DATENBLATT

One Identity Safeguard On Demand

SaaS-Bereitstellung für sicheres Speichern, Verwalten, Aufzeichnen und Analysieren von privilegierten Zugriffen

Vorteile

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

Cloud ohne Kompromisse

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. Doch es gibt die Möglichkeit, die Schäden zu begrenzen: mit einer On-Demand-Lösung, über die Sie sicher, effizient und vorschriftenkonform privilegierte Konten verwalten können.

Für IT-Manager sind solche Administratorkonten mit unbeschränktem Zugriff aus zahlreichen Gründen schwierig zu verwalten, u. a. aufgrund der immensen Anzahl der privilegierten Konten und der Personen, die darauf 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 On Demand wird als SaaS-Lösung bereitgestellt und kombiniert einen sicheren Passwort-Safe und eine Lösung zur Sitzungsverwaltung und -überwachung mit Bedrohungserkennung und Analysen, die alle über die Cloud verwaltet und bereitgestellt werden.

Mit Safeguard On Demand lässt sich die Bereitstellung privilegierter Anmelde-informationen mit rollenbasierter Zugriffsverwaltung und automatisierten Workflows automatisieren, steuern und absichern. Mit dem benutzerzentrierten Design von Safeguard On Demand profitieren Sie von einer steilen Lernkurve. Außerdem punktet die Lösung durch Flexibilität und Komfort, denn Sie können Kennwörter von einem beliebigen Ort aus und auf nahezu jedem Gerät verwalten. Das Endergebnis ist eine Lösung, die für den Schutz Ihres Unternehmens und für eine neue Freiheit sowie für neue Funktionen für privilegierte Benutzer sorgt.

Mit Safeguard On Demand können Sie privilegierte Sitzungen von Administratoren, Remote-Anbietern und anderen hochgradig risikobehafteten Benutzern steuern, überwachen und aufzeichnen. Der Inhalt der aufgezeichneten Sitzungen wird mit einem Index versehen. Das erleichtert das spätere Auffinden von Sitzungen und hilft bei der Vereinfachung und Automatisierung von Berichten. Diese Funktionalität lockert Ihre Anforderungen an Überwachung und Compliance. Darüber hinaus fungiert Safeguard On Demand 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.

Zudem enthält Safeguard On Demand privilegierte Analysefunktionen, mit denen Sie das Benutzerverhalten analysieren und bis dato unbekannte interne und externe Bedrohungen erkennen und verdächtige Aktivitäten ermitteln und ausmerzen können. Safeguard On Demand 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

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 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 On Demand 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 On Demand agiert im transparenten Modus, ohne dass Änderungen an Benutzer-Workflows erforderlich sind. Safeguard On Demand 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.

Biometrie des Benutzerverhaltens

Jeder Benutzer besitzt ein eigentümliches Verhaltensmuster, sogar beim Ausführen von identischen Aktionen wie Tippen oder Bewegen der Maus. Die in Safeguard On Demand integrierten Algorithmen untersuchen diese verhaltensbezogenen Eigenschaften. Die Analysen der Tastendruckdynamik und der Mausbewegung dienen zur Identifizierung von Sicherheitsverstößen sowie zur ständigen biometrischen Authentifizierung.

Ortsunabhängige Genehmigung

Mit One Identity Cloud Assistant können Sie Anfragen von überall aus und über praktisch jedes Gerät genehmigen oder ablehnen.

Persönlicher Kennworttresor

Alle Mitarbeiter Ihres Unternehmens 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 On Demand überwacht den Datenverkehr in Echtzeit und führt verschiedene Aktionen aus, 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. Sollten verdächtige Benutzeraktivitäten festgestellt werden, kann Safeguard On Demand das Ereignis protokollieren, eine Warnmeldung senden oder die Sitzung umgehend beenden.

Befehls- und Anwendungskontrolle

Safeguard On Demand unterstützt das Erstellen sowohl von schwarzen als auch von weißen Listen für Befehle und Fenstertitel.

Unterstützung zahlreicher Protokolle

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.

RESTful API

Safeguard On Demand 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.

Nach ISO 27001 zertifiziert

One Identity ist ein Unternehmen von Quest und ein führender globaler Anbieter von identitätsbasierten Sicherheitslösungen. Seine Cloud-Infrastruktur und -Prozesse sind gemäß der internationalen Norm ISO/IEC 27001 zertifiziert, die Best Practices für Systeme zum Informationssicherheitsmanagement vorgibt.

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 Safeguard On Demand 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 von Quest ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybridumgebung eine identitätszentrierte Sicherheitsstrategie zu implementieren. Dank unseres einzigartig breit gefächerten und integrierten Portfolios mit Angeboten zum Identitätsmanagement, einschließlich Kontoverwaltung, Identity Governance und Administration sowie Verwaltung des privilegierten Zugriffs, sind Unternehmen in der Lage, ihr volles Potenzial auszuschöpfen und Sicherheit dadurch zu erreichen, dass Identitäten in den Mittelpunkt des Programms gestellt werden und der ordnungsgemäße Zugriff für alle Benutzertypen, Systeme und Daten ermöglicht wird. Weitere Informationen finden Sie unter OneIdentity.com.

Datasheet-Safeguard-OnDemand-PG-DE-WL-64557