One Identity Safeguard

Sichere Speicherung, Verwaltung, Aufzeichnung und Analyse privilegierter Zugriffe

Einführung

Hacker entwickeln die Methoden, mit denen sie sich Zugriff auf Ihre Systemen und Daten verschaffen, ständig weiter. Letztlich zielen sie auf Ihre privilegierten Konten ab. 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 Anzahl der privilegierten Konten und der Personen, die auf diese zugreifen müssen. Neben diesen Herausforderungen umfassen herkömmliche Lösungen für Privileged Access Management (PAM) komplexe Architekturen, lange Bereitstellungszeiten und mühsame Verwaltungsanforderungen.

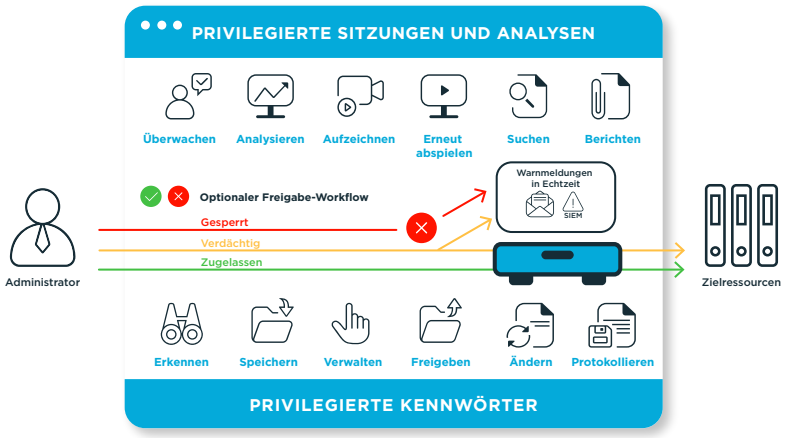
PAM muss jedoch nicht zwangsweise eine so große Herausforderung sein. One Identity Safeguard ist eine integrierte Lösung, die einen sicheren gehärteten Kennwort-Safe mit einer Lösung zur Sitzungsverwaltung und Überwachung mit Erkennung von Bedrohungen und Analysen verbindet. Damit werden privilegierte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

Vorteile

- **Eindämmung potenzieller Schäden** infolge einer Sicherheitsverletzung
- **Erfüllung von Compliance-Anforderungen**
- **Schnelle Amortisierung** durch vereinfachte Bereitstellung und Verwaltung
- **Effiziente Erstellung von Auditberichten**
- **Identifizierung und Beendigung von riskantem Verhalten** und ungewöhnlichen Ereignissen
- **Vereinfachung des Privileged Account Management**

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

Mit One Identity Safeguard for Privileged Passwords wird die Gewährung privilegierter Anmeldeinformationen mit rollenbasiertem Access Management und automatisierten Workflows automatisiert, gesteuert und gesichert.

Durch das benutzerzentrierte Design von Safeguard for Privileged Passwords finden sich Benutzer schnell zurecht. 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, Anbietern an einem anderen Standort und anderen Benutzern mit hohem Gefahrenpotenzial steuern, überwachen und aufzeichnen. Die Aktionen, die Benutzer in ihren Sitzungen vornehmen, werden aufgezeichnet und indiziert. Das erleichtert das spätere Auffinden von Sitzungsereignissen, hilft bei der Vereinfachung und Automatisierung der Berichterstellung und ermöglicht das einfachere Erfüllen von Audit- und Compliance-Anforderungen. 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.

Auditierung, Aufzeichnung und Wiedergabe kompletter Sitzungen

Sämtliche Aktivitäten während einer Sitzung werden bis hin zu Tastenanschlägen, Mausbewegungen und angezeigten Fenstern erfasst, indiziert und in manipulationssicheren Audit Trails gespeichert, die wie ein Video angezeigt und wie eine Datenbank durchsucht werden können. Sicherheitsteams können Sitzungen nach bestimmten Ereignissen durchsuchen und die Aufzeichnung von genau dem Punkt abspielen, wo die Suchkriterien erfüllt sind. Audit Trails werden zu Forensik- und Compliance-Zwecken verschlüsselt, mit Zeitstempeln versehen und kryptografisch signiert.

ONE IDENTITY by Quest

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 weiterhin vertraute Client-Anwendungen verwenden und ohne Unterbrechung ihrer täglichen Arbeitsabläufe auf Zielserver und -systeme zugreifen.

Benutzerverhaltensbiometrik

Jeder Benutzer hat ein ganz eigenes 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.

Support für Multi-Faktor-Authentifizierung

Es ist nicht ausreichend, den Zugriff auf Kennwörter lediglich mit einem anderen Kennwort zu schützen. Erweitern Sie die Sicherheit von Safeguard mittels Zwei-Faktor-Authentifizierung (2FA). Safeguard unterstützt jede RADIUS-basierte 2FA-Lösung.

Safeguard for Privileged Passwords unterstützt das Profil für SAML 2.0 Web Browser Single-Sign-On (SSO). So können Sie Authentifizierung im Verbund mit vielen verschiedenen STS-Servern und Services von Identitätsanbietern konfigurieren und deren MFA nutzen.

Bei privilegierten Konten ist unter Umständen ein von einer TOTP-Authentifizierungsstelle generierter Code als Authentifizierungsfaktor erforderlich. Safeguard Privileged Passwords kann als Authentifizierungsstelle fungieren und den entsprechenden Code zusammen mit Anmeldeinformationen/beim Sitzungs-Check-out bereitstellen.

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

Favoriten ermöglichen den schnellen Zugriff auf häufig genutzte Kennwörter über den Anmeldebildschirm. Sie können mehrere Kennwortanforderungen zu einem einzigen Favoriten zusammenfassen, sodass Sie mit einem Klick Zugriff auf alle benötigten Konten erhalten.

Erkennung

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

Warnmeldungen und Sperrung in Echtzeit

Safeguard for Privileged Sessions überwacht 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 Anwendungssteuerung

Safeguard for Privileged Sessions unterstützt das Erstellen von Negativlisten und 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 für 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 schnellen Appliance-basierten Bereitstellung und des vereinfachten Reroutings des Verkehrs können Sie mit One Identity Safeguard innerhalb weniger Tage Sitzungen aufzeichnen, ohne Ihre Benutzer bei der Arbeit zu stören.

RESTful API

Safeguard verwendet eine modernisierte REST-basierte API zum Herstellen einer Verbindung mit anderen Anwendungen und Systemen. Jede Funktion wird über die API verfügbar gemacht, um eine schnelle und einfache Integration zu ermöglichen, unabhängig von der gewünschten Aktion oder der Sprache, in der Ihre Anwendungen geschrieben sind.

Änderungskontrolle

Die Lösung ermöglicht eine konfigurierbare, granulare Änderungskontrolle für gemeinsam genutzte Anmeldeinformationen. 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 Privileged Access Management

Das One Identity Portfolio beinhaltet die branchenweit größte Auswahl an Lösungen für Privileged Access Management. 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 stellt Lösungen für Unified Identity Security bereit, die Kunden dabei helfen, ihren Cybersicherheitsstatus zu stärken und die für ihr Unternehmen unerlässlichen Mitarbeiter, Anwendungen und Daten zu schützen. Unsere Unified Identity Security Platform vereint erstklassige Lösungen für Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) sowie Active Directory Management (ADMgmt), mit denen Unternehmen von einem fragmentierten auf einen ganzheitlichen Ansatz für Identitätssicherheit umsteigen können. One Identity genießt weltweites Vertrauen und verwaltet über 500 Millionen Identitäten für mehr als 11.000 Unternehmen auf der ganzen Welt. Weitere Informationen finden Sie unter www.oneidentity.com.

Datasheet-2023-OI-Safeguard-US-PG-DE-WL-82102

ONE IDENTITY by Quest