ManageEngine
Privileged Identity Management Suite

EIN EINHEITLICHER ANSATZ ZUM SCHUTZ PRIVILEGIERTER IDENTITÄTEN UND ZUR REGELUNG PRIVILEGIERTER ZUGÄNGE

Mit dieser umfassenden Suite für Unternehmen können IT-Administratoren privilegierte Identitäten verwalten sowie den Zugang zu wichtigen Informationssystemen über eine einfache, einheitliche Plattform steuern und überwachen.

1 Passwortmüdigkeit eliminieren

Stellen Sie ein geschütztes zentrales Repository bereit, in dem eine unbegrenzte Anzahl an Passwörtern gespeichert und schnell abgerufen werden kann. Wirken Sie so der mit der wachsenden Zahl privilegierter Konten einhergehenden Passwortmüdigkeit entgegen. Identifizieren und sperren Sie ungenutzte oder vergessene privilegierte Zugänge, um deren Missbrauch zu verhindern.

2 Sicherheitslücken vermeiden

Erhöhen Sie die Sicherheit privilegierter Konten durch starke, nicht zu erratende Passwörter. Legen Sie strenge Richtlinien für die Passwortkomplexität, den regelmäßigen Austausch von Passwörtern und SSH-Schlüsseln sowie die pünktliche Verlängerung von SSL-Zertifikaten fest.

3 Identitätsdiebstahl verhindern

Schützen Sie die privilegierten Identitäten Ihres Unternehmens vor unberechtigten Zugriffen. Dämmen Sie Angriffe mit Multi-Faktor-Authentifizierung, sofortigen Benachrichtigungen bei Aktivitäten in privilegierten Konten und Sitzungsüberwachung in Echtzeit ein.

4 Interne Bedrohungen minimieren

Reduzieren Sie das Risiko unbeabsichtigter oder gezielter interner Bedrohungen mithilfe detaillierter rollenbasierter Zugangskontrollen. Gewähren Sie Usern zeitlich begrenzten Zugang zu wichtigen Informationssystemen, ohne Anmeldedaten im Klartextformat weiterzugeben.

5 Missbrauch vorbeugen und aufdecken

Legen Sie Genehmigungsprozesse für die Passwortwiederherstellung fest, um unnötige oder nicht autorisierte Zugriffe auf vertrauliche Ressourcen zu unterbinden. Überwachen Sie den Zugriff auf Passwörter und die Verwendung von Berechtigungen kontinuierlich durch Live-Feeds zu Aktivitäten und umfassende Audit-Trails. Erstellen Sie SNMP-Traps und senden Sie Syslog-Meldungen an Managementsysteme, um Anomalien schnell entdecken zu können.

6 Compliance-Anforderungen einhalten

Weisen Sie nach, dass Sie die Standards zur Kontrolle privilegierter Zugänge einhalten, die durch die DSGVO sowie NIST, PCI-DSS, FISMA, HIPAA, NERC-CIP, ISO/IEC 27001, SOX und andere Regelwerke vorgegeben werden. Starke Sicherungsmechanismen, eine solide User-Authentifizierung, die Funktionen für Zugangskontrolle und Passwortbereitstellung sowie detaillierte Berichte, unter anderem für Audits gemäß PCI-DSS, ISO/IEC 27001 und NERC-CIP, unterstützen Sie dabei.

7 IT-Produktivität steigern

Optimieren und automatisieren Sie die Abläufe zur Passwortzurücksetzung für Dienstkonten und andere privilegierte Konten, um die Produktivität zu erhöhen. Profitieren Sie von einem unterbrechungsfreien Zugang zu den Anmeldedaten wichtiger Datenbankressourcen dank optimal gestalteter Module mit hoher Verfügbarkeit.

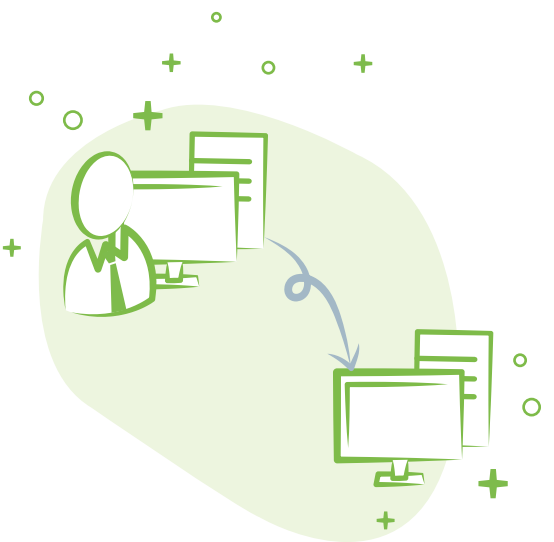
Erfüllen Sie alle Anforderungen Ihres Unternehmens an die Verwaltung privilegierter Identitäten mit Hilfe einer umfassenden Lösung, die zahlreiche grundlegende Dienste in einer zentralen Konsole bereitstellt.

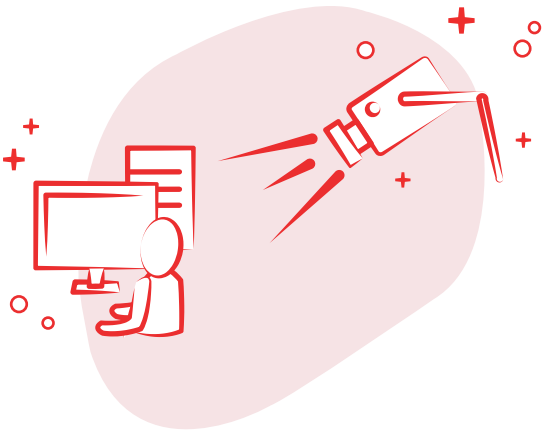
Management privilegierter Konten

Legen Sie bewährte Vorgehensweisen für eine effektive Verwaltung privilegierter Konten fest, um wichtige Datenserver und andere IT-Assets in Ihrer Umgebung zu schützen – unabhängig davon, ob sie eine passwort- oder schlüsselbasierte Authentifizierung nutzen. Dazu gehören Konten für Betriebssysteme, Datenbanken, Server, Anwendungen, Cloud-Plattformen und Netzwerkgeräte.

Management des Remote-Zugangs

Richten Sie zentrale Zugangskontrollen ein und legen Sie fest, wie sich Anwender mit den Zielsystemen verbinden können. Sorgen Sie mit der One-Click-Login-Funktion für höchste Sicherheit, da keine Anmeldedaten als Klartext geteilt werden müssen. Bündeln Sie Verbindungen in einem verschlüsselten Channel-Gateway, der keine direkte Verbindung zwischen User-Gerät und Remote-Host erfordert.



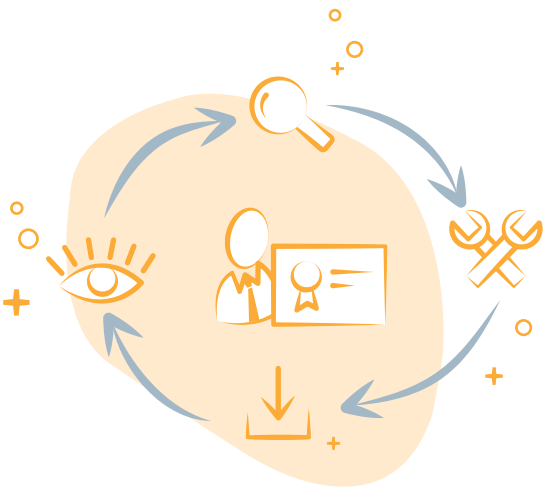


Management privilegierter Sitzungen

Zeichnen Sie die Aktivitäten Ihrer privilegierten Anwender auf kritischen IT-Ressourcen mit dem Privileged Session Monitoring als Video auf, um genau zu dokumentieren, welche Person wann auf welches System zugegriffen hat. So können Sie Missbrauch verhindern und bei Bedarf genau nachweisen, wer seinen privilegierten Zugang wann wofür genutzt hat.

SSL-Zertifikatverwaltung

Verschaffen Sie sich einen umfassenden Überblick über Ihre SSL-Umgebung, um diese vollständig zu kontrollieren. Vermeiden Sie Risiken durch unbemerkt ablaufende Zertifikate, veraltete Hash-Algorithmen und schwache Cipher Suites, die Sie das Vertrauen Ihrer Kunden kosten können. Profitieren Sie von einer durchgehenden Verwaltung des gesamten Zertifikatlebenszyklus.



Feature-Übersicht

- Finden Sie schnell Passwörter, SSH-Schlüssel und SSL-Zertifikate in Ihrem Netzwerk und legen Sie sie geschützt in einem zentralen Speicher ab.
- Teilen Sie Passwörter und SSH-Schlüssel sicher mit Usern für einen festgelegten Zeitraum und widerrufen Sie Berechtigungen automatisch.
- Generieren Sie ganz einfach SSH-Schlüsselpaare und verknüpfen Sie sie mit Usern. Weisen Sie Remote-Systemen neue, starke Passwörter zu.
- Automatisieren Sie den Erwerb, die Bereitstellung, Verlängerung und den Widerruf von SSL-Zertifikaten für öffentliche Domains über eine Integration in Let's Encrypt, die bekannte offene Zertifizierungsstelle.
- Tauschen Sie Passwörter und Schlüsselpaare dank strenger Passwortregeln regelmäßig aus. Legen Sie zuverlässige Abläufe für das Passwort-Management von Dienstkonten fest.
- Ersetzen Sie fest kodierte Anmeldedaten in Konfigurationsdateien und Skripten durch sichere APIs für die Passwortverwaltung zwischen Anwendungen bzw. zwischen Anwendungen und Datenbanken.
- Importieren Sie mit User-Konten verknüpfte Zertifikate in Ihren Active-Directory-Dienst. Automatisieren Sie die Verwaltung von Zertifikaten über deren gesamten Lebenszyklus durch die Integration in Ihre interne Zertifizierungsstelle.
- Legen Sie regelmäßige Netzwerk-Scans fest, um schwache Passwörter, Schwachstellen in SSL-Konfigurationen etc. aufzudecken.
- Stellen Sie sichere, zuverlässige und vollständig emulierte Remote-Verbindungen (über RDP, SSH und SQL) mit nur einem Klick her, ohne Passwörter oder Schlüssel als Klartext preiszugeben.
- Zeichnen Sie Sitzungen auf und archivieren Sie sie als Videodateien.
- Überwachen Sie aktive Sitzungen in Echtzeit, verfolgen Sie User-Aktivitäten und beenden Sie Sitzungen, wenn Sie verdächtige Aktivitäten feststellen.
- Nutzen Sie das umfassende Audit-Logging sowie die Live-Feeds, um User-Aktivitäten lückenlos aufzuzeichnen.
- Profitieren Sie von einer nahtlosen Integration in Active-Directory-/LDAP-basierte Dienste, Ticket-Systeme für Unternehmen, SIEM-Tools, Syslog-Server und SAML 2.0-Service-Provider.

Über ManageEngine

ManageEngine, die IT-Management-Sparte der ZOHO Corp., entwickelt flexible Lösungen, die sich für jedes Unternehmen eignen – unabhängig von Größe oder Budget. Die umfassende IT-Management-Software zeichnet sich durch einfache Bedienung, zahlreiche Features und eine hervorragendes Preis-/Leistungsverhältnis aus. Mit über 90 Produkten und kostenlosen Tools bietet ManageEngine alles, was IT-Abteilungen zur Verwaltung der IT-Umgebung benötigen. Ob Netzwerk- und Geräte-Management oder IT-Sicherheit und Service Desk: ManageEngine hat es sich zum Ziel gesetzt, die Unternehmens-IT noch besser miteinander in Einklang zu bringen, damit IT-Teams Zeit für neue Chancen und Themen haben.

Über MicroNova

Die MicroNova AG ist seit mehr als 15 Jahren exklusiver Vertriebspartner für die ManageEngine-Produkte in Deutschland. Das Unternehmen unterstützt seine Kunden nicht nur bei der Auswahl, Installation und Inbetriebnahme der für sie optimal geeigneten Software, sondern steht auch als deutschsprachiger Ansprechpartner für Fragen und Probleme zur Verfügung - vor Ort oder „remote" über die Service-Mitarbeiter in der Firmenzentrale bei München. Die erstklassige Hotline und erfahrene Techniker helfen beispielsweise, eventuelle Störungen schnell und zuverlässig zu beheben. Darüber hinaus bietet MicroNova offene Schulungen sowie individuelle Trainings für einen sicheren Umgang mit der jeweiligen Software an.

ManageEngine

MicroNova
Software und Systeme

www.manageengine.de/
passwordmanagerpro

Ihr ManageEngine-Partner:
MicroNova AG
Unterfeldring 17
D-85256 Vierkirchen
Tel.: +49 8139 9300-456
E-Mail: sales-ManageEngine@micronova.de
Support: support-ManageEngine@micronova.de
Web: www.ManageEngine.de