



MISSION STATEMENT

DataLocker's motto is "Simply Secure"

To provide easy to use, cost effective, military grade data encryption solutions to enterprises around the world.



- DataLocker products are developed and engineered in house since 2007.
- All products are TAA Compliant, meeting federal and military requirements.

THE WORLD'S MOST DEMANDING ORGS TRUST DATALOCKER

LEGAL



ENTERPRISE



GOVERNMENT



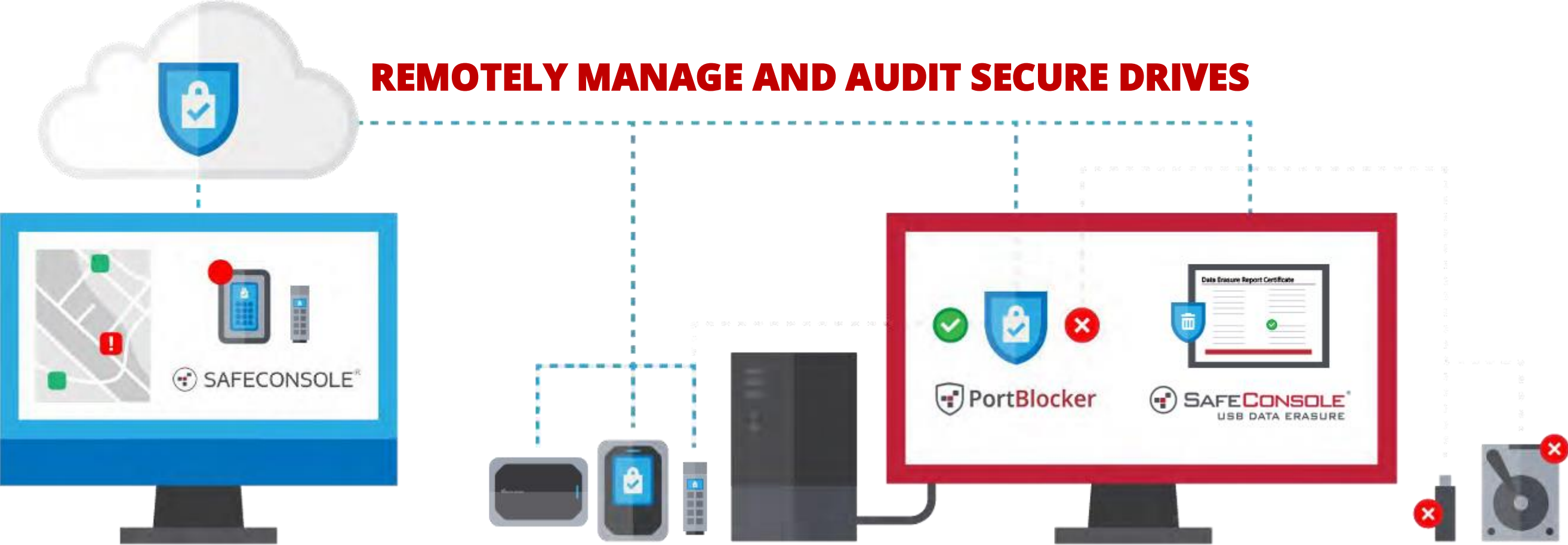
HEALTHCARE



FINANCIAL



THE DATALOCKER SOLUTION



SafeConsole Device Management

Encrypt data on an encrypted drive and make sure nobody but the right people can access it.

PortBlocker

Ensure that users only use approved USB devices to prevent malware intrusion.

Certified Data Erasure

Certified, cryptographic data sanitization for secure device decommissioning and lifecycle closure.

Built-In Anti-Malware

Automatically scan data for viruses and malware before its stored-on device.

Powered by **Trellix**

DL GO ENCRYPTED FLASH DRIVE

Simple. Secure. Affordable.





DL GO BENEFITS

SECURE



**FIPS 197 Certified
Hardware-based
AES 256-bit XTS
mode encryption**

DURABLE



**IP68: Tamper-
evident seal and
waterproof up to
6.5ft**

EFFORTLESS



**Biometric
Authentication
(optional)**

CONTROL



**Remotely Manage:
SafeConsole Enterprise
or MySafeConsole (SMB)**

FEATURES



Built-In Protection, No Setup Required

DL GO delivers enterprise-grade security with instant-on encryption—no drivers, no software installs, and no IT involvement.

- AES 256-bit XTS hardware encryption (FIPS 197 certified)
- Optional biometric unlock (Windows Hello, Touch ID)
- IP68 waterproof and tamper-evident casing
- Works on Windows, macOS, Linux (no software required)



Visibility & Control Without Complexity

Even unmanaged, DL GO provides essential user protections and secure file handling.

- Optional read-only mode to block malware or ransomware
- Easy-to-use interface for strong password creation
- USB 3.2 Gen 1 speeds for fast data transfer



Remote Management Made Easy

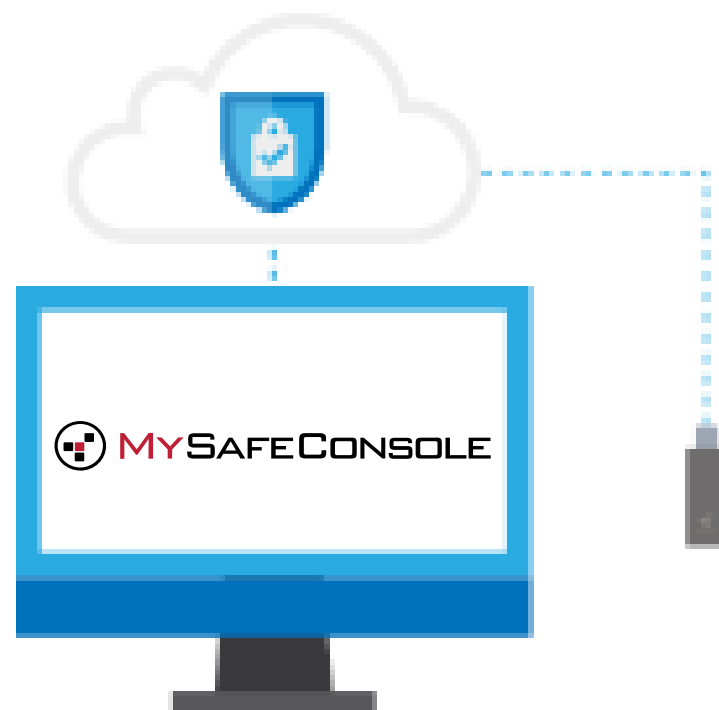
DL GO helps reduce risk, prove compliance, and maintain control – even without a dedicated IT team.

- View audit logs for device usage, file changes, and access history
- Enforce strong password policies and MFA
- Track device health, user activity, and security posture
- Set geofences or restrict IP with SafeConsole Enterprise

CENTRALIZED MANAGEMENT

MySafeConsole

- Password recovery
- Device usage history
- Security updates
- Option malware protection (Plus/Pro)
- Cloud-Only



SafeConsole Enterprise

- Centralized policy enforcement
- Detailed compliance audit logging
- Geofencing
- API integration
- Cloud or On-Prem deployments



DL GO FEATURE SUMMARY

CORE FEATURES

FIPS 197 CERTIFICATION

AES 256-bit XTS hardware encryption (FIPS 197 certified)



RUGGED DESIGN

Metal body, IP68 waterproof, tamper-evident seal



AUTHENTICATION

Optional biometric login + strong password support



COMPLIANCE READY

TAA compliant, meets GDPR, HIPAA, ISO 27001 standards



REMOTE MANAGEMENT

MANAGEMENT OPTIONS

MySafeConsole (individuals/SMBs) or SafeConsole Enterprise (advanced control)



PASSWORD RECOVERY

Remote recovery through secure cloud portal



REMOTE ACTION

Lock, wipe, detonate, or reassign devices



AUDIT CAPABILITIES

Track device usage, policy enforcement, file activity logs



USE CASES

Small Businesses

Simple, Centralized Device Management for Growing Teams



- **Problem:** Small businesses often lack dedicated IT teams but still need to protect data as it moves between employees, offices, and devices.
- **Solution:** DL GO with MySafeConsole delivers secure, encrypted storage with optional cloud-based management—no IT setup required.
- **Why DataLocker:** Enterprise-grade encryption and password recovery tools at a small business price, with zero technical overhead.

Non-Profit

Secure, Affordable Devices for Budget-Conscious Environments



- **Problem:** Non-profits are budget-conscious but still handle sensitive data about the communities they serve.
- **Solution:** DL GO provides affordable, hardware-encrypted USB storage with free MySafeConsole management for basic security control.
- **Why DataLocker:** A cost-effective way to safeguard personal and community data without compromising mission-critical funds.

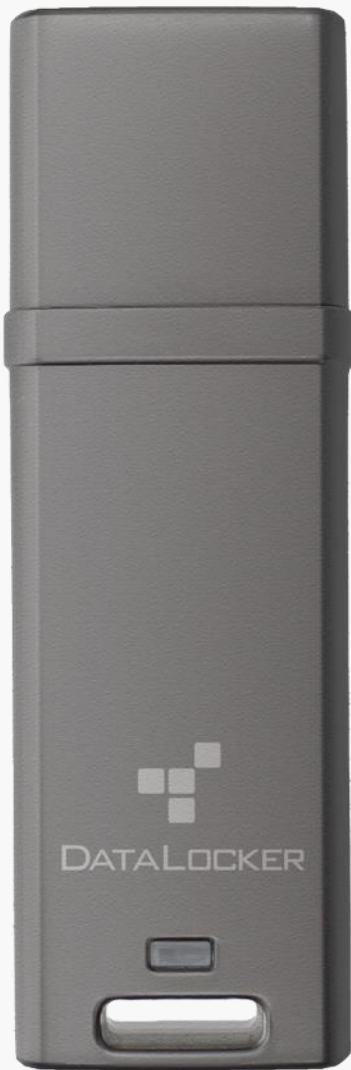
Legal

Advanced Security and Affordable Devices



- **Problem:** Legal teams need a simple, secure way to store and assign case files without overspending on high-end hardware.
- **Solution:** DL GO offers secure, password-protected USB drives that can be easily assigned per case and centrally managed if needed.
- **Why DataLocker:** Trusted, compliant encryption with flexible management—perfect for sensitive client data at scale and on budget.

SPECS



CAPACITIES

4GB, 16GB, 64GB

DIMENSIONS

L: 55.8mm (2.19 in)
W: 18.6 mm (.73 in)
D: 9.6 mm (.38 in)

WEIGHT

26 grams / 0.9 oz

STANDARDS AND CERTIFICATION

FIPS 197
TAA Compliance
FCC
CE
KCC
RoHS & WEEE

SYSTEM COMPATIBILITY

Windows and Mac OS. Limited capability on Linux. USB 3.0/USB 3.1/USB 3.2 Gen 1 compliant and 2.0 compatible.

CRYPTOGRAPHIC PROCESS

AES 256-bit XTS hardware encryption onboard

INTERFACE

USB 3.2 Gen (Type A)
USB-C accessory available for purchase

TEMPERATURE

Operating: 0°C to 70°C
Storage: -25° to 85°C

TRANSFER SPEEDS

USB 3.2 GEN 1:
4GB: 15MB/s READ,160MB/s WRITE
8GB &16GB: 160MB/s READ, 120MB/s WRITE

USB 2.0:
8GB–128GB: 30MB/s READ, 20MB/S WRITE

WATERPROOF

Up to 4ft: Conforms to IEC 60529 IPX8.
Product must be clean and dry before use

PART NUMBERS

DLGO-004
DLGO-016
DLGO-064
Available as optionally managed with a SafeConsole license (sold separately) or a MySafeConsole account.

WARRANTY

5-year limited warranty out of the box

1 Some of the listed capacity on a Flash storage device is used for formatting and other functions and thus is not available for data storage. As such, the actual available capacity for data storage is less than what is listed on the products.
2 Online management features not available for Linux.
3 Speed may vary due to host hardware, software and usage.

DATALOCKER MySafeConsole

Remote Device Management
Made Easy



MYSAFECONSOLE



Secure Password Recovery

Never lose access to your encrypted USB drive – even if you forget your password.



Remote Lock & Wipe

Protect your data instantly if a device is lost or stolen, with cloud-based controls.



Simple Cloud Management

Manage devices from anywhere with an easy-to-use dashboard – no IT required.



Optional, Not Overwhelming

Get powerful security features when you need them, with no impact on daily device use.

MYSAFECONSOLE FEATURES ON WINDOWS AND MAC OS

BASIC FEATURES

- ❑ Drive Password Recovery
- ❑ Limited Audit Logging
- ❑ Google SOO
- ❑ Biometric Login

PLUS FEATURES

EVERYTHING IN BASIC AND:

- ❑ Up to 5 Devices
- ❑ ANTI-MALWARE FOR SECURE USB
 - On-Board device Trellix® anti-malware
 - Automatically delete or remove malware on device
 - Real-time reporting on infected files and devices

PRO FEATURES

EVERYTHING IN PLUS AND:

- ❑ Up to 50 Devices
- ❑ File Type Restrictions
- ❑ Detailed File Audit Loggins
- ❑ Role-Based Permissions

USE CASES



Individuals

Protecting Personal Records

- **Use Case:** An individual wants to securely store sensitive personal documents—like tax returns, legal records, health history, or wills—on an encrypted USB drive. If the drive is lost or the password is forgotten, their data could be permanently inaccessible.
- **How MySafeConsole Helps:** By registering the DL GO drive with MySafeConsole, the user enables secure password recovery and can lock or wipe the device remotely if it's ever lost. They get peace of mind knowing their sensitive records are protected—without needing IT support.
- **Value:** Personal security, simplified. No subscriptions, no setup headaches—just always-on encryption and recovery access when it matters most.



Small Businesses

Affordable USB Without IT

- **Use Case:** A small business with no dedicated IT team needs a way to distribute encrypted USB drives to employees for transferring customer data, financial files, or contracts between devices or offices.
- **How MySafeConsole Helps:** Each DL GO drive can be registered and managed through MySafeConsole, enabling password resets, usage tracking, and remote locking in case a drive is misplaced. All of this is available through a simple cloud dashboard—no server setup, no technical expertise required.
- **Value:** MySafeConsole delivers essential USB device control and security features to small businesses—**without enterprise-level complexity or cost.**



Non-Profit

Low-Cost Data Protection for Sensitive Documents

- **Use Case:** A nonprofit organization collects and stores sensitive information about the communities it serves—including beneficiary records, internal reports, or donor information. They need secure portable storage, but budgets are limited.
- **How MySafeConsole Helps:** DL GO offers strong encryption at a low cost, and MySafeConsole provides free, optional device management that allows the organization to remotely reset passwords, track usage, and lock lost drives—all from a cloud interface that doesn't require technical knowledge or IT infrastructure.
- **Value:** Mission-driven organizations get enterprise-grade protection for sensitive data—while keeping overhead low and operations focused on impact.



DL450 FE OPTIMIZED SECURITY

Easy to use encrypted drive with
Flexible Authentication Options*

* Smart Card Authentication requires SafeConsole and Device Management license (sold separately)

COPYRIGHT DATALOCKER 2026

ENCRYPTION & PHYSICAL SECURITY

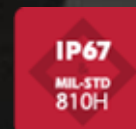
 DATALOCKER



FIPS-140-3 Level 3 (pending)* with hardened enclosure and internals



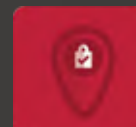
AES 256-bit XTS cryptographic module



Built for any environment - IP67 and Mil-STD 810H



Brute force password protection



Location-based security posture and on-board Antimalware (requires SafeConsole)



Flexible authentication, including Windows Hello/Touch ID or CAC, PIV, and YubiKey PIV (Smart card requires SafeConsole)

*The DL450 FE is a form-factor variant of the DL4 FE and uses the same FIPS 140-3 Level 3 validated cryptographic module architecture as the DL4 FE. DL450 FE validation is [pending](#).





FIPS 140-3 LEVEL 3 (pending)

Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. The DL450 FE is a form-factor variant of the DL4 FE and utilizes the same FIPS 140-3 Level 3 validated cryptographic module architecture.



REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

MODELS: Basic and Enterprise



THE DL450 FE STANDARD

Configure in seconds, secure data forever.



THE DL450 FE MANAGED SAFECONSOLE REQUIRED

All standalone features plus the ability to remotely manage a fleet of devices via SafeConsole.

FEATURES

DL450 FE BASIC

FIPS 140-3 LEVEL 3 CERTIFICATION Pending

True device level 3 pending with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. The DL450 FE is a form-factor variant of the DL4 FE and utilizes the same FIPS 140-3 Level 3 validated cryptographic module architecture. DL450 FE validation and certificate update is pending.

STRONG PASSWORDS POLICIES

Set rigorous password policies like using non-sequential, non-repeating characters, special characters and minimum character counts.

BRUTE FORCE PASSWORD PROTECTION

When in use, admins can configure how many failed password attempts are needed before the device destroys its payload.

NOTHING TO INSTALL

All encryption, administration, and authentication performed on the DL450 FE unit. (macOS requires a one-time driver installation with elevated privileges. Driver is bundled with on-board software for easy guided setup or can be mass-deployed via network management tools.)

MANAGED DL450 FE ENTERPRISE

ON BOARD ANTI-MALWARE

Automatically scans files and quarantines/destroys bad apps/files based on policy settings (optional upgrade. Requires SafeConsole).

REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

FLEXIBLE AUTHENTICATION

Supports password and biometric (Windows Hello/Touch ID) authentication; Managed edition adds smart card support (CAC, PIV, YubiKey – requires SafeConsole).

CERTIFIED DATA ERASURE

Verifiable erasure, automated certification, and centralized reporting. Requires SafeConsole).

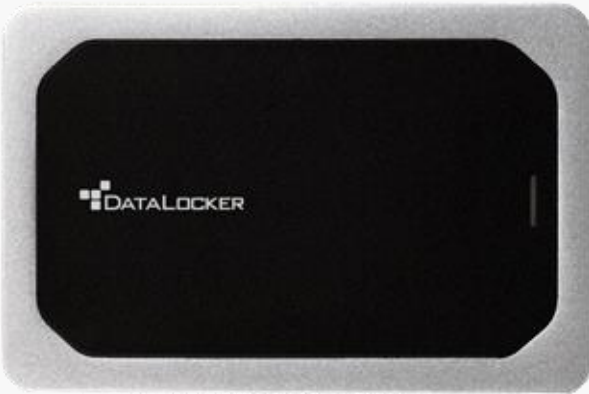
DATA GEOFENCING

SafeConsole uses geofencing, trusted networks, and ZoneBuilder to ensure a device changes its security posture based on its location (Admin configurable. Requires SafeConsole).

COMPREHENSIVE AUDIT CAPABILITIES

Have a complete record of file activity (including name changes on the device), password attempts, device locations and machines, device health, and policies in force (Admin configurable. Requires SafeConsole).

SPECS



CAPACITIES

SSD: 1 TB, 2 TB, 4 TB, 7.6 TB, 15.3 TB
HDD: 1 TB, 2 TB

DIMENSIONS

L: 12.3 cm W: 7.7 cm H: 2.1 cm
L: 4.8" W: 3" H: 0.82"

WEIGHT

.65 lb / 294 grams and up

TEMPERATURE

Operating: 0°C to 60°C
Storage: -20°C to 60°C

PHYSICAL SECURITY

Kensington® Security Slot Hardened
internals and enclosure

CRYPTOGRAPHIC PROCESS

FIPS 140-3 Level 3 pending*
AES 256-bit XTS hardware
encryption onboard

INTERFACE

USB-C on the device, compatible
with USB 3.2, USB 2.0 (7.6TB
drives & under)
15.3TB requires USB Type-C
(15W+) - to use on hosts with USB
A, a powered USB-A hub with
USB-C ports is required.
(USB-C to USB-A cable with USB-
A to USB-C adapter included)

AVERAGE TRANSFER SPEEDS

SSD version USB-C 3.2: 250 MB/s
read, 250MB/s write
HDD version USB-C 3.2: 150 MB/s
read, 100MB/s write
Instantly sanitize the DL4 storage
media with cryptographic erase
(NIST SP 800-88) in seconds**.

**STANDARDS AND
CERTIFICATION**

FIPS 140-3 Level 3* Validated TAA
Compliance, NATO-trusted
supply chain
IP67 and Mil-STD 810H Certified

COMPATIBILITY

Compatible with Windows® and
macOS® (Note: macOS requires
a one-time driver installation
with elevated privileges. Driver is
bundled with on-board software
for easy guided setup or can be
mass-deployed via network
management tools for no end-
user impact.)
USB 3.2 Gen 1 compliant and 2.0
compatible

DEVICE LANGUAGES

English, French, German, Spanish,
Japanese, Korean, Traditional
Chinese, and Simplified Chinese

PART NUMBERS

Standard (optional
managed)
DL450-1TB-FE
DL450-2TB-FE
DL450-SSD-1TB-FE
DL450-SSD-2TB-FE
DL450-SSD-4TB-FE
DL450-SSD-7.6TB-FE
DL450-SSD-15.3TB-FE
Managed (forced
managed) ***
DL450-1TB-FE-M
DL450-2TB-FE-M
DL450-SSD-1TB-FE-M
DL450-SSD-2TB-FE-M
DL450-SSD-4TB-FE-M
DL450-SSD-7.6TB-FE-M
DL450-SSD-15.3TB-FE-M

WARRANTY

3-year limited warranty

*The DL450 FE is a form-factor variant of the DL4 FE and uses the same FIPS 140-3 Level 3 validated cryptographic module architecture as the DL4 FE. DL450 FE validation is pending.

**Requires a Certified Data Erasure license (sold separately)

***Requires SafeConsole and a device management license (sold separately)



DL4 FE SECURE TO THE CORE

Our easiest to use, most secure,
and highest-capacity drive yet



ENCRYPTION & PHYSICAL SECURITY



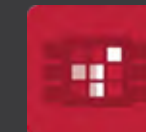
FIPS-140-3 Level 3 device validation with hardened enclosure and internals



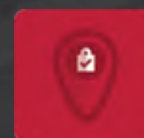
AES 256-bit XTS cryptographic module



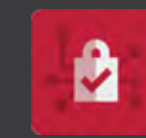
Common Criteria EAL5+ validation



Brute force password protection & randomizing keypad



Location-based security posture and on-board Antimalware (requires SafeConsole)



Admin Policies and User Data Recovery



**Powerful Encryption
Right Out of the Box**



**Never Risk Losing
Your Data**



**Ensure User Adoption
With Easy-to-Use
Touchscreen**



**Remotely Manage and
Audit Your Entire Fleet**



COMPLIANCE



FEATURE CALL-OUT



FIPS 140-3 LEVEL 3

True device level 3 certification with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Hardened internals and enclosure for increased physical security.



SILENT KILL

Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).



REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

MANAGEMENT



THE DL4 FE

Configure in seconds,
secure data forever.



THE DL4 FE MANAGED BY SAFECONSOLE

All standalone features plus the
ability to remotely manage a fleet of
devices via SafeConsole.

FEATURES

DL4 FE FEATURES

FIPS 140-3 LEVEL 3 CERTIFICATION

True device level 3 certification with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Hardened internals and enclosure for increased physical security.

SILENT KILL™

Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).

STRONG PASSWORDS POLICIES

Set rigorous password policies like using non-sequential, non-repeating characters, special characters and minimum character counts.

ADMIN POLICIES & USER DATA RECOVERY

Admins can set rigorous password policies (non-sequential, non-repeating special characters, minimum characters). Should users forget a password, admins can unlock the DL4 FE using the admin password. Admins can also recover the user's data by logging in with the admin password. The user will be forced to reset their password upon their next use.

BRUTE FORCE PASSWORD PROTECTION

When in use, admins can configure how many failed password attempts are needed before the device destroys its payload.

NOTHING TO INSTALL

All encryption, administration, and authentication performed on the DL4 FE unit. This means devices in standalone mode don't require a software agent; they work right out of the box.

MANAGED DL4 FE FEATURES

ON BOARD ANTI-MALWARE

Automatically scans files and quarantines/destroys bad apps/files based on policy settings (optional upgrade. Requires SafeConsole).

REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

CERTIFIED DATA ERASURE

Verifiable erasure, automated certification, and centralized reporting. Requires SafeConsole).

DATA GEOFENCING

SafeConsole uses geofencing, trusted networks, and ZoneBuilder to ensure a device changes its security posture based on its location (Admin configurable. Requires SafeConsole).

COMPREHENSIVE AUDIT CAPABILITIES

Have a complete record of file activity (including name changes on the device), password attempts, device locations and machines, device health, and policies in force (Admin configurable. Requires SafeConsole).

SPECS



CAPACITIES

SSD: 1 TB, 2 TB, 4 TB, 7.6 TB, 15.3 TB
HDD: 1 TB, 2 TB

DIMENSIONS

L: 12.3 cm W: 7.7 cm H: 2.1 cm
L: 4.8" W: 3" H: 0.82"

WEIGHT

.65 lb / 294 grams and up

PHYSICAL SECURITY

Kensington® Security Slot Hardened
internals and enclosure

CRYPTOGRAPHIC PROCESS

FIPS 140-3 Level 3 Validated,
Certificate #5091

AES 256-bit XTS hardware encryption onboard

Integrates a Common Criteria EAL 5+ certified secure microprocessor

INTERFACE

USB-C on the device, compatible with USB 3.2, USB 2.0 (8 TB drives and under)

(USB-C to USB-A and USB-C to USB-C cables included)

TRANSFER SPEEDS

USB C 3.2: 150 MB/s read,
100 MB/s write

USB 2.0: 40 Mb/s Read,
20 MB/s Write

STANDARDS AND CERTIFICATION

TAA Compliance
IP64 Certified
RoHS Compliant
FCC
CE

MANAGEMENT COMPATIBILITY

Microsoft Windows

OS COMPATIBILITY

Microsoft Windows, macOS®,
Linux® or any machine that
supports a USB mass storage
device

PART NUMBERS

DL4-1TB-FE
DL4-2TB-FE
DL4-SSD-1TB-FE DL4-SSD-2TB-FE DL4-SSD-4TB-FE DL4-SSD-7.6TB-FE DL4-SSD-15.3TB-FE

DEVICE LANGUAGES

English, French, German,
Spanish

WARRANTY

3-year limited warranty

TRUSTED BY



K350 SMALL FORM- FACTOR, HEAVYWEIGHT SECURITY

Our most durable and
portable drive.





THE ULTRA- DURABLE K350 **IP68-rated**

Dust, water, shock, and
vibration resistant.



K350 BENEFITS



Powerful Encryption
Right Out Of The Box



Protect Data at Scale



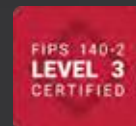
Ensure User Adoption
With Easy-to-Use Keypad



Remotely Manage &
Audit Your Entire Fleet



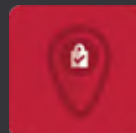
ENCRYPTION & PHYSICAL SECURITY



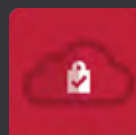
FIPS-140-3 Level 3
([Cert. #5092](#)) device
validation with
hardened enclosure
and internals



Common Criteria
EAL5+ validation



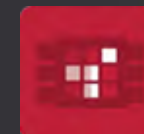
Location-based security
posture and on-board
Antimalware (requires
SafeConsole)



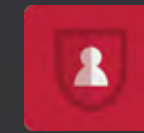
Remotely Manage &
Audit Your Entire
Fleet



AES 256-bit XTS
cryptographic module



Bruteforce password
protection &
randomizing keypad



Admin Policies and
User Data Recovery



Powerful
Encryption
Right Out Of
The Box



Protect Data at
Scale



Ensure User
Adoption With
Easy-to-Use
Keypad

EASE OF USE



**Screen
and
Keypad**



**Onboard
Customization**



Ultra-portable



**Platform
Agnostic**

COMPLIANCE



FEATURE CALL-OUT



FIPS 140-3 LEVEL 3

True device level 3 certification with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Hardened internals and enclosure for increased physical security.



SILENT KILL

Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).



REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

SAFECONSOLE MANAGEMENT PLATFORM



**Comprehensive
Audit Capabilities**



**Data
Geofencing**



**Remote Device
Detonation**



**On Board Anti-
malware
(Configurable)**



“NUCLEAR” OPTIONS



SILENTKILL™

Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).



REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

FEATURE SUMMARY

K350 FEATURES

FIPS 140-3 LEVEL 3 CERTIFICATION

FIPS 140-3 level 3 certification and pending Common Criteria EAL5+ certification. Provides always-on hardware based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Hardened internals and enclosure for increased physical security.

FULLY MANAGEABLE DEVICE

Use DataLocker SafeConsole to manage individual and groups of devices using automated policies.

ADMIN POLICIES & USER DATA RECOVERY

Admins can set rigorous password policies (non sequential, non-repeating special characters, minimum characters). Should users forget a password, admins can unlock the K350 using the admin password. Admins can also recover the user's data by logging in with the admin password. The user will be forced to reset their password upon their next use.

BRUTE FORCE PASSWORD PROTECTION

Admins can configure how many failed password attempts are needed before the device destroys its payload.

NOTHING TO INSTALL

All encryption, administration, and authentication is performed on the K350 unit. This means devices in standalone mode don't require a software agent; they work right out of the box.

MANAGED K350 FEATURES (Requires SafeConsole)

ON BOARD ANTI-MALWARE

Automatically scans files and quarantines/destroys bad apps/files based on policy settings.

REMOTE DEVICE DETONATION

Lets admins functionally destroy the device and its data remotely to protect against data or encryption key theft.

DATA GEOFENCING

SafeConsole uses geofencing, trusted networks, and ZoneBuilder to ensure a device changes its security posture based on its location.

COMPREHENSIVE AUDIT CAPABILITIES

Have a complete record of file activity (including name changes on the device), password attempts, device locations and machines, device health, and policies in force.

SPECS



CAPACITIES

16GB, 32GB*, 64GB,
128GB, 256GB, 512GB

DIMENSIONS

L: 9.98 cm (3.92 in)
W: 1.98 cm (.77 in)
D: 1.11 cm (.43 in)

WEIGHT

35 grams / .077/lbs

PHYSICAL SECURITY

IP68 rated. Hardened, epoxy sealed
internals and robust enclosure

INTERFACE

USB-A compatible with USB 3.2
Gen 1, USB 2.0

CRYPTOGRAPHIC PROCESS

FIPS 140-3 Level 3 Validated,
Certificate #5092

AES 256-bit XTS
hardware encryption
onboard

Integrates a Common Criteria
EAL 5+ certified secure
microprocessor

TRANSFER SPEEDS

190 MB/S Read/Write

BATTERY

Lithium-ion polymer charges
automatically over the powered
USB-port

**STANDARDS AND
CERTIFICATION**

FIPS 140-3 Level 3 (Cert. #5092)
TAA Compliance
IP68 Certified
MIL-STD-810G
RoHS Compliant
FCC
CE

**MANAGEMENT
COMPATIBILITY**

Microsoft Windows

DEVICE LANGUAGES

English

OS COMPATIBILITY

Microsoft Windows, macOS®,
Linux® or any machine that
supports a USB mass storage
device

**PART
NUMBERS**

SK350-016-FE
SK350-032-FE*
SK350-064-FE
SK350-128-FE
SK350-256-FE
SK350-512-FE

WARRANTY

3-year limited warranty

*32GB FIPS Pending

HARDWARE FEATURES

DL4FE & K350 FEATURES

FIPS 140-3 LEVEL 3 CERTIFICATION

True device level 3 certification with a Common Criteria EAL5+ certified controller inside. Provides always-on hardware-based encryption. Dedicated AES 256-bit XTS mode crypto engine meets rigorous cryptographic standards and is more secure than software-based alternatives. Hardened internals and enclosure for increased physical security.

SILENT KILL™

Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).

STRONG PASSWORDS POLICIES

Set rigorous password policies like using non-sequential, non-repeating characters, special characters and minimum character counts.

ADMIN POLICIES & USER DATA RECOVERY

Admins can set rigorous password policies (non-sequential, non-repeating special characters, minimum characters). Should users forget a password, admins can unlock the DL4 FE using the admin password. Admins can also recover the user's data by logging in with the admin password. The user will be forced to reset their password upon their next use.

BRUTE FORCE PASSWORD PROTECTION

When in use, admins can configure how many failed password attempts are needed before the device destroys its payload.

NOTHING TO INSTALL

All encryption, administration, and authentication performed on the DL4 FE unit. This means devices in standalone mode don't require a software agent; they work right out of the box.

MANAGED DL4FE & K350 FEATURES

ON BOARD ANTI-MALWARE

Automatically scans files and quarantines/destroys bad apps/files based on policy settings (optional upgrade. Requires SafeConsole).

REMOTE DEVICE DETONATION

Let's admins functionally destroy the device and its data remotely to protect against data or encryption key theft (Admin configurable. Requires SafeConsole).

DATA GEOFENCING

SafeConsole uses geofencing, trusted networks, and ZoneBuilder to ensure a device changes its security posture based on its location (Admin configurable. Requires SafeConsole).

COMPREHENSIVE AUDIT CAPABILITIES

Have a complete record of file activity (including name changes on the device), password attempts, device locations and machines, device health, and policies in force (Admin configurable. Requires SafeConsole).



SENTRY 5 HARDWARE ENCRYPTED USB





SENTRY 5 BENEFITS



FIPS 140-3 Level 3 Validated

Password protected
with hardware-based
AES 256-bit XTS mode
encryption



**MIL-STD-810F and
IP68 certified,**
extremely rugged solid zinc
metal casing encapsulated in
FIPS 140-3 tamper-resistant
epoxy



**Flexible authentication
options** Supports password and
biometric (Windows Hello/Touch
ID) authentication or smart card
support (CAC, PIV, YubiKey PIV)

SECURE USB FLASH DRIVE FOR COMPLIANCE



PASSWORD PROTECTED

Requires a mandatory password in included portable device software, verified in hardware, before accessing hardware encrypted files



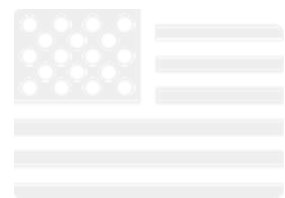
RUGGEDIZED AND WATERPROOF

Solid zinc metal casing sealed with tamper-resistant epoxy. IP68 certified: up to 6.5 feet of water (2.0 meters) and MIL-STD-810F certified: crash, drop, shock, vibration, and immersion



READ-ONLY MODE

Read-Only Mode to combat ransomware



ASSEMBLED IN USA



ENFORCED MANAGEMENT

With a SafeConsole® license (sold separately), this solution is optimized for large organizations utilizing SafeConsole device management. It includes features such as automated inventory, policy enforcement, auditing, and offers integration options with API, SIEM, and SSO. Available as an On-Premises and SaaS



WARRANTY

5-year device warranty out of the box

SECURE USB FLASH DRIVE FOR COMPLIANCE



SIMPLY SECURE

Digitally signed firmware, making it immune to BadUSB



DATALOCKER UPDATES

Gain immediate access to the most current DataLocker device software releases, ensuring a comprehensive and up-to-date solution



SYSTEM COMPATIBILITY

Compatible with Windows® and macOS®. Limited capability on Linux



SUSTAINABLE PACKAGING

Eco-friendly paper packaging



INTERFACE

USB 3.2 Gen 1 (type A), USB-C accessory available for purchase (SKU# CBLUSBAFCM)



CONSISTENCY

Internal and external serial number matching

MANAGED BY SAFECONSOLE® FEATURES

The Sentry 5 is manageable by SafeConsole. Requires separate SafeConsole license.



INTEGRATED INVENTORY

Automated device/user inventory



ON BOARD ANTI-MALWARE

Portable Trellix™ Enterprise Anti-malware
(sold separately)



COMPREHENSIVE AUDIT CAPABILITIES

Device and file audit for compliance



CUSTOM CONTROL

Custom device policies for password
and usage



SMART CARD AUTHENTICATION ENFORCEMENT

(CAC, PIV, YubiKey PIV), including optional
smart card-only access



CERTIFIED DATA ERASURE

Certified, cryptographic data sanitization
for secure device decommissioning and
lifecycle closure (sold separately)

SPECS



CAPACITIES

8GB, 16GB, 32GB, 64GB, 128GB, 256GB, 512GB

DIMENSIONS

L: 3.13 inches (79.5 mm) W: 0.79 inch (20 mm)
D: 0.39 inch (10 mm)

WEIGHT

1.76 oz (50 grams)

CRYPTOGRAPHIC PROCESS

FIPS 140-3 Level 3
Validated, [Cert #5140](#)

Password protected with hardware-based AES 256-bit XTS mode encryption
PROCESS

TEMPERATURE

Operating: 0°C to 50°C
Storage: -20°C to 85°C

INTERFACE

USB 3.2 Gen 1 (type A), USB-C accessory available for purchase (SKU# CBLUSBAFCM)

TRANSFER SPEEDS

8GB – 128GB: 260MB/s read, 190MB/s write

256GB: 240MB/s read, 170MB/s write

512GB: 310MB/s read, 250MB/s write

USB 2.0

8GB – 512GB: 30MB/s read, 20MB/s write

DEVICE LANGUAGES

English, French, Spanish, German, Japanese, Korean, Traditional Chinese, and Simplified Chinese

SYSTEM COMPATIBILITY

Compatible with Windows® and macOS®. Limited capability on Linux
USB 3.0/USB 3.1/USB 3.2 Gen 1 compliant and 2.0 compatible

STANDARDS AND CERTIFICATION

FIPS 140-3 Level 3 TAA-compliant
UKCA
FCC
CE
KC
Wee
Canada ICES
RCM (Australia/NZ)
Taiwan BSMI, RoHS
Japan VCCI
China RoHS
IP68 & MIL-STD-810F
NIST 800:88

RUGGEDIZED, DUST & WATERPROOF

IP68 (up to 6.5 feet of water, 2.0 meters), MIL-STD-810F certified: crash, drop, shock, vibration, immersion
Product must be clean and dry before use.
Solid zinc metal casing sealed with tamper-resistant epoxy

PART NUMBERS

S5-008-FE-M
S5-016-FE-M
S5-032-FE-M
S5-064-FE-M
S5-128-FE-M
S5-256-FE-M
S5-512-FE-M

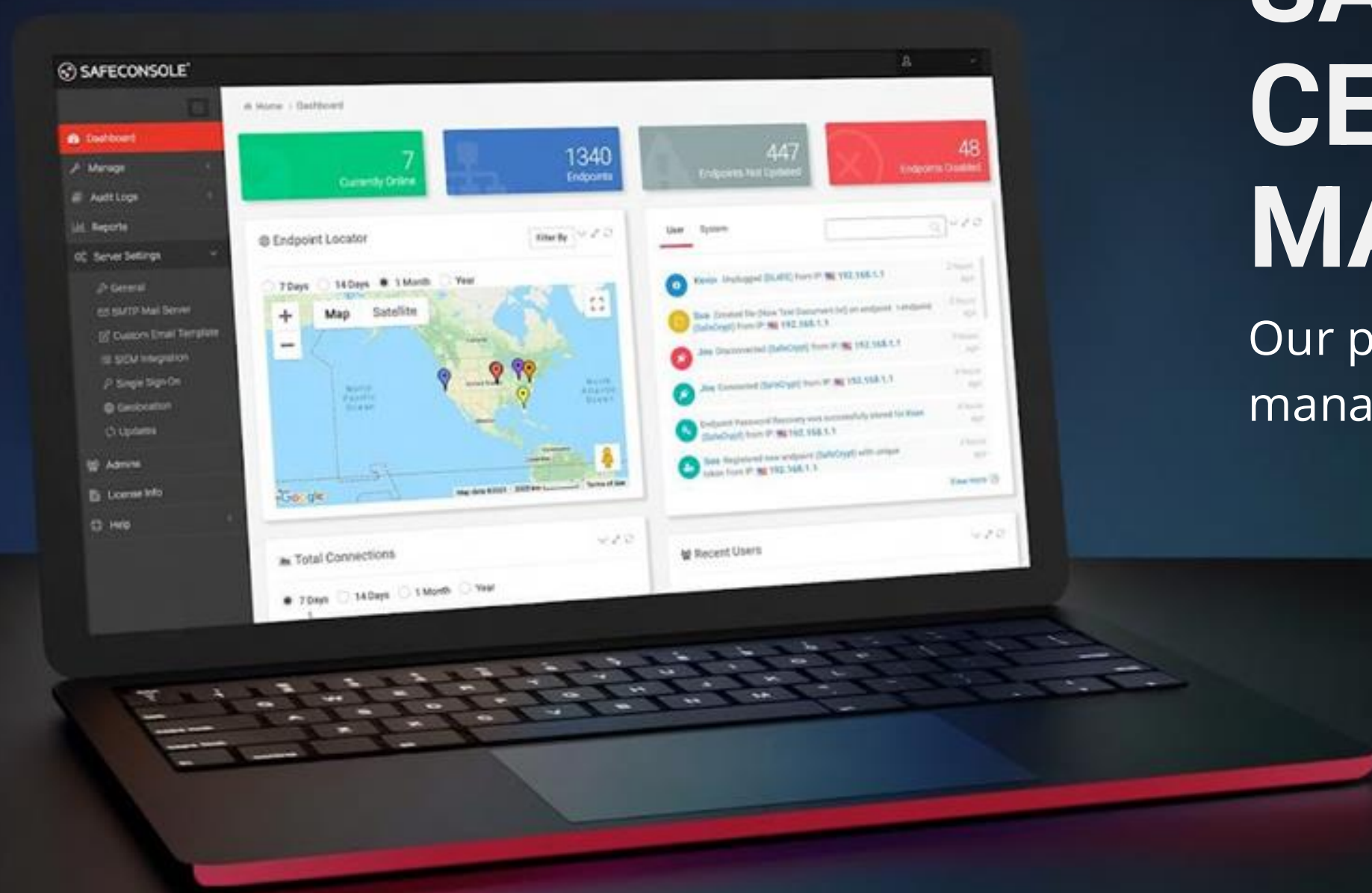
Available as forced managed (-M) with a SafeConsole® license (sold separately).

WARRANTY

5-year device warranty out of the box

DATALOCKER SAFECONSOLE CENTRAL MANAGEMENT

Our powerful, secure system to
manage your devices



SAFECONSOLE



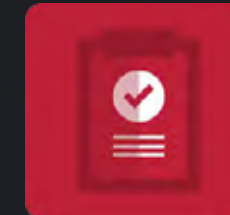
Enhance security for portable USB drives and workstation USB ports



Reduce time spent deploying and managing secure USB drives



Make tracking and compliance for secure USB drives simple with sophisticated auditing and reporting tools



Keep your workforce productive with easy-to-use devices and dynamic security postures

SAFECONSOLE MANAGEMENT PLATFORM

DEPLOY AS CLOUD (SAAS) OR ON-PREM*



Remotely provision, configure, manage, and audit your fleet of encrypted USB drives, while also unlocking powerful security features for DataLocker drives



Certified, cryptographic data sanitization for secure device decommissioning and lifecycle closure



On-board Trellix® anti-malware is always on to scan files on secure USB drives, remove or quarantine malware threats, and report information back to SafeConsole



Ensure that your workforce only uses approved USB devices to prevent malware intrusion or accidental file loss



*Uses Windows Installer, which can work from bare metal, virtual images or any cloud, including private clouds

FEATURES

SAFECONSOLE CLOUD/ON PREM FEATURES ON WINDOWS AND MAC OS

COMPLETE CENTRAL MANAGEMENT AND CONTROL FOR ADMINISTRATORS

USB DEVICE MANAGEMENT FOR SECURE USB

- Password policy configuration
- Automatic inventory directory of all users and devices
- Audit trail of device actions and file movements for compliance
- Remote password reset
- Managed standalone logins on Linux or any machine
- Remotely detonate (permanently destroy) device
- Remote factory reset/disable/deny access/set-as-lost
- Set to audit mode (restrict access and disable edits)
- Remotely re-assign device to new user
- Inactivity lock
- Write-protection (managed read-only)
- File restrictions (disallow/allow file extensions)
- Geofence (based on host IP)
- Custom unlock screen message
- Managed on Windows or Mac
- On Prem or Cloud deployment options

ANTI-MALWARE FOR SECURE USB

- On-Board device Trellix® anti-malware
- Automatically delete or remove malware on device
- Real-time reporting on infected files and devices

PORTBLOCKER FOR USB PORTS IN THE NETWORK

- Ensure only approved USB devices are used
- Completely lock-down USB ports at the hardware layer
- Report on unapproved device attempts
- Temporary USB device access

USB CERTIFIED DATA ERASURE

- Delivers certified, cryptographic data sanitization for SafeConsoleReady™ encrypted USB drives e
- Enables organizations to prove that sensitive data has been securely erased in compliance with NIST SP 800-88
- Provides verifiable erasure, automated certification, and centralized reporting
- Ensures secure data destruction without manual processes, disconnected tools, or operational risk.

ENTERPRISE FEATURES

- REST API access
- Single Sign On for Admins (SSO, SAML v2)
- SSO/SIEM integration
- SIEM external logging
- Kerberos SMTP server support
- Active Directory User Synchronization and Secure Active Directory User Synchronization (LDAPS)
- Dedicated Server IP addresses (Allows firewall whitelisting for outgoing traffic)
- Custom geographic server location (Meet compliance requirements)
- Unlimited user audit logs

USE CASES

FORTUNE 100

We serve thousands of federal and enterprise customers worldwide, including two-thirds of the Fortune 100.



MANUFACTURING

Ultra-secure data transport for air-gapped manufacturing white stations servicing OT networks.



LEGAL

Secure personal data, case files, and other confidential data information.



GOVERNMENT

Secure storage and remote management for orgs with the most demanding compliance standards.



FINANCE

Protect critical financial data whether it's stored at headquarters, on a remote laptop, or on a mobile USB drive.



HEALTHCARE

Secure transport of large-file-format HIPAA-governed data, such as advanced imaging files or even patient records.



ENERGY

Protect energy infrastructure, sensitive data, and delivery systems.

CENTRALIZED MANAGEMENT

MySafeConsole

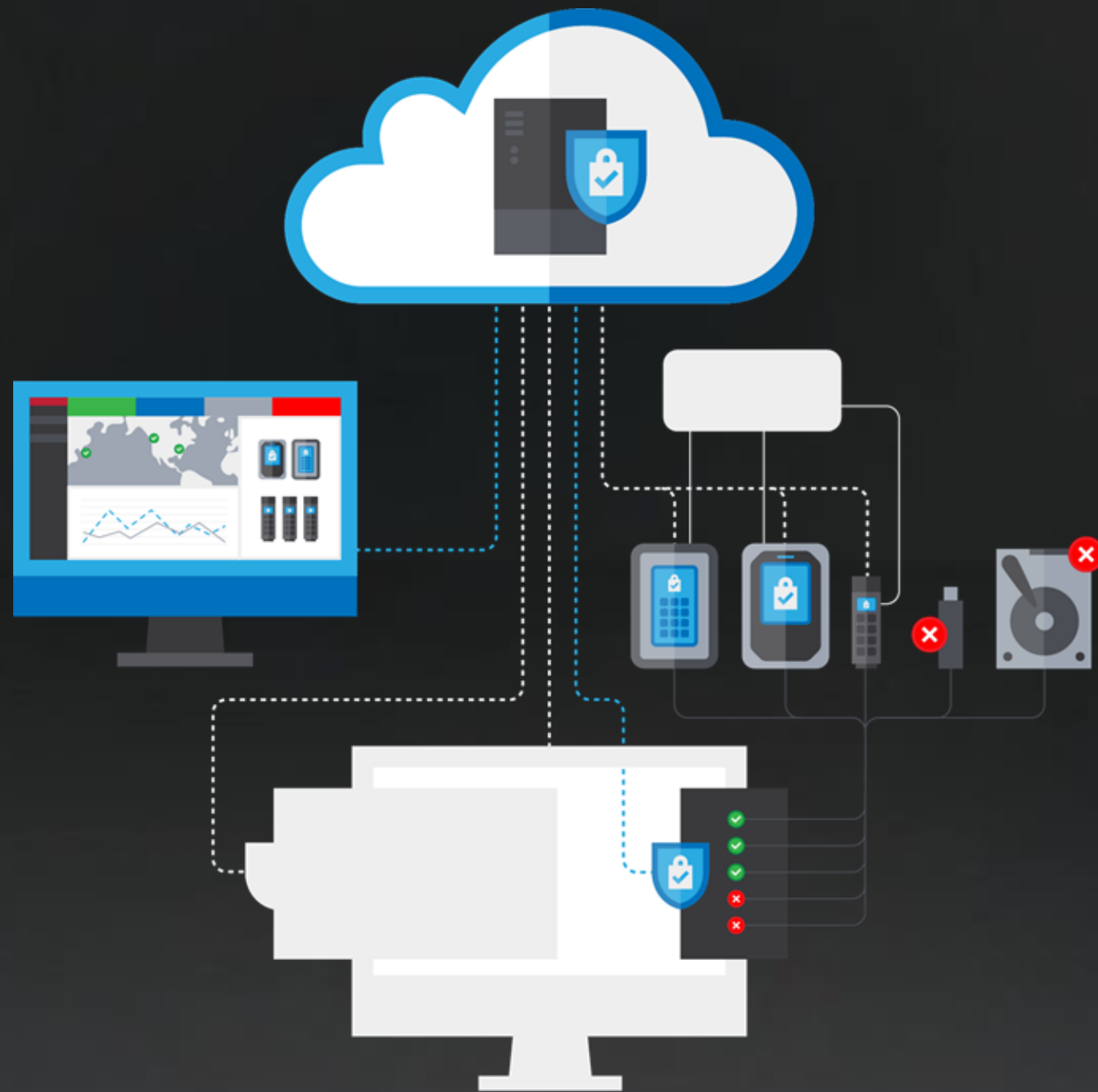
- Password recovery
- Device usage history
- Security updates
- Option malware protection (Plus/Pro)
- Cloud-Only



SafeConsole Enterprise

- Centralized policy enforcement
- Detailed compliance audit logging
- Geofencing
- API integration
- Cloud or On-Prem deployments





SAFECONSOLE USB Device Management

Enforce policies
Track and audit usage
Reporting

USB Device Management



Password Management

Securely reset passwords remotely without data loss and fully logged for compliance without sharing master passwords.



Compliance & Detailed Auditing

Maintain compliance with a real-time device inventory. Track file activities on encrypted USB drives with detailed auditing.



Device State Management

Instantly disable, wipe, or recover lost, stolen, or rogue USB drives remotely to protect your organization's sensitive data from unauthorized access.



File-Type Restrictions & Write Protection

Block unauthorized file types (like executables or MP3s) from being saved. Use write protection to lock drives in read-only mode, preventing malware infections on untrusted machines.



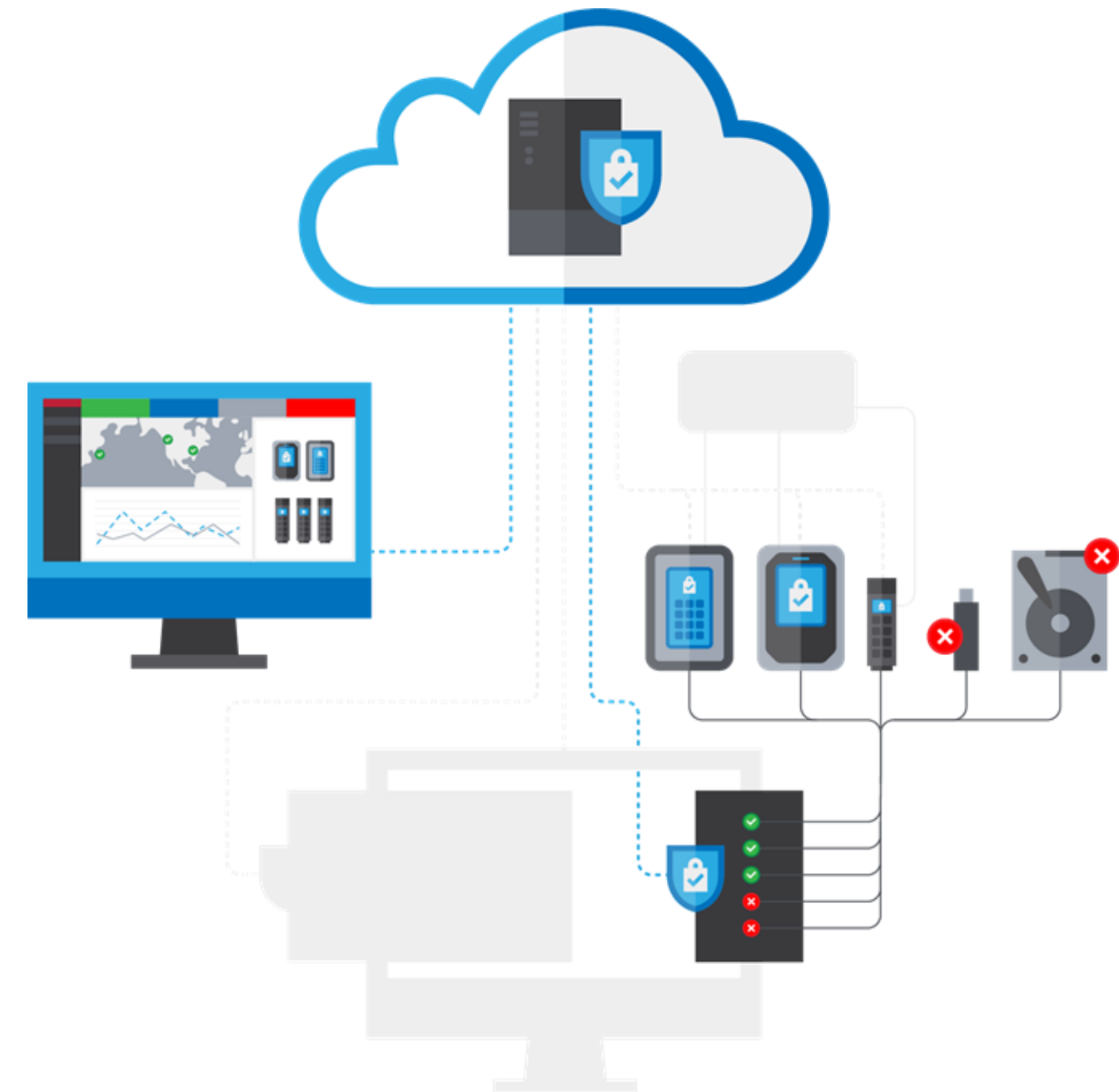
Geolocation & Geofencing

Track the physical location of your encrypted USB drives. Use geofencing to restrict device access to predefined geographic zones for maximum security.



ZoneBuilder - Create Trusted Zones

Create trusted zones where encrypted USB devices unlock automatically without passwords for seamless sharing. You can also restrict drive usage exclusively to these secure zones.



FEATURES



Why Choose SafeConsole USB Device Management?

- **USB Drive Encryption & Policy Enforcement:** Protect USB drives with AES 256-bit encryption, enforce password rules, and apply file-type and geolocation restrictions for enhanced security.
- **Secure Password Management:** Reset forgotten passwords securely with a hardware-validated, cryptographic method, fully logged for compliance without sharing master passwords.
- **Policy-Driven Authentication:** Strengthen security with additional authentication factors like certificates, 2FA, or SSO, ensuring admin and user accountability.
- **Zero-Touch Deployment & Enrollment:** Set up devices seamlessly through end-user self-enrollment or batch configuration with DeviceDeployer, ready for use straight from the box.

USB Device Management is licensed per device and is available with or without Anti-malware. Cannot be purchased as a standalone product. Requires an active SafeConsole server and SafeConsole Ready device.



Data Erasure Report Certificate

Device Information

Manufacturer	DataLocker, Inc.
Device Type	DataLocker Encrypted USB Device
Model	DataLocker Encrypted USB Device
Capacity	128 GB
Serial Number	G4400295
Asset ID	109229
Interface	USB 3.0
Firmware Version	5.96
Management	SafeConsole-Managed
Encryption Algorithm	AES-256 XTS - Hardware-Based

SafeConsole Confirmation

Crypto-Erase Command Is...	✓ Completed
Operator Identity Verified	✓ Logged
Device Check-In Timestamp	2026-01-20 06:49:41 GMT
Post-Erase Compliance Sta...	✓ Purged
Device Re-Provisioned?	No

Erasure Summary

Erasure Type	Crypto-Erase (Key Destruction)
Method	"Zeroize" command - Regenerates Keys
Start/End Time	2026-01-20 06:49:41 GMT
Time to Erase	< 1 second
Erasure Standard	NIST SP 800-88 Rev 1 - Purge
Result	✓ Erased Successfully
Performed By	j_doe@datalocker.com
Date & Time	2026-01-20 06:49:41 GMT
Verification Status	Key material destroyed

✓ DEVICE ERASURE SUCCESSFUL

This DataLocker encrypted USB device has been securely purged in compliance with:

- NIST SP 800-88 r1 Purge Requirements
- FIPS 140-3 Level 3 Secure Key Management

The device contains no recoverable user data and is safe for reuse, reassignment, or decommissioning.

2026-01-20 - DataLocker USB Data Erasure v1.0

SAFECONSOLE

USB Certified

Data Erasure

Tamper-Proof Data
Erasure with Certified
Reporting

USB Certified Data Erasure



Seamless Experience

Enable certified erasure through policy automation or initiate on-demand erasure directly within the SafeConsole management platform.



Guaranteed Compliance

Automatically generate certified proof-of-erasure certificates for audits, regulatory reporting, and governance requirements.



Zero Human Error

Replace manual wipe procedures with automated, policy-driven or on-demand cryptographic erasure.



Real-Time Reporting

Monitor erasure activity in real time with full audit logs, including device ID, user, timestamp, erasure method, and certificate reference.



End-to-End Security

Extend protection from first device use through secure disposal or reuse.



Tamper-Proof Reports

Unmodifiable audit trails with digital signatures, unique identifiers, and cryptographic hashing to verify integrity and compliance.



Data Erasure Report Certificate



Device Information

Manufacturer	DataLocker, Inc.
Device Type	DataLocker Encrypted USB Device
Model	Sentry ONE
Capacity	N/A
Serial Number	000FFE23C7ECB24030000365
Asset ID	N/A
Interface	USB 3.0
Firmware Version	6.6.0.0
Management	SafeConsole-Managed
Encryption Algorithm	AES-256 XTS - Hardware-Based

SafeConsole Confirmation

Crypto-Erase Command Issued	✓ Completed
Operator Identity Verified	✓ Logged
Device Check-In Timestamp	2026-02-27 04:00:42 GMT
Post-Erase Compliance Status	✓ Purged

Blockchain Verification

Chain ID	atcata_1afa8d38d54
Device	230A154F.000FFE23C7ECB24030000365
Chain Sequence	1
Certificate Hash	0bd0f95cdd5441b4a1bf6ca36e6aeb0f96947fc0bc972a877f9ecc8426f57
Previous Hash	GENESIS
Timestamp	2026-02-27 04:00:52 GMT

Erasure Summary

Erasure Standard	NIST SP 800-88 Rev 1 - Purge
Erasure Method	Cryptographic Erase - Execution of the cryptographic erasure destroys the cryptographic keys to ensure complete data erasure
Verification	The encryption keys have been destroyed and verified, making all prior data permanently inaccessible.
Start/End Time	2026-02-27 04:00:42 GMT
Time to Erase	< 1 second
Result	✓ Erased Successfully
Performed By	admin@company.com

✓ DEVICE ERASURE SUCCESSFUL

This DataLocker encrypted USB device has been securely purged in compliance with:

- NIST SP 800-88 r1 Purge Requirements
- FIPS 140-3 Level 3 Secure Key Management

The device contains no recoverable user data and is safe for reuse, reassignment, or decommissioning.

Digitally signed by SafeConsole (50d5266524fa)

Chain ID: atcata_1afa8d38d54

Hash: 0bd0f95cdd5441b4a1bf6ca36e6aeb0f96947fc0bc972a877f9ecc8426f57

Date: 2026-02-27 04:00:58 GMT


[Scan to Verify](#)

2026-02-27 - DataLocker USB Data Erasure v1.0

Why Choose SafeConsole USB Certified Data Erasure?

- **Certified Cryptographic Erasure:** Uses cryptographic erasure instead of destructive overwrite cycles — preserving device memory integrity while achieving defined data sanitization standards.
- **Manufacturer-Level Control:** As the device manufacturer, DataLocker performs erasure at the cryptographic layer, enabling standards-aligned data sanitization that third-party overwrite tools cannot achieve.
- **Built-In Compliance:** Native alignment with NIST 800-88 guidelines, eliminating external tools, manual workflows, and disconnected compliance reporting.
- **Platform-Native Integration:** Erasure, certification, reporting, and lifecycle management — all inside SafeConsole.

USB Certified Data Erasure is licensed per erasure and is available only as an add-on to USB Device Management. Cannot be purchased as a standalone product. Requires an active SafeConsole server and valid USB Device Management license per device.



SAFECONSOLE

AntiMalware

Powered by Trellix™

Automatic Detection and Removal
Always-On Protection
Active Monitoring & Real-Time Reporting

AntiMalware



Easy Deployment

Simply enable the Anti-Malware service through the SafeConsole management platform. No additional installations are needed on the endpoint.



Automatic Malware Detection and Removal

The integrated Trellix™ module automatically scans the USB drive for viruses, ransomware, trojan horses, worms, and other malware threats.



Always-On Protection

SafeConsole Anti-Malware provides continuous USB malware protection by running in the background on the encrypted device ensuring ongoing security without requiring administrator privileges.



Active Monitoring & Real-Time Reporting

Receive notifications in real-time when threats are detected. Admins can monitor malware activity through the SafeConsole admin portal.



Automatic Virus Definition Updates

Stay protected with automatic virus definition updates provided by Trellix™, ensuring your secure USB drives remain up-to-date.



Seamless Integration

Works alongside host antivirus software without conflict, providing comprehensive USB malware defense.



FEATURES



Total Threat Defense for your Managed Devices

A portable, built-in anti-malware application powered by Trellix runs in the background of your centrally managed devices.

Key Features

- Automatically scans for viruses, worms, trojan horses and other malware threats
- Automatically removes any viruses found on the device
- Reports to SafeConsole when and where the virus is removed
- Automatically updates when your device is unlocked
- Works in the background, complementing existing endpoint antivirus software without conflict

With an on-board antivirus that scans the files being stored on your secure mobile storage device, you can protect your files against threats when the device is being utilized on a Windows system

Anti-Malware is available as an add-on to USB Device Management. Cannot be purchased as a standalone product. Requires an active SafeConsole server and valid USB Device Management license per device.



DATALOCKER PORTBLOCKER

Prevent data loss with
USB-port blocking

MANAGED BY



PORTBLOCKER



Easy and Automatic

Admins will be notified when a blocked USB device is inserted and PortBlocker will deny access to the device. The instance will automatically be reported to the SafeConsole audit log. Admin can easily whitelist device for a set amount of time or permanently.



Seamless Integration

Seamlessly running in the background of user workstations, PortBlocker was built to work alongside existing SafeConsole features and policies.



Active Monitoring

When blocked USB devices are detected in a USB port, users are unable to read from or write to the USB and SafeConsole admins will receive notifications in the PortBlocker activity log within the central management platform.



Always-On Protection

Once installed by an admin, PortBlocker will start automatically and run in the background of the user's workstation and cannot be disabled by a non-privileged user or external programs.



Policy Enforcement

Restrict mass storage devices through SafeConsole whitelist policy (VID, PID, and serial number). Policies are updated automatically from SafeConsole.



Real-time Reporting

Endpoint activity audits are reported to SafeConsole in the Device Audit Logs.



REQUIREMENTS



Active SafeConsole Account

Windows™ 7, 10 or 11, macOS

512MB of RAM

1 GB of available hard-disk space

Connection to SafeConsole server for registration and policy updates

Intel Quad Core Atom processor, or equivalent x86 - x64 processor

Uses the WinINET (Internet Explorer) system user's proxy settings. Manual proxy settings or a pac script are supported.

A SafeConsole Account is required in order to utilize and deploy PortBlocker. A valid PortBlocker license is required for each workstation/system where PortBlocker is deployed (licenses are available for 1 or 3 years).



ALPHACAM H HIGH PERFORMANCE

TAA Compliant Optimized
Webcam



**High-Quality Image
with HD Video Capture**



**Easy Set Up with USB
Connection**



**Works With Any
Hardware**



**Microphone-Free to
Prevent Data Leaks**

FEATURES

ALPHACAM H & H2

OPTIMIZED FOR VIDEO CONFERENCES AND WEB EDUCATION

The AlphaCam H™ focuses on specific functions to optimize utility in video conferences and web education.

TAA COMPLIANT WEBCAM

The AlphaCam H is perfectly suited for one-to-one live video communication over the Internet for enterprises and public institutions allowing more dynamic meetings supported by the highest quality images. It also helps to enhance your web video education experience at home.

The only difference between the AlphaCam H and the AlphaCam H2 is that the AlphaCam H includes a built-in microphone, while the AlphaCam H2 does not. This makes the AlphaCam H2 suitable for environments that prohibit audio capture for security reasons.

ADDITIONAL FEATURES

- Full HD 1080p video resolution (supports up to 30 frames per second)
- Easy setup, no software or drivers. USB connectivity; UVC compliant
- Built-in privacy cover for added security when not in use
- Clip-on and stand style accessories included to fit notebooks, LCD or CRT monitors
- USB-C with USB-A converter included

VIDEO RESOLUTION

Full HD 1080p video resolution (supports up to 30 frames per second)

SNAPSHOT RESOLUTION

Up to 16 megapixel resolution (interpolated)

COMPATIBILITY

Works with all web-based collaboration/meeting systems: Teams, Vidyo, Zoom, BlueJeans, CISCO WebEx, Jabber, FaceTime, GoTo Meeting, Adobe Connect, Skype, & more

DIMENSIONS

58 x 40 mm (WxL) / camera
58 x 69 mm (WxL) / with cradle

WEIGHT

Approx 93.2g (3.29oz)

INTERFACE

High-speed USB 2.0 or higher (UVC, YUY2)
USB-C with USB-A converter included

STANDARDS AND CERTIFICATIONS

TAA Compliant, FCC, KC and CE

SYSTEM REQUIREMENTS

Windows® 7, Windows 8, or Windows 10
Mac® OS X 10.7 or higher
Linux OS 2.6.24 or higher
Chrome™ OS Version 29.0.1547.70 or higher
300MB free hard drive space

WARRANTY

3-year limited warranty

PART NUMBER

WCAM2000-G
WCAM2000-NOMIC-G

COUNTRY OF ORIGIN

South Korea



ALPHATALK OPTIMAL COMFORT

TAA Compliant USB Headset





**Better Conversation
with Background Noises
Eliminated**



TAA Compliant



**Free Up Your Hands To
Work On Other Tasks**



FEATURES

ALPHATALK

FREE UP YOUR HANDS

Utilizing a headset allows you to continue to work on other tasks while taking calls. There's no need to hang up while typing, taking notes, etc.

BETTER CONVERSATION

The most important function of a headset is to eliminate background noise and let callers hear your voice clearly. AlphaTalk's microphone delivers crystal-clear conversations for closer connections with your caller.

TAA COMPLIANT

Decrease vulnerability to security breaches. DataLocker's AlphaTalk is a TAA Compliant headset that protects you from a breach or leak of sensitive data.

BROAD COMPATIBILITY

Compatible with common calling applications across almost all platforms and operating systems: Windows 7/8/10, Mac OS X, and other devices with USB.

ADDITIONAL FEATURES

- Easy setup, no software or drivers. USB plug and play (USB 2.0 compliant)
- Adjustable headband for a custom fit
- Complete digital sound card with DSP technology
- Clear live voice transmission with VoIP
- Simple in-line controls with LED indicator
- Flexible microphone boom with noise cancellation
- Longer USB cable: 7.8 ft included

INPUT IMPEDANCE

32 Ohms ± 15%

SENSITIVITY (HEADPHONE)

95dB S.P.L/Mw (1k) ± 3dB

SENSITIVITY (MICROPHONE)

-44dB ± 3dB (0dB=1V/pa at 1kHz)

FREQUENCY RANGE (HEADSET)

20Hz-20KHz

FREQUENCY RANGE (MICROPHONE)

100Hz-10KHz

CABLE LENGTH

7.8ft (2.4m)

DIMENSIONS

Earpad Diameter: 2.5in

Microphone: 1in

Inline Controller: 2.5 x 1 x 0.5in

Package: 9 x 8in

WEIGHT

0.35lbs (160g)

CONNECTIONS

USB-A compatible (1.1, 2.0, 3.0)

SYSTEM REQUIREMENTS

Microsoft Windows 7, 8, 10, 11

Mac OS X 10.7 or higher

USB Port or Adapter (Type A)

STANDARDS AND CERTIFICATIONS

TAA Compliant, FCC, KC and CE

WARRANTY

3-year limited warranty

PART NUMBER

AT1000HS-G

LINKS TO ONLINE INFORMATION

Product Resource Center



Introduction Videos



DATALOCKER PARTNER PROGRAM

Helping each other reach new heights



PARTNER PROGRAM

3 Steps to Success

1. Meet with your DataLocker Territory Manager to create a target list of customers to pursue together
2. Setup a meeting and register the opportunity to earn a competitive pricing advantage
3. DataLocker will co-sell with you utilizing our sales and engineering support resources
4. Utilize our partner portal for additional resources

HOW TO PITCH DATALOCKER

Questions to ask

- What is your policy for allowing employees to use portable USB storage devices?
- What is your approach to protecting data on USB drives?
- Have you had any issues with unauthorized usage of USB flash drives - data theft?
- How do you protect against malware coming into your network over USB?
- Are you worried about ransomware? The easiest way to protect yourself is to have an offline encrypted backup of your important files.

Use Cases for Encrypted Storage

- To help customers utilize removable storage without compromising security or convenience (remote employees, hybrid environments, encrypted backups, data transfers, etc.).
- For implementing and applying security policies to portable USB drives (when devices are managed with central management).
- Predict and protect from data leaks before they occur.
- Provide an audit trail for a quick incident response when a data leak occurs (when devices are managed with central management).
- Offer an instant, cost-effective way to comply with HIPAA, SOX, DHS Initiatives, NRC, GLB, GDPR and any other directive that requires data encryption.

Target Customer Profile

- Medium to Large Enterprise
 - 250+ employees
 - PII/PHI Compliance Requirements
 - Organizations concerned with protecting/securing sensitive information
- Vertical Industries
 - Healthcare
 - Finance
 - Federal Government
 - Legal
 - Law Enforcement
 - Manufacturing
- Looking at the following products
 - Apricorn / iStorage (Encrypted USB devices)
 - Data Loss Prevention (DLP)

When Does a Customer Buy?

After...

- Data Breach
- Non-Compliance penalty
- Bad experience with complicated solutions
- Shift in compliance directives
- Merger/Acquisition

Prospecting Examples

“My name is and I am with ABC, we are a local IT solutions company. One of our main areas of focus is helping companies maintain compliance by securing their most sensitive data with our data-at-rest encryption solutions.

“I know how challenging enforcing security policies can be, especially when it comes to portable data. If the solution is too complicated for your employees to use, it defeats its purpose if they end up not using it. Am I on track here?

“The reason I am calling you is that we have centrally managed encryption solutions that can encrypt your data whether it is stored on a local folder, network folder or a cloud folder like OneDrive, Google Drive, etc.” We can also encrypt and manage your portable data through hardware encrypted USB flash drives, hard drives and SSDs.

“Through the same central management console, you can also enforce your USB port usage policy. Can you spare 15 minutes to discuss further?”

USE CASES



MANUFACTURING

Ultra-secure data transport for air-gapped manufacturing white stations servicing OT networks.



GOVERNMENT

Secure storage and remote management for orgs with the most demanding compliance standards (Dept. of Defense, NASA).



HEALTHCARE

Secure transport of large-file-format HIPAA-governed data, such as advanced imaging files or even patient records.

Thank you for your support

