DATENBLATT

Safeguard for Privileged Sessions

Risikoverringerung durch Steuerung, Überwachung und Aufzeichnung privilegierter Zugriffe

Vorteile

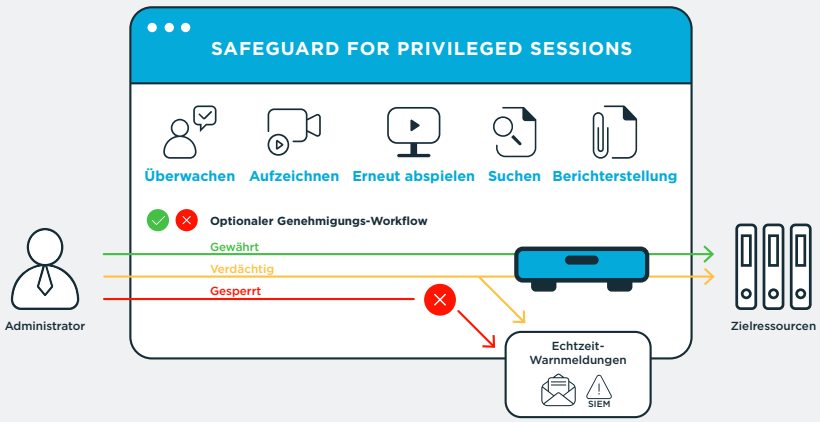
- Mindert das Risiko von Sicherheitsverstößen durch kontrollierten Zugriff auf sensible IT-Bestände
- Einfache Erfüllung von Compliance-Anforderungen für die Überwachung privilegierter Zugriffe
- Schnellere Erzielung des Mehrwerts dank vereinfachter Bereitstellung und Verwaltung
- Zufriedene Administratoren 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

Einführung

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 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.

Funktionen und Merkmale

Prüfung, Aufzeichnung und Wiedergabe der vollständigen Sitzung

Sämtliche Aktivitäten während einer Sitzung werden bis hin zum einzelnen Tastenanschlag, Mausbewegungen und angezeigten Fenstern erfasst, indexiert und in manipulationssicheren Audit Trails gespeichert, die wie ein Video angezeigt und wie eine Datenbank durchsucht werden können. Sicherheitsteams können Sitzungen nach bestimmten Ereignissen durchsuchen und die Aufzeichnung von genau dem Punkt abspielen, wo die Suchkriterien erfüllt sind. Audit Trails sind zu Forensik- und Compliance-Zwecken verschlüsselt, zeitgestempelt und kryptografisch signiert.

Warnmeldungen und Sperrung in Echtzeit

Verkehr wird in Echtzeit überwacht und verschiedene Aktionen ausgeführt, 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 das Ereignis protokollieren, eine Warnmeldung senden oder die Sitzung umgehend beenden.

Zwei Bedienmodi

Wählen Sie, welcher Modus auf Ihre Bedürfnisse zugeschnitten ist.

- **Workflow-Engine:** Eine Workflow-Engine, die Zeitbeschränkungen, mehrere Genehmigungsberechtigte, Prüfer, Notzugriff und Ablaufdaten für Richtlinien unterstützt. Sie bietet zudem die Möglichkeit, Ursachencodes einzugeben bzw. direkt in Ticketsysteme zu integrieren. Die Kennwortanforderungen können entweder automatisch oder manuell genehmigt werden. Für die manuelle Genehmigung können Sie beliebige Genehmigungsstufen definieren.
- **Instant On**: Nehmen Sie die Bereitstellung im Transparentmodus vor, sodass keine Änderungen am Workflow von Benutzern erforderlich sind. Es kann auch als Proxy-Gateway genutzt werden, das wie ein Router im Netzwerk funktioniert – für Benutzer und Server unsichtbar. Administratoren können bekannte Client-Anwendungen weiter nutzen und ohne Unterbrechung ihrer täglichen Routine auf Zielserver sowie Systeme zugreifen.

Proxyzugriff

Da Benutzer keinen direkten Zugriff auf Ressourcen haben, ist das Unternehmen gegen unbefugten und uneingeschränkten Zugriff auf sensible Daten und Systeme geschützt. Safeguard for Privileged Sessions kann Proxyverbindungen zu verschiedenen Zielressourcen herstellen und aufzeichnen, so unter anderem zu UNIX/Linux, Windows, Netzwerkgeräten, Firewalls und Routern.

Befehls- und Anwendungssteuerung

Safeguard for Privileged Sessions unterstützt das Erstellen sowohl von schwarzen als auch von weißen Listen für Befehle und Fenstertitel.

Personalisiertes Arbeiten

Selbst bei aktiviertem Workflow können Administratoren beim Zugriff auf privilegierte Sitzungen ihren Client sowie ihre Tools und Präferenzen wählen. Auf diese Weise entsteht eine nahtlose Lösung, die Administratoren den benötigten Zugriff liefert und gleichzeitig Compliance- und Sicherheitsvorschriften erfüllt.

Volltextsuche

Mit der Optical Character Recognition (OCR, Zeichenerkennung) Engine können Prüfer Volltextsuchen sowohl für Befehle als auch beliebige Texte vornehmen, die vom Benutzer im Inhalt der Sitzung gesehen werden. 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.

Automatische Anmeldung

Mit der Kennwortübernahmefunktion kann der Zugriff für automatische Anmeldung konfiguriert werden. Dadurch werden Sicherheit und Compliance verbessert, da der Benutzer das Kennwort nie zu sehen bekommt.

Unterstützung zahlreicher Protokolle

Vollständige Unterstützung von SSH-, Telnet-, RDP-, HTTP(s)-, ICA- und VNC-Protokollen. Zusätzlich können Sicherheitsteams entscheiden, welche Netzwerkdienste (z. B. Dateiübertragung, Shell-Zugriff usw.) innerhalb der Protokolle sie für Administratoren aktivieren/deaktivieren möchten.

Instant off

Indem sich One Identity Safeguard wie eine virtuelle Firewall verhält, erhöht das Programm den Schutz Ihrer Server durch beinahe umgehendes Beenden fragwürdiger oder boshafter Zugriffe. Um versehentliche Fehlkonfigurationen und andere menschliche Fehler zu vermeiden, unterstützt die Lösung außerdem das Vier-Augen-Prinzip bei der Autorisierung, sodass der überwachende Administrator die Sitzung jederzeit beenden kann.

Eingeschobene Bereitstellung

Dank der raschen Appliance-basierten Bereitstellung und vereinfachtem Rerouting des Verkehrs können Sie mit One Identity Safeguard Sitzungen in einigen Tagen aufzeichnen, ohne Ihre Benutzer zu stören.

Analysebereit

Sammeln Sie alle nötigen Informationen, um privilegierte Benutzer und deren Verhalten zu analysieren und interne sowie externe Bedrohungen zu erkennen.

Sicherer Zugriff auf ältere Systeme

Der sichere Zugriff auf Systeme lässt sich über Smartcards, Zwei-Faktor-Authentifizierung oder andere starke Authentifizierungsmethoden absichern. Da Safeguard als Proxy-Gateway für das System fungiert, wird eine strenge Authentifizierung für Ziele ermöglicht, die diese Methoden nicht systemintern unterstützen.

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. Mit unserer privilegierten Lösung für sichere Kennwörter und privilegierten Analysefunktionen können Sie auf der leistungsstarken Funktion der Sitzungsverwaltung von Safeguard for Privileged Sessions aufbauen. In unserem Produktangebot finden Sie Produkte 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 unterstützt Unternehmen bei der erfolgreichen Umsetzung von Identitäts- und Zugriffsmanagement (IAM). Mit unserem einzigartigen Portfolio an Lösungen für Identity Governance, Zugriffsverwaltung, Verwaltung privilegierter Konten und Identity-as-a-Service-Lösungen können Organisationen ihr volles Potenzial entwickeln, ohne Einschränkung durch Sicherheit, und profitieren dabei vom Schutz vor Bedrohungen. Weitere Informationen finden Sie unter OneIdentity.com.

Datasheet_2018_OISafeguard-PrivSessions_US_RS_34966