DefenderHardeningSuite

Einsatz-Leitfaden für Administratoren

V37
byteland software solutions
Stefan Matz

DHS zeigt den vollständigen Zustand von **Microsoft Defender Antivirus** und setzt jede offiziell skriptbare Einstellung – auch die, die die Windows-Sicherheit verbirgt (ASR-Regeln, Cloud-Blockstufe, Netzwerkschutz, Überwachter Ordnerzugriff, Updates der Sicherheitsinformationen). Der Katalog umfasst 25 Einstellungen, 19 davon setzbar, dazu die 19 ASR-Regeln. Es gibt zwei Einsatzwege: **lokal am Einzelrechner** und **per Skript für die Flotte**.

Lesen ohne Admin

Übersicht, Diff und Trockenlauf brauchen keine Rechte. Geschrieben wird als erhöhte Transaktion (eine UAC); nur sehr große Änderungen laufen in mehreren Blöcken – je eine UAC, vorher angekündigt.

Nichts Verwaltetes

Per GPO/Intune erzwungene Werte werden erkannt und **nie** überschrieben. Unbekannter Lesezustand → fail-closed.

Umkehrbar

Automatischer Snapshot vor jeder Änderung, Diff mit exaktem Cmdlet, Rückgängig je Eintrag. Nur dokumentierte Microsoft-Cmdlets, keine Registry-Schreibzugriffe.

1 Lokal am Einzelrechner

interaktiv (GUI) oder CLI

1. **Installieren.** MSI (Deutsch/Englisch) nach Program Files – eine UAC. Server Core: die headless `dhs` -CLI.
2. **Lesen.** DHS starten (ohne Admin) → **Übersicht**. Die Status-Ampeln zeigen den Härtungsstand:

   OK – erfüllt · Audit – beobachtet · Härten – Lücke
3. **Härten.** Profil → **Preset anwenden** → `hardening-asr-audit-cfa-audit` . Der Diff zeigt jede geplante Änderung; eine UAC wendet an. Ein Snapshot wird zuvor angelegt.

   Passt eine sehr große Änderung nicht in eine Kommandozeile, teilt DHS sie in Blöcke und erhöht jeden einzeln – Bestätigungsdialog und `dhs apply` nennen die Zahl der UAC-Abfragen vorab. Grund: DHS schreibt nie ein Skript auf die Platte.
4. **Beobachten & feinabstimmen.** Reiter **Ereignisse** (vier Log-Schleifen): Rechtsklick auf einen Treffer → punktgenauer Ausschluss. Oder der **Lern-Assistent** schlägt Ausschlüsse vor.
5. **Scharfstellen.** Nach 1–2 Wochen auf `hardening-asr-block-cfa-audit` wechseln (oder einzelne saubere Regeln auf Block). Überwachter Ordnerzugriff und Cloud folgen mit den `-cfa-block` -Presets.

> **CLI (skriptbar, Trockenlauf als Standard):** `dhs status` · `dhs apply --profile hardening-asr-audit-cfa-audit --apply`

2 Per Skript für die Flotte

GPO-Startskript oder RMM

1. **Baseline festlegen.** Ein Preset wählen – oder einen Rechner mit Weg 1 abstimmen und dessen Ist-Zustand als Vorlage nehmen (Referenzrechner).
2. **Deploy-Skript exportieren.** Profil → **Deploy-Skript exportieren**. Optional Referenz-Listen (Ausschlüsse, CFA-Listen, regelspezifische ASR-Ausschlüsse) per Häkchen einbetten.

   ```
   dhs export-script --preset NAME | --from-current [--include all] --output deploy.ps1
   ```

   Diese Listen gibt Defender nur erhöht heraus: `--include` holt sie einmalig mit Adminrechten (eine UAC) und **bricht ab**, wenn sie verweigert werden – nie ein Skript mit leeren Listen. Ein reines Preset-Skript braucht keine Rechte; im Assistenten führt der Hinweis-Balken zu *Als Administrator neu starten*.
3. **Verteilen als Computer-Startskript – nur an Client-OUs.** GPO: *Computerkonfiguration → Richtlinien → Windows-Einstellungen → Skripts → Start*. Läuft als **SYSTEM**, ohne Interaktion; auf Windows Server verweigert es den Lauf (Exit 4) – Server direkt mit DHS härten. (Alternativ: RMM als SYSTEM-Task.)

   Am besten im Reiter **Skripts** eintragen (nicht *PowerShell-Skripte*) – dann gilt der Bypass nur für diesen einen Aufruf statt maschinenweit: Skriptname `C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe` (absoluter Pfad – ein bloßer Name wird im Skript-Ordner der GPO gesucht, nicht im PATH, und läuft dann gar nicht), Parameter `-NoProfile -NonInteractive -ExecutionPolicy Bypass -File "<UNC-Pfad>"` . Ist die Ausführungsrichtlinie bereits **per GPO** erzwungen, wird der Parameter ignoriert – dann jene Richtlinie anpassen oder das Skript signieren.
4. **Prüflauf.** Erst mit `-DryRun` auf einem Testrechner. Log: `%ProgramData%\DefenderHardeningSuite\deploy.log` .

> **Achtung – Start, nicht Anmeldung:** Nur der SYSTEM-Kontext des **Computer-Startskripts** hat die Rechte für `Set-MpPreference` . Ein Benutzer-Anmeldeskript kann Defender nicht härten.

Das Skript ist ein **1:1-Abbild** der Referenzmaschine und beim Anwenden **standardmäßig monoton** (verstärkt nur – stuft nie herab; absenken kann nur der Administrator per `Enforce=$true` in der jeweiligen Zeile; manipulationsgeschützte Werte werden **nie** abgesenkt und tragen keinen Schalter). Es ist **idempotent** (bei jedem Boot sicher), überspringt GPO/Intune-verwaltete Werte und prüft nach dem Schreiben nach. DHS muss auf den Zielen nicht installiert sein.

Kurzreferenz

PRESETS (REIHENFOLGE WIE IN DHS: SANFT → SCHARF)

`hardening-asr-audit-cfa-audit`	**Hardening, ASR/CFA Audit** – volle Baseline, ASR und CFA nur beobachtend: blockiert nichts
`hardening-asr-block-cfa-audit`	**Hardening, ASR Block, CFA Audit** – ASR-Regeln 1–14 Block, 15–18 Überwachung, CFA weiter beobachtend
`hardening-asr-audit-cfa-block`	**Hardening, ASR Audit, CFA Block** – CFA auf Block (Zulassungsliste vorher!), ASR weiter beobachtend
`hardening-asr-block-cfa-block`	**Hardening, ASR/CFA Block** – ASR 1–14 **und** CFA auf Block
`hardening-plus-cfa-block`	**Hardening plus, ASR/CFA Block** – wie darüber, zusätzlich Cloudschutzstufe **Hoch Plus**
`byteland-recommended`	**byteland-Empfehlung (Arbeitsplatz)** – die auf byteland.de veröffentlichte Empfehlung: wie „plus“, zusätzlich Beispiel-Einsendung „alle Beispiele“, ASR 15–18 **Warnen** statt Überwachung
`hardening-aggressive-cfa-block`	**Hardening aggressive, ASR/CFA Block** – **Appliance-Profil** (Kasse, Kiosk, Terminal): Cloud **Nulltoleranz**, Beispiel-Einsendung „alle Beispiele“, Prüfintervall 2 h, ASR 1–16 Block, Previews 17/18 Warnen – am Arbeitsplatz hohes Fehlalarm-Risiko

Alle sieben teilen dieselbe Baseline (u. a. jeder Echtzeit- und Scan-Bereich ein, MAPS Erweitert, PUA und Netzwerkschutz Block, die drei Update-Einstellungen); Cloudschutzstufe, CFA und Beispiel-Einsendung staffeln sich wie oben – die letzten drei bilden die Leiter plus → byteland → aggressive. Regel 19 (Webshells) ist eine Server-Regel und bleibt auf Desktops deaktiviert. Die früheren Slugs `hardening-asr-audit`, `hardening-asr-block`, `hardening-asr-block-cfa` und `hardening-aggressive` gelten weiter als Aliase – bestehende Skripte und GPO-Befehle bleiben gültig.

GUT ZU WISSEN

Update	Hilfe → „Nach neuer Version suchen“ (manuell, keine Hintergrund-Telemetrie)
Feedback	Hilfe → „Fehler melden…“ öffnet das E-Mail-Programm (dhs@byteland.de)
Rückgängig	Verlauf (je Eintrag) oder Rollback auf Snapshot
Notfall	`dhs-recovery.ps1` stellt Snapshots ganz ohne DHS wieder her – **vor einer Deinstallation** Skript, README und ältesten Snapshot sichern
Zulassungen	Ausschlüsse → „Zulässige Bedrohungen“ zeigt Signatur-Zulassungen aus dem Schutzverlauf (in keiner Ausschlussliste sichtbar) – nur Anzeige, entfernt wird in der Windows-Sicherheit
App Control	läuft auch unter WDAC/AppLocker/Smart App Control (CLM) – Lesen und Anwenden

EXIT-CODES DES DEPLOY-SKRIPTS

0	Ziel erreicht (oder nichts zu tun)
1	ein Schreibvorgang schlug fehl / griff nicht (Tamper Protection, Richtlinie)
2	Defender-PowerShell-Modul nicht verfügbar
3	läuft nicht mit Administratorrechten
4	Windows Server – nur Clients, nichts getan (Server direkt mit DHS härten)

KONFIGURATION ÜBERTRAGEN

Profil → Aktuellen Zustand exportieren schreibt die **vollständige** Konfiguration: Einstellungen und ASR-Regelmodi, dazu die Ausschlüsse (Pfad/Prozess/Endung/IP), die CFA-Listen (erlaubte Apps und geschützte Ordner) und die regelspezifischen ASR-Ausschlüsse. Diese Listen verbirgt Defender vor einem Lesevorgang ohne Adminrechte – DHS fragt sie deshalb vor dem Schreiben einmal erhöht ab (eine UAC) und **bricht ab**, wenn das abgelehnt wird, statt eine unvollständige Datei zu hinterlassen. Beim **Importieren & anwenden** werden Listeneinträge nur **ergänzt**, nie entfernt. `dhs export-profile --output profile.json` · `dhs apply --profile profile.json --apply`

EHRLICHKEIT IM FLOTTEN-EINSATZ

Das Skript verteilt **lokale** Defender-Einstellungen. Echte Defender-**Richtlinien** (GPO/Intune) haben Vorrang und werden vom Skript als „verwaltet“ respektiert, nie überschrieben. Für zentrale Richtlinien-Verwaltung bleibt Intune / Defender for Endpoint zuständig.

Updates der Sicherheitsinformationen – von jedem Preset gesetzt

DIE DREI EINSTELLUNGEN

Prüfintervall	empfohlen **4** Stunden (`SignatureUpdateInterval`) – eine **zusätzliche** Prüfung neben dem täglichen Zeitplan. **0 = keine zusätzliche Prüfung** und damit der schwächste Wert; ein niedrigerer Wert außer 0 prüft öfter, unter etwa 4 h findet er kaum mehr, weil Microsoft nur wenige Pakete pro Tag veröffentlicht.
Vor der Überprüfung	empfohlen **ein** (`CheckForSignaturesBeforeRunningScan`) – eine geplante Überprüfung holt zuerst die aktuellen Signaturen.
Getaktete Netze	empfohlen **ein** (`MeteredConnectionUpdates`) – sonst schiebt Windows Signatur-Updates in getakteten Netzen auf; ein Notebook läuft dann tagelang veraltet, obwohl die Pakete nur wenige MB groß sind.

EINORDNUNG – KEIN CLOUD-ERSATZ

Die lokalen Signaturen sind das **Offline-Fundament**. Das Fenster zwischen zwei Paketen deckt die **Cloud** ab (MAPS, „Blockieren beim ersten Erkennen“, Cloudschutzstufe). Diese drei Einstellungen härten also den Offline-Rückfall – sie zählen vor allem dort, wo die Cloud-Verbindung schlecht ist oder Vorgaben eine dokumentierte Update-Kadenz verlangen. Ein Cloud-Ersatz sind sie nicht.

Das Deploy-Skript trägt sie als 1:1-Abbild der Referenzmaschine mit. Prüfintervall und getaktete Netze sind **Betriebsentscheidungen** und werden exakt gesetzt, in beide Richtungen; „vor der Überprüfung“ ist eine **Schutzeinstellung** und wird ohne Enforce nur ein-, nie ausgeschaltet.