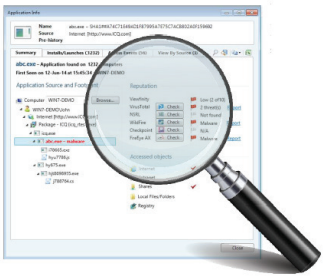
Viewfinity

Minimieren Sie effektiv lokale Administratorrechte und kontrollieren Sie Anwendungen auf Endpunkten und Servern.



Verwalten Sie alle Richtlinien für Privilegien, Anwendungen und Sicherheitsbewertungen an einem zentralen Ort.

Warum CyberArk?

CyberArk ist Ihr zuverlässiger Experte im Kampf gegen Cyber-Angriffe, bevor sich diese geschäftsschädigend auswirken.

Die Herausforderung

Benutzerkonten mit lokalen Administratorrechten bieten eine große und häufig ausgenutzte Angriffsfläche, jedoch kann der vollständige Entzug dieser Rechte zu ungewünschten Konsequenzen führen. Durch den Entzug von Privilegien können Unternehmen ihre Angriffsfläche zwar verringern, doch dieser Sicherheitsvorteil kann sich deutlich auf die Produktivität auswirken, wenn die Benutzer nicht mehr über die für ihre täglichen Aufgaben erforderlichen Rechte verfügen. Andererseits werden Privilegien für Administratoren entweder vollständig oder gar nicht erteilt. In der Folge haben Administratoren häufig unnötigerweise vollständige administrative Rechte für Server, wodurch sensible Server einem höheren Risiko ausgesetzt werden. Erschwerend kommt hinzu, dass Computer trotz der Bemühungen von Unternehmen, die Angriffsfläche durch Minimierung von Privilegien zu reduzieren, anfällig für Schadsoftware sein können, die ohne Privilegien auskommt..

Um die Angriffsfläche wirksam zu verringern und das Risiko eines schwerwiegenden Datendiebstahls zu minimieren, ohne die Produktivität zu gefährden, sollten Unternehmen über Werkzeuge verfügen, die flexible Least-Privilege-Richtlinien für Benutzer und Administratoren durchsetzen und kontrollieren, welche Anwendungen ausgeführt werden dürfen. Ohne solche Werkzeuge stehen Unternehmen folgenden Herausforderungen gegenüber:

- **Verlorene Geschäftsproduktivität.** Der Entzug aller Privilegien kann dazu führen, dass Benutzer bestimmte Aufgaben nicht mehr ausführen oder bestimmte Anwendungen für ihre täglichen Aufgaben nicht mehr verwenden können. Folglich können unflexible Richtlinien für Privilegien den Geschäftsbetrieb zum Stillstand bringen.

- **Hohe Helpdesk-Kosten.** Wenn IT-Richtlinien dazu führen, dass Benutzer ihren täglichen Aufgaben nicht mehr vollständig nachkommen können, muss das Helpdesk die erforderlichen Berechtigungen wiederherstellen. Dies kann sich erheblich auf die IT-Kosten auswirken und einen hohen Mehraufwand für das Support-Team bedeuten.

- **Erhöhte Sicherheitsrisiken durch „schleichende Ausweitung von Privilegien".** Entzieht ein Unternehmen seinen Benutzern alle Privilegien, muss das IT-Team diese von Fall zu Fall für bestimmte Aufgaben neu gewähren. Erneut gewährte Privilegien werden jedoch nur selten wieder entzogen. Diese „schleichende Ausweitung von Privilegien" öffnet erneut die mit der übermäßigen Erteilung administrativer Rechte verbundene Sicherheitslücke und macht das Unternehmen anfälliger für Bedrohungen.

- **Erhöhtes Risiko für Insider- und komplexe Bedrohungen.** Wenn Administratorrechte nach dem Prinzip „Alles oder nichts" vergeben werden, erhalten diese Administratoren häufig viel mehr Privilegien als nötig. Ohne rollenbasierte Richtlinien für Privilegien können sensible Systeme leicht von unerfahrenen Benutzern, böswilligen Insidern oder Angreifern, die unbefugten Kontozugriff erhalten haben, missbraucht oder beschädigt werden.

- **Erhöhtes Risiko für erfolgreiche Angriffe mit Schadsoftware.** Auch Unternehmen, die Benutzerrechte auf Windows-Geräten minimieren, können anfällig für Schadsoftware sein, die ohne entsprechende Privilegien auskommt. Ohne ergänzende Werkzeuge zur Kontrolle, welche Anwendungen ausgeführt werden dürfen, können sich Angreifer mithilfe von Schadsoftware Zugang zum Unternehmen verschaffen.

Die Lösung

CyberArk Viewfinity ermöglicht Unternehmen die Durchsetzung von Least-Privilege-Richtlinien für Benutzer und Administratoren sowie die Kontrolle von Anwendungen zur Verringerung der Angriffsfläche ohne Beeinträchtigung der Produktivität. Die Lösung hilft Unternehmen, Benutzern alltägliche lokale Administratorrechte zu entziehen. Gleichzeitig können Privilegien nahtlos erweitert werden, wenn vertrauenswürdige Anwendungen dies erfordern. Mit CyberArk Viewfinity können Sicherheitsteams darüber hinaus gezielte Least-Privilege-Richtlinien für Administratoren durchsetzen und so Aufgaben auf Windows-Servern effektiv trennen. Ergänzend zu dieser Privilegiensteuerung bietet die Lösung eine Möglichkeit zur Anwendungssteuerung, um die auf Endpunkten und Servern ausführbaren Anwendungen zu verwalten und zu kontrollieren sowie zu verhindern, dass böswillige Anwendungen in die Umgebung gelangen. Mit CyberArk Viewfinity haben Unternehmen folgende Möglichkeiten:

- **Automatische Erstellung von Richtlinien je nach Geschäftsanforderungen.** CyberArk Viewfinity erstellt automatisch Richtlinien zur Anwendungssteuerung und Ausweitung von Privilegien auf der Grundlage von vertrauenswürdigen Quellen, wie SCCM, Softwareanbietern, Updatern und mehr.

- **Durchsetzung gezielter Least-Privilege-Richtlinien für Windows-Administratoren.** CyberArk Viewfinity ermöglicht Sicherheitsteams die gezielte Kontrolle, welche Befehle und Aufgaben von einem Administrator je nach dessen Rolle auf Windows-Servern ausgeführt werden dürfen.

- **Nahtlose Ausweitung von Benutzerrechten nach Bedarf.** Nach dem Entzug lokaler Administratorrechte kann CyberArk Viewfinity die Privilegien je nach Richtlinie nahtlos erweitern, wenn vertrauenswürdige Anwendungen dies erfordern.

- **Schnelle Erkennung und Blockierung böswilliger Anwendungen.** Unbekannte Anwendungen werden automatisch mit kommerziell erhältlichen Blacklist-Datenbanken, wie VirusTotal und NSRL, abgeglichen, um schnell bekannte Schadsoftware zu identifizieren und globale Richtlinien zur Verhinderung der Ausführung dieser Anwendungen in der Umgebung zu aktualisieren.

- **Sichere Ausführung unbekannter Anwendungen im eingeschränkten Modus.** Unbekannte Anwendungen, die weder vertrauenswürdig sind noch als böswillig gelten, können im „eingeschränkten Modus" ausgeführt werden. Benutzer können Anwendungen in diesem Modus ausführen, wobei die Anwendungen daran gehindert werden, auf Unternehmensressourcen, sensible Daten oder das Internet zuzugreifen.

- **Nutzung von Integrationen mit Werkzeugen zur Bedrohungserkennung und Analyse unbekannter Anwendungen.** CyberArk Viewfinity kann unbekannte Anwendungen an Lösungen zur Bedrohungserkennung, wie Check Point, FireEye und Palo Alto Networks, zur automatischen Dateianalyse übermitteln. Diese Lösungen ermitteln dann den Grad der Vertrauenswürdigkeit, auf dessen Grundlage IT-Teams eine Entscheidung hinsichtlich der Blockierung oder Zulassung einer Anwendung in der Umgebung treffen können.

- **Erkennung sämtlicher Instanzen von Schadsoftware in der Umgebung.** Anhand eines Kernel-basierten Agenten auf jedem geschützten Gerät kann die Lösung sofort alle Instanzen einer böswilligen Anwendung innerhalb der Umgebung sowie die Herkunft jeder böswilligen Anwendung lokalisieren.

Vorteile

CyberArk Viewfinity ermöglicht Unternehmen die Verringerung ihrer Angriffsfläche bei gleichzeitiger Gewährleistung der Produktivität. Die Lösung bietet Unternehmen folgende Vorteile:

- **Beschleunigung der Amortisationszeit.** Minimieren Sie zeitintensiven, manuellen IT-Aufwand mithilfe von vertrauenswürdigen Quellen zur Automatisierung der Erstellung von Richtlinien für Privilegien für über 90 Prozent der Anwendungen innerhalb des Unternehmens.

- **Aufrechterhaltung der Produktivität ohne Beeinträchtigung der Sicherheit.** Ermöglichen Sie Benutzern ohne lokale Administratorrechte die sichere Ausführung unbekannter Anwendungen zur Erhaltung ihrer Produktivität.

- **Senkung des Risikos für Insider- und komplexe Bedrohungen.** Verhindern Sie versehentliche oder absichtliche Beschädigung geschäftskritischer Windows-Server durch Trennung von Aufgaben und gezielte Kontrolle administrativer Rechte basierend auf der jeweiligen Rolle.

- **Senkung des Risikos für Angriffe mit Schadsoftware.** Verhindern Sie proaktiv Angriffe mit Schadsoftware, um in die IT-Umgebung einzudringen, indem Sie kontrollieren, welche Anwendungen ausgeführt werden dürfen und auf welche Ressourcen jede Anwendung zugreifen darf.

- **Nutzung bestehender Investitionen zur schnellen und präzisen Erkennung von Bedrohungen.** Beschleunigen Sie die Analyse unbekannter Anwendungen mithilfe der Lösungen von Check Point, FireEye und Palo Alto Networks, um potenzielle Bedrohungen zu analysieren und zu erkennen.

- **Beschleunigung der Beseitigung von Bedrohungen.** Erkennen Sie schnell das Ausmaß von Bedrohungen und beschleunigen Sie Abhilfemaßnahmen, indem Sie einen klaren Einblick in den Umfang und die Herkunft böswilliger Anwendungen innerhalb der IT-Umgebung gewinnen.

Eine umfassende Lösung

CyberArk Viewfinity ist Teil der CyberArk Privileged Account Security Lösung, einer ganzheitlichen Lösung für den aktiven Schutz vor Angriffen, bei denen administrative Rechte ausgenutzt werden, um Zugang zum Herzen des Unternehmens zu gewinnen, sensible Daten zu stehlen und geschäftskritische Systeme zu beschädigen. Die Lösung hilft Unternehmen, ihre Angriffsfläche durch Entzug unnötiger lokaler Administratorrechte und Stärkung der Sicherheit privilegierter Accounts zu verringern. Die CyberArk Privileged Account Security Lösung schützt, isoliert, kontrolliert und überwacht kontinuierlich aktiv privilegierte Accounts auf bzw. in physischen und virtuellen Maschinen, Datenbanken, Anwendungen, Hypervisoren, Netzwerkgeräten, Sicherheitsgeräten und mehr. Die Produkte innerhalb der Lösung können unabhängig voneinander verwaltet oder zu einer umfassenden Sicherheitslösung für privilegierte Accounts kombiniert werden.

Technische Daten

Unterstützte Plattformen

Windows Desktop :

- Windows XP SP3
- Windows Vista SP1
- Windows 7 32 bits und 64-Bit
- Windows 8 32 bits und 64-Bit
- Windows 8.1 32 bits und 64-Bit
- Windows 10

Windows Server :

- Windows Server 2003 SP2 32-Bit und 64-Bit
- Windows Server 2008 32-Bits et 64-Bits
- Windows Server 2008 R2 64-Bits
- Windows Server 2012
- Windows Server 2012 R2

Umfassende Anwendungsunterstützung:

- Ausführbare Dateien
- MSI, MSU
- Administrative Aufgaben
- Snap-ins für Management Console
- Skripte
- Registrierungseinstellungen
- ActiveX-Steuerelemente
- COM-Objekte
- Web-Anwendungen

Flexible und sichere Anwendungsregeln:

- Abgleich von Dateipfaden
- Abgleich von Befehlszeilen
- Datei-Hashing (SHA-1)
- Produkt- und Dateiinformationen
- Vertrauenswürdiger Anbieter
- Vertrauenswürdiges SCCM
- Vertrauenswürdiges Software-Verteilungssystem
- Vertrauenswürdige Updater-Software
- Vertrauenswürdiges Netzwerk
- Vertrauenswürdiges Computer-Image
- Vertrauenswürdige AD-Gruppe
- Vertrauenswürdiges Produkt

Bereitstellungsoptionen

- Microsoft Group Policy (GPO)
- On-Premise-Server
- Software as a Service