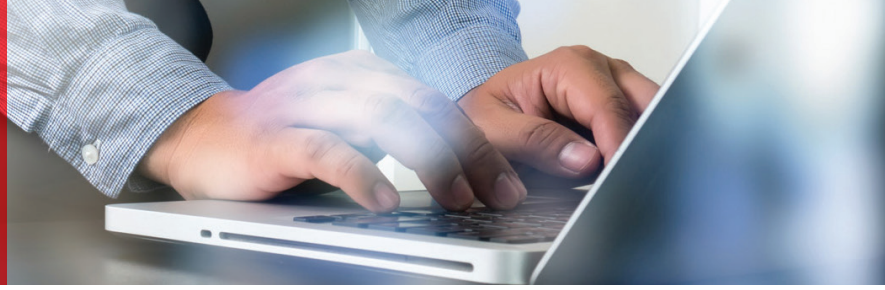

Centrify Authentication Service

Konsolidierung von Identitäten zur Verkleinerung der Angriffsfläche

Die heutige Gefahrenlandschaft unterscheidet sich grundlegend von der in der Vergangenheit, in der Menschen auf Infrastruktur, Datenbanken und Netzwerkgeräte einer Organisation zugriffen, die sich alle innerhalb eines klar abgegrenzten Bereichs befanden. Heute muss das Privileged Access Management (PAM) nicht nur Anfragen von Menschen verarbeiten, sondern auch solche von Maschinen, Diensten und APIs. Zwar gibt es immer noch gemeinsame Konten, im Hinblick auf eine verbesserte Sicherheit hat sich jedoch die Verwendung einzelner Identitäten durchgesetzt, denen geringstmögliche Berechtigungen zugeteilt werden können. Um in einer zunehmend heterogenen und verteilten Umgebung Angriffe von innen und Advanced Persistent Threats (APTs) zu verhindern sowie Branchenvorschriften und gesetzliche Bestimmungen wie PCI DSS oder SOX einzuhalten, benötigen IT-Organisationen eine Cloud-fähige „Zero Trust Privilege"-Lösung, die von zentraler Stelle aus den Überblick und die Kontrolle über Identitäten sowie die Verwaltung von privilegierten Zugriffsrechten und Aktivitäten ermöglicht.

Das herkömmliche PAM reicht für die Gefahrenlandschaft von heute nicht mehr aus

Das bisher verwendete Privileged Access Management (PAM) ist bereits seit Jahrzehnten im Einsatz und wurde zu einer Zeit entwickelt, als der gesamte privilegierte Zugriff auf Systeme und Ressourcen innerhalb desselben Netzwerks einer Organisation stattfand. In dieser Umgebung hatten System-Administratoren ein gemeinsames Root-Konto, das sie mittels eines Passworttresors auschecken konnten, meist, um auf Server, Datenbanken oder Netzwerkgeräte zuzugreifen. Diese Form des PAM hat seinen Zweck erfüllt.

Das heutige Umfeld ist jedoch nicht nur anders als früher – Cyberangreifer nutzen heute zudem kompromittierte privilegierte Zugriffsdaten zur Durchführung ihrer Angriffe. Unternehmen müssen daher lokale und gemeinsam genutzte Benutzerkonten mit statischen Anmeldedaten auf ihren Systemen abschaffen und stattdessen übergreifende, individuelle Benutzerkonten mit temporären Zugriffs-Tokens verwenden, um ihre Angriffsfläche zu verkleinern und so ihre Sicherheit zu verbessern. Gleichzeitig verlangen Branchenstandards und gesetzliche Vorschriften wie NIST 800-63 und PCI DSS nun erstmals Sicherheitskontrollen, die eine höhere Absicherung aufweisen, als dies mit Tresoren möglich ist.

Mehr als nur Erkennung und Sicherung von Passwörtern

Der Centrify Authentication Service gibt Kunden die erforderlichen Funktionen an die Hand, um mehr als nur Tresore zu erstellen, indem er es ermöglicht, genau zu überprüfen, wer privilegierte Zugriffsdaten anfordert. Dies lässt sich durch die Nutzung von Identitäten aus Unternehmensverzeichnissen, die Abschaffung lokaler Konten sowie die Verringerung der Gesamtanzahl von Benutzerkonten und Passwörtern erreichen, womit insgesamt die Angriffsfläche verkleinert wird.

VERZEICHNISÜBERGREIFENDES BROKERING

Vereinfachen Sie die Benutzerauthentifizierung auf Servern von sämtlichen Verzeichnisdiensten aus, einschließlich Active Directory, LDAP und Cloud-Verzeichnissen. Organisationen können die Vorteile der Cloud nutzen, ohne dabei neue isolierte Identitätsverzeichnisse oder komplexe Synchronisierungsmechanismen zu erstellen.

ZONEN-TECHNOLOGIE VON CENTRIFY

Fassen Sie komplexe und uneinheitliche UNIX- und Linux-Benutzeridentitäten mit der patentierten Zonen-Technologie von Centrify zügig in der Active Directory zusammen – ohne, dass Sie zuerst alle Benutzeridentitäten rationalisieren müssten. Centrify Zones bietet Ihnen die Möglichkeit, Benutzer, Computer, Rollen und Berechtigungen in einem hierarchischen Modell zu verwalten, das Sie nach Ihren Bedürfnissen gestalten können.

ACTIVE DIRECTORY BRIDGING

Sichern Sie Linux und UNIX mit denselben Identitätsdiensten, die aktuell zum Schutz des Zugriffs auf Windows-Systeme verwendet werden. Zentralisieren Sie die Verwaltung von Richtlinien und Benutzern für Linux- und UNIX-Systeme, um eine schnelle Zusammenlegung von Identitäten in der Active Directory zu ermöglichen. Sie erhalten eine umfassende Active-Directory-Integration selbst für die komplexesten Active-Directory-Architekturen.

VERWALTUNG LOKALER KONTEN UND GRUPPEN

Verwalten Sie Systembenutzerkonten genauso, wie Sie Benutzerkonten in der Active Directory verwalten würden. Sparen Sie Zeit und Geld, während Sie gleichzeitig die Produktivität Ihrer IT-Mitarbeiter steigern.

VERWALTUNG VON MASCHINENIDENTITÄTEN UND ZUGRIFFSDATEN

Verwalten Sie Maschinenidentitäten und deren Zugriffsdaten zentral in der Active Directory oder den Centrify Zero Trust Privilege Services, um eine unternehmensweite Vertrauensbasis für die Authentifizierung von maschinenübergreifenden Interaktionen auf Grundlage eines zentralen Vertrauensmodells zu errichten.

VERWALTUNG VON GRUPPENRICHTLINIEN

Verwalten Sie die Authentifizierung, Zugriffskontrollen und Gruppenrichtlinien bei Systemen, die nicht mit Windows arbeiten, genauso wie bei Windows-basierten. Nutzen Sie die Active-Directory-Gruppenrichtlinie, um die Firewall- und SSH-Konfiguration zu automatisieren, um zu entscheiden, welche Benutzer sich mit den einzelnen Systemen verbinden können, um inaktive Sitzungen zu beenden und für eine netzwerkbasierte Authentifizierung.

MFA BEI SYSTEM-ANMELDUNG

Die Anmeldung bei privilegierten Systemen ist häufig die wichtigste Angriffsschnittstelle, die vor Cyberangreifern geschützt werden muss, welche Informationen stehlen oder Schaden in der Umgebung anrichten wollen. Durch eine Multi-Faktor-Authentifizierung (MFA) bei der Anmeldung auf Linux-, UNIX- und Windows-Servers wird das Risiko eines Angriffs verringert und es werden strenge gesetzliche Vorschriften wie PCI DSS und NIST 800-63A eingehalten. Mit Centrify gehen Sie über eine MFA bei Serveranmeldung hinaus und wenden MFA überall an.

Vereinfachte Verlagerung von Arbeitspensen in die Cloud mithilfe von verzeichnisübergreifendem Brokering

Vereinfachen Sie die Benutzerauthentifizierung auf Servern aus sämtlichen Verzeichnisdiensten, einschließlich Active Directory, LDAP oder Cloud-Verzeichnissen wie dem von Google. Unternehmen können sich die Vorteile der Cloud zunutze machen, ohne dabei neue Identitätsspeicher zu schaffen, Identitätsverzeichnisse zu vervielfältigen oder die Sicherheit von privilegierten und lokalen Unternehmenszugriffen einzuschränken. Darüber hinaus sparen IT-Manager Zeit bei der Verwaltung einer heterogenen IT-Umgebung, wodurch sich dramatische Kosteneinsparungen für die Organisation erreichen lassen.

- Authentifizieren Sie sich für privilegierte Ressourcen über sämtliche Verzeichnisdienste – sowohl mit lokalen Geräten als auch in der Cloud.
- Ermöglichen Sie eine zentrale Authentifizierung und Zugriffskontrollen in einer räumlich verteilten Infrastruktur und nutzen Sie dabei Identitäten aus einer oder mehreren Active-Directory-Umgebungen, LDAP- oder Cloud-Verzeichnissen wie Centrify Directory oder Google Directory.

Identitätsmanagement und -konsolidierung für Linux und UNIX mithilfe von Active Directory Bridging

Der Centrify Authentication Service bietet Kunden die Möglichkeit, ihre IT-Infrastruktur zu vereinheitlichen, indem sie ihre Identitäts-, Authentifizierungs- und Zugriffsverwaltung für Linux und UNIX in der Microsoft Active Directory zusammenfassen. In diesem Zusammenhang war Centrify der erste Anbieter, der UNIX und Linux in die Active Directory integrierte, um mehrere Identitäten für einen einzelnen Benutzer zu ermöglichen. Im Magic Quadrant 2018 für Privileged Access Management weist Gartner speziell auf die einzigartige Expertise von Centrify in diesem Bereich hin, die sowohl für bestehende als auch für potenzielle Neukunden aufgrund ihres Potenzials zur Steigerung der IT-Produktivität, Verringerung der Wartungskosten und Verkleinerung der Angriffsfläche von großem Interesse ist.

- Verbinden Sie auf native Weise Linux- und UNIX-Systeme mit der Active Directory und verwandeln Sie das Host-System in einen Active-Directory-Client. Schützen Sie Systeme mittels derselben Authentifizierungs- und Gruppenrichtlinien-Dienste, die aktuell in Windows-Systemen implementiert sind.
- Legen Sie Benutzerprofile zusammen und setzen Sie eine klare Trennung von Aufgaben durch.
- Erweitern Sie das Gruppenrichtlinien-Management über Windows hinaus auch auf andere Systeme. Dies ist die einzige Lösung, um Benutzer- und Computerrichtlinien mit erweiterten Funktionen wie Gruppenfiltern und Loopback-Verarbeitung bereitstellen zu können. Konfigurationseinstellungen für Gruppenrichtlinien werden nahtlos in den Centrify UNIX Agent integriert, um sowohl Systemkonfigurationen als auch diejenigen der Benutzerumgebung verwalten zu können.
- Auch wenn zahlreiche Anbieter angeben, Kerberos zu unterstützen, bietet ausschließlich Centrify systemeigenen Support für die gesamte Komplexität und alle Nuancen der Active Directory.
- Umfangreiche CLI- und Scripting-Optionen erleichtern eine zeitsparende Automatisierung und unterstützen ein Application-to-Application Password Management (AAPM).

Lokale Benutzerkonten und Gruppen effizient verwalten

Mit dem Centrify Authentication Service können Kunden die Verwaltung lokaler Benutzerkonten und Gruppen in ihrer heterogenen Infrastruktur optimieren. Centrify automatisiert den Lebenszyklus lokaler Benutzerkonten und lässt sich bei Bedarf in Dienste oder Anwendungen mit Passworttresoren integrieren, um die gesamte Benutzerkonten- und Gruppenverwaltung auf einer Managementplattform zu zentralisieren.

- Verwalten Sie zentral den Lebenszyklus für Anwendungs- und Servicekonten und schützen Sie automatisch Anmeldedaten und Zugriff.
- Integrieren Sie die Passwortverwaltung für lokale Benutzerkonten mit bestehenden Passworttresoren, um die Registrierung von Benutzerkonten und die Erstellung von Passworttresoren für neue Benutzerkonten zu automatisieren.
- Zentralisieren Sie die Verwaltung lokaler Gruppen.

Verwaltung für Windows-, Linux- und UNIX-Server schnell zentralisieren

Die Zonen-Technologie von Centrify ermöglicht es Ihnen, Ihre heterogene Umgebung zu verwalten, indem Sie die Rechte, die ein Benutzer auf einem Windows-, Linux- oder UNIX-System hat, mit einer einzigen Identität verknüpfen, die in der Active Directory gespeichert und verwaltet wird.

- Richten Sie eine Hierarchie und Vererbung ein.
- Ermöglichen Sie eine schnelle Migration von UNIX-Identitäten in die Active Directory.
- Nutzen Sie Centrify Computer Roles für einzigartige Vorteile bei Verwaltung und Sicherheit.

Gruppenrichtlinien für Benutzer und heterogene Systeme durchsetzen

Centrify bietet umfassenden Support, um die Verwaltung von Gruppenrichtlinien auf Systeme auszuweiten, die nicht mit Windows arbeiten. Dies ist die einzige Lösung, um Benutzer- und Computerrichtlinien mit erweiterten Funktionen wie Gruppenfiltern und Loopback-Verarbeitung bereitstellen zu können.

- Setzen Sie Active-Directory-Gruppenrichtlinien auf Plattformen durch, die nicht mit Windows arbeiten.
- Verwalten Sie die Authentifizierung, Zugriffskontrollen und Gruppenrichtlinien für Systeme, die nicht mit Windows arbeiten.

Mit MFA bei Systemanmeldung sicherstellen, dass ausschließlich autorisierte Personen auf Ihre kritische Infrastruktur zugreifen können

Die Anmeldung an privilegierten Systemen stellt häufig die wichtigste Angriffsschnittstelle dar, die vor Cyberangreifern geschützt werden muss, die Informationen stehlen oder Schaden in der Umgebung anrichten wollen. Um sicherzustellen, dass ausschließlich autorisierte Personen auf Ihre sensiblen Systeme zugreifen, müssen Sie eine solide Authentifizierung per MFA durchsetzen. Centrify bietet eine hostbasierte Technologie, die sich nicht umgehen lässt, um ein MFA bei der Anmeldung in Systemen für Linux-, UNIX- und Windows-Server und -Workstations durchzusetzen.

- Stärken Sie Zero-Trust-Prinzipien mithilfe einer hostbasierten MFA-Erzwingung auf jedem Computer, die nicht umgangen oder übersprungen werden kann.
- Zentralisierte Integration von MFA-Diensten.
- Lokale MFA-Funktionen für UNIX und Linux.
- Nativ in den Anmeldeprozess integriertes Windows-MFA.

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