

Take Total Control of USB Drives ...and More!

Data-at-Rest Design Safely Automates, Secures Use of Any
Olixir Mobile DataVault Rugged, Transportable External Storage Device

SAFE FOR GOVERNMENT USE

Government users can be confident that devices have been secured and under their control while end-users work without interruption due to the transparent design. Just create a password for the drive or media for automated functionality.

SECURING ALL MEDIA TYPES

DeviceDefender™ detects any type of PC removable drives and media. It protects data transfer on Olixir's Mobile DataVault hard drives and flash drives with USB, Firewire, SATA or eSATA connectivity.

AUTOMATIC ENCRYPTION

Drag-and-drop any type of file or folder to automatically encrypt content on Mobile DataVault removable hard drives. Fast and powerful, industry leading 256 bit AES encryption is FIPS 140-2 certified and ensures sensitive content on removable drives remains protected.

TOTAL CONTROL

DeviceDefender™ detects and blocks unauthorized devices or optionally initiates anti-malware, anti-virus scans of removable media prior to use.

DEVICE PORTABILITY

DeviceDefender™ allows users to encrypt and decrypt when the device is being used on different PCs without client side software.

SECURFLASH®

DeviceDefender™ includes SecurFlash® software, a portable encryption and decryption application for Olixir's rugged, transportable hard drives and flash drives. SecurFlash® is automatically installed at the root level of all removable drives and media to deliver continued protection wherever users access their devices.

OPTIONAL ADMINISTRATIVE SERVER

DeviceDefender Administrator Server is a web-based application for IT and Security Administrators. Users set organizational policies for removable devices, track protected drives and files used inside or shared outside of the organization, enforce organizational password policies and configure policies associated with which devices can be used in the organization as well as offline usage policies.

Dynamically revoke user access if a user is no longer trusted or if a device is lost or stolen. Remotely recover forgotten passwords, disable access to lost or stolen drives, and integrate with Microsoft Windows Single Sign-On. A full forensics audit trail is included for investigation and discovery.

SYSTEM REQUIREMENTS

Pentium or AMD (800 MHZ or higher), and 256MB Memory. JAVA Runtime Environment (JRE) 6 or higher on the PC or Server. Microsoft® Windows 2000, XP Home, XP Professional, Vista (All Versions), Server 2000, Server 2003, Server 2008



GLUE GUNNING USB PORTS NOT REQUIRED

BENEFITS OF USING OLIXIR MOBILE DATAVAULT WITH DEVICE DEFENDER™

The key to protecting against viruses is to scan files *before* they are encrypted and written to a removable device.

Olixir's Mobile DataVault hard drives and flash drives with SecurFlash® can be managed using DeviceDefender™, a Java-based Web console that audits what files are written to secured removable drives.

DeviceDefender™ can also be used to enforce security policies. If a device is stolen, DeviceDefender™ can remotely erase it when it is inserted into an Internet-connected computer.

- Blocks unauthorized devices
- Automatic encryption of approved devices
- Launches anti-malware, anti-virus scan prior to access
- Supports all manufacturer devices and media
- FIPS 140-2 certified encryption
- Optional administrator central management
- Revokes access to lost or stolen devices

MILITARY-GRADE TRANSPORTABLE STORAGE
FASTEST DATA TRANSFER, SECURES USE FOR GOVERNMENT
...and Business Worldwide

