DriveLock Defender Integration

Handbuch 2020.1

DriveLock SE 2020

Inhaltsverzeichnis

1 Integration von Microsoft Defender in DriveLock

DriveLock bietet die Möglichkeit, Microsoft Defender über die DriveLock Management Konsole (DMC) mit Richtlinien zu konfigurieren und den aktuellen Status der DriveLock Agenten im DriveLock Operations Center (DOC) zu überwachen.

In der DMC können alle vorhandenen Einstellungen der Microsoft Defender Antivirus Gruppenrichtlinien (GPO) konfiguriert werden.

Ausgewählte Einstellungen werden direkt in der Taskpad-Ansicht angeboten und können so schnell konfiguriert werden:

- 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
- Art und Inhalt der Benachrichtigungen des Endbenutzers

Des weiteren können Einstellungen für den Defender-Scan von externen Laufwerken vorgenommen werden:

- Einsatz des Virenscanners beim Verbinden von externen Laufwerken und ggf. automatische Sperre des Zugriffs bei festgestellter Schadsoftware

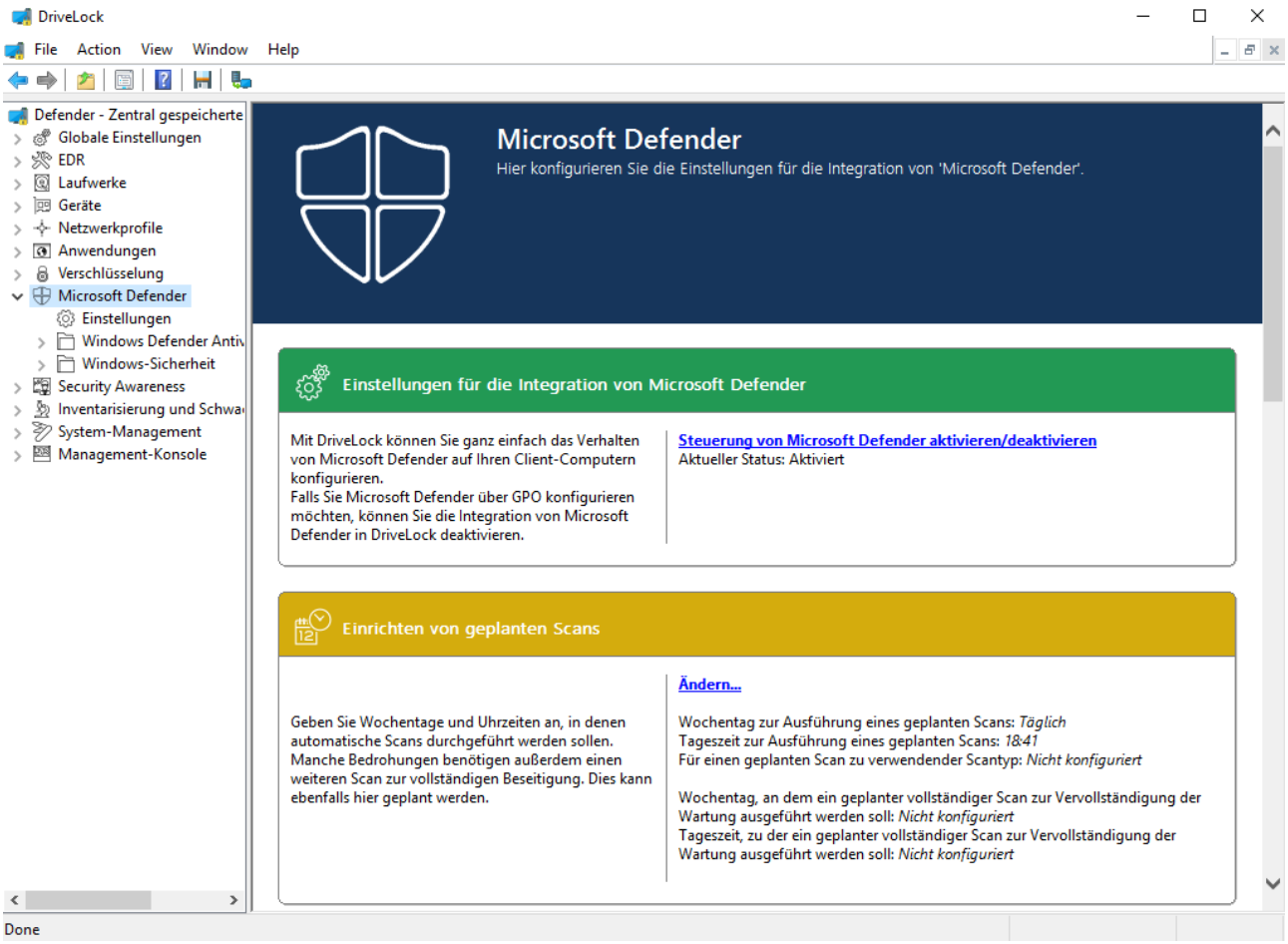
Im DriveLock Operations Center (DOC) können Sie sich Statusberichte über aktuelle Bedrohungen und den Zustand der DriveLock Agenten anzeigen lassen. Gefundene Bedrohungen lassen sich dort exakt analysieren und bei Bedarf können Benachrichtigungen bei Falschmeldungen oder irrelevanten Meldungen unterdrückt werden.

Achtung: Für das Microsoft Defender Management ist eine Lizenz erforderlich.

2 Konfiguration

2.1 Übersicht in der DriveLock Management Konsole

Die Richtlinie enthält den neuen Knoten **Microsoft Defender**, in der die Konfiguration vorgenommen werden kann. In dieser Übersicht nehmen Sie zunächst die Aktivierung (oder ggf. spätere Deaktivierung) vor und integrieren somit die Steuerung der Microsoft-Defender-Funktionalitäten in DriveLock.



Sollte sich eine andere Ansicht in Ihrer Richtlinie öffnen, liegt das an der Einstellung **Show basic configuration**. Um die vereinfachten Einstellungsmöglichkeiten sehen zu können, muss diese Einstellung auf der höchsten Ebene der Richtlinie aktiviert sein, siehe Abbildung:

2.2 Vereinfachte Konfiguration in der Taskpad-Ansicht

Neben der Aktivierung der Steuerung für Microsoft Defender, lassen sich in der Taskpad-Ansicht des Knotens **Microsoft Defender** weitere grundlegende Einstellungen konfigurieren.

- **Einrichten von geplanten Scans**:
  Hier können Zeiten festgelegt werden, zu denen automatische Scans durchgeführt werden sollen.
  Zum einen kann man hier die Zeit für einen geplanten Scan und den Scantyp angeben.
  Zum anderen kann die Zeit zum Vervollständigen der Wartung festgelegt werden.
  Diese Angabe ist nötig, weil manche Bedrohungen erst nach einem weiteren vollständigen Scan vom Microsoft Defender beseitigt werden können.

  > Hinweis: Wird die Zeit für den geplanten Scan an dieser Stelle festgelegt, verwendet DriveLock einen eigenen Scheduler, um den Scan zu der definierten Uhrzeit zu starten. Dabei werden Einstellungen wie **Zufälliges Festlegen von Zeiten für geplante Aufgaben** oder **Starten des geplanten Scans ausschließlich zu dem Zeitpunkt, zu dem der Computer eingeschaltet ist, aber nicht verwendet wird** nicht berücksichtigt. Der Scan startet immer zu der angegeben Zeit.

  Wenn Sie den standardmäßigen Scheduler vom Defender verwenden möchten, nehmen Sie bitte die entsprechenden Einstellungen im Unterknoten **Windows Defender Antivirus**, Einstellung **Scan** vor.

- **Scanoptionen**:
  Konfigurieren Sie hier die Antivirus-Scanoptionen.

- **Ausschlüsse**:
  Konfigurieren Sie hier die Ausschlüsse, um bestimmte Dateien von Microsoft Defender-Antivirus-Scans auszuschließen. Weitere Informationen finden Sie bei Microsoft.

- **Automatische Wartungsaktion**:
  Konfigurieren Sie hier die automatische Wartungsaktion für die einzelnen Bedrohungswarnungsebenen.
  Die Klassifizierung der einzelnen Bedrohungen nach der Bedrohungswarnungsebene (niedrig, mittel, hoch, schwerwiegend) ist in den Defender-Signaturdefinitionen hinterlegt. Man kann sich diese Information z.B. über Powershell mit dem Befehl Get-MpThreatCatalog anzeigen lassen. Die SeverityID entspricht der Bedrohungswarnungsebene:
  1 = Niedrig (Low)

2 = Mittel (Medium)
4 = Hoch (High)
5 = Schwerwiegend (Severe)

- **Verringerung der Angriffsfläche**:
  Legen Sie hier Regeln zur Verringerung der Angriffsfläche (Attack Surface Reduction - ASR) an.

2.3 Einstellungen für Microsoft Defender

Folgende allgemeine Einstellungen lassen sich für die Integration von Microsoft Defender in DriveLock konfigurieren:

- Steuerung von Microsoft Defender aktivieren/deaktivieren
- Bestehende Microsoft Defender-Konfiguration löschen
- Erweiterte Konfigurationsmöglichkeiten anzeigen

2.3.1 Steuerung von Microsoft Defender aktivieren/deaktivieren

Um die Steuerung des Microsoft Defenders auf DriveLock Agenten zu ermöglichen, muss in der Richtlinie die Einstellung **Steuerung von Microsoft Defender aktivieren/deaktivieren** aktiviert sein. Dies ist standardmäßig der Fall.

Hinweis: Diese Einstellung betrifft lediglich die Steuerung durch DriveLock und nicht die eigentliche Funktionalität von Microsoft Defender.

2.3.2 Bestehende Microsoft Defender-Konfiguration löschen

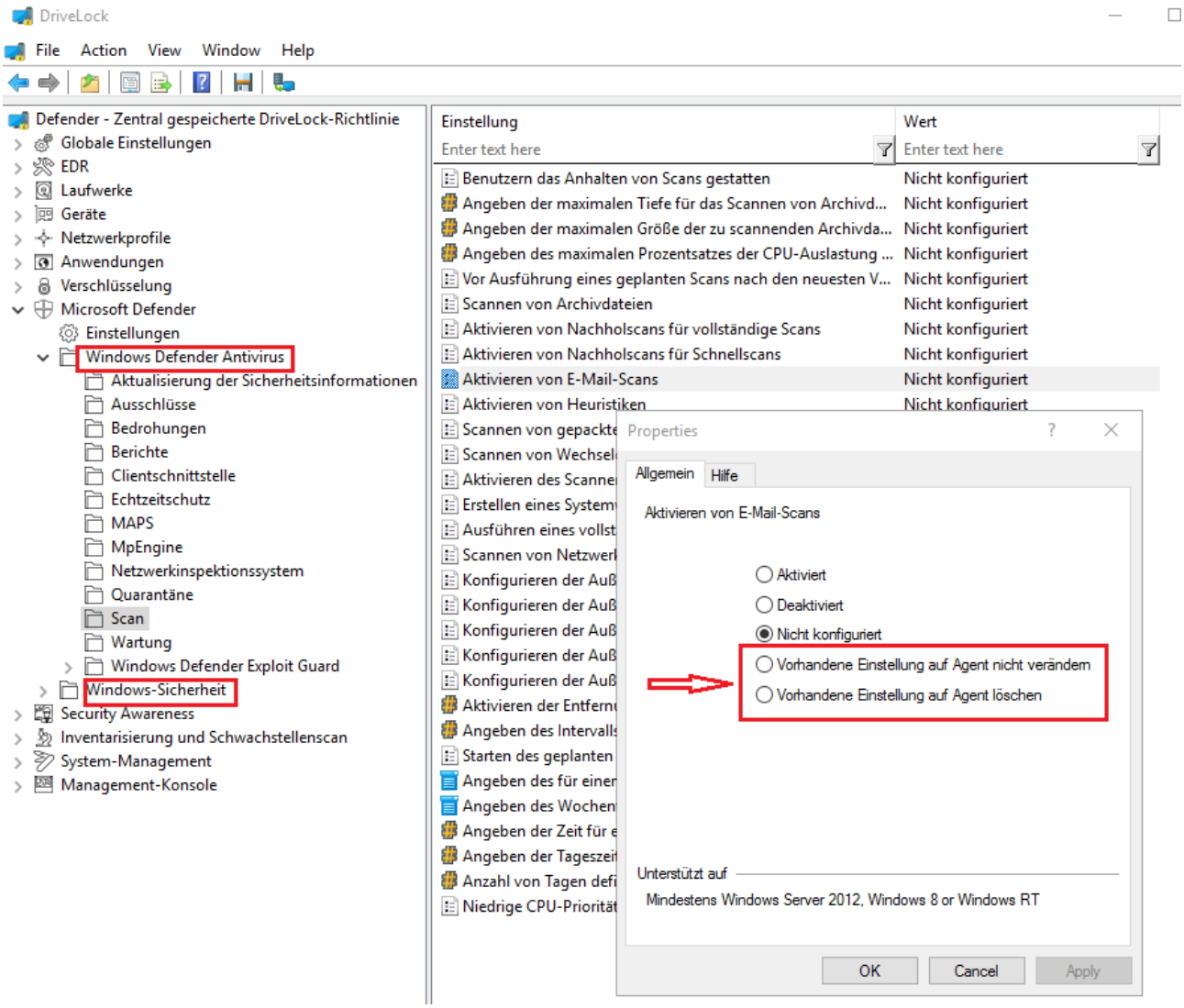
Mit der Einstellung **Bestehende Microsoft Defender-Konfiguration löschen** legen Sie fest, ob DriveLock existierende Defender-Einstellungen auf dem Agenten beibehalten oder vor dem Anwenden der Richtlinie löschen soll.

Standardmäßig behält DriveLock Agent die bestehende Defender-Konfiguration bei und setzt nur diejenigen Einstellungen, die in der DriveLock Richtlinie enthalten sind.

2.3.3 Erweiterte Konfigurationsmöglichkeiten anzeigen

Wenn Sie die Einstellung **Erweiterte Konfigurationsmöglichkeiten anzeigen** aktivieren, werden Ihnen zwei zusätzliche Konfigurationsmöglichkeiten in den Einstellungsdialogen der Knoten **Windows Defender Antivirus und Windows-Sicherheit** eingeblendet, die ansonsten nicht angezeigt werden.

Im Beispiel sehen Sie den Dialog für die Scan-Einstellungen für E-Mails:



Die Konfigurationsmöglichkeiten haben folgenden Effekt:

- **Vorhandene Einstellung auf Agent nicht verändern**:
  Wenn die Einstellung bereits auf dem Agenten gesetzt ist, wird DriveLock diese nicht verändern.

> Hinweis: Im Unterschied zu **Not configured** verändert DriveLock eine solche Einstellung nicht, unabhängig davon, ob sie in einer anderen zugewiesenen DriveLock Richtlinie gesetzt ist oder nicht. Das trifft auf Richtlinien zu, die in der Reihenfolge der Zuweisungen **vor** dieser Richtlinie kommen.

Anwendungsbeispiel:
Auf allen DriveLock Agenten sollen bestimmte Defender-Einstellungen gesetzt werden. Sie erstellen eine DriveLock-Richtlinie mit den entsprechenden Einstellungen und

weisen diese Ihren Agenten zu. Nun soll eine Abteilung einige dieser Einstellungen selbst konfigurieren können (z.B. per Gruppenrichtlinie, manuell oder mit einem anderen externen Tool). Um nicht die komplette Richtlinie kopieren zu müssen und nur diese wenigen Einstellungen zu verändern, können Sie eine neue Richtlinie erstellen und in dieser Richtlinie die betroffenen Einstellungen auf **Vorhandene Einstellung auf Agent nicht verändern** setzen. Diese neue Richtlinie weisen Sie den Agenten zu, und zwar so, dass sie in der die Reihenfolge nach der bestehenden Defender Richtlinie kommt.

- **Vorhandene Einstellung auf Agent löschen**:
  Wenn eine Defender Einstellung aus dem Knoten **Windows Defender Antivirus** auf diesen Wert gesetzt wird, wird diese Defender Einstellung auf dem DriveLock Agenten gelöscht. Der Defender wird somit seine Standardeinstellung verwenden.
  Diese Option ist vergleichbar mit der Einstellung Bestehende Microsoft Defender-Konfiguration löschen, mit dem Unterschied, dass sie für eine einzelne Einstellung verwendet wird, während **Bestehende Microsoft Defender-Konfiguration löschen** alle Einstellungen löscht.

2.4 Windows Defender Antivirus und Windows-Sicherheit

Die Unterknoten **Windows Defender Antivirus** und **Windows-Sicherheit** enthalten alle Einstellungen für den Microsoft Defender, die mit der Gruppenrichtlinie Stand Juni 2019 verteilt werden können.

Der DriveLock Agent speichert die Einstellungen aus der DriveLock Richtlinie an der gleichen Stelle in der Registry ab, an der auch Gruppenrichtlinieneinstellungen gespeichert werden. Die Defender-Einstellungen sind dann zu finden unter:

- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender` bzw.
- `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center`

Wenn die Einstellung Bestehende Microsoft Defender-Konfiguration löschen deaktiviert ist, ist es möglich, zusätzlich zu der DriveLock Richtlinie einen Teil der Einstellungen über die Gruppenrichtlinie oder mit einem anderen externen Tool zu verteilen.

2.5 Externe Laufwerke

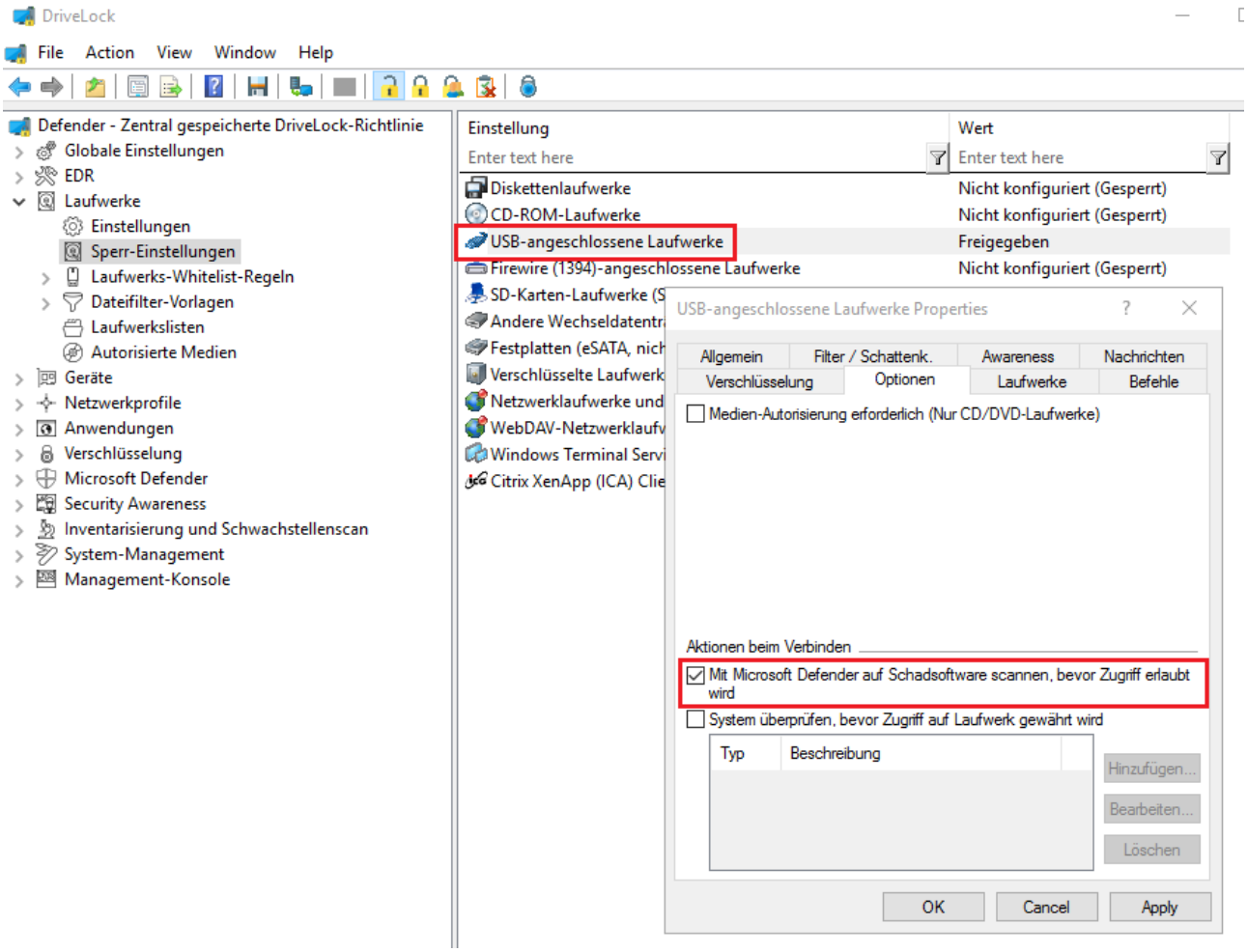
2.5.1 Externe Laufwerke scannen

Sie können ein externes Laufwerk in Richtlinien so konfigurieren, dass automatisch ein Virenscan gestartet wird, sobald es an den Computer angeschlossen wird. Anwender können dann erst auf das Laufwerk zugreifen, wenn der Scan abgeschlossen ist und keine Schadsoftware gefunden wurde.

2.5.2 Konfiguration über Sperr-Einstellungen

Gehen Sie folgendermaßen vor:

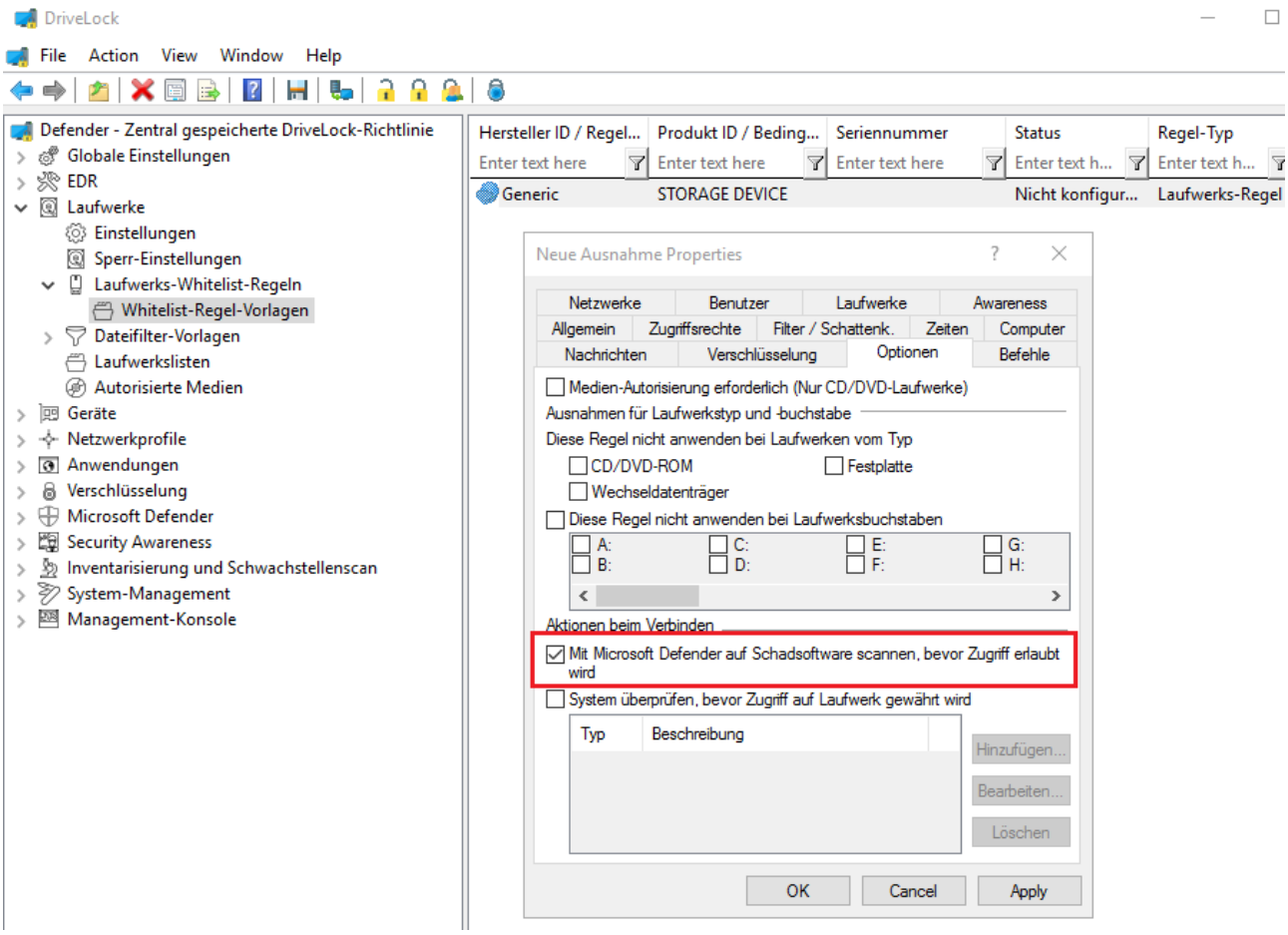
1. Öffnen Sie in der Richtlinie im Knoten **Laufwerke** den Unterknoten **Sperr-Einstellungen** und wählen Sie darin das entsprechende Laufwerk zum Bearbeiten aus.
2. Wechseln Sie im Dialog auf den Reiter **Optionen**.
3. Setzen Sie ein Häkchen bei der Option **Mit Microsoft Defender auf Schadsoftware scannen, bevor Zugriff erlaubt wird**.



2.5.3 Konfiguration über Laufwerks-Whitelist-Regeln

Gehen Sie folgendermaßen vor:

1. Öffnen Sie in der Richtlinie im Knoten **Laufwerke** den Unterknoten **Laufwerks-Whitelist-Regeln**. Legen Sie eine neue Whitelist-Regel an oder öffnen Sie eine bestehende zum Bearbeiten aus.
2. Wechseln Sie im Dialog auf den Reiter **Optionen**.
3. Setzen Sie ein Häkchen bei der Option **Mit Microsoft Defender auf Schadsoftware scannen, bevor Zugriff erlaubt wird**.



Hinweis: Wenn es sich um ein verschlüsseltes Laufwerk handelt, startet DriveLock den Scan, sobald das Laufwerk verbunden und entschlüsselt ist.

Auf dem DriveLock Agenten wird eine Nachricht im Taskleistensymbol angezeigt.

Wenn Microsoft Defender eine Bedrohung auf dem Laufwerk findet, macht sich das durch längere Scan-Laufzeit bemerkbar. Microsoft Defender versucht dann die Bedrohungen zu

beseitigen. Wenn das nicht gelingt, muss das Laufwerk getrennt und neu verbunden werden, damit Microsoft Defender das Entfernen der Bedrohung abschließen kann.

Der Benutzer bekommt eine Nachricht angezeigt, ob das Entfernen erfolgreich war und das Laufwerk damit zugreifbar ist.

Hinweis: Kann Microsoft Defender die Bedrohung nicht beseitigen, bleibt noch die Möglichkeit über eine temporäre Freigabe auf das Laufwerk zuzugreifen.

3 Ereignisse

3.1 Statusbericht und Ereignisse

Der DriveLock Agent sendet regelmäßig den aktuellen Defender Status an den DriveLock Enterprise Service (DES). Der Status umfasst Informationen wie Versionsnummern der Definitionen, letzte Scan-Zeiten und gefundene Bedrohungen.

Der Status wird nach dem Start des Dienstes und danach alle 24 Stunden gesendet. Zusätzlich passiert das auch nach Konfigurationsänderungen, nach dem Aktualisieren des Microsoft Defenders und beim Auftreten der Bedrohungen.

Hinweis: Der Status wird immer gesendet, unabhängig davon, ob die Option **Steuerung von Microsoft Defender aktivieren/deaktivieren** gesetzt ist oder nicht.

3.2 Microsoft Defender-Ereignisse

Im folgenden sind die Ereignisse erläutert, die der DriveLock Enterprise Service (DES) generiert. Ob diese Ereignisse an den DES gesendet und im DriveLock Operations Center (DOC) angezeigt werden, legen Sie in der Richtlinie im Knoten **EDR**, Unterknoten **Ereignisse** und dann **Microsoft Defender** in der Spalte **DriveLock Enterprise Service** fest.

Eine vollständige Liste aller DriveLock Ereignisse können Sie in der entsprechenden Dokumentation auf DriveLock OnlineHelp einsehen.

Nummer	Typ	Kurztext	Langtext	Erklärung
681	Error	Konfiguration von Microsoft Defender fehlgeschlagen	Fehler bei der Microsoft Defender-Konfiguration. Error code: [ErrorCode]. Error: [ErrorMessage]	Dieses Ereignis wird generiert, wenn die Microsoft Defender Einstellungen aus der DriveLock Richtlinie nicht angewendet werden konnten. Der ErrorCode ist der Windows Fehlercode.

Nummer	Typ	Kurztext	Langtext	Erklärung
682	Information	Microsoft Defender-Konfigurationsänderungen rückgängig gemacht	Konfigurationsänderungen an Microsoft Defender durch Dritte erkannt. Die Änderungen wurden rückgängig gemacht. Details: [Details]	Dieses Event wird generiert, wenn DriveLock Konfigurationsänderungen am Microsoft Defender durch Dritte erkannt hat und die Änderungen entsprechend der DriveLock Richtlinie rückgängig machen konnte. Es werden nur diejenigen Konfigurationsänderungen rückgängig gemacht, die in der DriveLock Richtlinie enthalten sind. Wenn die Option **Bestehende Microsoft Defender-Konfiguration löschen** gesetzt ist, werden zusätzlich alle Einstellungen entfernt, die nicht in der Richtlinie enthalten sind.
683	Error	Microsoft Defender-Konfigurationsänderungen konnten nicht rück-	Konfigurationsänderungen an Microsoft Defender durch Dritte	Dieses Event wird generiert, wenn DriveLock Konfigu-

Num-mer	Typ	Kurztext	Langtext	Erklärung
		gängig gemacht werden	erkannt. Die Änderungen konnten nicht rückgängig gemacht werden. Details: [Details]. Error code: [ErrorCode]. Error: [ErrorMessage]	rati-onsänderungen am Microsoft Defender durch Dritte erkannt hat und die Änderungen entprechend der DriveLock Richtlinie nicht wieder rückgängig machen konnte. Details: Enthält die Liste der gefundenen Konfigu-rati-onsänderungen
684	War-ning	Microsoft Defender-Bedrohung erkannt	Microsoft Defender hat die Bedrohung [DetectionName] ([DetectionType]) erkannt. Infizierte Datei: [Path] Laufwerk: [DriveLetter] Dateiname: [FileName] Dateinamens-Hash: [MD5Hash]	Dieses Event wird generiert, wenn Microsoft Defender eine Bedrohung erkannt hat. Im Unterschied zum Event 697 enthält dieses Event keine Hardware-Informationen über das betroffene

Nummer	Typ	Kurztext	Langtext	Erklärung
				Laufwerk, weil sie nicht ermittelt werden konnten. • DetectionName: Name der Bedrohung • DetectionType: Kategorie der Bedrohung, z.B. Trojaner, SpyWare, etc. • Path: Vollständiger Dateipfad • FileName: Dateiname • MD5Hash: MD5 aus dem Dateinamen
685	Warning	Microsoft Defender-Bedrohung erlaubt	Ein Benutzer hat eine Bedrohung erlaubt, die Microsoft Defender erkannt hat. Bedrohung: [DetectionName] Kategorie: [DetectionType]	Dieses Event wird generiert, wenn der Benutzer eine vom Microsoft Defender erkannte Bedrohung zugelassen hat.

Nummer	Typ	Kurztext	Langtext	Erklärung
686	Warning	Microsoft Defender-Bedrohung aus Quarantäne wiederherstellt	Ein Benutzer hat eine Bedrohung aus der Quarantäne wiederhergestellt, der durch Microsoft Defender erkannt wurde. Bedrohung: [DetectionName] Kategorie: [DetectionType]	Dieses Event wird generiert, wenn Microsoft Defender eine Bedrohung aus der Quarantäne wiederhergestellt hat.
687	Error	Fehler beim Aktualisieren der Microsoft Defender-Signatur	Signatur-Definition von Microsoft Defender konnte nicht aktualisiert werden. Details: [Details]	Dieses Event wird generiert, wenn die Signatur-Definitionen von Microsoft Defender nicht aktualisiert werden konnten.
696	Warning	Microsoft Defender-Bedrohung auf Netzlaufwerk erkannt	Microsoft Defender hat die Bedrohung [DetectionName] ([DetectionType]) erkannt. Infizierte Netzwerk-Datei: [Path] Netzlaufwerk: [NetDrivePath] ([NetDriveType]) Dateiname: [FileName] Dateinamens-Hash: [MD5Hash]	Dieses Event wird generiert, wenn Microsoft Defender eine Bedrohung auf einem Netzlaufwerk erkannt hat.
697	Warning	Microsoft Defender-Bedrohung	Microsoft Defender hat die Bedro-	Dieses Event wird generiert, wenn

Nummer	Typ	Kurztext	Langtext	Erklärung
		erkannt	hung [DetectionName] ([DetectionType]) erkannt. Infizierte Datei: [Path] Geräteidentifikation: [HWVendorID] [HWProductID] (Rev. [HWRevisionNumber]) (Seriennummer [HWSerialNumber]) Laufwerk: [DriveLetter] Dateiname: [FileName] Dateinamens-Hash: [MD5Hash]	Microsoft Defender eine Bedrohung erkannt hat. Im Unterschied zum Event 684 enthält dieses Event Hardware-Informationen über das betroffene Laufwerk.
698	Error	Microsoft Defender ist deaktiviert	Microsoft Defender ist deaktiviert und kann nicht von DriveLock aktiviert werden.	Dieses Event wird generiert, wenn in der Windows Defender Antivirus Service auf dem Agenten nicht läuft.
699	Information	Microsoft Defender-Konfiguration angewendet	Microsoft Defender-Konfiguration wurde erfolgreich angewendet.	Dieses Event wird generiert, wenn die DriveLock Richtlinie erfolgreich angewendet

Nummer	Typ	Kurztext	Langtext	Erklärung
				werden konnte.
700	Warning	Microsoft Defender hat die Ausführung verhindert	Microsoft Defender hat eine Aktion verhindert: [ASRRuleType] Erkennungszeit: [TimeStamp] Pfad: [FileName] Prozess: [ProcessName] Signatur-Version: [SignatureVersion] Engine-Version [EngineVersion] Produkt-Version: [ProductVersion] Benutzer: [UserName]	Dieses Event wird generiert, wenn eine der Regeln zur Verringerung der Angriffsfläche eine Aktion blockiert hat. • ASRRuleType: Name der Regel • TimeStamp: Zeitpunkt • FileName: Vollständiger Dateiname der betroffenen Datei • ProcessName: Betroffener Prozessname • SignatureVersion: Versionsnummer der Antivirus-Signatur • EngineVersion:

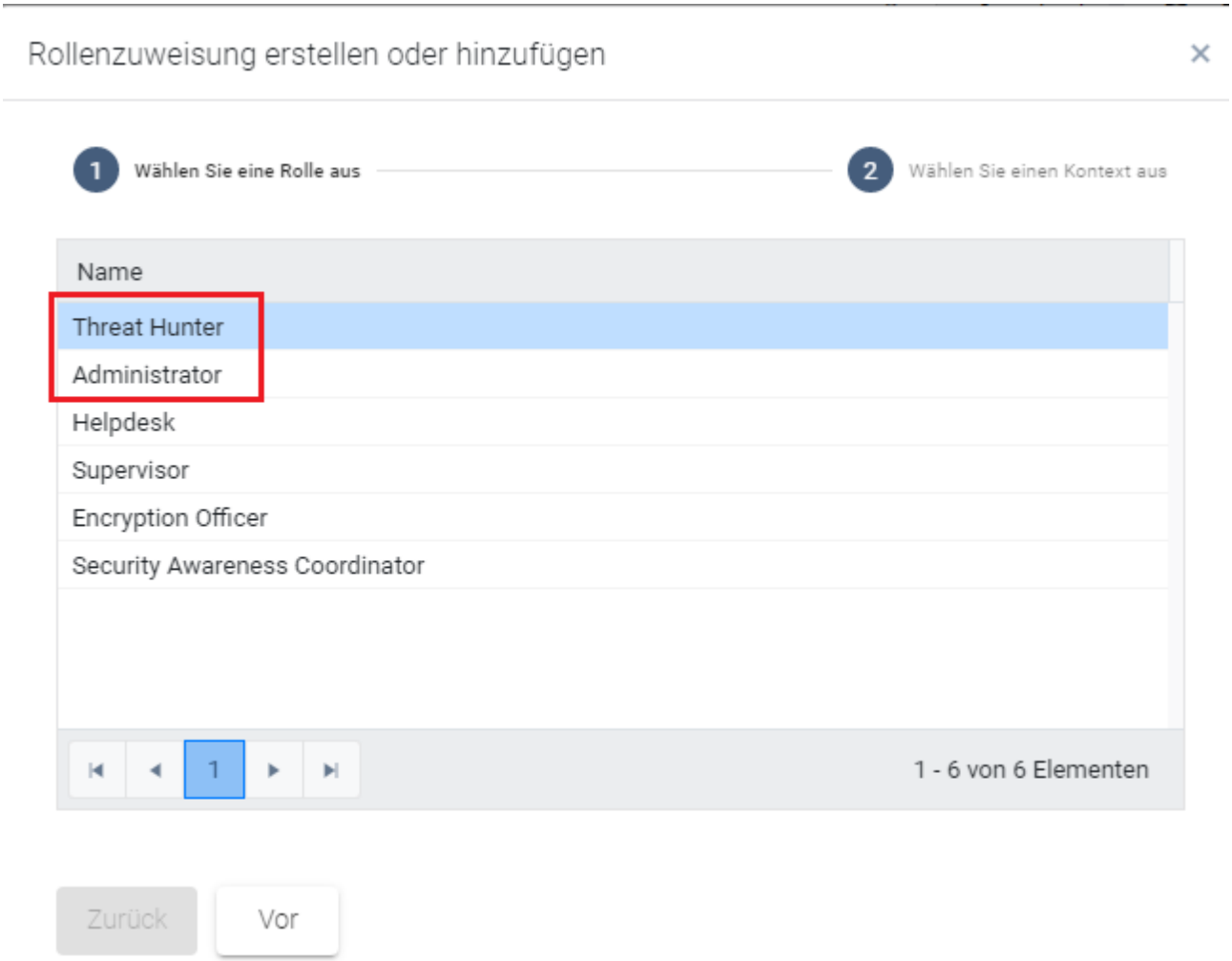
Nummer	Typ	Kurztext	Langtext	Erklärung
				Versionsnummer der NIS Engine (Network Realtime Inspection service) • ProductVersion: Versionsnummer des Defenders • UserName: Benutzername
701	Audit	Microsoft Defender hat die Ausführung protokolliert	Microsoft Defender hat eine Aktion protokolliert: [ASRRuleType] Erkennungszeit: [TimeStamp] Pfad: [FileName] Prozess: [ProcessName] Signatur-Version: [SignatureVersion] Engine-Version [EngineVersion] Produkt-Version: [ProductVersion]	Dieses Event wird generiert, wenn eine der Regeln zur Verringerung der Angriffsfläche im Überwachungsmodus angewendet wurde.

Nummer	Typ	Kurztext	Langtext	Erklärung
			Benutzer: [UserName]	
702	Error	Fehler beim Upload zu DES		Dies ist ein weiteres DES Event, das generiert wird, wenn das Senden des Status an den DES fehlschlägt. Dieses Event befindet sich im Knoten EDR, Unterknoten Ereignisse -> Allgemeine Ereignisse -> Server-Kommunikation.

4 Microsoft Defender Management im DOC

Im DriveLock Operations Center (DOC) wird der Status des Microsoft Defender auf den Agenten in der **Microsoft Defender**-Ansicht angezeigt. Weitere Informationen zum DOC finden Sie in der **DriveLock Control Center** Dokumentation auf DriveLock OnlineHelp.

Um die Micorsoft Defender-Ansicht sehen zu können, benötigen Sie die Administrator- oder Threat Hunter-Rolle (s. Abbildung).



Das DOC Dashboard zeigt den Microsoft Defender-Status mit verschiedenen Widgets ebenfalls an. Falls das Microsoft Defender-Dashboard nicht automatisch angezeigt wird, können Sie es über die entsprechende Vorlage hinzufügen.

4.1 Dashboard

Erläuterung der Widgets:

- **Bedrohungen**
  Gibt die Anzahl der Bedrohungen an, die im Moment für alle Computer unterdrückt sind. Ist eine Bedrohung nur für einen Computer unterdrückt, wird sie in dieser Ansicht nicht berücksichtigt.
- **Computer**
  Gibt Anzahl der Computer an, auf denen unterdrückte Bedrohungen existieren.
- **Neueste Microsoft Defender-Ereignisse**
  Zeigt Microsoft Defender-Ereignisse der letzten Woche an. Beachten Sie, dass dafür das Senden der Ereignisse zum DES aktiviert sein muss.
- **Microsoft Defender-Status** gibt einen Überblick über den Status von Microsoft Defender auf den Computern:
  - Nicht gesetzt: Der Status wurde bisher nicht gemeldet
  - Aktiv
  - Teilweise aktiv: Eine oder mehrere Microsoft Defender-Komponenten werden nicht ausgeführt, z.B. Echtzeitschutz
  - Inaktiv: Der Microsoft Defender Service läuft nicht
- **Bedrohungen nach Kategorie**
  Zeigt alle aufgetretenen Bedrohungen an und gruppiert sie nach Kategorie. Es wird nicht unterschieden, ob die Bedrohung bereits behoben oder noch offen ist.
- **Bedrohungen nach Schweregrad**
  Zeigt alle aufgetretenen Bedrohungen an und gruppiert sie nach Schweregrad. Es wird nicht unterschieden, ob die Bedrohung bereits behoben oder noch offen ist.
- **Verlauf der Bedrohungen nach Kategorie**
  Zeigt den Verlauf der Bedrohungen nach Kategorie an
- **Verlauf der Bedrohungen nach Schweregrad**
  Zeigt den Verlauf der Bedrohungen nach Schweregrad an
- **Verlauf nach Anzahl**
  Zeigt den Verlauf der betroffenen Computer nach Anzahl an
- **Aktivierbare Services oder Features**, **Schutz-Status**, **Service-Übersicht**, **Unterdrückte Bedrohungen**: Weitere Informationen im entsprechende Abschnitt hier.
- **Feature-Übersicht**

Zeigt die Anzahl der Computer an, auf denen die einzelnen Microsoft Defender-Features aktiviert sind.

4.2 Ansicht

In der Microsoft Defender-Ansicht finden Sie im oberen Bereich eine Leiste mit Widgets, die einen Überblick über den Status der Agenten geben. Wenn Sie eines der Widgets anklicken, wird im unteren Bereich die entsprechende Liste mit Computern oder Bedrohungen angezeigt. Wählen Sie einen Computer oder Bedrohung aus, um rechts daneben eine Detailansicht zu bekommen.

Erläuterung der Widgets:

- **Schutz-Status** zeigt den aktuellen Status der Computer
  - Betroffene Computer
    Anzahl der Computer, die offene Bedrohungen aufweisen, die nicht vom Microsoft Defender entfernt werden konnten
  - Nicht aktuell
    Anzahl der Computer, die keine offenen Bedrohungen haben, deren Microsoft Defender Signatur-Definitionen aktualisiert wurden und deren letzte Statusmeldung nicht länger als 1 Woche zurückliegt
  - Geschützt
    Anzahl der Computer, deren Microsoft Defender Signatur-Definitionen älter als 1 Woche sind oder deren letzte Statusmeldung länger als 1 Woche zurückliegt
  - Inaktiv
    Anzahl der Computer, auf denen Microsoft Defender Service nicht läuft
- **Service-Übersicht** zeigt die Anzahl der Computer an, auf denen der Windows Defender Antimalware Service bzw. Windows Defender Antivirus Network Inspection Service laufen.
- **Aktivierbare Services oder Features** zeigt die Anzahl der Computer an, auf denen Microsoft Defender Services bzw. Features vorhanden, aber nicht aktiv sind. Sie könnten noch eingeschaltet werden, um den vollen Schutz zu gewährleisten.
  - Aktivierbare Services sind Windows Defender Antimalware Service und Windows Defender Antivirus Network Inspection Service.
  - Aktivierbare Features sind der Zugriffsschutz, Echtzeitschutz, Verhaltensschutz und Manipulationsschutz. Dabei wird berücksichtigt, ob das entsprechende Feature überhaupt vorhanden ist. Z.B. ist der Manipulationsschutz erst ab Windows 10 1903 vorhanden.

> Hinweis: Dieses Widget berücksichtigt nicht die Einstellungen in der DriveLock Richtlinie. Selbst wenn ein Feature auf dem Computer aufgrund einer Richtlinie abgeschaltet wurde, wird es in dieser Liste angezeigt.

- **Unterdrückte Bedrohungen** gibt eine Übersicht über die unterdrückten Bedrohungen. DriveLock bietet die Möglichkeit an, bestimmte Bedrohungen, die für Sie ignorieren möchten, zu unterdrücken. Diese Bedrohungen und betroffene Computer werden hier angezeigt.
  - Computer
    Anzahl der Computer, auf denen Bedrohungen unterdrückt wurden
  - Bedrohungen
    Anzahl der unterdrückten Bedrohungen

Registerkarten:

1. **Computer mit Bedrohungen**
   Hier werden je nach gewähltem Kontext alle betroffenen Computer angezeigt.
   Die Detailansicht im rechten Bereich setzt sich aus verschiedenen Blöcken zusammen:
   - **Computer-Gesamtstatus** gibt einen Überblick über den Status des Microsoft Defender, wie z.B. Versionsnummern, vorhandene Features und Services und das letzte Aktualisierungsdatum. In dieser Ansicht sind diejenigen Zeilen rot unterlegt, die auf ein Problem hindeuten.
   - Offene/ Behobene/ Unterdrückte Bedrohungen
     Je nach Status der vorhandenen Bedrohungen werden sie unter offenen, behobenen oder unterdrückten Bedrohungen angezeigt. Bei den offenen Bedrohungen haben Sie die Möglichkeit, diese für den für den gewählten oder für alle Computer zu unterdrücken.
   - Der Link **Enzyklopädie öffnen** führt Sie zu einer Informations-Seite von Microsoft, auf der Sie weitergehende Informationen zu der Bedrohung bekommen.
   - Der Link **Details zur Bedrohung anzeigen** öffnet die Detailansicht zu dieser Bedrohung auf dem Computer, in der Sie sehen können welche Dateien betroffen sind oder wann die Bedrohung gefunden wurde.
   - **Eigenschaften**
     Die Eigenschaften beinhalten allgemeine Betriebssystem-Informationen und den detaillierten Status des Micrsosoft Defenders, so wie er z.B. über das Powershell-Befehl `Get-MpComputerStatus` auf einem Computer ausgegeben wird.

- Die Zeile **Letzte Aktualisierung** zeigt an, wann der DES zum letzten Mal einen Status vom Agenten bekommen hat.

2. **Erkannte Bedrohungen**
   Die Liste enthält alle Bedrohungen, die im Unternehmen gefunden wurden.
   Die Detailansicht rechts enthält dann jeweils eine Liste aus Computern, auf denen die Bedrohungen offen, behoben oder unterdrückt ist.

3. **Details zu erkannten Bedrohungen**
   Jede Bedrohung kann mehrfach auf dem gleichen Computer auftreten, z.B. in verschiedenen Verzeichnissen, auf verschiedenen USB Sticks oder mehrfach hintereinander. Die in der Liste angezeigten Elemente entsprechen dem Auftreten einer Bedrohung auf einem Computer. Es ist also möglich, dass mehrere Zeilen den gleichen Computer mit gleicher Bedrohung enthalten.
   In der Detailansicht werden betroffene Dateien und die Eigenschaften der Bedrohung angezeigt. In den Eigenschaften sieht man u.a. den Status der Bedrohung und wann die letzte Defender Aktion stattgefunden hat.

5 Fehlerbehebung

Bei aktiviertem Tracing werden folgende Protokolldateien auf dem Agenten erstellt:

- DlSvcDefender.log
- DES.log

Es ist möglich, den letzten Status, den der Agent an den DES geschickt hat, sich zusätzlich in eine Datei speichern zu lassen. Dafür muss Tracing aktiviert sein und folgender Registryschlüssel auf dem Agenten gesetzt werden:

- Registryschlüssel: `HKLM\Software\CenterTools\TraceLog`
- DWORD-Wert: DlSvcDefender_LogStatus
- Im Trace-Verzeichnis wird dann die Datei **DefenderStatus.json** abgespeichert.

Copyright