CYBERARK®

WHITEPAPER

VERBESSERUNG DER SAP-SICHERHEIT MIT DER PRIVILEGED ACCESS SECURITY LÖSUNG VON CYBERARK

Inhaltsverzeichnis

Zusammenfassung

Privilegierter Zugriff stellt die größte Sicherheitslücke dar, mit der sich SAP-Kunden heutzutage konfrontiert sehen. Privilegierte Accounts (Admin, Root etc.) gibt es in jeder Schicht einer SAP-Implementierung: vom zugrundeliegenden Betriebssystem bis zu den Unternehmensanwendungen, mit denen das Geschäft läuft. In den falschen Händen können sie dazu verwendet werden, den Betrieb zu stören, sensible Daten zu stehlen und die Geschäftsergebnisse zu beeinträchtigen.

Die SAP-Software unterstützt umfassende Authentifizierungs- und Autorisierungskontrollen, um nicht berechtigten Benutzern den Zugriff auf privilegierte Accounts zu verwehren. Viele Unternehmen verlassen sich jedoch auf ineffiziente und unwirksame manuelle Prozesse, um Anmeldedaten für privilegierte SAP-Accounts zu vergeben, aktualisieren oder widerrufen. Unzufriedene Mitarbeiter und Cyber-Kriminelle können inaktive Accounts ausnutzen und Passwörter stehlen, um Angriffe einzuleiten und sich vertrauliche Informationen anzueignen.

Die Privileged Access Security Lösung von CyberArk unterstützt SAP-Kunden dabei, Sicherheitsrisiken im Zusammenhang mit privilegiertem Zugriff zu mindern und ihre SAP-Investitionen zu schützen und auszuweiten. Die CyberArk-Lösung ergänzt die nativen Sicherheitsfunktionen und -lösungen von SAP und hilft Unternehmen dabei, Anmeldedaten für privilegierte Accounts sicher zu verwalten, die Aktivitäten mit privilegierten Accounts proaktiv zu überwachen und zu kontrollieren und Bedrohungen umgehend zu erkennen und zu verhindern.

Die CyberArk-Lösung unterstützt traditionelle SAP-ERP-Systeme sowie eine Vielzahl von SAP-Produkten und -Technologien wie SAP CRM, SRM, SCM, SAP NetWeaver, SAP HANA und Sybase ASE. Außerdem ist CyberArk ein offizielles Mitglied des SAP Partner Edge-Programms und bietet eine vollständig zertifizierte Integration in SAP NetWeaver an.

In diesem Whitepaper werden die Sicherheitsrisiken und -herausforderungen im Zusammenhang mit privilegierten SAP-Accounts untersucht und es wird erklärt, wie die Privileged Access Security Lösung von CyberArk SAP-Kunden dabei helfen kann, ihre Sicherheitsposition zu verbessern und geschäftskritische Anwendungen und Daten zu schützen.

Einführung

Unternehmen auf der ganzen Welt vertrauen auf SAP-Softwarelösungen, um die Zusammenarbeit zu verbessern, Geschäftseinblicke zu erhalten und der Konkurrenz immer einen Schritt voraus zu sein. Mehr als 388.000 Kunden im privaten und öffentlichen Sektor, darunter mehr als 91 Prozent Forbes-2000-Firmen, nutzen SAP-Software. Da die SAP-Lösungen für die Verwaltung von betriebsinternen Daten und die Ausführung geschäftskritischer Prozesse verwendet werden, sind sie ein beliebtes Ziel für Cyber-Angriffe. Hacker können versuchen, sich Zugriff auf SAP-Implementierungen zu verschaffen oder diese zu manipulieren, um proprietäre Informationen zu stehlen oder den Betrieb zu stören. Sicherheitsverletzungen können negative Auswirkungen auf die Produktivität und den Ruf eines Unternehmens haben und zu Datenlecks, Umsatzverlusten und rechtlichen Konsequenzen führen. Tatsächlich werden die Kosten für eine SAP-Sicherheitsverletzung auf durchschnittlich 5 Millionen USD geschätzt. Sicherheitsexperten gehen davon aus, dass die Angriffe auf SAP-Systeme in Zukunft noch häufiger und komplexer sein werden.

SAP-Softwarelösungen unterstützen administrativ definierte Rollen und Berechtigungen und beinhalten umfassende Zugriffskontrollen, um unbefugten Benutzern den Zugriff auf Systemressourcen und Geschäftsdaten zu verwehren. Viele SAP-Kunden vertrauen jedoch auf manuell aufwendige, fehleranfällige Administrationsprozesse, um die Sicherheit von Anmeldeinformationen zu verwalten. Passwörter und Zugriffschlüssel bleiben oft monate- oder sogar jahrelang unverändert, nachdem sie ausgegeben wurden. Ehemalige Mitarbeiter, Dienstleister und Geschäftspartner behalten oftmals noch lange nach dem Ende der Zusammenarbeit Zugriff auf kritische SAP-Anwendungen und -Systeme. So wird das Unternehmen dem Risiko von Sicherheitsverletzungen, schädlichen Angriffen und dem Diebstahl vertraulicher Daten ausgesetzt. Hacker können außerdem inaktive Accounts ausnutzen und Passwörter entwenden, um auf Systeme zuzugreifen, Schwachstellen aufzudecken und raffinierte Angriffe zu starten.

Schutz von privilegiertem Zugriff für SAP-Implementierungen

Privilegierte SAP-Accounts sind besonders anfällig für Cyber-Angriffe. Sie gewähren direkten Zugriff auf wichtige Unternehmenssysteme und sensible Daten. Externe Angreifer oder böswillige Insider können privilegierten Zugriff ausnutzen, um ein Unternehmen schachmatt zu setzen oder geistiges Eigentum sowie vertrauliche Kundeninformationen zu stehlen. Forrester schätzt, dass 80 Prozent der Sicherheitsverletzungen mit privilegierten Anmeldedaten in Zusammenhang stehen.

Privilegierte Accounts befinden sich in allen Schichten des SAP-Bestands (Anwendungsserver, Middleware und Datenbanken, Unternehmensanwendungen). SAP NetWeaver allein unterstützt vier verschiedene Arten von privilegierten Accounts:

- Benutzeradministrator
- Autorisierter Datenadministrator

- Autorisierter Profiladministrator
- Spezielle Benutzer (SAP*, DDIC, SAPCPIC, TMSADM und EARLYWATCH)

Privilegierte Accounts existieren auch in den zugrundeliegenden On-Premises- oder cloud-basierten Plattformen, die die SAP-Lösungen ausführen. Diese Accounts (Admin, Root, SYS usw.) gewähren autorisierten Benutzern uneingeschränkten administrativen Zugriff auf physische und virtuelle Server, Speichergeräte, Netzwerkgeräte und andere IT-Hardware und Softwareplattformen. Sie sind ebenfalls ein häufiges Ziel für Angreifer.

CyberArk Privileged Access Security Lösungen für SAP

CyberArk ist der globale Marktführer im Bereich der Sicherheit von privilegiertem Zugriff. Mehr als die Hälfte der Fortune-100-Firmen vertrauen beim Schutz ihrer kritischen IT-Ressourcen und Infrastruktur auf CyberArk. Die CyberArk Privileged Access Security Lösung wurde von Anfang an dazu entwickelt, zuverlässige Kontrolle über den privilegierten Zugriff für On-Premises-, Cloud- und Hybrid-Umgebungen, einschließlich SAP-Implementierungen, bereitzustellen. Die Lösungen schützt, verwaltet und prüft Anmeldeinformationen für privilegierte Accounts. Sie steuert Least-Privilege-Access und sichert, überwacht und analysiert die gesamte privilegierte Aktivität. Bei ungewöhnlichem Verhalten werden aktiv Warnmeldungen ausgegeben. Ein isolierter Vault-Server, eine einheitliche Policy Engine, eine umfassende Discovery Engine und mehrere Sicherheitsebenen bieten noch nie da gewesenen Schutz für privilegierte Accounts. Dabei sorgen sie gleichzeitig für hohe Skalierbarkeit und Zuverlässigkeit.

Die CyberArk Privileged Access Security Lösung unterstützt traditionelle SAP-ERP-Systeme sowie eine Vielzahl von SAP-Produkten und -Technologien wie SAP CRM, SRM, SCM, SAP NetWeaver, SAP HANA und Sybase ASE. Außerdem ist CyberArk ein offizielles Mitglied des SAP Partner Edge-Programms und bietet eine zertifizierte Integration in SAP NetWeaver an.

Die CyberArk Privileged Access Security Lösung ermöglicht IT-Unternehmen und Sicherheitsteams Folgendes:

- Zentrale Verwaltung des Zugriffs über privilegierte Benutzer-Accounts für On-Premises- und cloud-basierte Infrastruktur und Anwendungen.
- Proaktive Überwachung von Sicherheitsaktivitäten und Erkennung von Bedrohungen in On-Premises-, Cloud- und Hybrid-Umgebungen.
- Einfaches Widerrufen von Privilegien oder Aktualisieren der Sicherheitsanmeldedaten in Reaktion auf Bedrohungen oder Angriffe.

Vorteile einer einheitlichen Lösung für die Sicherheit von privilegiertem Zugriff

SAP-Implementierungen bestehen aus verschiedenen Softwarekomponenten und Anwendungen, die oftmals von unterschiedlichen Anbietern bereitgestellt werden, die wiederum andere Sicherheitsfunktionen und Toolsets unterstützen. Das führt dazu, dass viele Unternehmen auf eine Sammlung unterschiedlicher Authentifizierungs- und Autorisierungsmethoden für privilegierten Zugriff im gesamten Unternehmen vertrauen. Isolierte Sicherheitssysteme und -verfahren sind naturgemäß ineffizient und unwirksam und können die erhöhten Anforderungen an Agilität und Skalierbarkeit eines modernen Unternehmens nicht erfüllen. IT-Unternehmen und Sicherheitsteams haben keine vollständige Kontrolle und keinen umfassenden Einblick in die Implementierung; dadurch werden Risiko und Unsicherheit erhöht.

Die CyberArk Privileged Access Security Lösung hilft Unternehmen dabei, Risiken einzudämmen und Verfahren zu rationalisieren, indem Verwaltungssilos eliminiert, der Automatisierungsgrad erhöht und Sicherheitsfunktionen konsolidiert werden. Mit der CyberArk-Lösung haben Unternehmen folgende Möglichkeiten:

- Einführung einheitlicher Kontrollen für den privilegierten Zugriff in der gesamten SAP-Umgebung einschließlich Infrastruktur, Middleware, Datenbanken und Anwendungen.
- Implementierung eines ganzheitlichen Ansatzes für die Sicherheit des privilegierten Zugriffs, um blinde Flecken zu eliminieren, Schwachstellen zu reduzieren und die Sicherheitsposition zu stärken.
- Umfassender Einblick in die Aktivitäten privilegierter Benutzer zur Erkennung und Isolierung von raffinierten Angriffen in Echtzeit.
- Globales Widerrufen und Rotieren von privilegierten Anmeldedaten im gesamten Unternehmen, um Angriffe zu verhindern.
- Erstellung von unternehmensweiten Aktivitätsberichten zur Bewertung von Sicherheitslücken und Unterstützung von Compliance-Audits.
- Zentralisierung und Vereinfachung der Sicherheitsverwaltung, sodass wertvolle IT-Ressourcen entlastet werden und sich auf wichtige Geschäftsaufgaben konzentrieren können.

Die Lösung hilft Unternehmen bei der Risikominderung und beim Vereinfachen der Vorgänge, indem Verwaltungssilos eliminiert, der Automatisierungsgrad erhöht und konsistente Sicherheitsverfahren und -strategien in SAP-Infrastruktur, -Middleware, -Datenbanken und -Anwendungen implementiert werden.

Im Detail gewährt die CyberArk-Lösung SAP-Kunden die folgenden Möglichkeiten:

- Sichern von privilegierten Anmeldeinformationen, die in allen Schichten des SAP-Bestands genutzt werden, vom Betriebssystem, virtuellen Maschinen und Datenbanken bis zur Anwendung selbst. (Siehe Abbildung 1). CyberArk sichert grundlegende SAP-Komponenten und -Middleware, beliebte Datenbanken (SAP HANA, Sybase, Oracle, SQL Server, DB2 etc.) und Unternehmensanwendungen (ERP, CRM etc.).

- Verwalten der SAP-Anmeldeinformationen an einem einzigen zentralen Ort, wobei die Verwaltung vereinfacht und unbefugter Zugriff auf geschäftskritische Systeme und Anwendungen verhindert wird.
- Rotation und Aktualisierung von Anmeldeinformationen bei Bedarf oder in regelmäßigen Abständen auf Grundlage von Richtlinien.
- Isolation von Sessions privilegierter Benutzer und Durchsetzung starker Zugriffskontrollen, um geschäftskritische SAP-Systeme vor Gefahren durch Mensch und Maschine zu schützen.
- Erfassung und Überwachung der Aktivitäten in privilegierten Sessions für Mitarbeiter, Dienstleister und Geschäftspartner, was Sicherheitsteams sowohl beim Erkennen als auch beim Verhindern von nicht autorisiertem Zugriff auf privilegierte SAP-Accounts unterstützt.
- Verwaltung der Anmeldeinformationen für den Katalog sensibler Daten (DDIC) und den Software Update Manager, die im SAP-Upgradeprozess verwendet werden.

Die CyberArk Privileged Access Security Lösung ergänzt die nativen Sicherheitsfunktionen und -lösungen von SAP, einschließlich SAP Enterprise Threat Detection und SAP Governance Risk and Compliance (GRC). Die CyberArk-Lösung unterstützt Unternehmen beim Ausbau ihrer Sicherheitspositionen und der Erweiterung vorheriger Investitionen. Die gesamte Kommunikation zwischen den CyberArk- und SAP-Lösungskomponenten wird authentifiziert und verschlüsselt (mit SNC bei der Kommunikation mit SAP), um Abhörangriffe und den Diebstahl von Anmeldedaten zu verhindern.

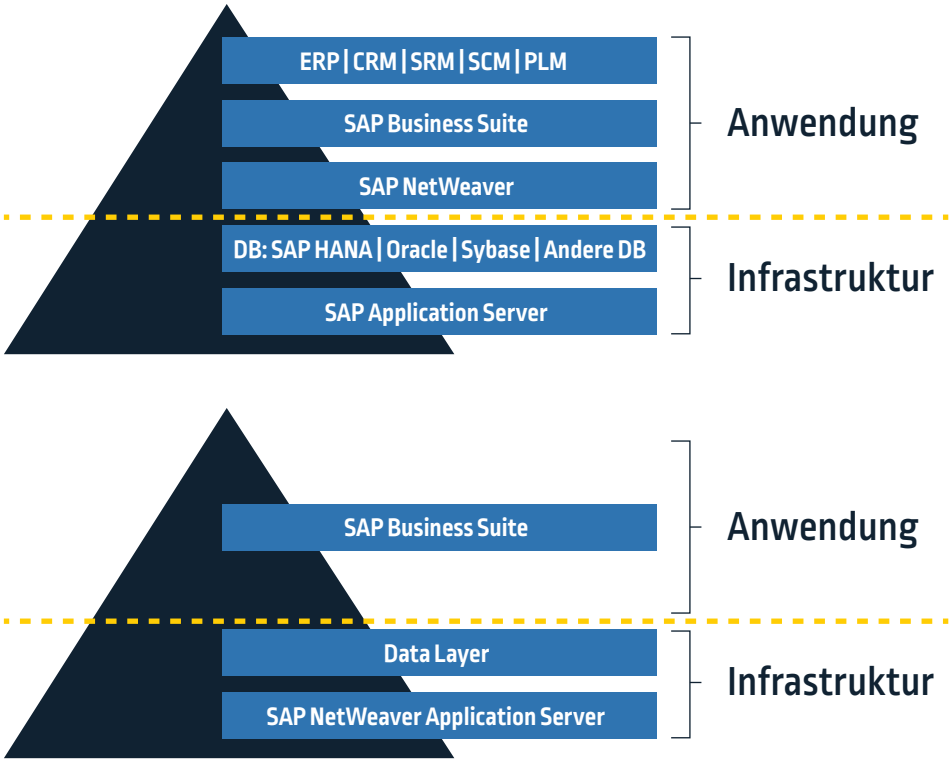

Abbildung 1 – Privilegierte Accounts sind in jeder Schicht der SAP-Implementierung vorhanden

CyberArk Privileged Access Security Lösung – SAP-Anwendungsfälle

Die CyberArk Privileged Access Security Lösung unterstützt eine Vielzahl von Anwendungsfällen. Sie sichert den privilegierten Zugriff im gesamten Technologiebestand von den zugrundeliegenden Plattformen bis zu den Business Applications und lässt sich in SAP-Lösungen und Drittanbieterprodukte integrieren. Sie stellt zuverlässige Passwortkontrollen für alle privilegierten Accounts bereit, speichert Anmeldeinformationen in einem sicheren Digital Vault, lässt Passwörter automatisch basierend auf Richtlinien rotieren und isoliert, erfasst und überwacht privilegierte Sessions. Die CyberArk-Lösung kann für die Verwaltung des privilegierten Zugriffs für autorisierte Mitarbeiter, Dienstleister und Dritte wie Geschäfts- und Supportpartner verwendet werden.

Schutz von SAP-Superuser-Accounts

Die CyberArk Privileged Access Security Lösung schützt die privilegierten Accounts (z. B. Admin, Root, SYS) der zugrundeliegenden Betriebssysteme und unterstützt somit die SAP-Implementierung. Sie ermöglicht privilegierten Benutzern, zugelassene Admin-Befehle ohne unnötige Root-Rechte direkt in einer Unix- oder Linux-Session auszuführen. Privilegierte Betriebssystem-Accounts gewähren direkten Zugriff auf geschäftskritische IT-Ressourcen und sind ein beliebtes Ziel für Angreifer.

Schutz von privilegierten Datenbank-Accounts

Die CyberArk Privileged Access Security Lösung schützt den privilegierten Zugriff auf SAP HANA und viele andere beliebte Datenbankplattformen wie Sybase, Oracle, SQL Server und DB2. Hacker versuchen oft, auf privilegierte Datenbank-Accounts zuzugreifen, um vertrauliche Geschäfts- und Kundendaten zu stehlen.

Schutz von privilegierten Accounts für Business Applications

Die CyberArk Privileged Access Security Lösung schützt den privilegierten Zugriff auf Unternehmensanwendungen (ERP, SCM, CRM etc.), die von SAP und anderen Softwareanbietern bereitgestellt werden. IT-Mitarbeiter und Geschäftsanwender nutzen diese Accounts, um Anwendungen zu verwalten, Geschäftsprozesse zu automatisieren und SAP-Systeme zu verbinden. Angreifer können versuchen, auf diese Accounts zuzugreifen, um den Betrieb zu stören oder Betrug zu begehen.

Schutz des Zugriffs über privilegierte Benutzer-Accounts durch Dritte

Die CyberArk Privileged Access Security Lösung schützt und kontrolliert privilegierten Zugriff durch Dritte wie Dienstleister und Geschäftspartner. Manche SAP-Kunden erhalten eventuell technischen Remotesupport von SAP oder anderen Unternehmen. Einige SAP-Kunden erweitern die Unternehmensanwendungen und Geschäftsprozesse möglicherweise auf Zweigniederlassungen, Tochterunternehmen oder Geschäftspartner. Diese Drittparteien brauchen eventuell Zugriff auf privilegierte Accounts im Zusammenhang mit Betriebssystemen, Middleware und Datenbankplattformen oder Business Anwendungen. Ein Cyber-Krimineller versucht vielleicht, als autorisierter Dritter aufzutreten, um Daten zu stehlen oder Systeme lahm zu legen.

Verbesserung der Regelkonformität

Die CyberArk Privileged Access Security Lösung hilft SAP-Kunden dabei, die Konformität mit Branchen- und Regierungsvorschriften wie Sarbanes Oxley (SOX), dem Payment Card Industry Data Security Standard (PCI DSS), der Datenschutz-Grundverordnung (DSGVO), ISO/IEC 27002, dem Health Insurance Portability and Accountability Act (HIPAA) und dem Society of Worldwide Interbank Financial Telecommunication (SWIFT) Customer Security Controls Framework zu verbessern. All diese verfügen über strenge Richtlinien für die Überwachung und Kontrolle des Zugriffs auf privilegierte Accounts.

Die manuelle Verwaltung von privilegierten SAP-Accounts ist von Natur aus kostenintensiv und riskant

Privilegierte Accounts sind allgegenwärtig. Sie existieren in jeder Hardware- und Softwarekomponente einer SAP-Implementierung. Sie dienen verschiedensten Zwecken und werden von einer Vielzahl an Abteilungen und Mitarbeitern genutzt, darunter IT-Personal, Sicherheitsteams und Geschäftsanwender.

Viele Unternehmen verwalten privilegierte Accounts immer noch manuell. Einzelne IT-Manager und SAP-Anwendungsadministratoren erstellen, aktualisieren und widerrufen Sicherheitsanmeldedaten manuell. Dabei notieren sie sich die Benutzer-IDs und Passwörter oftmals in Tabellen, auf Papier oder sogar Klebezetteln!

Diese uneinheitlichen Verwaltungsverfahren sind aufwendig und fehleranfällig und naturgemäß ineffizient und riskant. Allein die Menge an privilegierten Accounts kann überwältigend sein. Große Unternehmen können Hunderte von SAP-Instanzen auf Hunderten physischen und virtuellen Servern ausführen, die On-Premises und in der Cloud bereitgestellt werden. In jeder Schicht im SAP-Bestand können drei bis vier privilegierte Accounts existieren. In der gesamten SAP-Umgebung können daher Zehntausende privilegierte Accounts vorhanden sein.

Bei der manuellen Verwaltung von privilegierten Accounts werden Zeit und Ressourcen verschwendet und SAP-Administratoren und IT-Manager von ihren primären Geschäftsaufgaben abgehalten. Und es kommt noch schlimmer: Sie birgt unheimliche Sicherheitsrisiken. Die meisten Anwendungsadministratoren und IT-Mitarbeiter sind keine Sicherheitsexperten und kennen sich nicht mit den Best Practices für die Verwaltung privilegierter Accounts aus. Jede Abteilung verwendet möglicherweise einen eigenen Ansatz für den Schutz von privilegiertem Zugriff. So entstehen Sicherheitslücken, die sich raffinierte Angreifer zunutze machen können.

Zu allem Übel sind die Anmeldeinformationen für privilegierte Accounts im gesamten Unternehmen verteilt, wodurch eine breite Angriffsfläche für Hacker geschaffen wird. Unternehmenseigene Sicherheitsteams haben oftmals keinen umfassenden Einblick in die Aktivitäten privilegierter Accounts, sodass schädliche Angreifer unbemerkt in die SAP-Implementierungen gelangen und sich frei darin bewegen können, um Schwachstellen zu entdecken. Auch wenn die Eindringlinge entdeckt werden, haben die Sicherheitsteams keine Möglichkeit, Sicherheitsanmeldedaten global in der SAP-Implementierung zu widerrufen oder zu ändern. Ohne zentrale Sicherheitslösung für privilegierte Accounts kann es Tage dauern, bis ein ausgeklügelter Angriff isoliert und gestoppt wird.

Schutz von SAP-Upgrades

Die CyberArk Privileged Access Security Lösung kann zum Schutz von SAP-Systemen bei Software-Upgrades verwendet werden. Es ist privilegierter Zugriff nötig, um den SAP Software Update Manager auszuführen und während eines Software-Updates auf den SAP-DDIC-Account zuzugreifen. Die CyberArk-Lösung sorgt dafür, dass nur der Benutzer auf den SAP-Anwendungsserver und den DDIC-Account zugreifen kann, der entsprechend autorisiert wurde. Es kann ebenfalls eine Richtlinie formuliert werden, um sicherzustellen, dass Passwörter nur dann abgerufen werden können, wenn eine Bestätigung von einem autorisierten Manager oder einer Gruppe von Managern eingeholt wurde. Sobald das Upgrade abgeschlossen wurde, kann das DDIC-Account-Passwort automatisch geändert werden, damit der SAP-Administrator es nicht erneut verwenden kann. Der gesamte Prozess wird aufgezeichnet, überwacht und geprüft.

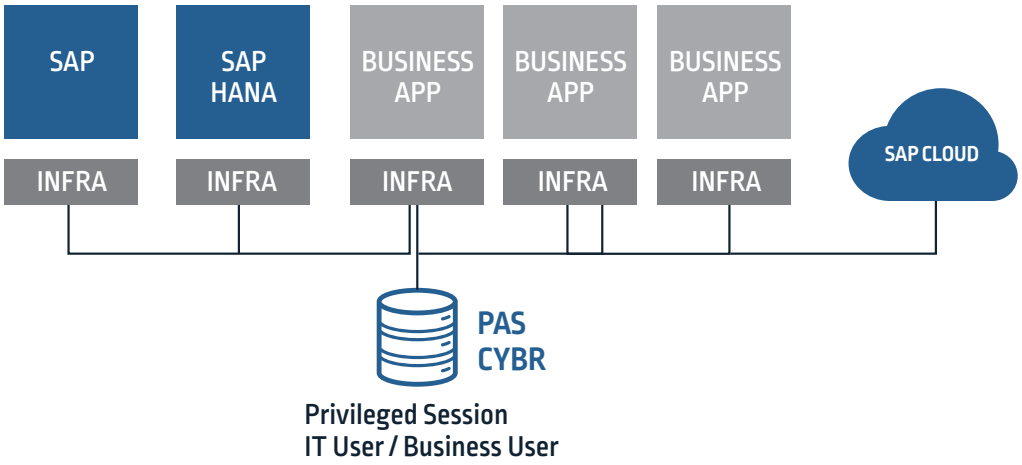

Abbildung 2

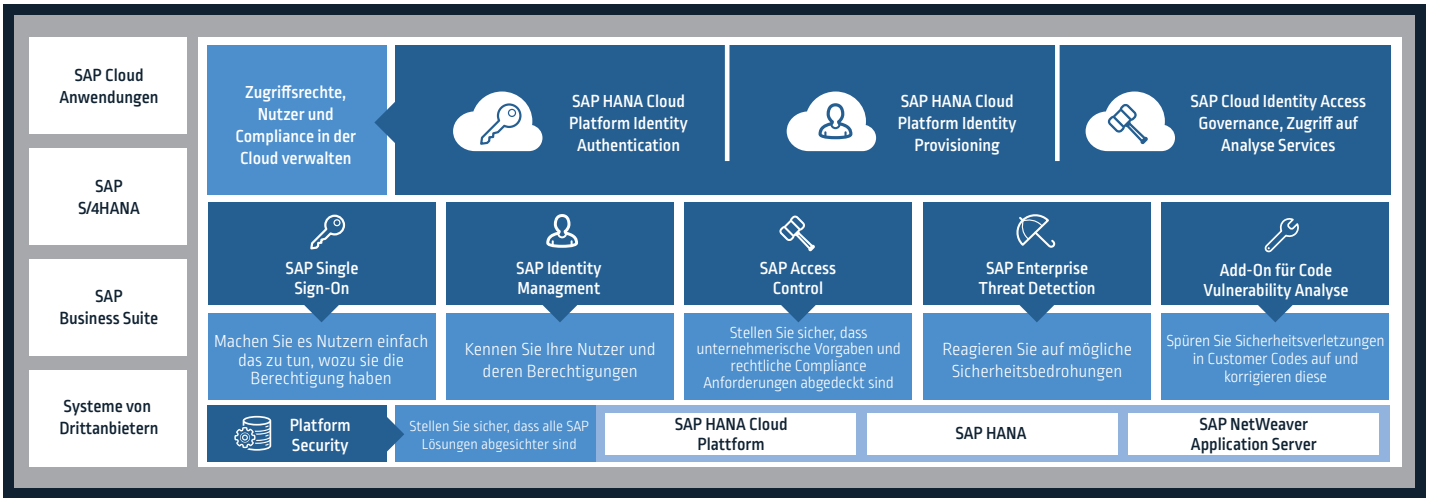

Abbildung 3

Fazit

Privilegierte Accounts gibt es in jeder Schicht einer SAP-Implementierung: von der zugrundeliegenden Infrastruktur bis zu den Unternehmensanwendungen, mit denen das Geschäft läuft. In den richtigen Händen sorgen sie für den Schutz von geschäftskritischen Ressourcen und Daten. In den falschen Händen können sie jedoch dazu verwendet werden, den Betrieb zu stören und vertrauliche Daten zu stehlen.

Viele Unternehmen vertrauen auf manuelle Prozesse zur Verwaltung privilegierter Accounts – ein riskantes und kostenintensives Unterfangen. Die CyberArk Privileged Access Security Lösung hilft SAP-Kunden bei der Stärkung ihrer Sicherheitsposition und der Rationalisierung von Verfahren, indem Verwaltungssilos eliminiert, der Automatisierungsgrad erhöht und konsistente Sicherheitsverfahren und -strategien in der gesamten SAP-Umgebung implementiert werden. Die CyberArk-Lösung ergänzt native SAP-Sicherheitsfunktionen und -Lösungen, lässt sich in eine Vielzahl von SAP-Produkte und -Technologien integrieren und unterstützt zahlreiche Anwendungsfälle. Die Lösung mindert Cyberrisiken, indem sie Unternehmen dabei hilft, Anmeldedaten für privilegierte Accounts sicher zu verwalten, die Aktivitäten privilegierter Accounts proaktiv zu überwachen und zu kontrollieren und Bedrohungen umgehend zu erkennen und zu verhindern.

Um mehr darüber zu erfahren, wie die CyberArk Privileged Access Security Lösung Ihnen beim Schutz Ihrer geschäftskritischen Anwendungen und Daten helfen kann, besuchen Sie www.cyberark.de.

Über CyberArk

CyberArk (NASDAQ: CYBR) ist der globale Marktführer für die Sicherheit von privilegiertem Zugriff und bietet eine kritische Schicht für IT-Sicherheit zum Schutz von Daten, Infrastruktur und Ressourcen im Unternehmen, in der Cloud und in der DevOps-Pipeline. CyberArk liefert die branchenweit kompletteste Lösung zur Minderung von Risiken im Zusammenhang mit privilegierten Anmeldeinformationen und vertraulichen Zugangsdaten. Weltweit führende Unternehmen, darunter mehr als 50 Prozent Fortune-100-Firmen, vertrauen auf CyberArk zum Schutz vor externen Angreifern und böswilligen Insidern. Als globales Unternehmen verfügt CyberArk über Firmensitze in Petach Tikva, Israel, sowie in Newton, Massachusetts, USA. Das Unternehmen besitzt außerdem Standorte in Amerika, EMEA, Asien-Pazifik und Japan.