

ENDPOINT SECURITY - DEVICE CONTROL

Organization-wide Device Management

To enhance productivity, organizations need to provide employees and partners access to data. With more employees working remotely, access is required from outside the network. But the potential impact of data loss, be it accidental or malicious, is a very real concern. And today, removable devices / media are the most common data leakage routes – no file copy limits, no encryption, no audit trails and no central management.

Lumension device Control:

- Centrally manages security policies regarding use of removable devices (e.g. USB flash drives) and media (e.g. DVDs,/CDs) using a whitelist / “default deny” approach.
- Enforces encryption policies when copying data to removable devices / media
- Prevents malware intrusion via removable devices / media adding a layer of protection to your network.
- Provides the visibility, forensics and reporting needed to demonstrate compliance with applicable laws

Key Features:

- Per Device Permissions
- File Type Filtering / Copy Limits
- Whitelist / “Default Deny”
- Offline Enforcement
- Flexible Policy with Granular Control
- Centralized Management / Admin Roles
- Policy Enforced Encryption
- Tamper-proof Agent
- File Tracking
- Flexible / Scalable Architecture



1.- Discover: Identify all removable devices that are now or have ever been connected to your end-points.

2.- Assess: Categorize all “plug and play” devices by class, group, model and /or specific ID and define policy through a whitelist approach.

3.- Implement: Enforce file copy limitations, file type filtering and forced encryption policies for data moved onto removable devices.

4.- Monitor: Track all policy changes, administrator activities and file transfers to ensure continuous policy enforcement.

5.- Report: Provide visibility into device and data usage to demonstrate compliance with corporate and/or regulatory policies.

About Bowman Technologies:

We have over 17 years of experience satisfying the needs of our customer and helping them to improve their business applications’ performance and protecting their digital assets.

We were established in 2002 and since then, we have:

- Maintained a phenomenal growth over the years.
- Experience in providing high quality solutions in diverse business areas.
- Consistent record of 60% of business coming from repeat customers
- A dedicated team of brilliant engineering professionals.
- And the most important, we are a very customer oriented organization.



Benefits

- Enable Secure Use of Productivity Tools, like USB Sticks
- Protects Data from Loss / Theft
- Enhances Security Policy Enforcement
- Limits Malware Intrusion via USB Devices
- Delivers Precise Control with Access Limits

Supported Devices

- USBs Flash Drives
- Wireless LAN
- ZIP Drives
- Digital Cameras
- Apple Devices
- CD/DVD
- Tape Drives
- Scanners
- Hard Drives
- Smart Card Readers
- Floppy Drives
- USBs Printers
- Biotech Drives
- Modems

Supported Connectivity

- USB
- LPT
- FireWire
- IrDA
- Bluetooth
- IDE
- Wi-Fi
- COM
- PCMCIA
- S-ATA
- PS/2
- SCSI