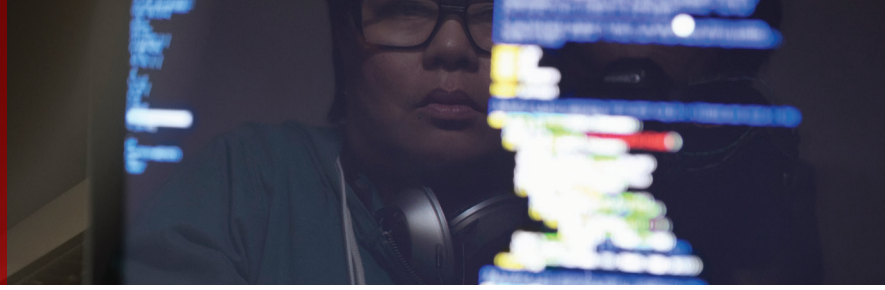

Centrify Audit and Monitoring Service

Schützen Sie Ihre Umgebung mit einem hohen Maß an Absicherung

Bei privilegierten Sitzungen ist es natürlich am besten, alles zu überprüfen. Dank der Dokumentation aller durchgeführten Aktionen können Audit-Protokolle nicht nur für forensische Analysen zum Erkennen des genauen Problems verwendet werden, sondern auch dazu, die durchgeführten Aktionen einem bestimmten Benutzer zuzuordnen. Da diese Sitzungen derart kritisch sind, hat es sich auch bewährt, sie per Video aufzuzeichnen. Dieses kann anschließend geprüft oder als Nachweis für Ihre kritischsten Wirtschaftsgüter oder in stark regulierten Branchen verwendet werden. Es gibt zahlreiche Bestimmungen, einschließlich PCI-DSS für Zahlungskartendaten, die diese Prüfungsstandards ausdrücklich verlangen. Wenn Sie über eine Sicherheitsabteilung verfügen, bietet es sich an, diese Audit-Daten in ihr bestehendes SIEM-System (Security Information and Event Management) zu integrieren, um so automatisch riskante Aktivitäten zu erkennen und Warnungen auszugeben.

Alles prüfen

Branchenanalysten und Aufsichtsbehörden sind sich einig, dass heutzutage die Ursache Nr. 1 für Sicherheitsverletzungen der Missbrauch privilegierter Zugangsdaten ist. Privilegierte Zugangsdaten sind der „Schlüssel zum Königreich" und ermöglichen einen uneingeschränkten „Rundgang" durch die gesamte Infrastruktur. Ein einzelner kompromittierter privilegierter Zugriffscode reicht aus, um einen Millionenschaden anzurichten. Deshalb legen interne Prüfer und Aufsichtsbehörden spezifische Kontrollen und Berichterstattungsanforderungen bezüglich der Nutzung dieser Zugangsdaten fest.

Auch kleine und mittlere Organisationen müssen eine Vielzahl von Branchenstandards und gesetzlichen Vorschriften einhalten, was besondere Herausforderungen bei der Erfassung, Zusammenführung und Bestätigung von privilegierten Zugriffen mit sich bringt.

Häufig haben Organisationen keinen kontinuierlichen Überblick über ihre Konformität, was dazu führt, dass Audits und Zertifizierungen zu enormem Stress führen, bei dem der Arbeitsaufwand für interne Prüfer und Compliance-Mitarbeiter kurzfristig durch die Decke geht.

Nicht selten werden deshalb nur Stichproben entnommen und lediglich ein Teil bestimmter Kontrollen durchgeführt, sodass in Bezug auf Konformität und Sicherheit zahlreiche blinde Flecken bleiben. Im Allgemeinen macht sich das Einholen von Antworten von einer großen Anzahl an Interessenvertretern und das Auswerten verschiedenster Datensätze hinsichtlich Effizienz und Genauigkeit bemerkbar.

Mit Blick auf die Sicherheit ist es wichtig, spezifische und detaillierte Informationen zu verdächtigen Aktivitäten im Rahmen privilegierter Sitzungen zu erhalten. Sicherheitsmanager können unmittelbar Gegenmaßnahmen ergreifen, um potenzielle Risiken oder gerade stattfindende Angriffe direkt vom Warnungsbildschirm aus abzuwehren. Darüber hinaus können sie eine Sitzung aufgrund ihres Risikos sowohl manuell als auch automatisch beenden.

In jüngster Vergangenheit wurden öffentlich bekannt gewordene Datenschutzverletzungen durch Insider ermöglicht, die Backdoor-Benutzerkonten erstellten, durch die traditionelle Passworttresore umgangen werden konnten. Darüber hinaus finden privilegierte Benutzer häufig Möglichkeiten, den Passworttresor in ihrer Arbeitsumgebung zu umgehen, um sich so ihre tägliche Arbeit zu erleichtern. Bei dieser Art des betrügerischen Zugriffs werden oft lokal auf Servern gespeicherte SSH-Schlüssel genutzt, was die Angriffsfläche einer Organisation vergrößert und das Risiko einer Sicherheitsverletzung erhöht.

Schützen Sie Ihre Umgebung mit einem hohen Maß an Absicherung

Der Centrify Audit and Monitoring Service bietet Kunden die Möglichkeit, ihre Compliance-Pflichten mithilfe von Audits und Berichten zu erfüllen und gleichzeitig alle risikobehafteten Arbeitsabläufe durch das Einrichten einer hostbasierten Überwachung stillzulegen. Der Dienst unterstützt Sie beim Aufzeichnen aller privilegierten Sitzungen und Metadaten und ordnet Aktivitäten bestimmten Personen zu, sodass ein umfassendes Bild ihrer Ziele und Erfolge entsteht.

SITZUNGSAUFZEICHNUNG UND AUDIT

Zeichnen Sie eine ganzheitliche Sicht privilegierter Aktivitäten auf Windows- und Linux-Servern, IaaS und Datenbanken auf und verwalten Sie diese Aufzeichnungen. So erhalten Sie eine zentrale Quelle für Nachweise in Bezug auf individuelle und gemeinsam genutzte Benutzerkonten. Weisen Sie Ihre Konformität mithilfe von Berichten zu den Zugriffsrechten und zugehörigen Aktivitäten aller Benutzer nach.

GATEWAY-SITZUNGSÜBERWACHUNG UND -KONTROLLE

Erreichen Sie ein neues Maß an Überblick über privilegierte Sitzungen auf kritischer Infrastruktur. Administratoren beobachten die Aktivitäten im Rahmen von Remote-Sitzungen in Echtzeit und haben die Möglichkeit, verdächtige Sitzungen über das Centrify Admin Portal umgehend zu beenden.

HOSTBASIERTE AUDITS, AUFZEICHNUNGEN UND BERICHTE ZU SITZUNGEN

Stellen Sie mithilfe der hostbasierten Audit-Funktion sicher, dass Sitzungsaufzeichnungen nicht umgangen werden können. Entdecken Sie betrügerische Aktivitäten wie die Erstellung und Installation von SSH-Schlüsselpaaren, mit denen Ihre Sicherheitskontrollen leicht umgangen werden könnten, und ordnen Sie diese Aktivitäten dem jeweiligen Benutzer zu. Überprüfen Sie alle Aktivitäten in privilegierten Sitzungen auf Prozessebene mit forensischer Genauigkeit, um Sicherheitsprüfungen durchzuführen, Gegenmaßnahmen zu ergreifen sowie zur Einhaltung der Konformität und zur Verhinderung von Manipulationen.

> **„Es gibt keine Verordnung, bei deren Einhaltung uns Centrify noch nicht geholfen hat. Heute wird jeder Zugriff eines Administrators auf einen Server aufgezeichnet. Ich kann einen Bericht abrufen, ihn auszudrucken und ihn dem Prüfer übergeben."**
>
> — Peter Manina, IT-Spezialist und UNIX Systemarchitekt, State of Michigan Department of Technology, Management and Budget

Sitzungsaufzeichnung und Audits für privilegierte Zugriffe

Erfassen und prüfen Sie privilegierte Sitzungen, die gemeinsam genutzte ebenso wie individuelle Benutzerkonten verwenden, per umfassender Video- und Metadatenerfassung. Der Centrify Audit and Monitoring Service bietet Kunden die Möglichkeit, forensische Analysen durchzuführen und Hi-Fi-Aufzeichnungen für Audits und zur Einhaltung der Konformität zu nutzen.

- Erfassen und sammeln Sie Daten in Hi-Fi-Aufzeichnungen aller privilegierten Sitzungen auf Gateway-Ebene. Der Centrify Audit and Monitoring Service speichert Sitzungen in einer leicht zu durchsuchenden SQL-Serverdatenbank, die einen ganzheitlichen Überblick darüber ermöglicht, was wirklich passiert ist. Die durchsuchbare Playback-Funktion des Dienstes bietet IT-Sicherheitsmanagern und Prüfern die Möglichkeit, einen genauen Blick auf die Aktivitäten von Benutzern und deren Auswirkungen zu werfen, sodass Sie den Missbrauch privilegierter Zugriffsrechte oder die Ursache eines Sicherheitsvorfalls ermitteln können.
- Zeichnen Sie alle privilegierten Sitzungen und Metadaten auf. So können Sie sämtliche Aktivitäten bestimmten Personen zuordnen und erhalten ein umfassendes Bild ihrer Ziele und Erfolge.
- Weisen Sie nach, dass Sicherheitskontrollen vorhanden sind und wie vorgesehen funktionieren und dass Sie die gesetzlichen Anforderungen erfüllen. Finden Sie Sitzungsaufzeichnungen mittels Suche nach Servern, Benutzern oder mit individuellen Suchkriterien. Sie finden problemlos alle Sitzungen eines bestimmten Benutzers oder auf einem bestimmten Server oder können Sitzungen auf Grundlage einer Reihe von individuell gewählten Filterkriterien suchen. Dies erleichtert nicht nur forensische Untersuchungen, gleichzeitig können Sie auch proaktiv Bedrohungen durch Insider oder verdächtige Aktivitäten erkennen.
- Erhalten Sie einen umfassenden Überblick mit einheitlichen Zugriffs- und Aktivitätsberichten auf einer gemeinsamen Plattform. Individuell anpassbare und vordefinierte Abfragen sowie gebrauchsfertige Berichte zur Einhaltung von SOX- und PCI-Anforderungen bieten Informationen zu Kontrollen beim Zugriff auf privilegierte Benutzerkonten, Passwortprüfungen und privilegierten Sitzungen unter Windows, Linux und UNIX.

Privilegierte Sitzung auf IaaS und auf internen Systemen überwachen und kontrollieren

Machen Sie sich eine gemeinsame Audit-Infrastruktur zunutze, um privilegierte Aktivitäten in Ihrer Infrastruktur zu erfassen und aufzuzeichnen – egal, ob diese auf fest installierten Geräten oder in der Cloud ablaufen. Erkennen Sie verdächtige Benutzeraktivitäten, um in Echtzeit vor möglicherweise gerade stattfindenden Angriffen gewarnt zu werden. Der Centrify Audit and Monitoring Service bietet Ihnen die Möglichkeit, privilegierte Sitzungen, die gemeinsam genutzte ebenso wie individuelle Benutzerkonten verwenden, zu überwachen und zu kontrollieren.

- Erreichen Sie ein neues Maß an Überblick über privilegierte Sitzungen auf kritischer Infrastruktur. Administratoren beobachten die Aktivitäten im Rahmen von Remote-Sitzungen in Echtzeit und haben die Möglichkeit, verdächtige Sitzungen über das Centrify Admin Portal umgehend zu beenden. Dieses Vier-Augen-Prinzip bietet Administratoren die Möglichkeit, die Aktivitäten eines Remote-Mitarbeiters oder ausgelagerter IT-Aufgaben zu überwachen, indem sie sich in die gerade stattfindenden Sitzungen live einwählen. Sie können jede Aktion eines privilegierten Benutzers beobachten oder die Sitzung beenden, wenn eine Aktivität verdächtig erscheint.
- Privilegierte Zugriffsdaten werden erfasst und gespeichert, um eine solide Abfrage mithilfe von Protokollmanagement-Tools und der Integration von externen Berichterstattungs-Tools zu ermöglichen. Eine optimierte Integration von SIEM und Warn-Tools wie Micro Focus® ArcSight™, IBM® QRadar™ und Splunk® ermöglicht ein schnelles Erkennen von Risiken und verdächtigen Aktivitäten.

Mithilfe hostbasierter Sitzungs-Audits, -Aufzeichnungen und -Berichte vermeiden, dass privilegierte Zugriffsdaten gefälscht oder umgangen werden

Durch einen Ansatz, bei dem die Audits, Aufzeichnungen und Berichte vom Host erzwungen werden, wird schlussendlich eine bessere Kontrolle des privilegierten Zugriffs in Ihrer Umgebung erreicht. Der Centrify Audit and Monitoring Service erweitert seine gatewaybasierten Funktionen mit einem hostbasierten Ansatz, der sicherstellt, dass Ihre privilegierten Zugriffskontrollen nicht umgangen werden, wie dies möglich wäre, wenn Sie ausschließlich einen Passwort-/Geheimnistresor verwenden würden.

- Erfassen und sammeln Sie Daten mittels Hi-Fi-Aufzeichnungen aller privilegierten Sitzungen auf allen Servern ihrer lokalen und cloudbasierten Infrastruktur. Speichern Sie Sitzungen in einer leicht zu durchsuchenden SQL-Serverdatenbank und erhalten Sie so einen ganzheitlichen Überblick darüber, was genau ein bestimmter oder auch alle Benutzer auf Ihren Systemen wann genau gemacht haben.
- Die hostbasierten Audit-, Aufzeichnungs- und Berichtfunktionen von Centrify für Sitzungen ermöglichen eine fortschrittliche Überwachung auf Prozessebene mit Shell-basiertem Auditing, um verdächtige Änderungen an Anwendungen zu erkennen.
- Das Centrify File Integrity Monitoring erkennt Änderungen an Konfigurationen und kritischen Dateien in Echtzeit und bietet so die Möglichkeit, Sicherheitswarnungen im SIEM-System einer Organisation auszulösen, um vor dem Erstellen einer Hintertür oder dem Umgehen eines Passworttresors zu warnen.
- Eine durchsuchbare Playback-Funktion bietet IT-Sicherheitsmanagern und Prüfern die Möglichkeit, einen genauen Blick auf die Aktivitäten der Benutzer zu werfen, den Missbrauch von privilegierten Zugriffsrechten oder die Ursache eines Sicherheitsvorfalls zu erkennen.
- Erstellen Sie Berichte zu Zugriffen, Checkouts, Sitzungen und zur Nutzung privilegierter Zugriffsdaten auf Windows, Linux, UNIX und der Netzwerkinfrastruktur.
- Optimierte Integration mit SIEM, Warn- und Berichterstattungs-Tools.

Unsere Mission besteht darin, die Hauptursache für Sicherheitsverletzungen – den Missbrauch privilegierter Zugriffsrechte – zu stoppen. Centrify ermöglicht es seinen Kunden mit einem Cloud-fähigen „Zero Trust Privilege"-Ansatz, den Zugang zu Infrastruktur, DevOps, Cloud, Containern, Big Data und anderen Angriffsflächen in modernen Unternehmen zu sichern. Weitere Informationen erhalten Sie unter www.centrify.com.

Hauptsitz (USA) +1 (669) 444 5200
Europa, Naher Osten und Afrika (EMEA)
+44 (0) 1344 317950
Asien/Pazifik +61 1300 795 789
Brasilien +55 11 3958 4876
Lateinamerika +1 305 900 5354
sales@centrify.com

www.centrify.com