



DATENBLATT

DE

Endpoint Privilege Manager

Urheberrecht 2026 Segura® | Alle Rechte vorbehalten
Dokumentklassifizierung: Öffentlich | März 2026



Endpoint Privilege Manager

Vom Least-Privilege-Prinzip zu maximaler Sicherheit: Segura® EPM

In zunehmend komplexen IT-Infrastrukturen sind eine konsequente Kontrolle administrativer Berechtigungen sowie die effektive Umsetzung des Least-Privilege-Prinzips entscheidend, um das Sicherheitsniveau zu erhöhen und das Risiko von Datenvorfällen zu minimieren. An dieser Stelle setzt der Segura® Endpoint Privilege Manager (EPM) an.

Als leistungsfähige Privileged Elevation and Delegation Management (PEDM)-Lösung ermöglicht EPM die kontrollierte und sichere Ausführung privilegierter Funktionen auf Windows- und Linux-Endpunkten.

Permanente Administratorrechte sind nicht Bestandteil des Konzepts. Mit EPM erfolgt die Vergabe erhöhter Berechtigungen temporär und an spezifische Anwendungen gebunden. Dadurch können Aufgaben mit administrativen Anforderungen ausgeführt werden, ohne die Sicherheit der IT-Umgebung zu beeinträchtigen.

Features



Granulare Anwendungskontrolle:

Privilegierte Ausführung auf Basis genehmigter Aktionslisten:

Autorisierte User können Administratorrechte zur Ausführung definierter Anwendungen anfordern, sodass ausschließlich geschäftskritische Applikationen mit erhöhten Berechtigungen sicher ausgeführt werden.



Umfassendes Windows-Endpoint-Management:

Zugriff auf die Systemsteuerung mit Administratorrechten (nur Windows):

User können administrative Aufgaben wie die Anpassung von Datums- und Uhrzeiteinstellungen durchführen, wodurch eine effektive Verwaltung zentraler Systemkonfigurationen gewährleistet wird.

Sicherer Zugriff auf sensible Daten in

Netzwerkverzeichnissen (nur Windows): Gewährleistet ein Höchstmaß an Sicherheit für freigegebene Dateien und Verzeichnisse im Netzwerk und schützt geschäftskritische Informationen vor Bedrohungen.

Automatisierte Anwendungsausführung und Zugriff über Makros (nur Windows):

Wiederkehrende Aufgaben werden durch Automatisierung optimiert, während gleichzeitig eine strikte Kontrolle über privilegierte Aktionen erhalten bleibt. Die Benutzerfreundlichkeit von Segura® unterstützt eine effiziente und kontrollierte Umsetzung dieser Prozesse.

Malware-Analyse (nur Windows): Spezialisierte Funktionen zur Malware-Analyse schützen Windows-Endpunkte zuverlässig vor Cyberbedrohungen.

Workflow-Erstellung (nur Windows): Aufgaben und Prozesse lassen sich durch individuell definierte Workflows

automatisieren und vereinfachen, wodurch das Privilegienmanagement optimiert und die operative Effizienz gesteigert wird.

Offline-Nutzung (nur Windows): Die Verwaltung von Berechtigungen für Windows-Endpunkte ist auch im Offline-Betrieb möglich und eignet sich besonders für Umgebungen mit eingeschränkter Konnektivität.

→ **Umfassendes Linux-Privilegienmanagement:**

Integration von Anmeldeinformationen in Gruppenrichtlinien:

Jede Authentifizierung wird auf Basis von Zeitparametern, Aufrufen, Berechtigungen sowie zusätzlichen Gruppenrichtlinien validiert, wodurch die Sicherheit von Linux-Endpunkten gestärkt wird.

Zusätzliche Sicherheitsebene für Anwendungen: Segura® EPM fungiert direkt als LSM (Linux Security Modules) über ACL, PAM, SELinux und sudo, ohne dass eine Neukompilierung des Kernels erforderlich ist, und ergänzt so eine zusätzliche Schutzschicht.

Vollständiges SUDO-Management (nur Linux): Durch die Definition granularer Richtlinien wird eine vollständige Kontrolle über mit SUDO ausgeführte Aktionen auf Linux-Endpunkten ermöglicht und das Sicherheitsniveau erhöht.

→ **Vereinfachte Compliance und Auditierung:**

Sitzungsaufzeichnung unter Windows und Linux: SUDO-Aktionen auf Linux-Endpunkten sowie Sitzungen unter Windows werden aufgezeichnet, um Audit-Anforderungen zu erfüllen, Compliance sicherzustellen und eine lückenlose Nachvollziehbarkeit privilegierter Aktivitäten zu gewährleisten.

Vorteile



Schutz vor Datendiebstahl:

Die Lösung korreliert Ereignisse zur Identifikation verdächtiger Aktivitäten und stellt erweiterte Sicherheitsmechanismen zum Schutz geschäftskritischer Daten bereit.



Vollständige Nachvollziehbarkeit von Aktionen:

Die umfassende Protokollierung privilegierter Aktionen verbessert Audit-Prozesse, unterstützt forensische Analysen und stärkt die Verantwortlichkeit innerhalb der Infrastruktur.



Verhinderung von Privilegienmissbrauch:

Durch die Isolierung kritischer Umgebungen sowie die Korrelation von Ereignissen ermöglicht der Segura® Endpoint Privilege Manager die frühzeitige Erkennung und Eindämmung von Fällen des Privilegienmissbrauchs.



Einhaltung regulatorischer Vorgaben:

Der Endpoint Privilege Manager (EPM) schafft die erforderliche Reife und Kontrolle über privilegierte Aktionen und unterstützt Sie bei der wirksamen Umsetzung regulatorischer Anforderungen.



Entdecken Sie
die Vorteile von
Segura® für Ihr
Unternehmen

[Demo ansehen](#)

[in](#) [▶](#) /segura
[o](#) [f](#) [X](#) segura.security
www.segura.security

Kontakt: kontakt@dagma.eu

segura®
IK