CenterTools DriveLock™

DriveLock™ hilft Ihnen, Sicherheitsaufgaben zu bewältigen

Die unkontrollierte Verwendung von mobilen Geräten, Anwendungen und Netzwerkverbindungen kann zum Diebstahl oder der Entwendung vertraulicher Daten führen und den Netzwerkbetrieb stören. Ein verlorener oder gestohlener Computer kann zu verschiedenen schweren Haftungsansprüchen gegenüber Ihrer Firma führen. Organisationen erkennen immer mehr die Anforderderung, ihre Netzwerk-Endpunkte unter Kontrolle zu bekommen. DriveLock™ kann Ihnen dabei helfen, viele allgemeine sicherheitsrelevante Aufgaben zu erfüllen.

"Ich muss den Diebstahl vertraulicher Daten bei der Verwendung mobiler Geräte verhindern."

- DriveLock ermöglicht Administratoren detaillierte Kontrolle der erlaubten mobilen Speichergeräte und wer diese wann, wo und wie verwenden darf.
- Konfiguration verschiedenster Lese- und Schreibberechtigungen für verschiedene Dokumententypen.

"Ich muss den versehentlichen Datenverlust durch verlorene oder gestohlene Speichermedien verhindern."

- Administratoren können die Verschlüsselung aller Daten, die auf mobile Speichergeräte kopiert werden, erzwingen.
- Die Verschlüsselung ist absolut transparent für die Anwender.
- Die Verschlüsselung kann mit jedem Wechseldatenträger verwendet werden, es muss keine extra Hardware gekauft werden.

"Anwender müssen auf verschlüsselte Daten von jedem Computer zugreifen können."

- Die Mobile Encryption Application ermöglicht den Zugriff auf verschlüsselte Daten, auch ohne DriveLock.
- Es wird keine Softwareinstallation oder Lizenz benötigt, um die Mobile Encryption Anwendung zu benutzen.
- Anwender greifen mit ihrem persönlichen Passwort auf die Daten zu, das während der initalen Verschlüsselung gewählt wurde.

"Ich muss Daten auf lokalen Festplatte schützen, um diese nicht durch Verlust oder Diebstahl zu gefährden."

- Die DriveLock Full-Disk-Encryption verschlüsselt komplette Festplatten, inklusive der System-Partition.
- Sie können eine starke Two-Factor Authentifizierung erzwingen, ohne Verbindung zur Server-Infrastruktur.
- Um Sicherheitsstandards zu erfüllen, ist eine FIPS140-2 zertifizierte Veschlüsselung mit AES-256 möglich.

"Ich muss Bedrohungen und Instabilitäten durch Verwendung nicht zugelassener Geräte unterbinden."

- DriveLock ermöglicht dem Administrator, verschiedenste Gerätetypen genaustens zu kontrollieren.
- Über Whitelist-Regeln können unternehmensweit Geräte freigegeben oder gesperrt werden.
- Eine einfache Geräteerkennung spürt jede aktuelle und vergangene Verwendung von Geräten auf, auch auf Computern ohne DriveLock.

"Um Richtlinien und Gesetze zu erfüllen, muss die Verwendung mobiler Geräte überwacht werden."

- DriveLock protokolliert die Verwendung aller Geräte und der kopierten Dateien
- Schattenkopien enthalten eine exakte Kopie der Daten, die für eine forensische Analyse verwendet werden können.
- Das Security Reporting Center fasst alle überwachten Daten zusammen und erlaubt dem Administrator die Erstellung detaillierter Berichte.

"Ich muss sicherstellen, dass Anwender sich nur mit authorisierten Netzwerken verbinden können."

- DriveLock stellt sicher, dass nur freigegebene Netzwerke verwendet werden können (Active Directory Standort, Wireless SSID, etc.).
- Geräte und Anwendungs-Regeln können auf bestimmte Netzwerke eingeschränkt werden.
- DriveLock kann die Verwendung von WLAN unterbinden, wenn der Computer mit einem kabelgebundenem LAN verbunden ist.

"Ich muss die Verwendung unauthorisierter Anwendungen unterbinden."

- Der Application Launch Filter gibt Ihnen die genaue Kontroller, wer, welche Anwendungen wann ausführen darf.
- Die Blacklist-Regeln hindern die Anwender daran, bekannte, gefährliche Programme auszuführen.
- Die Whitelist-Regeln schränken die Anwender auf freigegebene Programme ein und blockt automatisch jede unerwünschte Software.
- Unterschiedliche Konfigurationsmöglichkeiten, spezielle Regeln und die Kombination von Whitelist- und Blacklist-Regeln bieten ein Maximum an Flexibilität.

"Eine Geräte- und Anwendungskontrolle muss sich in die bestehende Infrastruktur integrieren."

- Für die Verteilung der DriveLock Richtlinien werden keine dedizierten Server oder andere zentrale Ressourcen benötigt.
- DriveLock integriert sich automatisch in Active Directory und Novell Netzwerke.
- Der DriveLock Agent benötigt kaum Systemressourcen, nur die Übertragung von Events zum zentralen Server erzeugt Netzwerkverkehr.

"Netzwerk- und Sicherheitstools müssen einfach zu implementieren und administrieren sein."

- DriveLock verwendet die vertraute Microsoft Management Konsole, die intuitiv und einfach zu bedienen ist.
- Benutzerdefinierte Nachrichten informieren den Anwender, wenn ein Gerät gesperrt wird.
- Die Whitelist-Regeln können auf erkannten Geräte basieren, um schnell und einfach Regeln zu erstellen.