140-2 validierte 256bit AES-Verschlüsselung mit der zentralen Verwaltung durch SafeConsole.



PortBlocker

Als optionale Lizenz für SafeConsole ermöglicht PortBlocker das Sperren der USB-Ports und die Freigabe autorisierter USB-Laufwerke.

*Managed/Enterprise Modelle benötigen immer eine SafeConsole Laufwerkslizenz (separat erhältlich)

SafeConsole-kompatible Laufwerke vergangener Generationen: SafeStick, Safe2Go, DataTraveler Vault 3.0, IronKey D300M, Sentry 3 FIPS, Sentry 3.0, Sentry FIPS

FLEXIBLE BEREITSTELLUNGSOPTIONEN

CLOUD SERVICE

- In wenigen Minuten einsatzbereit
- Log-In und Verwaltung von jedem Ort aus
- Support per Email- und Telefon
- Preis pro Laufwerk und Jahr zzgl. einer einmaligen Setup-Gebühr

ON-PREM INSTALLATION

- Benötigt einen dedizierten Windows Server
- Log-In und Verwaltung von jedem Ort aus
- Geringe Anforderungen an Hardware und Bandbreite
- Ideal für die Verwaltung von 300 oder mehr Laufwerken

Besuchen Sie
datalocker.com/safeconsole
 für weitere Details, Demos und
 Preisinformationen.

PCI COMPLIANCE

Die für SafeConsole Cloud genutzten Datacenter wurden nach nationalen und/oder internationalen Sicherheitsstandards zertifiziert.

SafeConsole Cloud ist eine Single-Tenant-Lösung, bei der für jeden Kunden ein eigener, virtueller Server verwendet wird. Dabei werden keine Daten von den USB-Laufwerken in der Cloud gespeichert. Lediglich die Management-Konsole selbst wird in der Cloud gehostet.

ARTIKELNUMMERN

Hier finden Sie die SafeConsole-Artikelnummern:
datalocker.com/safeconsole/#_scpartnumbers

KONTAKT ZUM VERTRIEB

🌐 datalocker.com
 ✉ emea@datalocker.com
 ☎ +49 21 91 437 9702