DATENBLATT

One Identity Privileged Access Management

Treten Sie der uneingeschränkten Nutzung privilegierter Konten entgegen – mit Privileged Access Management.

Vorteile

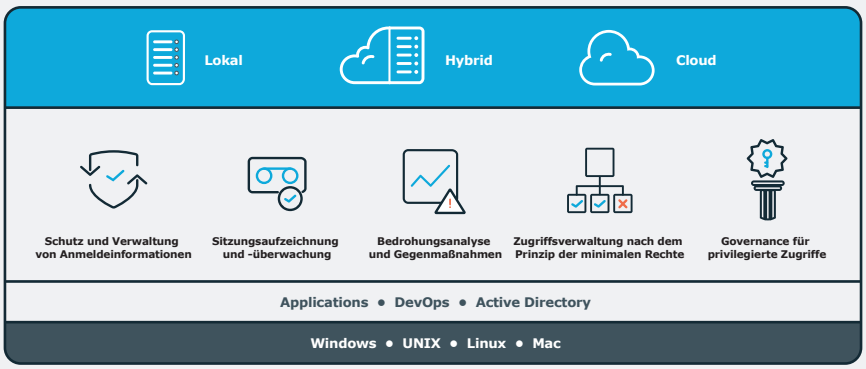
- Unternehmensweite Steuerung des Zugriffs der Administratoren
- Verbesserte Effizienz, Sicherheit und Compliance
- Einfache Nachverfolgung und Audit aller privilegierten Aktivitäten

One Identity Lösungen für Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) ermöglichen die unternehmensweite Kontrolle über den Zugriff der administrativen Konten. One Identity Lösungen für Verwaltung privilegierter Zugriffsrechte steigern die Effizienz und verbessern die Sicherheit und Compliance. Administratoren werden nur die Rechte gewährt, die sie benötigen – nicht mehr und nicht weniger. Zudem werden alle Aktivitäten geprüft und nachverfolgt.

One Identity Lösungen umfassen diesbezüglich die granulare, richtlinienbasierte Delegation der Anmeldeinformationen des Superusers, Sitzungsüberwachung und -wiedergabe wie auch Keystroke-Logging. Sichere und automatisierte Workflows regeln die Herausgabe der privilegierten Anmeldeinformationen an Administratoren sowie die Verwaltung von Kennwörtern in Applikationen in A2A-Szenarien, also von Anwendung-zu-Anwendung und auch von Anwendung-zu-Datenbank. Das Produktangebot von One Identity für Privileged Access Management beinhaltet folgende Lösungen:

One Identity Safeguard for Privileged Passwords sorgt für die sichere Speicherung, die automatische Änderung und die gesteuerte Vergabe der privilegierten Kennwörter und damit für eine individuelle Verantwortung über eine Vielzahl von eingesetzten Systemen, Geräten und Anwendungen hinweg. Die Lösung stellt außerdem sicher, dass Administratoren, die höhere Zugriffsrechte benötigen (üblicherweise durch gemeinsam genutzte Anmeldedaten für die Konten UNIX Root oder Windows Administrator), dieser Zugriff gemäß festgelegten Richtlinien und entsprechenden Genehmigungen gewährt wird. Alle Aktionen werden vollständig auditiert und nachverfolgt und Kennwörter werden sofort nach Ihrer Rückgabe geändert. Application Password Management, eine Funktion von One Identity Safeguard for Privileged Passwords, ersetzt hartcodierte Anwendungs- und Datenbankkennwörter durch programmgesteuerte Aufrufe, die Kontoanmeldeinformationen dynamisch abrufen.

Die Sicherheitslösungen von One Identity beinhalten umfassende Angebote, die hinsichtlich der Verwaltung des privilegierten Zugriffs auf die Bedürfnisse der unterschiedlichsten und anspruchsvollsten Unternehmen eingehen.



One Identity Safeguard for Privileged Sessions bietet Sitzungskontrolle, Proxy, Audit, Aufzeichnung und Wiedergabe für hochgradig risikobehaftete Benutzer wie Administratoren und Remote-Anbieter. Der Inhalt von aufgezeichneten Sitzungen wird indiziert, sodass Sie zur Erfüllung von Audit- und Compliance-Anforderungen ganz einfach Ereignisse durchsuchen und automatisch Berichte erstellen können.

One Identity Lösungen ermöglichen die unternehmensweite Kontrolle über Verwaltungszugriff.

Zudem dient Safeguard for Privileged Sessions als Proxy, untersucht den Protokollverkehr auf Anwendungsebene und kann Verkehr zurückweisen, der gegen das Protokoll verstößt. Damit ist für effektiven Schutz gegen Angriffe gesorgt.

Mit One Identity Safeguard for Privileged Analytics können Sie fragwürdiges Verhalten überwachen und zuvor unbekannte Bedrohungen innerhalb und außerhalb Ihres Unternehmens aufdecken. Unter Verwendung von Verhaltensanalysetechnologie erkennt Safeguard for Privileged Analytics Abweichungen und ordnet sie basierend auf dem Risiko ein, sodass Sie sie priorisieren und entsprechende Maßnahmen ergreifen können, um so letztendlich Datensicherheitsverletzungen zu vermeiden.

One Identity Safeguard for Sudo hilft Unternehmen mit UNIX/Linux Umgebungen dabei, die Verwaltung privilegierter Konten mit Sudo zu optimieren. Die Plug-ins der Lösung optimieren Sudo 1.8.1 (und höher) mit einem zentralen Richtlinienserver, einer zentralen Verwaltung von Sudo und der sudoers-Richtliniendatei, der zentralen Berichterstellung für Zugriffsrechte und Aktivitäten bei Sudo sowie mit Keystroke-Logging von Sudo-Aktivitäten. Die Lösung ermöglicht eine einfache, intuitive und konsistente Verwaltung von Sudo im gesamten Unternehmen und eliminiert dabei die separate Verwaltung.

Mit One Identity Safeguard Authentication Services wird Safeguard for Sudu optimiert, indem UNIX/Linux Identitäten in Microsoft® Active Directory® integriert werden und Sie eine zentrale Verwaltungsschnittstelle und Richtlinie einrichten können, um die Delegierung von UNIX-Root-Konten zu steuern. Safeguard Authentication Services sorgen für eine zentralisierte Authentifizierung und bieten Single Sign-On für UNIX/Linux, wobei Identitäten vereint und Verzeichnisse konsolidiert werden – für eine einfachere Verwaltung und bessere Compliance.

Active Roles bietet die Möglichkeit, das Active Directory Administratorkonto präzise zu delegieren und den Administratorzugriff zentral zu steuern. Dies erfolgt auf Basis klar definierter Rollen, Regeln und Richtlinien.

Mit Privilege Manager for Windows werden Benutzerkonten entsprechend Best Practices nur die erforderlichen Mindestberechtigungen gewährt. Bestimmten Anwendungen und ActiveX Steuerelementen werden jedoch bei Bedarf mehr Rechte erteilt. Sie können erweiterte Ausführungsberechtigungen für Anwendungen, Funktionen und Steuerungen Ihrer Wahl festlegen. Zugriffsrechte können für bestimmte Benutzer, Benutzergruppen, Organisationseinheiten, Betriebssysteme, Computergruppen, Büros oder Anwendungen festgelegt werden. Alle privilegierten Aktivitäten können mithilfe von Berichten mit nur einem Klick geprüft werden.

Identity Manager lässt sich in Safeguard integrieren, um Privileged Access Governance (PAG) sicherzustellen. Die Funktionen von Identity Manager für die Bereitstellung von Konten, Lebenszyklusmanagement und Zugriffsverwaltung können gleichzeitig mit den Funktionen von Safeguard für privilegierte Konten und Sitzungsverwaltung verwendet werden. PAG stellt sicher, dass Benutzer mit privilegierten Konten den erforderlichen Zugang auf Konten erhalten. Mithilfe regelmäßiger Bescheinigungen wird der privilegierte Zugriff belegt und sichergestellt, dass er korrekt zugewiesen wird.

Weitere Informationen

Weitere Informationen über die Verwaltung privilegierter Zugriffsrechte finden Sie unter oneidentity.com/solutions/privileged-access-management/

Infos über One Identity

One Identity von Quest ermöglicht es Unternehmen, lokal, in der Cloud oder in einer Hybrid-Umgebung 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_2020_PrivilegedMgrSUDO_RS_60268