



Durchsetzung des Least-Privilege-Prinzips auf Servern

Schützen Sie Server mit nahtlosen richtlinienbasierten Autorisierungskontrollen und MFA im Detail

Die digitale Transformation verändert Unternehmen weiterhin mit zunehmender Komplexität und fragmentierten Identitäten in allen Umgebungen. Es ist von entscheidender Bedeutung, den privilegierten Zugriff auf Server durch Identitätskonsolidierung und zentralisierte Verwaltung von Berechtigungen auf Windows-, Linux- und Unix-Servern zu vereinfachen und zu schützen.

Delinea kontrolliert nahtlos und granular den privilegierten Zugriff auf Server mit Just-in-Time- und Just-Enough-Berechtigungen und bietet Identitätssicherung mit mehrschichtiger MFA-Durchsetzung, um laterale Bewegungen zu verhindern und gleichzeitig die Verantwortlichkeit zu erhöhen.

✓ Konsequentes Erzwingen von Least Privilege

- Verwalten Sie Richtlinien für privilegierten Zugriff und MFA-Durchsetzung in Active Directory (AD) (patentierbare Zonen) oder von den meisten Cloud-Identitätsanbietern. Eine einzige Unternehmensidentität für die Benutzeranmeldung.

✓ Minimieren des Risikos mit Best Practices

- Erfüllen Sie die gesetzlichen Vorschriften und die Best Practices für Zero Trust und Least Privilege zum Schutz vor Ransomware und Angriffen auf Ihre Daten.

✓ Erhöhen Sie Berechtigungen granular

- Wenden Sie Richtlinien auf Host-Ebene an, um eine genauere Kontrolle über Berechtigungserhöhungen zu erhalten. Implementieren Sie Self-Service-Workflows zur Automatisierung von Just-in-Time-Zugriffsanfragen.

✓ Durchsetzung von adaptiver MFA

- MFA-Richtlinien, die bei der Anmeldung und für die Berechtigungserhöhung unter Windows, Linux und Unix durchgesetzt werden, um die Identitätssicherheit zu erhöhen und die Anforderungen an die Versicherung gegen Cyberrisiken zu erfüllen.

✓ Erfüllen Sie Compliance-Anforderungen einfacher

- Forensischer Audit Trail und Sitzungsaufzeichnungen für die Sicherheitsüberprüfung, Incident Response, die Einhaltung von Vorschriften und vollständige Rechenschaftspflicht.

Vorteile von Server PAM



ERHÖHUNG DER SICHERHEIT & RISIKOEINDÄMMUNG

Verwalten Sie den Zugriff zentral mit Just-in-Time(JIT)- und Just-Enough(JE)-Privilegien, und gewährleisten Sie Identitätssicherung mit Multi-Faktor-Authentifizierung (MFA) bei der Systemanmeldung und bei der Erhöhung der Berechtigungen, um laterale Bewegungen zu verhindern und sich an den Best Practices für Least Privilege und Zero Trust zu orientieren.



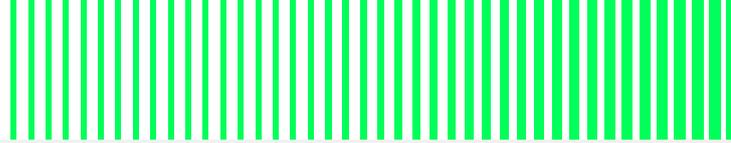
IDENTITÄTSKONSOLIDIERUNG & VERBESSERTE PRODUKTIVITÄT

Beseitigen Sie die große Anzahl nicht verwalteter lokaler Konten und verwenden Sie Unternehmensverzeichnis-konten für den Zugriff auf Windows, Linux oder Unix On-Premise oder in der Cloud, um die Identitätsausweitung zu begrenzen und Workflows zu vereinfachen.



EINFACHERE PRÜFUNG PRIVILEGIERTER AKTIVITÄTEN

Nutzen Sie detaillierte, hostbasierte Prüfungen und Sitzungsaufzeichnungen, um potenziell schädliche privilegierte Aktivitäten zu identifizieren und Kontrollen für die Einhaltung unveränderter Prüfdaten nachzuweisen.



Kontrollieren Sie den privilegierten Zugriff auf Server On-Premise und in der Cloud

Delinea schützt den privilegierten Zugriff auf Server durch Identitätskonsolidierung und zentralisierte Verwaltung von Just-in-Time- und Just-Enough-Privilegien. Multi-Directory-Brokering vereinfacht die Administratorauthentifizierung und konsolidiert Identitäten, wodurch Vertrauen zwischen unterschiedlichen Identitätsanbietern und Windows- und Linux-Instanzen in hybriden IT-Umgebungen hergestellt wird. Die MFA-Durchsetzung bei der Serveranmeldung und die Berechtigungserhöhung sorgen für zusätzliche Identitätssicherung beim Zugriff auf sensible Systeme. Echtzeit-Sitzungsüberwachung und -aufzeichnung auf jedem Server sorgen für vollständige Transparenz und verwertbare Ereignisdetails.

✓ Authentifizierung

Vereinfachen Sie die Benutzerauthentifizierung bei Servern über jeden beliebigen Verzeichnisdienst, wie Active Directory und OpenLDAP und Cloud-Verzeichnisse wie Azure AD, Okta oder Ping. Sichern Sie den Zugriff auf virtuelle Linux-, Unix- und Windows-Systeme und -Container. Erzwingen Sie MFA für eine stärkere Identitätssicherung.

- Multi-Directory-Brokering
- Rechneridentität, delegierte Rechnerzugangsdaten und Zugangsdatenverwaltung
- Verwaltung von Authentifizierungsrichtlinien
- MFA bei Systemanmeldung
- Zentrale Verwaltung des Lebenszyklus lokaler Konten und Gruppen

✓ Berechtigungserhöhung

Setzen Sie das Least-Privilege-Prinzip in der Windows-, Linux- und UNIX-Infrastruktur On-Premise, in der Cloud und in mehreren Clouds durch. Reduzieren Sie bestehende Privilegien und verhindern Sie laterale Bewegungen, um das Risiko einer Datenschutzverletzung oder eines Ransomware-Angriffs zu minimieren. Bei Bedarf können Administratoren eine kurzzeitige Erweiterung ihrer Privilegien anfordern.

- Konsistente und automatisierte Verwaltung von Sicherheitsrichtlinien
- Berechtigungserhöhung zur Durchsetzung von Least Privilege
- Just-in-Time-Workflow zur Berechtigungserhöhung
- MFA bei Berechtigungserhöhung

✓ Audit und Überwachung

Erkennen Sie den Missbrauch von Zugriffsberechtigungen, vereiteln Sie Angriffe und weisen Sie die Einhaltung von Vorschriften nach – mit einem detaillierten Audit Trail und Videoaufzeichnungen aller privilegierten Aktivitäten.

- Granulare Ereignisprotokollierung und -prüfung auf Hostebene
- Durchsuchbare Aufzeichnungen zur visuellen Analyse
- Ganzheitliche Sicht auf privilegierte Aktivitäten auf Windows- und Linux-Servern, IaaS und Datenbanken
- Berichte über die Berechtigungen jedes Benutzers und die damit verbundenen Aktivitäten zur Einhaltung der Compliance

✓ Cloudnativ

Die Bereitstellung über die cloudnative Delinea-Plattform ermöglicht eine einheitliche Verwaltung, beschleunigt die Wertschöpfung und senkt die Gesamtbetriebskosten durch umfassende Privilegienverwaltung.

- Durch die kontinuierliche Erkennung werden privilegierte Konten und Identitäten in Ihrem Netzwerk nahtlos identifiziert
- MFA im Detail sorgt für Identitätssicherung
- Überwachen Sie privilegierte Aktivitäten über privilegierte Konten und Identitäten hinweg, um die Verantwortlichkeit zu erhöhen
- Durch KI-gesteuerte Analysen können potenziell gefährliche Aktivitäten privilegierter Benutzer schnell identifiziert werden
- Marketplace vereinfacht die Integration mit bestehenden IT- und Sicherheitslösungen

Weitere Informationen unter [Delinea.com/de](https://delinea.com/de)

Delinea

Delinea ist ein führender Anbieter für Privileged-Access-Management-Lösungen (PAM) für das moderne, hybride Unternehmen. Die Delinea-Plattform erweitert PAM nahtlos, indem sie eine Autorisierung für alle Identitäten bereitstellt und den Zugriff auf die wichtigsten Hybrid-Cloud-Infrastrukturen und sensiblen Daten eines Unternehmens kontrolliert, um Risiken zu reduzieren, Compliance zu gewährleisten und die Sicherheit zu vereinfachen. Delinea reduziert die Komplexität und definiert Grenzen für den Zugriff für Tausende von Kunden weltweit. Zu unseren Kunden zählen Kleinunternehmen ebenso wie die weltweit größten Finanzinstitute, Sicherheitsbehörden und Unternehmen mit kritischer Infrastruktur. delinea.com/de