DATENBLATT

Safeguard for Sudo

Erweitern und ergänzen Sie sudo durch zentrale Verwaltung

Vorteile

- Steigerung der Effizienz und Verbesserung der Richtlinieneinheitlichkeit mit der zentralen Verwaltung von sudo auf allen Ihren Unix/Linux Servern
- Verbesserung der Sicherheit durch Logging und Reporting aller sudo-Tastatureingaben
- Vereinfachung der Compliance und der Einhaltung Prüfbestimmungen durch Zugangskontrolle und Berichten zu Benutzeraktivitäten
- Optimierung der Administration durch eine zentrale komfortable Konsole für die Verwaltung von sudo, Active Directory und der Root-Delegierung im Unternehmen

Inhaltsübersicht

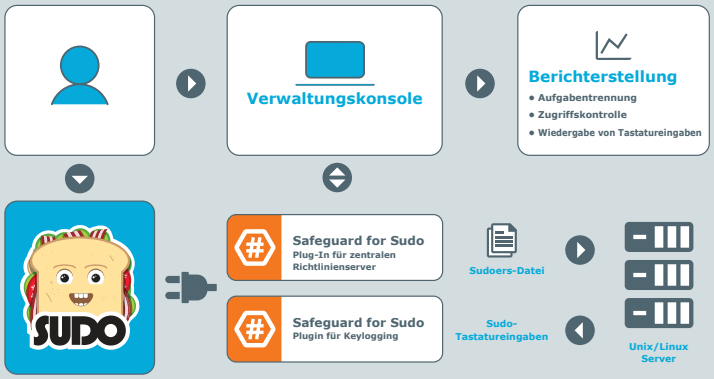
Die weitaus meisten Unix/Linux Organisationen nutzen das Open-Source-Projekt sudo für Root-Konto-Delegierungen zur Verwaltung privilegierter Konten. Sudo hat sich als wertvoll erwiesen, wobei aber seine Verwaltung mühsam sein kann. Sudo-Richtlinien sind häufig uneinheitlich geschrieben und werden auf unterschiedlichen Servern uneinheitlich ausgeführt, und sudo bietet nicht die Möglichkeit zur Überwachung der wichtigen Superuser-Zugriffe und -Aktivitäten, die für Sicherheits- und Compliance-Initiativen so entscheidend sind.

Safeguard for Sudo hilft Organisationen mit UNIX/Linux Umgebungen dabei, die Verwaltung privilegierter Konten mit sudo zu optimieren. Die Safeguard for Sudo Plug-Ins ergänzen Sudo 1.8.1 (und höher) durch einen zentralen Richtlinienserver, die zentrale Verwaltung von sudo und der sudoers-Richtliniendatei, das Reporting der sudoers-Zugriffsrechte und -Aktivitäten sowie das Keylogging aller mit sudo durchgeführten Aktivitäten.

Die Verwaltung von sudo mit Safeguard for Sudo auf einigen wenigen, Dutzenden, Hunderten oder auch Tausenden von Unix/Linux Servern ist einfach, intuitiv und einheitlich. Sie macht Schluss mit der separaten Verwaltung von sudo in jedem einzelnen System, die die Quelle von so viel Ineffizienz und Uneinheitlichkeit ist, und ermöglicht es den Organisationen, wirklich zu sehen, wer was mit sudo macht. Und weil Sudo durch Safeguard for Sudo ergänzt und nicht ersetzt wird, benötigen Endbenutzer und Administratoren keine neuen Schulungen und rufen nicht häufiger beim Helpdesk an, während die Lösung sich schneller bezahlt macht. Außerdem ermöglicht das Konzept der Zentralisierung die Erstellung von Berichten zu sudo-Aktivitäten, zur sudo-Richtlinie (sudoers) und selbst zum Änderungsverlauf von sudoers, wodurch die Zugangskontrolle und das Reporting für Prüfungen und Compliance vereinfacht wird. Und schließlich erweitert ein separates Plug-In die zentrale Administration von sudo um Keylogging mit Such- und Wiedergabefunktionen.

Verbesserung der Sicherheit und Steigerung der Effizienz

Safeguard for Sudo ergänzt sudo um Plug-Ins für einen zentralen Richtlinienserver und Keylogging und bietet damit mehr Sicherheit und Effizienz.



Funktionen und Merkmale

Erweiterung von sudo

Erweitern Sie sudo mit Plug-Ins (zentraler Richtlinienserver und Keylogging), die in das modulare System von sudo passen und es erweitern, um neue Funktionen.

Zentrale sudo-Richtlinie

Nutzen Sie einen zentralen Service für die Richtliniendurchsetzung auf allen Ihren UNIX/Linux Servern. Damit müssen Administratoren nicht mehr die Bereitstellung von sudoers auf jedem einzelnen System verwalten, was die Sicherheit verbessert und den Administrationsaufwand reduziert.

Zentrale Berichterstellung

Verfolgen Sie auf einfache Weise nach, welche und wann Änderungen an sudoers vorgenommen wurden, einschließlich Versionierung mit der Möglichkeit, zu jeder beliebigen Vorversion zurückzukehren. Sie können sehen, wer wann welche Änderungen an der Richtliniendatei für sudo vorgenommen hat, und nachverfolgen, wer in irgendeinem der verwalteten Systeme welche von sudo akzeptierten oder abgelehnten Befehle ausgeführt hat.

Keine Schulungen erforderlich

Vermeiden Sie Schulungen und minimieren Sie Helpdesk-Anrufe. Die Plug-Ins von Safeguard for Sudo erweitern die Möglichkeiten von sudo und gestatten es Benutzern ihr vorhandenen Wissen über sudo anzuwenden und eine schnellere Amortisierung zu realisieren. Bei anderen Lösungen müssen erst neue Befehle und eine neue Syntax erlernt werden, was mehr Schulungsaufwand und mehr Helpdesk-Anrufe zur Folge hat.

Keylogging

Nachverfolgung von Tastatureingaben von Administratoren, die Aktionen mit sudo durchführen. Das Keylogging-Plug-In von Safeguard for Sudo bietet eine umfassende Protokollierung von in allen Systemen durchgeführten Aktivitäten und ausgeführten Befehlen. Der Bericht lässt sich filtern, um die benötigten Daten rasch zu finden. Zum Beispiel können Sie nach bestimmten Befehlen filtern oder nach Befehlen, die während eines bestimmten Zeitraums ausgeführt wurden.

Zentrale Verwaltung

Verwenden Sie die Management Console for Unix für die Verwaltung von sudo und anderen One Identity Lösungen. Dadurch werden administrative und prüfungsbezogene Aufgaben in der gesamten UNIX Umgebung erheblich vereinfacht.

Durchsetzung der Aufgabentrennung

Mit der Management Console for Unix können Sie die Aufgabentrennung (SoD, Separation of Duty) durchsetzen und Benutzern eine bestimmte Rolle zuweisen. Auf Basis der jeweiligen Rolle sind diese dann nur zur Durchführung bestimmter Aufgaben berechtigt.

Sudo-Offline-Richtlinien-Cache

Sorgen Sie für einen unterbrechungsfreien Weiterbetrieb im Falle eines Netzwerk- oder Serverausfalls.

Skript-Kompatibilität

Stellen Sie die Kompatibilität mit vorhandenen Skript-Dateien mit eingebetteten sudo-Befehlen sicher. Andere Lösungen für die Verwaltung privilegierter Zugriffe verwenden andere Befehle und eine andere Syntax, weshalb vorhandene Skripts nicht laufen und potenziell hohe Kosten für das Testen und Nachbearbeiten von Skripts für verschiedene Unix Systeme entstehen.

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

Schutz für privilegierte Sitzungen

Reduzieren Sie Ihr Risiko durch die Kontrolle, Überwachung und Aufzeichnung von privilegierten Zugriffen

Vorteile

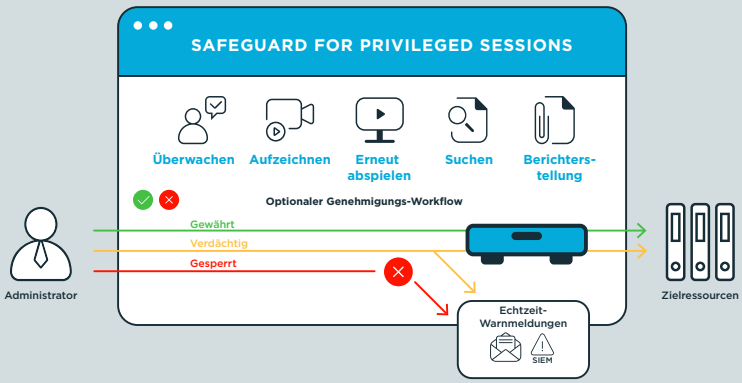
- Mindert das Risiko von Sicherheitsverstößen durch kontrollierten Zugriff auf sensible IT-Bestände
- Einfache Erfüllung von Compliance-Anforderungen für die Überwachung privilegierter Zugriffe
- Schnellere Erzielung des Mehrwerts dank vereinfachter Bereitstellung und Verwaltung
- Zufriedene Administratoren dank ermöglichter Verwendung bekannter Tools zur Systemverwaltung
- Maximale Produktivität dank schneller Lernkurve und elegantem Benutzeroberflächendesign
- Weniger Aufwand für Überwachungsberichte dank schnellem Zugriff auf alle benötigten Informationen
- Verfolgung des Zugriffs auf jede beliebige Systemart dank Host-unabhängiger Gestaltung ohne Agent
- Beschleunigte Reaktion auf Vorfälle dank schneller Volltextsuche in aufgezeichneten Sitzungen

Einleitung

Das Gewähren von unkontrolliertem privilegierten Zugriff für interne Administratoren, Drittanbieter, Auftragnehmer und Dienstanbieter kann ein enormes Risiko bergen. Denn damit öffnen Sie die Tür für Angreifer, die privilegierte Konten an sich reißen, und kriminelle Administratoren. Die unerfreulichen – und teuren – Auswirkungen dieser Art von Risiko haben kürzliche und weit bekannt gemachte Vorfälle immer wieder gezeigt. Für echte Sicherheit und Compliance müssen Sie mehr tun, als nur den Zugriff auf Konten privilegierter Benutzer zu kontrollieren. Sie müssen überwachen und aufzeichnen, was diese mit ihrem privilegierten Zugriff anstellen.

Mit One Identity Safeguard for Privileged Sessions von Quest können Sie privilegierte Sitzungen von Administratoren, Anbietern an einem anderen Standort und anderen Benutzern mit hohem Gefahrenpotential steuern, überwachen und aufzeichnen. Der Inhalt der aufgezeichneten Sitzungen wird zur vereinfachten Suche nach Ereignissen indexiert. Dies hilft auch bei der automatischen Berichterstellung, damit Sie Ihre Prüfungs- und Compliance-Anforderungen einfach erfüllen können.

Safeguard for Privileged Sessions dient außerdem als Proxy, das den Protokollverkehr auf Anwendungsebene untersucht. Dies sorgt für effektiven Schutz gegen Angriffe durch Ablehnung jeglichen Verkehrs, der gegen das Protokoll verstößt. Im Transparentmodus sind nur minimale Änderungen an Ihrem Netzwerk erforderlich und Benutzer müssen ihren aktuellen Workflow und Client-Anwendungen nicht ändern, wodurch die Implementierung zum Kinderspiel wird. Allerdings können Workflow-Regeln strenger konfiguriert werden, sodass beispielsweise eine vorherige Autorisierung durch den Benutzer erforderlich ist, wodurch der Zugriff auf bestimmte Ressourcen eingeschränkt wird, oder Warnmeldungen eingehen, wenn eine Verbindung die voreingestellte Zeitbegrenzung überschreitet. Zudem kann Safeguard Sitzungen in Echtzeit überwachen und verschiedene Aktionen ausführen: Wenn ein risikobehafteter Befehl oder Anwendung erscheint, kann Ihnen One Identity Safeguard eine Warnmeldung senden oder die Sitzung umgehend beenden.



Aufzeichnung und Überwachung aller privilegierten Zugriffe

Dank Volltextsuche sowie Warnmeldungen und Sperrung in Echtzeit verringert Safeguard Ihr Risiko bei gleichzeitig einfacherer Erfüllung von Compliance-Anforderungen.

Schutz für privilegierte Sitzungen

Reduzieren Sie Ihr Risiko durch die Kontrolle, Überwachung und Aufzeichnung von privilegierten Zugriffen

Vorteile

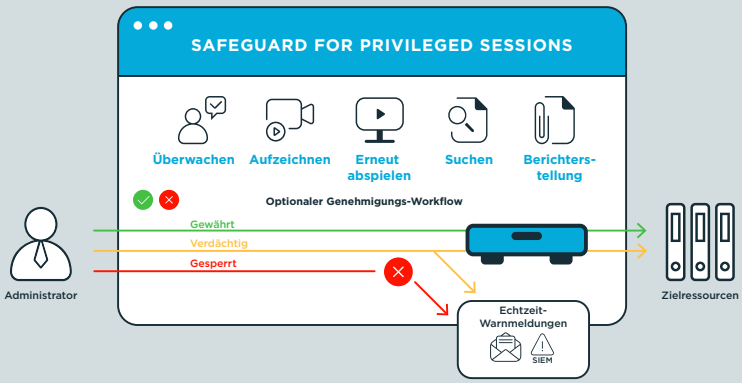
- Mindert das Risiko von Sicherheitsverstößen durch kontrollierten Zugriff auf sensible IT-Bestände
- Einfache Erfüllung von Compliance-Anforderungen für die Überwachung privilegierter Zugriffe
- Schnellere Erzielung des Mehrwerts dank vereinfachter Bereitstellung und Verwaltung
- Zufriedene Administratoren dank ermöglichter Verwendung bekannter Tools zur Systemverwaltung
- Maximale Produktivität dank schneller Lernkurve und elegantem Benutzeroberflächendesign
- Weniger Aufwand für Überwachungsberichte dank schnellem Zugriff auf alle benötigten Informationen
- Verfolgung des Zugriffs auf jede beliebige Systemart dank Host-unabhängiger Gestaltung ohne Agent
- Beschleunigte Reaktion auf Vorfälle dank schneller Volltextsuche in aufgezeichneten Sitzungen

Einleitung

Das Gewähren von unkontrolliertem privilegierten Zugriff für interne Administratoren, Drittanbieter, Auftragnehmer und Dienstanbieter kann ein enormes Risiko bergen. Denn damit öffnen Sie die Tür für Angreifer, die privilegierte Konten an sich reißen, und kriminelle Administratoren. Die unerfreulichen – und teuren – Auswirkungen dieser Art von Risiko haben kürzliche und weit bekannt gemachte Vorfälle immer wieder gezeigt. Für echte Sicherheit und Compliance müssen Sie mehr tun, als nur den Zugriff auf Konten privilegierter Benutzer zu kontrollieren. Sie müssen überwachen und aufzeichnen, was diese mit ihrem privilegierten Zugriff anstellen.

Mit One Identity Safeguard for Privileged Sessions von Quest können Sie privilegierte Sitzungen von Administratoren, Anbietern an einem anderen Standort und anderen Benutzern mit hohem Gefahrenpotential steuern, überwachen und aufzeichnen. Der Inhalt der aufgezeichneten Sitzungen wird zur vereinfachten Suche nach Ereignissen indexiert. Dies hilft auch bei der automatischen Berichterstellung, damit Sie Ihre Prüfungs- und Compliance-Anforderungen einfach erfüllen können.

Safeguard for Privileged Sessions dient außerdem als Proxy, das den Protokollverkehr auf Anwendungsebene untersucht. Dies sorgt für effektiven Schutz gegen Angriffe durch Ablehnung jeglichen Verkehrs, der gegen das Protokoll verstößt. Im Transparentmodus sind nur minimale Änderungen an Ihrem Netzwerk erforderlich und Benutzer müssen ihren aktuellen Workflow und Client-Anwendungen nicht ändern, wodurch die Implementierung zum Kinderspiel wird. Allerdings können Workflow-Regeln strenger konfiguriert werden, sodass beispielsweise eine vorherige Autorisierung durch den Benutzer erforderlich ist, wodurch der Zugriff auf bestimmte Ressourcen eingeschränkt wird, oder Warnmeldungen eingehen, wenn eine Verbindung die voreingestellte Zeitbegrenzung überschreitet. Zudem kann Safeguard Sitzungen in Echtzeit überwachen und verschiedene Aktionen ausführen: Wenn ein risikobehafteter Befehl oder Anwendung erscheint, kann Ihnen One Identity Safeguard eine Warnmeldung senden oder die Sitzung umgehend beenden.



Aufzeichnung und Überwachung aller privilegierten Zugriffe

Dank Volltextsuche sowie Warnmeldungen und Sperrung in Echtzeit verringert Safeguard Ihr Risiko bei gleichzeitig einfacherer Erfüllung von Compliance-Anforderungen.