KuppingerCole Report

LEADERSHIP COMPASS

von Anmol Singh | März 2019

Privileged Access Management

Privileged Access Management (PAM) hat sich in den letzten Jahren in eine Reihe von kritischen Technologien entwickelt, die in einigen der bedeutendsten Bereiche der modernen Cybersicherheit eingesetzt werden. Der weiterhin wachsende PAM-Markt ist in eine Phase der Konsolidierung eingetreten, die von einem verstärkten Preiswettbewerb und einem schärferen Kampf um Marktanteile gekennzeichnet ist. Dieser Leadership Compass bietet eine detaillierte Analyse des PAM-Markts und seiner wichtigsten Akteure, um führende Unternehmen in den Bereichen Sicherheit und IAM dabei zu unterstützen, die richtigen Produkte für ihre jeweiligen Anforderungen in Bezug auf Cybersicherheit zu finden.

von **Anmol Singh**
asi@kuppingercole.com
März 2019

Leadership Compass
Privileged Access Management
von KuppingerCole

Inhalt

1 Übersicht ... 6

1.2 Marktsegment ... 6

1.3 Erforderliche Funktionen ... 8

2 Leadership ... 14

3 Korrelierte Ansicht ... 22

3.1 Markt-/Produktmatrix ... 22

3.2 Produkt-/Innovationsmatrix ... 24

3.3 Innovations-/Marktmatrix ... 26

4 Produkte und Anbieter auf einen Blick ... 28

4.1 Bewertungen auf einen Blick ... 28

5 Produkt-/Service-Evaluierung ... 30

5.1 ARCON ... 31

5.2 BeyondTrust ... 32

5.3 CA Technologies ... 33

5.4 Centrify Corporation ... 34

5.5 CyberArk ... 35

5.6 EmpowerID ... 37

5.7 FUDO Security ... 38

5.8 Hitachi ID ... 39

5.9 I-Sprint ... 40

5.10 Krontech ... 41

5.11 ManageEngine ... 42

5.12 Micro Focus ... 44

5.13 MT4 Networks ... 45

5.14 One Identity ... 46

5.15 Osirium ... 48

5.16 Sectona ... 49

5.17 SSH.COM ... 50

5.18 Thycotic ... 51

5.19 WALLIX ... 53

6 Vielversprechende Anbieter ... 54

6.1 Deep Identity ... 54

6.2 Devolutions 54
6.3 HashiCorp 55
6.4 HelpSystems 55
6.5 IdentityAutomation 56
6.6 Iraje 56
6.7 MasterSAM 57
6.8 NRI Secure Technologies 57
6.9 ObserveIT 58
6.10 OnionID 58
6.11 Oracle 59
6.12 Remediant 59
6.13 Saviynt 60
6.14 SecureLink 60
6.15 Venafi 61
6.16 XTON Technologies 61
7 Methodologie 62
7.2 Arten von Leadership 62
7.3 Produktbewertung 63
7.4 Anbieterbewertung 65
7.5 Bewertungsskala für Produkte und Anbieter 66
7.6 Netzdiagramme 67
7.7 Einbeziehung und Ausschluss von Anbietern 68
8 Copyright 70

Tabellenverzeichnis

Tabelle 1: Vergleichsübersicht der Bewertungen der Produktfunktionen 28
Tabelle 2: Vergleichsübersicht der Anbieterbewertungen 29
Tabelle 3: Bedeutende Stärken und Schwächen von ARCON 31
Tabelle 4: Bewertung von ARCON 31
Tabelle 5: Bedeutende Stärken und Schwächen von BeyondTrust 32
Tabelle 6: Bewertung von BeyondTrust 33
Tabelle 7: Bedeutende Stärken und Schwächen von CA Technologies 34
Tabelle 8: Bewertung von CA Technologies 34
Tabelle 9: Bedeutende Stärken und Schwächen von Centrify 35
Tabelle 10: Bewertung von Centrify 35
Tabelle 11: Bedeutende Stärken und Schwächen von CyberArk 36

Tabelle 12: Bewertung von CyberArk ... 36
Tabelle 13: Bedeutende Stärken und Schwächen von EmpowerID ... 37
Tabelle 14: Bewertung von EmpowerID ... 37
Tabelle 15: Bedeutende Stärken und Schwächen von FUDO Security ... 38
Tabelle 16: Bewertung von FUDO Security ... 39
Tabelle 17: Bedeutende Stärken und Schwächen von Hitachi ID ... 39
Tabelle 18: Bewertung von Hitachi ID ... 40
Tabelle 19: Bedeutende Stärken und Schwächen von I-Sprint ... 40
Tabelle 20: Bewertung von I-Sprint ... 41
Tabelle 21: Bedeutende Stärken und Schwächen von Krontech ... 42
Tabelle 22: Bewertung von Krontech ... 42
Tabelle 23: Bedeutende Stärken und Schwächen von ManageEngine ... 43
Tabelle 24: Bewertung von ManageEngine ... 43
Tabelle 25: Bedeutende Stärken und Schwächen von Micro Focus ... 44
Tabelle 26: Bewertung von Micro Focus ... 44
Tabelle 27: Bedeutende Stärken und Schwächen von MT4 Networks ... 45
Tabelle 28: Bewertung von MT4 Networks ... 46
Tabelle 29: Bedeutende Stärken und Schwächen von One Identity ... 46
Tabelle 30: Bewertung von One Identity ... 47
Tabelle 31: Bedeutende Stärken und Schwächen von Osirium ... 48
Tabelle 32: Bewertung von Osirium ... 48
Tabelle 33: Bedeutende Stärken und Schwächen von Sectona ... 49
Tabelle 34: Bewertung von Sectona ... 49
Tabelle 35: Bedeutende Stärken und Schwächen von SSH.COM ... 50
Tabelle 36: Bewertung von SSH.COM ... 51
Tabelle 37: Bedeutende Stärken und Schwächen von Thycotic ... 52
Tabelle 38: Bewertung von Thycotic ... 52
Tabelle 39: Bedeutende Stärken und Schwächen von WALLIX ... 53
Tabelle 40: Bewertung von WALLIX ... 53

Abbildungsverzeichnis

Abbildung 1: Architekturmodell von PAM-Tools und -Technologien ... 10
Abbildung 2: Overall Leadership im Marktsegment Privileged Access Management ... 14
Abbildung 3: Product Leaders im Marktsegment Privileged Access Management ... 16
Abbildung 4: Innovation Leaders im Marktsegment Privileged Access Management ... 18
Abbildung 5: Market Leaders im Marktsegment Privileged Access Management ... 20
Abbildung 6: Markt-/Produktmatrix ... 22
Abbildung 7: Produkt-/Innovationsmatrix ... 24
Abbildung 8: Innovations-/Marktmatrix ... 26

Weitere relevante Dokumente (in englischer Sprache)

Advisory Note: Identity & Access Management/Governance Blueprint - 70839

Advisory Note: IAM Predictions and Recommendations 2014-2018 - 71120

Advisory Note: Secure your Cloud against Industrial Espionage - 70997

Advisory Note: Cloud IAM: More than just Single Sign-On to Cloud Applications - 71031

Advisory Note: The new ABC for IT: Agile Businesses – Connected - 70998

Advisory Note: Connected Enterprise Step-by-step - 70999

Architecture Blueprint: Access Governance and Privilege Management - 79045

Executive View: ARCON Privilege Manager - 70950

Executive View: BeyondTrust PowerBroker for Unix & Linux - 70363

Executive View: CA Privileged Access Management Suite - 79047

Executive View: Centrify Next-Gen Access Platform - 79036

Executive View: Cloud Standards Cross Reference - 71124

Executive View: EmpowerID - 70894

Executive View: EU Guidelines for Cloud Service Level Agreements - 71154

Executive View: Vendor Overview CyberArk - 70280

Executive View: Hitachi ID Privileged Access Manager - 80030

Executive View: i-Sprint AccessMatrix Universal Sign-On - 71064

Executive View: Krontech SingleConnect - 80031

Executive View: ManageEngine Password Manager Pro - 70613

Executive View: Micro Focus Privileged Account Manager - 71314

Executive View: One Identity Safeguard - 79042

Executive View: Osirium: Privileged Access Management - 70836

Executive View: SSH.COM PrivX - 70302

Executive View: Thycotic Privilege Manager - 80004

Executive View: Wallix AdminBastion - 71266

Leadership Compass: Cloud IAM/IAG - 71121

Leadership Compass: Identity Provisioning - 71139

Leadership Compass: Enterprise Key and Certificate Management - 70961

Leadership Compass: Enterprise Single Sign-On - 70962

Leadership Compass: Privilege Management - 72330

Leadership Compass: Access Management and Federation - 71147

Leadership Compass: Access Governance & Intelligence - 71145

1 Übersicht

Der KuppingerCole Leadership Compass bietet einen Überblick über die Anbieter und ihre jeweiligen Produkte oder Services in einem bestimmten Marktsegment. Dieser Leadership Compass konzentriert sich auf das Marktsegment des On-Premise- oder cloudbasierten Privileged Access Management. PAM hat sich als eine der wichtigsten IAM-Technologien erwiesen, die eine direkte Bedeutung und Auswirkung auf das Cybersicherheitsprogramm eines Unternehmens hat.

1.2 Marktsegment

Im Zeitalter der digitalen Transformation entwickeln sich nicht nur die Anforderungen an die IT stetig weiter, sondern auch die eingesetzten Verfahren. Um relevant zu bleiben, müssen Organisationen sich immer wieder neu erfinden, indem sie agil arbeiten und innovativer werden. Neue Technologieinitiativen, wie zum Beispiel der digitale Arbeitsplatz, DevOps, Sicherheitsautomatisierung und das Internet der Dinge, vergrößern weiterhin die Angriffsfläche eines Unternehmens und bergen neue digitale Gefahren. Um wettbewerbsfähig und gesetzeskonform zu bleiben, müssen Organisationen aktiv nach neuen Möglichkeiten suchen, Sicherheitsrisiken zu evaluieren und zu verwalten, ohne ihre Geschäftsabläufe zu stören. Leader im Bereich Sicherheit haben deshalb das dringende Bedürfnis, die Sicherheitsposition ihres Unternehmens fortlaufend zu verbessern, indem sie geeignete Kontrollen implementieren, um solche Gefahren zu vermeiden.

In den letzten Jahren hat Privileged Access Management (PAM) sich zu einem der bedeutendsten Bereiche der Cybersicherheit im Zusammenhang mit IAM (Identity and Access Management) entwickelt. PAM-Lösungen konzentrieren sich auf die Identifizierung, Absicherung und Verwaltung von privilegierten Anmeldeinformationen und den daraus entstehenden Zugriff innerhalb der IT-Umgebung einer Organisation. Das einst als technologische Option zur Optimierung der administrativen Effizienz durch die Verwaltung von Passwörtern und anderen Unternehmensgeheimnissen betrachtete PAM hat sich als eine der wichtigsten Technologien zur Abwehr von Cyberangriffen und Anmeldedatenverlusten erwiesen. Heute ist PAM dank mehrerer sicherheitsspezifischer und operativer Vorteile sowohl für Sicherheits- und Risikomanagementspezialisten als auch für I&Q-Fachleute (Infrastruktur und Operation) in verschiedensten Branchen relevant.

Privileged Access Management umfasst eine Reihe von kritischen Cybersicherheitskontrollen zur Bekämpfung von Sicherheitsrisiken im Zusammenhang mit privilegierten Nutzern und privilegiertem Zugang in Unternehmen. Es gibt in erster Linie zwei Arten von privilegierten Nutzern:

1. Privilegierte Geschäftsnutzer - mit Zugriff auf sensible Daten und Informations-Assets, wie beispielsweise Personalverwaltungsdaten, Gehaltsdetails, Finanzdaten, geistiges Eigentum eines Unternehmens usw. Dieser Zugriffstyp wird üblicherweise Anwendungsnutzern mittels Geschäftsrollen über Anwendungskonten zugewiesen.

2. Privilegierte IT-Nutzer - mit Zugriff auf die zugrunde liegende IT-Infrastruktur eines Unternehmens. Dieser Zugriffstyp wird im Allgemeinen IT-Administratoren mittels administrativen Rollen über Systemkonten, Softwarekonten oder operativen Konten gewährt.

Die privilegierte Natur dieser Konten bietet ihren jeweiligen Benutzern einen uneingeschränkten und häufig nicht überwachten Zugriff auf die IT-Assets eines Unternehmen, was nicht nur gegen grundlegende Sicherheitsprinzipien, wie bspw. Least Privilege, verstößt, sondern auch die Möglichkeit, individuelle Rechenschaft für privilegierte Aktivitäten zu etablieren, empfindlich eingeschränkt. Aufgrund ihres umfangreicheren Zugriffs auf sensible Daten und kritische Operationen stellen privilegierte Konten eine signifikante Bedrohung für die Sicherheitslage eines Unternehmens insgesamt dar. Führende Unternehmen im Bereich Sicherheit müssen deshalb mehr Fokus auf die Identifizierung und Verwaltung dieser Konten legen, um die von ihrem Missbrauch ausgehenden Bedrohungen zu vermeiden.

Erhältliche IAM-Tools (Identity and Access Management) wurden speziell für die Verwaltung der Identität und des Zugriffs von Standardbenutzern konzipiert und bieten deshalb nicht die Funktionen, die für das Management von privilegierten Zugriffsszenarien erforderlich sind, wie zum Beispiel die Verwaltung des Zugriffs auf gemeinsam verwendete Konten, die Überwachung privilegierter Aktivitäten sowie die kontrollierte Erhöhung von Zugriffsprivilegien. Privileged Access Management-Tools wurden genau für solche Szenarien entwickelt und umfassen spezielle Technologien und Prozesssteuerungen, welche den Schutz der digitalen Assets eines Unternehmens erhöhen, indem sie den Missbrauch von privilegiertem Zugriff verhindern.

Während bisher Vaults für Anmeldeinformationen, Passwortrotation, kontrollierte Erhöhung sowie Delegierung im Mittelpunkt des Interesses im Hinblick auf PAM-Tools standen, entwickeln sich heute neue und höher entwickelte Funktionen, wie Privileged User Analytics, risikobasiertes Session Monitoring und Advanced Threat Protection zum neuen Standard. Da die Angriffsfläche sich immer mehr vergrößert und die Anzahl sowie die Raffinesse der Angriffe jährlich steigt, ist eine integrierte und umfangreichere PAM-Lösung erforderlich, die ungewöhnliches Verhalten automatisch erkennt und automatisierte Behebungsmaßnahmen ergreift. Ein erfolgreicher Angriff kann nach wenigen Minuten schon wieder vorbei sein, deshalb müssen PAM-Lösungen diese ohne menschliches Eingreifen abwehren können. Und obgleich umfassendere PAM-Suites und -Lösungen auf dem Markt erhältlich sind, verfolgen Anbieter unterschiedliche Ansätze, um das zugrunde liegende Problem der Einschränkung, Überwachung und Analyse von privilegiertem Zugriff sowie der Nutzung gemeinsamer Konten zu lösen.

Zu den wichtigsten Herausforderungen, die eine Verwaltung des privilegierten Zugriffs erforderlich machen, zählen:

- Missbrauch gemeinsam verwendeter Anmeldeinformationen
- Missbrauch erweiterter Privilegien durch autorisierte Nutzer
- Diebstahl von privilegierten Anmeldeinformationen durch Cyber-Kriminelle
- Missbrauch von Privilegien in Drittparteisystemen, und
- versehentlicher Missbrauch erweiterter Privilegien durch Nutzer

Darüber hinaus gibt es mehrere weitere betriebliche, governance-spezifische sowie rechtliche Anforderungen im Zusammenhang mit privilegierten Zugriffsrechten:

- Entdeckung von gemeinsam verwendeten Konten, Software- und Servicekonten innerhalb der IT-Infrastruktur
- Identifizierung und fortlaufendes Tracking der Eigentümer von privilegierten Konten über ihre jeweilige Lebensdauer

- Etablierung und Verwaltung privilegierter Sessions in Zielsystemen für eine verbesserte betriebliche Effizienz von Administratoren
- Auditing, Aufzeichnung und Überwachung von privilegierten Aktivitäten zwecks gesetzlicher Compliance
- Verwaltung und Überwachung des Verwaltungszugriffs von IT-Outsourcing-Anbietern und MSPs auf interne IT-Systeme, und
- Verwaltung und Überwachung des privilegierten Zugriffs von Geschäftsnutzern und IT-Administratoren auf Cloud-Infrastrukturen und -Anwendungen

Folglich wurden mehrere Technologien und Lösungen als Antwort auf diese Gefahren entwickelt, die außerdem eine verbesserte Aktivitätsüberwachung und Bedrohungserkennung bieten.

1.3 Erforderliche Funktionen

In diesem Leadership Compass konzentrieren wir uns auf Lösungen, mit denen Unternehmen die Risiken in Verbindung mit privilegiertem Zugriff über individuelle oder gemeinsam verwendete Konten innerhalb On-Premise- und Cloud-Infrastrukturen verringern können. Die zur Verwaltung von privilegiertem Zugriff verwendeten Tools und Technologien werden unter verschiedenen Bezeichnungen auf dem Markt angeboten — Account Management, Privileged Identity Management, Privileged User Management und Least Privilege, um nur einige wenige zu nennen. Wir haben diesen Markt in der Vergangenheit als PxM bezeichnet, haben aber nun beschlossen, diese Bezeichnung in „Privileged Access Management" oder „PAM" zu ändern, um den Aspekt des „Access Management" (Zugriffsmanagement) hervorzuheben, der sich in erster Linie auf die Verwaltung des privilegierten Zugriffs von Benutzern und IT-Administratoren über individuelle oder gemeinsam verwendete Konten sowie andere Mechanismen zur Delegierung oder Steigerung von Privilegien bezieht.

Bei KuppingerCole klassifizieren wir den Markt für Privileged Access Management (PAM) anhand der folgenden Haupttechnologien, wobei PAM-Anbieter ein unterschiedliches Maß an Unterstützung für PAM-Funktionen bereitstellen:

Shared Account Password Management (SAPM): Shared Account Password Management ermöglicht die sichere Verwaltung von privilegierten Anmeldeinformationen, einschließlich für Systemkonten, Service-Konten oder Anwendungskonten, die üblicherweise gemeinsam verwendet werden. Im Herzen von SAPM-Produkten steht ein verschlüsselter und gehärteter Passwort-Tresor zur Ablage von Passwords, Schlüsseln und anderen privilegierten Anmeldeinformationen zwecks einer kontrollierten, geprüften und richtlinienbasierten Freigabe und Aktualisierung. Als Basisanforderung unterstützen diese Produkte eine periodische, regelmäßige oder ereignisbasierte Zufallsgenerierung von Passwörtern und anderen Anmeldeinformationen.

Privileged Session Management (PSM): Privileged Session Management ermöglicht die Erstellung einer privilegierten Session in Zielsystemen, einschließlich grundlegendem Auditing und Monitoring von privilegierten Aktivitäten. Darüber hinaus bieten PSM-Tools Authentifizierung, Autorisierung sowie Single Sign-On (SSO) für Zielsysteme.

Application-to-Application Password Management (AAPM): AAPM ist eine Erweiterung von SAPM-Tools und dient zur Verwaltung von Konten, die von Anwendungen oder Systemen zwecks Kommunikation mit anderen Anwendungen oder Systemen (wie z.B. Datenbanken) verwendet werden. Dies umfasst die Nutzung von Service-Konten zur Ausführung bestimmter Funktionen oder zur Auslösung von Prozessen mit den dafür erforderlichen Privilegien für eine erfolgreiche Ausführung.

Mit AAPM-Tools können fest programmierte Anmeldeinformationen im Code von Anwendungen, in Scripts sowie in anderen Konfigurationsdateien eliminiert werden, da sie einen Mechanismus (üblicherweise APIs) bieten, mit dem Anmeldeinformationen auf Anfrage auf sichere Weise bereitgestellt werden können.

Session Recording and Monitoring (SRM): Bei SRM handelt es sich um eine Erweiterung von PSM-Tools, die fortgeschrittenes Auditing, Monitoring sowie die Evaluierung von privilegierten Aktivitäten während einer privilegierten Session bietet, einschließlich — neben weiteren Funktionen — Keystroke-Logging, Aufzeichnung von Video-Sessions, Screen Scraping, OCR-Konvertierung sowie weiterer Technologien zur Überwachung von Sessions.

Controlled Privilege Elevation and Delegation Management (CPEDM): Diese Technologie unterstützt die kontrollierte Erhöhung sowie die richtlinienbasierte Delegierung der Privilegien eines Nutzers zu Super-User-Privilegien zu administrativen Zwecken..

Privileged User Behavior Analytics (PUBA): PUBA verwendet Data-Analytics-Verfahren und erkennt Bedrohungen anhand von anormalem Verhalten im Vergleich zu etablierten Verhaltensprofilen von Administrationsbenutzern sowie Benutzergruppen und Administratorrollen.

Privilege Account Discovery and Lifecycle Management (PADLM): PADLM-Tools nutzen Erkennungsmechanismen, um gemeinsam verwendete Konten, Software-Konten, Service-Konten sowie andere unverschlüsselte/als Klartext vorliegende Anmeldeinformationen innerhalb einer IT-Infrastruktur zu erkennen. Sie bieten Workflow-Funktionen zur Identifizierung und Nachverfolgung der operativen und technischen Eigentümerschaft im Laufe ihres Lebenszyklus und können Statusveränderungen erkennen, Benachrichtigungen auslösen und erforderliche Gegenmaßnahmen ergreifen.

Endpoint Privilege Management (EPM): EPM umfasst Funktionen zur Verwaltung von Bedrohungen in Verbindung mit lokalen Administrationsrechten in Windows, Mac oder auf anderen Endpunkten. Prinzipiell bieten EPM-Tools eine kontrollierte und überwachte Eskalation der Privilegien eines Benutzers auf Endpunkten und beinhalten Funktionen wie das Whitelisting von Anwendungen zum Schutz von Endpunkten. Gemäß unserer Definition umfassen EPM-Lösungen in erster Linie drei verschiedene Technologien:

a. **Application Control**: Mit dieser Technologie können Unternehmen steuern, welche Anwendungen auf einem Endpunkt ausgeführt werden dürfen. Dies erfolgt üblicherweise mittels Whitelisting von Anwendungen — dabei werden nur bekannte, sichere Anwendungen zu einer freigegebenen Liste hinzugefügt und dürfen ausgeführt werden. Application Control bietet einen effektiven Schutz vor den Herausforderungen der Schatten-IT für Unternehmen.
b. **Sandboxing**: Diese Technologie verfolgt den Ansatz, unbekannte Anwendungen oder Programme in Isolation auszuführen, indem der Zugriff auf Ressourcen (bspw. Dateien, Registrys usw.) für diese Anwendungen oder Programme eingeschränkt wird. Diese Technologie, die auch als Application Isolation bekannt ist, bietet einen effektiven Schutz vor Cyberangriffen, indem böswillige Programme in Isolation ausgeführt werden, sodass ihre Möglichkeiten zur Verursachung von Schäden eingeschränkt werden.
c. **Privilege Management:** Diese Technologie umfasst die Verwaltung von Benutzer- sowie Anwendungsprivilegien. Im Hinblick auf User Privileged Management ermöglicht diese Technologie eine kontrollierte und überwachte Erhöhung zu lokalen Admin-Privilegien. In Bezug auf Application Privilege Management bietet sie eine ausnahmen- oder richtlinienbasierte Erhöhung von Administrationsrechten für bekannte und genehmigte Anwendungen, sodass diese erfolgreich ausgeführt werden können.

Privileged Access Governance (PAG): PAG liefert wertvolle Einblicke im Hinblick auf den Status des privilegierten Zugriffs zur Unterstützung des Entscheidungsfindungsprozesses. PAG umfasst privilegierte Zugriffszertifizierungen und ermöglicht individualisierbares Reporting sowie Dashboarding.

Gemäß der bei KuppingerCole verwendeten Definition von PAM-Lösungen bestehen diese aus den Tools und Technologien, die in Abbildung 1 dargestellt sind.

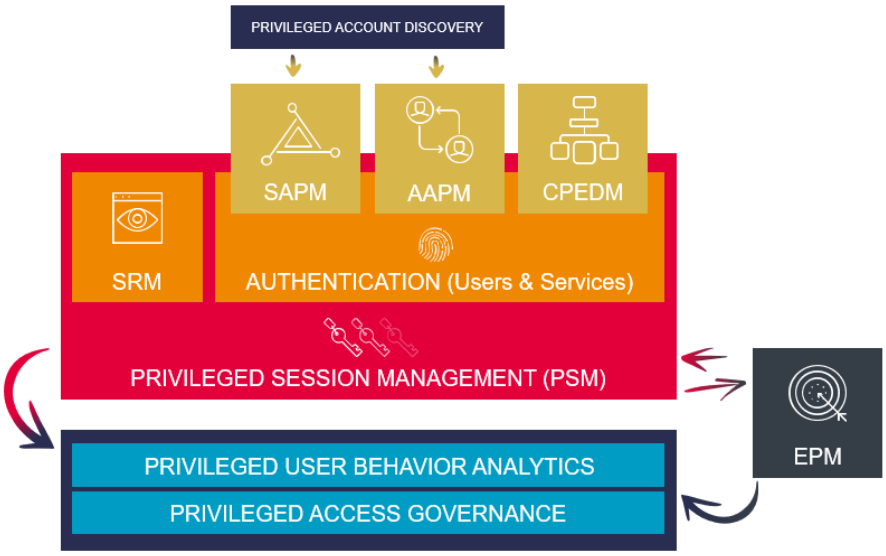


Abbildung 1: Architekturmodell von PAM-Tools und -Technologien

Privileged Account Discovery and Lifecycle Management (PADLM)
Shared Account Password Management (SAPM)
Privileged Session Management (PSM)
Session Recording and Monitoring (SRM)
Privileged User Behavior Analytics (PUBA)
Controlled Privilege Elevation and Delegation Management (CPEDM)
Application-to-Application Password Management (AAPM)
Endpoint Privilege Management (EPM)
Privileged Access Governance (PAG)

Wir betrachten alle Produkttypen, die Kunden dabei unterstützen, die Herausforderungen von Privileged Access Management vollständig oder teilweise zu lösen. Dies umfasst u. a. Session Monitoring & Recording sowie Password Vaults oder Privileged User Behavior Analytics.

Wir beziehen keine Universal-Tools, wie z. B. Identity Provisioning-Tools oder Real Time Security Intelligence, welche die spezifischen Anforderungen im Bereich Privileged Access Management nur sehr bedingt unterstützen. Allerdings ist die Integration mit solchen Lösungen ein Punk auf der Liste der Funktionen, die wir in unserer Analyse als relevant erachten.

Wir suchen insbesondere nach Funktionen in den folgenden Bereichen im Zusammenhang mit privilegiertem Zugriff:

- Shared Account Password Management
- Privileged Single Sign-On (SSO-Zugriff auf mehrere privilegierte Sessions)
- Privileged Account Discovery & Lifecycle Management
- Session Monitoring, Analysis & Recording
- Privileged User Behavior Analytics
- Privilege Elevation Management (Restriction)
- Application-to-Application Password Management
- Endpoint Privilege Management
- Reporting, Audit & Compliance

Wir schätzen integrierte Lösungen mit einer engen Integration der unterschiedlichen Funktionen. Die wichtigsten Funktionen, die wir in den verschiedenen PAM-Bereichen erwarten, umfassen:

- Shared Account Password Management
  - ✓ Password Vaulting
  - ✓ Zentrales Management gemeinsam verwendeter Kontenprivilegien
  - ✓ Automatische Rotation von Anmeldeinformationen oder OTPs
  - ✓ Sicherer Zugriff auf privilegierte Anmeldeinformationen
- Privileged Single Sign-On (SSO-Zugriff auf mehrere privilegierte Sessions)
  - ✓ Einfaches Management von Session-Zuweisungen an Benutzer
  - ✓ Ad-hoc-Zugriff sowie Zugriff mit Vorabgenehmigung, einschließlich Unterstützung für Genehmigungslebenszyklen
  - ✓ Einfache, aber sichere Benutzeroberflächen
- Privileged Account Discovery & Lifecycle Management
  - ✓ Automatische Erkennung von privilegierten Konten auf Servern, Clients und anderen Systemen im Anwendungsbereich (z. B. Netzwerkgeräte)
  - ✓ Integration von CMDBs
  - ✓ Einfache (automatisierte) Gruppierung von Konten und Systemen
- Session Monitoring, Analysis & Recording
  - ✓ Session Monitoring
  - ✓ Session Recording
  - ✓ Session Analysis
  - ✓ All dies sowohl für CMD- als auch GUI-basierte Sessions

- Privileged User Behavior Analytics
  - ✓ Erkennung von Anomalien im Verhalten von privilegierten Benutzern
  - ✓ Anpassung der Analyse an individuelle Anforderungen
  - ✓ Unterstützung für Privacy und Compliance, z. B. 4-Augen-Prinzip bei der Überprüfung von Anomalien
- Privilege Elevation Management (Controlled Privilege Elevation)
  - ✓ Eingeschränkter Zugriff (mit den wenigsten Privilegien) auf verwaltete Systeme
  - ✓ Befehlsfilter
  - ✓ Befehls-/Shell-Substitution
- Application-to-Application Password Management
  - ✓ Identifizierung von fest programmierten Anmeldeinformationen in Scripts, Konfigurationsdateien usw.
  - ✓ APIs als Ersatz für fest programmierte Anmeldeinformationen
  - ✓ Anwendungs- oder Service-Authentifizierung mittels Password Vault zwecks Checkout oder Injection von Anmeldeinformationen
- Endpoint Privilege Management
  - ✓ Application Control (Whitelisting/Blacklisting-Funktionen)
  - ✓ Application Sandboxing (Ausführung von nicht oder weniger vertrauenswürdigen Anwendungen in einer kontrollierten Umgebung)
  - ✓ Erhöhung von Privilegien lokaler Benutzer
- Reporting, Audit & Compliance
  - ✓ Flexible Reporting-Schnittstellen, anpassbar

Eng integrierte Lösungen, die alle wichtigen Funktionen abdecken, sind eines der wichtigsten Kriterien auf unserer Liste, denn Kunden bevorzugen integrierte Ansätze im Vergleich zu einzelnen, nicht integrierten oder nur lose miteinander gekoppelten Lösungen.

Wir legen besonderes Augenmerk auf die Integration in vorhandene Sicherheitsinfrastrukturen, um konsolidiertes Monitoring, Analytics, Governance oder Compliance für verschiedene Arten von Informationsspeichern und Anwendungen zu ermöglichen. Dies umfasst in erster Linie die Integration mit SIEM-/SoC-Lösungen, vorhandene Systeme für Identity & Access Management sowie Technologien für Security Governance.

Darüber hinaus betrachten wir die folgenden zusätzlichen architektonischen und operativen Aspekte in unserer Anbieterbewertung:

- Unterstützung für eine große Zahl von Zielsystemen
- Unterstützung für Cloud-Services und -Plattformen
- Mehrmandantenfähigkeit
- Unterstützung für High Availability (HA) sowie automatisierte Failover-Konfigurationen
- Einfache Integration mit Sicherheitslösungen von Drittanbietern, einschließlich ITSM, SIEM usw.
- Bereitstellungsformate: Hardware oder Virtual Appliances, PAM-as-a-Service oder verwaltete Host-Services
- Bereitstellungstypen: Agent oder Netzwerk-Proxy/Gateway-basiert, Remote Passive Monitoring Scalability und Performance Impact
- Einfache Implementierung und Erstkonfiguration, einschließlich Reibung im Hinblick auf administratives Verhalten
- Flexibilität und Benutzerfreundlichkeit der Management-Konsole und der Benutzeroberfläche im Allgemeinen

2 Leadership

Die Auswahl eines Produkt- oder Serviceanbieters sollte nicht ausschließlich auf der vergleichenden Bewertung in einem KuppingerCole Leadership Compass basieren. Der Leadership Compass bietet einen Vergleich auf der Grundlage standardisierter Kriterien und kann dabei helfen, Anbieter zu identifizieren, die genauer in Augenschein genommen werden sollten. Allerdings erfordert eine fundierte Auswahl eine nachfolgende Detailanalyse sowie eine Pilotphase als Proof of Concept auf der Grundlage der spezifischen Kriterien des Kunden.

Vor dem Hintergrund unserer Analyse der Produkte eines Anbieters erstellen wir mehrere Leadership-Bewertungen, auf die Unternehmen bei ihrer Produktevaluierung zurückgreifen können. Die Bewertung bezüglich Overall Leadership bietet einen kombinierte Übersicht über die Bewertungen bezüglich:

- Product Leadership
- Innovation Leadership
- Market Leadership

Abbildung 2: Overall Leadership im Marktsegment Privileged Access Management

Bei der Betrachtung des Leader-Segments in der Bewertung bezüglich Overall Leadership ergibt sich ein Bild, das typisch für Märkte ist, die sich noch in der Entwicklung befinden — es gibt weniger Anbieter im Leader-Segment als im Challenger-Segment. Nachdem der Markt im vergangenen Jahr um 3 bis 4 neue Anbieter gewachsen ist, ist er nun übervoll. Wir haben ca. 20 Anbieter für unseren Leadership Compass ausgewählt, sowie 10 weitere zu erwähnende Anbieter im Abschnitt „Vielversprechende Anbieter", welche die Teilnahme abgelehnt oder unsere grundlegenden Evaluationskriterien nicht erfüllt haben.

CyberArk behält seine führende Position in der Bewertung des PAM-Markts bezüglich Overall Leadership bei, jedoch dicht gefolgt von BeyondTrust. Nach signifikanten Optimierungen bezüglich ihrer Produktstrategien und Partnerschaften machen Centrify und Thycotic einen großen Schritt nach vorne, gefolgt von CA Technologies mit . One Identity hat seine führende Position unter den etablierten PAM-Akteuren nach kürzlichen Änderungen an seiner Produktarchitektur in Kombination mit Marketingmaßnahmen wieder eingenommen.

Dank eines stärkeren Fokus auf Prozessinnovation und Privileged Access Governance platziert HitachiID sich im Segment der Challenger, dicht gefolgt von WALLIX. ARCON, das sich im Challenger-Segment einen beachtlichen Vorsprung vor Micro Focus und EmpowerID gesichert hat., ist ihnen auf den Fersen.

Zu den weiteren Anbietern im Challenger-Segment zählen ManageEngine und SSH.COM — beide machen dank ihrer verbesserten Bewertung bezüglich Marktpräsenz und Partnerschaftsökosystemen einen deutlichen Schritt nach vorne in das Challenger-Segment.

MT4 Networks, Osirium und Fudo Security platzieren sich mit ihren zielgerichteten PAM-Funktionen neben dem Challenger-Segment.

Krontech, iSprint und Sectona befinden sich im Followers-Segment, da sie entweder sehr neu auf dem Markt sind und noch dabei sind, im Markt Fuß zu fassen, oder weil ihre Herangehensweise an den PAM-Markt angesichts der PAM-Anforderungen der Kunden nicht besonders relevant ist.

Overall Leaders (in alphabetischer Reihenfolge):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- One Identity
- Thycotic

Die erste der drei spezifischen Leadership-Bewertungen bezieht sich auf Product Leadership. Diese Darstellung basiert hauptsächlich auf der Analyse von Produkt-/Servicefunktionen sowie der allgemeinen Fähigkeiten der unterschiedlichen Produkte/Services.

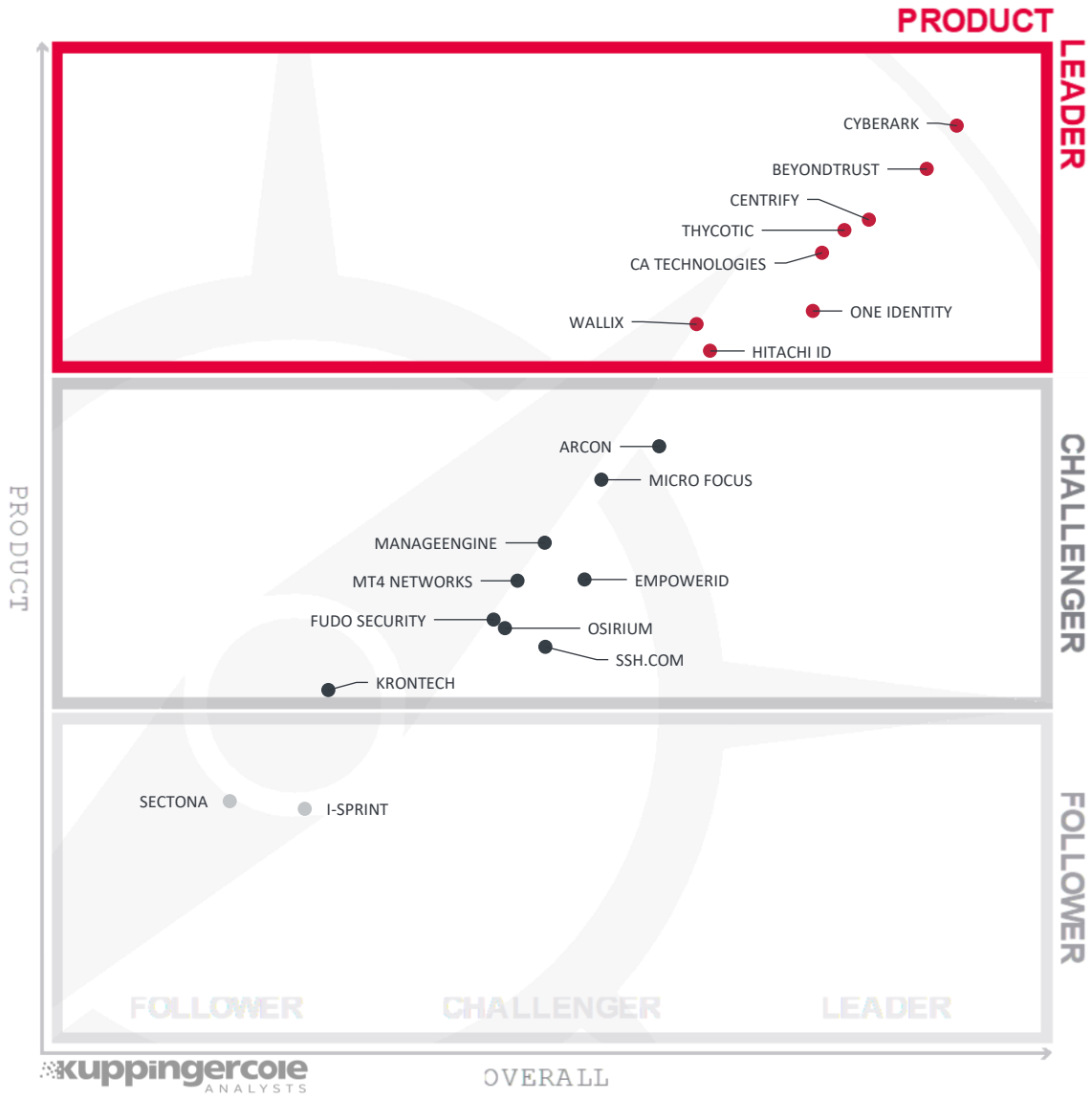


Abbildung 3: Product Leaders im Marktsegment Privileged Access Management

Die Bewertung in Bezug auf Product Leadership basiert im Besonderen auf der funktionalen Stärke und der Vollständigkeit der Produkte. Hier konnten einige weitere Anbieter sich im Leader-Segment positionieren. Der führende Anbieter ist erneut CyberArk, gefolgt von BeyondTrust. Beide verfügen über umfassende, allgemeine Funktionen, die eine starke Grundlage für die Implementierung von Privilege Access Management bieten.

Hinter diesen beiden Leadern folgen Centrify und Thycotic, die ebenfalls starke und funktional umfassende PAM-Produkte auf dem Markt anbieten. Als nächstes finden wir den Anbieter CA Technologies, der seine relative Position im Segment der Product Leaders aufgrund von Unklarheiten im Zusammenhang mit seiner Übernahme von Broadcom verloren hat. Der nächste Anbieter im Leader-Segment ist WALLIX, welcher sich von einem Point-Anbieter zu einem Suite-Anbieter weiterentwickelt hat und eine starke Alternative zu den führenden Anbietern darstellt. Zu guter Letzt konnte sich auch HitachiIDim Leaders-Segment positionieren — dieser Anbieter hat dank seiner PAM-Funktionen sowie der engen Integration mit seinem Identity Manager einen Schritt nach vorne gemacht.

ARCON und Micro Focus befinden sich im oberen Bereich des Challenger-Segments, gefolgt von ManageEngine, MT4 Networks und EmpowerID als Gruppe. All diese Anbieter verfügen über starke PAM-Funktionen, die gut für die spezifischen PAM-Anforderungen von Kunden geeignet sein können. Fudo Security, Osirium, SSH.COM und Krontech haben spezifische Stärken, weisen aber noch gewisse Lücken hinsichtlich der Tiefe und Breite der unterstützten Funktionen auf. Deshalb liegen sie etwas zurück im Challenger-Segment.

Schließlich folgen Sectona und iSprint im Followers-Segment — all diese Anbieter haben relativ neue PAM-Produkte und sind noch mit der Ausführung ihrer PAM-Produkt-Roadmap befasst.

Product Leader (in alphabetischer Reihenfolge):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Hitachi-ID
- One Identity
- Thycotic
- WALLIX

Ein weiterer Aspekt, den wir bei der Bewertung von Produkten/Services in Betracht ziehen, sind Innovationen. Unserer Ansicht nach stellen Innovationen eine Schlüsselfunktion in IT-Marktsegmenten dar. Kunden benötigen Innovationen, um mit der stetigen Weiterentwicklung und neuen Herausforderungen Schritt zu halten. Innovationen beschränken sich nicht auf die regelmäßige Bereitstellung neuer Releases, sondernfolgen einem kundenorientierten Upgrade-Ansatz, der die Kompatibilität mit früheren Versionen — insbesondere auf API-Ebene — sicherstellt, und sie umfassen neue, hochmoderne Funktionen, welche neue Kundenanforderungen erfüllen.

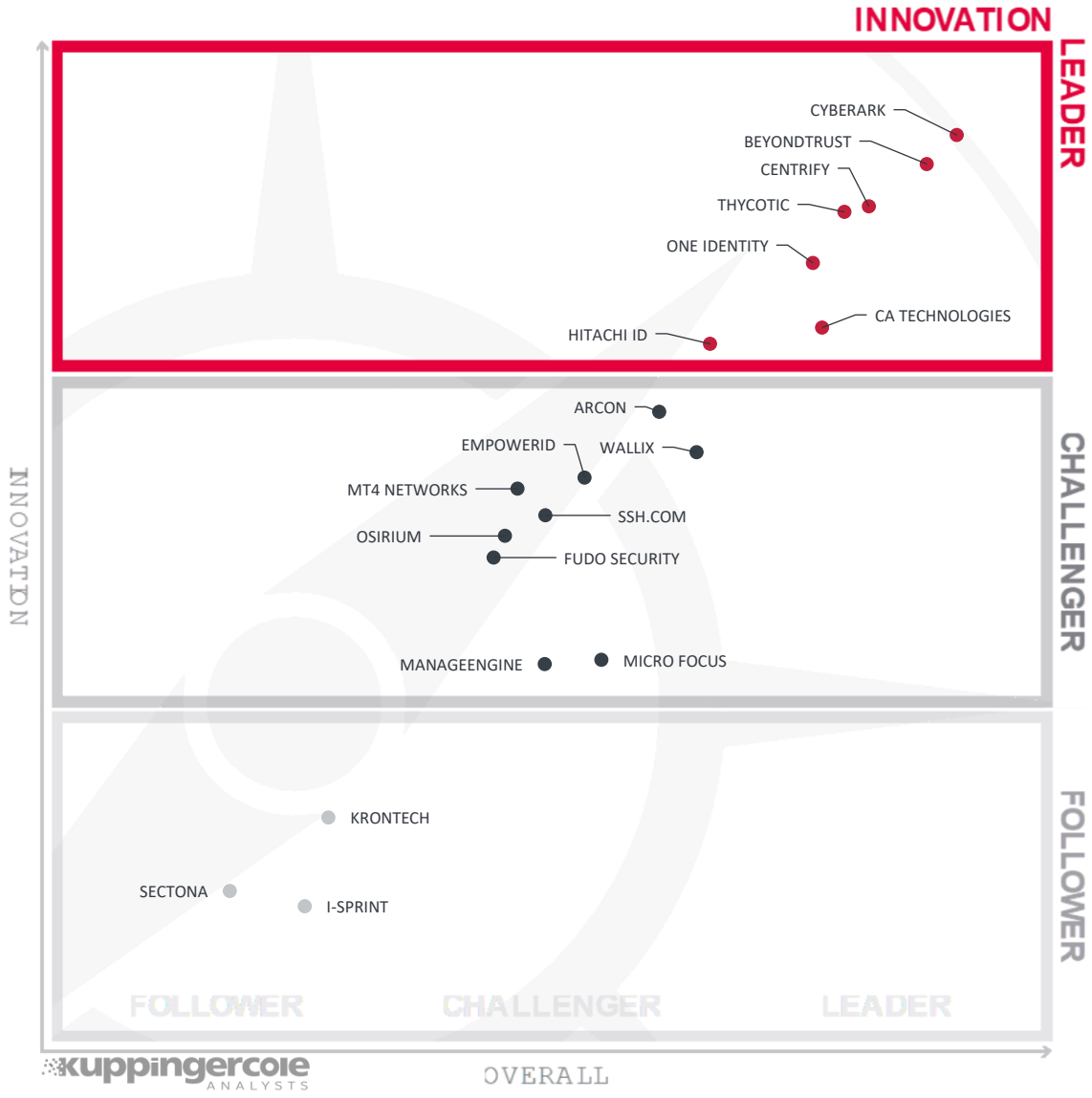


Abbildung 4: Innovation Leaders im Marktsegment Privileged Access Management

Im Hinblick auf Innovation Leadership zeigt sich ein anderes Bild. Während die meisten Anbieter immer noch Lücken im Hinblick auf den Funktionsumfang aufweisen, was sich auf ihre Bewertung bezüglich der Product Leadership auswirkt, stecken sie sehr viel Arbeit in innovative Funktionsbereiche. Deshalb finden sich viele Anbieter im Segment der Innovation Leader.

Erneut steht CyberArk dank seines Fokus auf konstante Innovationen in einer schwierigen Betriebsumgebung an der Spitze. Mit einigem Abstand zu CyberArk folgt BeyondTrust, das intern auch eine gute Kultur für organische Innovationen aufwies, aber durch kürzliche Übernahme- und Fusionsaktivitäten beeinträchtigt wurde. Es folgen Centrify und Thycotic, die nahe beieinander liegen, was ihren im Vergleich zu ihren Wettbewerbern gesteigerten Fokus auf Innovationen aufzeigt. Auf dem nächsten Platz steht One Identity, das eine beeindruckende und innovative Produkt-Roadmap verfolgt und seinen Kunden erfolgreich Mehrwert bietet. Dahinter finden sich CA Technologies und HitachiID, die über ein gutes Verständnis des Markts verfügen und in relevanten Bereichen nach wie vor innovativ sind.

Im oberen Bereich des Segments der Challenger in Bezug auf Innovation Leadership konnten sich ARCON und WALLIXpositionieren. Es folgen EmpowerID, MT4 Networks und SSH.COM, Osirium sowie Fudo Security — all diese Anbieter setzen sich stark für technologische Innovationen ein, bleiben aber im Hinblick auf den erwarteten Mehrwert für Kunden hinter den höher bewerteten Anbietern zurück. Weiter unten im Segment der Challenger finden sich Micro Focus und ManageEngine. Beide verfügen über breitere Sicherheitsportfolios und haben einige Fortschritte gemacht, konzentrieren sich angesichts ihrer Marktpräsenz aber immer noch relativ wenig auf PAM-Innovationen.

Krontech, Sectona und iSprint platzieren sich im Segment der Follower — allen diesen Anbietern ist es bisher nicht gelungen, ein ausreichendes Verständnis für Marktinnovationen zu zeigen.

Schließlich gibt es noch einen Anbieter im Segment der Follower — ManageEngine. Die Zielgruppe dieses Anbieters ist der KMU-Markt, und er zeigt nicht das gleiche Maß an Innovation wie andere Anbieter.

Innovation Leader (in alphabetischer Reihenfolge):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Hitachi ID Systems
- One Identity
- Thycotic

Zu guter Letzt betrachten wir den Bereich Market Leadership, d. h. die Anzahl der Kunden, das Partnerökosystem, die globale Reichweite sowie weitere Faktoren, welche die Führungsrolle in einem Markt beeinflussen. Nach unserer Ansicht erfordert Market Leadership eine globale Reichweite.

Abbildung 5: Market Leaders im Marktsegment Privileged Access Management

Hier hat CyberArk die Führung im Segment der Leaders übernommen. In den letzten Jahren hat CyberArk sich als prominentester Anbieter auf dem Markt für Privileged Access Management etabliert. CyberArk wird dicht gefolgt von BeyondTrust, das aufgrund seiner kürzlichen Übernahme durch Bomgar einen guten Sprung vorwärts in Bezug auf die Marktposition machen konnte. CA Technologies ist ein weiterer großer Softwareanbieter, dessen PAM-Produkt einen signifikanten Kundenstamm aufweist und der über ein bemerkenswert großes und etabliertes Partnerökosystem mit globaler Reichweite verfügt. Als nächstes folgen Centrify und One Identity, die jeweils ein selektives, aber insgesamt starkes Partnerökosystem sowie einen wachsenden Kundenstamm besitzen.

Durch die Partnerschaft mit IBM konnte Thycotic seine Marktposition ausbauen, während Micro Focus von HPE dabei unterstützt wird, sein Partnerökosystem auszubauen und zu festigen.

WALLIX und HitachiID haben sich am oberen Ende des Challenger-Segments positioniert, dicht gefolgt von ManageEngine, ARCON, EmpowerID und SSH.COM. Des Weiteren finden sich Osirium, Fudo Security, MT4 Networks und i-Sprint im Challenger-Segment — diese Anbieter verfügen entweder nicht über ein globales Partnerökosystem oder weisen eine unterdurchschnittliche Anzahl von Implementierungen auf.

Aufgrund ihrer eingeschränkten Marktreichweite und Zukunftsprognosen bevölkern Krontech und Sectona das Follower-Segment.

Market Leader (in alphabetischer Reihenfolge):

- BeyondTrust
- CA Technologies
- Centrify
- CyberArk
- Micro Focus
- One Identity
- Thycotic

3 Korrelierte Ansicht

Während die Leadership-Diagramme führende Unternehmen in verschiedenen Kategorien aufzeigen, suchen viele Kunden beispielsweise nicht nur nach einem Product Leader, sondern nach einem Anbieter mit einer Lösung, die sowohl funktionsreich ist als auch stetig verbessert wird. Eine solche Lösung hätte eine starke Position im Hinblick auf Product Leadership sowie in Bezug auf Innovation Leadership inne. Deshalb stellen wir zusätzliche Analysen bereit, die verschiedene Leadership-Kategorien miteinander korreliert und mehr Informationen und Einblicke bieten.

3.1 Markt-/Produktmatrix

Die erste dieser korrelierten Ansichten bezieht sich auf Product Leadership und Market Leadership.

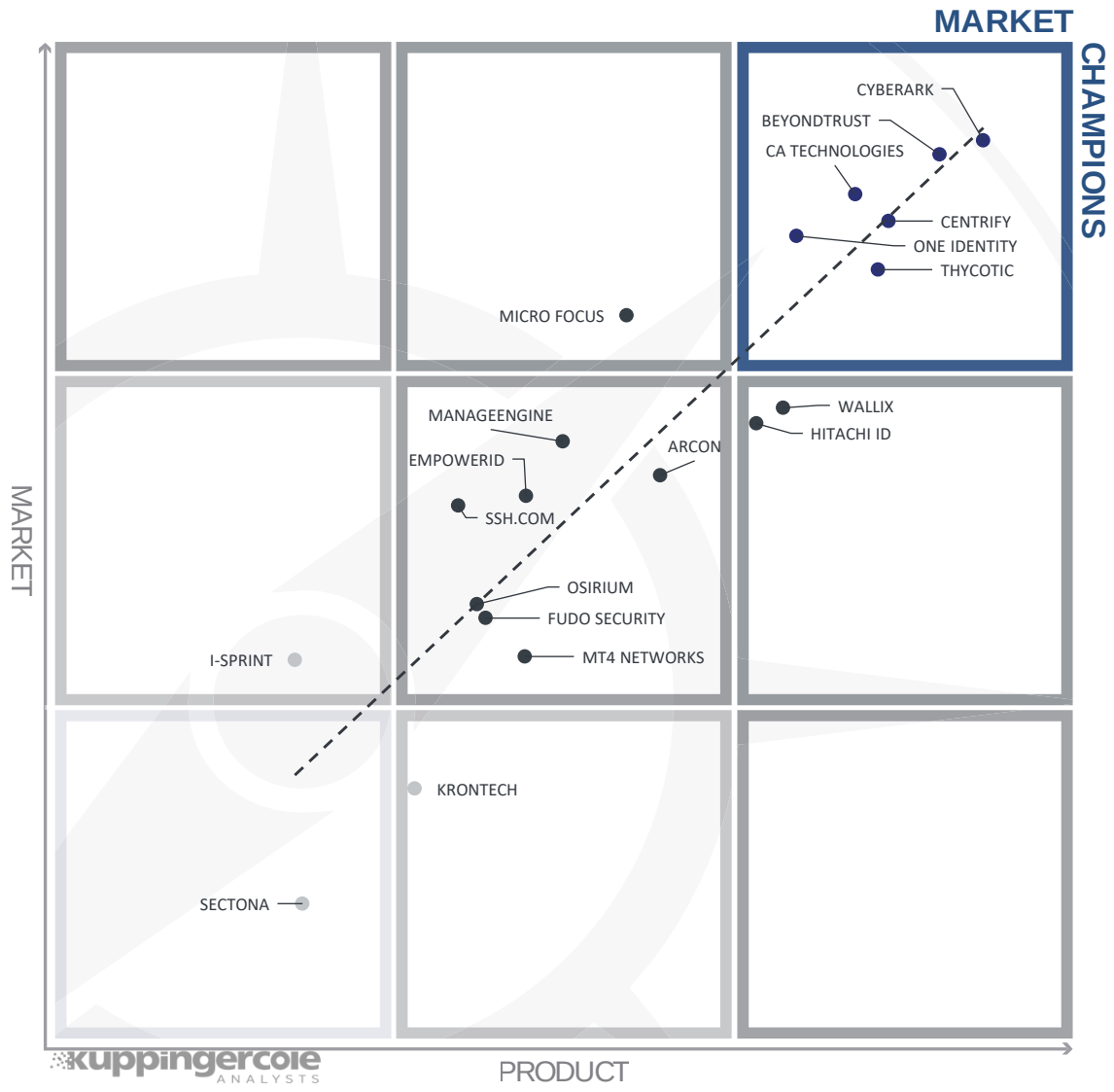


Abbildung 6: Markt-/Produktmatrix Anbieter, die unterhalb der Linie angesiedelt sind, haben eine schwächere Marktposition als auf der Grundlage der Ausgereiftheit ihrer Produkte zu erwarten wäre. Oberhalb der Linie angesiedelte Anbieter hingegen sind sozusagen „Überflieger", wenn man die Bewertungen in Bezug auf Market Leadership sowie Product Leadership miteinander vergleicht.

Dieser Vergleich zeigt anschaulich, welche Anbieter in unserer Analyse in Bezug auf Product Leadership eine bessere Position erreicht haben als in Bezug auf die Analyse der Market Leadership. Je weiter ein Anbieter in der oberen rechten Ecke angesiedelt ist, desto besser ist seine kombinierte Position. Bei Anbietern oberhalb der Linie handelt es sich sozusagen um „Überflieger" auf dem Markt. Es ist nicht überraschend, dass es sich dabei hauptsächlich um sehr große Anbieter handelt, während die Anbieter unterhalb der Linie noch nicht so fest auf dem Markt etabliert sind, aber im Allgemeinen umfassende und innovative Funktionen bieten.

Die Matrix zeigt ein Bild, das typisch für sich entwickelnde Marktsegmente ist — mit einer eher breiten Verteilung der verschiedenen Akteure auf die einzelnen Quadranten und einer eher schwachen Korrelation zwischen Market Leadership und Product Leadership.

Im oberen rechten Kasten befinden sich CyberArk, BeyondTrust, CA Technologies, Centrify, One Identity und Thycotic. Diese Anbieter führen sowohl die Produkt- als auch die Marktbewertung an.

Im linken Kasten hat sich Micro Focus positioniert, dessen Bewertung in Bezug auf Market Leadership besser als sein Rang im Hinblick auf Product Leadership ist.

Im Kasten darunter liegen HitachiID und WALLIX — dies weist auf ihre höheren Qualitäten im Bereich Product Leadership im Vergleich zu Market Leadership hin.

Im mittleren Kasten sind (in alphabetischer Reihenfolge) ARCON, EmpowerID, Fudo Security, ManageEngine, MT4 Networks, Osirium und SSH.COM angesiedelt — alle diese Anbieter verfügen über respektable Positionen in Bezug auf Product und Market Leadership und stellen deshalb interessante Alternativen zu den führenden Anbietern dar.

Schließlich befinden i-Sprint, Krontech und Sectona sich in den Kästen am unteren Ende des Diagramms. Dies weist auf niedrigere Ränge in Bezug auf Product und Market Leadership hin.

3.2 Produkt-/Innovationsmatrix

Die zweite Ansicht stellt die Aspekte Product Leadership und Innovation Leadership in Relation zueinander. Es ist nicht überraschend, dass es bis auf wenige Ausnahmen eine relativ gute Korrelation zwischen diesen beiden Aspekten gibt. Diese Verteilung und Korrelation sind typisch für die meisten Märkte mit einer signifikanten Anzahl etablierter Anbieter sowie einigen kleineren Akteuren.

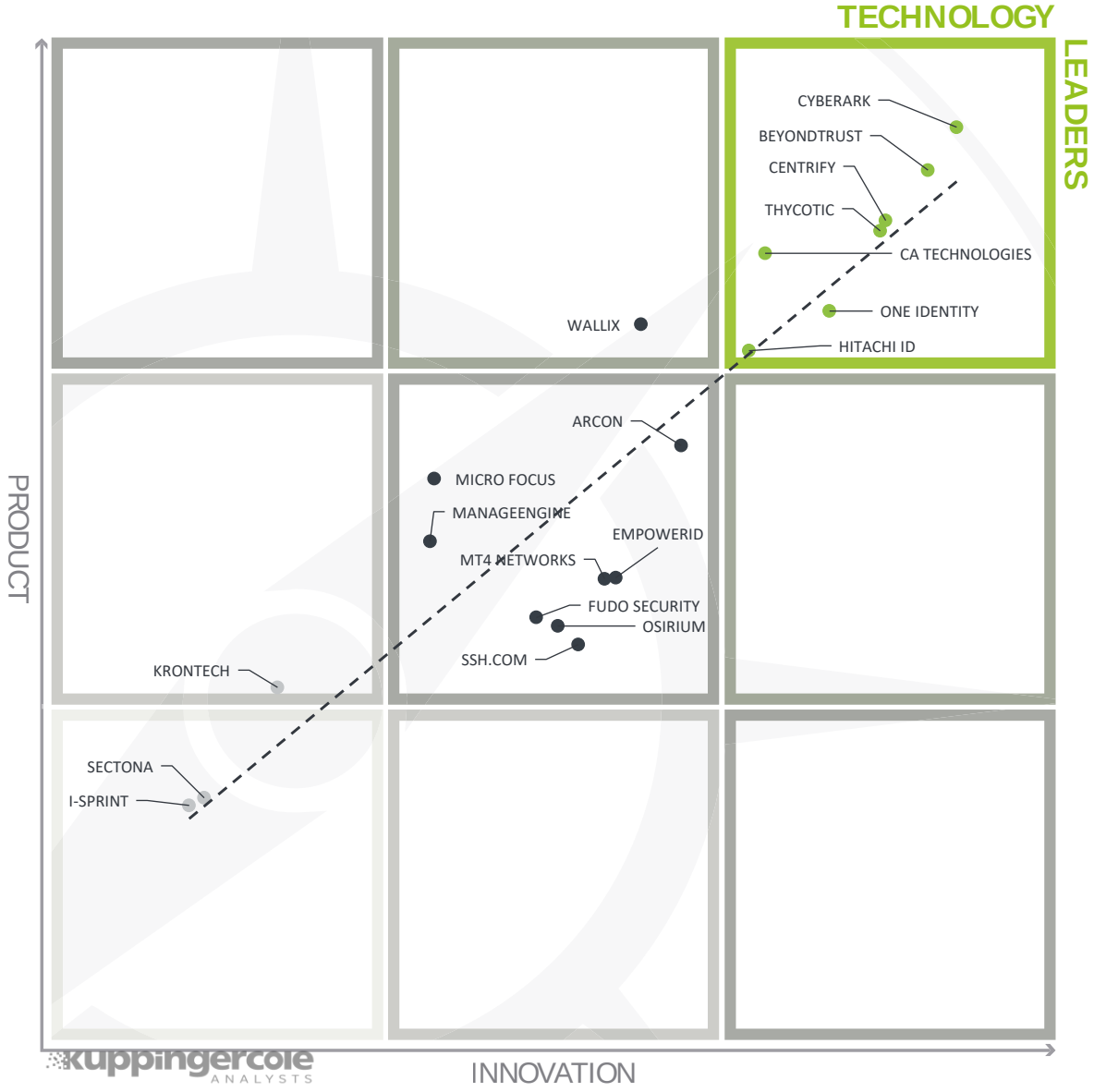


Abbildung 7: Produkt-/Innovationsmatrix Anbieter unterhalb der Linie sind weniger innovativ, während Anbieter oberhalb der Linie im Vergleich zu ihrer aktuellen Position bezüglich Product Leadership innovativer sind.

Hier ist eine gute Korrelation zwischen den Bewertungen in Bezug auf Product und Innovation Leadership erkennbar. Dabei liegen die meisten Anbieter nahe der gepunkteten Linie, die eine gesunde Mischung aus Product und Innovation Leadership im Markt darstellt. Im Segment der Technology Leaders befinden sich die meisten der führenden Anbieter in der oberen rechten Ecke, großflächig im gesamten Kasten verteilt.

Die am besten positionierten Anbieter sind CyberArk, BeyondTrust, CA Technologies, Centrify, HitachiID, One Identity und Thycotic — sie alle liegen nahe der Line, die ein gutes Gleichgewicht zwischen Produktfunktionen und Innovationen beschreibt. CA Technologies liegt etwas entfernt oberhalb der Linie, was einen stärkeren Fokus auf Product Leadership im Vergleich zu Innovation Leadership bedeutet.

Im linken Kasten hat sich WALLIX positioniert — hier liegt der Fokus mehr auf Product als auf Innovation Leadership im PAM-Markt.

Im gleichen Kasten und in der Nähe der Linie liegen RSA Security und Beta Systems, die Technology Leaders sind und ein gutes Gleichgewicht zwischen Produkt- und Innovationsstärke bieten.

Unter dem Kasten der Technology Leaders und in der Mitte des Diagramms sind ARCON, EmpowerID, Fudo Security, ManageEngine, Micro Focus, MT4 Networks, Osirium und SSH.COM angesiedelt, die sowohl im Hinblick auf Product Leaderships als auch im Hinblick auf Innovation Leadership Challenger darstellen.

Schließlich befinden i-Sprint, Krontech und Sectona sich in den Kästen am unteren Ende des Diagramms, was auf niedrigere Ränge in Bezug auf Product und Innovation Leadership hindeutet.

3.3 Innovations-/Marktmatrix

In der dritten Matrix ist das Verhältnis zwischen Innovation Leadership und Market Leadership dargestellt. Manche Anbieter verfügen über eine gute Marktposition, ohne Innovation Leader zu sein. Dies stellt möglicherweise eine Gefahr für die zukünftige Marktposition dieser Anbieter dar, je nachdem, ob sie ihre Position in Bezug auf Innovation Leadership verbessern können. Andererseits haben besonders innovative Anbieter gute Chancen, ihre Marktposition zu verbessern, aber sie könnten auch einen Bankrott erleiden. Diese Gefahr besteht insbesondere bei kleineren Anbietern.

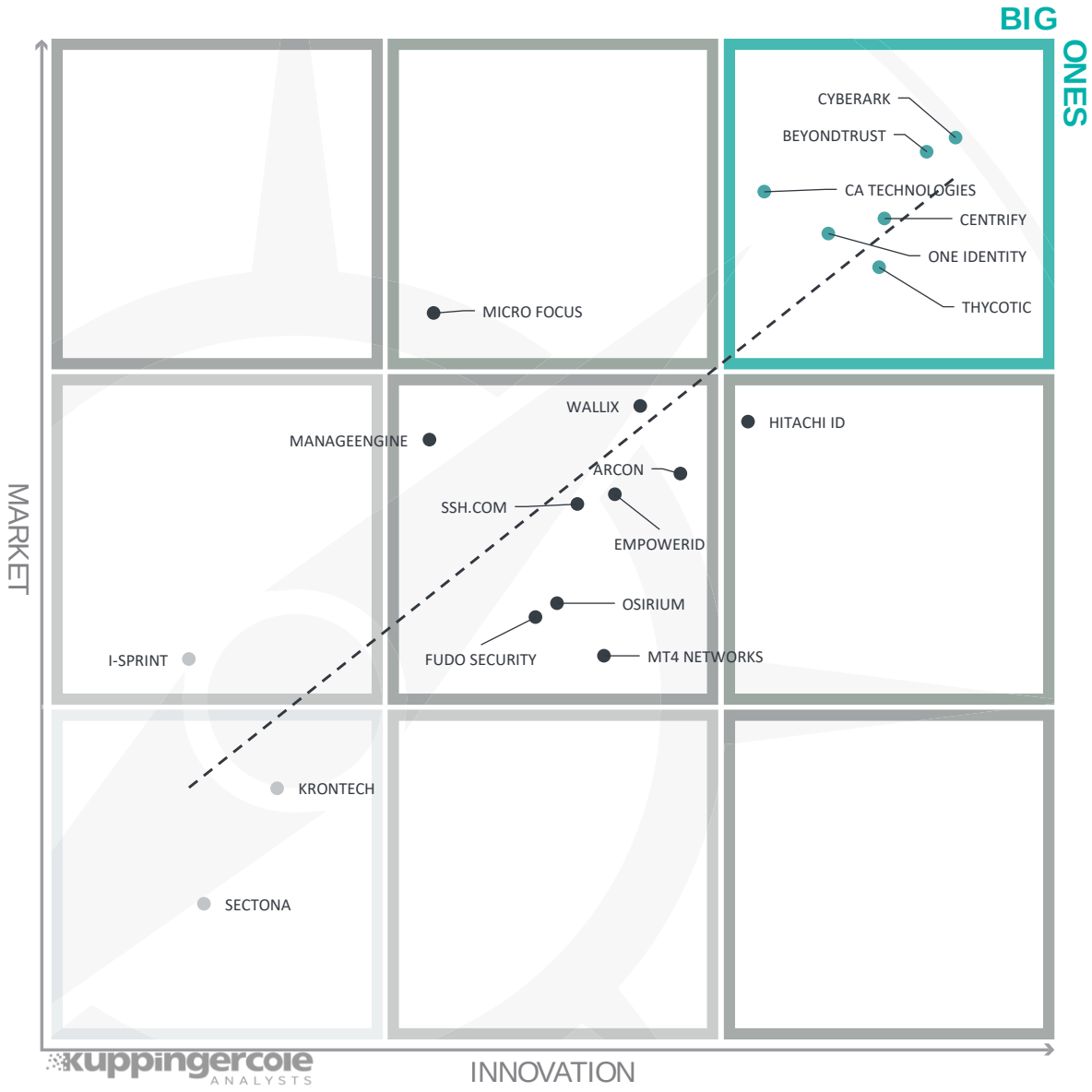


Abbildung 8: Innovations-/Marktmatrix

Anbieter oberhalb der Linie verfügen im Vergleich zu ihrer relativ schwachen Position in Bezug auf Innovation Leadership über eine gute Marktposition, während Anbieter unterhalb der Linie vor dem Hintergrund ihrer Innovationsfähigkeit das größte Potential für eine Verbesserung ihrer Marktposition aufweisen.

Im oberen rechten Kasten sind CyberArk, BeyondTrust, CA Technologies, Centrify, One Identity und Thycotic angesiedelt, die alle im Markt erfolgreich sind, aber auch eine hohe Innovationskraft aufweisen.

Links von ihnen liegt — etwas von der Linie entfernt — Micro Focus aufgrund seines starken Marktfokus, aber eingeschränkten Innovationsfähigkeit. Im Kasten unterhalb der Leader hat sich HitachiID etabliert, das im Vergleich zu seiner Market Leadership-Bewertung über eine bessere Innovationsbewertung verfügt und dadurch ein stärkeres Wachstumspotenzial aufweist.

Im mittleren Kasten sind weitere Challenger angesiedelt — ARCON, EmpowerID, Fudo Security, ManageEngine, MT4 Networks, Osirium, SSH.COM und WALLIX.

Schließlich befinden i-Sprint, Krontech und Sectona sich in den Kästen am unteren Ende des Diagramms. Dies liegt in ihren eingeschränkten Bewertungen in Bezug auf Market Leadership sowie Innovation Leadership begründet, wobei i-Sprint über eine bessere Market Leadership-Bewertung als die anderen beiden Anbieter verfügt.

4 Produkte und Anbieter auf einen Blick

Dieser Abschnitt bietet einen Überblick über die verschiedenen Produkte, die wir im Rahmen dieses KuppingerCole Leadership Compass zu Privileged Access Management analysiert haben. Neben der Bewertungsübersicht bieten wir noch weitere Vergleiche, in denen wir die Aspekte Product Leadership, Innovation Leadership und Market Leadership in Relation zueinander setzen. Dies ermöglicht beispielsweise die Identifizierung von höchst innovativen, aber spezialisierten Anbietern oder lokalen Akteuren, die starke Produktfunktionen bieten, aber noch nicht über eine globale Marktpräsenz und einen großen Kundenstamm verfügen.

4.1 Bewertungen auf einen Blick

Eine vergleichende Übersicht aller in diesem Dokument bewerteten Produkte auf der Grundlage unserer Evaluation finden Sie in Tabelle 1.

Produkt	Sicherheit	Funktionalität	Integration	Kompatibilität	Usability
ARCON	positiv	positiv	sehr positiv	positiv	sehr positiv
BeyondTrust	sehr positiv	sehr positiv	positiv	sehr positiv	sehr positiv
CA Technologies	sehr positiv	sehr positiv	positiv	positiv	sehr positiv
Centrify	sehr positiv	positiv	sehr positiv	sehr positiv	sehr positiv
CyberArk	sehr positiv	sehr positiv	sehr positiv	sehr positiv	sehr positiv
EmpowerID	positiv	neutral	sehr positiv	positiv	positiv
FUDO Security	positiv	positiv	neutral	neutral	positiv
Hitachi ID	sehr positiv	sehr positiv	sehr positiv	sehr positiv	positiv
I-Sprint	neutral	positiv	neutral	schwach	positiv
Krontech	neutral	positiv	neutral	neutral	neutral
ManageEngine	positiv	positiv	positiv	positiv	sehr positiv
Micro Focus	positiv	positiv	positiv	positiv	positiv
MT4 Networks	positiv	sehr positiv	positiv	neutral	positiv
One Identity	positiv	sehr positiv	positiv	positiv	sehr positiv
Osirium	positiv	neutral	positiv	neutral	positiv
Sectona	neutral	neutral	neutral	neutral	neutral
SSH.COM	positiv	neutral	positiv	positiv	neutral
Thycotic	sehr positiv	sehr positiv	sehr positiv	positiv	sehr positiv
WALLIX	sehr positiv	sehr positiv	positiv	positiv	sehr positiv

Tabelle 1: Vergleichsübersicht der Bewertungen der Produktfunktionen

Zusätzlich bieten wir in Tabelle 2 jeweils vier weitere Bewertungen zu den Anbietern, die über die im vorherigen Abschnitt vorgestellte Produktübersicht hinausgehen. Während die Bewertung der Finanzstärke sich auf den Anbieter bezieht, beziehen die anderen Bewertungen sich auf das Produkt.

Anbieter	Innovationskraft	Marktposition	Finanzstärke	Netzwerk
ARCON	sehr positiv	positiv	positiv	positiv
BeyondTrust	sehr positiv	sehr positiv	sehr positiv	sehr positiv
CA Technologies	positiv	sehr positiv	sehr positiv	sehr positiv
Centrify	sehr positiv	sehr positiv	sehr positiv	sehr positiv
CyberArk	sehr positiv	sehr positiv	sehr positiv	sehr positiv
EmpowerID	positiv	positiv	positiv	positiv
FUDO Security	neutral	positiv	positiv	neutral
Hitachi ID	sehr positiv	positiv	sehr positiv	positiv
I-Sprint	neutral	neutral	positiv	positiv
Krontech	neutral	neutral	positiv	schwach
ManageEngine	neutral	sehr positiv	sehr positiv	positiv
Micro Focus	neutral	sehr positiv	sehr positiv	sehr positiv
MT4 Networks	positiv	neutral	positiv	positiv
One Identity	sehr positiv	sehr positiv	sehr positiv	positiv
Osirium	positiv	neutral	neutral	positiv
Sectona	neutral	schwach	neutral	neutral
SSH.COM	positiv	positiv	positiv	sehr positiv
Thycotic	sehr positiv	sehr positiv	sehr positiv	sehr positiv
WALLIX	positiv	positiv	positiv	sehr positiv

Tabelle 2: Vergleichsübersicht der Anbieterbewertungen

Tabelle 2 erfordert zusätzliche Erläuterungen zur Bewertung „Sehr schwach”:

In Bezug auf die Innovationsfähigkeit weist diese Bewertung darauf hin, dass der jeweilige Anbieter keine oder nur sehr wenige der höher entwickelten Funktionen bietet, nach denen wir in dieser Analyse gesucht haben, wie beispielsweise Unterstützung für DevOps, Privileged User Behavior Analytics, integrierte Privileged Access Governance, Mehrmandantenfähigkeit und integrierte High Availability.

Im Hinblick auf die Marktposition bedeutet diese Bewertung, dass ein Anbieter nur eine sehr einschränkte Sichtbarkeit außerhalb oder sogar innerhalb von regionalen Märkten, wie Frankreich oder Deutschland, aufweist. Üblicherweise ist in diesem Fall auch die Anzahl bestehender Kunden gering.

Bezüglich der Finanzstärke wird diese Bewertung vergeben, wenn keine Informationen über die Finanzstärke vorliegen oder wenn ein Anbieter über einen sehr begrenzten Kundenstamm verfügt. Es gelten jedoch noch weitere Kriterien. Dies bedeutet nicht, dass der jeweilige Anbieter sich in einer kritischen finanziellen Lage befindet, allerdings ist das Potenzial für umfangreiche Investitionen für schnelles Wachstum augenscheinlich begrenzt. Andererseits ist es auch möglich, dass Anbieter mit einer guten Bewertung zahlungsunfähig werden und vom Markt verschwinden.

Schließlich wird in Bezug auf das Partnernetzwerk die Bewertung "kritisch" verwendet, wenn ein Anbieter über kein oder nur ein sehr eingeschränktes Partnernetzwerk in Bezug auf die Anzahl der Partner und die regionale Präsenz verfügt. Dies ist möglicherweise in den Unternehmensrichtlinien begründet, um das eigene Beratungs- und Systemintegrationsgeschäft zu schützen. Wir sind jedoch fest davon überzeugt, dass ein erfolgreicher Markteintritt und das Wachstum von Unternehmen in einem Segment von starken Partnerschaften abhängen.

5 Produkt-/Service-Evaluierung

Dieser Abschnitt enthält eine kurze Bewertung für jedes im Rahmen dieses KuppingerCole Leadership Compass analysierte Produkt/jeden analysierten Service. Für viele dieser Produkte sind zusätzliche KuppingerCole Product Reports und Executive Views verfügbar, die detaillierte Informationen bieten.

5.1 ARCON

Mit der ARCON Privilege Account Management Suite des im indischen Mumbai ansässigen Unternehmens ARCON kann der privilegierte Zugriff in heterogenen IT-Systemen verwaltet werden. Die Privileged Account Management Suite von ARCON wird als Bündel verschiedener Module bereitgestellt, die getrennt lizenziert und als Software-, Virtual Appliance-, physische Appliance- und als PAM as a Service-Option angeboten werden. Während die meisten PAM-Funktionen als Teil der PAM-Suite angeboten werden, sind PUBA und CPEDM als separate Module von ARCON erhältlich.

Hauptsächlich auf der Grundlage eines ASP.NET-Frameworks erweitert ARCON ein Set aus APIs und integriert Benutzerkonfiguration, Vault- und Servicezugrifffunktionen in Web-UIs. Dank integrierter Unterstützung für die meisten auf dem Markt erhältlichen Betriebssysteme, Server, Netzwerkgeräte und SaaS-Anwendungen bietet ARCON Passwortmanagement, feinkörnige Zugriffs- und Befehlssteuerung für Datenbanken — eine Funktion, die den meisten führenden PAM-Anbietern auf dem Markt fehlt. ARCONs Fähigkeit, individuelle Konnektoren für Passwort- und Kontenmanagement für Altsysteme und -anwendungen zu entwickeln, wird von mehreren Unternehmen als klarer Vorteil betrachtet, die alte Infrastrukturen als wichtig für kritische Geschäftsfunktionen erachten.

Stärken	Herausforderungen
• Funktionsreiche, umfassende PAM-Lösung • Große Ziel-Connector-Base • Weiche OPT- und biometrische Authentifizierung • Granulare Befehlssteuerung für Datenbanken • Einfache Integration mit SIEM und Help-Desk-Tools • Einfache Implementierung und Administration • Verfügbar als gehostete oder verwaltete Services sowie PAM as a Service	• Client-basierter Ansatz erzeugt zusätzliche Wartungsaufwände • Erhöhte, aber eingeschränkte Durchdringung der Märkte in Nordamerika und Europa • Inkonsistente Preisgestaltung in verschiedenen Regionen und Branchen • Steigendes, aber noch schwaches Markenbewusstsein in manchen Märkten • Eingeschränkte, aber ausreichende EPM-Funktionen

Tabelle 3: Bedeutende Stärken und Schwächen von ARCON

Zusätzlich zu nativen, softwarebasierten OTP-Authentifizierungsmethoden zur Initialisierung von Sessions bietet ARCON eine OOB-Integration mit RSA und Entrust für Hardware-OTP-Tokens sowie mit Gemalto für biometrische Authentifizierungsmethoden.

Sicherheit	positiv
Funktionalität	positiv
Integration	sehr positiv
Kompatibilität	positiv
Usability	sehr positiv

Tabelle 4: Bewertung von ARCON

Mit lokaler Präsenz in London, Dubai, Kenia, Toronto und auf den Philippinen sowie einem Operations- und einem R&D-Zentrum in Mumbai erlebt ARCON ein stetiges Wachstum in den Regionen Asien-Pazifik, naher Osten sowie Afrika.
Indische IT-Giganten wie HCL, Wipro, Tech Mahindra und Tata Consultancy Services zählen zu ARCONs wichtigsten Vertriebspartnern und helfen dem Unternehmen dabei, sich als vielversprechender PAM-Anbieter für große, komplexe Rechenzentren zu etablieren.

Dank der Produktarchitektur in Kombination mit der integrierten hohen Verfügbarkeit, der Echtzeit-Passwortreplikation und den automatischen Wiederherstellungsfunktionen ist ARCONs Suite die bevorzugte Wahl für große, verteile Implementierungen in Rechenzentren, die Mehrmandantenfähigkeit sowie Anwendungsfälle mit Remote-Zugriff für Drittparteien erfordern.

5.2 BeyondTrust

Das in den USA ansässige Unternehmen BeyondTrust ist ein langjähriger, etablierter PAM-Anbieter und bildet heute eine kombinierte Entität, die aus den nennenswerten Übernahmen von Lieberman Software, Avecto und BeyondTrust durch Bomgar im Jahr 2018 resultiert. Das aus den ambitionierten Übernahmen und Fusionen entstandene Unternehmen hat den Namen BeyondTrust beibehalten und ist möglicherweise einer der größten PAM-Anbieter in Bezug auf den Gesamtumsatz sowie die Kundenzahl. Die Privileged Access Management-Plattform von BeyondTrust ist nun ein kombiniertes Produkt für alle wichtigen PAM-Streams. Das Privileged Password & Session Management umfasst Passwort-Vaults sowie die SAPM-Fähigkeiten der früheren Produkte PowerBroker Password Safe und Lieberman RED. Eine Kombination aus Avecto Defendpoint und PowerBroker for Windows bildet ein starkes EPM-Produkt mit einigen signifikanten Funktionsüberschneidungen. Durch die Remote Access Management-Fähigkeiten von Bomgar bietet BeyondTrust eine der umfassendsten PAM-Plattformen auf dem Markt mit einigen kurzfristigen Herausforderungen im Hinblick auf die Produktintegration.

Stärken	Herausforderungen
• Seit langem auf dem Markt etabliertes Produkt, jetzt mit dem potenziell größten Marktanteil • Der host-basierte Ansatz für CPEDM bietet eine starke und granulare Befehlskontrolle für die Erhöhung von Privilegien. • Die Integration mit der beliebten Schwachstellenmanagementplattform des Anbieters ermöglicht herausragende Funktionen für Asset Discovery und die Bedrohungserkennung. • Der integrierte, sichere Zugriff aus der Ferne mittels PAM bietet eine verbesserte Sichtbarkeit und Kontrolle im Hinblick auf Fernzugriff durch Dritte. • Eine ausgedehnte globale Präsenz und die Konsolidierung von Partnerschaften stärkt die Wettbewerbsfähigkeit des Anbieters und führt zu weiteren Marktchancen. • Das weiter vereinfachte Preismodell ist eine starke Alternative im Vergleich zu Wettbewerbern.	• Beträchtliche Funktionsüberschneidungen aufgrund mehrerer Übernahmen durch Bomgar im letzten Jahr • Schwierigkeiten bei der Rationalisierung von Sales- und Partnerschaftskanälen senden gemischte Signale an den Markt • Erweiterte Pipeline für Engineering- und Entwicklungsteams zur Integration verschiedener Produkte unter einem Dach und zur Bereitstellung einer konsolidierten Plattform • Schwierige Positionierung im Vergleich zu Microsofts Device Guard sowie Komponenten von AppLocker für Desktop EPM • Inkonsistente Skalierbarkeit und Verfügbarkeit in allen Produkten • Während die grundlegenden Anforderungen unterstützt werden, fehlt in relativer Hinsicht ein zielgerichteter Ansatz für DevOps, PUBA und PAG

Tabelle 5: Bedeutende Stärken und Schwächen von BeyondTrust

Die Integration mit der Schwachstellenmanagementplattform von BeyondTrust bietet hochentwickelte Funktionen zur Bedrohungsanalyse mittels Asset Discovery, Schwachstellenevaluierung, Risikobewertung und integrierten Reporting-Features. BeyondTrust verfügt über eine klare Integrations-Roadmap und verspricht seinen Kunden einen reibungslosen Übergang zur integrierten Plattform.

Sicherheit	sehr positiv
Funktionalität	sehr positiv
Integration	positiv
Kompatibilität	sehr positiv
Usability	sehr positiv

Tabelle 6: Bewertung von BeyondTrust

Ein ausgedehntes Vertriebs- und Partnerökosystem birgt ein enormes Wachstumspotenzial für BeyondTrust sowohl in neuen Regionen als auch in neuen Branchen. Im Kern bietet BeyondTrust weiterhin eine zuverlässige Lösung für Unternehmen, die PAM-Anforderungen in einer komplexen IT-Hybridumgebung abdecken möchten.

5.3 CA Technologies

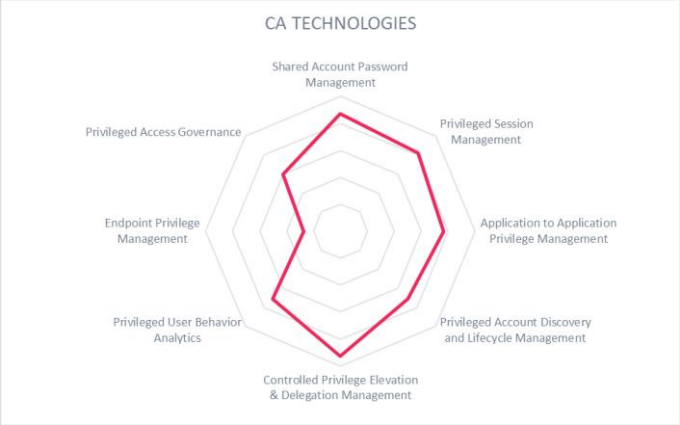
Das in New York ansässige Unternehmen CA Technologies blickt auf eine lange und erfolgreiche Geschichte als führender Anbieter auf dem Markt für Identity & Access Management zurück, in erster Linie dank verschiedener, im Laufe von zehn Jahren vorgenommenen Übernahmen. Die jüngste Übernahme von CA Technologies durch Broadcom führt zu einer signifikanten Veränderung sowie zu Unklarheiten bezüglich der Zukunft des Sicherheitsportfolios und der IAM-Produktlinie von CA. Allerdings hat Broadcom in der frühen Phase der Integration deutliches Interesse am Sicherheitsportfolio von CA gezeigt.

CA Technologies bietet die CA Privileged Access Management Suite an, die aus CA Privileged Access Manager, CA Privileged Access Manager Server Control und CA Threat Analytics besteht — integriert in eine Plattform mit flexiblen Lizenzierungsoptionen. Als früherer Market Leader in Bezug auf PAM hat CA Technologies signifikante Investitionen in die Konsolidierung seines legendären Privileged Access Management-Produkts getätigt und Funktionen aus der Übernahme von Xceedium Xsuite in Form einer einheitlichen Plattform ergänzt. Auf der Basis eines der ältesten und zuverlässigsten Privileged Access Management-Produkte auf dem Markt (CA Access Control) nutzt die CA PAM-Suite eine signifikanten Implementationsbasis, ein Direktvertriebsteam sowie ein starkes Channel-Partnernetzwerk in verschiedenen Regionen, um Wettbewerber hinter sich zu lassen und sich als führender PAM-Anbieter zu positionieren.

Stärken	Herausforderungen
• Unterstützung für eine große Zahl von Zielsystemen • Volle Unterstützung für AAPM • Unterstützung für virtualisierte Umgebungen und Cloud-Umgebungen • Feinkörnige Befehlssteuerung • Unterstützung sowohl für host-basierte als auch proxy-basierte PAM-Ansätze • UNIX AD Authentication Bridging zur Ausdehnung von AD-Richtlinien auf UNIX-Systeme • Starkes Partnerökosystem	• Unterstützung für DevOps ist vorhanden, aber in einer frühen Entwicklungsphase • CPEDM ist umfangreich, aber teuer • Threat Analytics unterstützt keine individuellen Anpassungen • Fehlende zielgerichtete Kommunikation von Broadcom erhöht die Unsicherheit bezüglich zukünftiger Investitionen von Broadcom in das Sicherheitsportfolio von CA • Fehlender Fokus auf mittlere Marktsegmente

Tabelle 7: Bedeutende Stärken und Schwächen von CA Technologies

Der CA Privileged Access Manager ist eine einfach zu implementierende Lösung für Privileged Access Management in physischen, virtuellen und Cloud-Umgebungen und bietet kombinierte Funktionen für SAPM, AAPM und PSM in einer Lösung. CA Threat Analytics bietet hochentwickelte Maschinenlerntechniken für Threat Analytics zur automatischen Erkennung von riskantem privilegierten Verhalten. CA PAM Server Control umfasst eine agentenbasierte Architektur zum Abfangen von Befehlen und zur Einschränkung von Befehlen auf der Ebene des OS-Kernels. Dies ermöglicht eine feinkörnige Befehlskontrolle und Erhöhung von Privilegien sowie die Authentifizierung von UNIX- und Linux-Benutzern mittels Anmeldeinformationen für AD und Kerberos zum UNIX AD Bridging.



Sicherheit	sehr positiv
Funktionalität	sehr positiv
Integration	positiv
Kompatibilität	positiv
Usability	sehr positiv

Tabelle 8: Bewertung von CA Technologies

Als natürliche Wahl für die meisten mittleren bis großen Unternehmen mit komplexen PAM-Anforderungen liefert CA PAM eine native Integration mit der IAM-Suite des gleichen Anbieters, um zusätzliche Vorteile zu bieten. Bestehende CA-Kunden sollten mehr Klarheit bezüglich der geplanten Produkt-Roadmap nach der Übernahme von CA durch Broadcom fordern.

5.4 Centrify Corporation

Das US-amerikanische Unternehmen Centrify bietet das Produkt Centrify Infrastructure Services als umfassende Lösung für Privileged Access Management mit SAPM und Remote-Zugriffsfunktionen an. Durch die Nutzung seiner Access Management-Fähigkeiten bietet Centrify integriertes Adaptive MFA sowie Brokered Authentication für Privileged Access. Centrify Infrastructure Services wird in erster Linie als SaaS über AWS Marketplace implementiert, ist aber auch als Managed-On-Premises-Option verfügbar.
Die Lösung bietet außerdem CPEDM, Just in Time Privileged Access über integrierte Workflows oder über Drittparteien, wie beispielsweise ServiceNow, Auditing und Monitoring für Hosts sowie für Gateways, Adaptive MFA for Privileged Access sowie Privileged Analytics.

Implementierungsoptionen umfassen ein SaaS-Modell, die Implementierung über den AWS Marketplace, die Cloud-Implementierung sowie eine On-Premise-/durch den Kunden verwaltete Option.

Stärken	Herausforderungen
• Tiefe AD-Integration zur Unterstützung von komplexen Multi-Domänen-/Forest-Konfigurationen • Starke Unterstützung für MFA und Identity Federation mit Risk Adaptive-Funktionen • Integrierte MDM-/MAM-Funktionen • Ausgereiftes PAM als Serviceangebot zusätzlich zu einer verwalteten On-Premise-Implementierung • Starke Privilege Analytics mit hochentwickelten Maschinenlerntechniken • Geeignet für Hybrid- sowie containerbasierte IT-Umgebungen • Eine gut funktionierende Marketing-Maschinerie mit starkem Messaging bzgl. Zero-Trust-Ansatz	• Die On-Premise-Implementierung ist relativ neu im Vergleich zum cloud-basierten Ansatz des Anbieters. • Keine umfassendes Endpoint Privilege Management für Desktops • Die Preise liegen am höheren Ende des Spektrums. • Ein wachsendes, aber relativ eingeschränktes Partnerökonetzwerk • Ein starker Fokus auf die USA als Hauptmarkt hat das Wachstum auf den Märkten EMEA und Asien gehemmt.

Tabelle 9: Bedeutende Stärken und Schwächen von Centrify

Der Centrify Privileged Access Service bietet Password Vaults für SAPM sowie Secure Remote Access auf Zielsysteme für privilegierte Benutzer. Neben Adaptive MFA sowie Identitätskonsolidierung bietet der Centrify Authentication Service auch UNIX-AD Bridging. Der Privileged Analytics Service dieses Anbieters nutzt Maschinenlerntechniken, um Bedrohungsanalysen zu ermöglichen und Zugriffsrichtlinien auf der Grundlage des Benutzerverhaltens zu erzwingen.

Sicherheit	sehr positiv
Funktionalität	positiv
Integration	sehr positiv
Kompatibilität	sehr positiv
Usability	sehr positiv

Tabelle 10: Bewertung von Centrify

Centrifys Auditing & Monitoring Service bietet eine detaillierte Überwachung und Prüfung auf der Shell- sowie der Prozessebene und unterstützt sowohl host- und proxy-basierte Implementierungen. In Kombination mit dem kürzlich umbenannten IDaaS des Anbieters, Idaptive, sowie integrierten MDM-Funktionen ist Centrify interessant für Unternehmen, die integrierte Identity Federation, eine tiefe AD-Integration, starke MFA-Unterstützung sowie mobiles Zugriffsmanagement für privilegierten Zugriff suchen.

5.5 CyberArk

CyberArk verfügt über Niederlassungen in Israel sowie den USA und ist seit langem ein führender Anbieter auf dem Markt für Privileged Access Management. Das 1999 in Israel gegründete Unternehmen CyberArk konzentriert sich ausschließlich auf die Sicherung von privilegierten Zugriffen innerhalb der IT-Umgebung eines Unternehmens durch kontinuierliches Wachstum und Innovationen. CyberArk bietet seine Core Privileged Access Security-Lösung als vollständig integrierte Suite aus verschiedenen Modulen an, nämlich Credential Management (früher Enterprise Password Vault), Session Management (früher Privileged Session Manager), Threat Analytics (früher Privileged Threat Analytics) sowie On-Demand Privileges Manager für privilegierte Erhöhungen.

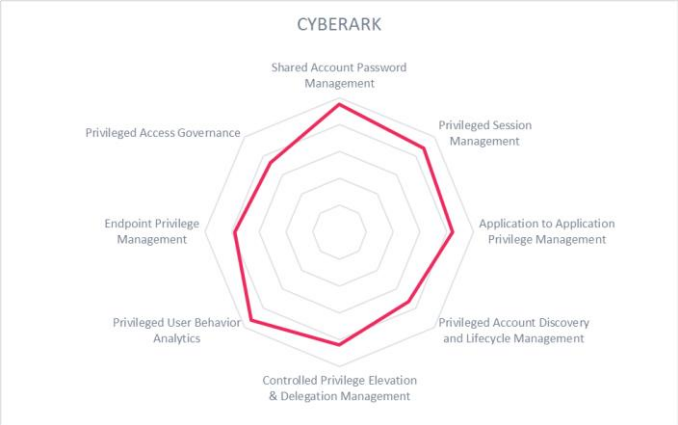
Seine DevOps- und Apps Secrets Management-Lösung besteht aus Conjur sowie Application Identity Manager (AIM) als AAPM-Komponente. CyberArk Endpoint Privilege Manager (EPM) ist ein separates, aber integrierbares Produkt mit Endpoint Privilege Management-Funktionen.

Stärken	Herausforderungen
• Breite Unterstützung für Zielplattformen • Einfache Integration eigener Komponenten sowie Komponenten von Drittanbietern • Intuitives und robustes UI-Design • Starke Bedrohungs-Analytics zur Erkennung und Behebung von Bedrohungen in Echtzeit • Effektive DevOps-Unterstützung • Breite Unterstützung für Cloud-Anwendungen und -Infrastruktur • Bequemes und neu konzipiertes Preismodell • Starkes und funktionales Partnerökosystem	• Die hohe Modularität der Lösung könnte für gewisse Implementierungen unvorteilhaft sein • Möglicherweise schwierige Begründung der Lösungskomplexität für einfache PAM-Umgebungen • Mangelnder Fokus auf kleine und mittlere Marktsegmente • Markterwartung: Schneller Wandel und maximaler Unternehmenswert innerhalb eines zulässigen Risikobereichs sorgen für zusätzlichen Druck

Tabelle 11: Bedeutende Stärken und Schwächen von CyberArk

Die meisten der auf Flexibilität, Skalierbarkeit und hohe Verfügbarkeit ausgelegten Komponenten von CyberArk können auf Hardware, in VMs, in AWS, Azure oder Google Cloud installiert werden.

CyberArk Conjur, das als Enterprise- sowie als Open Source-Version verfügbar ist, bietet Secret Management in nativen Cloud-, DevOps-, und Containerized-Umgebungen sowie in anderen dynamischen Umgebungen, sodass Entwickler von Benutzern, Anwendungen, Microservices, Containern, APIs usw. verwendete geheime Daten in der gesamten DevOps-Pipeline schützen und verwalten können, um die Implementierung von Anwendungen beschleunigen und vereinfachen können. Das als Virtual Appliance angebotene CyberArk Privileged Threat Analytics ist ein weiteres ausgereiftes Produkt dieses Anbieters, das sich auf die Erkennung von Benutzeranomalien sowie gefährlichen Aktivitäten konzentriert und in die Privileged Session Management-Lösung sowie in Endpoint Privilege Manager integriert werden kann, um Bedrohungen zu erkennen und zu melden.



Sicherheit	sehr positiv
Funktionalität	sehr positiv
Integration	sehr positiv
Kompatibilität	sehr positiv
Usability	sehr positiv

Tabelle 12: Bewertung von CyberArk

CyberArk ist nach wie vor der Anbieter der Wahl für globale Unternehmen, die eine umfassende, marktführende PAM-Lösung für komplexe PAM-Anforderungen suchen.

5.6 EmpowerID

Das im US-amerikanischen Ohio ansässige Unternehmen EmpowerID bietet im Rahmen seines weitgefassten IAM-Portfolios verschiedene Produkte an, wobei das neueste Tool EmpowerID Privileged Access Management (PAM) für die Verwaltung von gemeinsam verwendeten, privilegierten Zugriffsfunktionen sowie Sessions Recording & Auditing für allgemeine Zugriffsprotokolle konzipiert wurde. Das größtenteils auf Microsoft-Technologie basierende Tool von EmpowerID bietet Integrations- und Leistungsvorteile für Microsoft-basierte Unternehmen, insbesondere für bestehende Kunden seiner User Provisioning- und Identity Governance-Produkte.

Stärken	Herausforderungen
• Als neues Produkt rundet PAM das IAM-Portfolio des Anbieters ab und kann gut in eine weiter gefasste IAM-Suite integriert werden. • Integrierte Unterstützung bzgl. Workflow & Policy Management für eine starke PAG • Führende Unterstützung für Adaptive Authentication	• Ausführung in erster Linie auf Windows-Plattformen, • Mangel an Funktionen für hochentwickeltes AAPM sowie Privilege Elevation • Endpoint Privilege Management (EPM) nicht vorhanden • Eingeschränkte Suchfunktionen bzgl. grafischer Sessions • EIN kleines, aber erlesenes Partnerökosystem, das sich hauptsächlich auf Europa konzentriert

Tabelle 13: Bedeutende Stärken und Schwächen von EmpowerID

Das PAM-Produkt von EmpowerID stellt grundlegende Funktionen für Shared Account Password Management (SAPM) über einen gesicherten, verschlüsselten Password Vault sowie Privileged Session Management (PSM) für SSH-, RDP und webbasierte SSO-Sessions bereit, die für den Zugriff auf privilegierte Systeme in Unternehmen verwendet werden. Auf diese Weise ergänzt EmpowerID sein IAM-Portfolio und unterstützt die Kunden seiner bestehenden IAM-Produkte, die grundlegende PAM-Funktionen zur Verwaltung von privilegiertem Zugriff benötigen.

Während EmpowerID PAM das Auschecken von Anmeldeinformationen aus dem Password Vault mittels APIs und einem nativen PowerShell-Modul unterstützt, wird hochentwickeltes Application to Application Password Management (AAPM) nicht unterstützt. Außerdem umfasst EmpowerID PAM keine Funktionen zur Erhöhung von Privilegien oder für Endpoint Privilege Management (EPM). Während die Wiedergabe, die Suche und das Reporting bezüglich Sessions möglich sind, wird Privileged User Behavior Analytics noch nicht unterstützt.

Sicherheit	positiv
Funktionalität	neutral
Integration	sehr positiv
Kompatibilität	positiv
Usability	positiv

Tabelle 14: Bewertung von EmpowerID

EmpowerID PAM ist ohne Aufpreis für die Verwaltung von EmpowerID-Infrastrukturen enthalten, aber es sind zusätzliche Lizenzen erforderlich, um die Lösung in der gesamten IT-Umgebung bereitzustellen. Die Integration in die adaptive Authentifizierung und das Workflow-Management des Identity Governance-Produkts des gleichen Anbieters bieten eine leistungsfähigere Authentifizierung von privilegierten Benutzern und Privileged Access Governance. Dank des Richtlinien- und Workflow-Managements für privilegierten Zugriff, das als Teil der integrierten IAM-Lösung von EmpowerID erhältlich ist, ist EmpowerID der Anbieter der Wahl für Unternehmen, die Microsoft-Technologien nutzen und die eine gute Basisunterstützung für SAPM und PSM mit einer verbesserten Privileged Access Governance (PAG) suchen.

5.7 FUDO Security

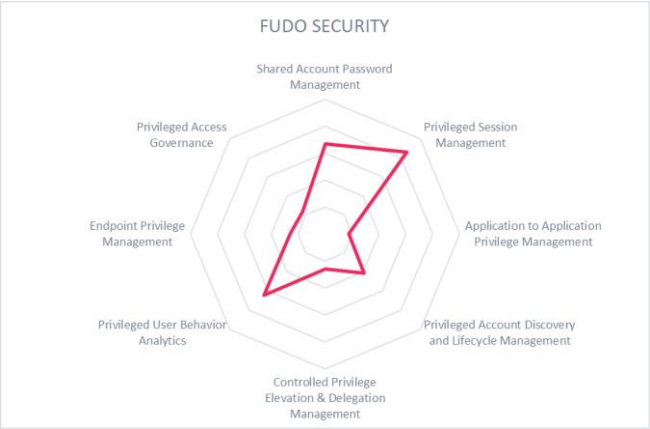
Das in Kalifornien ansässige Unternehmen FUDO Security, das früher unter dem Namen Wheel Systems firmierte, bietet FUDO PAM als sein primäres PAM-Produkt auf dem Markt an. Darüber hinaus bietet FUDO Session Recorder als eigenständiges Produkt für Remote Session Monitoring an. FUDO Security verfügt über eine signifikante Implementierungsbasis in Europa sowie im Nahen Osten und plant, seine Geschäfte auf Nordamerika und Asien auszuweiten.

Stärken	Herausforderungen
• Unterstützung für eine große Zahl von Zielsystemen • Starke PSM- & SRM-Funktionen • Mehrmandantenfähig & HA-Unterstützung • Verwendung von verhaltensbasierter Biometrik für hochentwickelte Privileged Analytics • Die Appliance-basierte Bereitstellung bietet eine schnellere Implementierung und Konfiguration.	• Eingeschränkte AAPM-Funktionen • CPEDM und EPM fehlen • Schwache Marketing-Maschinerie • Keine Unterstützung für Cloud-Plattformen und DevOps • Eingeschränkte Partnerschaften und Kompatibilität mit Sicherheitstools von Drittanbietern • Eingeschränkte Partnerökosysteme und Präsenz außerhalb von EMEA

Tabelle 15: Bedeutende Stärken und Schwächen von FUDO Security

FUDO Security wird als Hardware sowie Virtual Appliance angeboten; zusätzliche Lizenzen für HA- und VM-Optionen sind verfügbar. FUDO PAM unterstützt eine große Zahl von Zielsystemen für Shared Account Password Management (SAPM) und bietet ein starkes Privileged Session Management (PSM) sowie Session Recording & Monitoring (SRM). Dank verfügbarer Vorkehrungen für Dual Control und Session Delegation bietet FUDO Security eine eigene MFA-Lösung sowie OAuth-Integrationsmöglichkeiten für externe Authentifizierungsanbieter, wie beispielsweise Yubikey. Die Stärke der PAM-Lösung von FUDO liegt in ihren Funktionen für Session Recording, die ein umfassendes Bit-für-Bit-Session Recording auf Protokollebene umfassen, einschließlich Mausbewegungen, Subsessions, Dateitransfers, USB-Zugang, Sound, ausgeblendete Fensterinhalte sowie einer vollständige OCR-Konvertierung von Sessions.

Dank eines agentenlosen Ansatzes ermöglicht FUDO PAM eine schnelle Implementierung und Erstkonfiguration. FUDO's HA-Architektur unterstützt Multi-Master-, Multi-Knoten-HA-Konfigurationen und ist für geografisch verteilte Implementierungen geeignet. Während FUDO herausragende SRM-Funktionen bietet, bietet der Bereich für Privileged Analytics, der als Unterstützung für Geschäftsentscheidungen bietet, noch Raum zur Verbesserung. FUDO mangelt es außerdem an Möglichkeiten zur Integration und Kompatibilität für Sicherheitslösungen von Drittanbietern, wie IGA- und UEBA-Tools für Privileged Governance und Behavioral Analytics.



Sicherheit	positiv
Funktionalität	positiv
Integration	neutral
Kompatibilität	neutral
Usability	positiv

Tabelle 16: Bewertung von FUDO Security

Da FUDO nur grundlegende AAPM-Funktionen bietet, fehlen CPEDM- sowie Desktop-EPM-Funktionen. Unternehmen, die eine regionale Integrationsunterstützung sowie eine schnellere Implementierung mit gemeinsamem Passwortmanagement und starke Session Recording- und Monitoring-Funktionen suchen, sollten die PAM-Lösung von FUDO in Betracht ziehen.

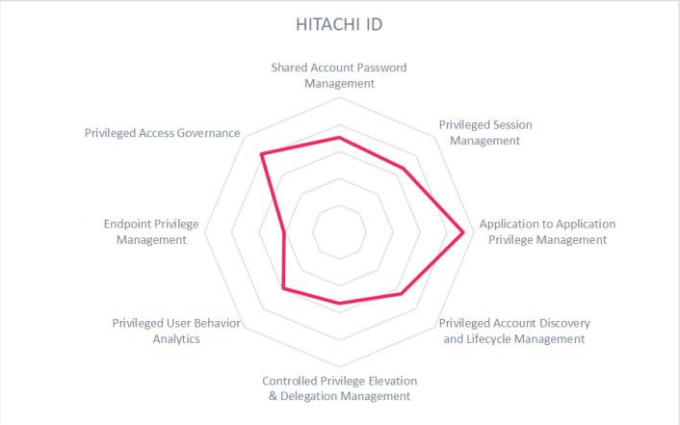
5.8 Hitachi ID

Hitachi ID mit Sitz in Kanada ist ein global agierender IAM-Softwareanbieter, der ursprünglich unter dem Namen MTech Information Technology firmierte und im Jahr 2008 von Hitachi übernommen wurde. Das Unternehmen bietet die Lösung Hitachi ID Privileged Access Manager als Hauptprodukt auf dem PAM-Markt an. Dank robuster SAPM-Funktionen stellt Hitachi ID Privileged Access Manager ein breiter aufgestelltes PAM-Produkt an, das die meisten Enterprise-PAM-Funktionen umfasst. Durch ihre einfache Implementierbarkeit sowie ihre Eignung für schlanke privilegierte Operationen ist diese Lösung ein starker Herausforderer für einige der führenden Anbieter auf dem Markt.

Stärken	Herausforderungen
• Starke Kontextunterstützung für API-/Service-Authentifizierung • Aktiv-Aktiv-Architektur für hohe Verfügbarkeit • Integrierte 2FA-Authentifizierung • Session Recording ist ohne Aufpreis inbegriffen • Detaillierte Kontoerkennung und -bereitstellung • Mobile Unterstützung für Access Request Management • Die Zugriffszertifizierungsfunktion von Hitachi ID Identity Manager ist ohne Aufpreis inbegriffen.	• Eingeschränkte CPEDM-Funktionen • Kein EPM-Modul • Keine effektive Vertriebs- und Marketingmaschinerie • OOB-Konnektoren für Cloud-Anwendungen sind begrenzt, werden aber ausgebaut. • Das eingeschränkte Partnerökonetzwerk hemmt die Marktreichweite und das Wachstum.

Tabelle 17: Bedeutende Stärken und Schwächen von Hitachi ID

Die Lösung unterstützt eine erschöpfende Liste von physischen sowie virtuellen Zielsystemen. Privilege Elevation basiert auf einer befristeten Mitgliedschaft in einer Sicherheitsgruppe sowie einer SSH-Trust-Injektion anstatt einer Befehlszeile oder Shellsubstitution. Der Identity Express: Privileged Access Edition umfasst Geschäftsregeln sowie Richtlinien rund um den Privileged Access Manager, um die Kontrolle bezüglich des Zugriffs auf privilegierte Konten und Sicherheitsgruppen in einer Vielzahl von Systemen zu vereinfachen. Auf diese Weise können PAM-Implementierungen über verschiedene Kunden standardisiert werden. Die meisten relevanten IAM-Funktionen sind im Lieferumfang des MasterSAM PAM enthalten, einschließlich Erkennung, Zugriffszertifizierung, SoD-Erkennung und Richtliniendurchsetzung zusammen mit der Anfrage und Genehmigung von Gruppenmitgliedschaften in Verzeichnisobjekten, welche die Echtzeitüberwachung von AD-Gruppen unterstützen, um nicht autorisierte Out-of-Band-Fehler zu erkennen und rückgängig zu machen



Sicherheit	sehr positiv
Funktionalität	sehr positiv
Integration	sehr positiv
Kompatibilität	sehr positiv
Usability	positiv

Tabelle 18: Bewertung von Hitachi ID

Insgesamt bietet Hitachi ID eine gute Unterstützung für IT-Hybridumgebungen sowie SaaS für PAM, einschließlich Konnektoren für die häufigsten Cloud-Anwendungen und -Plattformen. Durch kürzliche Produktverbesserungen hat Hitachi ID sich zu einem vielversprechenden PAM-Anbieter entwickelt, der in Anbieterevaluationen durch Unternehmen mit kritischen Anforderungen in Bezug auf SAPM, PSM und PAG berücksichtigt werden sollte.

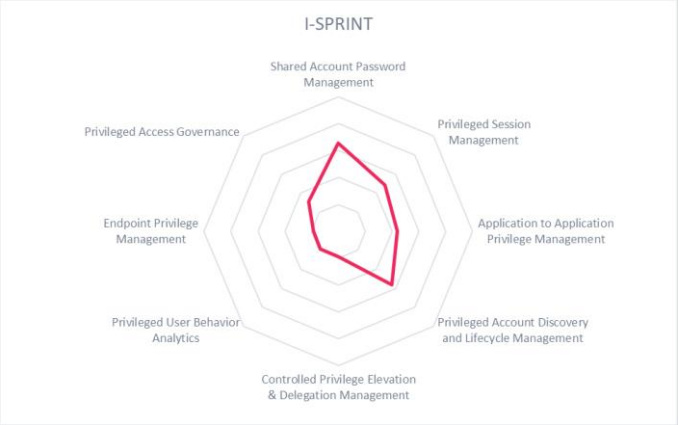
5.9 I-Sprint

Das aus Singapur stammende Unternehmen I-Sprint ist ein Anbieter für Zugriffsmanagement, und sein PAM-Produkt ist AccessMatrix Universal Credential Manager. Dank seiner signifikanten Präsenz in Asien, insbesondere in Südostasien (SEA) und China, konzentriert I-Sprint sich in erster Linie auf asiatische Unternehmen und hat ein hervorragendes Verständnis für regionale Geschäftsprozesse, die wesentlich von globalen Standards abweichen.

Stärken	Herausforderungen
• Einfache Implementierung und Erstkonfiguration • Starke Authentifizierungsunterstützung über UAS • HSM-Integration bietet starke Verschlüsselung und unterstützt Anwendungsfälle mit hoher Sicherheit • Gutes Verständnis regionaler PAM-Anforderungen • Unterstützt PAM-spezifische Verordnungen in der Region	• Noch nicht ausgereift, verschiedene PAM-Funktionen fehlen • Marketing ist regional ausgerichtet und nicht effektiv • Regionaler Fokus hemmt die globale Reichweite und schränkt das Marktwachstum ein • Trotz Wachstum ist das Partnerökosystem klein und regional

Tabelle 19: Bedeutende Stärken und Schwächen von I-Sprint

Der Universal Credential Manager (UCM) stellt einen virtuellen Passwort-Safe mit starker Verschlüsselung bereit und verwendet HSM-Geräte zur Ablage von privilegierten Konten und Anmeldeinformationen. I-Sprint Privileged Session Manager (PSM) bietet einen Windows RDP Gateway Recorder als Add-On sowie eine Reihe von Netzwerkprotokoll-Proxymodulen zur Überwachung und Aufzeichnung von privilegierten Sessions, die Videoaufzeichnungen sowie die Wiedergabe von Sessions für forensische Analysen unterstützen. Die Lösung bietet außerdem Command Access Control für ausgewählte Protokolle.



Sicherheit	neutral
Funktionalität	positiv
Integration	neutral
Kompatibilität	schwach
Usability	positiv

Tabelle 20: Bewertung von I-Sprint

UCM ermöglicht die Erkennung von privilegierten Konten auf der Grundlage der Systemkonfiguration und erstellt entsprechende, zu verwaltende Berichte in UCM. Darüber hinaus bietet UCM das programmatische Auschecken von Passwörtern durch Anwendungen mittels PKI-Zertifikatauthentifizierung. UCM profiziert signifikant vom I-Sprints Flaggschiff-Produkt für Authentifizierung, Access Matrix Universal Authentication Manager, indem es mehrfache Authentifizierungsformfaktoren und Session Management für privilegierte Benutzer verwendet und die durch UCM generierten Upsell-Verkaufsmöglichkeiten nutzt.

I-Sprint UCM ist weiterhin ein sich entwickelndes Produkt auf dem PAM-Markt mit grundlegenden Vorkehrungen für Account Management, Session Recording & Auditing. I-Sprint verfügt über eine wachsende Konnektorenbasis sowie Integrationen für Zielsysteme, einschließlich SaaS-Apps, aber es fehlen bestimmte PAM-Funktionen, sodass es derzeit noch keine vollständige PAM-Lösung anbietet. Allerdings könnte sich dies schneller als erwartet ändern, da I-Sprint weiter in die Entwicklung seines UCM-Produkts investiert, um globale Standards zu erreichen.

Kleine und mittlere Unternehmen mit grundlegenden SAPM- und PSM-Anforderungen sowie Bedarf an regionaler Implementierungsunterstützung und Prozessverständnis sollten I-Sprint bei ihrer Evaluation von PAM-Anbietern berücksichtigen.

5.10 Krontech

Das türkische Unternehmen Krontech ist der Technologiezweig von Kron, einer an der Börse in Istanbul gehandelten Aktiengesellschaft. Krontech bietet die Single Connect PAM-Suite an, dass verschiedene Module zur Verwaltung von privilegiertem Zugriff umfasst. Als relativ neuer Akteur auf dem Markt, der sein erstes Produkt im Jahr 2013 auf den Markt brachte, ist Krontech hauptsächlich in Europe tätig, gefolgt von Nordamerika, Kanada und Asien.

Das Modul Single Connect Dynamic Password Controlled umfasst ein sicheres, als agentenlose Version angebotenes Password Vault für SAPM- und AAPM-Funktionen. Session Manager stellt PSM-Funktionen bereit und unterstützt die meisten Session-Arten mit Session Recording, Playback und Dual Control. Der MFA Manager bietet Single Sign-on (SSO) und MFA für privilegierte Benutzer auf Zielsystemen und unterstützt SMS- sowie Soft-OTP-Methoden zusätzlich zur OOB Mobile Push-Authentifizierung.

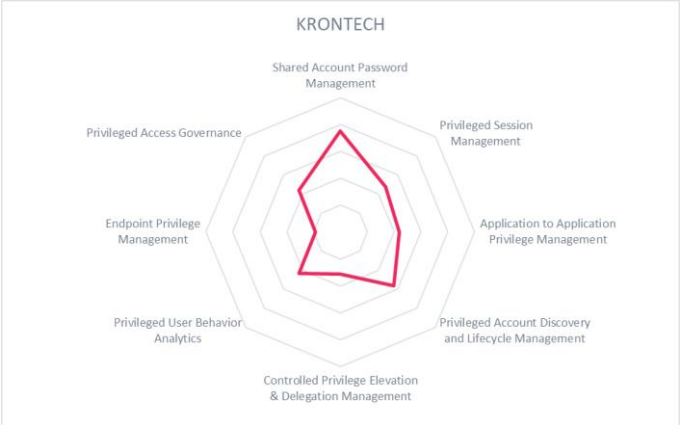
Stärken	Herausforderungen
• Separate Module für markante PAM-Funktionen, integriert im Rahmen einer gemeinsamen PAM-Plattform • Gutes Markt- und Technologieverständnis • Gutes UI-Design für erweitertes UX • Starke Unterstützung für Datenbankadministrationsrechte • Früher und effektiver Fokus auf privilegierte Task-Automatisierung • Unterstützung für wenige, aber die häufigsten IaaS-Plattformen	• CPEDM-, EPM-, PUBA- und PAG-Funktionen fehlen • Marketingbotschaften sind fragmentiert und versprechen tendenziell zu viel • Eingeschränkte Vertriebskanäle und Partnerökosystem • Markenbewusstsein weiterhin schwach mit eingeschränkten Kundenreferenzen • Relativ neuer Akteur in einem etablierten Markt

Tabelle 21: Bedeutende Stärken und Schwächen von Krontech

Access Directory Manager bietet integrierte Unterstützung für TACACS+- und RADIUS-Protokolle zur Steuerung des Zugriffs auf Netzwerkgeräte, wie SSH- und Telnet-Sessions. Der Single Connect Data Access Manager ist das Modul für privilegierten Datenbankzugriff. Es umfasst Activity Monitoring für privilegierte Datenbank-Sessions. Dies ermöglicht die Verwaltung von DB-Admin-Rollen und zugewiesenen DB-Privilegien mit feinkörniger Befehlssteuerung und dynamischem Daten-Masking. Der Single Connect Privileged Task Automation (PTA) Manager zielt hauptsächlich auf Telekom.-Serviceanbieter ab und ermöglicht eine verbesserte betriebliche Effizienz durch die Delegation von Aufgaben anstatt Privilegien sowie automatisierte, routinemäßige Privilege-Operationen.

Sicherheit	neutral
Funktionalität	positiv
Integration	neutral
Kompatibilität	neutral
Usability	neutral

Tabelle 22: Bewertung von Krontech



Obwohl PAM-as-a-Service nicht angeboten wird, unterstützt das Single Connect Cloud-PAM-Modul Single Connect-PAM-Funktionen für AWS, Azure und Google Cloud-Plattformen an. Durch seine grundlegenden SAPM- und PSM-Funktionen ist Krontech Single Connect interessant für kleine und mittelständische Unternehmen (KMU) mit einem Bedarf an der Eliminierung von routinemäßigen Aufgaben mittels Privileged Task Automation, was für schnellere und schlankere privilegierte Operationen sorgt. Darüber hinaus sollte das Tool auch interessant für Unternehmen sein, die besseres Database Activity Monitoring sowie dynamisches Daten-Masking auf der Grundlage von Datenbank-Privilegien benötigen.

5.11 ManageEngine

Das Unternehmen ManageEngine mit Hauptsitz im US-amerikanischen Pleasanton ist Teil der in Indien ansässigen Zoho Corporation, die 1996 gegründet wurde. Das PAM-Produkt von ManageEngine, der Password Manager Pro, kam 2007 auf den Markt und ist dank seiner Vorteile eines der beliebtesten PAM-Produkte im KMU-Marktsegment.

ManageEngine führt die meisten seiner Geschäfte von indischen Chennai aus und verfügt nach Zahlen über einen der größten Kundenstämme auf dem PAM-Markt. Allerdings liegen die entsprechenden Geschäftsgrößen innerhalb des unteren Quartils.

Stärken	Herausforderungen
• Unterstützung für eine große Zahl von Zielsystemen, einschließlich Hypervisors • Starke automatische Erkennungsfunktionen • Gebündelte Middleware- und Datenbankkomponenten • Nahtlose Integration mit innerhalb eines breiteren Portfolios für Sicherheits- und IT-Infrastrukturmanagement-Software • Angemessene Preisgestaltung und einfache Lizenzierung • Großes und funktionales Partnerökosystem	• Fehlende CPEDM-, PUBA- und PAG-Funktionen • Nur verfügbar als On Premise-Software-Implementierung • Keine Integration mit IGA-Tools • Fokus auf KMU-Marketplace • Keine Konnektorenunterstützung für Cloud-Anwendungen und cloud-basierte Implementierung

Tabelle 23: Bedeutende Stärken und Schwächen von ManageEngine

Der Password Manager Pro unterstützt eine Vielzahl von Zielplattformen, einschließlich Hypervisors, Altsystemen und Infrastrukturkomponenten. Der als Software oder Virtual Appliance verfügbare Password Manager Pro (PMP) wird zusammen mit Apache Tomcat und RDBMS und der Option angeboten, zwischen MS SQL Server oder MySQL als Backend-RDBMS zu wählen. Darüber hinaus wird PMP auf dem Amazon Web Services- und dem Microsoft Azure-Marktplatz angeboten, um eine Implementierung auf Amazon EC2 und Microsoft Azure-anzubieten.

Dank der integrierten hohen Verfügbarkeit, der Datenreplikation sowie den Funktionen zur Notfallwiederherstellung positioniert PMP sich als Enterprise-Tool. Im Rahmen eines vernünftigen, nutzerbasierten Preismodells sind alle PAM-Funktionen als Teil der Basisproduktinstallation verfügbar und können je nach gekaufter Lizenz aktiviert und deaktiviert werden. Das Produkt kann mit allen LDAP-konformen Directory Services (einschließlich AD) für die Benutzerverwaltung und -authentifizierung integriert werden und integriert OOB mit den meisten Authentifizierungsanbietern.

Sicherheit	positiv
Funktionalität	positiv
Integration	positiv
Kompatibilität	positiv
Usability	sehr positiv

Tabelle 24: Bewertung von ManageEngine

Dank der Remote-Login-Funktion können Administratoren emulierte RDP-, SSH-, VNC- und SQL-Sessions über einen Nutzer-Browser starten, ohne dass installierte Plug-Ins oder Endpunktagenten erforderlich sind. Die Sessions werden durch den PMP-Server getunnelt und die Aufzeichnungen werden zwecks Wiedergabe sowie forensischen Prüfungen aufbewahrt. PMP integriert OOB mit EventLog Analyzer (SIEM) sowie ServiceDesk Plus (ITSM) von ManageEngine sowie mit SIEM- und ITSM-Tools von Drittanbietern. Da eine Integration mit IGA-Tools jedoch nicht möglich ist, fehlen PAG-Funktionen.

Dank eines großen Kundenstamms und eines starken Partnerökosystems ist ManageEngine PMP in erster Linie für Unternehmen interessant, die in Sicherheits- und IT-Managementprodukte von ManageEngine investiert haben und bessere Leistungen für einen bestimmten Preis wünschen.

5.12 Micro Focus

Das britische Unternehmen Micro Focus bietet den Micro Focus Privileged Account Manager als primäres PAM-Produkt an, dessen Ursprünge auf Novell sowie die spätere NetIQ-Codebase zurückgehen. Micro Focus führt eine umfassende Produkt-Roadmap und ist mit Hewlett Packard Enterprise (HPE) fusioniert. Die Auswirkungen der Übernahme von Micro Focus durch Hewlett Packard Enterprise (HPE) sind jedoch noch unklar. Vermutlich werden die laufenden Bemühungen bezüglich einer wesentlichen Produkterneuerung des Identity & Access Management-Portfolios mithilfe der umfangreichen Erfahrung von HPE im Hinblick auf Entwicklung und Professional Service fortgeführt.

Stärken	Herausforderungen
• Umfassende PAM-Funktionen • Session Management-Unterstützung für Geschäftsanwendungen und Datenbanken • Skalierbare und flexible Lösungsarchitektur • Risikobasierte Analytics-Unterstützung für PSM • Großer Kundenstamm und ein starkes Partnerökosystem, gestärkt durch HPE-Übernahme	• Fehlende hochentwickelte AAPM-Funktionen • EPM-Funktionen (Endpoint Privilege Management) fehlen • Komplexe Implementierung und Konfiguration • Kürzliche Übernahme durch HPE sorgt für Unsicherheiten bezüglich langjähriger Marktposition • Relativ abgeschwächte Marketingbotschaft und -ausführung

Tabelle 25: Bedeutende Stärken und Schwächen von Micro Focus

Mit dem Micro Focus Privileged Account Manager, der früher unter der Bezeichnung NetIQ Privileged User Manager (PUM) bekannt war, bietet Micro Focus ein umfassendes PAM-Portfolio mit einigen hochentwickelten PSM- und Risk Analytics-Funktionen. Durch ein Enterprise Password Vault für Shared Account Password Management (SAPM) stellt es einen Framework Manager für Controlled Privilege Elevation auf Unix-/Linux-Systemen bereit. Aufgrund mangelnder Unterstützung für erweitertes Application to Application Password Management (AAPM) bietet Micro Focus Privileged Account Manager detailliertes Keystroke Logging und Video Session Recording für privilegierte Benutzerverbindungen. Mithilfe eines Gateway-Ansatzes unterstützt das Produkt Privileged Session Management für eine Vielzahl von Systemen, einschließlich Enterprise Business-Anwendungen wie SAP-Datenbanken und beliebte SaaS-Anwendungen. Kürzliche Produktfortschritte zur Unterstützung von risikobasierten Analytics bezüglich privilegierter Aktivitäten könnten von Interesse für manche Kunden sein.

Sicherheit	positiv
Funktionalität	positiv
Integration	positiv
Kompatibilität	positiv
Usability	positiv

Tabelle 26: Bewertung von Micro Focus

Aus architektonischer Sicht führt Micro Focus eine Roadmap aus, bei der das Unternehmen sich von einem reinen hostbasierten Ansatz hin zu einer Mischung aus proxy- und hostbasierter Architektur bewegt. Dies ermöglicht tiefergehende Integrationen auf bestimmten Zielsystemen, während andere Funktionen wie Password Vaults etc. zentral ausgeführt und verwaltet werden. Insgesamt handelt es sich beim Privileged Account Manager von Micro Focus um ein gutes PAM-Produkt mit nützlichen PAM-Funktionen, die man von einem etablierten Anbieter auf dem Markt erwarten würde. Nach einigen signifikanten Investitionen und Anstrengungen zur Wiederbelebung des IAM-Produktportfolios in letzter Zeit war Micro Focus langsamer dabei, sich an die schnell verändernden IAM-Anforderungen seiner vorhandenen Kunden und des Markts im Allgemeinen anzupassen. Micro Focus PAM spricht Unternehmen an, die bereits über die beliebten Produkte NetIQ Identity und Access Manager verfügen, sodass tiefergehende Integrationen für eine verbesserte Privileged Access Control und Governance möglich sind.

5.13 MT4 Networks

Das im brasilianischen São Paulo ansässige Unternehmen MT4 Networks verfügt über mehrere Netzwerkmanagementprodukte, wobei Senhasegura das Flaggschiff-Produkt ist. Senhasegura besteht aus mehreren Modulen und bietet umfassende PAM-Funktionen. Mit seinem bisher hauptsächlich in Brasilien konzentrierten Kundenstamm breitet Senhasegura sich aufgrund der kulturellen Affinität und der Sprachunterstützung auf einfache Weise in Lateinamerika aus. Senhasegura besteht aus über 15 eng miteinander verbundenen Funktionskomponenten und ist als Virtual Appliance oder Hardware Appliance erhältlich.

Stärken	Herausforderungen
• Umfassendes, die meisten PAM-Bereiche abdeckendes PAM-Angebot • Unterstützt eine große Zahl von Zielsystemen, insbesondere Netzwerkgeräte • Betrieblich effiziente UI • Flexibilität zur Entwicklung von Konnektoren für Altsysteme • Höchst modulare, aber gut integrierte Komponenten	• Mangelnde Sprach- und Prozessunterstützung • Inkonsistente und schwache Marketingbotschaft • Fehlende risikobasierte Analytics • Eingeschränkte CPEDM-Funktionen • Fehlende Privileged Access Governance-Funktionen • Kleiner Anbieter mit begrenzter globaler Präsenz und einem kleinen Partnerökosystem

Tabelle 27: Bedeutende Stärken und Schwächen von MT4 Networks

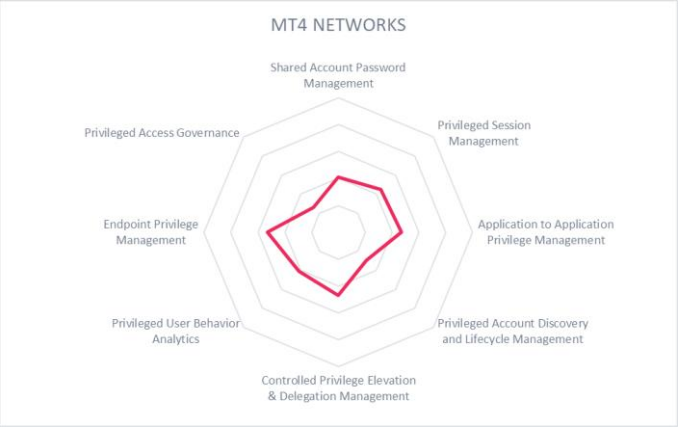
Mit einem Funktionsmodul für nahezu jede PAM-Funktion auf dem Markt verfügt Senhasegura über breitgefächertes Features, aber in manchen Bereichen fehlt es dem Produkt an Funktionstiefe, wie bspw. Accounts Onboarding, risikobasierter Analytics, Endpoint Privilege Management sowie Privileged Access Governance. Allerdings bietet Senhasegura im Vergleich zu den meisten neuen Marktakteuren über ein eher umfangreiches PAM-Produkt.

Senhasegura hat seit unserer letzten Produktbewertung mehrere neue Module vorgestellt, insbesondere Senhasegura Threat Analysis und Behavior Analysis, aber es fehlen ausreichende Kundenreferenzen bezüglich der technischen und funktionalen Ausgereiftheit dieser Module. Zusätzlich zu den vielen grundlegenden PAM-Modulen für Account und Password Management bietet Senhasegura SSH Key Management, Erkennung von Accounts, AAPM sowie ein MFA-Modul für Endpunkte.

Als agentlose Architektur ermöglicht es eine einfache Installation und Konfiguration unter Beibehaltung der Administrator-UX. Ein Set aus Infrastrukturmodulen bietet eine hohe Verfügbarkeit, Load Balancing und erweiterte Monitoring-Funktionen.

Sicherheit	positiv
Funktionalität	sehr positiv
Integration	neutral
Kompatibilität	neutral
Usability	positiv

Tabelle 28: Bewertung von MT4 Networks



Als PAM-Produkt auf Enterprise-Ebene, das weiterentwickelt wird und wettbewerbsfähig ist, ist es das Ziel von Senhasegura, sich über Brasilien hinaus auf Märkten in Lateinamerika, Europa sowie im Nahen Osten weiterzuentwickeln. Senhasegura ist ein sinnvoller PAM-Anbieter für Unternehmen jeder Größe in Südamerika, die regionale Integration und Sprachunterstützung wünschen. Senhasegura sollte weitere Sprachen unterstützen und ein effektives Partnerökosystem aufbauen, um auf globalen Märkten erfolgreich zu sein.

5.14 One Identity

Das kalifornische Unternehmen One Identity, ein Quest Software Business, bietet eine gute Auswahl von Produkten für die Verwaltung und die Absicherung von privilegiertem Zugriff für Unternehmen an. Als einst sehr beliebte PAM- und IGA-Technologie hat Quest unter dem Dach von Dell beträchtliche Marktanteile verloren, bevor es sich im Jahr 2016 abspaltete. Seitdem hat Quest signifikante Investitionen in Marketing und Entwicklung sowie in Innovationen unternommen, um im Markt aufzuholen, und hat in einigen Fällen die Erwartungen des Markts deutlich übertroffen.

Stärken	Herausforderungen
• Starke Funktionen sowohl für Unix/Linux sowie für Windows-Umgebungen • Basierend auf etablierter, in der Branche beliebter Technologie • Unix-AD Bridging und Privilege Account Management in AD-Hybridumgebungen • Globale Präsenz und ein starkes Partnerökosystem • Integration mit One Identity Manager und anderen One Identity-Produkten	• Begrenzte Anpassungsmöglichkeiten insbesondere für Privileged Password Manager • Eingeschränkte Unterstützung für Cloud-Anwendungen und -Infrastruktur • Erhöhte, aber begrenzte DevOps-Unterstützung

Tabelle 29: Bedeutende Stärken und Schwächen von One Identity

Das PAM-Portfolio von One Identity zielt auf die Verwaltung und Absicherungen der meisten PAM-Anwendungsfälle ab und umfasst One Identity Safeguard, Privileged Access Suite for Unix, Active Roles sowie Privilege Manager for Windows.

Das als Hardware Appliance bereitgestellte Safeguard for Privileged Passwords (SPP) ist eine Vault-Komponente für SAPM. Safeguard for Privileged Analytics (SPA) wird zusammen mit der PSM-Komponente — Safeguard for Privileged Sessions (SPS) — als Virtual Appliance oder Hardware Appliance angeboten und analysiert privilegierte Aktivitäten, um Anomalien zu erkennen.

Die als installierbares Client-Paket erhältliche Privileged Access Suite (PAS) for Unix ist eine umfassende Suite mit Unix-AD Bridging, Authentifizierung, Root-delegation, Sudo-Erweiterung und zentralisierter Verwaltung von Richtlinien in Unix-basierten Systemen. Privilege Manager for Windows bietet CPEDM-Funktionen für Windows-basierte Plattformen. Ein weiteres Schlüsselprodukt — Active Roles — bietet Privileged Account Management in AD-Hybrid-Umgebungen.

Während Produkte für Password Vaults und Session Management gut integriert wurden und in einer einzigen Managementkonsole verfügbar sind, ist die Integration mit CPEDM-Produkten noch Teil der zukünftigen Roadmap von One Identity.

Sicherheit	positiv
Funktionalität	sehr positiv
Integration	positiv
Kompatibilität	positiv
Usability	sehr positiv

Tabelle 30: Bewertung von One Identity

One Identity hat die vorgeschlagene Roadmap ausgeführt, die einige wichtige Meilensteine in Bezug auf Produktverbesserungen umfasste, und wir erwarten, dass das Unternehmen bei einer weiterhin starken Ausführung langfristig erfolgreich sein wird und einen klaren Entwicklungspfad für bestehende und neue Kunden aufzeigt.

5.15 Osirium

Das britische Unternehmen Osirium bietet eine PxM-Plattform an, die aus verschiedenen Produkten für Privileged Access Management besteht. Diese umfassen PAM (Privileged Account Management), PSM (Privileged Session Management), PTA (Privileged Task Automation) und PBM (Privileged Behavior Management) sowie einen MAP-Server. Osirium verfolgt einen eigenständigen PAM-Ansatz, indem es Passwörter von Benutzern löst und sie stattdessen Benutzerrollen zuweist. Neben der agentenlosen Herangehensweise liegt die Stärke von Osirium in der task-basierten Ausführung von Privilegien, was aus betrieblicher Sicht effizienter ist, insbesondere für routinemäßige Verwaltungsaufgaben.

Stärken	Herausforderungen
• Der task-basierte Ansatz ermöglicht mehr Sicherheit, betriebliche Effizienz und geringere Fehlerraten. • Der Gateway-Ansatz bietet Flexibilität zur Erweiterung von PAM für verschiedenste Zielsysteme, insbesondere ICS-Umgebungen. • Gute Unterstützung für Privileged Behavior Analytics	• Keine konventionellen AAPM- und CPEDM-Funktionen • EPM fehlt • Task-basierter Ansatz nicht geeignet für dynamische oder fließende IT-Umgebungen • Begrenzte globale Präsenz, fehlendes globales Partnerökosystem

Tabelle 31: Bedeutende Stärken und Schwächen von Osirium

Osiriums Privileged Access Management-Produkt bietet grundlegende Unterstützung für die Verwaltung von Passwörtern für gemeinsam verwendete Konten und erzwingt das Prinzip des Least Privilege Access. Das Privileged Session Management-Produkt bietet die erforderlichen Funktionen zur Überwachung und Aufzeichnung von privilegierten Sessions sowohl in Befehlszeilen- als auch in grafischen Sessions. Die PxM-Plattform von Osirium umfasst Privileged Task Management und hebt sich von Konkurrenzprodukten ab, indem sie einen task-basierten Ansatz für privilegierte Aktivitäten bietet. Während dieser Ansatz eine effiziente Herangehensweise in ausgereiften IT-Umgebungen darstellen kann, hat er nur eingeschränkte Relevanz für dynamische oder fließende IT-Umgebungen, in denen es schwierig sein kann, administrative Aufgaben vorab zu definieren.

Der task-basierte Ansatz von Osirium kann den Bedarf an CPEDM mittels Packaging von erhöhten Privilegien in einem vordefinierten Task eliminieren und ermöglicht das Delegieren von Tasks. Dank einer Reihe integrierter Vorlagen für vorkonfigurierte Tasks und einer guten Protokollunterstützung können Tasks über verschiedene Geräte und Managementschnittstellen ausgeführt werden. Der „Gateway"-Ansatz von Osirium könnte insbesondere für unterstützende PAM-Anforderungen in Legacy- sowie ICS-Umgebungen (Industrial Control System) geeignet sein.

Sicherheit	positiv
Funktionalität	neutral
Integration	positiv
Kompatibilität	neutral
Usability	positiv

Tabelle 32: Bewertung von Osirium

Osirium stellt eine vielversprechende Alternative zu konventionellen Vault-Technologien auf dem PAM-Markt dar und zielt darauf ab, Mehrwert für Unternehmen zu schaffen, die für einen solchen Ansatz bereit sind. Osirium verfügt über einen kleinen Kundenstamm, der sich in erster Linie auf Großbritannien konzentriert, sowie über ein kleines Partnernetzwerk und ist eine gute Wahl für Unternehmen, die auf ICS/IIoT ausgerichtet sind.

5.16 Sectona

Das im Jahr 2017 im indischen Mumbai gegründete Unternehmen Sectona ist der jüngste der neuen Akteure auf dem PAM-Markt und bietet das PAM-Produkt Spectra Privileged Access Management an. Sectona wird von seinen ursprünglichen Gründern finanziert und hat Mittel zur Unterstützung seiner laufenden Geschäftstätigkeit gesammelt. Dank des erfahrenen Managements bietet Sectona einen kollaborativen, plattform-übergreifenden PAM-Ansatz, der auf die Umsetzung von Geschäftswerten durch Enterprise-Integrationen abzielt.

Stärken	Herausforderungen
• Relativ junges Startup mit erfahrenem Management • Schnellere Reaktionen auf Kundenfragen und Individualisierungen dank kleinerer Unternehmensgröße • Der kollaborative, plattformübergreifende Ansatz ermöglicht Integrationen, welche die gewünschte Flexibilität liefern. • Gutes Verständnis von regionalen PAM-Anforderungen und Kundenwünschen • Wenige, aber gut ausgewählte Partner	• Trotz eines markanten Ansatzes stößt dieser Anbieter verspätet zu einem etablierten Marktsegment. • Wachsendes, aber eingeschränktes PAM-Funktionsset • Funktionen begrenzt auf PSM ohne bewährtes AAPM, CPEDM und Privilege Analytics • Seine Präsenz ist fast ausschließlich auf Asien begrenzt, mit wenigen Kunden im Nahen Osten sowie in Nordamerika.

Tabelle 33: Bedeutende Stärken und Schwächen von Sectona

Spectra bietet ein integriertes Plugin Designer Kit (PDK), das es Kunden ermöglicht, auch ohne umfangreiche Coding-Erfahrung eigene Konnektoren zur Unterstützung von PSM und SAPM für nicht standardmäßige Anwendungen zu entwickeln und auf diese Weise Entwicklungskosten einzusparen. Die Stärke von Spectra ist die PSM-Technologie, die Zugriff auf privilegierte Sessions über alle Browser mit HTML5-Unterstützung auf beliebigen Plattformen bietet, ohne dass Agenten oder Plug-Ins installiert werden müssen. Dies beinhaltet SSH- und RDP-Sessions sowie Unterstützung für Thick-Client-Anwendungen mittels Virtualisierung über Jump-Hosts. Sectona Push for Desktop and Mobile bietet Benachrichtigungen zu hochriskanten Aktivitäten in Echtzeit sowie die Kontrolle über PCs und mobile Geräte.

Sicherheit	neutral
Funktionalität	neutral
Integration	neutral
Kompatibilität	neutral
Usability	neutral

Tabelle 34: Bewertung von Sectona

Spectra PAM bietet zusätzlich ein Erkennungsmodul für Plattformen mit virtueller und Cloud-Infrastruktur, einschließlich VMWare, AWS und Azure zwecks Erkennung von Accounts. Spectra umfasst ein Kollaborationsmodul, dass die Abhängigkeit von Screen Sharing-Tools von Drittanbietern zum Zweck der gemeinsamen Nutzung kritischer privilegierter Sessions mit internen und externen Nutzern verringert. Da keine Plug-Ins erforderlich sind, funktioniert das Screen Sharing sowie die Zusammenarbeit bei Spectra über einen einzigen Port, sodass die gesamte Session aufgezeichnet werden kann.

Spectra bietet keine detaillierten CPEDM-, EPM- oder Privilege Analytics-Funktionen und ist somit keine vollständige PAM-Plattform. Durch die frühe Unterstützung für Privileged Task Automation und die einfache Integration mit verschiedenen ITSM- und SIEM-Plattformen ist Spectra von Sectona eine gute Wahl für kleine bis mittlere Unternehmen, die sichere Remote Access- sowie PSM-Funktionen mit Unterstützung für schlankere privilegierte Operations und regionaler Integration suchen. Sectona bietet Spectra außerdem als MSP-Edition zur Bereitstellung von verwalteten PAM-Services für IT-Serviceanbieter an.

5.17 SSH.COM

Das im finnischen Helsinki ansässige Unternehmen SSH.COM bietet PrivX als primäres Produkt auf dem PAM-Markt an. PrivX ist ein relativ neues SSH.COM-Produkt auf dem Markt und soll eine Alternative zu konventionellen Shared Account Password Management-Technologien darstellen, indem es eine Zertifikatsautorität für SSH- und RDP-Zugriff bereitstellt. PrivX agiert als Zertifikatsautorität für SSH- und RDP-Clients, indem es Zertifikate mit kurzer Gültigkeit für On-Demand-Zugriff ausstellt. Während dieser Ansatz Password Vaults für spezifische SSH- und RDP-Zugriffe überflüssig macht, bietet das Produkt keine Lösung für grundlegende Anwendungsfälle in Bezug auf Shared Account Password Management, wie beispielsweise Password Vaulting oder Passwortrotation. Darüber hinaus bietet PrivX keine Session Management-Funktionen, wie z. B. Session Auditing, Recording oder Monitoring von privilegierten Aktivitäten.

Stärken	Herausforderungen
• Ein einzigartiger Ansatz mit begrenzter Reichweite zur Verwaltung von SSH- und RDP-Zugriffen mit guten Session Monitoring-Funktionen • Globale Präsenz mit einem starken Partnerökosystem	• Mangelnde grundlegende PAM-Funktionen, wie Passwortmanagement für gemeinsam verwendete Konten sowie Privilege Elevation • Detaillierte, aber eingeschränkte Funktionen zur Verwaltung von SSH-Schlüsseln und Session Monitoring • Fehlender Fokus auf Innovationen hat das Unternehmenswachstum in den letzten Jahren gehemmt • Keine Unterstützung für hochentwickelte PAM-Funktionen, wie Privileged Behavior Analytics Relatively • Eingeschränkte Unterstützung für Windows-Systeme, einschließlich RDP-Sessions sowie Session Indexing und Aktivitätssuche

Tabelle 35: Bedeutende Stärken und Schwächen von SSH.COM

PrivX verspricht die Bereitstellung von rollenbasierten On-Demand-Zugriffen mittels kurzfristig gültigen Zertifikaten und kann über OpenID Connect nicht nur für eigene — selten eingesetzte — Directorys, sondern auch für AD-, LDAP- und andere Directorys von Drittanbietern eingesetzt werden. Neben der Verwaltung von Zugriffen auf Hosts in On-Premise- sowie Cloud-Umgebungen bietet PrivX eine konsolidierte Ansicht von Zielressourcen in Hybrid-Umgebungen zur Verwaltung von Zugriffen und zur Überprüfung von Nutzeraktivitäten. Die Account Management-Funktionen beschränken sich auf SSH- und RDP-Zugriffe und bieten keine Password Vaults für System- oder Anwendungskonten. Universal SSH Key Manager bietet Lifecycle Management für SSH-Schlüssel, was die Erkennung, Bereitstellung, Rotation und Deaktivierung von Schlüsseln auf IT-Endpunkten umfasst. Während CryptoAuditor detailliertes Session-Monitoring sowie Filter auf Protokollebene bietet, werden verschiedene PSM-Funktionen wie Dual Control oder Session Delegation nicht unterstützt.

Sicherheit	positiv
Funktionalität	neutral
Integration	positiv
Kompatibilität	positiv
Usability	neutral

Tabelle 36: Bewertung von SSH.COM

Mit PrivX bietet SSH.COM einen einzigartigen Ansatz zur Verwaltung von Zertifikaten für SSH- und RDP-Zugriffe, indem das Produkt eine Zertifikatsautorität bilde und Anmeldeinformationen für einmaligen Zugriff ausstellt. SSH.COM ist interessant für Unternehmen, die entweder einen vault-freien Ansatz zur Verwaltung von RDP- und SSH-Zugriffen mit grundlegenden PSM-Funktionen bevorzugen, oder die ihre vorhandene PAM-Lösung durch diese Funktionen ergänzen möchten. In diesem Fall sollten die Integrationsanforderungen evaluiert und entsprechend berücksichtigt werden.

5.18 Thycotic

Das in Washington D. C. (USA) ansässige Unternehmen Thycotic bietet seine Secret Server-Plattform als primäre PAM-Produkt auf dem Markt an. Secret Server ist für seine umfassenden Funktionen sowie für seine einfache Implementierung und Konfiguration bekannt, die Produktimplementierungs- und Upgrade-Zyklen signifikant verringern können. Die vor kurzem geschlossene Partnerschaft zwischen Thycotic und IBM hat die Marktexpansion von Thycotic mithilfe des großen Kundenstamms, der starken Präsenz sowie der regionalen Verbindungen von IBM neben einem starken globalen Vertriebs- und Marketingteam beschleunigt. Während diese Partnerschaft Cross-Selling-Möglichkeiten sowohl für Thycotic als auch IBM bedeutet, muss der gewünschte Mehrwert für bestehende Kunden durch die tiefere technologische Integration von Secret Server mit der IBM Cloud-Plattform sich noch einstellen.

Stärken	Herausforderungen
• Unterstützung für eine große Zahl von Zielsystemen • Einfache und effiziente Benutzeroberfläche • Unterstützung für mobilen Zugriff • Starke Unterstützung für AAPM • Die Partnerschaft mit IBM vergrößert die Vertriebs- und Marktreichweite • Einfache Implementierung und Konfiguration • Bereit für die Cloud, ausgereiftes PAMaaS in Betrieb • Einfache Anpassung und Unterstützung für Microsoft-Plattform	• Auf der Basis des .NET-Frameworks, läuft in erster Linie auf Windows-Stacks

Tabelle 37: Bedeutende Stärken und Schwächen von Thycotic

Durch die frühe Einführung der PAMaaS-Plattform Secret Server Cloud und der Übernahme von Arellia zwecks Bereitstellung von Windows EPOM verzeichnete Thycotic in den letzten Jahren ein enormes Wachstum. Eine aggressive und effektive Nutzung von Vertriebs- und Marketingkanälen hat wesentlich zu dieser eindrucksvollen Wachstumsrate beigetragen.

Neben den häufigsten PAM-Funktionen bietet Thycotic Secret Server auch Unterstützung für eine große Zahl von Zielsystemen sowie ein großes Set aus APIs zur individuellen Anpassung von Secret Server an. Privilege Manager ist die agentenbasierte EPM-Lösung von Thycotic für Endpunkte unter Windows und Mac mit umfangreichen EPM-Funktionen, einschließlich Application Control und Privilege Elevation. Die Privilege Behavior Analytics-Lösung von Thycotic überwacht Nutzeraktivitäten in Secret Server-Implementierungen und kann bei der Erkennung von Anomalien auf der Grundlage eines Alert-Schwellenwerts Warnungen ausgeben.

Sicherheit	sehr positiv
Funktionalität	sehr positiv
Integration	sehr positiv
Kompatibilität	positiv
Usability	sehr positiv

Tabelle 38: Bewertung von Thycotic

Dank seiner beeindruckenden Palette an OOB-Integrationen und der Unterstützung für Cloud-Infrastrukturen sowie DevOps-Prozesse ist Thycotic interessant für Unternehmen, die eine umfassende und effektive PAM-Lösung mit schnelleren Implementierungszyklen und einfacher Konfiguration suchen und die intern mehr auf den Technologie-Stack von Microsoft ausgerichtet sind.

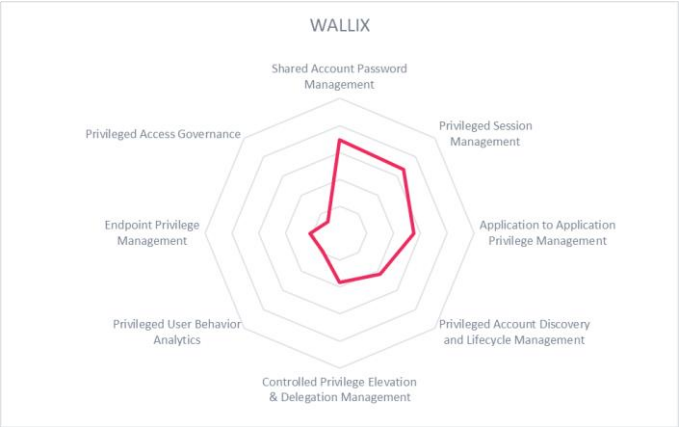
5.19 WALLIX

Das in Frankreich ansässige Unternehmen WALLIX bietet WALLIX Bastion als sein primäres PAM-Produkt auf dem Markt an. Im Kern von Bastion stehen Password Management, Session Management sowie Access Management mit integrierten Zugriffsanfragen und -Genehmigungsfunktionen. WALLIX verfügt über einen großen Implementierungsstamm in Europa sowie im Nahen Osten sowie über eine eingeschränkte Präsenz in Nordamerika und in Asien.

Stärken	Herausforderungen
• Unterstützung für eine große Zahl von Zielsystemen • Führende PSM-Funktionen • Webzugriffs-Gateway sowie eine einzige Managementkonsole für alle Bastion-Instanzen • Mehrmandantenfähig & HA-Unterstützung • Starke Ausführung einer gut durchdachten Produkt-Roadmap	• Kein EPM-Modul • Eingeschränkte Funktionen für CPEDM und Privileged Analytics • Keine Unterstützung für Cloud-Plattformen und DevOps • Eingeschränkte Partnerschaften und Kompatibilität mit Sicherheitstools von Drittanbietern • Eingeschränkte Partnerökosysteme und Präsenz außerhalb von EMEA

Tabelle 39: Bedeutende Stärken und Schwächen von WALLIX

Dank seines proxybasierten Ansatzes agiert Bastion als Webzugriffs-Gateway samt Protokollzugriff und hoher Verfügbarkeit. Zusätzliche Jump-Server können auf einfache Weise konfiguriert werden, um Bastion für neue Zielsysteme hochzuskalieren. Dank seiner Mehrmandantenfähigkeit ist Bastion in den meisten Implementierungsformen verfügbar, wobei mehrere MSSPs einen verwalteten, gehosteten PAM-Service anbieten. WALLIX Bastion bietet eine starke Verschlüsselung und hochentwickelte Session Management-Funktionen ohne Interferenzen mit der administrativen UX.



Sicherheit	sehr positiv
Funktionalität	sehr positiv
Integration	positiv
Kompatibilität	positiv
Usability	sehr positiv

Tabelle 40: Bewertung von WALLIX

Bastion AAPM verwendet den Fingerabdruck des den Service oder die Anwendung aufrufenden Prozesses, um das Auschecken der Anmeldeinformationen aus dem Bastion-Vault abzusichern. Bastion bietet ein eingeschränktes CPEDM mit Injektion von Superuser-Anmeldeinformationen an, aber kein Sudo oder Shell-Ersatz.

WALLIX stellt kein Desktop-EPM bereit. Die Integration mit anderen Sicherheitstools, einschließlich IGA für Privileged Access Governance, ist eingeschränkt und umfasst nicht die erforderliche Kompatibilität. Privileged Analytics bietet WALLIX aktuell nicht an, aber das Unternehmen plant die Einführung dieser Funktion im weiteren Verlauf des Jahres 2019. WALLIX hat in den letzten Jahren signifikante Fortschritte gemacht, indem das Unternehmen eine gut strukturierte Produkt-Roadmap verfolgt. Auf diese Weise konnte es sich in diesem LC im Bereich der Product Leader positionieren. WALLIX hat sich eindeutig von einem Anbieter für Remote Session Management-Technologien zu einem vollständigen PAM-Lösungsanbieter auf einem bereits etablierten Markt entwickelt. Unternehmen mit häufigen SAPM- und AAPM-Anforderungen, die eine starke Verschlüsselung sowie PSM benötigen, sollten einen genaueren Blick auf WALLIX Bastion werfen.

6 Vielversprechende Anbieter

Neben den in diesem Leadership Compass im Detail vorgestellten Unternehmen beobachten wir noch einige weitere Anbieter, die nennenswerte Privileged Access Management-Funktionen auf dem Markt anbieten. Einige dieser Anbieter haben entschieden, aus unternehmensinternen Gründen nicht an diesem Leadership Compass teilzunehmen, aber da wir sie interessant und erwähnenswert finden, haben wir beschlossen, sie in diesem Kapitel zu nennen. Diese Anbieter passen entweder nicht vollständig in das PAM-Marktsegment, da sie einen anderen Ansatz bezüglich PAM verfolgen, oder weil sie aktuell nicht die erforderlichen Auswahlkriterien erfüllen, um in unserem Leadership Compass berücksichtigt zu werden. Im Folgenden stellen wir diese Anbieter kurz vor.

6.1 Deep Identity

Deep Identity ist in Singapur ansässig und ein regionaler Anbieter für Identity Management-Software. Es bietet Deep PIM als primäres PAM-Produkt an, das prinzipiell aus Software-Plugins aus Deep Identity Manager besteht und einen Privileged Access Server (PAS) umfasst, der als Gateway zwecks Errichtung und Verwaltung des Zugriffs auf Zielsysteme fungiert. Während Deep IM Workflows auf die Bereitstellung von Konten und zur Genehmigung von Zugriffsanfragen ausdehnt, fehlen dieser Lösung mehrere grundlegende PAM-Funktionen, wie u. a. die Erkennung von privilegierten Konten, Shared Account Password Management (SAPM) sowie Controlled Privilege Elevation & Delegation Management (CPEDM).

Obgleich das PIM-Gateway Unterstützung für privilegierte RDP-Verbindungen zu Windows-Servern sowie Session Logging & Recording mit textbasierten Suchfunktionen bietet, bietet es keine Unterstützung für die Verwaltung von privilegierten Konten und Aktivitäten in Cloud-Anwendungen und -Plattformen.

Mit einer guten lokalen Präsenz in Asien, insbesondere Südostasien (SEA) ist Deep PIM eine gute Ergänzung für bestehende Deep Identity Manager-Implementierungen, um zusätzliche Privileged Session Management-Funktionen zu nutzen. Außerdem spricht es Unternehmen mit grundlegenden PSM-Anforderungen an, die regionale Implementierungs- und Integrationsunterstützung benötigen.

6.2 Devolutions

Das kanadische Unternehmen Devolutions bietet das Produkt Devolutions Password Server als primäres PAM-Produkt an, dass Password Vaults und Passwortmanagement für Geschäftskunden sowie IT-Administratoren bereitstellt.

Die Devolutions Privileged Account Management-Plattform ist als On-Premises-Option verfügbar und ermöglicht rollenbasierten Zugriff für Benutzer, die sich über den Password Server als gemeinsamem Einstiegspunkt mit Zielsystemen verbinden. Webbasierte Anmeldeinformationen werden synchronisiert, gespeichert und mithilfe der Browser-Erweiterung Devolutions Web Login nachverfolgt, die für die häufigsten Webbrowser verfügbar ist. Mit dieser Erweiterung können Benutzer Zielwebseiten über die Devolutions-Webkonsole öffnen, ohne eigene Anmeldeinformationen verwenden zu müssen.

Der Devolutions Launcher ermöglicht Credentials Injection über den Password Server, um Remote-Sessions über verschiedene Verbindungsprotokolle von der Admin-Schnittstelle aus starten zu können. Die Integration mit Remote Desktop Manager bietet Privileged Session Management über Remote-RDP-Verbindungen und kann mit einer Vielzahl von Anbietern für VPN-Verbindungen integriert werden — für eine nahtlose Verbindung zu Remote-Zielsystemen.

Dank Password Safe stellt Devolutions eine grundlegende Lösung für Shared Account Password Management zur Verfügung, die sich auf eine einfache Verwendung und Anwendungsfälle mit Remote Support Management konzentrieren. Untersuchen, die SAPM-Funktionen auf Einsteigerniveau und sicheren Remote Access benötigen, sollten einen genaueren Blick auf Devolutions setzen.

6.3 HashiCorp

Das US-amerikanische Unternehmen HashiCorp aus San Francisco ist ein Anbieter für Anwendungsentwicklung und Implementierungsmanagementsoftware für Rechenzentren. Auf der Grundlage von Open Source bietet HashiCorp ein sicheres Password Vault, dass sich in die Anwendungsentwicklungs- und Implementierungsmanagementmodule desselben Anbieters integrieren lässt, um eine höchst integrierte DevOps-Plattform zu erzielen.

Das Vault ist in drei Varianten verfügbar — für Einzelnutzer, Teams und Unternehmen — je nach Komplexität der beteiligten Entwicklungs- und Implementierungsprozesse. Während die grundlegenden Funktionen von Password Vaults, wie Verschlüsselung, sichere Speicherung, Schlüsselrotation, Vault-Agent, Richtlinien für die Zugriffssteuerung sowie Checkout-Workflows für Anmeldeinformationen in allen drei Vault-Varianten enthalten sind, sind MFA, Governance sowie weitere Funktionen, die für die Unterstützung von Umgebungen mit mehreren Rechenzentren — wie beispielsweise Notfallwiederherstellung und Replizierung — erforderlich sind, nur als Teil der Team- oder Enterprise-Version erforderlich.

Als unvollständige PAM-Plattform bietet HashiCorp Password Vaults, sowie sicheres Application-to-Application Password Management zur Unterstützung von DevOps-Initiativen auf Enterprise-Ebene. Während mehrere andere PAM-Anbieter ähnliche Funktionen zur Unterstützung von DevOps anbieten, stellt HashiCorp einen guten Ausgangspunkt für Unternehmen dar, die PAM im Rahmen von Anwendungsentwicklungs- und -implementierungsprozessen einführen möchten.

6.4 HelpSystems

Das in Minnesota ansässige, US-amerikanische Unternehmen HelpSystems bietet Sicherheitslösungen für Infrastrukturen mit IBM i-Series. Das PowerTech-Portfolio des Unternehmens konzentriert sich auf Zugriffskontrolle und Session Monitoring für privilegierte Benutzer auf IBM iSeries- sowie Unix-/Linux-Systemen. PowerTech umfasst eine vollständige PAM-Lösung mit separat lizenzierten Modulen für Passwortmanagement, MFA, Session Recording & Monitoring sowie Privilege Elevation.

PowerTech Authority Broker bietet die kontrollierte Erhöhung von Privilegien für IBM iSystems und ermöglicht detailliertes Auditing und Logging von Administratoraktivitäten. HelpSystems übernahm das kalifornische Unternehmen Fox Technologies sowie dessen Produkt BoKS Server Control als Flaggschiff-Lösung für die Zugriffssteuerung unter Unix & Linux. In Form des PowerTech Identity and Access Managers ergänzt der Anbieter sein Portfolio nun um Passwortmanagement für gemeinsam verwendete Konten sowie Privilege Elevation für Unix- und Linux-Systeme.

HelpSystems stellt keine Funktionen zur Erhöhung von Privilegien oder zur Verwaltung von Endpunkten für Windows-Plattformen bereit. Mit einem der seltenen Produkte, welche die IBM iSerie unterstützen, spricht das PowerTech-Portfolio von HelpSystem Unternehmen an, die Mainframe-Privilegien verwalten müssen und eine zentralisierte Administration auf IBM iSerien- und Unix-/Linux-Systemen in einer IT-Hybrid-Umgebung fordern.

6.5 IdentityAutomation

Das im US-amerikanischen Houston ansässige Unternehmen IdentityAutomation ist ein IAM-Lösungsanbieter. Es bietet RapidIdentity Privileged Access Management als sein primäres PAM-Produkt auf dem Markt an. Identity Automation hat sich vom Systemintegrator zum Systemanbieter entwickelt und bietet eine große Zahl von IAM-Technologien, wobei Privileged Access Management eine der neuesten Ergänzungen des RapidIdentity-Portfolios ist. RapidIdentity bietet ein grundlegendes PAM-Funktionsset mit Shared Account Passwird Management, Application-to-Application Password Management sowie Basisfunktionen zum Auditing und Logging privilegierter Aktivitäten. SSH-Schlüssel werden unterstützt.

Mithilfe von automatisierten Workflows zur Erhöhung von Privilegien unterstützt RapidIdentity PAM integriertes MFA für privilegierten Zugriff, aber es fehlen Funktionen zur kontrollierten Erhöhung von Privilegien sowie für Session und Endpoint Privilege Management. Durch die Übernahme von Healthcast, einem Anbieter für Zugriffsmanagementlösungen für das Gesundheitswesen bietet IdentityAutomation die erforderlichen Konnektoren für spezialisierte Systeme für das Gesundheitswesen sowie die erforderliche Domänenerfahrung. RapidIdentity PAM ist interessant für Organisationen, insbesondere im Gesundheitswesen, die eine integrierte PAM-Lösungen mit Password Management, MFA sowie grundlegendem Auditing und Reporting zu privilegierten Aktivitäten benötigen.

6.6 Iraje

Das indische Unternehmen Iraje bietet Privileged Identity Manager (PIM) als vollständige PAM-Lösung an, die über interessante Funktionen und die nötige Flexibilität verfügt, um sich an wechselnde Geschäftsanforderungen anzupassen. Durch seine agentenlose Herangehensweise an PAM unterstützt Iraje eine große Zahl von Zielsystemen und ist als Software sowohl als Virtual Appliance als auch als Hardware Appliance verfügbar.

Iraje bietet einen nativen Datenbank-Client, einen Schema Extender sowie ein Datenbanküberwachungsmodul in Verbindung mit seinem PIM-Produkt, das sich auf die Absicherung privilegierter Datenbankoperationen konzentriert. Es sind weitere Module für 2FA und SSO verfügbar, aber es fehlen Endpoint Privilege Management sowie hochentwickelte AAPM-Funktionen, wie Application oder Process Fingerprinting.

Die PIM-Lösung von Iraje zielt darauf ab, eine umfassende PAM-Lösung für KMU in Asien bereitzustellen, und soll Kunden ansprechen, die Flexibilität benötigen, um PAM an detailliertere Auditing- und Monitoring-Anforderungen bezüglich Datenbankoperationen in einer verteilten IT-Umgebung anzupassen. Allerdings zeigt das Unternehmen nicht nur augenscheinlich inkonsistente Marketingstrategien, sondern es fehlt auch ein ausreichendes Feedback aus der Branche, um die Produktreife sowie die Kundenaufklärung von Iraje bewerten zu können.

6.7 MasterSAM

Der in Singapur angesiedelte Anbieter MasterSAM, ein Unternehmen der Silverlake Group, bietet mehrere separat lizenzierte Produkte zur Verwaltung von privilegiertem Zugriff. MasterSAM Star Gate verfolgt einen proxybasierten Ansatz bezüglich Shared Account Password Management (SAPM) sowie Application to Application Password Management (AAPM) mit integrierten SSO- und 2FA-Funktionen. MasterSAM's Produkte Secure @Windows und Secure @ Unix/Linux basieren auf einem hostbasierten Ansatz bezüglich Controlled Privilege Elevation & Delegation (CPEDM) für Windows- und Unix-/Linux-Plattformen, wobei das Produkt Frontline Recording und Monitoring für Windows-Desktopumgebungen bereitstellt. Das Produkt MasterSAM Analyst stellt zentralisiertes Logging, Auditing sowie Review für privilegierte Aktivitäten bereit. Während hochentwickelte ARM-Funktionen fehlen, bietet MasterSAM ein vollständigeres und ausgereifteres PAM-Portfolio mit einem wettbewerbsfähigen Kosten-Nutzen-Vorschlag im Vergleich zu anderen etablierten Market Leaders weltweit. Das malaysische Unternehmen Firmus Security ist der größte Integrationspartner — das Unternehmen bietet Integration sowie Managed Host Services für MasterSAM PAM in der Region an.

MasterSAM bietet eines der vernünftigsten Preismodelle auf dem Markt und spricht APAC-basierte Unternehmen an, die regionale Integrationsunterstützung sowie Implementierungsflexibilität suchen, indem es einen proxybasierten, hostbasierten oder Hybrid-Ansatz verfolgt.

6.8 NRI Secure Technologies

Das in Japan ansässige Unternehmen NRI Secure Technologies bietet Funktionen für Privileged Session Management (PSM) primär mit seinem Produkt SecureCube Access Check an. Auf der Grundlage eines Gateway-basierten Ansatzes ist SecureCube Access Check eine Erweiterung des Powerbroker Password Safe von BeyondTrust. Die NTT Software Corporation baut auf seiner PAM-Lösung iDoperation auf der Grundlage von Access Check auf und bietet Session Recording, Monitoring und Review-Funktionen. Zur Unterstützung von Workflows für Genehmigungsanfragen mit rollenbasierten Zugriffskontrollrichtlinien bietet Access Check einen einzigartigen Ansatz für die Zugangskontrolle bezüglich privilegierter Nutzer. Access Check beinhaltet keine Funktionen für Application to Application Password Management (AAPM), aber das Produkt unterstützt Befehlsfilter sowie detailliertes Session Monitoring und Alerting. Darüber hinaus ermöglicht SecureCube Access Check auch Zugriffskontrolle sowie die Überwachung von Dateitransfers und Datenbanksessions für Oracle RDBMS.

Da der Großteil seines Kundenstamms in Japan ansässig ist, eignet SecureCube Access Check sich insbesondere für ostasiatische Unternehmen, die regionale Integrationsunterstützung sowie detailliertes Privileged Session Auditing & Monitoring wünschen.

6.9 ObserveIT

ObserveIT bietet eine umfassende, agentenbasierte PSM-Plattform, die in einer Vielzahl von IT-Systemen implementiert und skaliert werden kann. ObserveIT stellt detaillierte Funktionen zur Analyse des Nutzerverhaltens sowie zur Live-Aufzeichnung von Sessions bereit und ist einer der wenigen spezialisierten Anbieter, die aus dem Bereich des Session Recording and Monitoring (SRM) stammen und ihr Geschäftsfeld auf andere PSM-Funktionen ausgedehnt hat. Zusätzlich zur Überwachung und Aufzeichnung von CLI- und GUI-Sessions in visuellen Formaten, was die Erstellung eines detaillierten Benutzeraktivitätenprotokolls aus den aufgezeichneten Daten ermöglicht, bietet ObserveIT hochentwickelte User Behavior Analytics, die Anomalien im Benutzerverhalten erkennt und Warnungen ausgibt. ObserveIT ermöglicht außerdem Live-Reaktionen auf Sessions, sodass diese auf der Grundlage von Daten aus User Behavior Analytics oder von externen Produkten, wie zum Beispiel SIEM-Tools (Security Information and Event Management) zur Laufzeit unterbrochen werden können.

Bei der visuellen Aufzeichnung über Endpunkte kann ObserveIT Sessions aus einer Vielzahl von Systemen erfassen. Es unterstützt alle wichtigen Protokolle, wie RDP (Remote Desktop Protocol), einschließlich Citrix-Varianten, SSH, Telnet und direkten Logins an Anwendungskonsolen. Ein agentenbasierter Ansatz ermöglicht eine detaillierte Protokollierung und somit eine sinnvollere und effizientere Aktivitätensuche im Gegensatz zu anderen, ähnlichen Lösungen, die in erster Linie proxy- oder gateway-basiert sind. Dank seines gut etablierten, globalen Partnerökosystems ist ObserveIT der Anbieter der Wahl für Unternehmen, die entweder nur über kritische PSM-Anforderungen verfügen oder die ihre vorhandene PAM-Implementierung durch stärkere PSM-Funktionen ergänzen möchten.

6.10 OnionID

Das amerikanische Unternehmen OnionID verfolgt einen differenzierten Ansatz bezüglich Privileged Access Management, indem es mehrere Bereitstellungsoptionen anbietet, einschließlich PAM-as-a-Service, On-Premise oder als cloud-gehosteter Service. Die Herangehensweise von OnionID an PAM hebt sich insbesondere durch die Bereitstellung von fertigen Vorlagen und Zugriffsanfrage-Workflows für das Passwortmanagement durch verschiedene Web- und SaaS-Anwendungen über eine gemeinsame Managementkonsole ab. Im Rahmen einer agentenlosen Lösung stellt OnionID eine Ebene von grundlegenden PAM-Steuerungen bereit, die ein natives oder drittes Authentifizierungsverfahren vorhandenen Methoden für privilegierten Zugriff vorzieht und eine Befehlsfilterung in Echtzeit sowie die Kontrolle über bereits erstellte Sessions ermöglicht.

Zusätzlich zur Unterstützung von DevOps-Initiativen durch die Bereitstellung einer Out-of-the-Box-Integration mit den meisten DevOps-Tools bietet OnionID SSH Key Management sowie Privileged Behavior Analytics auf der Basis von Endpunkt- und Benutzerattributen. OnionID stellt keine Funktionen für Application to Application Password Management (AAPM) oder für Controlled Privilege Elevation & Delegation bereit, aber es unterstützt grundlegende Befehlsfilter. Aufgrund einer Reihe von nativen Integrationen für SaaS, IaaS und Social Media-Plattformen stellt OnionID eine interessante Alternative zu einigen etablierten Anbietern von PAM as a Service dar, die aktuell cloud-basierte PAM-Services auf den Markt bringen. OnionID verfügt über einen kleinen, auf Nordamerika beschränkten Kundenstamm und ist interessant für Unternehmen, die eine schnelle Implementierung einer leichten Lösung für Privileged Session Management benötigen, die über vorhandene Authentifizierungstechnologien hinausgeht und fertige Autorisierungs-Workflows für die Verwaltung von privilegierten Zugriffen auf beliebte Cloud-Anwendungen und -Plattformen bereitstellt.

6.11 Oracle

Das kalifornische Unternehmen Oracle ist ein beliebter und fest etablierter Software-Gigant, der Oracle Privileged Account Manager als PAM-Produkt auf dem Markt anbietet. Dieses Produkt ist in erster Linie auf Oracle Middleware und Technologie-Stacks ausgerichtet. Dank hochentwickelter Integrationen für die Verwaltung von privilegierten Konten bezüglich Oracle Fusion Middleware-Produkten und der PaaS-Infrastruktur von Oracle ist OPAM die bevorzugte PAM-Option für Unternehmen, die bereits über verschiedene Oracle-Technologien verfügen. OPAM kann mit dem IAM-Portfolio von Oracle integriert werden, einschließlich Oracle Identity Governance (OIG), das die Bereitstellung von Konten, den rollenbasierten Administrationszugang sowie Workflows zur Überprüfung von Zugriffen auf Privileged Access Management ausdehnt.

Oracle hat der Produktentwicklungs-Roadmap für OPAM eine Weile lang weniger Aufmerksamkeit geschenkt, was sich ändern sollte. Die Lizenz für OPAM ist häufig ohne Aufpreis in größeren Produktpaketen von Oracle inbegriffen, wird von Kunden aber aufgrund der damit verbundenen komplexen Implementierung, fehlenden wichtigen PAM-Funktionen wie Privilege Elevation sowie der Integration mit fremden Produkten häufig nicht vollumfänglich genutzt. Die signifikante globale Präsenz der Technologieinfrastruktur von Oracle in Kombination mit seinem branchenführenden Vertrieb und dem starken Partnerökosystem sorgt dafür, dass OPAM eher eine Notwendigkeit als eine gezielte Wahl für viele Oracle-Kunden weltweit darstellt. Dies ändert sich jedoch, da viele PAM-Anbieter eine einfache Integration mit Oracle-Technologien anbieten.

6.12 Remediant

Remediant ist ein neuer Akteur auf dem Markt, der einen sehr markanten Null-Vertrauen-Ansatz bezüglich PAM verfolgt. Remediant bietet SecureONE als agent- und vault-loses PAM-Produkt an, um Herausforderungen rund um privilegierte Zugriffe zu lösen, indem es privilegierten Zugriff auf einer Just-in-Time- und Just-Enough-Basis (Least Privilege) bereitstellt. Auf diese Weise wird der Bedarf an gemeinsam verwendeten Passwörtern eliminiert. SecureONE nutzt einen Null-Vertrauen-Sicherheitsansatz und verringert die Angriffsfläche in signifikantem Maß, indem es den privilegierten Zugriff nur auf genehmigte System beschränkt und indem es 2FA in den Prozess implementiert, um zusätzliches Vertrauen zu schaffen.

SecureONE ermöglicht die Integration mit SIEM-Lösungen, um die Erkennung von privilegierten Eskalationen und die Identifizierung von potenziellen Risiken zu verhindert. Remediant verfolgt zwar einen bemerkenswerten PAM-Ansatz, aber dieser ist nicht vollkommen einzigartig und erinnert an das, was manche Anbieter wie Osirium auf dem PAM-Markt versuchen, um eine Nische zu finden.

Während SecureONE einen Ersatz für allgemeine Shared Account Password Management-Lösungen darstellt, fehlen dieser Lösung Funktionen für Controlled Privilege Elevation und Endpoint Privilege Management.

Unternehmen, die eine schnelle PAM-Implementierung wünschen und bereit für einen vault-losen PAM-Ansatz sind, sollten einen Blick auf StepONE werfen — Remediants Testversion von SecureONE zu Testzwecken und zur Demonstration der Produktfunktionen in Anbieter-PoC-Präsentationen.

6.13 Saviynt

Das in Kalifornien (USA) ansässige Unternehmen Saviynt ist einer der führenden Anbieter für cloud-basierte IGA-Services und tritt mit einem einzigartigen, vault-freien PAM-Ansatz auf dem PAM-Markt in Erscheinung. Saviynt PAM nutzt den Password Vault von Hashicorp. Das Produkt unterstützt aktuell SSH- und RDP-Verbindungen zu den am weitesten verbreiteten IaaS-Plattformen. Eine neue Verbindungsanfrage ruft einen temporären Docker-Container in der Saviynt-Cloud auf, um die Zielverbindung mittels Zugriffsgenehmigungen aus einer definierten Benutzerrolle darzustellen. Die privilegierten Aktivitäten im Container werden mithilfe eines Keystroke-Loggers erfasst und für die Durchsuchung und Analyse durch AWS Elastic Search bereitgestellt.

Dank seines markanten und neuen Ansatzes bezüglich Privileged Session Management-Technologien (PSM) ermöglicht Saviynt Just-in-Time sowie Just-for-Use privilegierten Zugriffe auf Zielanwendungen. Obgleich die Lösung sich derzeit noch in einer frühen Entwicklungsphase befindet, erwarten wir, dass sie die Erfahrung von Saviynt in Bezug auf Cloud-Implementierungen nutzen wird, und empfehlen deshalb Unternehmen, die bereit für die Cloud sind oder bereits über Produkte von Saviynt verfügen, diesen Ansatz in Zukunft im Auge zu behalten.

6.14 SecureLink

Das im texanischen Austin (USA) ansässige Unternehmen SecureLink ist ein Anbieter für sichere Remote Access-Lösungen als PSM-Produkt für die Verwaltung von Zugriffsprivilegien für Drittanbieter. Der Service von SecureLink wird in erster Linie in zwei Service-Varianten angeboten — SecureLink für Unternehmen und SecureLink für Anbieter.

SecureLink für Unternehmen zielt auf die Verwaltung des Remote-Zugriff durch Drittparteien ab und bietet Kontrollen für die Verwaltung von Zugriffsprivilegien für externe Anbietertechniker und Systemadministratoren mit detaillierter Protokollierung und Auditing von ausgelagerten Operationen. Die andere Servicevariante, SecureLink für Anbieter, konzentriert sich auf die Bereitstellung von Remote-Unterstützung für Kunden durch die Automatisierung von routinemäßigen Verwaltungsaufgaben und die Bereitstellung von task-basierten Privilegien. Beide Services erfordern das Gateway von SecureLink als leichtes Software-Plug-In, welches Remote-Zugriff für Technologieanbieter ermöglicht.

SecureLink ist eine gute Wahl in Bezug auf PSM-Technologien für Unternehmen, die PSM as a Service zur Kontrolle des Remote-Zugriff durch Dritte mit hochauflösender Auditing-Kontrolle für die erforderliche Sichtbarkeit von ausgelagerten privilegierten Operationen erfordern.

6.15 Venafi

Das amerikanische Unternehmen Venafi bietet TrustAuthority an, eine Plattform zum Schutz der Maschinenidentität, die außerdem ein umfangreiches Management zur Absicherung von privilegierten Zugriffen mittels SSH-Schlüsseln für Unternehmen jeder Größe und in unterschiedlichsten Branchen. SSH-Schlüssel werden für privilegierte Vorgänge in Unix-Umgebungen verwendet und stellen eine signifikante Sicherheitsbedrohung dar, da die meisten Unternehmen nicht über Richtlinien zum Umgang mit und zur Rotation von SSH-Schlüsseln verfügen. Venafi TrustAuthority bietet kontinuierliche Prozesse zur Erkennung, zur Inventur sowie zur Überwachung von SSH-Schlüsseln in der IT-Infrastruktur und ermöglicht eine automatische Schlüsselrotation.

Venafi TrustAuthority stellt eine zentrale SSH-Schlüsselverwaltung bereit und bietet eine unternehmensweise Sichtbarkeit über SSH-Schlüsselbestände und SSH Trust Relationships. Darüber hinaus ermöglicht Venafi die Automatisierung des SSH-Schlüssellebenszyklus von der Bereitstellung bis hin zur Deaktivierung von Schlüsseln. Dabei werden alle SSH-Schlüssel gesichert und überwacht, um das Risiko eines nicht autorisierten Zugriffs auf kritische Systeme zu minimieren.

Venafi wird von KuppingerCole nicht als reiner PAM-Anbieter eingestuft, da das Unternehmen wichtige Basisfunktionen, die für die Betrachtung als PAM-Anbieter erforderlich sind, nicht anbietet. Während mehrere Anbieter die Verwaltung von SSH-Schlüsseln als Teil ihrer SAPM-Lösung unterstützen, bietet Venafi die am besten entwickelten Funktionen für die Verwaltung von SSH-Schlüsseln auf dem Markt an. Venafi ist interessant für Unternehmen, die über eine kritische Sicherheitsanforderung bezüglich der Sichtbarkeit und Kontrolle von nicht verwalteten SSH-Schlüsseln sowie anderen Anmeldeinformationen verfügen, die für privilegierten Zugriff erforderlich sind.

6.16 XTON Technologies

Das in den USA ansässige Unternehmen XTON Technologies ist ein weiterer nennenswerter neuer Akteur auf dem Markt. Sein Produkt Xton Access Manager ist auf PAM-Anforderungen im mittleren Marktsegment ausgerichtet. XTON bietet Privileged Account Management und Server Access Control als Produktivlösungen an, die minimale Ressourcen zur Implementierung und Wartung benötigen und deshalb schlankere PAM-Vorgänge ermöglichen. Sein agentenloses Produkt für Account Management, XTAM, bietet einen webbasierten Password Vault sowie die Erkennung von Konten, Shared Account Password Management und Privileged Session Management, einschließlich Passwortrotation, Zugangsanfrage-Workflows und Session / Keystroke Recording mit Wiedergabe. Während XTON keine Funktionen für Controlled Privilege Elevation and Delegation Management (CPEDM) umfasst, unterstützt es Elevated Script Automation für routinemäßige Privilege-Eskalationsaufgaben, was die Effizienz des Administrators erhöht.

Für einen neuen Marktakteur bietet XTON ein deutlich breiteres PAM-Technologieportfolio, das sich gut an der Marktausrichtung orientiert und neue entstehende PAM-Anforderungen von Unternehmen erfüllt. XTAM kann mit Lösungen von ITSM-, SIEM- und MFA-Anbietern integriert werden und ist eine skalierbare Lösung für On-Premise-, Hybrid- oder Cloud-.

Implementierungen. Auf der Grundlage offener Software-Standards bietet XTON ein unbegrenztes Abonnement-Preismodell und bildet somit eine realistische Alternative zu vielen etablierten PAM-Anbietern dar, insbesondere im mittleren Marktsegment.

7 Methodologie

Der Leadership Compass von KuppingerCole dient dazu, einen Überblick über ein bestimmtes IT-Marktsegment zu geben und die führenden Akteure in diesem Marktsegment zu identifizieren. Dieser Compass unterstützt Sie dabei, die Anbieter und Produkte/Services in einem bestimmten Marktsegment ermitteln, die Sie bei Ihren Produktentscheidungen in Betracht ziehen sollten.

Wir weisen darauf hin, dass es die Entscheidung für einen Anbieter nicht ausschließlich auf der Grundlage der Informationen in diesem Bericht gefällt werden sollte.

Kunden sollten in jedem Fall ihre spezifischen Anforderungen definieren und detailliert analysieren, welche Lösungen ihre Anforderungen erfüllen. Dieser Report enthält keine Empfehlungen bezüglich der Wahl eines Anbieters für ein spezifisches Kundenszenario. Dies sollte ausschließlich auf der Grundlage einer detaillierteren und umfassenderen Analyse der Kundenanforderungen sowie eines präziseren Abgleichs dieser Anforderungen mit den Produktfunktionen erfordern, d. h. einer vollständigen Auswertung.

7.2 Arten von Leadership

Im Rahmen der Evaluation der Produkte in diesem Leadership Compass betrachten wir vier Leadership-Kategorien:

- Product Leader: Als Product Leader gelten bahnbrechende Produkte im jeweiligen Marktsegment. Diese Produkte bieten größtenteils das, was von Produkten in diesem Marktsegment erwartet wird. Sie sind ausgereift.
- Market Leader: Market Leader sind Anbieter mit einem großen, globalen Kundenstamm und einem starken Partnernetzwerk zur Unterstützung ihrer Kunden. Eine fehlende globale Präsenz oder eine unzureichende Vielfalt an Partnern kann verhindern, dass ein Anbieter zum Market Leader wird.
- Innovation Leader: Innovation Leader sind Anbieter, die neue Ideen, Systeme oder Methoden im jeweiligen Marktsegment entwickeln. Sie bieten mehrere der innovativsten und neuesten Funktionen, die wir uns im jeweiligen Marktsegment erhoffen.
- Overall Leader: Overall Leader werden anhand einer kombinierten Bewertung ermittelt. Dabei werden die Stärke der Produkte, die Marktpräsenz sowie die Innovationskraft der Anbieter berücksichtigt. Overall Leader weisen möglicherweise geringfügige Schwächen in manchen Bereichen auf, aber sie sind dennoch Overall Leader, weil sie in allen Bereichen überdurchschnittlich sind.

In jeder Leadership-Kategorie bewerten wir Produkte in drei Segmenten:

- Leader: Zu dieser Kategorie zählen die führenden Produkte, wie oben beschrieben. Leader sind Produkte, die in bestimmten Bereichen außergewöhnlich stark sind.
- Challenger: Zu dieser Kategorie zählen Produkte, die noch nicht Leader sind, die aber bestimmte Stärken aufweisen, die sie zu einem Leader machen könnten. Typischerweise sind diese Produkte ebenfalls ausgereift und möglicherweise bahnbrechend in Bezug auf bestimmte Anwendungsfälle und Kundenanforderungen.

- Follower: Diese Kategorie umfasst Produkte, die in manchen Bereichen Schwächen aufweisen, wie beispielsweise eine eingeschränkte Funktionalität oder lediglich eine regionale Präsenz. Die besten dieser Produkte weisen möglicherweise bestimmte Stärken auf, aufgrund derer sie eine gute oder vielleicht sogar die beste Wahl für bestimmte Anwendungsfälle und Kundenanforderungen sind, während sie unter anderen Bedingungen nur eingeschränkt nützlich sind.

Unsere Bewertung basiert auf einem breitgefächerten Input sowie auf unserer Erfahrung im jeweiligen Marktsegment. Der Input besteht aus Erfahrungen aus KuppingerCole Beratungsprojekten, dem Feedback von Kunden, die das Produkt einsetzen, technischen Foren, der Produktdokumentation sowie einem Fragebogen, der vor der Erstellung dieses KuppingerCole Leadership Compass versendet wurde, als primären Informationsquellen.

7.3 Produktbewertung

Als Analyst-Unternehmen evaluiert KuppingerCole regelmäßig Produkte/Services und Anbieter. Neben anderen Veröffentlichungen und Services werden die Ergebnisse in den KuppingerCole Leadership Compass Reports, den KuppingerCole Product Reports und den KuppingerCole Vendor Reports veröffentlicht. KuppingerCole verwendet eine standardisierte Bewertung, um einen schnellen Überblick über unsere Bewertung der Produkte oder Anbieter zu bieten. Die Erstellung eines schnellen Überblicks über die Produktbewertung von KuppingerCole erfordert eine Herangehensweise, die Klarheit, Genauigkeit und umfassende Informationen auf einen Blick kombiniert.

KuppingerCole zieht die folgenden Produkteigenschaften zur Bewertung heran:

- Sicherheit
- Funktionalität
- Integration
- Kompatibilität
- Usability

Sicherheit – Die Sicherheit wird durch den Grad an Sicherheit innerhalb des Produkts bestimmt. Die Informationssicherheit ist ein Schlüsselelement und eine der Hauptanforderungen des KuppingerCole IT-Modells (Nr. 70129 Scenario Understanding IT Service and Security Management[1]). Folglich sind ein ausgereifter Sicherheitsansatz sowie ein gut definiertes, internes Sicherheitskonzept wichtige Faktoren für die Evaluation von Produkten. Defizite, wie z. B. ein fehlendes oder ein nur sehr grob definiertes internes Berechtigungskonzept, werden als Sicherheitsprobleme definiert. Bekannte Sicherheitslücken und Hacks gelten ebenfalls als Schwächen. Die Bewertung fußt auf dem Schweregrad dieser Schwächen sowie auf der Herangehensweise des Anbieters an diese Herausforderungen.

Funktionalität – Dieses Kriterium wird anhand der folgenden drei Faktoren bestimmt: Der erste Faktor umfasst die durch den Anbieter zugesicherten Funktionen. Der zweite Faktor ist der aktuelle Stand der Branche, während der dritte Faktor die Erwartungen umfasst, die KuppingerCole zwecks Erfüllung von Kundenanforderungen von der jeweiligen Branche hat. In ausgereiften Marktsegmenten sind der Stand der Branche und die Erwartungen von KuppingerCole quasi deckungsgleich. In Wachstumsmärkten können signifikante Abweichungen auftreten, so dass kein einziger Anbieter die Erwartungen von KuppingerCole erfüllt.

[1] http://www.kuppingercole.com/report/mksecnario_understandingiam06102011

Dies würde zu einer relativ niedrigen Bewertung für alle Produkte in diesem Marktsegment führen. Wenn die durchschnittlichen Erwartungen von Kunden an die Anbieter in einem Marktsegment nicht erfüllt werden, führt dies normalerweise zu einer schlechteren Bewertung, sofern ein Produkt nicht über andere Funktionen oder Ansätze verfügt, die von Vorteil für Kunden sind.

Integration— Der Aspekt der Integration wird anhand des Grads gemessen, in dem ein Anbieter verschiedene Technologien oder Produkte in sein Portfolio integriert hat. Wenn wir also den Begriff Integration verwenden, beziehen wir uns auf den Grad, in dem Produkte miteinander agieren. Dieser Aspekt kann untersucht werden, indem man betrachtet, welche Schritte ein Administrator bei der Implementierung, im Betrieb, bei der Verwaltung oder bei der Außerbetriebnahme des Produkts ergreifen muss. Das Maß an Integration wird anschließend in einen direkten Zusammenhang mit diesem Aufwand gebracht. Zum Beispiel: Wenn jedes Produkt einen eigenen Datensatz aus Namen und Passwörtern für jeden Benutzer verwaltet, dann sind die Produkte nicht gut integriert. Auch wenn Produkte mehrere Datenbanken oder unterschiedliche Verwaltungstools mit inkonsistenten Benutzerschnittstellen verwenden, dann sind diese Produkte ebenfalls nicht gut integriert. Wenn ein Administrator jedoch mit einem einzigen Benutzernamen und -passwort alle Aspekte der Produkt-Suite verwalten kann, dann wurde ein höherer Grad der Integration erreicht.

Kompatibilität — Der Begriff „Kompatibilität" hat mehrere Bedeutungen. Wir verwenden den Begriff der „Kompatibilität" im Hinblick auf die Fähigkeit eines Produkts zur Zusammenarbeit mit den Produkten, Standards oder Technologien anderer Anbieter. In diesem Kontext handelt es sich um den Grad, in dem der Anbieter seine Produkte oder Technologien als kompatibel mit anderen Produkten oder Standards konzipiert, die außerhalb der Produktfamilie eine wichtige Rolle spielen. Hierzu zählt auch die Erweiterbarkeit, die anhand des Grads gemessen wird, in dem ein Anbieter die Erweiterung seiner Technologien und Produkte für die Zwecke seiner Kunden ermöglicht. Für uns ist die Erweiterbarkeit so bedeutend, dass wir ihr den gleichen Stellenwert wie der Kompatibilität verleihen, um ihre hohe Bedeutung zu unterstreichen und um sicherzustellen, dass sowohl Anbieter als auch Kunden diesen Aspekt verstehen. Für die weitere Entwicklung ist eine gute Dokumentation nicht mehr ausreichend. Wir bewegen uns auf eine Ära zu, in der eine akzeptable Erweiterbarkeit den programmatischen Zugang über gut dokumentierte uns sichere APIs erfordern wird. Weitere Informationen zur Natur und zum aktuellen Stand der Erweiterbarkeit und Kompatibilität finden Sie im Dokument zu Open API Economy (Nr. 70352 Advisory Note: The Open API Economy[2]).

Usability — Das Kriterium der Benutzerfreundlichkeit bezieht sich auf den Grad, in dem ein Anbieter verschiedenen Nutzergruppen den Zugang zu seinen Technologien und Produkten ermöglicht. Hierbei spielen üblicherweise zwei Aspekte der Usability eine Rolle: die Perspektive des Endnutzers sowie die Sicht des Administrators. Manchmal reicht eine gute Dokumentation aus, um für eine angemessene Usability zu sorgen. Allerdings haben wir hohe Erwartungen im Hinblick auf gut integrierte Benutzerschnittstellen sowie die Konsistenz bezüglich verschiedener Benutzeroberflächen eines Produkts oder bei verschiedenen Produkten desselben Anbieters. Zudem erwarten wir, dass Anbieter verbreiteten, etablierten Ansätzen im Hinblick auf Benutzeroberflächendesigns folgen.

[2] http://www.kuppingercole.com/report/cb_apieconomy16122011

Wir konzentrieren uns auf die Sicherheit, die Integration, die Kompatibilität und die Usability aus den folgenden wichtigen Gründen:

- Gesteigerte menschliche Teilnahme — Menschliche Eingriffe auf verschiedenen Ebenen eines Systems stellen das höchstmögliche Risiko sowohl in Bezug auf die Kosten als auch im Hinblick auf mögliche Ausfälle für alle Arten von IT-Systemen dar.
- Mangelnde Sicherheit, Funktionalität, Integration, Kompatibilität und Usability — Defizite in diesen Bereichen führen unmittelbar zu mehr menschlichen Eingriffen bei der Implementierung und Wartung von IT-Systemen.
- Erhöhtes Ausfallrisiko bezüglich Identität und Sicherheit — Vermehrte menschliche Systemeingriffe und Defizite bezüglich der Sicherheit, Funktionalität, Integration, Kompatibilität und Usability führen nicht nur zu signifikant höheren Kosten, sondern unweigerlich auch zu mehr Fehlern und Ausfällen. Dies eröffnet Gelegenheiten für Angriffe und Ausfälle.

Bei von KuppingerCole durchgeführten Technologie- und Produktbewertungen spielt das vom Anbieter bereitgestellte Maß an Sicherheit, Funktionalität, Integration, Kompatibilität und Usability eine besonders wichtige Rolle, da Defizite in manchen oder allen diesen Bereichen unweigerlich zu Mängeln bezüglich Identität und Sicherheit führen.

7.4 Anbieterbewertung

Bei der Evaluierung von Anbietern werden verschiedene Bewertungen herangezogen. Wir bewerten Anbieter in Bezug auf die folgenden Aspekte:

- Innovationskraft
- Marktposition
- Finanzstärke
- Netzwerk

Innovationskraft – Dieser Aspekt wird anhand der Fähigkeit gemessen, Innovationen in eine bestimmte Richtung voranzutreiben, die mit KuppingerColes Verständnis des jeweiligen Marktsegments übereinstimmt. Die Innovationskraft an sich bietet keinen Mehrwert, sondern sie muss deutliche Vorteile für den Kunden bedeuten. Allerdings ist die Innovationskraft ein wichtiger Faktor für das Vertrauen in einen Anbieter, denn innovative Anbieter bleiben mit größerer Wahrscheinlichkeit bahnbrechend. Ein wichtiges Element dieses Aspekts der Bewertung durch KuppingerCole ist die Unterstützung von Standardisierungsinitiativen, sofern vorhanden. Innovationen ohne Standardisierung führen häufig zu Lock-In-Szenarien. Deshalb trägt die aktive Teilnahme an Standardisierungsinitiativen zu einer positiven Bewertung der Innovationsstärke bei.

Marktposition – Die Marktposition wird anhand der Position des Anbieters im Markt oder in den relevanten Marktsegmenten gemessen. Hierbei handelt es sich um eine Durchschnittsbewertung in Bezug auf alle Märkte, in denen ein Anbieter aktiv ist, d.h., dass eine schwache Position in einem Marktsegment nicht zu einer sehr niedrigen Gesamtbewertung führt. Dieser Faktor berücksichtigt die Präsenz des Anbieters in wichtigen Märkten.

Finanzstärke — Während die Unternehmensgröße an sich für KuppingerCole nicht relevant ist, stellt die Finanzstärke dennoch einen wichtigen Faktor für Kunden im Rahmen der Entscheidungsfindung dar. Im Allgemeinen spielen öffentlich zugängliche Finanzinformationen in dieser Bewertung eine bedeutende Rolle. Fremdfinanzierte Unternehmen erhalten eine schlechtere Bewertung, da sie mit größerer Wahrscheinlichkeit das Ziel von Übernahmen sein können, was ein potenzielles Risiko für Kunden bedeutet, die sich für Produkte dieser Unternehmen entscheiden.

Ökosystem — Dieser Aspekt bezieht sich auf das Partnernetzwerk eines Anbieters. Dabei geht es hauptsächlich um den Partnerstamm eines Anbieters und seine Vorgehensweise als verantwortungsvoller Akteur in heterogenen IT-Umgebungen.

Bitte beachten Sie jedoch auch in diesem Zusammenhang, dass die meisten Bewertungen in einem KuppingerCole Leadership Compass sich auf die spezifischen Produkte sowie das Marktsegment beziehen, die im Rahmen dieser Analyse betrachtet werden. Sie stellen keine Gesamtbewertung des jeweiligen Anbieters dar.

7.5 Bewertungsskala für Produkte und Anbieter

Im Hinblick auf Anbieter und Produktfunktionsbereiche verwenden wir — über die Leadership-Bewertung in verschiedenen Kategorien hinaus — separate, fünfstufige Bewertungen. Diese Stufen lauten:

Sehr positiv	Herausragende Unterstützung für den jeweiligen Bereich, wie z. B. Produktfunktionen, oder eine herausragende Position des Unternehmens, beispielsweise im Hinblick auf seine finanzielle Stabilität.
Positiv	Starke Unterstützung für den jeweiligen Bereich oder eine starke Position des Unternehmens, aber mit einigen geringfügigen Lücken oder Schwächen. In Bezug auf Sicherheit kann diese Bewertung zum Beispiel auf einige Lücken in der feinkörnigen Kontrolle administrativer Berechtigungen hinweisen, während sie im Hinblick auf die Marktreichweite bedeuten kann, dass zwar ein Partnernetzwerk mit globaler Reichweite existiert, dieses aber eine geringe Zahl von Partnern umfasst.
Neutral	Akzeptable Unterstützung für den jeweiligen Bereich oder eine akzeptable Position eines Unternehmens, aber mit mehreren nicht erfüllten Anforderungen. Hinsichtlich der Funktionalität kann diese Bewertung beispielsweise bedeuten, dass einige der wichtigen, von uns festgelegten Anforderungen nicht erfüllt werden, andere jedoch wohl. Bezüglich Unternehmensbewertungen kann dies unter anderem auf eine lediglich regionale Präsenz hindeuten.
Schwach	Unterdurchschnittliche Fähigkeiten in Bezug auf die Produktbewertung oder signifikante Herausforderungen im Hinblick auf die Unternehmensbewertung, wie z. B. ein sehr kleines Partnerökosystem.
Sehr schwach	Große Schwächen in verschiedenen Bereichen. Diese Bewertung bezieht sich üblicherweise auf die Unternehmensbewertung bezüglich Marktposition oder Finanzstärke und weist darauf hin, dass der jeweilige Anbieter sehr klein ist oder nur über sehr wenige Kunden verfügt.

7.6 Netzdiagramme

Zusätzlich zu den Bewertungen in unseren Standardkategorien, wie Product Leadership und Innovation Leadership, stellen wir auch Netzdiagramme für alle bewerteten Anbieter bereit. Dabei betrachten wir spezifische Fähigkeiten für das im jeweiligen Leadership Compass untersuchte Marktsegment. Bezüglich des LC zu Privileged Access Management betrachten wir die folgenden acht Bereiche:

Shared Account Password Management (SAPM)	Funktionen für die Verwaltung der Passwörter gemeinsam verwendeter Konten, Passwortrotation, Single Sign-on für privilegierte Konten sowie zugehörige Funktionen.
Privileged Session Management (PSM)	Funktionen zur Erstellung von privilegierten Sessions auf Zielsystemen, einschließlich grundlegendem Auditing und Monitoring von privilegierten Aktivitäten, mit Authentifizierung, Autorisierung und Single Sign-On (SSO) auf Zielsystemen.
Application to Application Privilege Management (AAPM)	Funktionen zur Verwaltung von Konten, die von Anwendungen oder Systemen zur Kommunikation mit anderen Anwendungen oder Systemen verwendet werden (wie z. B. Datenbanken usw.), mit Identifizierung und Eliminierung von fest programmierten Anmeldeinformationen im Anwendungscode, in Scripts sowie in anderen Konfigurationsdateien mithilfe eines Austauschmechanismus (üblicherweise APIs), um Anmeldeinformationen auf sichere Weise bereitzustellen.
Session Recording & Monitoring (SRM)	Fortgeschrittenes Auditing, Monitoring und Evaluation von privilegierten Aktivitäten während einer privilegierten Session, einschließlich — neben weiteren Funktionen — Keystroke-Logging, Aufzeichnung von Video-Sessions, Screen Scraping, OCR-Konvertierung sowie weiteren Technologien zur Überwachung von Sessions.
Privileged User Behavior Analytics (PUBA)	Data-Analytics-Verfahren zur Erkennung von Bedrohungen anhand von anormalem Verhalten im Vergleich zu etablierten Verhaltensprofilen von Administrationsbenutzern sowie Benutzergruppen und Administratorrollen.

Privilege Account Discovery & Lifecycle Management (PADLM)	Erkennung von gemeinsam verwendeten Konten, Software-Konten, Servicekonten und anderen unverschlüsselten/als Klartext abgelegten Anmeldeinformationen in der gesamten IT-Infrastruktur, mit Integration in ITAM- oder CMDB-Tools zur Nachverfolgung des Kontoeigentümers etc.
Endpoint Privilege Management (EPM)	Verwaltung von privilegierten Konten auf Endpunkten, einschließlich der Identifizierung solcher Konten, Anwendungs-Whitelisting, einer kontrollierten Ausführungsumgebung sowie anderer Funktionen zur Verwaltung lokaler Administrationsrechte auf Desktops sowie mobilen Endpunkten
Privileged Access Governance (PAG)	Privilegierte Zugriffszertifizierungen und individualisierbares Reporting sowie Dashboarding

Die Netzdiagramme bieten zusätzliche Informationen, indem sie aufzeigen, in welchen Bereichen ein Produkt Stärken oder Schwächen aufweist. Einige Produkte weisen Lücken in bestimmten Bereichen und Stärken in anderen Bereichen auf. Diese könnten eine gute Wahl sein, wenn nur bestimmte Funktionen erforderlich sind. Andere Lösungen bietet starke Funktionen in allen Bereichen und sind deshalb im Allgemeinen besser geeignet für strategische Entscheidungen im Hinblick auf Privileged Access Management.

7.7 Einbeziehung und Ausschluss von Anbietern

KuppingerCole bemüht sich, alle Anbieter innerhalb eines bestimmten Marktsegments in seine Leadership Compass-Dokumente einzubeziehen. Das Dokument hat eine globale Reichweite und deckt auch Anbieter ab, die nur in regionalen Märkten, wie z. B. Deutschland, Russland oder die USA, vertreten sind.

Allerdings gibt es möglicherweise eine Reihe von Anbietern, die aus verschiedenen Gründen in diesem Leadership Compass nicht erwähnt werden.

- Eingeschränkte Marktsichtbarkeit: Möglicherweise gibt es Anbieter und Produkte, die uns trotz unserer stetigen Marktstudien und unserer Zusammenarbeit mit Beratungskunden noch unbekannt sind. Dies ist üblicherweise ein klares Anzeichen dafür, dass es sich nicht um einen Market Leader handelt.
- Verweigerung der Teilnahme: Manche Anbieter entscheiden sich möglicherweise dafür, nicht an unserer Evaluation teilzunehmen und möchten nicht Teil dieses Compass sein. KuppingerCole berücksichtigt die Produkte dieser Anbieter üblicherweise dennoch, sofern ausreichende Informationen für die Bewertung zur Verfügung stehen, um auf diese Weise einen umfassenden Überblick über die führenden Anbieter im jeweiligen Marktsegment zu bieten.

- Unzureichende Informationsbereitstellung: Produkte von Anbietern, die nicht die von uns für den Leadership Compass angeforderten Informationen bereitgestellt haben, finden in diesem Dokument keine Erwähnung, es sei denn, es stehen Informationen aus anderer Quelle zur Verfügung.
- Grenzfälle: Einige Produkte weisen möglicherweise nur eine geringfügige Überscheidung mit dem von uns analysierten Marktsegment auf. In diesen Fällen beschließen wir unter Umständen, das Produkt nicht in den KuppingerCole Leadership Compass aufzunehmen.

Das Ziel besteht darin, einen umfassenden Überblick über die Produkte in einem bestimmten Marktsegment zu bieten. KuppingerCole stellt regelmäßige Updates seiner Leadership Compass-Dokumente bereit.

Einen kurzen Überblick über nicht in diesem Dokument aufgeführte Anbieter und ihre Privileged Access Management-Produkte finden Sie in Kapitel 6 „Vielversprechende Anbieter und Marktsegmente". In diesem Kapitel stellen wir auch einige andere interessante Angebote rund um Privileged Access Management sowie in anderen verwandten Marktsegmenten vor.

8 Copyright

© 2019 KuppingerCole Analysts AG alle Rechte vorbehalten. Jegliche Vervielfältigung und Verbreitung dieser Publikation ohne vorherige schriftliche Erlaubnis ist untersagt. Alle Schlussfolgerungen, Empfehlungen und Vorhersagen in diesem Dokument stellen die anfängliche Sicht von KuppingerCole dar. Durch die Einholung weiterer Informationen und tiefgreifende Analysen bedingte geringfügige oder beträchtliche Änderungen an diesen Positionen sind vorbehalten. KuppingerCole lehnt jegliche Garantieansprüche in Bezug auf die Vollständigkeit, Genauigkeit und/oder Adäquatheit dieser Informationen ab. Obwohl KuppingerCole-Dokumentationen unter Umständen legale Belange in Verbindung mit Informationssicherheit und Technologien behandeln, ist KuppingerCole kein Anbieter von Rechtsdienstleistungen oder Rechtsberatung und die Veröffentlichungen des Unternehmens sollten nicht als solche herangezogen werden. KuppingerCole schließt jegliche Haftung für Fehler oder Unzulänglichkeiten der in diesem Dokument enthaltenen Informationen aus. Jede ausgedrückte Meinung kann zu jeder Zeit Änderungen unterliegen. Alle Produkt- und Firmennamen sind unregistrierte™ oder registrierte® Warenmarken der jeweiligen Eigentümer. Ihre Verwendung impliziert keinerlei Zugehörigkeit oder Unterstützung der jeweiligen Firma.

The Future of Information Security – Today

KuppingerCole Analysts unterstützt IT-Fachleute mit herausragendem Fachwissen bei der Ausarbeitung von IT-Strategien und damit verbundenen Entscheidungsprozessen. Als führende Analysefirma bietet KuppingerCole Analysts anbieterneutrale Informationen aus erster Hand. Mit unseren Dienstleistungen haben Sie einen sicheren und zuverlässigen Partner an Ihrer Seite, um essentielle Entscheidungen für Ihr Unternehmen zu treffen.

KuppingerCole Analysts ist seit seiner Gründung im Jahr 2004 eine in Europa ansässige Analysefirma mit Fokus auf Informationssicherheit und Identity- and Access Management (IAM). KuppingerCole Analysts steht für Fachwissen, Vordenken, herausragende praktische Relevanz und eine anbieterneutrale Sicht auf die Marksegmente der Informationssicherheit. Alle wichtigen Aspekte werden abgedeckt: Identity and Access Management (IAM), Unternehmensverfassung und Abschlussprüfung, Sicherheit in der Cloud und in virtuellen Umgebungen, Informationsschutz, Mobilfunk- und Softwaresicherheit, System- und Netzwerksicherheit, Sicherheitskontrolle, Analyse und Berichterstattung, Unternehmensführung, Organisation und Richtlinien.

Für weitere Informationen kontaktieren Sie bitte **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstrasse 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com