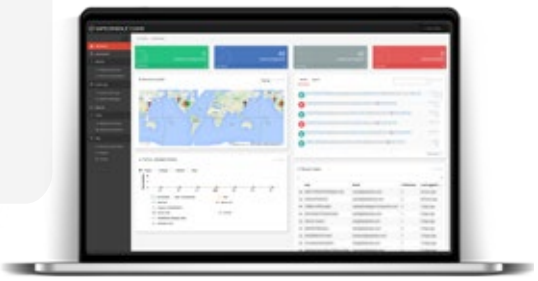
SAFECONSOLE®
USB-DEVICE-MANAGEMENT PLATTFORM

VERWALTEN SIE ALLE

SAFECONSOLEReady®

ENDGERÄTE IN EINER SICHEREN KOMMANDOZENTRALE.



DAMIT SIE STETS WISSEN WO SICH IHRE VERTRAULICHEN DATEN BEFINDEN

Durch DataLocker Verschlüsselungslösungen können vertrauliche Daten bei Transport, Speicherung und Austausch geschützt werden. Und zusätzlich ermöglicht die SafeConsole® die zentrale Verwaltung der Endgeräte, ganz gleich wo sie sich gerade befinden.

SafeConsole ist die sichere Kommandozentrale für verschlüsselte Endgeräte, die u. a. die externen verschlüsselten Festplatten DL3 und DL3FE, den verschlüsselten USB Stick Sentry®3 FIPS und bald auch die Cloud Verschlüsselungslösung SafeCrypt®, sowie die selbst-verschlüsselnden optischen Medien EncryptDisc® unterstützt. Weitere SafeConsoleReady® Endgeräte sind von unseren Partnern Kingston® Technology und CardWave® erhältlich.*

SafeConsole® ist die ideale Lösung für mobile Mitarbeiter, die an mehreren Standorten auf vertrauliche Daten oder geistiges Eigentum Zugriff haben sollen. SafeConsole® erlaubt dabei sowohl kleineren Unternehmen, als auch sehr großen Organisationen die effiziente und transparente Administration und Kontrolle Ihrer verschlüsselten Endgeräte.

LEISTUNGSMERKMALE VON SAFECONSOLE

Inventarisierung. Überwachen Sie weltweit alle verschlüsselten Endgeräte inklusive ihres Aufenthaltsortes. Active Directory wird zur einfachen Nachverfolgung der Benutzer, sowie ihrer Geräte und Computer unterstützt (OnPrem Version).

Audit. Sehen Sie jederzeit welche Dateien auf Ihren DataLocker Endgeräten gespeichert oder gelöscht wurden. Sie haben Zugriff auf ein komplettes Audit-Protokoll zur Beobachtung von Nutzeraktivitäten inklusive Verbindungen, fehlgeschlagenen Anmeldungen, wiederhergestellten Passwörtern und Verlustberichten.

Kontrolle. Setzen Sie Ihre Sicherheitsrichtlinien, wie z. B. Passwortregeln, Dateityp- oder geographische Beschränkungen, usw. durch. Passwörter können zurückgesetzt, der Nur-Lesen-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 eingesetzten, verschlüsselten Endgeräte. Wählen Sie aus Berichten, welche Konfiguration, geographischen Standort, Status, Aktualisierungen, letzte Aktivität und vieles mehr enthalten.

ZUSÄTZLICHE LEISTUNGSMERKMALE

GEOLOCATION AND GEOFENCING

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

EINFACHE UND SCHNELLE BEREITSTELLUNG

SafeConsole erlaubt eine einfache Integration für kleine und große Organisationen, auch unter Verwendung von Active Directory (AD). Administratoren können sich mit Ihren AD Benutzerdaten anmelden. Nach der Einrichtung von SafeConsole werden den Anwendern dann sichere USB-Laufwerke zugeordnet. Jedes Endgerät ist dabei mit einem eindeutigen Nutzer in der SafeConsole, sowie mit dem Nutzer im Unternehmensverzeichnis (falls vorhanden) verbunden.

PUBLISHER

Hierdurch können Administratoren portable Applikationen oder Inhalte auf den verschlüsselten Bereich des Endgerätes übertragen und somit stets aktuell halten.

ZONE-BUILDER

Nach der Installation eines sicheren Zertifikates werden PCs als vertrauenswürdige Systeme erkannt und erlauben zusätzliche Merkmale in Bezug auf Sicherheit und Benutzerfreundlichkeit:

RESTRICT ermöglicht die Verwendung von USB-Laufwerken nur an vertrauenswürdigen Systemen.

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

ANTI-MALWARE

In Partnerschaft mit McAfee kann optional ein Anti-Malware Schutz integriert werden, 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 gereinigt wurden.

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

Powered by McAfee

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

DATALOCKER®
SIMPLY SECURE

SAFECONSOLE®
USB-DEVICE-MANAGEMENT PLATTFORM

ZENTRALE VERWALTUNG VON LAUFWERKSNUTZUNG, PASSWÖRTERN UND MEHR

Überwachen Sie den Zugriff auf und die Verwendung von USB-Laufwerken durch eine Vielzahl flexibler Sicherheitsrichtlinien.

- Setzen Sie Laufwerks-spezifische Regeln für Passwortlänge und -komplexität, sowie die Passwort-Änderungsfrequenz durch.
- Ermöglichen Sie Helpdesk-Personal die unkomplizierte Remote-Unterstützung von Anwendern, die Ihr Passwort vergessen haben.
- Beschränken Sie die Verwendung von USB-Laufwerken auf ausgewählte Systeme durch Whitelisting von IP-Adressen oder Adressbereichen.
- Sperren oder löschen Sie Laufwerke, setzen Sie Passwörter zurück, Aktualisieren Sie Richtlinien, Erzwingen Sie einen Nur-Lesen-Modus - alles remote von der SafeConsole aus!
- Aktivieren und Verwalten Sie die optionale McAfee Anti-Malware Software auf einigen ausgewählten oder auf allen USB-Laufwerken.
- Sehen Sie jederzeit welche Dateien auf Ihren DataLocker Endgeräten gespeichert oder gelöscht wurden.
- Bestimmen Sie die Dateitypen, die auf den verwalteten Laufwerken gespeichert werden dürfen.

UNTERSTÜTZTE SAFECONSOLEREADY® LAUFWERKE

Kingston DataTraveler Vault Privacy 3.0 und DataTraveler 4000 G2 (managebar)
Schützen Sie sensible Unternehmensdaten mit 256bit AES-Verschlüsselung und FIPS-140-2 Zertifizierung (DT4000G2).

DataLocker DL3 and DL3 FE Festplatten
Diese beiden externen USB Festplatten haben einen neuen Standard für Hardware-verschlüsselte portable Massenspeicher gesetzt. Weder Software noch Treiber werden benötigt um die Laufwerke einzurichten, zu verschlüsseln und zu verwalten.

DataLocker Sentry 3 FIPS USB-Flash Laufwerk
Sentry 3 FIPS bietet neben DataLockers zertifizierter und erprobter Technologie eine FIPS-140-2 Level 3 Zertifizierung, sowie eine Hardware-basierte 256bit AES-Verschlüsselung.

*Vorgängermodelle, die mit SafeConsole kompatibel sind: Sentry 3.0, Sentry FIPS

FLEXIBLE BEREITSTELLUNG IN DER CLOUD ODER ONPREMISES

CLOUD-HOSTED SERVICE

- Keine Server Hardware-Investitionen oder Wartung
- In wenigen Minuten einsatzbereit
- Log-In und Verwaltung von jedem Ort aus
- Preis pro Endgerät und Jahr zzgl. einmaliger Setup-Gebühr

ON-PREM

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

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

Unseren Verkauf erreichen Sie per Email unter emea@datalocker.com oder Sie besuchen datalocker.com/contact-us