DriveLock
securing your digital tomorrow

DriveLock Microsoft Security Tools: Holen Sie das Maximum aus Microsoft Security-Funktionen* mit DriveLock heraus.

eBook

* BitLocker, Defender Antivirus, Firewall Management, Local Users & Groups Management

DriveLock
securing your digital tomorrow

Inhalt

1. Verwalten Sie Ihre Microsoft-Produkte zentral, reduzieren Sie Ihren Pflegeaufwand und profitieren Sie von wichtigen Zusatzfunktionen.

BitLocker Festplattenverschlüsselung, Defender Antivirus und die lokalen Sicherheitseinstellungen im Betriebssystem gehören zu einem Set an Security Lösungen, die Microsoft seinen Kunden zur Verfügung stellt.
Für viele Unternehmen sind diese fester Bestandteil ihres IT Sicherheitskonzepts: Jede Sicherheitslösung bedeutet eine Hürde mehr, die Angreifer überwinden müssen. Ziel ist es, Cyberkriminellen ihre Arbeit so schwer wie möglich zu machen.

Mit der Zunahme an Security Tools steigt die Komplexität für Administratoren und Sicherheitsverantwortliche. Sicherheitsrichtlinien, Profile und Berechtigungen müssen verwaltet werden. Anders gesagt: Je mehr Tools, Endgeräte und User desto komplexer wird es.

Mit der Devise „IT Security made easy" setzen wir uns als Endpoint Security Spezialist zum Ziel, mehr aus den Microsoft Security Tools herauszuholen. DriveLock optimiert deren Verwaltung und ermöglicht das Einrichten zentraler Sicherheitsrichtlinien. So werden die Lösungen auch der Komplexität großer Unternehmen mit Tausenden von Arbeitsplätzen, Berechtigungen und Profilen gerecht. Dabei verwalten Administratoren die Sicherheitsfunktionen zentral in einer Management Konsole mit einem einzigen Agenten.

DriveLock optimiert aber nicht nur das Management der Microsoft Security Tools, sondern ergänzt sie auch um wichtige Funktionen und schafft durch die Kombination der aus den Betriebssystemen erhobenen Daten mit DriveLock einen echten Mehrwert, der in mehr Sicherheit mündet.

Mit DriveLock verleihen Sie Ihren Microsoft Security Tools vollen Schub!
Testen Sie DriveLock kostenlos und unverbindlich unter https://www.drivelock.com/de/microsoft-security-tools

2. Warum wir aus betriebssystemeigenen Tools noch mehr herausholen können.

Die großen Anbieter von Betriebssystemen wie Microsoft haben ihre integrierten Sicherheitsfunktionen kontinuierlich verbessert. Die integrierten Sicherheitsfunktionen umfassen Sicherheitskontrollen zur Datensicherheit/ Festplattenverschlüsselung, Antivirenschutz, Schutz vor Zero Day-Exploits und Firewall Management. Sie können aus der Betriebssystemoberfläche verwaltet werden. Die Lösungen werden – je nach Lizenzumfang – bei der Anschaffung des Betriebssystems mitgeliefert. Zudem müssen IT Verantwortliche nicht länger eine Vielzahl von Lösungen anschaffen. Viele Fachleute für IT Sicherheit in Unternehmen, planen den Einsatz von Sicherheitstools zu erhöhen - als Bestandteil Ihrer IT-Sicherheitsstrategie.

Mehr Daten, mehr Information, mehr Sicherheit.

Die Microsoft Security Tools decken in der zunehmend professionellen Welt der Cyberattacken wichtige Grundfunktionen für IT Sicherheit ab und liefern wertvolle Daten. Intelligente Software zur Abwehr von Bedrohungen (sog. Threat-Intelligence-Lösungen) wie die DriveLock Zero Trust Platform, verarbeiten die vom Betriebssystem erhobenen Sicherheitsprotokolldaten weiter. Sie erweitern die IT-Schutzfunktionen um einen verhaltensbasierten Schutz, insbesondere durch die Analyse der Laufzeitaktivitäten von Anwendungen und Geräten, und bieten somit noch mehr Sicherheit.

In Kombination mit Daten aus den Sicherheitskontrollen schützt die DriveLock Zero Trust Platform IT-Umgebungen noch besser vor Cyberattacken und weist auch auf potenziell laufende Angriffe hin. Demnach ergänzt DriveLock seine eigene Funktionalität vorteilhaft mit denen der Microsoft Security Tools und bietet optimalen Schutz. Mit der Microsoft Security Tool Anwendung bietet DriveLock eine zentrale Verwaltung über eine einzige Oberfläche und ermöglicht IT-Abteilungen ein komfortableres Arbeiten.

DriveLock
securing your digital tomorrow

3. DriveLock verstärkt die Funktionalitäten der Microsoft Security Tools.

DriveLock schöpft das Maximum aus den Microsoft Security Tools und eigenen Sicherheitsfunktionen. DriveLock bündelt die jeweiligen Stärken der Microsoft Security Tools und unterstützt sie im Zusammenspiel ideal. Darüber hinaus verbessert DriveLock durch seine integrierten Sicherheitsfunktionen, wie z. B. **Device Control, Application Whitelisting oder Security Awareness**, das Schutzniveau der Endpoints deutlich.

Das sind die Vorteile der Verwaltung von Microsoft Security Tools mit DriveLock:

- DriveLock vereinfacht die Konfiguration der wichtigsten, im Betriebssystem verankerten Schutzmaßnahmen von einer zentralen Stelle aus.
- DriveLock ermöglicht die ganzheitliche Darstellung des aktuellen Sicherheitsniveaus über alle Schutzmaßnahmen hinweg.
- DriveLock reichert die Verhaltensanalyse mit den vom Betriebssystem gesammelten Ereignisdaten an und vervollständigt die Compliance-Übersicht.
- DriveLock veredelt die von den Betriebssystemherstellern angebotenen Sicherheitsfunktionen.
- DriveLock ermöglicht die Anwendung und Kontrolle von Microsoft Security Tools unabhängig von der jeweiligen Infrastruktur der OS-Hersteller und passt sich dennoch individuell an die hybride Kundeninfrastruktur mit unterschiedlichen Endgeräten an.

DriveLock kann nicht nur Sicherheitselemente zentral verwalten und überwachen, sondern die Lösung benötigt nur einen einzigen Agenten auf den Endpunkten.

Mit DriveLock benötigen Sie nur einen einzigen Agenten auf dem Endpoint:
Sie verwalten und überwachen die **Microsoft Sicherheitsfunktionen zentral in einer Management Konsole**.
Das spart Ressourcen und vermeidet Inkompatibilitäten.

DriveLock ermöglicht ein integriertes Management der Microsoft Security Tools sowohl lokal installiert („on premise“) als auch aus der Cloud.

4. Die Bausteine der Verwaltung von Microsoft Security Tools mit DriveLock.

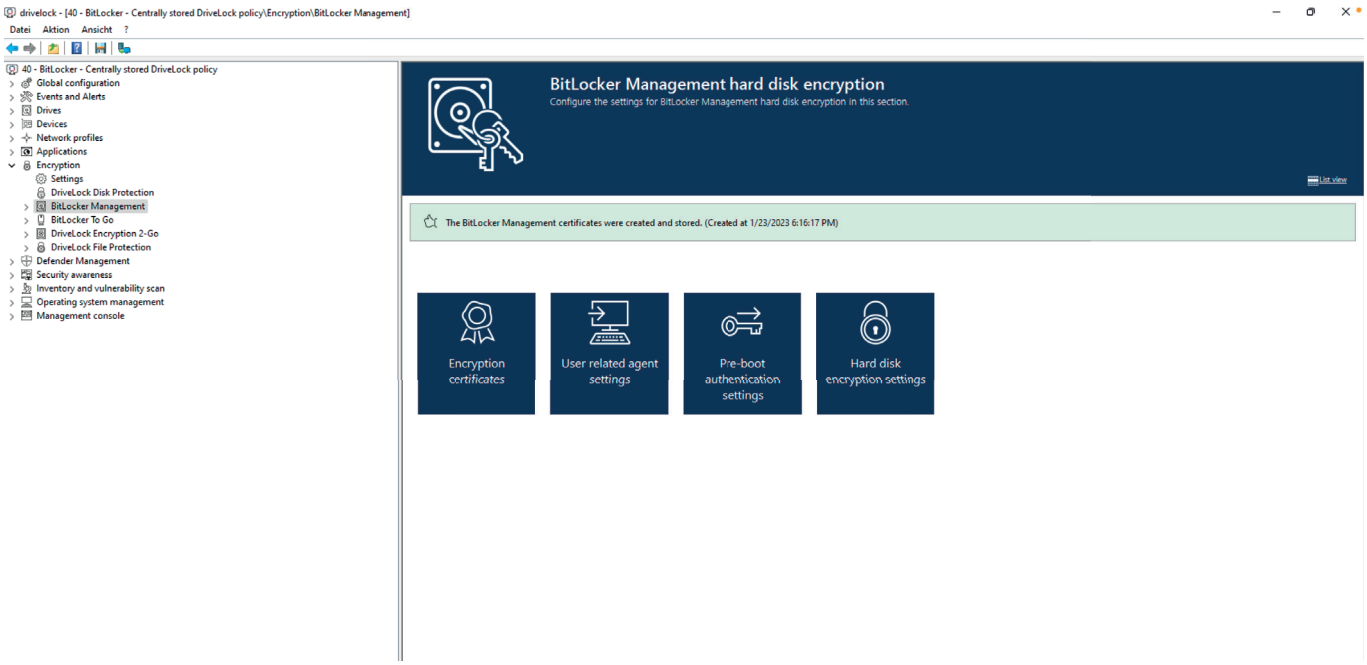
4.1 BitLocker Management

Festplattenverschlüsselung ist eine wirksame Maßnahme zum Datenschutz und zur Wahrung der Vertraulichkeit von Informationen. Sie ist die einfachste 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. So reduzieren Sie den Administrationsaufwand durch ein zentrales Management aller Einstellungen.

Die 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 Notfallanmeldung.



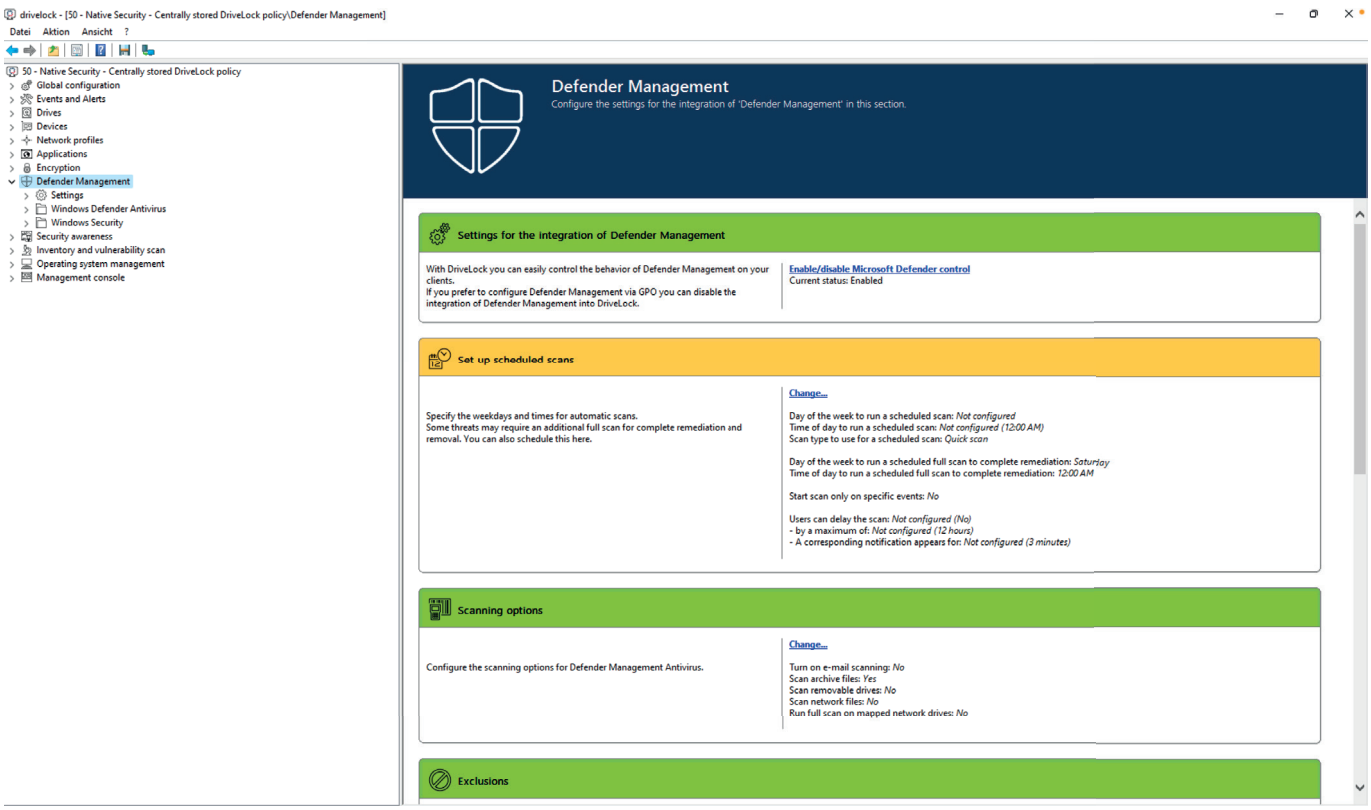
4.2 Defender Antivirus Management

Der in Windows 10/11 vorinstallierte Echtzeitschutz Microsoft Defender Antivirus leistet einen wichtigen Beitrag zur Erkennung und Beseitigung von Schadsoftware und unerwünschten Programmen. Doch Virenscanning ist nur ein Baustein in einer kompletten Sicherheitslösung.

DriveLock integriert das Management von Microsoft Defender Antivirus in seine Zero Trust Platform und ermöglicht eine gemeinsame, komfortable zentrale Verwaltung der DriveLock Präventionswerkzeuge **Applikationskontrolle, Schnittstellenkontrolle** und **Security Awareness** mit Microsoft Defender Antivirus.

Die Vorteile des DriveLock Defender Antivirus Managements:

- zentrale richtliniengesteuerte Konfiguration
- scannt extern angeschlossene Laufwerke auf Bedrohungen, bevor sie freigeschaltet werden
- gewährt jederzeit den Einblick in die aktuelle Sicherheitslage
- visualisiert die Klassifizierung von gefundener Malware
- zeigt Statusänderungen und Bedrohungsgrade im Zeitverlauf
- Wiederverwendung der Scan-Ergebnisse und Nutzung für andere DriveLock-Funktionen wie zentrale Alarme



4.3 Firewall Management

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-Richtlinien noch besser im Griff.

Mit DriveLock-Richtlinien regeln Sie ganz einfach die ein- und ausgehenden Verbindungen. Zusätzlich können die Firewall-Richtlinien mit den Kriterien wie Zeit, Netzwerkverbindung, Rechner oder sogar Benutzer in der DriveLock Richtlinie verknüpft werden.

Die Vorteile des DriveLock Firewall Managements:

- verwaltet einfach und zentral sämtliche Einstellungen der Windows Firewall
- nutzt die Vorteile von DriveLock-Richtlinien, um flexibel auf unternehmensspezifische Sicherheitsanforderungen reagieren zu können
- DriveLock-Richtlinien ermöglichen die dynamische Anpassung der Firewall Einstellungen im laufenden Betrieb basierend auf aktuellem Benutzer, Gruppen, Computern oder Zeit

4.4 Local Users & Groups Management

Insbesondere die im Betriebssystem vordefinierten lokalen Konten und Gruppen sind das Ziel von Angreifern. Der Zweck dieser Integration 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, indem z. B. das Passwort des Kontos „Administrator" oder auch der Name täglich nach dem Zufallsprinzip geändert wird.

Die wichtigsten Vorteile des DriveLock Local Users & Groups Management:

- effektiver Schutz vor „Privilege Escalation"
- zentrale Verwaltung aller lokalen Konten und Gruppen auf jedem Endpunkt
- automatisches Aktivieren oder Deaktivieren von Konten auf dem Betriebssystem
- 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
securing your digital tomorrow

5. Fazit: DriveLock und Microsoft Security Tools - ein perfektes Zusammenspiel.

Microsoft Security Tools und DriveLock Dienste arbeiten zusammen und ergänzen sich gegenseitig. Mit DriveLock schaffen wir für unsere Nutzer einen Mehrwert, indem wir alle Dienste von einer Benutzeroberfläche aus und mit einem Agenten anbieten.

DriveLock hat es sich zur Aufgabe gesetzt, Unternehmensdaten, Geräte und Systeme zu schützen. Um dies zu erreichen, setzen wir auf Technologien und Lösungen, die auf dem Zero Trust Modell basieren. DriveLock bringt Zero Trust auf die Endgeräte. Die voll integrierte Zero Trust Platform unterstützt mehrere Betriebssysteme und Endgeräte und wird sowohl als On-Premise-Lösung als auch als Cloud Managed Security Service angeboten.

Die DriveLock Zero Trust Platform kombiniert die Elemente:

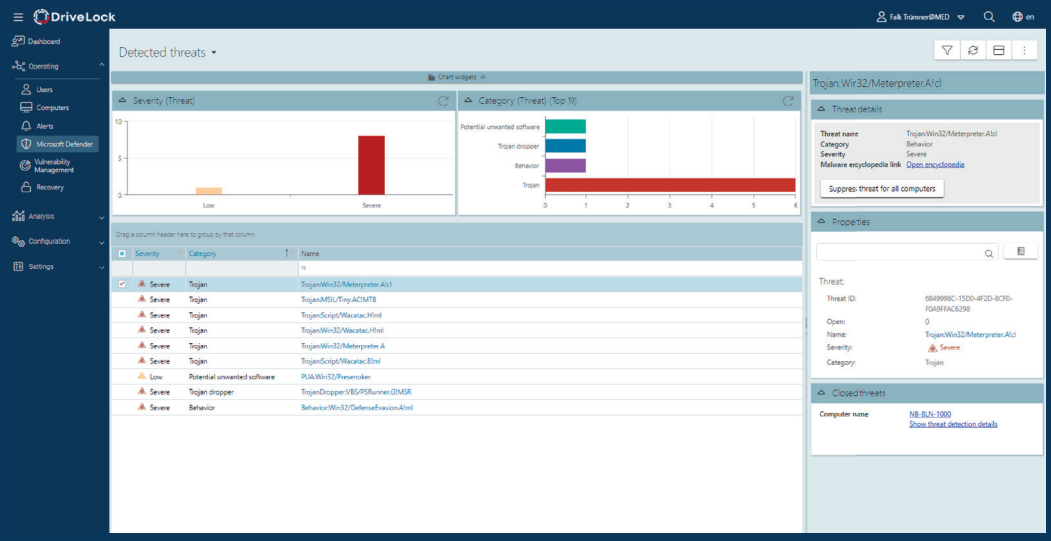
- Data Protection
- Endpoint Protection
- Security Awareness und
- Access Control

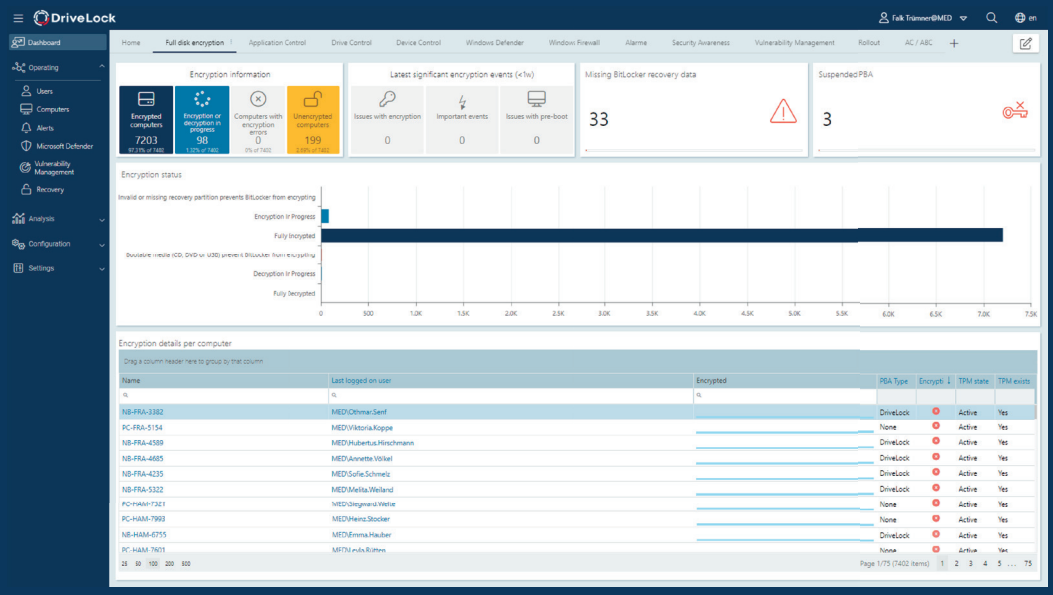
Wir bieten ganzheitlichen Schutz mittels verschiedener Anwendungen, u. a.:

- Festplatten- oder Wechseldatenträgerverschlüsselung zum Schutz der Daten von gestohlenen oder verlorenen Laptops und Wechseldatenträgern
- Application Control zum Schutz vor Zero-Day-Attacken und „living off the land"-Angriffen (fileless)
- Gerätekontrolle bietet Schutz vor Malware und somit auch vor Datendiebstahl
- Security Awareness Trainings stärken Ihre Human Firewall und binden Anwender in die Sicherheitsstrategie ein
- Integriertes BitLocker & Defender Management - Integriertes Management der Microsoft Security Tools (BitLocker + PBA, MS Defender und MS Firewall, Privilege Escalation Prevention)

Außerdem bietet DriveLock:

- einheitliche Oberfläche zur Konfiguration sämtlicher Schutzfunktionen/Anwendungen/Schutzmaßnahmen - DriveLock Management Console (DMC)
- Web-basierte und anpassbare Oberfläche mit umfangreichen Auswertungs- und Analysemöglichkeiten - DriveLock Operations Center (DOC)





Wir unterstützen mehrere Umgebungen, sowohl Fat Clients als auch virtuelle Umgebungen.

Kontaktieren Sie uns!

DriveLock SE
+49 89 546 364 90
info@drivelock.com

www.drivelock.com