Drei wichtige Gründe für privilegiertes Identitätsmanagement (und ein überraschender Vorteil)

Ein ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Februar 2015 für
Centrify erstellt

EMA™
IT & DATENMANAGEMENT UNTERSUCHUNGEN, BRANCHENANALYSEN & CONSULTING

Inhaltsverzeichnis

Kurzfassung

Hochprivilegierter Zugang ist einer der heikelsten Aspekte im IT-Bereich. Administratoren-Konten haben die Möglichkeit, umwälzende und fundamentale Änderungen an IT-Systemen vorzunehmen, von denen das Geschäft abhängen kann. Wenn sie auf nicht beabsichtigte Weise benutzt werden, kann dies zu einem breiten Spektrum an Schäden führen, angefangen bei Compliance-Verletzungen, die mit Geldbußen geahndet werden, bis hin zu Sicherheitsvorfällen, die das Vertrauen in die Marke und die Einnahmen verringern.

Aus diesen und anderen Gründen werden die Sichtbarkeit des privilegieren Zugangs und Kontrollen empfohlen oder sind sogar erforderlich:

- Durch eine Vielzahl von Gesetzesvorschriften
- Um eine verantwortungsvolle Unternehmensführung zu gewährleisten
- Zur Verbesserung der Sicherheit

Die Verwaltung von Privilegien beschäftigt sich nicht nur mit diesen Problemen und Bedenken. In diesem Bericht untersuchen Analysten von ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) die Arten, durch die die Transparenz von und Kontrolle der Privilegien Unternehmen nicht nur beim Erreichen dieser Ziele hilft, sondern auch noch einen Vorteil bietet, dessen sich viele nicht bewusst sind: Eine verbesserte IT-Zuverlässigkeit, die die Betriebskosten senken kann. Diese Schrift untersucht die Charakteristika einer effektiven Lösung und bietet auch den durch die EMA-Untersuchungen erbrachten Nachweis, der den Wert eines konsistenteren Ansatzes in Bezug auf die operative Steuerung durch IT stützt.

Privilegierter Zugang: Vorteile und Risiken

Wenn es um den Zugang zu und die Änderung von IT-Systemen mit hohem Geschäftswert geht, besitzen privilegierte Nutzer wie Administratoren normalerweise den größten Handlungsspielraum. Oftmals sind es die technisch begabtesten Nutzer im IT-Bereich, die typischerweise für die Bereitstellung und Verwaltung von Funktionalitäten zuständig sind, die für das Geschäft von größter Bedeutung sind, angefangen bei bedeutenden, alltäglichen Funktionen bis hin zu strategischen Fähigkeiten, die es dem Unternehmen ermöglichen, wettbewerbsfähig zu bleiben. Sie tragen auch eine beträchtliche Verantwortung in Bezug auf für Ihren Geschäftsbereich typische Aktivitäten, wie die Verwaltung von geschäftlichen Anwendungen.

Doch diese Macht birgt auch Risiken. Diese IT-Komplexität führt dazu, dass kleine Änderungen, selbst wenn sie von höchst kompetenten Mitarbeitern durchgeführt werden, große Auswirkungen auf die Verfügbarkeit, Leistung und/oder Integrität von Ressourcen haben. Böswillige Gruppen innerhalb oder außerhalb des Unternehmens können sich den Zugang auf Administrator-Ebene zu Nutze machen und dem Geschäft so schwerwiegende Schäden zufügen. Durch die zunehmende Raffinesse und Tücke moderner Angriffe über Malware und andere Methoden ist es üblich, dass Angreifer Zugang zu diesen Privilegien erhalten und diese missbrauchen, indem sie sich als vertrauenswürdige Mitarbeiter ausgeben.

Privilegierte Nutzer wie Admistratoren haben oft den größten Handlungsspielraum, doch diese Macht birgt Risiken

Privilegiertes Identitätsmanagement (PIM): Nicht nur eine gute Idee…

Unternehmen suchen aus den folgenden Gründen verstärkt nach besseren Kontrollen des privilegierten IT-Zugangs:

Zu Compliance-Zwecken

Eine Reihe von Regulierungsmaßnahmen empfiehlt spezielle Kontrollen im Rahmen des Risikomanagements bei hochprivilegiertem IT-Zugang oder schreiben sie sogar vor. Beispielsweise verlangen Gesetze wie der Sarbanes-Oxley Act („SOX“), dass börsennotierte Unternehmen Vorgänge und Kontrollen einrichten, um eine verantwortungsvolle Unternehmensführung zu gewährleisten.

In Anbetracht der großen Bedeutung von IT bei der Verwaltung und Dokumentation geschäftlicher Aktivitäten und Leistung, ist der Schutz von Unternehmenssystemen vor dem Missbrauch von Administratorenprivilegien einer der gängigsten Wege zur Ausübung dieser Kontrolle.

Der Payment Card Industry Data Security Standard (PCI DSS) Version 3.0 ein Regelwerk zur Abwicklung von Kreditkartentransaktionen, verlangt vergleichbare Maßnahmen zum Schutz der Daten des Karteninhabers, besonders bei der Aufteilung von Pflichten (Best Practices und Anforderung 6) und bei der Überwachung und dem Einsatz von Kontrollen zum hochprivilegierten Zugang (Anforderungen 7 und 8).

Im Versorgungsbereich schreiben die North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards -Vorschriften nicht nur Authentifizierung, Zugangskontrolle, Übertragung des Zugriffs und Aufgabenteilung vor, sondern verlangen auch die vollständige und kontinuierliche Überwachung, Archivierung und das Auditing des Zugangs.

Im Regierungsbereich gelten Anleitungen wie vom U.S. National Institutes of Standards and Technology (NIST) Special Publication 800-53A Rev 4 weithin als Referenz. Sie schreibt die Steuerung sensiblen IT-Zugangs, Aufgabenteilung und besondere Sorgfalt beim administrativen Zugang vor.

Diese Regierungsmaßnahmen wirken sich auch auf Branchen wie die Gesundheitsfürsorge aus. In den Vereinigten Staaten wurde die Sicherheitsrichtlinie zur Umsetzung der Rechtsvorschriften des Health Insurance Portability and Accountability Act (HIPAA) übernommen, die Zugangskontrollen als besonderen Aspekt zur Sicherung elektronisch geschützter Gesundheitsdaten nennt.

Warum ist in diesen Vorschriften ständig von der Notwendigkeit der Überwachung und Kontrolle des privilegierten Zugangs die Rede?

Um das Vertrauen in Geschäftspraktiken zu sichern

Privilegierte Zugänge steuern häufig die fundamentalsten Aspekte der IT, vom Angebot und der Konfiguration auf Grundlagenebene, bis zu den feinsten Nuancen der Anwendungsverwaltung und den Erfahrungen der Endnutzer. Diese Fähigkeiten können ohne Beschränkungen zu einem echten Schaden führen, und dies nicht nur bei den für das Geschäft bedeutsamen IT-Systemen.

Der Sarbanes-Oxley Act und die PCI DSS betonen beispielsweise die Bedeutung der Aufgabenteilung zur Gewährleistung der verantwortungsvollen Kontrolle von Geschäftsabläufen. Die Verwaltung von Privilegien und die Überwachung in der IT helfen sicherzustellen, dass geschäftliche Systeme nicht manipuliert werden können,

um das Unternehmen oder dessen Kunden zu betrügen, missbrauchen, bestehlen oder um Vermögenswerte zu betrügen, indem die Kontrolle über die Systeme erlangt wird, die damit umgehen.

Aufgabenteilung bei der administrativen IT-Kontrolle trägt dazu bei, sicherzustellen, dass Aufzeichnungen zur Unternehmensleistung nicht verändert werden können, um unverantwortliche oder illegale Aktivitäten zu verbergen oder Systeme. die verantwortungsvolles Geschäftsgebaren gewährleisten sollen, nicht getäuscht oder untergraben werden können. Da der Besitz administrativer IT-Privilegien diese Aufgabenteilung bei den Systemen, die geschäftskritische Transaktionen und Daten bearbeiten, einrichten und ändern kann, trägt die Steuerung und Kontrolle von

Administratorprivilegien nicht nur zur Sicherstellung der Integrität von Richtlinien bei, sondern auch, dass die Umsetzung dieser Trennung unverändert bleibt.

Privilegierte Zugänge steuern häufig die fundamentalsten Aspekte der IT. Diese Fähigkeiten können ohne Beschränkungen zu einem echten Schaden führen, nicht nur bei den für das Geschäft bedeutsamen IT-Systemen

Zur Sicherheit

Administrator-Privilegien werden selten an eine Person übertragen, die nicht als vertrauenswürdiger Insider angesehen wird, jedoch können auch sehr fähige Mitarbeiter, auf die das Unternehmen sich verlässt, zu einer Bedrohung werden, wenn Administratorprivilegien missbraucht werden. Zu den Beispielen zählen Fälle wie der von Roger Duronio, dem UBS-Systemadministrator, der für das Legen einer „Logikbombe“ verurteilt wurde, die einen Großteil des Systems des Finanzgiganten beschädigte, oder Terry

Childs, der der Stadt die Kontrolle über San Franciscos FiberWAN-Netzwerks abgenommen hat, indem er sich weigerte, administrative Zugangsdaten freizugeben.

Missbrauchsfälle umfassen eine steigende Anzahl bekannter Handelsmarken und andere Unternehmenseinheiten, welche Drittanbietern privilegierten Zugang zu ihren Netzwerken und Systemen gaben, der dann ausgenutzt wurde. Die Konten wurden genutzt, um Zugang zum Unternehmen zu erhalten.

Eine weitaus größere Bedrohung besteht aus externen Angreifern, die Administrator-Privilegien als Angriffsfläche auswählen, da sie ihnen die direkte Kontrolle von geschäftlichen Systemen ermöglicht, die hohe Vermögenswerte oder kritische Funktionalitäten handhaben. Zusammengenommen geht aus diesen internen und externen Bedrohungen die Notwendigkeit einer effizienteren Sicherheit für administrative IT-Zugänge hervor. Die Mandiant 2014 Threat Landscape Infografik zeigte auf, dass 100% aller Sicherheitsverstößen durch die Nutzung von Insider-Zugangsdaten begangen wurden, entweder von einem skrupellosen, als vertrauenswürdig angesehenen Insider oder durch eine externe Bedrohung, die diese Zugangsdaten missbraucht hat.

Der 2014 Verizon Data Breach Investigation Report zeigt an, dass sich Insider-bezogene Sicherheitsverstöße seit dem Bericht aus dem Jahr 2013 leicht erhöht haben.[1] Zusammen mit dem Mandiant-Bericht, zeigt dies an, dass Insider nicht böswilliger, sondern Ihre Zugangsdaten häufiger missbraucht werden. Berichte von Sicherheitsanbietern wie Symantec's 2014 Internet Security Threat Report Vol. 19 zeigen, dass sich auf Schlüsselpersonal gerichtete Phishing-Attacken seit ihrem 2013-Bericht um 91 % erhöht haben. Die Angreifer werden immer besser darin, ihre zukünftigen Opfer ausfindig zu machen und an ihrer Stelle APT-Malware für eine fortschrittliche, andauernde Bedrohung einzusetzen.

Aus all diesen Gründen - Compliance, Business Assurance und Sicherheit - sind Unternehmen dazu getrieben, mehr Transparenz und Kontrolle des IT-Zugangs durchzusetzen, unabhängig von der Art des Systems: Unix-, Linux- oder Microsoft Windows-Hosts, bei Betriebssystemen und Anwendungen im Rechenzentrum vor Ort oder „in der Cloud“.

... sondern ein echter Vorteil für das Geschäft

Neben den oben genannten Gründen, sollten Unternehmen beachten, dass privilegiertes Identitätsmanagement auch ein Mittel zur Vermeidung oder Reduzierung von Kosten darstellt.

Reduzierung der IT-Kosten

Durch Verbesserung der IT-Zuverlässigkeit

- **Autorisiertes Personal … doch nicht autorisierte Änderungen** – Viele Unternehmen setzen Konfigurations- und Änderungskontrollprozesse ein, um Störungen aufgrund von IT-Änderungen zu reduzieren, doch eine Vielzahl von Faktoren trägt oft dazu bei, dass administrative Aktivitäten ohne die vereinbarten Änderungskontrollen stattfinden. Notfälle und dringender Bedarf, Personal das keine Ahnung von den Änderungsbeschränkungen hat, schlichte Fehler oder - vielleicht alarmierender -Personen, die administrative Zugangsprivilegien besitzen, von denen das Unternehmen keinerlei Ahnung hat, gehören nur zu einigen der Beispiele. Einige von diesen, wie Notfälle, können rein zufällig auftreten. Auch die besten Mitarbeiter machen mal Fehler. Diese Faktoren sollten Unternehmen überdenken lassen, wie sie mit IT-Änderungen umgehen. Die reine Komplexität von IT macht es schwer, jedes mögliche Kontrollszenario vorherzusehen, doch Beschränkungen der benötigten Privilegien können in fast jedem Fall dazu beitragen, Problempunkte zu erkennen, wo notwendig bessere Kontrollen bei IT-Änderungen einzurichten und eine hohe Transparenz administrativer Aktivitäten beizubehalten, die eine genauere Ursachenanalyse von IT-Problemen ermöglicht.

1 Seite 8, Abbildung 5

- **Autorisiertes Personal, autorisierte Änderungen … doch unbeabsichtigte Konsequenzen** – Autorisierte Administratoren und Techniker evaluieren Änderungen und setzen sie entsprechend um, doch die Änderungen haben unerwartete Auswirkungen. Konfigurationsänderungen und Patch-Installationen sind häufige Beispiele. Änderungen können getestet werden, doch Kleinigkeiten im Produktionsumfeld können sich von Mal zu Mal ändern. Das Ausmaß der Änderungen kann den Erwartungen nicht entsprechen, was zu unabsichtlich im System gemachten Änderungen führt, oder Änderungen, die außerhalb des geplanten Bereichs auftreten. Änderungen können mit bestehenden, nicht dokumentierten Konfigurationen in Konflikt stehen und so zu Instabilität und Ausfällen führen. Selbst wenn jeder Aspekt einer Änderung gut dokumentiert, getestet und vorhergesehen wurde, fallen manche Änderungen anders aus als erwartet. Die Umsetzung kann unvollständig sein oder zu einem Ausfall infolge einer Reihe von auftretenden Fehlern führen. Änderungen, die aufgrund von Einschränkungen bei Leistung oder Verfügbarkeit oder von Ausfällen rückgängig gemacht und neu evaluiert werden müssen, zählen zu den bedeutendsten Bestandteilen der IT-Kosten. Privilegierte Zugangskontrollen können dazu beitragen, diese durch genaue Definition der Zugangsziele, Protokollieren administrativer Aktivitäten oder Beschränkung bzw. Beibehaltung des Umfangs des privilegierten Zugangs sowie der Nutzer, die Administrator-Aufgaben ausüben dürfen, niedrig zu halten. Starke Transparenz privilegierter Aktivitäten trägt in diesen Fällen ebenfalls zum Erkennen der spezifischen Ursachen bei.

Die EMA-Untersuchung stützt diese Erkenntnisse. In einer Studie mit weltweit mehr als 200 Unternehmen, [2] hat nur ein Viertel aller Befragten alle vier „Plan–Do–Check–Act" (PDCA) IT-Änderungsmanagement Meilensteine erreicht:

- Festlegen von Zielen des Änderungsmanagements (Plan)
- Tatsächliche Umsetzung dieser Ziele in die Praxis (Do)
- Überwachung der Einhaltung dieser Ziele und Aufdecken von Abweichungen (Check), sowie
- Reaktion auf Abweichungen falls erforderlich (Act).

Im Vergleich zu den anderen 75 % in dieser Studie, hatten diese Bestleistenden:

- Die Hälfte der durchschnittlichen Sicherheitsvorfälle, die eine nicht geplante Reaktion erforderten
- Weniger Fälle von nicht erfolgreichen IT-Änderungen, die eine Korrektur erfordern
- Ein größeres Server-to-System-Administrator-Verhältnis
- Mehr rechtzeitig und im Rahmen des Budgets fertig gestellte IT-Projekte mit den geplanten Features.

Durch Verringerung von Datenverlust durch privilegiertes Identitätsmanagement

Eine EMA-Umfrage aus dem Jahr 20143 zeigt, dass 29 % aller befragten IT-Fachleute aufgrund des Mangels an besseren Tools zum Identifizieren von Aktivitäten wie dem Missbrauch von privilegiertem Zugang, der zu Datenschutzverletzungen und Ausfällen führen kann, frustriert sind. 32 Prozent dieser IT-Fachleute sagten auch, dass ihre Unternehmen Probleme mit dem Erkennen funktionaler bzw. nicht funktionaler Sicherheitskontrollen haben.

Privilegiertes Identitätsmanagement bietet bessere Tools, um gegen diese Probleme anzugehen. Dadurch erfolgt die Überwachung, Durchsetzung und Meldung von Kontrollen zur Regulierung der Nutzung des privilegierten Zugangs. Wenn Zugang gewährt wird, zeigt die Transparenz des privilegierten Zugangs nicht nur an, wenn administrative Aktionen der Grund für Probleme mit der

Wenn eine übliche Methode zur Verwaltung und Durchsetzung von Richtlinien für Auditing, Autorisierung und Authentifizierung sowohl bei Rechenzentren vor Ort als auch bei ortsunabhängigen anwendbar ist, dann können die IT-Betriebskosten durch eine konsistente Kontrolle administrativer Handlungen durch die zur schnelleren Problemlösung führende, umfassende Transparenz dieser Handlungen weiter gesenkt werden.

[2] *IT Risk Management: Five Aspects of High Performers that Set Them Apart*, EMA Anwendungsvorschläge, Juli 2011
[3] *The Evolution of Data Driven Security*, EMA-Untersuchungsbericht, Februar 2014

IT-Leistung, Verfügbarkeit oder Integrität sind, sondern kann auch ihr Auftreten durch das proaktive Verhindern von Aktivitäten, die zu Ausfällen führen, vermeiden.

Wenn eine übliche Methode zur Verwaltung und Durchsetzung von Richtlinien für Auditing, Autorisierung und Authentifizierung sowohl bei Rechenzentren vor Ort als auch bei ortsunabhängigen anwendbar ist, dann können die IT-Betriebskosten durch eine konsistente Kontrolle administrativer Handlungen durch die zur schnelleren Problemlösung führende, umfassende Transparenz dieser Handlungen weiter gesenkt werden.

- Autorisierte Identität … doch nicht autorisierte Nutzung, Zugang zu Daten und deren Exfiltration – Sobald sie sich im Umfeld befindet, nutzt Malware die Identität eines Opfers, um sich innerhalb dieses Umfelds lateral zur Erkundung zu bewegen, und die externen Bedroher mit internen Zugangsdaten zu versorgen und um letztendlich Daten zu entfernen. Diese Aktivitäten führen direkt zu höheren IT-Wartungs- und Supportkosten. Es ist jedoch noch schlimmer, wenn es um Kundendaten geht, da Sicherheitsverstöße dann Millionen an Bereinigungs- und Benachrichtigungskosten verursachen können. Nach der 2014 IBM/Ponemon Cost of Data Breach Study belaufen sich die gezahlten Durchschnittskosten pro Sicherheitsverstoßfall auf 145 USD und die durchschnittlichen Gesamtkosten betragen 3,5 Millionen USD. Die Bereinigungskosten einiger Sicherheitsverstöße bei bedeutenden US-Händlern betrugen 2014 von mehr als 4 Millionen USD bis zu über 100 Millionen USD. Die Umsatzeinbußen dieser Verkäufer rangierten zwischen 40 Millionen USD bis zu mehr als 1 Milliarde USD. Organisationen sollten erkennen, wie privilegiertes Identitätsmanagement dazu beitragen kann, diese Kosten zu senken. Dies erfolgt durch die effektivere Kontrolle von Privilegien und deren Überwachung und Benachrichtigung, falls sie auf verdächtige Art genutzt werden.

Die Charakteristika einer effektiven Lösung

Was sollte eine effektive Lösung dieser Probleme umfassen? Wie kann die Technologie des privilegierten Identitätsmanagements dazu beitragen, die Möglichkeit zum Reduzieren der IT-Betriebskosten und geschäftlichen Verluste durch eine verbesserte IT-Verantwortbarkeit zu Geld zu machen?

Ein umfassender Ansatz sollte:

- Unternehmen dazu in die Lage versetzen, eine Anzahl flexibler Parameter zur Kontrolle des Administratorzugangs festzulegen, wie Zeitfenster, bestimmte Personen oder Zugangsziele und den Zugang auf bestimmte Bereiche oder Funktionen beschränken, die zur Ausführung der Aufgabe notwendig sind.
- Verschiedene Identitäten zusammenführen, um eine einheitliche Identitäts-"Person" über alle unterschiedlichen Betriebssysteme und Umgebungen hinweg zu erstellen. Dies verbessert das Berichtswesen und reduziert Auditzeiten und kriminaltechnische Ermittlungen.
- Verknüpfen des auf Rollen basierenden Nutzerzugangs zu kritischen Systemen, Anwendungen und Diensten mit spezifischen Nutzeridentitäten. Dies unterstützt die Verknüpfung von administrativen Konten, die häufig von einer Gruppe qualifizierter Fachleute gemeinsam genutzt werden, mit der persönlichen Rechenschaft und verbessert sowohl den Grad der Transparenz und Kontrolle.
- Stärkung der Effizienz durch Aushebelung der bestehenden Identitätsspeicher ohne Schemamodifikation zur Beibehaltung einer allgemein verwendeten Infrastruktur zur Feststellung sowohl von individuellen Nutzern als auch von administrativen Konten. Die Möglichkeit, diese Ressourcen über verschiedene Zugangsziele hinweg in einem heterogenen Unternehmen zu nutzen, um die Nutzeridentität im gesamten Unternehmen zu vereinheitlichen, ist ein wesentlicher Vorteil.
- Das Anbieten einer skalierbaren, durchsuchbaren und umfassenden Audit- und Berichtslösung für Nutzeraktivitäten in kritischen Systemen, einschließlich der Möglichkeit, sowohl in Befehlszeilen- und grafischen Nutzersitzungen („Video-Wiedergabe“).
- Zentralisierung der Privilegtransparenz und -kontrolle durch eine „einzige Glasscheibe“, für die Verwaltung, die Richtlinien und Berichte zu allen Servern und Nutzern. Dies erhöht die Effizienz (die zu einer weiteren Reduzierung der Kosten beiträgt) und stellt einen einheitlichen und konsistenten Ansatz für die Verwaltung innerhalb des gesamten Umfelds dar.
- Integration des Auditings der Nutzeraktivität wie Syslog- und Windows Event Log-Daten mit anderen zentralisierten

Überwachungs- und Berichtstechnologien wie Security Information and Event Management (SIEM).

- Durchsetzung der Politik des geringstmöglichen Zugangs durch umfassende Transparenzkontrolle während gleichzeitig die Möglichkeit besteht, kontrollierte Zugangsrechte zu erweitern, ohne dazu komplette Administratorenrechte oder Root-Zugang zu vergeben.
- Skalierung durch die Verwaltung von Zehntausenden Identitäten über heterogene Betriebssysteme hinweg, Unterstützung Zehntausender Systeme.

EMA-Perspektive

Es wurde einmal gesagt: „Aus großer Macht folgt große Verantwortung“. Auf privilegierten IT-Zugang trifft dies zu. Administratorkonten können große Auswirkungen auf für das Geschäft bedeutsame IT-Systeme und Funktionen haben, die nicht nur Unternehmen selbst, sondern auch seine Kunden und Aktionäre betreffen.

Privilegiertes Identitätsmanagement schränkt die Gefährdung durch diese Risiken durch genaueste Kontrolle dazu, wer was wann macht und wie diese administrativen Rechte ausgeübt werden, ein. Die Überprüfung privilegierter Konten dokumentiert, wie diese Macht ausgeübt wurde. Bei verantwortungsvoller Nutzung, zeigt sie an, wie IT-Interaktionen zu Dienstproblemen geführt haben können. Die Kontrolle von Privilegien trägt bei böswilliger Nutzung dazu bei, Risiken zu senken, während die Überprüfung von Privilegien Aktionen aufzeigen kann, die dazu beitragen, die Auswirkungen von Vorfällen zu verringern und eine faire und verantwortungsvolle Umsetzung zu unterstützen.

Die Auswirkungen des hochprivilegierten Zugangs im IT-Bereich können selbst bei verantwortungsvoller Nutzung nicht überblickt werden. Durch moderne Ansätze zur Verwaltung von Privilegien und Transparenz können Unternehmen eine umfassendere Compliance unterstützen, dazu beitragen, die Integrität des Geschäfts zu gewährleisten und gegen Sicherheitsrisiken vorgehen, während sie gleichzeitig von der Kostenersparnis und anderen Vorteilen einer verbesserten IT-Zuverlässigkeit profitieren.

Die Auswirkungen des hochprivilegierten Zugangs im IT-Bereich können selbst bei verantwortungsvoller Nutzung nicht überblickt werden. Durch moderne Ansätze zur Verwaltung von Privilegien und Transparenz können Unternehmen eine umfassendere Compliance unterstützen, dazu beitragen, die Integrität des Geschäfts zu gewährleisten und gegen Sicherheitsrisiken vorgehen, während sie gleichzeitig von der Kostenersparnis und anderen Vorteilen einer verbesserten IT-Zuverlässigkeit profitieren.

Über Centrify

Centrify bietet vereinheitlichtes Identitätsmanagement über Cloud-, Rechenzentren- und mobile Umgebungen hinweg, die für die Anwender zu einem einzigen Login (SSO) und einer vereinfachten Identitätsinfrastruktur für IT führen. Centrifys vereinheitlichte Identitätsmanagementsoftware und cloudbasierte Identity-as-a-Service (IDaaS)-Lösungen nutzen die bestehende Identitätsinfrastruktur eines Unternehmens, um ein einziges Login, Multifaktor-Authentifizierung, privilegiertes Identitätsmanagement und Prüfungen zur Compliance und Mobilgerätemanagement zu ermöglichen. Centrify-Kunden können normalerweise ihre Gesamtkosten für Identitätsmanagement und Compliance um mehr als 50 Prozent senken, während sie die Flexibilität des Unternehmens und allgemeine Sicherheit erhöhen. Centrify wird weltweit von mehr als 5.000 Kunden verwendet, einschließlich von nahezu der Hälfte der Fortune 50 und mehr als 60 Bundesbehörden. Bitte besuchen Sie http://www.centrify.com/, um weitere Informationen zu erhalten.

Über Enterprise Management Associates, Inc.

Enterprise Management Associates (EMA) wurde 1996 gegründet und ist ein führendes Branchenanalyseunternehmen, das einen tiefgehenden Einblick in das gesamte Spektrum der IT- und Datenmanagementtechnologien bietet. EMA-Analysten besitzen eine einzigartige Kombination aus praktischer Erfahrung, Einblick in die Erfolgsmethoden der Branche und ein umfassendes Wissen über derzeitige und geplante Anbieterlösungen, die den Kunden von EMA hilft, ihre Ziele zu erreichen. Erfahren Sie mehr über EMAs Untersuchungs-, Analyse- und Beratungsdienstleistungen für Unternehmenssparten, IT-Fachkräfte und IT-Anbieter auf www.enterprisemanagement.com oder blogs.enterprisemanagement.com. Sie können EMA auf Twitter, Facebook oder LinkedIn folgen.

Hauptsitz:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Telefon: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2685.020515