DATENBLATT

Privileged Access Suite for UNIX

Vereinfachte UNIX Sicherheit und Verwaltung und Einhaltung von Complianceanforderungen

Vorteile

- Optimiert die Verwaltung von Identitäten und des Zugriffs in heterogenen Umgebungen
- Konsolidiert die Verwaltung von UNIX Identitäten in Active Directory
- Setzt Zugriff nach dem Least-Privilege-Prinzip durch
- Flexible UNIX Delegierungsfunktionen
- Umfassende Steuerung über eine einzige Konsole
- Einhaltung von Complianceanforderungen und Auditvorgaben für die gesamte UNIX Umgebung
- Zentrale Verwaltung von Richtlinien für alle UNIX/Linux Server

Systemanforderungen

Eine vollständige Liste der Systemanforderungen finden Sie unter oneidentity.com/privileged-access-suite-for-unix

UNIX Systeme (einschließlich Linux und Mac OS) weisen naturgemäß unterschiedliche Herausforderungen in Bezug auf Sicherheit und Verwaltung auf. Da native UNIX-basierte Systeme nicht miteinander verknüpft sind, ist für jeden Server bzw. jede Betriebssysteminstanz eine eigene Authentifizierungs- und Autorisierungsquelle erforderlich – einschließlich Superuser-Authentifizierung über das Root-Konto.

Ohne eine Möglichkeit zur effektiven Verwaltung von Identitäten für UNIX und Nicht-UNIX-basierte Systeme und zur Steuerung und Überwachung der Verwendung des Root-Kontos stehen Organisationen vor dem Problem einer unkoordinierten, ineffizienten und hochgradig inkonsistenten Verwaltung und weisen ein erhöhtes Risiko von potenziellen schwerwiegenden Sicherheitsvorfällen auf.

Mit der Privileged Access Suite for UNIX, Teil der One Identity Produktfamilie, können Sie diese in UNIX-basierten Systemen auftretenden inhärenten Sicherheits- und Verwaltungsprobleme lösen und dabei gleichzeitig für Einhaltung der Complianceanforderungen sorgen. Die

ONE IDENTITY

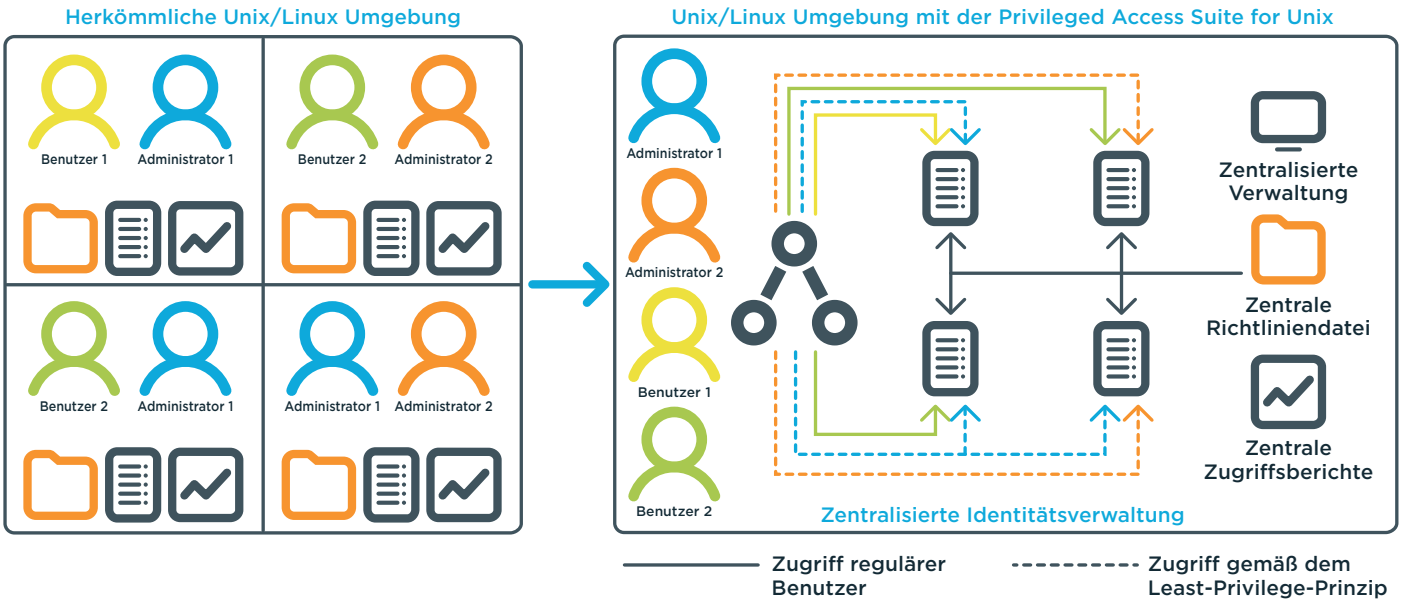


Abbildung 1 – Die Privileged Access Suite for Unix vereint und konsolidiert Identitäten. Gleichzeitig werden klare Verantwortlichkeiten und Zugriff nach dem Least-Privilege-Prinzip im Rahmen einer einzigen Richtliniendatei definiert. Auch die Berichterstellung ist zentralisiert und umfasst die gesamte UNIX/Linux Umgebung.

Suite vereint und konsolidiert Identitäten, weist individuelle Verantwortlichkeiten zu und ermöglicht eine zentralisierte Berichterstellung für Benutzer- und Administratorzugriff auf UNIX.

Mit der Privileged Access Suite for UNIX erhalten Sie eine komplette Sicherheitslösung für UNIX, die Microsoft® Active Directory® Bridge und Root-Delegierungslösungen in einer Konsole vereint. Dies ermöglicht Organisationen eine zentrale Transparenz und optimierte Verwaltung der Identitäten und Zugriffsrechte über die gesamte UNIX Umgebung hinweg.

Active Directory Bridge

Die Privileged Access Suite for UNIX erweitert mithilfe der Active Directory Bridge die Authentifizierung und Autorisierung von Active Directory (AD) auf UNIX, Linux und Mac OS Systeme. Mit Authentication Services, der One Identity AD Bridge-Lösung, können Sie die separate Authentifizierung und Autorisierung nativ in UNIX zugunsten der zentralen Verwaltung einer Identität und eines Kontos in AD ersetzen.

UNIX Systeme sind über ein einziges gut verwaltetes Konto als "vollwertige Bestandteile" in AD integriert, was die Effizienz des Identity-LifeCycle-Managements steigert. Die Stärken der AD Authentifizierung gestatten es UNIX, die sichere Kerberos Authentifizierung zu nutzen, wodurch die Sicherheit erhöht wird.

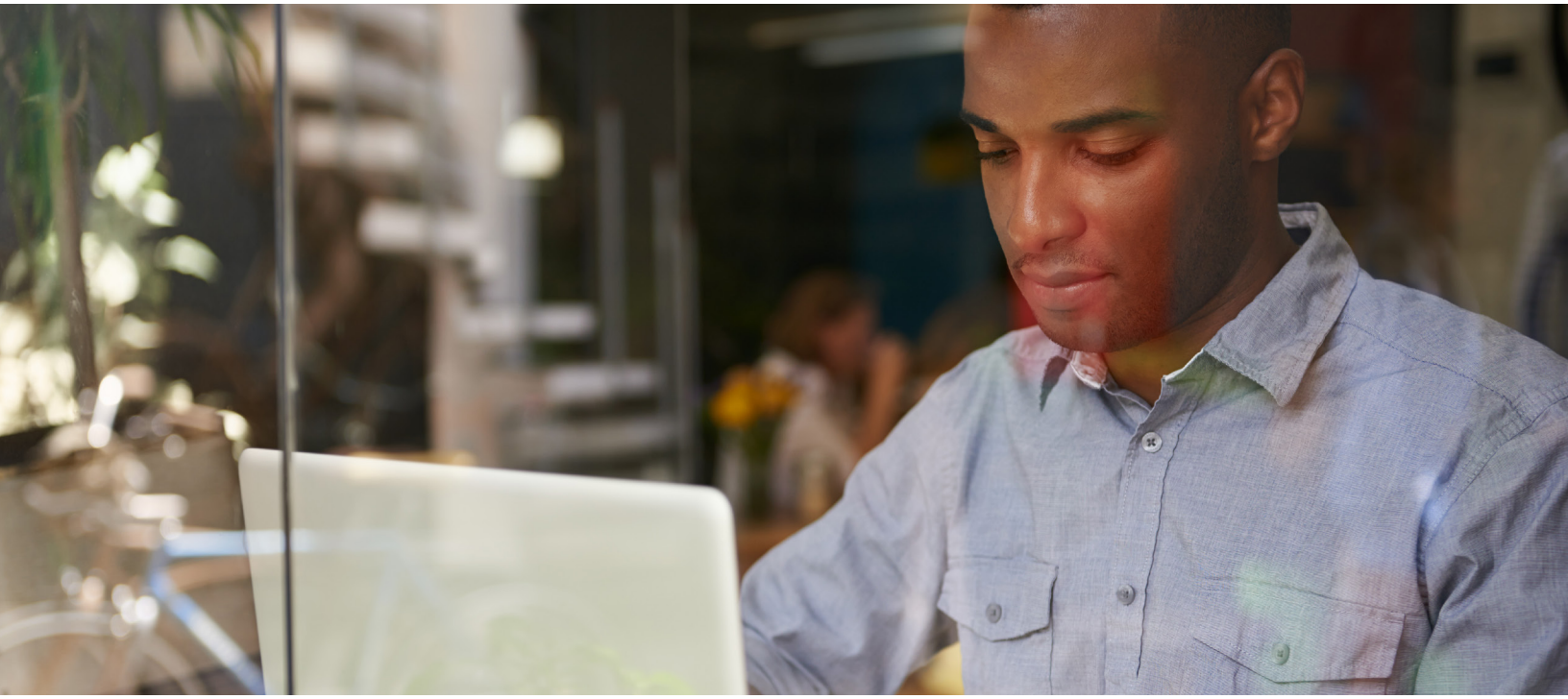
Root-Delegation

Die Privileged Access Suite for UNIX bietet zwei unterschiedliche Ansätze für das Delegieren des UNIX-Root-Kontos. Mit der Suite wird sudo entsprechend Ihren Anforderungen entweder erweitert oder ersetzt. Wenn Sie sich für eine Erweiterung von sudo mit Privilege Manager for Sudo entscheiden, können Sie alles, was sie über sudo wissen und an sudo schätzen, weiter verwenden. Sie erweitern sudo um einen zentralen Policy-Server, eine zentralisierte Verwaltung und zentralisierte Erstellung von Berichten zu Zugriffsrechten und Aktivitäten sowie zu Tastatureingaben, die während der Ausführung von Aktivitäten über sudo getätigt werden.

Wenn Sie sich dazu entscheiden, sudo durch Privilege Manager for Unix zu ersetzen, können Sie weiterhin die UNIX Root-Rechte entsprechend den zentralisierten Richtlinienberichten über die Zugriffsrechte delegieren. Allerdings können Sie die Berechtigungen granularer definieren und Sie haben die Möglichkeit, die Tastatureingaben aller Aktivitäten seit der Anmeldung eines Benutzers aufzuzeichnen, und nicht nur die Befehle mit dem Präfix "su". Zusätzlich wird mit dieser Option die Sicherheit verbessert, indem die Ausführung von Shells und Remote-Hostbefehlen eingeschränkt wird. Gleichzeitig werden Binärdateien vor Zugriff durch Befehle geschützt, die unerkannt an erweiterte Zugriffsrechte gelangen.

Funktionen und Merkmale

Konsolidierte Identitäten – Erleichtern Sie die Verwaltung der Identitäten, indem Sie Unix Konten und rollenbasierten Zugriff vereinen, zentral verwaltet in AD und einer einzigen AD Identität.



Zugriff nach dem Least-Privilege-Prinzip – Gewähren Sie Administratoren nur die zum Ausführen ihrer Aufgaben erforderlichen Rechte und schützen Sie sich dabei vor den Gefahren, die mit zu umfangreichen Zugriffsrechten einhergehen. Den jeweiligen Administratoren werden nur die zum Ausführen ihrer Aufgaben erforderlichen Rechte gewährt.

Zentralisierte Verwaltung und Administration – Konfigurieren Sie einheitliche Zugriffsrichtlinien an einer Stelle für Ihre gesamte UNIX Umgebung und setzen Sie diese ebenso zentral durch.

Sudo-Berichte – Erstellen Sie mühelos Berichte zu sudo-Zugriffsrechten und meistern Sie so eine der größten Herausforderungen im Hinblick auf den Einsatz von sudo in einem Unternehmen. Da Endbenutzer wie gewohnt arbeiten können, ist keine Schulung erforderlich, was die Zugriffsberichterstellung für die Prüfung vereinfacht und zur Einhaltung von Compliance beiträgt.

360°-Transparenz – Verwenden Sie eine einzelne Konsole für die Bereitstellung von integrierten und umfassenden Funktionen für Steuerung und Transparenz hinsichtlich UNIX/ Linux Aktivitäten. Verschaffen Sie sich einen Überblick darüber, wer eine Zugriffsrichtlinie erstellt hat, was diese beinhaltet und wann sie angewendet wurde. Privileged Access Suite for Unix ist darüber hinaus die einzige Lösung, die eine zentralisierte Berichterstellung zu individuellen Zugriffsrechten innerhalb Ihrer gesamten sudo-Umgebung bietet und gleichzeitig eine Enterprise-Lösung für die Delegation ist, die an Benutzerkontodaten in AD gebunden ist.

Vertrauen und Kontrolle – Sorgen Sie für klare Verantwortlichkeiten und Transparenz im Hinblick auf Aktivitäten und Rechte, um Compliance- und Sicherheitsanforderungen zu erfüllen. Audit-Funktionen umfassen Erstellen von Richtlinienberichten und Historie, Änderungsnachverfolgung und -Rollback sowie Erstellen von Protokollen zu Tastatureingaben.

Single Sign-On – Erzielen Sie "echtes Single Sign-On" für die gesamte UNIX, Linux und Mac OS Umgebung und darüber hinaus auch für die wichtigsten Standardanwendungen wie SAP, Siebel usw.

Weitere Informationen

Weitere Informationen über Privileged Access Suite for UNIX finden Sie unter oneidentity.com/privileged-access-suite-for-unix

Über One Identity

Die One Identity Lösungen für Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM) bieten IAM für den Praxiseinsatz und umfassen geschäftsorientierte, modulare, integrierte und zukunftsfähige Lösungen für Identity Governance, Zugriffsverwaltung und Verwaltung privilegierter Konten.

Weitere Informationen finden Sie unter OneIdentity.com

Datasheet-PrivAccessSuite4UNIX-US-KJ-DE-WL

ONE IDENTITY