DATENBLATT

One Identity Safeguard for Privileged Passwords

Verringern der Risiken von gemeinsam genutzten privilegierten Anmeldeinformationen

Vorteile

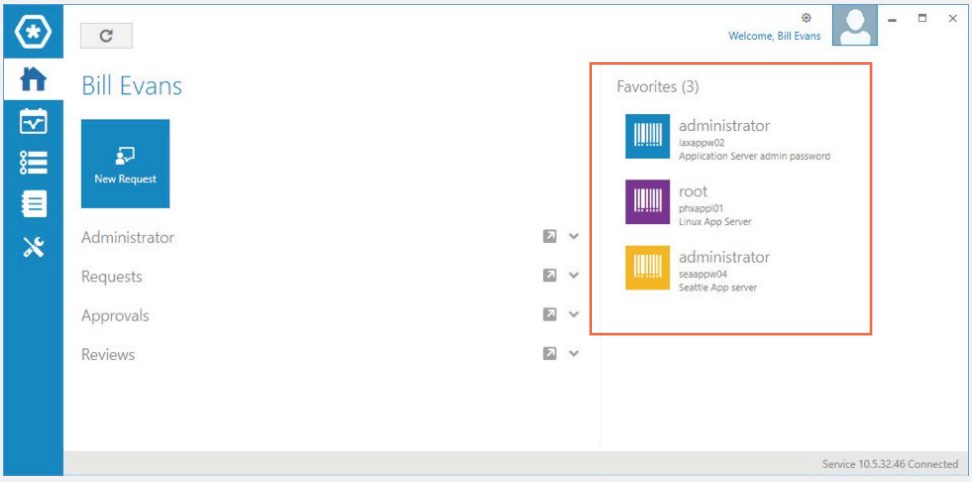
- Abschwächen des Schadens einer Sicherheitsverletzung, indem der Zugriff auf privilegierte Konten kontrolliert wird
- Einhaltung von Compliance-Anforderungen für privilegierte Konten
- Schnellere Wertschöpfung mit vereinfachter Bereitstellung und fortlaufender Verwaltung
- Maximierung der Produktivität mit einer kleinen Lernkurve und elegantem Design der Benutzeroberfläche
- Einfachere und schnellere Erstellung von Audit-Berichten

Einleitung

In jüngster Zeit haben Vorfälle immer wieder gezeigt, dass die Kennwörter privilegierter Konten die am meisten gefährdeten – und möglicherweise die gravierendsten – Sicherheitselemente in den Systemen sind. Mit diesen Kennwörter kann die größte Hürde mühelos überwunden werden. Fallen sie in die Hände von Hackern, haben sie uneingeschränkten Zugriff auf Ihre Systeme und Daten. Und wie Sie gesehen haben kann das für den Ruf und das geistige Eigentum eines Unternehmens verheerend sein.

Bisher haben privilegierte Anmeldeinformationen für Reibungspunkte gesorgt und die Produktivität sowohl von täglichen als auch von langfristigen Prozessen beeinträchtigt. Diese Frage stellt IT-Manager und Sicherheitsbeauftragte vor die schwierige Aufgabe, Sicherheit gegen die Benutzerfreundlichkeit abzuwägen. Bis jetzt. Mit One Identity Safeguard for Privileged Passwords können Sie beides optimieren.

Mit One Identity Safeguard for Privileged Passwords wird der Prozess des Gewährens privilegierter Anmeldeinformationen dank rollenbasierter Zugriffsverwaltung und automatisierter Workflows automatisiert, gesteuert und gesichert. Es kann als gehärtete Appliance bereitgestellt werden, damit Sie sich nicht mehr darum sorgen müssen, wie Sie den Zugriff auf die Lösung selbst absichern. Dadurch können Sie außerdem die Integration mit Ihren Systemen und IT-Strategien beschleunigen. Zudem verläuft die Lernkurve dank des nutzerorientierten Designs sehr kurz und Kennwörter lassen sich von überall aus und über fast jedes Gerät verwalten. Das Ergebnis ist eine Lösung, die Ihrem Unternehmen Sicherheit bietet und privilegierte Benutzer mit neuen Funktionen sowie einem neuen Grad an Freiheit ausstattet.



Schnellzugriff auf Ihre Kennwörter

Favoriten ermöglichen den schnellen Zugriff auf häufig genutzte Kennwörter über den Anmeldebildschirm.

Funktionen und Merkmale

Versionskontrolle:

Damit können Sie Kennwortanforderungen von autorisierten Benutzern für Konten, für die sie eine Zugriffsberechtigung haben, effizient verwalten. Hierfür steht Ihnen eine sichere Webbrowserverbindung zur Verfügung, die auch mobile Geräte unterstützt.

Workflow Engine

Eine Workflow-Engine, die Zeitbeschränkungen, Prüfer, mehrere Genehmigungsberechtigte, Notzugriff und Ablaufdaten für Richtlinien unterstützt. Sie bietet auch die Möglichkeit zur Eingabe von Ursachencodes und/oder zur direkten Integration mit Ticketing-Systemen. Die Kennwortanforderungen können entweder automatisch genehmigt werden oder mehrere Genehmigungsebenen erfordern.

Ermittlung

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

Ortsunabhängige Genehmigung

Mit One Identity Starling können Sie alle Anfragen von überall aus genehmigen oder ablehnen, ohne im VPN angemeldet sein zu müssen.

Favoriten

Greifen Sie direkt über den Anmeldebildschirm schnell auf die Kennwörter zu, die Sie am meisten verwenden.

Immer online

Da diese Lösung für verteiltes Clustering konzipiert wurde, profitieren Sie von echter Hochverfügbarkeit. Darüber hinaus ermöglichen die Funktionen zum eigenständigen Lastausgleich einen höheren Durchsatz und kürzere Antwortzeiten, wenn Sie Kennwörter oder Sitzungen über beliebige Geräte anfordern.

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.

Aktivitäts-Center

Mithilfe eines Tools zur Erstellung von Abfragen können Sie jederzeit schnell und mühelos sämtliche Aktivitäten anzeigen lassen. Berichte können individuell auf den intendierten Empfänger zugeschnitten werden, ob IT-Experte oder Führungskraft. Sie entscheiden, welche Daten hinzugefügt oder entfernt werden, und können genau die Informationen zusammenstellen, die benötigt werden. Zudem können Sie Abfragen planen und die Daten speichern oder in verschiedenen Formaten exportieren.

Unterstützung für Zwei-Faktor-Authentifizierung

Es reicht nicht aus, den Zugriff auf Kennwörter mit einem anderen Kennwort zu schützen. Erweitern Sie die Sicherheit von Safeguard mittels Zwei-Faktor-Authentifizierung (2FA). Safeguard unterstützt jede beliebige RADIUS-basierte 2FA-Lösung und schließt im One Identity Hybrid-Abonnement eine unbegrenzte Two-Factor Authentication ein.

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. Eingeschlossen sind die unbegrenzte Starling Two-Factor Authentication, um den Zugriff auf Safeguard zu schützen, und die Starling Access Certification for Safeguard, mit der sie privilegierte Zugriffsrechte vergeben und die Compliance gewährleisten können. Die Bereitstellung sämtlicher One Identity-Lösungen wird durch ein einziges Abonnement aktiviert.

Smartcard-Unterstützung

Verwenden Sie starke Authentifizierungsmethoden, um den Zugriff auf Ihren Tresor abzusichern.

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 Zugriffsmanagement (IAM). Mit unserem einzigartigen Portfolio an Lösungen für Identitätsverwaltung, Zugriffsmanagement, Verwaltung privilegierter Konten und Identity-as-a-Service-Lösungen können Organisationen ihr volles Potenzial entwickeln, ohne Einschränkung durch Sicherheitsaspekte, jedoch mit umfassendem Schutz vor Bedrohungen.

Erfahren Sie mehr unter OneIdentity.com

Datasheet_2019-Safeguard-PrivPass_RS_41020