

# BITLOCKER MANAGEMENT

## Erweiterte Microsoft Festplattenverschlüsselung



### **komfortabel - umfassend - sicher**

- ▶ ermöglicht die zentrale Konfiguration und unternehmensweite Umsetzung von Verschlüsselungsrichtlinien
- ▶ unterstützt alle gängigen BitLocker-Authentifizierungsmethoden mit TPM und Passwort
- ▶ gewährt jederzeit Blick auf Verschlüsselungsstatus einzelner Geräte über das Compliance Dashboard
- ▶ sicheres und zentrales Management von BitLocker Recovery-Keys
- ▶ Unterstützung von BitLocker To Go für die kontrollierte Verschlüsselung externer mobiler Laufwerke und Datenträger
- ▶ leistungsfähige Pre-Boot-Authentication (DriveLock PBA) ermöglicht u.a. weitere Authentifizierungsmethoden, die Remote-Stillegung gestohlener Geräte und Notfalleinmeldung

## Warum Festplattenverschlüsselung?

Der Schutz von Daten hat im digitalen Zeitalter höchste Priorität für Unternehmen. Der Verlust vertraulicher Informationen bedeutet nicht nur finanziellen Schaden sondern auch Reputations- und Vertrauensverlust. Daten mit Hilfe einer Festplattenverschlüsselung zu schützen, ist die einfachste Prävention vor Datenverlust, -manipulation oder -diebstahl. Eine Festplattenverschlüsselung wird vom BSI sowohl für Desktop-Clients als auch Notebooks empfohlen, insbesondere für Daten mit einem hohen Schutzbedarf.

Die Festplattenverschlüsselung ist zudem elementarer Bestandteil eines Zero Trust Sicherheitsansatz. Im Rahmen dieses Sicherheitskonzepts sollten sensible Information verschlüsselt werden und eine Entschlüsselung nur mit berechtigtem Zugang möglich sein.

## DriveLock BitLocker Management

Microsoft stellt für viele Windows-Versionen die BitLocker Festplattenverschlüsselung kostenlos zur Verfügung. Doch mit steigenden regulatorischen Anforderungen ist diese allein oft nicht ausreichend.

DriveLock BitLocker Management verwaltet Ihre bestehende BitLocker Installation und erweitert diese um wichtige Funktionen:

- zentrale, vom Active Directory (AD) unabhängige Konfiguration der BitLocker Disk Encryption – auch für Rechner ohne AD-Anbindung
- Verwaltung und Analyse des Sicherheitsstatus der Systemumgebung im gesamten Computer Life Cycle über die moderne, web-basierte Management Konsole von DriveLock
- sicheres One-Time Recovery mit automatischem Schlüsseltausch

Zudem unterstützen wir auch die Verschlüsselung externer Datenträger mit BitLocker To Go.

## Wichtiges Add-on: DriveLock PBA for BitLocker

Die optionale eigens entwickelte Pre-Boot Authentication (DriveLock PBA for BitLocker) ermöglicht nicht nur den sicheren, vertrauenswürdigen Start des Rechners (Secure Boot), sondern **erweitert den limitierten Funktionsumfang der BitLocker eigenen PBA**. Somit bleibt die Vertraulichkeit der abgelegten Daten auch im Falle von Verlust oder Diebstahl des Notebooks oder Desktops erhalten.

Die BitLocker PBA wird dabei durch die DriveLock PBA ersetzt. Das Betriebssystem selbst wie auch weitere Third Party Sicherheitslösungen können ohne Beeinträchtigung initialisiert und gestartet werden.

Unsere DriveLock PBA bietet Ihnen gegenüber der BitLocker PBA wesentliche Vorteile:

- Login mit Windows Benutzername / Domäne und Passwort
- Zwei-Faktor Authentifizierung mittels kryptographischer Smartcards oder Token
- Single-Sign-On am Windows Betriebssystem möglich
- Self-Service Notfalleinmeldung bei vergessenen Zugangsdaten
- Netzwerk-Unlock: Sichere automatisierte Freischaltung bei Netzwerkverbindung mit dem zentralen DriveLock Enterprise Server
- Synchronisation der Benutzer mit dem Microsoft Active Directory für Initial-Auslieferungen oder Updateprozesse
- individualisierbarer Anmeldebildschirm
- Unterstützung für eine große Anzahl an internationalen Tastaturbelegungen
- On-Screen-Tastatur für die Anmeldung an touch-fähigen Windowsgeräten wie Microsoft Surface

## Wussten Sie übrigens? BitLocker Management aus der Cloud

DriveLock Managed Security Services ermöglichen das BitLocker Management auch aus der Cloud heraus. Profitieren Sie von:

- ▶ Kostenvorteilen
- ▶ schneller Bereitstellung & automatischen Updates
- ▶ vordefinierten Sicherheitsrichtlinien

Mehr erfahren Sie unter [drivelock.de/managed-security-services/](https://drivelock.de/managed-security-services/)

## Ihre Vorteile von DriveLock BitLocker Management im Überblick

- ▶ reduzierter Administrationsaufwand durch zentrales Management von Policies, Stilllegungs- und Recovery-Maßnahmen
- ▶ erweitere Authentifizierungsmethoden: Smartcards, Token, Netzwerkstart und Single-Sign-On
- ▶ 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 Cloud

### Alles aus einer Hand:

DriveLock bietet BitLocker Management als einen Baustein seiner Zero Trust Plattform zur Realisierung einer gesamtheitlichen Sicherheitsstrategie an.