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.
- DataLocker acquired IronKey Enterprise Management Service & IronKey Hard Drives in February 2016.

THE WORLD'S MOST DEMANDING ORGS TRUST DATALOCKER

LEGAL

- Whitaker Chalk Attorneys & Counselors
- GW Garfunkel Wild, P.C. Attorneys at Law
- Epstein Becker Green
- Poyner Spruill Attorneys at Law
- ulmer berne llp Attorneys
- KSM Katz Sapper & Miller

ENTERPRISE

- Lockheed Martin
- General Dynamics
- Honeywell
- Northrop Grumman
- GE
- DreamWorks Studios
- Walt Disney Imagineering

GOVERNMENT

- Department of the Navy, United States of America
- NASA
- U.S. Department of Homeland Security
- Department of Commerce, United States of America
- U.S. Department of the Interior, March 3, 1849

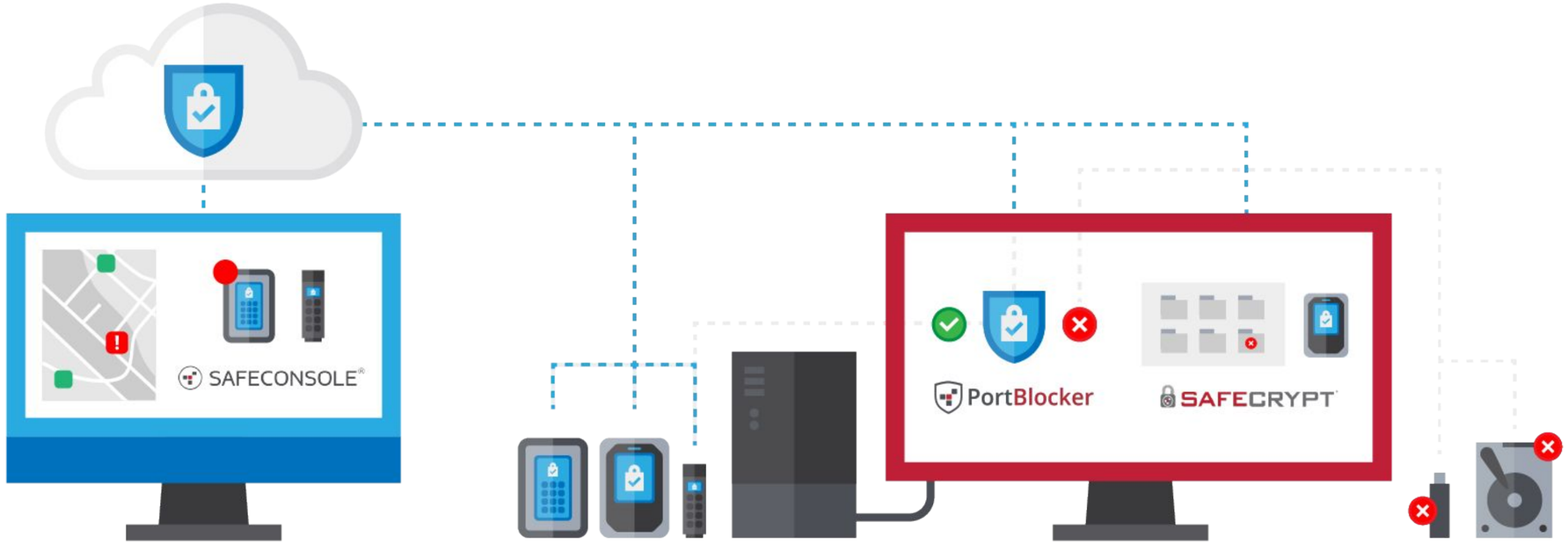
HEALTHCARE

- Allscripts
- UnitedHealthcare
- Saint Luke's Health System
- Children's of Alabama
- Banner Health
- Kaiser Permanente

FINANCIAL

- Lloyds Bank
- Federal Reserve Bank of New York, Incorporated May 18, 1914
- Deloitte.
- KPMG cutting through complexity
- Experian A world of insight

THE DATALOCKER SOLUTION



SafeConsole

Remotely manage and audit secure drives

DataLocker Secure Drives

Encrypt data on a mobile 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.

SafeCrypt

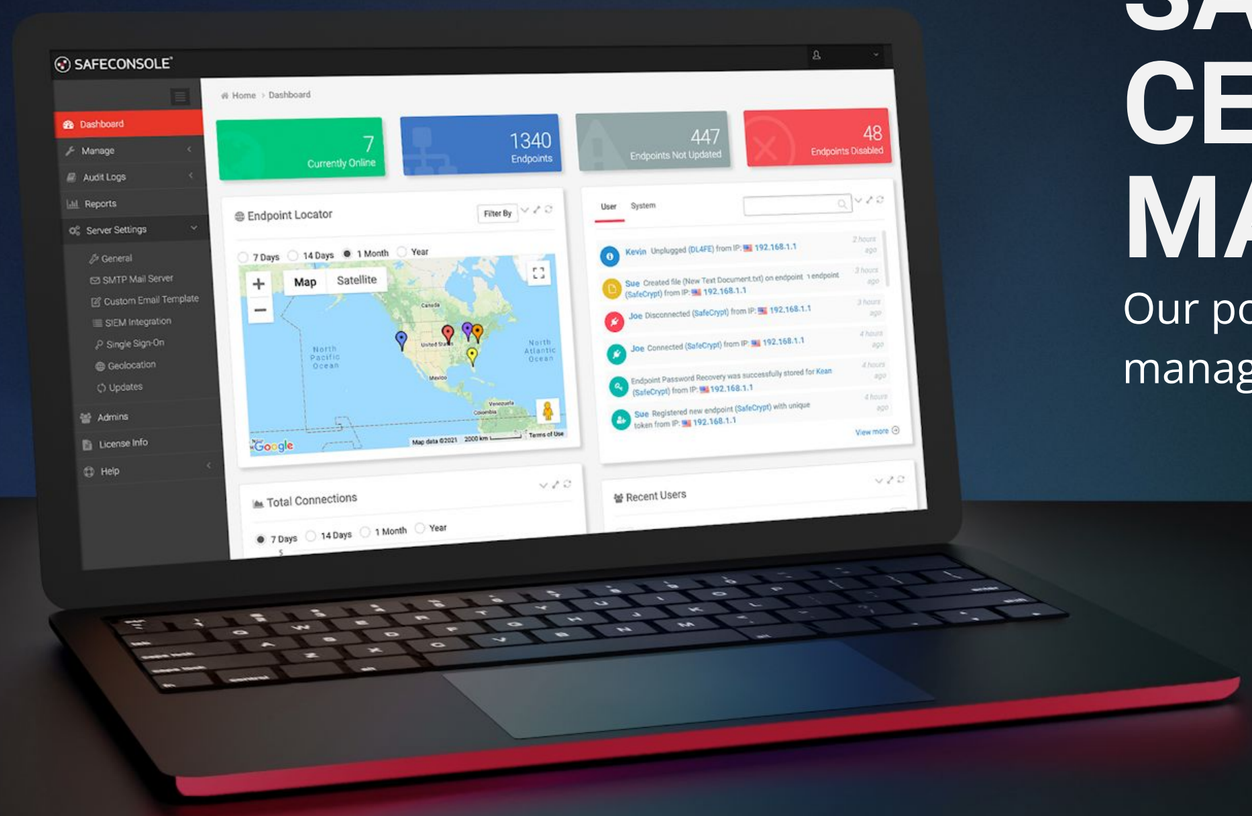
Encrypt any data stored on a workstation to lock up any sensitive data

DataLocker®

Built-In Anti-Malware Powered by McAfee
Automatically scan data for viruses and malware before its stored on device

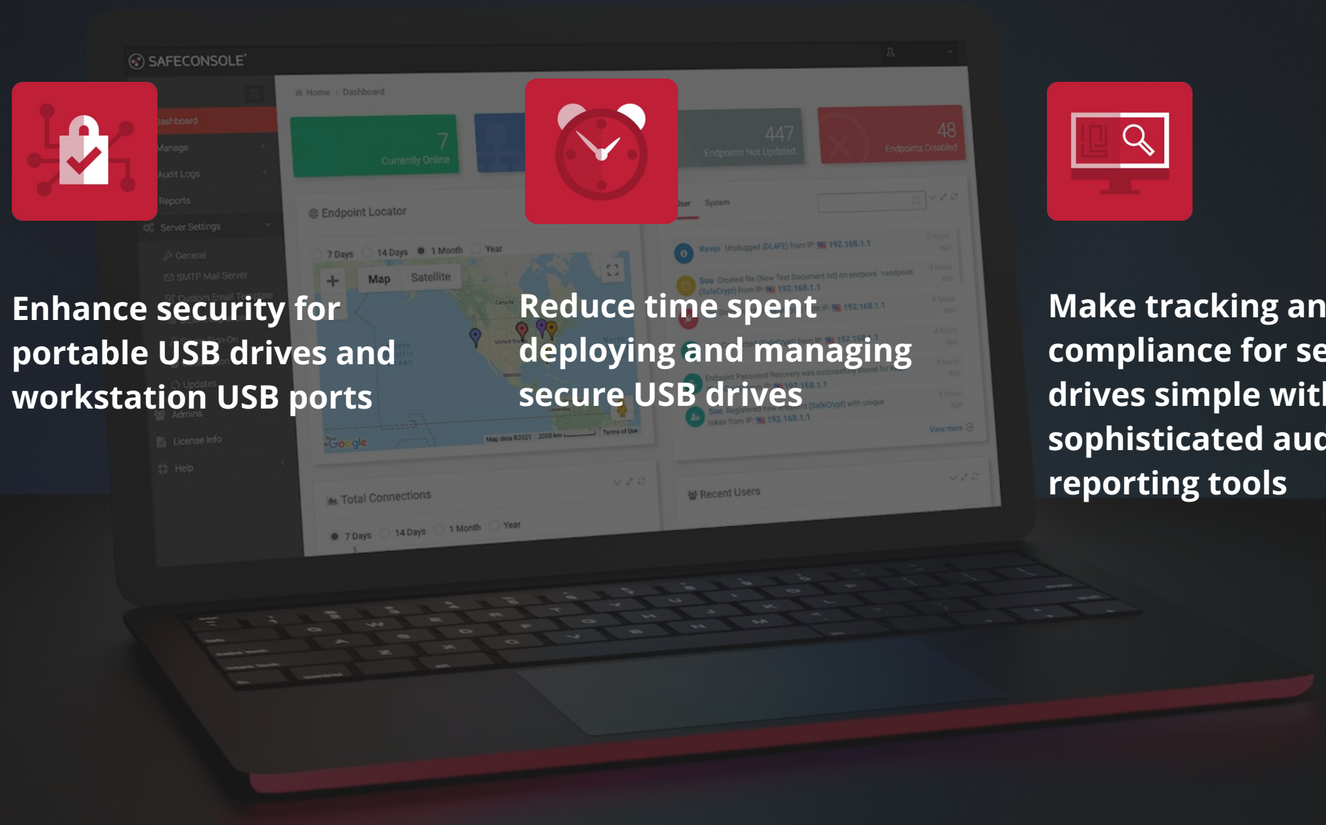
DATALOCKER SAFECONSOLE CENTRAL MANAGEMENT

Our powerful, secure system to manage your devices and more



DataLocker®

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

DataLocker®

SAFECONSOLE MANAGEMENT PLATFORM

DEPLOY AS CLOUD (SAAS) OR ON-PREM*

SafeConsole DeviceControl

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

SafeConsole SafeCrypt

Store and secure local or cloud data in an encrypted virtual drive

SafeConsole Anti-Malware

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

SafeConsole PortBlocker

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

DataLocker®

FEATURES

SAFECONSOLE CLOUD/ON PREM FEATURES ON WINDOWS AND MAC OS

COMPLETE CENTRAL MANAGEMENT AND CONTROL FOR ADMINISTRATORS

DEVICE CONTROL 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 McAfee® 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

SAFECRYPT FOR FILES AND FOLDERS

- Virtual encrypted drive for Windows or Mac OS
- Centrally managed Virtual Encrypted Drive on desktop that allows secure storage and separation of work files and folders
- Setup as a shared Remote Network Drive - locally encrypt and sync securely with network (NAS), OneDrive, Google Drive and more.
- Keep locked drives separated from the host operating system

PRO FEATURES

- Premium support tier (2 hour max response time)
- Dedicated team of support managers
- Priority support queue
- Advanced hardware replacement with RMA
- ZoneBuilder: secure auto-login and device restriction

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

SAFECONSOLE MANAGED DRIVES

ENCRYPTED FLASH DRIVES

- Sentry K350 (available only for Windows)
- Sentry K300 (available only for Windows)
- Sentry ONE
- Origin SC100
- Kingston DT4000G2M-R/DT4000G2DM
- Kingston DTVP30M-R/DTVP30DM
- IronKey S1000
- IronKey D300M/D300SM

ENCRYPTED PORTABLE HARD DRIVES

- DataLocker H300
- DataLocker H350
- DataLocker DL3 FE (available only for Windows)
- DataLocker DL3 (available only for Windows)
- DataLocker DL4 FE (available only for Windows)

K350
SMALL FORM-FACTOR, HEAVYWEIGHT SECURITY

Our most durable and portable drive.

FIPS 140-2 LEVEL 3 CERTIFIED
TAA COMPLIANT
COMMON CRITERIA EAL5+ CERTIFIED
AES 256-BIT XTS AES 256 ENCRYPTION

DataLocker®

THE ULTRA-DURABLE K350

IP67-rated

Dust, water, shock, and vibration resistant.

DataLocker®

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-140-2 Level 3 (Cert. #4008) device validation with hardened enclosure and internals

Common Criteria EAL5+ validation

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

AES 256-bit XTS cryptographic module

Bruteforce password protection & randomizing keypad

Admin Policies and User Data Recovery

DATALOCKER®

- **FIPS-140-2 Level 3 (Cert. #4008) device validation with hardened enclosure and internals**
- **Common Criteria EAL5+ validation**
- **Location-based security posture and on-board Antimalware** (requires SafeConsole)
- **Powerful Encryption Right Out Of The Box**
- **Protect Data at Scale**
- **AES 256-bit XTS cryptographic module**
- **Bruteforce password protection & randomizing keypad**
- **Admin Policies and User Data Recovery**
- **Ensure User Adoption With Easy-to-Use Keypad**
- **Remotely Manage & Audit Your Entire Fleet**

DATALOCKER®

EASE OF USE

Screen and Keypad

Onboard Customization

Ultra-portable

Platform Agnostic

COMPLIANCE

FEATURE CALL-OUT

FIPS 140-2 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

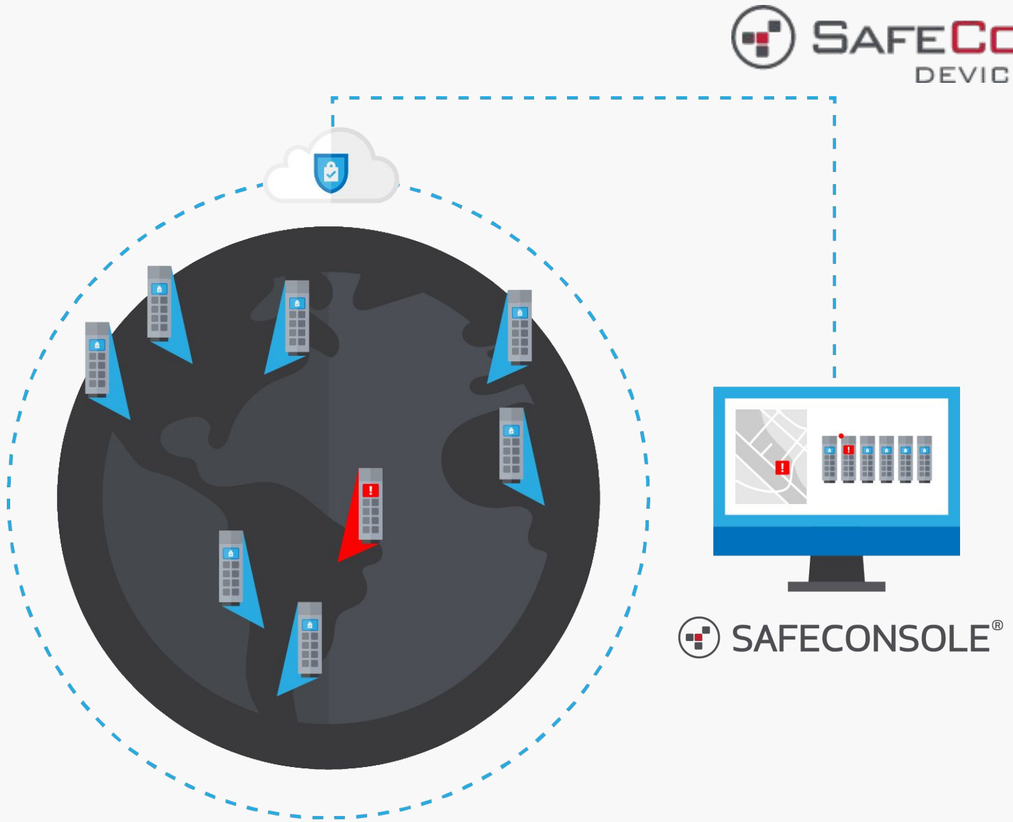
Allow users under duress to destroy the device or the stored data without leaving traces by entering a special code (admin configurable).

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).

DATALOCKER®

FEATURE SUMMARY

K350 FEATURES

FIPS 140-2 LEVEL 3 CERTIFICATION

FIPS 140-2 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, 64GB, 256GB

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
IP67 rated. Hardened, epoxy sealed internals and robust enclosure.

CRYPTOGRAPHIC PROCESS
FIPS 140-2 Level 3 Device Certified (Cert. #4008). Common Criteria cPP certification pending*

AES 256-bit XTS hardware encryption onboard

Integrates a Common Criteria EAL 5+ certified secure microprocessor

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

TRANSFER SPEEDS
190 MB/S Read/Write

STANDARDS AND CERTIFICATION
FIPS 140-2 Level 3 (Cert. #4008)
TAA Compliance
IP67 Certified
MIL-STD-810G
RoHS Compliant
FCC
CE

MANAGEMENT COMPATIBILITY
Microsoft Windows Lithium-ion polymer charges automatically over the powered USB-port

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

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

PART NUMBERS
SK350-016-FE
SK350-064-FE
SK350-256-FE

DEVICE LANGUAGES
English

WARRANTY
3-year limited warranty

*The K350 is in process to achieve Common Criteria cPP certification. The official listing as a Product under Evaluation by NIAP is expected in 2021.

DATALOCKER®

SENTRY ONE
ENCRYPTED FLASH DRIVE

Secure, mobile, fast.

FIPS 140-2 LEVEL 3 CERTIFIED
TAA COMPLIANT
AES 256-BIT XTS AES 256 ENCRYPTION

DATALOCKER®

SENTRY ONE BENEFITS

FIPS 140-2 Level 3 Certified

Hardware-based AES 256-bit XTS mode encryption

Tamper evident seal and waterproof up to 4ft

Conforms to IEC 60529 IPX8

Remotely manageable with SafeConsole

DATALOCKER®

FEATURE CALL-OUT

3 FIPS 140-2

POWERFUL ENCRYPTION

Everything you need to encrypt data is built into the FIPS 140-2 Level 3 and pending Common Criteria EAL5+ certification. No drivers. No setup. Just iron-clad, hardware-based AES 256-bit encryption in an easy-to-use interface, which is further guarded by an army of automated security policies.

PROTECT DATA AT SCALE

Remote management available with SafeConsole, lets admins fully control or terminate devices over the internet. Rapid, no-hands, automated deployment at scale is available for managed Sentry One drives.

REMOTELY MANAGE & AUDIT

Sentry ONE drives are remotely manageable with SafeConsole, giving admins the ability to remotely lock or wipe drives, reset passwords, view last-used locations, and see what data has been added, removed, or changed on the drive. Set device or group-specific policies for all the drives in your fleet.

DATALOCKER®

MANAGEMENT

Comprehensive Audit Capabilities

Data Geofencing

Remote Device Detonation

On Board Anti-malware (Configurable)

FEATURE SUMMARY

SENTRY ONE FEATURES

FIPS 140-2 LEVEL 3 CERTIFICATION

FIPS 140-2 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 provide a one-time password to allow the user back into their device. 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.

READ-ONLY MODE

Admins can configure the Sentry ONE to read-only mode, ensuring that no malicious data can be written to the device.

MANAGED SENTRY ONE 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.

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.

SPECS

CAPACITIES
8GB, 16GB, 64GB, 128GB

DIMENSIONS
L: 7.79 cm (3.09 in)
W: 2.22 cm (.87 in)
D: 1.21 cm (.47 in)

WEIGHT
54 grams / 1.9 oz

STANDARDS AND CERTIFICATION
FIPS 140-2 Level 3 (Cert. #2929)
TAA Compliance
FCC
CE
VCCI & KC
RoHS & WEEE

SYSTEM COMPATIBILITY
Windows 10, 8.1, 8, 7 (SP1)
Mac OS X v.10.9.x - 10.13.x
Linux v2.6 + 2
Citrix Ready (XenDesktop, XenApp compatible)
Two (2) free drive letters required for use on Windows

CRYPTOGRAPHIC PROCESS
FIPS 140-2 Level 3 Device Certified (Cert. #2929). Common Criteria cPP certification pending*

AES 256-bit XTS hardware encryption onboard

Integrates a Common Criteria EAL 5+ certified secure microprocessor

INTERFACE
USB 3.2 Gen 1 - Backward compatible with USB 2.0 & 1.1

TEMPERATURE
Operating: 0°C to 60°C
CStorage: -20° to 85°C

TRANSFER SPEEDS
USB 3.2 GEN 1:
8GB &16GB: 165MB/s READ, 22MB/s WRITE
32GB: 250MB/s read, 40MB/s WRITE
64GB & 128GB: 250MB/s READ, 85MB/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
SONE008
SONE016
SONE032
SONE064
SONE128
SONE008M
SONE016M
SONE032M
SONE064M
SONE128M

WARRANTY
5-year limited warranty

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®

COMMON CRITERIA CC EAL5+ CERTIFIED

FIPS 140-2 LEVEL 3 CERTIFIED

TAA COMPLIANT

AES 256-BIT XTS AES 256 ENCRYPTION

DL4 FE
SECURE TO THE CORE

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

DATALOCKER®

ENCRYPTION & PHYSICAL SECURITY

FIPS 140-2 LEVEL 3 CERTIFIED

FIPS-140-2 Level 3 device validation with hardened enclosure and internals

AES 256-BIT XTS AES 256 ENCRYPTION

AES 256-bit XTS cryptographic module

COMMON CRITERIA EAL5+ CERTIFIED

Common Criteria EAL5+ validation

Bruteforce password protection & randomizing keypad

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

Admin Policies and User Data Recovery

DATALOCKER®

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

DATALOCKER®

COMPLIANCE

FEATURE CALL-OUT

FIPS 140-2 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).

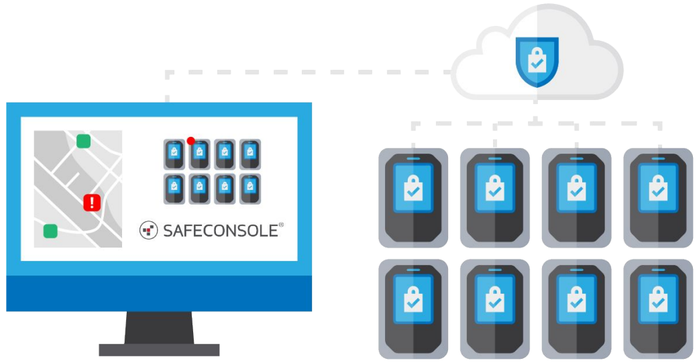
REMOTE DEVICE DETONATION

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 140-2 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).

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: 500 GB, 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 140-2 Level 3 Device (#3972) and Common Criteria cPP certification pending.
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
DL4-500GB-FE
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

*The DL4 FE has been designed for FIPS 140-2 Level 3 and is being tested by an accredited NIST lab. The product is in process for certification and is officially listed by NIST. DL4 FE is also in process to achieve Common Criteria cPP certification. The official listing as a Product under Evaluation by NIAP is expected in March 2021.

**IP64 certification pending.

DATALOCKER®

AES 256-BIT XTS
AES 256
ENCRYPTION

TAA
COMPLIANT

DATALOCKER (IRONKEY) H300 BASIC AND ENTERPRISE

HARDWARE ENCRYPTED AND MANAGEABLE USB 3.2 GEN 1 EXTERNAL HARD DRIVES

DATALOCKER

Hardware-based AES 256-bit XTS mode encryption

Built to Survive Years of Wear and Tear

Competitively Priced with a 5 Year Warranty

Remotely Manage and Audit Your Entire Fleet

DATALOCKER

FEATURES

H300

BASIC

Designed to meet the high security and performance needs of enterprises and government agencies, the DataLocker H300 Basic is encased in a tamper-resistant, high-strength aluminum enclosure and features AES 256-bit hardware encryption, USB 3.2 Gen 1 performance and a Section 508 compliant control panel localized into eight languages around the world.

ENTERPRISE

H300 Basic plus cloud-based or on-premises centralized management to customize security policies and deploy and manage secure portable devices across networks and security environments.

MANAGED H300 FEATURES

KEEP DATA SAFE

Hard drives that rely on software to enable encryption keys are vulnerable to cold-boot and malware attacks because they export AES encryption keys to the host PC. Even hardware encrypted drives that store their credentials on the hard drive are susceptible to attacks. DataLocker hard drives use the DataLocker Cryptochip to store user credentials and the encryption keys to protect against online and physical attacks so you can be confident you're protecting sensitive data. You can also further protect the device with the optional on-board antivirus and malware protection that scans all on- board files upon lock and at regular intervals providing IT with an accurate account of the drive's contents.

DESIGNED TO PROTECT

DataLocker's hardware-based encryption and password verification is always on and can't be disabled by malware or a careless user. DataLocker H300 hard drives provide robust support for complex and custom password policies including length, special characters, expiration and more with an auto-lock feature enabled. The device will either self-destruct or disable (if previously enabled) back to its default state if there are 10 consecutive failed password attempts. Managed DataLocker H300 Enterprise hard drives are the only drives to offer password reset without erasing data.

IMMUNE TO ATTACKS

On every start-up, the firmware's integrity and authenticity of the DataLocker H300 Basic and Enterprise device is validated. The firmware and read-only application partition can only be updated by trusted and signed contents. Digital firmware signing and verification, along with the DataLocker Cryptochip, prevent a hacker or malware from taking control of the hard drives and launching "BadUSB" or "Stuxnet" type of attacks.

STREAMLINE USABILITY

A multi-language control panel is available in German, French, Spanish, Japanese, Korean, Simplified Chinese and Traditional Chinese, in addition to English, empowering the user to access data without relying on the help desk.

H SERIES TOUGH

With the DataLocker H series, you will never have to sacrifice reliability or performance for protection. Rely on durable, quality-tested DataLocker H300 hard drives to keep data private and secure at a price that is budget friendly.

*Requires IronKey EMS license or SafeConsole license (sold separately)

DATALOCKER®

MANAGEMENT

H300 BASIC

Configure in seconds, secure data forever

H300 ENTERPRISE MANAGED BY SAFECONSOLE

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

SPECS

CAPACITIES
500GB, 1 TB, 2 TB

DIMENSIONS
L: 26.8 mm (1.06 in)
W: 86.6 mm (3.41 in)
D: 124.6 mm (4.91 in)

INTERFACE
USB 3.2 GEN 1 (Backwards Compatible)

SECURITY FEATURES
AES 256-bit XTS mode
Hardware-based encryption
Hardware-based password protection
Automatic data protection upon device removal
Tamper-resistant, aluminum enclosure

STANDARDS AND CERTIFICATIONS
FCC
CE
C-TICK
ICES-003
VCCI
BSMI
KCC
WEEE Compliant
RoHS Compliant
Section 508 Compliant

SYSTEM COMPATIBILITY
Microsoft Windows 8.1/8/7/XP (Prof. and Home SP3)
macOS® 10.10 - 10.15
Linux® 2.6+ or higher
Citrix Ready (XenDesktop, XenApp compatible)

PART NUMBERS
MXKB1B500G5001-B (500GB)
MXKB1B001T5001-B (1TB)
MXKB1B002T5001-B (2TB)
MXKB1B500G5001-E* (500GB)
MXKB1B001T5001-E* (1TB)
MXKB1B002T5001-E* (2TB)

*Requires SafeConsole license (sold separately), also compatible with Ironkey EMS

DEVICE LANGUAGES
English, Traditional Chinese, Simplified Chinese, French, German, Japanese, Korean, Spanish

WARRANTY
5-year limited warranty

TRADE AGREEMENTS ACT COMPLIANT (TAA)
Assembled in U.S.A.

FIPS 140-2 LEVEL 3 CERTIFIED

TAA COMPLIANT

H350
SECURE TO THE CORE

A true military-grade, enterprise class mobile storage device for government and business.

DATALOCKER®

Powerful Encryption Right Out of the Box

Built to Survive Years of Wear and Tear

FIPS 140-2 Level 3 and NATO Certified

Remotely Manage and Audit Your Entire Fleet

DATALOCKER

COMPLIANCE

FEATURES

H350

BASIC

The DataLocker H350 Basic is FIPS 140-2 Level 3 certified to meet the highest security and performance needs of government agencies, military, healthcare, financial services and business organizations. Encased in a tamper resistant, high-strength aluminum enclosure, the drive features AES-XTS 256-bit hardware encryption, USB 3.2 Gen 1 performance and a Section 508 compliant control panel locialized into eight languages around the world.

ENTERPRISE

H350 Basic plus cloud-based or on-premises centralized management to customize security policies and deploy and manage secure portable devices across networks and security environments.

MANAGED H350 FEATURES

SIMPLIFY COMPLIANCE

DataLocker H350 Enterprise external hard drives make it easier to pass your data compliance audits, and to keep up with the growing list of information security mandates your agency or organization must meet, including FIPS, FISMA, GLBA, HIPPA, HITECH, and PCI.

CENTRALIZED MANAGEMENT

Rely on IronKey EMS** or SafeConsole to administer DataLocker H350 Enterprise hard drives along with other management ready devices to enforce policies. Both solutions are available in On-Prem or Cloud hosted versions and include advanced management features such as the exclusive Active Malware Defense.

With central management IT admins can centrally administer policies, securely reset passwords without deleting the drive's contents, re-commission devices that are no longer in use and remotely wipe or disable lost or stolen drives. Enterprise devices are also not usable until activated through the management system by the end user freeing up IT resource time. Existing IronKey EMS customers can also manage their IronKey Enterprise S1000, D300M/SM flash drives, and DataLocker H350 Enterprise hard drives from IronKey EMS. SafeConsole customers can now manage their DataLocker H300 and H350 enterprise hard drives with client 6.0 or later.

PERSISTENT PROTECTION

DataLocker's hardware-based encryption and password verification is always on and can't be disabled by malware or a careless user. DataLocker H350 hard drives provide robust support for complex and custom password policies including length, special characters, expiration and more. And after 10 failed consecutive password attempts, the device will either self-destruct or return to its default state. Managed DataLocker H350 Enterprise hard drives are also the only drives to offer secure password reset without erasing all the data on the drive or using a backdoor to reset the password. And with digital firmware signing and verification, along with the DataLocker Cryptochip, a hacker or malware is prevented from launching "BadUSB" or "Equation Group" type of attacks.

FAST AND RUGGED

DataLocker H350 encrypted external hard drives deliver leading performance via a fast, USB 3.2 Gen 1 connection and the H series' on-board security processor all protected by a five year warranty. Durable, quality-tested and military-grade, the DataLocker H350 drive's sleek, rugged aluminum housing ensures components stay protected no matter where the drive goes.

*Requires IronKey EMS license or SafeConsole license (sold separately)

**EMS is reaching end of life January 1, 2023. Visit this page for more information: https://support.datalocker.com/support/solutions/articles/4000155571-ironkey-ems-cloud-service-end-of-life-eol-announcement

DATALOCKER®

MANAGEMENT

FIPS 140-2 LEVEL 3 CERTIFIED

Protected by AES-XTS 256-bit encryption

SAFECONSOLE

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

SPECS

CAPACITIES
500GB, 1 TB, 2 TB

DIMENSIONS
L: 26.8 mm (1.06 in)
W: 86.6 mm (3.41 in)
D: 124.6 mm (4.91 in)

INTERFACE
USB 3.2 GEN 1 (Backwards Compatible)

SECURITY FEATURES
FIPS 140-2 Level 3 validated[1]
AES 256-bit XTS mode
Hardware-based encryption
Hardware-based password protection
Automatic data protection upon device removal
Tamper-resistant, aluminum enclosure

STANDARDS AND CERTIFICATIONS
FIPS 140-2 Level 3 (entire device)
NATO Restricted
FCC
CE
C-TICK
ICES-003
VCCI
BSMI
KCC
WEEE Compliant
RoHS Compliant
Section 508 Compliant

SYSTEM COMPATIBILITY
Microsoft Windows 10/8.1/8/7
macOS® 10.10 - 10.15
Linux® 2.6+ or higher
Citrix Ready (XenDesktop, XenApp compatible)

FORMAT OPTIONS
FAT32 supports cross platform usage (Windows, Mac, Linux)
NTFS is Windows but supports large individual files greater than 4 GB

PART NUMBERS
MXKB1B500G5001FIPS-B (500GB)
MXKB1B001T5001FIPS-B (1TB)
MXKB1B002T5001FIPS-B (2TB)
MXKB1B500G5001FIPS-E* (500GB)
MXKB1B001T5001FIPS-E* (1TB)
MXKB1B002T5001FIPS-E* (2TB)

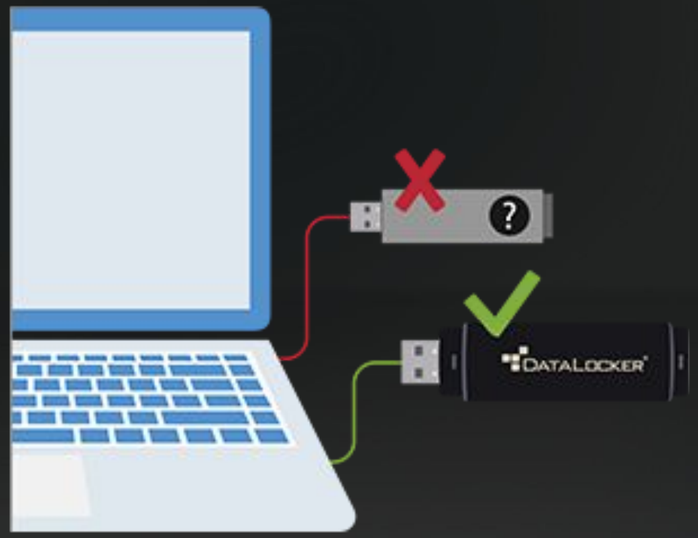
DEVICE LANGUAGES
English, Traditional Chinese, Simplified Chinese, French, German, Japanese, Korean, Spanish

WARRANTY
5-year limited warranty

TRADE AGREEMENTS ACT COMPLIANT (TAA)
Assembled in U.S.A.

[1]FIPS Certification #2826
*Requires IronKey EMS license or SafeConsole license (sold separately)

PortBlocker



MANAGED BY SAFECONSOLE®

DATALOCKER PORTBLOCKER

Prevent data loss with
USB-port blocking

DataLocker®

PORTBLOCKER

SafeConsole 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.

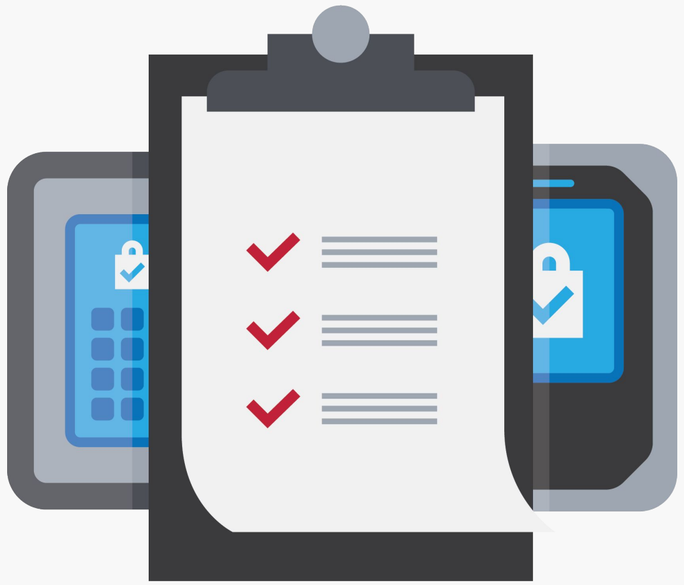
Always-On Protection
Once installed by an admin, PortBlocker will start automatically and run in the background of the user's workstation and cannot be disabled by a non-privileged user or external programs.

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.

DataLocker

REQUIREMENTS



Active SafeConsole Account

Windows™ 7 or 10, macOS

512 MB 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).

DATALOCKER
SAFECRYPT

Encrypt any file, store it
anywhere with virtual drives

Encrypted Virtual Drive

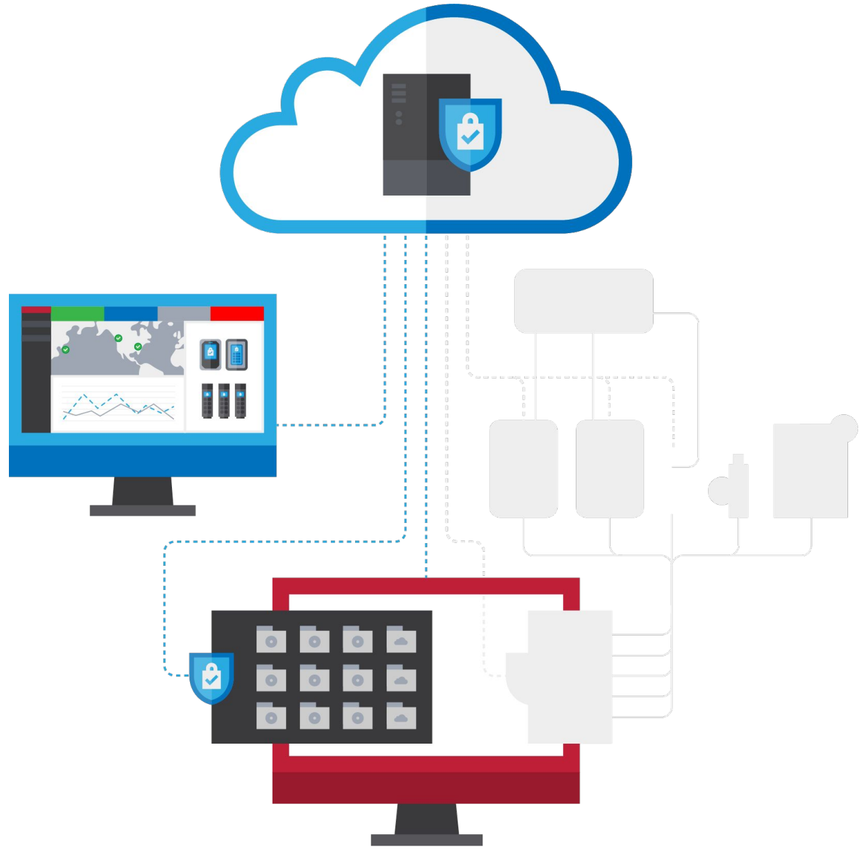
SAFECONSOLE® MANAGED

DataLocker®

SAFECRYPT

SafeConsole SAFECRYPT

Encrypt Any File, Store It Anywhere With Virtual Drives



Encryption Made Easy
Point your application to the SafeCrypt virtual drive letter and your data is fully encrypted using AES 256 FIPS 140-2 mode encryption

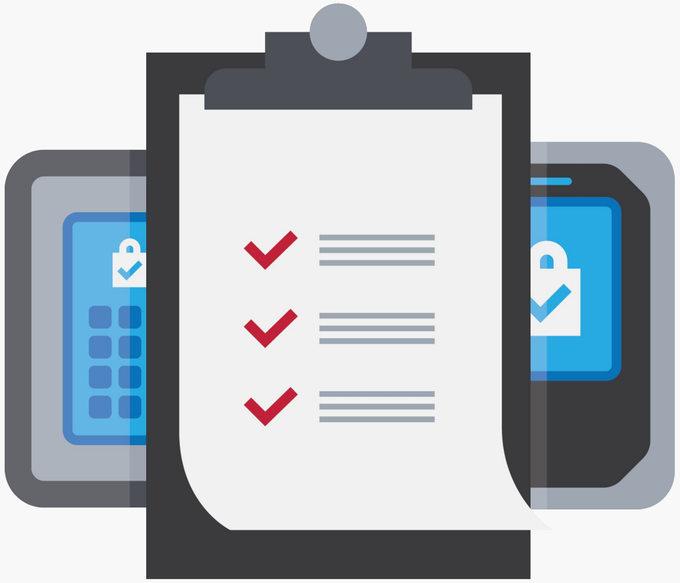
Advanced Security
Offer Advanced security like encrypted file names, read only mode, file type restrictions and options two factor authentication

Fully Compatible & Secure Virtual Drive
Supported by Windows and macOS, SafeCrypt is compatible with local files, network drives, external media and all major cloud providers

Flexible and Expandable
SafeCrypt offers quick deployment, scalable storage capacities, and central management. It is the lowest cost-per-gigabyte encrypted storage solution.

DataLocker

SPECS



CRYPTOGRAPHIC PROCESSES
AES 256-bit/CTR Mode

STANDARDS AND CERTIFICATIONS
FIPS 140-2 Validated Crypto Engine (Cert #2768)

LICENSE TYPE
1 or 3 year licenses available

PART NUMBERS
SCM-1, SCM-3, SCM-1R, SCM-3R

A new or existing SafeConsole Account is required in order to utilize and deploy SafeCrypt. A SafeCrypt license is required for each managed SafeCrypt encrypted virtual drive.

TAA COMPLIANT

ALPHACAM W
HIGH PERFORMANCE

TAA Compliant Optimized Webcam

DATALOCKER®

High-Quality Image with HD Video Capture

Easy Set Up with USB Connection

Works With Any Hardware

Microphone-Free to Prevent Data Leaks

DATALOCKER®

FEATURES

ALPHACAM W

OPTIMIZED FOR VIDEO CONFERENCES AND WEB EDUCATION

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

TAA COMPLIANT WEBCAM

The AlphaCam W 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.

ADDITIONAL FEATURES

- HD video capture (up to 1280 x 720) Vivid 5 MP photo capture
- Easy setup, no software or drivers. USB connectivity; UVC compliant
- No built-in microphone eliminates conflict with computer microphones and headsets
- Clip-on and stand style accessories included to fit notebooks, LCD or CRT monitors
- Longer USB cable: 6.5 ft (2 m) included

SPECS

VIDEO RESOLUTION
Performs HD 720p video resolution (supports up to 30 frames per second)

SNAPSHOT RESOLUTION
Up to 5 megapixel resolution

IM SERVICE
Compatible with leading IM services, Facetime, and Skype

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)

STANDARDS AND CERTIFICATIONS
TAA Compliant, FCC, KC and CE

SYSTEM REQUIREMENTS
Microsoft Windows XP Service Pack 2 or higher
Mac OS X 10.6 or higher
Linux® 2.6+
Minimum Pentium !V 2.4GHz CPU 200 MB Internal HDD
DirectX 9.0 or higher

WARRANTY
3-year limited warranty

PART NUMBER
WCAM1000-G

COUNTRY OF ORIGIN
South Korea

DATALOCKER®

TAA COMPLIANT

ALPHATALK
OPTIMAL COMFORT

TAA Compliant USB Headset

DATALOCKER®

Better Conversation with Background Noises Eliminated

Free Up Your Hands To Work On Other Tasks

TAA Compliant

DataLocker®

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.

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.

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.

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

DATALOCKER®

SPECS

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

DATALOCKER®

Introduction Videos

SAFECONSOLE®

PortBlocker

SAFECRYPT

DATALOCKER PARTNER PROGRAM

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.

DATALOCKER SOLUTIONS

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

DATALOCKER®

SIMPLY SECURE