CYBERARK®

Die CyberArk Privileged Account Security Lösung

Eine umfassende Lösung zum Schutz sowie zur Überwachung, Erkennung, Warnmeldungserstellung und Reaktion auf privilegierte Account-Aktivitäten

Inhalt

Der Privileged Account — eine reale, ernst zu nehmende Bedrohung

Kriminelle Hacker verrichten rund um die Welt enorme Schäden mit professionellen Cyber-Attacken. Sie sind gut organisiert, auf einem technisch hohen Niveau und zielen auf die wertvollsten Güter Ihres Unternehmens ab. Die Angreifer durchbrechen die Perimetersicherung und verschaffen sich internen Zugang. Im Netzwerk angelangt, ermächtigen sie sich des Zugriffs auf kritische Ressourcen, um Unternehmen verheerende Schäden zuzufügen, die zu beschädigten Reputationen, finanziellen Verlusten und entwendetem geistigen Eigentum führen können.

Auch die Öffentlichmachung empfindlicher Daten durch Mitarbeiter und die interne Sabotage sind häufig anzutreffende Bedrohungen. Bei 100 Prozent[1] aller kürzlich verzeichneten Sicherheitsvorfälle kamen entwendete, missbrauchte oder unsicher verwendete Anmeldeinformationen zum Einsatz.

Privilegierte Accounts stellen die größte Sicherheitslücke dar, mit der sich Unternehmen heutzutage konfrontiert sehen. Warum konzentrieren sich Angreifer innerhalb und außerhalb des Netzwerks auf Privileged Accounts?

- Privileged Accounts finden sich in Netzwerkgeräten, Datenbanken, Anwendungen, Servern und Social-Media-Accounts On-Premise sowie in angebundenen Cloud- und in ICS-Systemen.
- Privileged Accounts bieten umfassenden Zugriff auf empfindliche Daten und Systeme
- Privileged Accounts nutzen gemeinsam verwendete administrative Zugriffe und anonymisieren damit ihre Benutzer
- Privileged Accounts verleihen ihren Benutzern umfassende Rechte − häufig weitaus mehr, als sie für die Ausführung ihrer Aufgaben benötigen
- Die Aktivitäten privilegierter Accounts werden nicht überwacht und dokumentiert und stellen daher ein hohes Sicherheitsrisiko dar

Vereinfacht gesagt gestatten sie es jedem, der in ihren Besitz gelangt, die Ressourcen eines Unternehmens zu kontrollieren, Sicherheitssysteme zu deaktivieren und auf eine Fülle sensibler Daten zuzugreifen. Allen Prognosen zufolge wird sich der Missbrauch privilegierter Konten in Zukunft noch verschärfen, sollten Unternehmen jetzt keine Maßnahmen ergreifen. Der Schutz privilegierter Accounts sollte zentraler Bestandteil der IT-Sicherheitsstrategie eines jeden Unternehmens sein. Privileged Accounts stellen ein Sicherheitsproblem dar, weshalb spezielle Kontrollmechanismen für die Sicherung, Überwachung, Erfassung und Maßnahmenergreifung im Zusammenhang mit den Aktivitäten privilegierter Konten erforderlich sind.

Privileged-Account-Anmeldedaten – der Schlüssel zur IT-Festung

Privileged-Account-Anmeldedaten sind der Schlüssel zur IT-Festung eines Unternehmens. Sie werden benötigt, um Zugriff auf alle privilegierten Konten zu erlangen, und sie sind das ausgemachte Angriffsziel von externen Hackern und böswilligen Insidern, um sich direkten Zugriff auf das Herzstück des Unternehmens zu verschaffen. Deshalb sind geschäftskritische Systeme und sensible Daten nur so sicher wie die privilegierten Zugangsdaten, die für den Zugriff auf diese Ressourcen benötigt werden.

Die meisten Unternehmen heutzutage vertrauen auf eine Kombination aus Passwörtern und SSH-Keys zur Authentifizierung von Benutzern und Systemen für privilegierte Accounts. Ungesicherte Anmeldedaten können von Angreifern missbraucht werden, um Zugriff auf privilegierte Konten zu erhalten und sie für Angriffe auf das Unternehmen zu verwenden. Studien zur Cyber-Sicherheit belegen, dass der erfolgreiche Zugriff auf ein privilegiertes Konto die gemeinsame Grundvoraussetzung aller erfolgreichen Cyber-Angriffe ist.

1 2013 CyberSheath Report, APT Privileged Account Exploitation

Und seit Unternehmen vermehrt Schutzmaßnahmen für ihre privilegierten Passwörter einführen, verlagern Angreifer ihre Strategien zunehmend auf die Kompromittierung von SSH-Keys, die beim Schutz von Privileged Accounts häufig übersehen werden. Im Jahr 2013 hat über die Hälfte der vom Ponemon Institute befragten Unternehmen angegeben, Ziel eines SSH-orientierten Angriffs gewesen zu sein.

Um die Anmeldedaten ihrer IT-Umgebung zu schützen, gezielte Angriffe abzuwehren und empfindliche Daten außerhalb der Reichweite von Angreifern zu halten, müssen Unternehmen eine Privileged-Account-Sicherheitsstrategie einsetzen, die den Schutz und die Überwachung aller privilegierten Zugangsdaten inklusive Passwörtern und SSH-Keys gewährleistet.

Lernen Sie von den Experten: CyberArk Privileged Account Security

CyberArk ist führend, wenn es um den Schutz privilegierter Accounts geht. Wir verfügen über mehr Erfahrung auf diesem Gebiet als jeder andere Anbieter und setzen diese Kompetenz gezielt ein, um unsere Kunden bei der Minimierung von Risiken im Zusammenhang mit privilegierten Benutzerkonten zu unterstützen.

Zur Vermeidung gravierender Datenverluste bedarf es einer Sicherheitsstrategie, die speziell auf Risiken im Zusammenhang mit privilegierten Benutzerkonten zugeschnitten ist. CyberArks Privileged Account Security Lösungen bieten umfassende Schutz-, Überwachungs-, Erkennungs-, Warnmeldungserstellungs- und Reporting-Funktionen, die Unternehmen bei der Abwehr von internen und externen Angriffen unterstützen.

Unterschätzen Sie Ihr Risiko?

Der CyberArk Privileged Account Security & Compliance Survey Report hat ergeben, dass 86 Prozent aller großen Unternehmen ihr Privileged-Account-Sicherheitsproblem entweder nicht bewusst ist oder dass sie es massiv unterschätzen. 30 Prozent der Befragten glaubten, in ihren Netzwerken existierten zwischen 1–250 privilegierte Accounts. Für Unternehmen einer Größenordnung von 5000 Mitarbeitern wird die Anzahl privilegierter Accounts aber auf mindestens fünf bis zehn Mal höher geschätzt. Die Studie ergab ebenfalls, dass mehr als ein Drittel der Befragten nicht wusste, wo im Unternehmensnetzwerk die privilegierten Konten zu suchen wären.

Und mit den erhöhten Risiken fortgeschrittener Angriffe sind auch Compliance-Anforderungen wie PCI DSS, Sarbanes Oxley, NIST, NERC-CIP, HIPAA und andere an die Kontrolle, das Management und die Überwachung privilegierter Kontenzugriffe gestiegen.

Unternehmen, die über kein umfassendes Verständnis ihrer Privileged-Account-Umgebung verfügen, haben ein erhöhtes Risiko nicht bestandener Audits und damit empfindlicher Bußgelder und Strafen – und sie laufen Gefahr, gravierende Datenverluste zu erleiden.

Wer sind Ihre Privileged-Account-Benutzer?

Unternehmen sind sich ihrer zahlreichen Privileged-Account-Zugänge häufig nicht bewusst. Nur sehr wenige setzen Sicherheits- und Audit-Richtlinien ein, um die Risiken im Zusammenhang mit ihnen einzudämmen. Ein anonymer, unkontrollierte Zugriff auf diese Konten kann für Unternehmen gravierende Konsequenzen bedeuten.

Die CyberArk Privileged Account Security Lösung

Drittanbieter. Privilegierte Zugänge ermöglichen es Dienstleistern, unbehelligt unter dem Deckmantel der Anonymität zu operieren. Innerhalb des Netzwerks haben externe Dienstleister die Möglichkeit, Rechte zu erhöhen, um Zugriff auf empfindliche Daten im gesamten Unternehmen zu erlangen.

Hypervisor und Cloud-Server-Manager. Geschäftsprozesse wie in den Bereichen Finance, HR und Einkauf werden zunehmend in die Cloud ausgelagert und stellen ein hohes Datensicherheitsrisiko dar, da Cloud-Administratoren über umfassende Zugriffsrechte verfügen.

System-Administratoren. Für beinahe jedes Gerät in einer IT-Umgebung gibt es gemeinsam genutzte privilegierte Konten mit erhöhten Rechten und ungehindertem Zugriff auf die zugrunde liegenden Betriebssysteme, Netzwerke, Server und Datenbanken.

Anwendungen und Datenbank-Administratoren. Anwendungen und Dantenbank-Administratoren verfügen über umfassende Rechte zur Administration der ihnen zugewiesenen Systeme. Diese Rechte ermöglichen ihnen darüber hinaus den Zugriff auf nahezu alle anderen Datenbanken und Anwendungen im Unternehmensnetzwerk.

Ausgewählte Geschäftsanwender. Führungskräfte und IT-Personal verfügen häufig über privilegierten Zugriff auf Geschäftsanwendungen, die empfindiche Daten enthalten. In den Händen der falschen Personen können diese Anmeldeinformationen Zugang zu Unternehmensfinanzdaten, geistigem Eigentum und anderen empfindlichen Daten bedeuten.

Social Media. Privilegierter Zugriff wird für die Administration interner und externer sozialer Netzwerke des Unternehmens gewährt. Mitarbeiter und Dienstleister erhalten privilegierten Zugang, um diese Social-Media-Accounts zu verwenden. Ein Missbrauch dieser Anmeldedaten kann zu einer Öffentlichmachung emfpindlicher Daten und zu Reputationsschäden einer Marke oder eines leitenden Angestellten führen.

Anwendungen. Anwendungen benutzen privilegierte Accounts, um mit anderen Anwendungen, Skripten, Datenbanken, Web-Services und mehr zu kommunizieren. Diese Konten werden oft übersehen und stellen ein wesentliches Sicherheitsrisiko dar, da ihre Anmeldedaten häufig im Programmcode eingebettet und statisch sind. Hacker können diese Angriffspunkte ausnutzen, um sich privilegierte Zugriffe innerhalb des gesamten Unternehmens zu verschaffen.

Policy first: Risikomanagement in Einklang mit Unternehmenszielen bringen

Eine effektive Sicherheitsstrategie verlangt die Schaffung, Implementierung und Durchsetzung privilegierter Account-Sicherheitsrichtlinien, um die Risiken eines schwerwiegenden Vorfalls zu minimieren. Effektive Unternehmenssicherheit und -Compliance beginnen mit gut durchgesetzten Unternehmensrichtlinien. Ein Policy-First-Ansatz gewährleistet, dass die Risiken externer und interner Angriffe reduziert und staatliche sowie branchenspezifische Compliance-Anforderungen erfüllt werden können.

Die CyberArk Shared Technology Platform

Von Grund auf für Privileged-Account-Sicherheit entwickelt, kombiniert CyberArk eine leistungsstarke Basis-Infrastruktur mit den einzelnen Sicherheitsprodukten und bietet damit die branchenweit umfassendste Sicherheitslösung für On-Premise-, Cloud- und ICS-Umgebungen.

Das Herz der Infrastruktur bilden ein isolierter Vault-Server, eine einheitliche Policy Engine, die Discovery Engine und mehrere Sicherheitsebenen, die Skalierbarkeit, Zuverlässigkeit und höchste Sicherheit für privilegierte Accounts gewährleisten.

CyberArk Produkte bieten Schutz, Management und Audit von Benutzer- und Anwendungszugangsdaten, Least-Privilege-Zugriff, Kontrolle von Anwendungen an Endpunkten und Servern und sie sichern, überwachen und analysieren alle privilegierten Aktivitäten – und übermitteln bei auffälligem Verhalten Warnmeldungen. Als manipulationssichere und skalierbare Enterprise-Komplettlösung bietet sie höchsten Schutz vor komplexen externen und internen Bedrohungen sowie Überwachung, Erkennung und Reaktionsfähigkeit selbst für hochgradig verteilte Umgebungen.

Jedes Gerät, jedes Rechenzentrum –
On-Premise, Cloud und ICS

Master Policy™ – vereinfacht, einheitlich und unübertroffen für eine Policy-First-Strategie

Die Master Policy ist eine innovative Policy Engine mit einer einfachen zentralen Benutzeroberfläche in natürlicher Sprache, über die Sicherheitsrichtlinien für privilegierte Accounts festgelegt, verwaltet und überwacht werden können. Der ursprünglich komplexe Prozess der Transformation von Geschäftsvorgaben und -prozeduren in durchsetzbare technische Richtlinien ist für alle Stakeholder eines Unternehmens, inklusive Sicherheits-, Risiko- und Audit-Teams, jetzt leicht verständlich und einfach verwaltbar. Die Master Policy ist im Kern des Systems verankert, stellt Richtlinien für alle Privileged-Account-Sicherheitsprodukte von CyberArk bereit und bietet damit ein vereinfachtes, einheitliches und unübertroffenes Richtlinien-Management.

Die Master Policy überführt Sicherheitsvorgaben in technische Richtlinien und ermöglicht die Verwaltung dieser Richtlinien mithilfe natürlicher Sprache. Privileged-Account-Sicherheitskontrollen können nun innerhalb von Minuten implementiert werden und vereinfachen damit einen effektiven Sicherheitsprozess, der ohne die Master Policy Tage oder Wochen beanspruchen würde. Die Master Policy bietet eine schnelle Implementierung und hohe Flexibilität für die Durchsetzung unternehmensweiter Richtlinien und ermöglicht gleichzeitig die kontrollierte Anwendung granularer Ausnahmen, um den Anforderungen von Betriebssystemen, Regionen, Abteilungen und Unternehmensbereichen entsprechen zu können.

Digital Vault™

Der prämierte, patentierte Digital Vault™ ist ein isolierter, gehärteter Server mit Verschlüsselung nach FIPS 140-2, der nur auf Vault-Protokolle reagiert. Zur Gewährleistung der Zugriffssicherheit interagieren alle CyberArk Produkte unmittelbar mit dem Digital Vault und verwenden gemeinsame Daten, die es allen Produktmodulen und -komponenten ermöglichen, sicher miteinander zu kommunizieren und von den Vorteilen der sicheren (und manipulationssicheren) Speicherung von Passwörtern, SSH-Keys, Richtlinieneinstellungen und Audit-Logs zu profitieren. Einzelne Schwachstellen werden vermieden.

- **Aufgabentrennung und starke Zugriffskontrolle.** Der Administrator des Vaults hat keinen Zugriff auf die im Vault gespeicherten Zugangsdaten, wodurch eine effektive Aufgabentrennung gewährleistet wird. Die Lösung unterstützt viele Authentifizierungsmethoden, um die Sicherheit und Kontrolle des Zugriffs auf und der Aktivitäten von allen privilegierten Anmeldeinformationen zu gewährleisten.
- **Mehrere Sicherheitsebenen.** Die sieben integrierten Sicherheitsebenen für Authentifizierung, Zugriffskontrolle, Verschlüsselung, manipulationssichere Speicherung und den Datenschutz ohne Hintertür oder DBA-Zugang bieten beispiellose Sicherheit für privilegierte Accounts.
- **Hohe Verfügbarkeit und Disaster Recovery.** Die Infrastruktur ist auf hohe Verfügbarkeit ausgelegt und bietet integrierte, ausfallsichere Maßnahmen, um Disaster-Recovery-Anforderungen zu erfüllen und zu übertreffen, inklusive sicherer Backup- und einfacher Wiederherstellungsfähigkeiten.

Discovery Engine

Die Discovery Engine erkennt jede Änderung in der IT-Umgebung. Sie gewährleistet, dass alle Privileged-Account-Aktivitäten ausgewiesen und sicher sind, und liefert so jederzeit einen aktuellen Schutz. Änderungen der Privileged Accounts werden beim Hinzufügen und Entfernen von Servern und Workstations automatisch erkannt.

Integration der Enterprise-Klasse

CyberArks Privileged Account Security Lösung unterstützt Ihre bestehenden Investitionen mit schlüsselfertigem Support für zusätzliche Geräte, Netzwerke, Anwendungen und Server inklusive Websites und Social Media.

- **SIEM.** Vollständige wechselseitige Integration mit SIEM-Anbietern verbessert die Bedrohungserkennung und Wanrmeldungserstellung. CyberArk übermittelt Ereignisse privilegierter Zugriffe und Aktivitäten sowie bei der Überwachung privilegierter Sitzungen erkannte Aktivitäten auf Kommandoebene an SIEM-Lösungen.
- **Hybrid Cloud.** Die Unterstützung von Hybrid-Cloud-Umgebungen ermöglicht die Erkennung und den Schutz von Hypervisor- und Gast-Zugängen für Cloud-Administratoren, AWS, SaaS-Anwendungen und Social-Media-Accounts wie Twitter, Facebook und LinkedIn.
- **Vulnerability Manager.** Umfassende Integration mit führenden Vulnerability-Management-Anbietern ermöglicht eine vereinfachte Durchführung „authentifizierter Scans“ (auch „Deep Scans“ genannt) und die Bereitstellung von Privileged Accounts über den Vault, wenn der Serverzugriff für einen Scan-Vorgang benötigt wird.
- **Gestion des identités.** Integration mit führenden Lösungen für das Identity & Access Management (IAM) gewährleistet die Account-Bereitstellung für diese Lösungen auf Basis von Verzeichnisinformationen, Gruppenmitgliedschaften und Identity-Governance-Richtlinien. Die Integrationen ermöglichen es unseren Kunden zudem, frühere Investitionen mit sicherer Authentifizierung wie PKI, Radius, web-sso, LDAP und mehr zu nutzen.
- **Helpdesk.** Integration mit Ticketing-Systemen wie Remedy, HEAT, HP Service Manager und In-House-Lösungen. Die Funktionen umfassen die Anfragevalidierung, Erstellung neuer Serice-Anfragen und Integration mit Freigabeprozessen wie Manager-Freigabe (duale Kontrolle) und zeitlich festgelegte Verfügbarkeit.

Skalierbare, flexible und schlanke Architektur

Die CyberArk Privileged Account Security Lösung wirkt sich minimal auf die bestehende IT-Umgebung aus und schützt so vorhandene Investitionen. Alle Komponenten arbeiten unabhängig voneinander, verwenden aber gemeinsame Ressourcen und Zugangsdaten. Dieser flexible Ansatz ermöglicht es Unternehmen, Projekte auf Abteilungsebene zu initiieren und über Zeit eine komplexe, verteilte Unternehmenslösung zu entwickeln.

CyberArk Produkte

Jedes Produkt der CyberArk Privileged Account Security Lösung kann eigenständig betrieben und unabhängig verwaltet werden, während es Ressourcen und Daten aus der gemeinsamen Infrastruktur nutzt.

Die Produkte im Einzelnen dienen jeweils einer speziellen Anforderung der Privileged-Account-Sicherheit und bieten in Kombination eine umfassende, sichere Lösung für Betriebssysteme, Server, Datenbanken, Anwendungen, Hypervisoren, Netzwerkgeräte, Sicherheitsanwendungen und mehr, sowohl On-Premise als auch in Cloud- und ICS-Umgebungen.

Schritte zum Schutz Ihrer Privileged Accounts:

- Legen Sie zuerst Richtlinien fest
- Ermitteln Sie alle privilegierten Accounts und Anmeldedaten
- Schützen und verwalten Sie alle privilegierten Benutzer- und Anwendungsanmeldedaten
- Kontrollieren, sichern und überwachen Sie privilegierte Zugriffe auf Server und Datenbanken, Websites, SaaS und jegliche Zielanwendungen
- Stellen Sie Least-Privilege-Zugriffe für Geschäftsandwender und Administratoren bereit
- Kontrollieren Sie Anwendungen an Endpunkten und Servern
- Verwenden Sie Echtzeit-Privileged-Account-Überwachung, um aktive Angriffe zu identifizieren und Maßnahmen zu ergreifen

Enterprise Password Vault®

Schutz, Management und Audit privilegierter Passwörter

Der Enterprise Password Vault verhindert den Missbrauch privilegierter Benutzerpasswörter und gewährleistet Ordnung und Sicherheit für anfällige Konten. Der Enterprise Password Vault schützt privilegierte Passwörter auf Grundlage von Sicherheitsrichtlinien für privilegierte Accounts und steuert, wer zu welcher Zeit Zugriff auf welche Passwörter erhält. Dank dieses automatisierten Prozesses wird die zeitaufwendige und fehleranfällige manuelle Verfolgung und Aktualisierung privilegierter Passwörter reduziert, wodurch sich Audit- und Compliance-Anforderungen problemlos erfüllen lassen.

- Erkennt privilegierte Accounts und abhängige Dienste und leitet diese Konten an den Digital Vault zur Verwaltung weiter
- Kontrolliert den Zugriff auf privilegierte Account-Passwörter auf Grundlage von Richtlinien
- Bietet anpassbare Abläufe für Passwortanfragen, inklusive dualer Kontrollen und Integration mit Helpdesk-Ticketing-Systemen
- „Click-to-Connect"-Fähigkeit, um Passwörter vor dem Blick von Endbenutzern zu schützen
- Durchführung periodischer Passwortwechsel auf Grundlage Ihrer Anforderungen
- Bietet Steuerungen für Einmalpasswörter
- Integriert mit Helpdesk- und Ticketing-Systemen
- Verfiziert fortlaufend Anmeldedaten, stellt veraltete Passwörter wieder her und setzt diese zurück
- Erhält Warnmeldungen zu potenziell kompromittierten Privileged Accounts von Privileged Threat Analytics und rotiert automatisch betroffene Anmeldedaten

SSH Key Manager™

Schutz, Rotation und Überwachung privilegierter SSH-Keys

Der SSH Key Manager unterstützt Unternehmen dabei, unautorisierten Zugriff auf private SSH-Keys zu verhindern, die häufig von privilegierten Unix-/Linux-Benutzern und -Anwendungen für die Authentifizierung privilegierter Accounts verwendet werden. Der SSH Key Manager schützt und rotiert privilegierte SSH-Keys auf Grundlage Ihrer Privileged-Account-Sicherheitsrichtlinien und -kontrollen und überwacht den Zugriff auf geschützte SSH-Keys. Mithilfe dieser Lösung erlangen Unternehmen die Kontrolle über ihre SSH-Keys, die Zugriff auf privilegierte Accounts bieten, häufig jedoch nicht verwaltet werden.

- Gewährleistet sichere Speicherung und Kontrolle des Zugriffs auf private SSH-Keys im Digital Vault
- Rotiert SSH-Key-Paare automatisch auf Grundlage von Unternehmensrichtlinien
- Unterstützt und setzt effektive Zugriffskontrollen für die Authentifizierung und Verwaltung von Anfragen für erhöhte Privilegienrechte durch
- Verwaltet SSH-Keys auf Grundlage voreingestellter Richtlinien
- Ermöglicht Administratoren die Überwachung und Berichterstellung für die Verwendung von SSH-Keys durch Benutzer und Anwendungen

Privileged Session Manager®

Schutz, Kontrolle und Echtzeit-Sitzungsüberwachung und -aufzeichnung

Der Privileged Session Manager schützt, kontrolliert und überwacht privilegierte Benutzerzugriffe sowie Aktivitäten für wichtige UNIX-, Linux- und Windows-basierte Systeme, Datenbanken, virtuelle Maschinen, Netzwerkgeräte, Mainframes, Websites, SaaS und mehr. Er bietet einen zentralen Zugriffspunkt, hindert Schadsoftware vor dem Überspringen auf Zielsysteme und zeichnet jeden Tastaturanschlag und Mausklick für kontinuierliche Überwachung auf.

DVR-artige Aufzeichnungen liefern umfassende Bilder von Sitzungen inklusive Such-, Lokalisierungs- und Warnmeldungsfähigkeit für empfindliche Ereignisse, ohne die Notwendigkeit einer Log-Filterung. Die Echtzeit-Überwachung gewährleistet einen fortlaufenden Schutz für privilegierte Zugriffe sowie Echtzeit-Intervention für den sofortigen Abbruch von verdächtigen Aktivitäten. Der Privileged Session Manager ist darüber hinaus umfassend mit SIEM-Lösungen von Drittanbietern integriert und übermittelt Warnhinweise bei unüblichen Aktivitäten.

- Bietet einen zentralen Kontrollpunkt für privilegierte Sitzungen
- Schützt privilegierte Passwörter und SSH-Keys vor fortschrittlichen Angriffstechniken wie der Aufzeichnung von Tastaturaktivitäten und Pass-the-Hash-Angriffen
- Schützt und kontrolliert privilegierte Sitzungen, um Schadsoftware und Zero-Day-Attacken am Umgehen von Sicherheitsmechanismen zu hindern
- Erweitert die Überwachung privilegierter Sitzungen auf Anwendungs-Clients, Web-Anwendungen und Websites über spezielle Schnittstellen
- Erstellt und indexiert manipulationssichere Aufzeichnungen privilegierter Sitzungen
- Bietet Kontrolle auf Kommandozeilenbasis sowie nativen SSH-Zugriff, während gleichzeitig der sichere Zugang für privilegierte Benutzer unter Verwendung von Passwörtern und SSH-Keys gewährleistet bleibt
- Exportiert Daten an SIEM-Produkte für die forensische Analyse privilegierter Sitzungen
- Bietet AD-Bridge-Funktionen, die es Unternehmen ermöglichen, Unix-Benutzer und -Konten, die über die CyberArk-Plattform mit AD verbunden sind, zentral zu verwalten.

Privileged Threat Analytics™

Analyse und Meldung bösartiger Aktivitäten über privilegierte Accounts

CyberArk Privileged Threat Analytics ermöglicht Unternehmen die Erkennung und Meldung von sowie Reaktion auf ungewöhnliche privilegierte Aktivitäten, die auf einen laufenden Angriff hindeuten. Hierzu erfasst CyberArk Privileged Threat Analytics gezielt Daten aus verschiedenen Quellen wie CyberArk Digital Vault, SIEM-Lösungen und Netzwerk-Taps und -Switches. Die Lösung wendet daraufhin eine komplexe Kombination aus statistischen und deterministischen Algorithmen auf diese Daten an, um bösartige Aktivitäten privilegierter Accounts zu ermitteln, wodurch sich Anzeichen für Kompromittierungen frühzeitig erkennen lassen.

- Erkennung und Meldung in Echtzeit
- Ermöglicht die automatische Reaktion auf erkannte Vorfälle
- Erstellt Profile typischen privilegierten Benutzerverhaltens
- Identifiziert Anomalien inklusive bösartiger Aktivitäten privilegierter Accounts sowie verdächtigen Kerberos-Datenverkehrs, die auf einen laufenden Angriff hindeuten
- Passt die Bedrohungsanalyse durch selbstlernende Algorithmen fortlaufend an ein sich änderndes Risikoumfeld an
- Korreliert Vorfälle und ordnet sie Bedrohungsstufen zu
- Erhöht den Wert bestehender SIEM-Lösungen mit schlüsselfertigen Integrationen
- Verbessert Auditing-Prozesse mit informativen Daten zu Benutzermustern und -aktivitäten

Application Identity Manager™

Schutz, Management und Audit eingebetteter Zugangsdaten für Anwendungen

Der Application Identity Manager ersetzt hartcodierte Passwörter und lokal gespeicherte SSH-Keys in Anwendungen und Skripten. CyberArks Application Identity Manager stellt sicher, dass Ihre hohen Unternehmensanforderungen an Verfügbarkeit und Geschäftskontinuität auch bei komplexen, verteilten Netzwerkumgebungen erfüllt werden. Das Produkt ersetzt statische eingebettete Zugangsdaten ohne Beeinträchtigung der Anwendungsperformance und in vielen Fällen ohne Codeänderungen.

- Ersetzt hartcodierte Passwörter und lokal gespeicherte SSH-Keys mit einem Skript, dass es diesen Anwendungen ermöglicht, die Anmeldeinformationen nach Bedarf über den Digital Vault zu beziehen
- Stellt einen sicheren, lokalen Cache auf dem Server für hohe Verfügbarkeit und die Aufrechterhaltung eines hohen Leistungsstandards zur Verfügung
- Ermöglicht den spontanen Austausch von Passwörtern ohne Beeinträchtigung der Systemleistung
- Authentifiziert Anwendungen bei Passwortanfragen auf Grundlage von Eigenschaften wie Pfad- und Anwendungssignatur
- Gewährleistet eine hohe Verfügbarkeit und Zuverlässigkeit für Produktionssysteme
- Bietet eine einzigartige patentierte Lösung zur Verwaltung von Anmeldedaten für Datenpunkte auf Anwendungsservern

Endpoint Privilege Manager

Gewährleisten Sie Privilege-Sicherheit an Endpunkten

Der Endpoint Privilege Manager schützt Benutzerrechte an Endpunkten und dämmt Gefahren frühzeitig ein. Durch nahtloses Erhöhen von Privilegien für autorisierte Anwendungen und Aufgaben ermöglicht er den Entzug lokaler Administratorrechte bei minimaler Beeinträchtigung der Benutzeraktivität. Eine Anwendungskontrolle mit automatisierter Richtlinienerstellung ermöglicht es, Schadsoftware an der Ausführung zu hindern und unbekannte Anwendungen mit eingeschränkten Rechten ausführen zu lassen. In Kombination mit dem Schutz der Anmeldeinformationen wird Schadsoftware daran gehindert, sich auszubreiten, und Angriffe werden bereits am Endpunkt abgewehrt.

- Ermöglicht den Entzug von Administratorrechten für Geschäftsanwender, ohne deren Produktivität zu beeinträchtigen.
- Erhöht automatisiert Berechtigungen und erstellt Anwendungskontrollrichtlinien für mehr als 90 Prozent der Anwendungen in der Umgebung
- Trennt die Aufgaben auf Windows-Servern über die Kontrolle von Administratorrechten auf Benutzerrollenbasis
- Erhöht nahtlos Berechtigungen auf Richtlinienbasis, um die Ausführung autorisierter Anwendungen und Befehle zu ermöglichen
- Hindert böswillige Anwendungen daran, in die Umgebung zu gelangen und sich im Netzwerk zu verbreiten
- Ermöglicht Benutzern die Ausführung von Anwendungen mit eingeschränkten Rechten, um ihre Produktivität nicht zu beeinträchtigen
- Unterstützt Unternehmen dabei, den Diebstahl von Anmeldeinformationen in Windows und populären Web-Browsern zu erkennen und zu unterbinden
- Integration mit Check Point, FireEye und Palo Alto Networks Lösungen zur Bedrohungserkennung ermöglicht die automatisierte Analyse unbekannter Anwendungen
- Ermittelt den Ursprung und sämtliche Instanzen bösartiger Anwendungen innerhalb der Umgebung, um die Wiederherstellung zu beschleunigen
- Unterstützt drei Deployment-Methoden inklusive Server, SaaS und Microsoft GPO

On-Demand Privileges Manager™

Least-Privilege-Zugriffskontrolle für Unix und Linux

Der On-Demand Privileges Manager ermöglicht es privilegierten Benutzern, Admin-Befehle ohne unbenötigte Root- oder Admin-Rechte direkt in einer Unix-/Linux-Session ausführen Diese sichere und Enterprise-fähige Lösung erlaubt – ähnlich wie beim sudo-Konzept – eine einheitliche, korrelierte Protokollierung aller Superuser-Aktivitäten und verbindet diese mit individuellen Benutzernamen, ohne die Benutzer dabei in ihrer Arbeit einzuschränken. Eine granulare Zugriffssteuerung wird gewährt, während gleichzeitig die kontinuierliche Überwachung aller von Superusern ausgeführten administrativen Befehle auf Grundlage ihrer Rollen und Aufgaben gewährleistet bleibt.

- Ersetzt konventionell verwendete sudo-Lösungen durch eine zentral gesteuerte Alternative, die eine granulare Rechtesteuerung und sichere Speicherung von Audit-Logs gewährleistet
- Bietet den Nachweis sicherer, verwalteter und kontrollierter Superuser-Berechtigungen für Auditoren
- Stellt detaillierte Audit-Trails individueller Root-Berechtigungserhöhungen mit Zeitpunkt und Begründung zur Verfügung
- Beschränkt Superuser-Berechtigungen auf das notwendige Minimum,um das Missbrauchs- und Fehlerrisiko zu reduzieren
- Autorisiert Benutzer-Zugriff auf vollständige delegierte Root-Shells, um eine intuitive Arbeit in Einklang mit Arbeitsabläufen zu ermöglichen
- Verbindet Root-Konten und -Aktivitäten mit einem persönlichen Benutzernamen
- Ermöglicht das Whitelisting/Blacklisting auf Benutzer- und/oder System-Basis

Warum die CyberArk Privileged Account Security Lösung wählen?

Enterprise-bewährte, branchenführende Experten

Mit unserer preisgekrönten, patentierten Technologie und nachweislichen Expertise bieten wir als einziger Hersteller einen vollständigen Schutz vor Insider-Angriffen und komplexen Bedrohungen von außen, der Sicherheitsrisiken effektiv senkt und höchsten Compliance-Anforderungen genügt.

CyberArk ist führend bei Installationen in großen verteilten und virtuellen Umgebungen und der Beseitigung von Sicherheitsproblemen im Zusammenhang mit privilegierten Accounts. Wir unterstützen eine enorme Auswahl von Geräten On-Premise sowie in der Cloud und in ICS-Umgebungen. CyberArk ist der einzige Anbieter mit einer nativen Lösung, die umfassenden Schutz von Anmeldedaten, Sitzungssicherheit, Least-Privilege- und Anwendungskontrolle, kontinuierliche Überwachung und die frühzeitige Erkennung von Bedrohungen sowie Berichterstellung für privilegierte Kontenaktivitäten bietet.

Beginnen Sie heute mit der Ermittlung Ihres Privileged-Account-Risikos

CyberArk DNA™ (Discovery & Audit) ist ein kostenloses Analysetool, mit dessen Hilfe Sie die privilegierten Accounts innerhalb Ihres Unternehmens lokalisieren können. Durch die Sichtbarmachung Ihrer Benutzerkonten, SSH-Keys, Service-Konten, Geräte und Anwendungen können wir Sie dabei unterstützen, das Ausmaß der Sicherheitsrisiken in Zusammenhang mit Ihren privilegierten Accounts nachvollziehen können. Das Tool assistiert Ihnen bei der Erstellung Ihres Business-Case bzw. der Planung Ihres Privileged-Account-Sicherheitprojekts, um Sie bei der Ermittlung Ihrer drängendsten Sicherheitslücken und der Projektpriorisierung zu unterstützen.

Während die meisten Unternehmen sich für eine sofortige unternehmensweite Lösung entscheiden, liegt die besondere Stärke der CyberArk Lösung darin, dass Sie mit Ihrem Privileged-Account-Sicherheitsprojekt zunächst dort ansetzen können, wo Ihre größten Sicherheitslücken bestehen. Einige Unternehmen beginnen mit dem Schutz privilegierter Anmeldedaten und weiten die Lösung auf die Überwachung aus, sobald die Prioritäten sich verschieben.

Da die Infrastruktur mit der initialen Lösung bereits implementiert wird, gestaltet sich die Erweiterung um zusätzliche Komponenten einfach, und Sie können den Schutz Ihrer privilegierten Konten schrittweise ausweiten. Mit der Komplettlösung erhält Ihr Unternehmen schließlich umfassende Sicherheit vor Insider-Angriffen und fortgeschrittenen Cyber-Bedrohungen.

Über CyberArk

CyberArk ist auf den Schutz vor fortschrittlichen Cyber-Angriffen spezialisiert, die Schwächen in der Berechtigungsvergabe für privilegierte Zugriffe auf IT-Systeme ausnutzen und Unternehmen damit direkt ins Herz treffen. Weltweit führende Unternehmen vertrauen auf die Lösungen von CyberArk zum Schutz ihrer kritischen Daten, Infrastrukturen und Anwendungen.

Seit mehr als einem Jahrzehnt ist CyberArk der führende Anbieter für den Schutz von Unternehmen vor Cyber-Attacken, die unter dem Deckmantel von Insider-Privilegien operieren und auf kritische Unternehmensdaten abzielen. CyberArk bietet heute als einziger Anbieter eine neue Kategorie zielgerichteter Sicherheitslösungen, die es führenden Unternehmen ermöglichen, nicht länger auf Cyber-Bedrohungen zu reagieren, sondern diese zu antizipieren und die Ausbreitung von Attacken einzudämmen, bevor irreparable Unternehmensschäden entstehen. Zu einer Zeit, in der Auditoren und Aufsichtsbehörden anerkennen, dass privilegierte Accounts das bevorzugte Mittel von Cyber-Attacken sind und des besonderen Schutzes bedürfen, gewährleisten CyberArks Sicherheitslösungen die Erfüllung höchster Compliance- und Audit-Anforderungen und schützen die wertvollsten Güter Ihres Unternehmens.

Weitere Informationen unter www.cyberark.de.