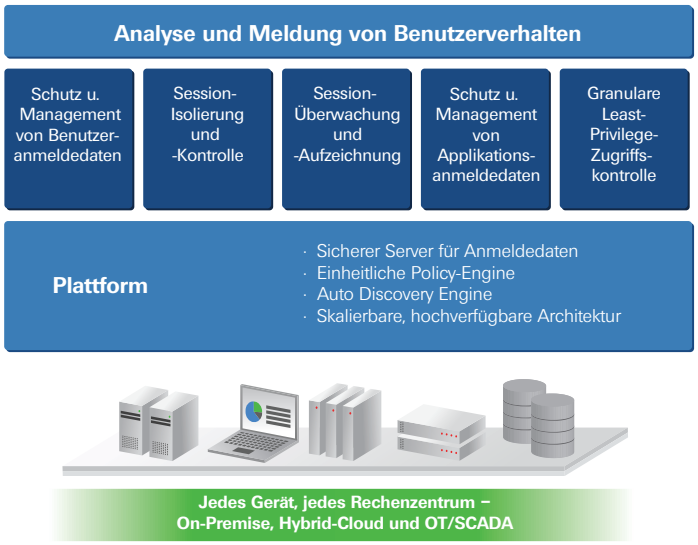
Privileged Account Security Lösung

Zunächst einmal empfiehlt es sich, privilegierte Benutzerkonten in das zentrale Sicherheitskonzept des Unternehmens zu integrieren. Sie sind ein potenzielles Sicherheitsproblem und erfordern spezielle Kontrollmechanismen zur Überwachung aller damit zusammenhängenden Aktivitäten

Die größte Sicherheitslücke, mit der sich Unternehmen heute konfrontiert sehen sind privilegierte Benutzerkonten, die bei nahezu jeder Cyber-Attacke missbraucht werden. Jeder Angreifer, der in ihren Besitz gelangt, kann die Ressourcen von Unternehmen kontrollieren, Sicherheitssysteme deaktivieren und auf riesige Mengen sensibler Daten zugreifen.

Um diese Konten und die geschäftskritischen Ressourcen zu schützen, zu denen sie Zugriff bieten, brauchen Unternehmen umfassende Kontrollen für die Sicherung, Überwachung, Erfassung und Reaktion auf alle Privileged-Account-Aktivitäten.

CyberArk ist Ihr zuverlässiger Experte für den Schutz privilegierter Benutzerkonten. Unsere Privileged Account Security Lösung wurde von Grund auf für ein Höchstmaß an Sicherheit für privilegierte Benutzerkonten in allen Umgebungen – ob On-Premise, in einer Hybrid Cloud oder in Industrial Control Systems beziehungsweise SCADA-Systemen konzipiert. Sie schützt und überwacht Systeme, erkennt, meldet und bekämpft Bedrohungen und bietet dabei ein hohes Maß an Manipulationssicherheit, Skalierbarkeit und Adaptiermöglichkeiten für komplexe verteilte Umgebungen. Damit kann ein maximaler Schutz vor Bedrohungen von innen und außen realisiert werden.



Warum CyberArk?

CyberArk bietet als einziger Hersteller einen vollständigen Schutz vor Insider-Angriffen und hochentwickelten Bedrohungen von außen und erfüllt gleichzeitig anspruchsvollste Compliance-Anforderungen. CyberArk ist führend bei Installationen in großen verteilten und virtuellen Umgebungen und der Beseitigung von Sicherheitsproblemen im Zusammenhang mit privilegierten Benutzerkonten.

CyberArk Shared Technology Platform:

Digital Vault™: Der prämierte, patentierte Digital Vault ist ein isolierter, gehärteter Server mit Verschlüsselung gemäß FIPS 140-2, der ausschließlich auf die Vault-Protokolle reagiert – dies bietet beispiellose Sicherheit.

Master Policy™: Master Policy ist eine innovative Policy-Engine mit einer einfachen, bedienerfreundlichen Benutzeroberfläche in natürlicher Sprache, mit dem Sicherheitsrichtlinien für privilegierte Benutzerkonten festgelegt, verwaltet und überwacht werden können.

Discovery Engine: Die Discovery Engine erkennt jede Veränderung der IT-Umgebung und bietet konstanten, stets aktuellen Schutz. So wird gewährleistet, dass alle Privileged-Account-Aktivitäten ausgewiesen und sicher sind.

Skalierbare, flexible, Low-Impact -Architektur: Die Cyberark Privileged Account Security Lösung wirkt sich minimal auf Ihre bestehende IT-Umgebung aus und schützt so Ihre Wertanlagen.

Integration der Enterprise-Klasse: Die Cyberark Privileged Account Security Lösung unterstützt zahlreiche Geräte, Netzwerke, Server und Applikationen einschließlich Websites und sozialer Medien, , und kann nahtlos in bestehende Systeme integriert werden.

Privileged Account Security Produkte

Jedes Produkt der CyberArk Pivileged Account Security Lösung kann eigenständig betrieben und unabhängig verwaltet werden, auch wenn es gleichzeitig Ressourcen und Daten aus der gemeinsamen Infrastruktur nutzt. In der Kombination bilden die Produkte eine komplette Sicherheitslösung.

Enterprise Password Vault™

Schutz, Management und Audit privilegierter Anmeldedaten

Der Enterprise Password Vault verhindert den Missbrauch privilegierter Passwörter und schützt vertrauliche Benutzerkonten. Er sichert privilegierte Zugangsdaten gemäß Ihren Sicherheitsrichtlinien für die Privileged Account Security und kontrolliert, wer wann auf welche Passwörter zugreifen kann. Automatische Passwort-Rotation erleichtert die zeitaufwändige und fehleranfällige Aufgabe der manuellen Verfolgung und Aktualisierung von privilegierten Zugangsdaten, sodass Audit- und Compliance-Anforderungen problemlos erfüllt werden.

SSH Key Manager™

Management, Rotation und Schutz privilegierter SSH-Keys

SSH Key Manager verhindert unbefugten Zugriff auf privilegierte Benutzerkonten, die mit SSH-Keys geschützt sind. SSH Key Manager bietet sichere Speicherung und Zugriffskontrolle für private SSH-Keys, verwaltet die Berechtigungsnachweise für systeminterne public SSH-Keys und ermöglicht eine effektive Berichterstattung darüber, wer wann welche Keys benutzt hat. Key-Paare werden gemäß der Sicherheits-Policy automatisch ausgetauscht, sodass Unternehmen ihre Sicherheit erhöhen, ohne die IT-Abteilung zusätzlich zu belasten.

Privileged Session Manager™

Überwachung, Kontrolle und Isolierung von privilegierten Sessions

Privileged Session Manager versetzt Sicherheitsteams in die Lage, Gefahren im Netzwerk schnell zu erkennen und entsprechend zu reagieren. Echtzeitüberwachung ermöglicht die sofortige Ermittlung verdächtiger Aktivitäten. Benutzersitzungen lassen sich per Fernzugriff beenden, sodass laufende Attacken schnell unterbunden werden können. Anhand durchsuchbarer DVR-ähnlicher Aufzeichnungen können Sicherheits- und Audit-Teams Vorfälle problemlos lokalisieren, ohne zahlreiche Protokolle durchsehen zu müssen. Durch die Überwachung, Kontrolle und Isolierung privilegierter Sessions erhöht das Produkt die Sicherheit, beschleunigt die Reaktionszeit auf Vorfälle und trägt dazu bei, Compliance-Anforderungen zu erfüllen.

Privileged Threat Analytics™

Analyse und Meldung von böswilligen Aktivitäten in privilegierten Benutzerkonten

Als branchenweit einzige zielgerichtete Analyselösung für Gefahren, die sich spezifisch gegen privilegierte Accounts richten, ermittelt CyberArk Privileged Threat Analytics bisher nicht aufspürbare böswillige Aktivitäten in diesen Benutzerkonten. Durch die Anwendung patentierter Analysealgorithmen auf einen umfangreichen Bestand von Verhaltensinformationen liefert die Lösung hochpräzise, direkt nutzbare Informationen, mit denen die Sicherheitsteams sofort gegen Angriffe vorgehen können

Application Identity Manager™

Schutz, Management und Audit von eingebetteten Applikationsanmeldedaten

Application Identity Manager entfernt hart kodierte Zugangsdaten wie Passwörter und SSH-Keys aus Anwendungen und Skripten. Die Lösung stellt sicher, dass die Anforderungen an Verfügbarkeit und Betriebskontinuität auch bei komplexen, verteilten Netzwerkumgebungen erfüllt werden. Das Produkt eliminiert eingebettete Anwendungskonten, ohne dass die Anwendungsleistung beeinträchtigt wird. Häufig entsteht nicht einmal Programmieraufwand

On-Demand Privileges Manager™

Least-Privilege-Zugriffskontrolle für UNIX, Linux und Windows

Mit dem On-Demand Privileges Manager können privilegierte Benutzer Admin-Befehle direkt in einer Unix-Session eingeben, ohne auf Root- oder Admin-Rechte angewiesen zu sein. Diese Enterprise-fähige Lösung erlaubt (ähnlich wie beim sudo-Konzept) eine einheitliche, korrelierte Protokollierung aller Superuser-Aktivitäten und verbindet diese mit einem individuellen Benutzernamen, ohne die Benutzer dabei in ihrer Arbeit einzuschränken. Die von Superusern ausgeführten Befehle können anhand ihrer Rollen- und Aufgabendefinition überwacht werden. Gleichzeitig ist eine granulare Zugriffskontrolle gegeben.

Ermitteln Sie Ihr Privileged-Account-Risiko noch heute – mit CyberArk DNA™

CyberArk DNA™ (Discovery & Audit) ist ein kostenloses Analysetool, mit dem privilegierte Benutzerkonten im Unternehmen lokalisiert werden können. Durch eine klare Bestandsaufnahme aller Servicekonten, Geräte und Anwendungen kann das Ausmaß der Risiken festgestellt werden, die mit privilegierten Accounts verbunden sind. Das Tool unterstützt bei der Aufstellung eines Business Case und der Planung eines Sicherheitsprojekts, indem es Schwachstellen aufzeigt und die Priorisierung erleichtert

Technische Daten

Verschlüsselungsalgorithmen:
- AES-256, RSA-2048
- HSM-integration
- Kryptografie nach FIPS 140-2

Hochverfügbarkeit:
- Unterstützt Clustering
- Mehrere Disaster-Recovery-Standorte
- Integration mit unternehmenseigenem Backup-System

Zugriffs- und Arbeitsfluss-Management:
- LDAP-Verzeichnisse
- Identitäts- und Zugriffsmanagement
- Ticketing- und Arbeitsfluss-Systeme

Mehrsprachiges Portal:
- Englisch, Französisch, Deutsch, Spanisch, Russisch, Japanisch, Chinesisch (vereinfacht und traditionell), brasilianisches Portugiesisch, Koreanisch

Authentifizierungsmethoden:
- Benutzername und Passwort, LDAP, Windows-Authentifizierung, RSA SecurID, Web-SSO, RADIUS, PKI und Smartcards

Kontrolle:
- SIEM-Integration, SNMP-Traps, E-Mail-Mitteilungen

Beispiele für unterstützte Systeme:
- Betriebssysteme: Windows, *NIX, IBM iSeries, Z/OS, OVMS, HP Tandem, MAC OS, ESX/ESXi, XenServer
- Windows-Anwendungen: Dienstkonten wie SQL Server-Dienste im Cluster, Scheduled Tasks, IIS-Anwendungspools, COM+, anonymer Zugriff unter IIS, Clusterdienst
- Datenbanken: Oracle, MSSQL, DB2, Informix, Sybase, MySQL und jede ODBC-kompatible Datenbank
- Sicherheitsanwendungen: CheckPoint, Nokia, Juniper, Cisco, Blue Coat, IBM, TippingPoint, SourceFire, Fortinet, WatchGuard , Industrial Defender, Acme Packet, Critical Path, Symantec, Palo Alto, RSA Authentication Manager
- Netzwerkgeräte: Cisco, Juniper, Nortel, HP, 3com, F5, Nokia, Alactel, Quintum, Brocade, Voltaire, RuggedCom, Avaya, BlueCoat, Radware, Yamaha, McAfee NSM
- Anwendungen: SAP, WebSphere, WebLogic, JBOSS, Tomcat, Oracle ERP, Peoplesoft, TIBCO, Cisco
- Verzeichnisse: Microsoft, Sun, Novell, UNIX, CA
- Fernsteuerung und -überwachung: IBM, HP iLO, Sun, Dell DRAC, Digi, Cyclades, Fijitsu
- Virtuelle Umgebungen: VMware vCenter und ESX
- Speicher: NetApp
- Generische Schnittstellen: jedes SSH-/Telnet-Gerät
- Windows-Registrierung für jede Web-Anwendung, z. B Facebook, Twitter, LinkedIn
- Ferngesteuerte WMI-Befehlsausübung
- ODBC- Passwörter in Datenbanktabellen
- Konfigurationsdateien (flat, INI, XML)* – z. B. Konfigurationsdateien für Anwendungsserver b zw. jede Applikations-/Script-Konfigurationsdatei

©CyberArk Software Ltd. I cyberark.com