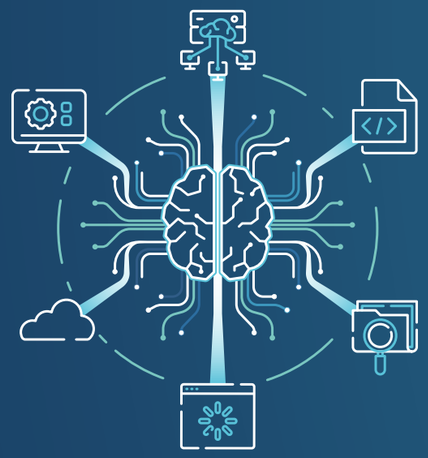
AGENTIC AI CONTROL

ENDPOINT PROTECTION FÜR DAS ZEITALTER AUTONOMER KI

DriveLock

DriveLock Agentic AI Control: Endpoint Protection für die KI-Ära

KI-Agenten steigern die Produktivität – aber auch das Risiko



Agentic AI verändert die Rolle von KI im Unternehmen grundlegend. Moderne KI-Tools beantworten nicht mehr nur Fragen.

- **Sie greifen auf lokale Daten zu**
- **Sie starten Prozesse**
- **Sie nutzen Plugins**
- **Sie kommunizieren mit externen Services**
- **Sie interagieren mit Unternehmensdaten**

Wie ermöglichen Unternehmen produktive KI-Nutzung, ohne die Kontrolle über ihre Endpoints zu verlieren?

Viele Unternehmen verfügen heute über kaum Transparenz darüber,

- **Welche KI-Tools genutzt werden**
- **Welche Plugins, Skills oder MCP-Server aktiv sind**
- **Welche Daten KI-Agenten lesen oder weitergeben**
- **Welche Prozesse oder Netzwerkverbindungen ausgelöst werden**

Ohne Sichtbarkeit gibt es keine wirksame Kontrolle. Genau hier setzt DriveLock an.

DriveLock erweitert bewährte Endpoint-Protection-Konzepte um die Kontrolle von Agentic AI.

Anstatt eine komplett neue Sicherheitskategorie zu schaffen, überträgt DriveLock etablierte Prinzipien wie:

Application Control
Application Behavior Control
File Access Control
Endpoint Visibility

auf neue KI-Artefakte wie:

AI Desktop Apps
Browser-KI und Plugins
Skills
MCP-Server
AI-Konfigurations- und Memory-Dateien

So können Unternehmen KI sicher einführen – mit klaren Richtlinien, Auditierbarkeit und kontrollierten Zugriffsrechten.

Warum klassische Security-Ansätze nicht mehr ausreichen

Agentic AI verhält sich zunehmend wie Software mit eigener Handlungsfähigkeit.

Ein KI-Agent kann:

- **Dateien öffnen und analysieren**
- **Tools und Skripte starten**
- **Browser-Aktionen durchführen**
- **Externe Services kontaktieren**
- **Über MCP-Server auf weitere Systeme zugreifen**

Das Problem: Viele dieser Aktivitäten passieren außerhalb klassischer Security-Modelle.

KI-Agenten benötigen deshalb dieselben Sicherheitsleitplanken wie Anwendungen und Benutzer – nur dynamischer.

Mit DriveLock behalten Sie die Kontrolle

Der erste Schritt zu wirksamer Kontrolle ist die Schaffung von Transparenz.
DriveLock hilft Unternehmen zu erkennen:

- **Welche KI-Tools auf Endpoints installiert sind**
- **Welche Benutzer KI-Agenten verwenden**
- **Welche Skills und Plugins aktiv sind**
- **Welche MCP-Server eingebunden wurden**
- **Welche Prozesse, Dateien oder Netzwerkziele genutzt werden**

So entsteht erstmals eine belastbare Grundlage für sichere KI-Governance.

AGENTIC AI SICHER NUTZEN – STATT KI ZU BLOCKIEREN

1. **Kontrollierte KI-Nutzung mit klaren Guardrails**:
   DriveLock unterstützt Unternehmen dabei, KI produktiv und gleichzeitig sicher einzusetzen.
2. **AI Tool & Skill Control:**
   Kontrollieren Sie, welche KI-Tools, Plugins, Skills oder MCP-Server genutzt werden dürfen.
3. **AI Behaviour Control:**
   Begrenzen Sie den Zugriff von KI-Agenten auf Dateien, Ordner, Prozesse und Netzwerkziele.
4. **Policy Packs:**
   Nutzen Sie vorkonfigurierte Richtlinien für gängige KI-Anwendungen wie ChatGPT Desktop, Claude Desktop, Copilot oder Cursor.
5. **Kontrollierter Self Service:**
   Ermöglichen Sie Benutzern gezielte Freigaben – inklusive Zeitlimit, Berechtigungen und Audit-Trail.
6. **Monitoring-to-Policy:**
   Leiten Sie Sicherheitsrichtlinien direkt aus realem Nutzungsverhalten ab.

Der pragmatische Ansatz für sichere KI-Adoption

Viele Anbieter versprechen vollständigen Schutz vor allen KI-Risiken.
DriveLock verfolgt einen praxisnahen Ansatz:

1. **Sichtbarkeit schaffen**
2. **Risiken verstehen**
3. **Richtlinien definieren**
4. **KI kontrolliert freigeben**
5. **Nutzung auditierbar machen**

So bleibt KI ein Produktivitätsgewinn – und wird nicht zum Blind Spot der Endpoint Security.

AGENTIC AI BRAUCHT ENDPOINT CONTROL ÜBERZEUGEN SIE SICH!

Sprechen Sie mit unseren Experten

Jetzt unverbindlich 30 Tage gratis testen

AUSGEZEICHNET UND ZERTIFIZIERT

DriveLock SE
Landsberger Straße 396 | 81241 München
+49 (89) 546 36 49-0 | info@drivelock.com

DriveLock