Gold Microsoft Partner

Microsoft

DATENBLATT

# One Identity Safeguard

**Sicheres Speichern, Verwalten, Aufzeichnen und Analysieren von privilegierten Zugriffen**

## Vorteile

- Eindämmen potenzieller Schäden infolge einer Sicherheitsverletzung
- Erfüllung von Compliance-Anforderungen
- Schnelle Amortisierung durch vereinfachte Bereitstellung und Verwaltung
- Effiziente Erstellung von Prüfberichten
- Identifizieren und Stoppen von riskantem Verhalten und ungewöhnlichen Ereignissen
- Vereinfachung der Verwaltung privilegierter Konten

## Einführung

Hacker entwickeln die Methoden, mit denen sie sich Zugriff auf Ihre Systemen und Daten verschaffen, ständig weiter. Letztlich möchten sie an Ihre privilegierten Konten kommen. Bei nahezu jeder relevanten Sicherheitsverletzung der letzten Zeit erfolgte der Zugriff auf kritische Systeme und Daten über kompromittierte privilegierte Konten. Mit den richtigen Lösungen können Sie den aufgrund einer Datensicherheitsverletzung auftretenden Schaden eingrenzen: Nutzen Sie diese Lösungen zur Bereitstellung eines sicheren, effizienten und konformen Zugriffs auf privilegierte Konten.

Für IT-Manager sind diese Konten mit unbeschränktem Zugriff aus zahlreichen Gründen schwierig zu verwalten, u. a. aufgrund der bloßen Zahl der privilegierten Konten und der Personen, die auf diese zugreifen müssen. Neben diesen Herausforderungen umfassen herkömmliche Lösungen für die Verwaltung privilegierter Konten (Privileged Access Management, PAM) komplexe Architekturen, lange Bereitstellungszeiten und mühsame Verwaltungsanforderungen.

PAM kann zwar eine große Herausforderung darstellen, muss es jedoch nicht. One Identity Safeguard ist eine integrierte Lösung, die einen sicheren gehärteten Kennwort-Safe mit einer Sitzungsverwaltung und Überwachung mit Erkennung von Bedrohungen und Analysen verbindet. Damit werden privilegierte Zugriffe sicher gespeichert, verwaltet, dokumentiert und analysiert.


## Sicherer privilegierter Zugriff ohne Kompromisse

Schützen Sie Ihre privilegierten Konten stressfrei durch sicheres Speichern, Verwalten, Aufzeichnen und Analysieren von privilegierten Zugriffen, und stellen Sie Ihre Administratoren und Prüfer mit One Identity Safeguard zufrieden.

## Safeguard for Privileged Passwords

One Identity Safeguard for Privileged Passwords automatisiert, kontrolliert und sichert den Prozess der Erteilung privilegierter Anmeldeinformationen mit rollenbasierter Zugriffsverwaltung und automatisierten Workflows. Das benutzerzentrierte Design von Safeguard for Privileged Passwords bedeutet eine reduzierte Lernkurve. Zudem können Sie mit der Lösung Kennwörter von einem beliebigen Ort aus und auf nahezu jedem Gerät verwalten. So erhalten Sie eine Lösung, die für den Schutz Ihres Unternehmens sorgt sowie für eine neue Freiheit und neue Funktionen für privilegierte Benutzer.

## Safeguard for Privileged Sessions

Mit One Identity Safeguard for Privileged Sessions können Sie privilegierte Sitzungen von Administratoren, Remote-Anbietern und anderen hochgradig risikobehafteten Benutzern steuern, überwachen und aufzeichnen. Die Aktionen, die Benutzern in ihren Sitzungen vornehmen, werden aufgezeichnet und mit einem Index versehen. Das erleichtert das spätere Auffinden von Sitzungen, hilft bei der Vereinfachung und Automatisierung der Berichterstellung und lockert Ihre Anforderungen an Prüfung und Compliance. Darüber hinaus fungiert Safeguard for Privileged Sessions als Proxy. Es inspiziert den Protokollverkehr auf Anwendungsebene und kann Datenverkehr abweisen, der das Protokoll verletzt – und wird dadurch zu einem wirksamen Schutzschild gegen Angriffe.

## Safeguard for Privileged Analytics

Mit One Identity Safeguard for Privileged Analytics können Sie Analysen des Benutzerverhaltens für sich nutzen und noch unbekannte interne und externe Bedrohungen entdecken sowie verdächtige Aktivitäten erkennen und unterbinden. Safeguard for Privileged Analytics bewertet die potenziellen Risikostufen von Bedrohungen, sodass Sie Ihre Reaktion priorisieren, bei unmittelbaren Bedrohungen sofort eingreifen und letztlich Datensicherheitsverletzungen verhindern können.

# Funktionen und Merkmale

## Richtlinienbasierte Freigabekontrolle

Über einen sicheren Webbrowser mit Unterstützung für mobile Geräte können Sie Zugriff anfordern und Genehmigungen für privilegierte Kennwörter und Sitzungen erteilen. Je nachdem, welche Richtlinie in Ihrem Unternehmen gilt, können Anforderungen automatisch oder erst nach Freigabe durch zwei oder mehr Stellen genehmigt werden. Unabhängig davon, ob in Ihren Richtlinien die Identität und Zugriffsberechtigungen der anfordernden Person, die Uhrzeit und der Tag des Anforderungsversuchs, die jeweils angeforderte Ressource oder alle diese Punkte berücksichtigt werden, können Sie One Identity Safeguard gemäß Ihren individuellen Anforderungen konfigurieren. Zudem können Sie Ursachencodes eingeben und/oder eine Integration mit Ticketing-Systemen vornehmen.

## Prüfung, Aufzeichnung und Wiedergabe kompletter Sitzungen

Die gesamte Sitzungsaktivität – bis hin zum Drücken von Tasten, Mausbewegungen und geöffneten Fenstern – wird erfasst, indiziert und in einem manipulationssicheren Prüfprotokoll gespeichert, das wie ein Video angesehen und wie eine Datenbank durchsucht werden kann. Sicherheitsteams können in den Sitzungen nach spezifischen Ereignissen suchen und die Aufzeichnung von der genauen Stelle aus, an der die Suchkriterien auftraten, wiedergeben. Audit Trails sind zu Forensik- und Compliance-Zwecken verschlüsselt, zeitgestempelt und kryptografisch signiert.

## Sofort betriebsbereit

Safeguard for Privileged Sessions kann im transparenten Modus bereitgestellt werden, ohne dass Änderungen an Benutzerworkflows notwendig sind. Zudem kann Safeguard als Proxygateway fungieren und die Funktion eines Routers im Netzwerk übernehmen – unsichtbar für Benutzer und Server. Administratoren können die von ihnen bevorzugten Client-Anwendungen weiter benutzen und auf Zielserver und -systeme ohne Unterbrechung ihrer täglichen Routine zugreifen.

## Biometrie des Benutzerverhaltens

Jeder Benutzer besitzt ein eigentümliches Verhaltensmuster, sogar beim Ausführen von identischen Aktionen wie Tippen oder Bewegen der Maus. Die in Safeguard for Privileged Analytics eingebauten Algorithmen analysieren diese von Safeguard for Privileged Sessions erfassten Verhaltenscharakteristiken. Die Analysen der Tastendruckdynamik und der Mausbewegung dienen zur Identifizierung von Sicherheitsverletzungen sowie zur ständigen biometrischen Authentifizierung.

## Ortsunabhängige Genehmigung

Mit One Identity Starling Two-Factor Authentication können Sie Anfragen von überall aus über nahezu jedes Gerät genehmigen oder ablehnen, ohne im VPN angemeldet sein zu müssen.

## Persönlicher Kennworttresor

Alle Mitarbeiter können in einem kostenlosen persönlichen Kennworttresor Kennwörter für Nicht-Verbund-Unternehmenskonten speichern und auf Zufallsbasis erzeugen. Damit kann Ihr Unternehmen ein sanktioniertes Tool nutzen, mit dem sich auf sichere Weise Kennwörter weitergeben und wiederherstellen lassen und das damit dringend benötigte Sicherheit und Transparenz für Unternehmenskonten bietet.

## Favoriten

Greifen Sie direkt über den Anmeldebildschirm schnell auf die Kennwörter zu, die Sie am meisten verwenden. Sie können mehrere Kennwortanforderungen zu einem einzigen Favoriten zusammenfassen, sodass Sie mit einem Klick Zugriff auf alle benötigten Konten erhalten.

## Ermittlung

Dank Host-, Verzeichnis- und Netzwerkermittlungsoptionen können Sie privilegierte Konten oder Systeme in Ihrem Netzwerk schnell erkennen.

## Warnen und Blockieren in Echtzeit

Safeguard for Privileged Sessions beobachtet den Netzwerkverkehr in Echtzeit und führt verschiedene Aktionen durch, wenn in der Befehlszeile oder auf dem Bildschirm ein bestimmtes Muster erscheint. Vordefinierte Muster können ein risikobehafteter Befehl oder Text in einem textorientierten Protokoll oder ein verdächtiger Fenstertitel bei einer grafischen Verbindung sein. Wenn eine verdächtige Benutzeraktion erkannt wird, kann Safeguard das Ereignis protokollieren, eine Warnmeldung senden oder die Sitzung umgehend beenden.

## Befehls- und Anwendungskontrolle

Safeguard for Privileged Sessions unterstützt sowohl die Erstellung von Negativlisten als auch von Positivlisten für Befehle und Fenstertitel.

## Unterstützung zahlreicher Protokolle

Safeguard for Privileged Sessions bietet vollständige Unterstützung der Protokolle SSH, Telnet, RDP, HTTP(s), ICA und VNC. Zusätzlich können Sicherheitsteams entscheiden, welche Netzwerkdienste (z. B. Dateiübertragung, Shell-Zugriff usw.) innerhalb der Protokolle sie für Administratoren aktivieren/deaktivieren möchten.

## Volltextsuche

Mit der OCR-Engine (Optical Character Recognition) können Prüfer Volltextsuchen sowohl für Befehle als auch beliebige Texte vornehmen, die der Benutzer im Inhalt der Sitzungen sieht. Sie kann sogar Dateioperationen auflisten und übertragene Dateien zur Überprüfung extrahieren. Die Möglichkeit, Sitzungsinhalte und Metadaten zu durchsuchen, beschleunigt und vereinfacht die Forensik und IT-Fehlerbehebung.

## Drop-in-Bereitstellung

Dank der raschen Appliance-basierten Bereitstellung und vereinfachtem Rerouting des Verkehrs können Sie mit One Identity Safeguard Sitzungen in einigen Tagen aufzeichnen, ohne Ihre Benutzer zu stören.

## RESTful API

Safeguard nutzt eine modernisierte REST-basierte API für die Verbindung mit anderen Anwendungen und Systemen. Jede Funktion wird über die API bereitgestellt, die eine schnelle und einfache Integration ermöglicht, unabhängig davon, was Sie tun möchten oder in welcher Sprache Ihre Anwendungen geschrieben sind.

## Änderungskontrolle

Die Lösung ermöglicht eine konfigurierbare, granulare Änderungskontrolle für gemeinsam genutzte Anmeldedaten. Dabei erlaubt sie unter anderem die Aufschlüsselung nach Zeitpunkt und letzter Verwendung und kann zwischen manuellen und erzwungenen Änderungen unterscheiden.

## Der One Identity Ansatz für die privilegierte Zugriffsverwaltung

Das One Identity Portfolio bietet derzeit das branchenweit umfassendste Angebot an Lösungen für die Verwaltung privilegierter Konten. Doch damit nicht genug: Im One Identity Softwareportfolio finden Sie auch Lösungen für die präzise Delegierung von UNIX-Root-Konten und Active Directory-Administratorkonten, Add-Ons für Enterprise-Bereitstellungen des Open Source-Tools sudo und Keylogger für UNIX-Root-Aktivitäten. Alle diese Optionen sind eng in unsere branchenführende Active Directory Bridging-Lösung integriert.

## Über One Identity

One Identity unterstützt Unternehmen bei der erfolgreichen Umsetzung von Identitäts- und Zugriffsverwaltung (IAM). Mit unserem einzigartigen Portfolio an Lösungen für Identitäts-Governance, Zugriffsverwaltung, Verwaltung privilegierter Konten und Identity-as-a-Service-Lösungen können Unternehmen ihr volles Potenzial entwickeln, ohne Einschränkung durch Sicherheit, und profitieren dabei vom Schutz vor Bedrohungen.
Weitere Informationen erhalten Sie unter OneIdentity.com.


Datasheet_2021-Safeguard_PG_DE-WL_68957