DATENBLATT

One Identity Safeguard

Sicheres Speichern, Verwalten, Aufzeichnen und Analysieren von privilegierten Zugriffen

Vorteile

- Abmildern des potenziellen Schadens von Sicherheitsverstößen
- Erfüllung von Compliance-Anforderungen
- Schnelle Amortisierung durch vereinfachte Bereitstellung und Verwaltung
- Effiziente Erstellung von Überwachungsberichten
- Identifizierung von privilegierten Benutzern mit hohem Risiko, riskantem Verhalten und ungewöhnlichen Ereignissen
- Vereinfachung der Verwaltung privilegierter Konten

Einleitung

Hacker entwickeln die Methoden, mit denen sie sich Zugang zu Ihren 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. Sie können den aufgrund einer Datensicherheitsverletzung auftretenden Schaden durch die Bereitstellung von Lösungen eingrenzen, die eine sichere, effiziente und konforme Methode für den Zugriff auf privilegierte Konten zur Verfügung stellen.

Für IT-Manager sind diese Konten mit unbeschränktem Zugriff aus zahlreichen Gründen schwierig zu verwalten, u. a. aufgrund der schieren Anzahl 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. Der privilegierte Zugriff wird sicher gespeichert, verwaltet, aufgezeichnet und analysiert.

Sicherer privilegierter Zugang ohne Einbußen

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

Safeguard for Privileged Passwords

Mit One Identity Safeguard for Privileged Passwords wird der Prozess des Gewährens privilegierter Anmeldeinformationen dank rollenbasierter Zugriffsverwaltung und automatisierter Workflows automatisiert, gesteuert und gesichert. 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. Das Endergebnis ist eine Lösung, die für Schutz Ihres Unternehmens und für eine neue Freiheit sowie für neue Funktionen für privilegierte Benutzer sorgt.

Safeguard for Privileged Sessions

Mit One Identity Safeguard for Privileged Sessions können Sie privilegierte Sitzungen von Administratoren, ortsfernen Geschäftspartnern und anderen Personen mit hohen Risiken steuern, überwachen und aufzeichnen. Der Inhalt der aufgezeichneten Sitzungen wird mit einem Index versehen. Dies erleichtert das spätere Auffinden von Sitzungen und hilft bei der Vereinfachung und Automatisierung von Berichten. Diese Funktionalität lockert Ihre Anforderungen an Überwachung und Konformität. 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 arbeiten lassen und dadurch erfahren, welche privilegierten Benutzer das größte Risiko darstellen, Sie können noch unbekannte interne und externe Bedrohungen entdecken und verdächtige Aktivitäten erkennen und unterbinden. Safeguard for Privileged Analytics bewertet die potenziellen Risikostufen von Bedrohungen, sodass Sie Ihre Reaktion priorisieren können – sofortiges Eingreifen bei unmittelbaren Bedrohungen – und letztlich Datenpannen verhindern

Funktionen und Merkmale

Richtlinienbasierte Freigabekontrolle

Zum Anfordern des Zugriffs auf privilegierte Kennwörter und Sitzungen und zur Genehmigung wird ein sicherer Webbrowser mit Unterstützung für mobile Geräte verwendet. Je nachdem, welche Richtlinie in Ihrer Organisation gilt, können Anforderungen automatisch oder erst nach Prüfung 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 – Sie können 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 herunter zu Tastendrücken, 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. Die Prüfprotokolle sind verschlüsselt, mit Zeitstempel versehen und für Konformitäts- und forensische Zwecke kryptografisch signiert.

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.

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 Sicherheitsverstößen sowie zur ständigen biometrischen Authentifizierung.

Ortsunabhängige Genehmigung

Dank One Identity Starling Two-Factor Authentication können Sie Anfragen von überall aus und mit praktisch jedem Gerät genehmigen oder ablehnen, auch wenn Sie nicht im VPN sind.

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. Bei den vordefinierten Mustern könnte es sich um riskante Befehle oder Texte innerhalb eines textorientierten Protokolls oder um einen verdächtigen Fenstertitel in einer Verbindung mit grafischer Oberfläche handeln. Sobald eine verdächtige Aktion eines Benutzers erkannt wird, kann Safeguard das Ereignis protokollieren, eine Warnung absenden oder die Sitzung sofort beenden.

Ermittlung von risikobehafteten Benutzern

Safeguard evaluiert die Gewährung von Befugnissen mithilfe von Regeln zur Risikoklassifizierung, um Konten mit hohen Risiken zu identifizieren. Es werden proaktive Benachrichtigungen gesendet, wenn der Status eines Benutzerprofils durch Änderungen an den gewährten Berechtigungen hochriskant wird. Dies eliminiert das Risiko durch unnötige oder inaktive Berechtigungen, die andernfalls missbräuchlich oder unsachgemäß verwendet werden könnten.

Befehls- und Anwendungskontrolle

Safeguard for Privileged Sessions unterstützt die Aufnahme von Befehlen und Fenstertiteln in schwarze oder weiße Listen.

Sofort betriebsbereit

Safeguard for Privileged Sessions kann in einem transparenten Modus bereitgestellt werden, in dem keine Änderungen am Benutzer-Workflow erforderlich sind. Safeguard kann wie ein Router im Netzwerk als Proxy-Gateway fungieren – unsichtbar für Benutzer und für den Server. Administratoren können die von ihnen bevorzugten Client-Anwendungen weiter benutzen und auf Zielserver und -systeme ohne Unterbrechung ihrer täglichen Routine zugreifen.

Unterstützung zahlreicher Protokolle

Vollständige Unterstützung der Protokolle SSH, Telnet, RDP, HTTP(s), ICA und VNC. Daneben können Sicherheitsteams entscheiden, welche Netzwerkdienste (z. B. Dateitransfer, Shell-Zugriff usw.) sie für Administratoren aktivieren oder deaktivieren möchten.

Volltextsuche

Prüfer können mithilfe der OCR-Engine (Optische Zeichenerkennung, Optical Character Recognition) eine Volltextsuche nach Befehlen und nach für den Benutzer im Kontext seiner Sitzungen angezeigten Texten durchführen. Es können sogar Dateioperationen angezeigt und übertragene Dateien zur Überprüfung extrahiert werden. Die Möglichkeit, Inhalt und Metadaten von Sitzungen zu durchsuchen, beschleunigt und vereinfacht die forensische und die IT- Fehlersuche.

Drop-in-Bereitstellung

Wegen der einfachen Appliance-basierten Bereitstellung und einer vereinfachten Umleitung des Datenverkehrs können Sie mit Safeguard nach wenigen Tagen Sitzungen 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.

One Identity Hybrid-Abonnement

Erweitern Sie die Fähigkeiten von Safeguard mit dem One Identity Hybrid-Abonnement, das sofortigen Zugriff auf die über die Cloud bereitgestellten Funktionen und Dienste ermöglicht. Dazu gehören die „allesfressende“ Starling Two-Factor Authentication, die den Safeguard-Zugang und Starling Identity Analytics & Risk Intelligence for Safeguard schützt, sodass Sie riskante Benutzer und Berechtigungen bereits im Vorfeld erkennen können. Die Bereitstellung sämtlicher One Identity-Lösungen wird durch ein einziges Abonnement aktiviert

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.

Infos über One Identity

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

Datasheet_2018_Safeguard_US_RS_34981