Device Control
Intelligente Schnittstellenkontrolle

Flexibel, einfach und effizient

- Einfache Konfiguration integrierter Geräte durch Machine Learning
- Nur gewünschte Geräte und externe Laufwerke werden zugelassen
- Proaktives Unterbinden von CD/DVD-Brennern
- Verhindert Dateitransfer über unverschlüsselte oder nicht zugelassene Medien
- Ermöglicht Kontrolle, wer welche Datei auf welches Medium kopiert hat
- Verschlüsselt externe USB-Datenträger auf Wunsch automatisch und sicher
- Schult Mitarbeiter im sicheren Umgang mit Daten und externen Datenträgern
- Umfangreiche forensische Analyse und Reporting

Flexibel, aber einfach und effizient

USB-Sticks sind weiterhin ein beliebtes Medium, um Daten auszutauschen. Trotz diverser Cloud-Share-Dienste wie Dropbox und dergleichen werden weiterhin USB-Sticks verwendet. Ebenfalls nutzen Mitarbeiter USB-Ports im Unternehmen zum Laden von Mobiltelefonen oder anderen Devices. Auch hierdurch kann eine Ransomware auf ein Device gelangen.
Diverse Studien zeigen, dass 80% der Arbeitnehmer bereits einmal Daten von einem oder auf einen USB-Stick kopiert oder Geräte zum Laden an den USB-Port gekoppelt haben, ohne die Folgen zu berücksichtigen. Hierbei sind vertrauliche Firmendaten plötzlich in die Öffentlichkeit gelangt oder Unternehmen hatten auf einmal eine Ransomware oder einen Trojaner auf allen Devices, die erheblichen Schaden angerichtet haben oder verbrecherische Aktivitäten – wie Erpressung – zur Folge hatten.

Doch wie kann ein Unternehmen diese Vorgänge überwachen oder gar unterbinden?

Wie kann ein Unternehmen erzwingen, dass beispielsweise angesteckte USB-Sticks automatisch verschlüsselt werden?
Die Antwort ist ganz einfach: **DriveLock Device Control** kontrolliert alle Wechseldatenträger und Geräte – von der Überwachung einer Betriebsvereinbarung bis zur Durchsetzung strenger Richtlinien sind alle Varianten einer Unternehmensrichtlinie denk- und einstellbar. Die schnelle Verteilung aller Einstellungen über Windows-Gruppenrichtlinien oder Konfigurationsdateien macht die Einführung von **DriveLock Device Control** dabei zum Kinderspiel.

Kontrolle von externen Laufwerken

- **Flexibelste Kontrolle aller extern angeschlossenen Medien: SIE legen fest, wer zu welchem Zeitpunkt welche Laufwerke verwenden darf.**
- **Integrierte Datenflusskontrolle durch Datentypprüfung: SIE legen fest, wer welche Dateien lesen oder kopieren darf.**
- **Umfangreiches Audit von Dateioperationen inklusive Schattenkopien: SIE können kontrollieren, wer zu welchem Zeitpunkt welche Datei auf welches Medium kopiert hat.**

Kontrolle von Netzlaufwerken

- **Zusätzliche Sicherheit bei Netzwerkfreigaben oder WebDAV-basierten Laufwerken: SIE legen fest, wer zu welchem Zeitpunkt welche Laufwerke verwenden darf.**
- **Integrierte Datenflusskontrolle durch Datentypprüfung: SIE bestimmen, wer welche Dateien wohin kopieren darf.**

Ausnahmen, multidimensional

Neben grundsätzlichen Richtlinien für alle Arten von Geräten kann man über Ausnahmeregeln (Whitelists) alle Einstellungen auch nach verschiedenen Kriterien vornehmen. Insgesamt 17 Dimensionen stehen hier zur Verfügung – von Benutzern und Gruppen über Tageszeiten bis hin zum Netzwerkstandort sind hier der Flexibilität keine Grenzen gesetzt.

Weitere Features

- **Größtmögliche Flexibilität durch umfassende Konfigurationsmöglichkeiten.**
- **Vordefinierte Dateifiltergruppen der gängigsten Dateitypen.**
- **Offline-Freigabe über Freischaltcodes.**
- **Remotezugriff auf Agenten und Anzeige der aktuell gültigen Einstellungen.**
- **Proaktives Unterbinden der Verwendung von CD/DVD-Brennern.**
- **Mehrsprachige, selbst konfigurierbare Benutzermeldungen.**
- **Sichere Freigabeoptionen und benutzerfreundliches Self-Servicing.**

Verschlüsselung zum Mitnehmen – DriveLock Encryption-2-Go (add-on)

Damit Sie auch von Windows- und Mac-Rechnern ohne DriveLock auf Ihre verschlüsselten Container oder Dateien auf externen Laufwerken zugreifen können, haben wir für Sie DriveLock Encryption 2-Go entwickelt.

Encryption-2-Go bietet es an, Dateien auf Wechseldatenträgern entweder mittels eines verschlüsselten Containers oder aber auf Datei- und Verzeichnisebene sicher zu verschlüsseln. Dies kann vom Endbenutzer gewählt oder vom DriveLock Administrator vorgegeben werden.

Mit DriveLock Encryption 2-Go können verschlüsselte Container als normales Laufwerk verbunden oder getrennt werden.

Die Verschlüsselung auf Verzeichnisebene erlaubt es z.B., alle Dateien auf einem Wechseldatenträger zu chiffrieren, aber ein separates Verzeichnis im Klartext vorzusehen, mittels dessen der Endbenutzer Dateien geregelt exportieren kann.

Auf Rechnern ohne DriveLock können die chiffrierten Daten mittels „DriveLock Mobile“ entschlüsselt werden.

Diese Anwendung muss dabei nicht installiert (mit Administrationsrechten) werden, sondern kann einfach als eigenständige Anwendung gestartet werden.