



# DATALOCKER SENTRY K350 ENCRYPTED USB DRIVE

FIPS 140-2 Level 3\* Encrypted Portable Drive With Powerful Remote Management

## SECURE. MOBILE. FAST.



Quick intuitive setup and operation with on-board screen



Use strong and complex passwords with ease



Local device admin can help device user with password recovery



Manageable by SafeConsole for increased control and security



The K350 is a password protected, FIPS 140-2 Level 3 certified\*, encrypted USB drive featuring a screen that streamlines setup and operation. If the K350 is centrally managed, additional layers of organizational control strengthen the portable storage security posture further. Meet the strictest requirements and work with ease anywhere there is USB mass storage. The K350 is the slim and strong addition to DataLocker's complete portfolio of securely managed solutions, plus it's backed by a limited 3-year warranty.

### Powerful Encryption Right Out Of The Box

Everything you need to encrypt data is built into the FIPS 140-2 Level 3 and Common Criteria certified\* K350. 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 both managed and unmanaged K350 drives using the DeviceDeployer tool.

### Ensure User Adoption With Easy-to-Use Keypad

The on board screen streamlines setup and operation making it easier to operate than any keypad device on the market. The screen gives end-users quick access to secure data and allows them to customize device settings. On-screen instructions make setup fast and easy.

### Remotely Manage & Audit Your Entire Fleet

All K350 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.



\*The K350 is in process to achieve FIPS 140-2 Level 3 by NIST and Common Criteria ePP certification. The official listing as a Product under Evaluation by NIAP is expected in 2021.



Get a Custom Demo

[datalocker.com](https://datalocker.com) | [sales@datalocker.com](mailto:sales@datalocker.com)

# THE SENTRY K350 ENCRYPTED USB DRIVE

## FIPS 140-2 LEVEL 3 CERTIFICATION

FIPS 140-2 level 3 certification and Common Criteria EAL5+ certification (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. 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.

# THE SENTRY K350 MANAGED FEATURES (Requires SafeConsole)

## REMOTE DEVICE DETONATION

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

## ON BOARD ANTI-MALWARE

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

## 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.

## TECHNICAL SPECIFICATIONS

### 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 Certification pending.  
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

USB 2.0: Final speeds pending

### STANDARDS AND CERTIFICATION

FIPS 140-2 Level 3 (pending)  
TAA Compliance  
IP67 Certified  
MIL-Std 810G  
RoHS Compliant  
FCC  
CE

### MANAGEMENT COMPATIBILITY

Microsoft Windows

### 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

Part numbers pending

### DEVICE LANGUAGES

English

### WARRANTY

3-year limited warranty