DriveLock
securing your digital tomorrow

DriveLock Native Security Management: Komfortable und zentrale Verwaltung der Microsoft Sicherheitsfunktionen

Microsoft BitLocker Festplattenverschlüsselung, Defender Antivirus, Firewall Management und die lokalen Sicherheitseinstellungen im Betriebssystem gehören zu einem Set an nativen Security Lösungen, die Microsoft seinen Kunden zur Verfügung stellt. Für viele Unternehmen sind sie fester Bestandteil ihres IT Sicherheitskonzepts. DriveLock vereinfacht das Management der nativen Security Lösungen, ergänzt sie um wichtige Funktionen und schafft einen echten Mehrwert zu mehr effektiver Cyber-Sicherheit.

Große Anbieter von Betriebssystemen wie Microsoft haben ihre integrierten Sicherheitsfunktionen kontinuierlich erwei tert. Die unter dem Begriff „Native Security" oder „OS Security" bezeichneten Sicherheitsfunktionen umfassen Sicherheitskontrollen zur Datensicherheit/Festplattenverschlüsselung, Antivirenschutz, Schutz vor Zero Day-Exploits und Firewall Management. Sie können aus der Betriebssystemoberfläche heraus verwaltet werden. Die Lösungen werden je nach Lizenzumfang bei der Anschaffung des Betriebssystems mitgeliefert. IT Verantwortliche müssen nicht länger auf eine Vielzahl von Lösungen setzen.

Die nativen Sicherheitsangebote decken in der immer professionelleren Welt der Cyberattacken nicht nur wichtige Grundfunktionen für IT Sicherheit ab, sondern liefern wertvolle Daten. **Bei deren Weiterverarbeitung durch ein professionelles Tool erlangen Sie zusätzlich einen verhaltensbasierten Schutz und somit mehr Sicherheit**. Hier kommt DriveLock ins Spiel.

DriveLock Native Security Management

DriveLock optimiert die Verwaltung nativer Sicherheitsfunktionen und ermöglicht das Einrichten zentraler Sicherheitsrichtlinien. So werden native Lösungen auch der Komplexität großer Unternehmen mit Tausenden von Arbeitsplätzen, Berechtigungen und Profilen gerecht.

DriveLock erweitert auch den Funktionsumfang um wichtige Features, wie zum Beispiel die Microsoft BitLocker Festplattenverschlüsselung um eine leistungsfähige Pre-Boot-Authentifizierung (PBA).

Native Sicherheitsfunktionen generieren zusätzlich nützliche Informationen für die Verhaltensanalyse. Damit kann DriveLock seine Lösung mit Sicherheitsprotokolldaten aus dem Betriebssystem ergänzen und weiterverarbeiten. Durch die Analyse der Laufzeitaktivitäten von Anwendungen und Geräten bietet DriveLock einen verhaltensbasierten Schutz, und kann potenziell laufende Angriffe erkennen und darauf reagieren.

Mit dem Native Security Management Modul bietet DriveLock eine zentrale Verwaltung über eine einzige Oberfläche und ermöglicht IT-Abteilungen ein komfortables Arbeiten.

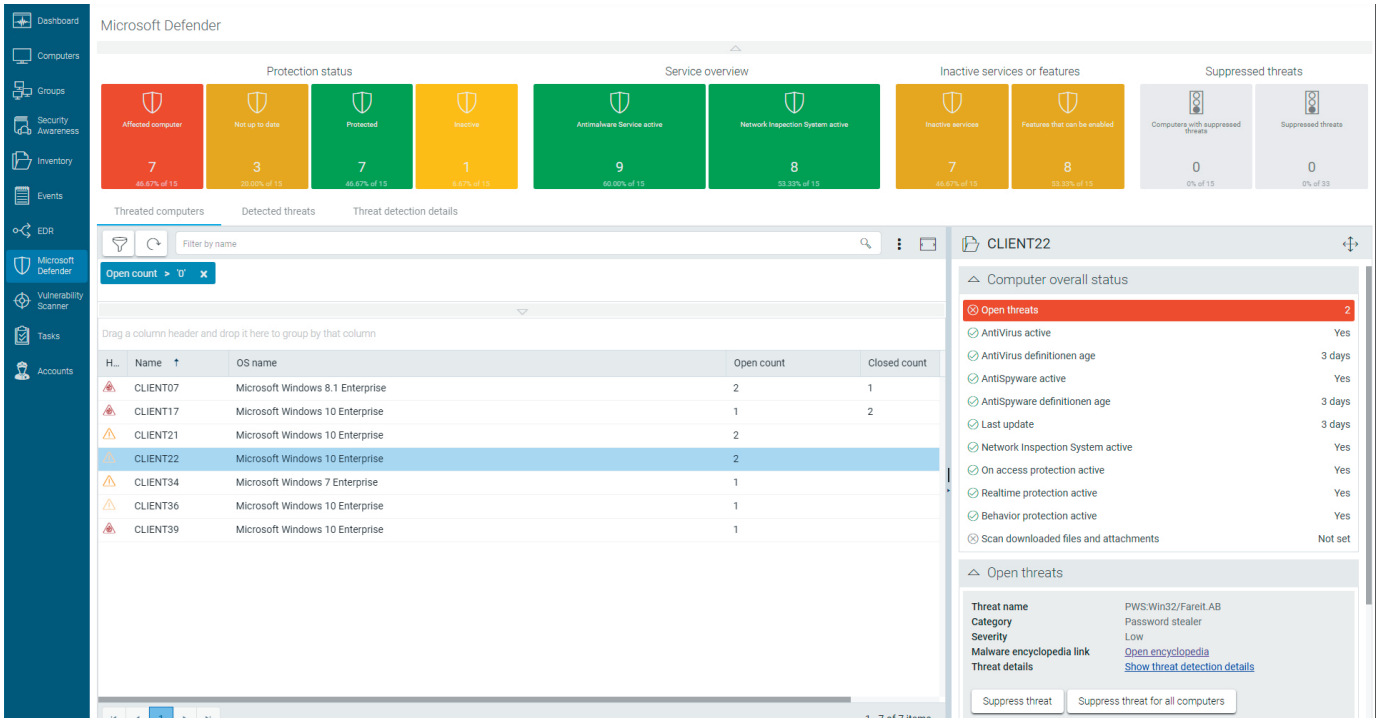
Mit DriveLock holen Sie mehr aus Native Security heraus!

Vorteile DriveLock Native Security Management

+ SCHONT RESSOURCEN UND VERMEIDET INKOMPATIBILITÄTEN
+ VEREINFACHT DIE KONFIGURATION DER WICHTIGSTEN, IM BETRIEBSSYSTEM VERANKERTEN SCHUTZMASSNAHMEN VON EINER ZENTRALEN STELLE AUS
+ ERMÖGLICHT DIE DARSTELLUNG DES SICHERHEITSNIVEAUS ÜBER ALLE SCHUTZMASSNAHMEN HINWEG
+ REICHERT DIE VERHALTENSANALYSE MIT DEN VOM BETRIEBSSYSTEM GESAMMELTEN EREIGNIS DATEN AN UND VERVOLLSTÄNDIGT DIE COMPLIANCE-ÜBERSICHT
+ VEREDELT DIE VON DEN BETRIEBSSYSTEMHERSTELLERN ANGEBOTENEN SICHERHEITSFUNKTIONEN
+ ERMÖGLICHT DIE ANWENDUNG UND KONTROLLE NATIVER SICHERHEIT UNABHÄNGIG VON DER JEWEILIGEN INFRASTRUKTUR DER OS-HERSTELLER UND PASST SICH DENNOCH INDIVIDUELL AN DIE HYBRIDE KUNDENINFRASTRUKTUR AN

Cyberbedrohungen - Status Quo

+ DIE KOSTEN FÜR DATA BREACHES BELAUFEN SICH IM 3-STELLIGEN MILLIONEN-BEREICH.
+ Ø FOLGEKOSTEN EINER ATTACKE: 4,2 MIO. US-$



Vorteil von DriveLock Native Security – ein Agent

DriveLock verwaltet und überwacht die Microsoft Sicherheitsfunktionen nicht nur zentral in einer Management-Konsole, sondern Sie benötigen mit Drivelock nur einen **einzigen Agenten auf dem Endpoint:** Das schont Ressourcen und vermeidet Inkompatibilitäten.

DriveLock ermöglicht ein integriertes Management aller Module sowohl lokal installiert („on premise") als auch als Managed Service aus der Cloud.

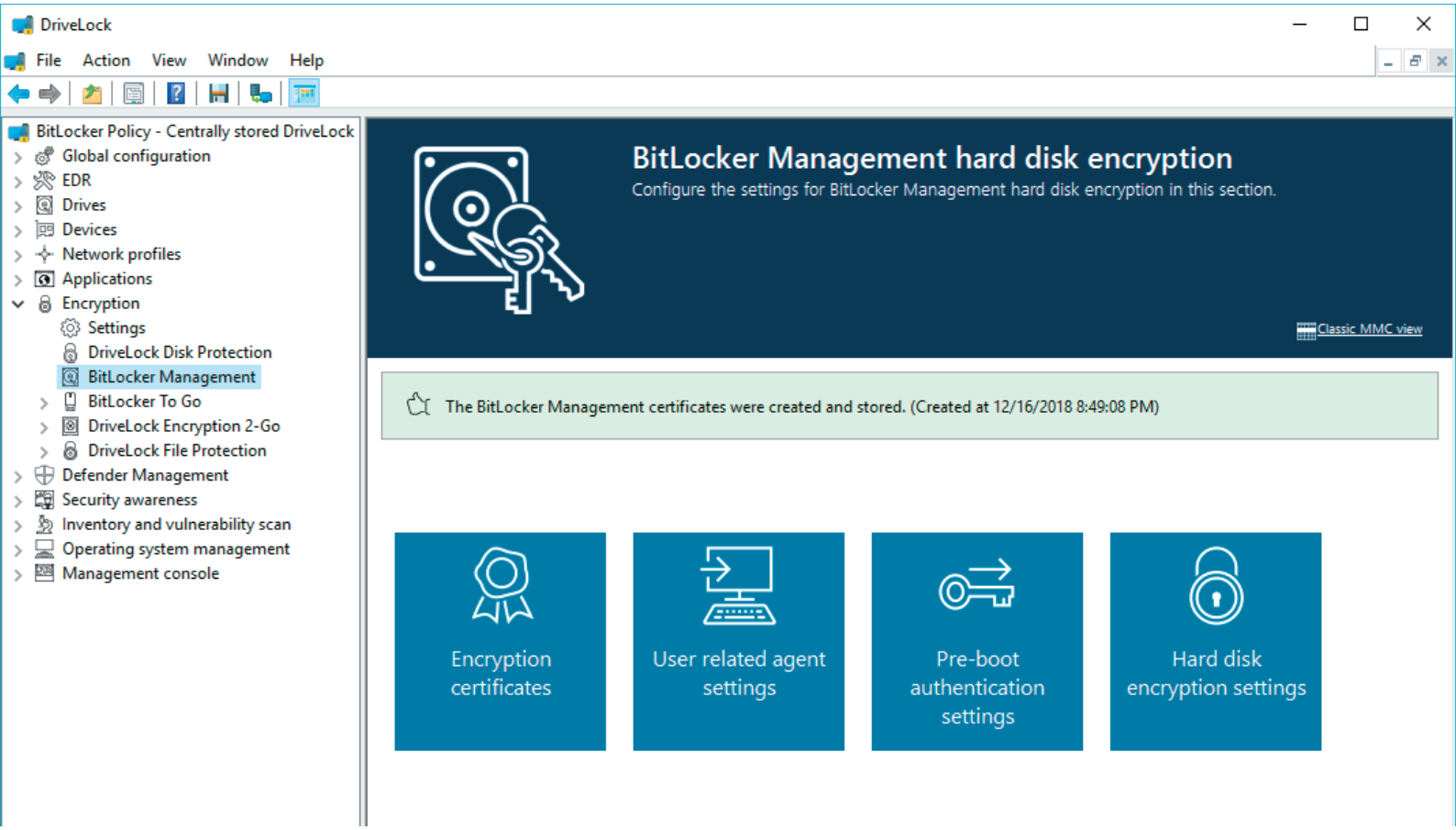
Die Bausteine des DriveLock Native Security Managements

Microsoft Defender Antivirus Management

Der in Windows 10 integrierte Echtzeitschutz Microsoft Defender Antivirus leistet einen wichtigen Beitrag zur Erkennung und Beseitigung von Schadsoftware und unerwünschten Programmen. Doch Antiviren-Software ist nur ein Baustein in einer kompletten Sicherheitslösung. DriveLock nutzt die Scan-Ergebnisse optimal, integriert das Management von Microsoft Defender Antivirus in seine Zero Trust-Plattform und ermöglicht eine gemeinsame, komfortable und zentrale Verwaltung zusammen mit den DriveLock Werkzeugen zur Prävention und Erkennung. Das sind die DriveLock Applikationskontrolle, Schnittstellenkontrolle und Endpoint Detection & Response (EDR).

Vorteile des DriveLock Defender Antivirus Managements

- **VERWALTEN SIE ALLE MS DEFENDER AV-EINSTELLUNGEN INNERHALB EINER DRIVELOCK RICHTLINIE ZENTRAL, EINFACH UND SCHNELL OHNE GRUPPENRICHTLINIEN.**
- **MANAGEMENT AUCH OHNE MICROSOFT INTUNE ODER SCCM MÖGLICH.**
- **GEWÄHRT JEDERZEIT DEN EINBLICK IN DIE AKTUELLE SICHERHEITSLAGE**
- **VISUALISIERT DIE KLASSIFIZIERUNG VON GEFUNDENER SCHADSOFTWARE UND ZEIGT STATUSÄNDERUNGEN UND BEDROHUNGS-GRADE IM ZEITVERLAUF**
- **NUTZT SCAN-ERGEBNISSE FÜR DRIVELOCK-FUNKTIONEN WIE APPLIKATIONS- UND GERÄTE KONTROLLE UND EDR**
- **IM ZUSAMMENSPIEL MIT DER DRIVELOCK SCHNITTSTELLENKONTROLLE SCANNEN SIE EXTERNE DATENTRÄGER VOR IHRER FREIGABE UND BENUTZUNG.**
- **DRIVELOCK EDR NUTZT DIE SCAN-ERGEBNISSE ALS BASIS FÜR REGELN ZUR ERKENNUNG, LÖST ALARME AUS UND LEITET MASSNAHMEN ALS REAKTION EIN.**



Microsoft BitLocker Management

Festplattenverschlüsselung ist eine wirksame Maßnahme zum Datenschutz und Wahrung der Vertraulichkeit von Informationen. Sie ist eine effektive Prävention vor Datenverlust, -manipulation oder -diebstahl und wird vom Bundesamt für Informationssicherheit für Desktop-Clients und Notebooks empfohlen. 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 wie One-Time-Recovery oder eine zentrale, vom Active Directory (AD) unabhängige Konfiguration der BitLocker Disk Encryption. Mit DriveLock BitLocker Management reduzieren Sie den Administrationsaufwand durch ein zentrales Management aller Einstellungen.

Vorteile des DriveLock BitLocker Managements

- + ERMÖGLICHT DIE ZENTRALE KONFIGURATION UND UNTERNEHMENSWEITE UMSETZUNG VON VERSCHLÜSSELUNGSRICHTLINIEN
- + REDUZIERT DEN ADMINISTRATIONSAUFWAND
- + ENTHÄLT EIN COMPLIANCE DASHBOARD
- + ERMÖGLICHT EINE ZENTRALE, VOM ACTIVE DIRECTORY UNABHÄNGIGE KONFIGURATION
- + LEISTET EIN SICHERES ONE-TIME RECOVERY MIT AUTOMATISCHEM SCHLÜSSELTAUSCH
- + BIETET EINE LEISTUNGSFÄHIGE PRE-BOOT-AUTHENTIFIZIERUNG: DRIVELOCK PBA FÜR BITLOCKER. DIESE ERMÖGLICHT U.A. WEITERE AUTHENTIFIZIERUNGSMETHODEN UND NOT FALLANMELDUNG.

DriveLock
securing your digital tomorrow

Vereinfachte Verwaltung von Firewall-Regeln

Microsoft Firewall hat zum Ziel, an vorderster Front primäre Einfallstore für Kriminelle zu schließen, u. a. durch Aktivierung bzw. Deaktivierung von Portfreigaben. Mit DriveLock haben Sie die Verwaltung von Microsoft Defender Firewall-Regeln noch besser im Griff. Mit DriveLock-Richtlinien regeln Sie ganz einfach die ein- und ausgehenden Verbindungen. Zusätzlich können die Firewall-Regeln mit den Kriterien wie Zeit, Netzwerkverbindung, Computer oder Benutzer in der DriveLock Policy verknüpft werden.

Vorteile des DriveLock Firewall Managements

- + VERWALTET EINFACH UND ZENTRAL SÄMTLICHE EINSTELLUNGEN DER LOKALEN WINDOWS FIREWALL
- + NUTZT DIE VORTEILE VON DRIVELOCK-RICHTLINIEN, UM FLEXIBEL AUF UNTERNEHMENSSPEZIFISCHE SICHERHEITSANFORDERUNGEN REAGIEREN ZU KÖNNEN
- + DRIVELOCK-REGELN ERMÖGLICHEN DIE DYNAMISCHE ANPASSUNG DER FIREWALL EINSTELLUNGEN IM LAUFENDEN BETRIEB BASIEREND AUF AKTUELLEM BENUTZER, GRUPPEN, COMPUTERN ODER ZEIT.

Local Users & Groups Management

Insbesondere die im Betriebssystem vordefinierten lokalen Konten und Gruppen sind das Ziel von Angreifern. Der Zweck dieser Integration in DriveLock ist der Schutz vor so genannten „Privilege Escalation"-Angriffen, bei denen versucht wird, auf bestehende Konten mit administrativen Rechten zuzugreifen oder diese zu übernehmen. Diese Konten können Sie mit DriveLock zusätzlich schützen: Sowohl das Passwort des Administratorkontos als auch dessen Name können täglich zufällig vergeben werden. Verwalten Sie mit DriveLock Ihre lokalen Benutzer und Gruppen. Jedes lokale Konto auf einem einzelnen Computer kann erstellt, aktualisiert oder gelöscht werden. Passwort-Einstellungen sind ebenfalls möglich. Der DriveLock Agent speichert jedes Passwort sicher verschlüsselt, so dass das Arbeiten mit einer „run as" Kommandozeile weiterhin möglich ist. Auf Basis von Regeln lassen sich die Einstellungen automatisch ändern, wenn ein Benutzer vom Home Office ins Firmennetzwerk wechselt und umgekehrt.

Vorteile des DriveLock Local Users & Groups Managements

- + DIESE SEHR EFFEKTIVE METHODE SICHERT IHREN ARBEITSPLATZ NOCH BESSER AB.
- + SCHÜTZT VOR „PRIVILEGE-ESCALATION"
- + ZENTRALE VERWALTUNG ALLER LOKALEN KONTEN UND GRUPPEN AUF JEDEM COMPUTER
- + AUTOMATISCHES AKTIVIEREN ODER DEAKTIVIEREN VON BETRIEBSSYSTEM-KONTEN
- + ZUFÄLLIGE PASSWORTÄNDERUNG DER KONTEN
- + „RUN AS" (AUSFÜHREN ALS) KOMMANDOZEILE AUF NOCH SICHERERE UND KOMFORTABLERE WEISE
- + AUTOMATISCHES ÄNDERN VON EINSTELLUNGEN IN ABHÄNGIGKEIT DAVON, OB MAN SICH Z. B. IM LAN ODER ZU HAUSE BEFINDET

DriveLock: Experte für IT- und Datensicherheit seit mehr als 20 Jahren

Das deutsche Unternehmen DriveLock SE wurde 1999 gegründet und ist inzwischen einer der international führenden Spezialisten für cloud-basierte Endpoint-und Datensicherheit. Die Lösungen umfassen Maßnahmen der Prävention wie auch zur Erkennung und Eindämmung von Angreifern im System.

DriveLock ist Made in Germany mit Entwicklung und technischem Support aus Deutschland.