Management von Microsoft Defender Antivirus

Mehr als nur Microsoft Antivirenscanner-Konfiguration

komfortabel – integrativ - ganzheitlich sicher

- zentrale Konfiguration für alle Präventionswerkzeuge über die DriveLock Management-Konsole erübrigt zusätzliche Managementlösungen wie Microsoft Intune oder SCCM.
- Defender-Einstellungen können auf die Sicherheitsfunktionen der DriveLock Applikationskontrolle abgestimmt werden.
- Alle Defender AV-Einstellungen sind innerhalb einer DriveLock Richtlinie einfach und schnell zu konfigurieren. Es müssen keine einzelnen Gruppenrichtlinien verteilt werden.
- Im Zusammenspiel mit DriveLock Schnittstellenkontrolle kann die Freigabe von externen Laufwerken an das Ergebnis eines Defender AV-Scans gekoppelt werden.
- Bedrohungen aus AV-Scans können in der DriveLock EDR (Endpoint Detection & Response)-Lösung Alarme auslösen, die wiederum automatisierte Prozesse als Reaktion (Start einer Informations-kampagne, Skriptausführung usw.) starten.
- Eigene Defender-Ansicht im DriveLock Operations Center erfüllt rechtliche Nachweispflichten und ermöglicht Compliance-Berichte.

DriveLock managed Microsoft Defender Antivirus

Der unter Windows 10 vorinstallierte **Echtzeitschutz Microsoft Defender Antivirus** ist der von Microsoft entwickelte Virenschutz zur Erkennung und Beseitigung von Schadsoftware und anderen potenziell unerwünschten Programmen.

DriveLock i**ntegriert** das Management von Microsoft Defender Antivirus in seine Zero Trust Plattform und ermöglicht eine gemeinsame zentrale Verwaltung der DriveLock Präventionswerkzeuge **Applikationskontrolle, Schnittstellenkontrolle und EDR mit dem Microsoft Antivirenscanner.**

So können DriveLock Kunden das Risiko noch weiter minimieren, Daten durch Malware, Spyware oder Ransomware zu verlieren, und alles über eine zentrale Plattform in DriveLock managen.

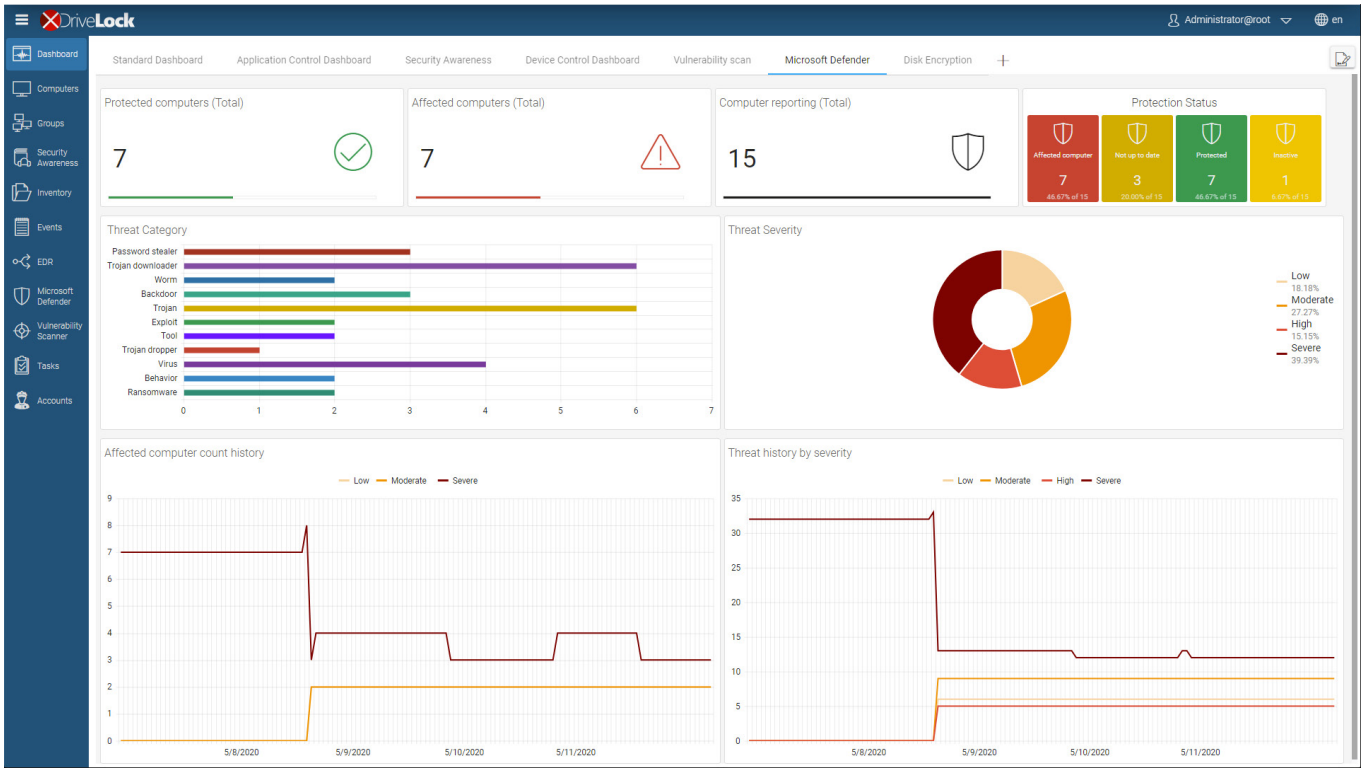
Über die DriveLock Management Konsole lassen sich unter anderem die folgenden Windows Defender Client Einstellungen per DriveLock **Richtlinien konfigurieren:**

- Scan-Einstellungen bei Dateizugriffen und Art der Reaktion bei gefundener Schadsoftware
- Ausnahmeregelungen für Dateiüberprüfungen oder Prozesse
- regelmäßige Scan-Überprüfungen mit Datum und Uhrzeit, Häufigkeit und Art der Reaktion
- Einsatz des Virenscanners beim Verbinden von externen Laufwerken und ggf. automatische Sperre des Zugriffs bei festgestellter Schadsoftware
- Art und Inhalt der Benachrichtigungen des Endbenutzers

Die **DriveLock EDR-Funktionen** ermöglichen durch die Integration von Microsoft Defender Antivirus zusätzliche Reaktionen. Bei der Erkennung von Schadsoftware lassen sich automatische Prozesse starten, die eine weitere Ausbreitung wirksam verhindern, wie z.B. das Herunterfahren oder Isolieren von Computern im Netzwerk.

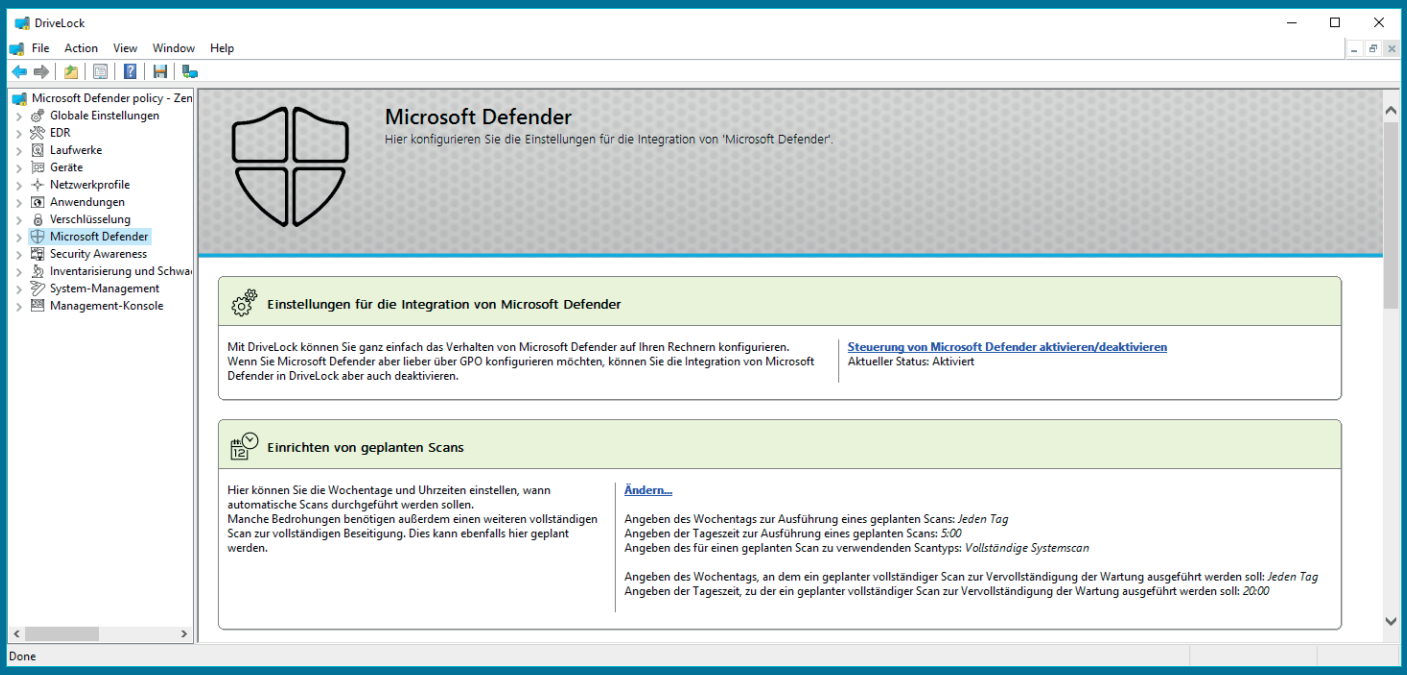
Das moderne **DriveLock Operations Center** bietet mit einem eigenen Virenschutz-Dashboard eine schnelle Übersicht über das aktuelle Schutzniveau und erlaubt Administratoren nicht nur eine detaillierte Auswertung einzelner Systeme, sondern ermöglicht auch bei Sicherheitsvorfällen das Ausführen von zusätzlichen Aktivitäten, wie zum Beispiel den Start eines kompletten Scans, eines Computers oder die manuelle Aktualisierung von Bedrohungsdefinitionen.

Der Überblick über gefundene Bedrohungen, Ergebnisse von Defender Sicherheitsprüfungen und den Zustand der durch DriveLock geschützten Computer hilft Verantwortlichen, die Einhaltung von Compliance Richtlinien und Effektivität der Schutzmaßnahmen zu beurteilen und nachzuweisen.



Ihre Vorteile von DriveLock Microsoft Defender Management im Überblick

- Konfiguration der Sicherheitseinstellungen von DriveLock und Microsoft Defender Antivirus über eine einzige Richtlinie
- Management der Systemumgebung mit Hilfe von Dashboards und modularer Übersichtsgrafiken über das zentrale und web-basierte DriveLock Operations Center
- Einfache Konfigurationsmöglichkeiten



- Automatische Reaktionsmöglichkeiten auf erkannte Bedrohungen, wie zum Beispiel das Sperren des Benutzerzugriffs oder die Anwendung verschärfter Sicherheitseinstellungen

Alles aus einer Hand:
DriveLock bietet Defender Antivirus Management als einen Baustein seiner Zero Trust Plattform zur Realisierung einer gesamtheitlichen Sicherheitsstrategie an.

DriveLock SE • Germany • France • Australia • Singapore • Middle East • USA
sales@drivelock.com • www.drivelock.com