

ZENTRALES BITLOCKER MANAGEMENT MIT DRIVELOCK



- ▶ Zentrale Konfiguration und ganzheitliche Umsetzung der BitLocker Verschlüsselungspolicy
- ▶ Unterstützung von Authentifizierungsmethoden wie Smartcard, Token oder Netzwerkstart
- ▶ Unterstützung aller gängigen BitLocker Authentifizierungsmethoden
- ▶ Compliance Dashboard: Verschlüsselungsstatus einzelner Geräte immer im Blick
- ▶ Sicheres und zentrales Management von BitLocker Recovery-Keys
- ▶ Stilllegung von verlorenen oder gestohlenen Geräten bei erneuter Netzwerkverbindung
- ▶ Verhindern von unbefugtem Zugriff bei außer Betrieb genommenen oder recycelten Endgeräten

Zentrales BitLocker Management mit DriveLock

Die kostenfreie BitLocker-Verschlüsselung ist ein großer Vorteil für Microsoft-Kunden und leistet einen wichtigen Beitrag zu einer verbesserten IT-Security von Unternehmen. Doch mit steigenden regulatorischen Anforderungen ist die BitLocker-Verschlüsselung allein oft nicht ausreichend. Um diese Funktionen ordnungsgemäß zu verwalten, ist eine Managementkonsole zwingend erforderlich.

Durch die Integration der BitLocker-Verwaltung in das DriveLock-Portfolio erhalten Benutzer eine benutzerfreundliche Oberfläche für die Verwaltung aller Funktionen in einer einzigen DriveLock-Konsole.

DriveLock ergänzt die BitLocker-Funktionalitäten daher um wichtige Zusatzfunktionen.

Hierzu gehören insbesondere erweiterte Konfigurationsoptionen, die zentrale Konfiguration und damit auch die ganzheitliche, unternehmensweite Umsetzung von Verschlüsselungsrichtlinien. Darüber hinaus haben Administratoren über die Management Console den Verschlüsselungsstatus einzelner Geräte immer im Blick.

Das Management von BitLocker mit DriveLock ermöglicht zentralisiertes Reporting und Hardware-Management sowie einen integrierten Challenge-/Response-basierten Helpdesk.

DriveLock bietet mit seiner Pre-Boot-Authentifizierung weitere kritische Security-Funktionalitäten und unterstützt Authentifizierungsmethoden wie Smartcard, Token oder Netzwerkstart. Dies sind relevante Funktionen für einen compliance-konformen Schutz Ihrer Endgeräte.

DriveLock Managed Security Services ermöglichen das BitLocker Management auch aus der DriveLock Cloud heraus und reduzieren damit Ihren Administrationsaufwand signifikant.

Ihre Vorteile:

▶ Reduzierter Administrationsaufwand durch zentrales Management von

- ▶ Policies,
- ▶ Stilllegungs-
- ▶ und Recovery-Maßnahmen
- ▶ Erweiterte Authentifizierungsmethoden: Smartcards, Token, Netzwerkstart
- ▶ Compliance-Dashboard: Verschlüsselungsstatus einzelner Geräte unternehmensweit immer im Blick
- ▶ Integrierte Reporting- & Forensics-Funktionen
- ▶ Unterstützt Multi- und Roaming-User
- ▶ DriveLock Managed Security Services ermöglichen BitLocker Management aus der DriveLock Cloud