DATALOCKER

DATALOCKER (IRONKEY) H350 BASIC AND ENTERPRISE

Secure, Centrally Managed Encrypted External Hard Drives

HARDENED MOBILE DATA STORAGE

When it comes to equipping mobile workforces with solutions that reliably and verifiably protect sensitive data, nobody beats DataLocker. And for government agencies and regulated enterprises needing secure mobile storage solutions with capacities of up to 2TB, nothing beats DataLocker H350 external USB 3.2 Gen 1 hard drives.

FIPS 140-2 Level 3 Certified From End To End

DataLocker H350 hard drives are FIPS 140-2 Level 3 validated (Certificate #2826), so they meet even the most stringent 256-bit encryption requirements mandated for government agencies, defense contractors, and healthcare and financial services enterprises. And with DataLocker H350, you'll get something else most competing solutions don't offer: the assurance that the entire drive – not just its encryption components – has been certified compliant with the FIPS 140-2 Level 3 standard. (Device-wide certification protects you from threats such as "BadUSB" and "Equation Group" attacks that target non-encryption components.) End to end, DataLocker has you —and your data – covered.

Flexible Options To Meet A Range of Needs

Choose from two versions: DataLocker H350 Basic and DataLocker H350 Enterprise. Both include our signature DataLocker Cryptochip for full disk encryption and a Section 508 Compliant control panel available in eight languages. Opt for DataLocker H350 Enterprise for the ability to centrally manage devices across the enterprise and around the world. And you can easily upgrade Basic drives to the managed H350 Enterprise hard drives.*

Key Features

DATALOCKER H350 BASIC
The DataLocker H350 Basic is FIPS 140-2 Level 3[1] certified to meet the hightest 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.

DATALOCKER H300 ENTERPRISE*
Get all the same features as the 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.

Benefits

Lock down sensitive data with **FIPS 140-2 Level 3** certified drives protected by AES-XTS **256-bit encryption**.

Securely carry up to **2TB of storage space**.

Centrally manage password policies, monitor device usage, reset passwords without deleting drive contents, and even remotely disable or destroy lost or stolen drives.**

Take advantage of all the performance improvements of **USB 3.2 Gen 1** with fast read/write speeds.

Built to survive years of wear and tear, and shielded in a solid, **tamper-resistant aluminum** enclosure.

Protect your H series investment with our **five-year limited warranty**.

*Requires IronKey EMS license or SafeConsole license (sold separately)
**DataLocker H350 Enterprise only

[1]FIPS Certification #2826

Get a Custom Demo

datalocker.com | sales@datalocker.com

THE DATALOCKER (IRONKEY) H350 MANAGED FEATURES

SIMPLIFY COMPLIANCE WITH DATALOCKER
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 PUTS YOU IN CONTROL
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 H300 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 AGAINST THREATS
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.

**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

TECHNICAL SPECIFICATIONS

CAPACITIES
500 GB, 1 TB, 2 TB

DIMENSIONS
L: 26.8 mm W: 86.6 mm
H: 124.6 mm

L: 1.06" W: 3.41" H: 4.91"

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
Anti-virus and malware protection (optional on H350 Enterprise drives only)
Tamper-resistant, aluminum enclosure

STANDARDS AND CERTIFICATION
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 and Linux® 2.6+ or higher
Citrix Ready (XenDesktop, XenApp compatible)

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

PART NUMBERS
MXKB1B500G5001FIPS-B,
MXKB1B001T5001FIPS-B,
MXKB1B002T5001FIPS-B,
MXKB1B500G5001FIPS-E*,
MXKB1B001T5001FIPS-E*,
MXKB1B002T5001FIPS-E*

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)

DataLocker®
Simply Secure

Get a Custom Demo

datalocker.com | sales@datalocker.com