BeyondTrust

>>> Praxisorientierte Anwendung von Zero-Trust-Prinzipien beim Privileged Access Management (PAM)

Umsetzung von Zero Trust *mit* Privileged Access Management (PAM)

INHALTSVERZEICHNIS

Einführung: Zero-Trust-Schritte

Zero-Trust-Prinzipien und -Architekturen werden im öffentlichen und privaten Sektor breit angenommen und eingesetzt. Veraltete Sicherheitsarchitekturen und Netzwerksicherheitssysteme sind schlichtweg ineffektiv in einer Welt, die stärker auf Cloud- und Remote-Work-Umgebungen baut. Inzwischen sind Zero-Trust-Prinzipien zu den wirksamsten Ansätzen für den Umgang mit erhöhtem Risiko für hochsensible Identitäten, Assets und Ressourcen geworden.

NIST SP 800-207[1] wird als Zero-Trust-Framework allgemein anerkannt. Das NIST bezeichnet diesen SP als „definitive Quelle für ZTA-Konzepte und -Grundlagen". Diese erste Veröffentlichung (circa August 2020) thematisierte vor allem Zero-Trust-Konzepte auf einer übergeordneten Ebene. Sie diente nicht als Grundlage für die Entwicklung und Implementierung von Zero Trust auf praktischer Ebene.

Zur Zero-Trust-Implementierung in der Praxis müssen Unternehmen verstehen, welche Technologien und Konfigurationen tatsächlich auf der Basis von Grundsätzen implementiert werden können, die den theoretischen Anforderungen entsprechen. Zu diesem Zweck hat das NIST die SP NIST 1800-35[2] zur Implementierung von Zero Trust (circa Dezember 2022) veröffentlicht, damit diese Lücke geschlossen werden kann. Mittlerweile gibt es Lösungen, die sowohl die theoretischen als auch die praktischen Anforderungen von Zero Trust erfüllen können. Hier setzt dieses Whitepaper über Technologien von BeyondTrust an.

Dieses Dokument richtet sich an IT- und Sicherheitsexperten, welche die Prinzipien von Zero Trust gemäß NIST in reale Produktfunktionen für Privileged Access Management (PAM) und sicheren Remote-Zugriff überführen wollen, die Zero Trust in öffentlichen oder privaten Unternehmen ermöglichen.

Keine digitalen Identitäten müssen zwingender geschützt werden als diejenigen, die privilegierten Zugriff auf Systeme, Daten, Anwendungen und andere sensible Ressourcen haben. Nahezu jeder Angriff erfordert inzwischen Privilegien für die erste Schwachstellennutzung oder für Seitwärtsbewegungen innerhalb eines Netzwerks.

PAM schützt privilegierte Konten und Anmeldedaten und erzwingt granular das Least-Privilege-Prinzip. Jede Sitzung mit privilegiertem Zugriff wird überwacht und verwaltet – egal, ob es sich um Personen oder Rechner, Mitarbeiter oder Drittanbieter handelt. **Wie in den NIST-Veröffentlichungen dargelegt ist PAM außerdem entscheidend für eine Zero-Trust-Architektur (ZTA) und die Einhaltung der sieben Zero-Trust-Grundsätze.**

Themen im Whitepaper:

- Wichtige Zero-Trust-Definitionen und -Konzepte gemäß NIST-Vorgaben
- Auswirkungen von Zero Trust auf die Sicherheit
- Praktische Schritte zur Implementierung von Zero Trust mit Privileged Access Management- und Secure Remote Access-Lösungen
- BeyondTrust-Unterstützung für Unternehmen auf dem Weg zu Zero Trust
- Konzeptionelle Überlegungen für Zero-Trust-Architekturen

[1] https://csrc.nist.gov/publications/detail/sp/800-207/final

[2] https://csrc.nist.gov/publications/detail/sp/1800-35/draft

NIST 800-207 und 1800-35B: Definition von Zero Trust und Zero-Trust-Architekturen (ZTA)

Definition von Zero Trust

Das National Institute of Standards and Technology (NIST) definiert Zero Trust (ZT) als „ein sich weiterentwickelnder Satz an Cybersicherheitsparadigmen, die den Schutz von statischen, netzwerkbasierten Perimetern auf Benutzer, IT-Assets und IT-Ressourcen verlagern". Das NIST erklärt weiter, dass die Sammlung an Konzepten auf Basis von Zero-Trust-Grundsätzen dazu vorgesehen sind, „Ungewissheiten bei der Durchsetzung präziser Least-Privilege-Zugriffsentscheidungen pro Anfrage in Informationssystemen und -diensten im Rahmen eines angreifbaren Netzes zu minimieren".

In der Praxis bedeutet das, kein grundsätzliches Vertrauen vorauszusetzen, eine kontinuierliche Authentifizierung durchzuführen und Zugriffe granular auf das erforderliche Minimum zu beschränken sowie Segmentierungs- und Mikrosegmentierungsstrategien anzuwenden und Zugriffe kontinuierlich zu überprüfen. **Privileged Access Management (PAM) ist eine grundlegende Technologieplattform zur Durchsetzung jeder dieser erforderlichen Zero-Trust-Sicherheitskontrollen.**

> *„Die Wechselwirkungen zwischen den Produkten in der Suite [von BeyondTrust] sind so perfekt und durchdacht aufeinander abgestimmt, dass wir unsere Möglichkeiten bei der Durchsetzung von Zero-Trust-Vorgaben maximieren können."*
>
> *Brandon Haberfeld, Globaler Leiter Plattformsicherheit, Investec*

Das Hauptziel von Zero Trust ist der Schutz von Unternehmensressourcen (insbesondere, aber nicht ausschließlich von Daten). Wie in NIST SP 1800-35B beschrieben, ist dieses Ziel infolge der aktuellen Netzwerkherausforderungen zunehmend wichtiger geworden:

- Netzwerke sind zu dezentralen, perimeterlosen Umgebungen geworden, in denen Ressourcen sowohl auf lokale Umgebungen als auch mehrere Clouds verteilt sind.
- Viele Benutzer benötigen überall, jederzeit und von jedem Gerät aus Zugriff, um ihre Aufgaben im Unternehmen bewältigen zu können.
- Daten werden programmgesteuert gespeichert, übertragen und über verschiedene Grenzen unter der Kontrolle unterschiedlicher Organisationen verarbeitet, um den sich stetig weiterentwickelnden Geschäftsszenarien gerecht zu werden.
- Es reicht nicht mehr, einfach nur Zugriffskontrollen am Rand der Unternehmensumgebung durchzusetzen und davon auszugehen, dass alle Systeme innerhalb des Perimeters vertrauenswürdig sind.

Daher kann der Netzwerkstandort nicht mehr als Hauptkomponente für den Sicherheitsstatus einer Ressource dienen. Stattdessen geht das Zero-Trust-Modell davon aus, dass kein IT-Asset oder Benutzerkonto einfach nur auf Grundlage des physischen oder Netzwerkstandorts oder des Asset-Besitzers vorbehaltlos vertraut werden kann. Benutzer und Gerät müssen vor Beginn einer Sitzung auf einer Unternehmensressource authentifiziert und autorisiert werden.

Definition von Zero-Trust-Architekturen

Die NIST-Sonderveröffentlichung (Special Publication: SP) 800-207 definiert eine Zero-Trust-Architektur (ZTA) als „einen Cybersicherheitsplan eines Unternehmens, der Zero-Trust-Konzepte einsetzt und Komponentenbeziehungen, Workflow-Planung und Zugriffsrichtlinien umfasst. Daher bezeichnet ein Zero-Trust-Unternehmen sowohl die Netzwerkinfrastruktur (physisch und virtuell) als auch Betriebsrichtlinien, die als Folge eines Zero-Trust-Architekturplans eingesetzt werden“.

Das NIST beschreibt weiter, dass der primäre Fokus einer ZTA der „Schutz von Daten und Ressourcen ist. Sie ermöglicht einen sicheren, autorisierten Zugriff auf Unternehmensressourcen, die über On-Premise- und Cloud-Umgebungen verteilt sind, so dass hybride Mitarbeiter und Partner orts- und zeitunabhängig von jedem Gerät aus auf Ressourcen zugreifen können, die zur Erfüllung der Geschäftsziele erforderlich sind".

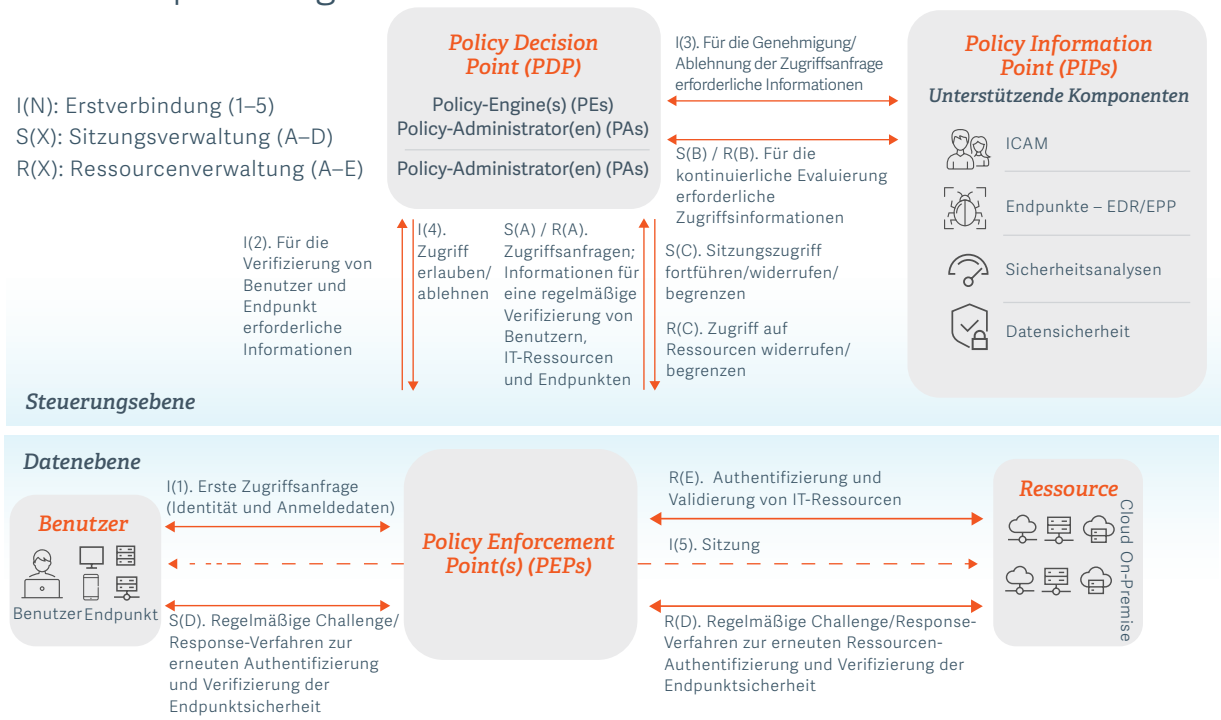
Die Konzepte und Prinzipien einer Zero-Trust-Architektur nach NIST SP 800-207 werden auf „Unternehmensnetzwerke angewendet, die aus vorab festgelegten Geräten und Komponenten bestehen und kritische Unternehmensressourcen sowohl lokal als auch in der Cloud speichern". Gemäß SP 1800-35B führt die ZTA eine kontinuierliche Verhaltensanalyse und risikobasierte Bewertung der Zugriffstransaktionen oder -sitzungen in Echtzeit durch. „Bei jeder Zugriffsanfrage verifiziert die ZTA die Identität und Rolle des anfordernden Benutzers, den Status und die Anmeldedaten des anfordernden Geräts und ggf. noch weitere Daten. Wird die definierte Richtlinie erfüllt, stellt die ZTA dynamisch eine sichere Verbindung her, um alle Daten zu schützen, die zu und von der IT-Ressource übertragen werden."

Jede Zugriffsanfrage wird anhand folgender Prüfungen evaluiert:

- Der zum Zeitpunkt des Zugriffs verfügbare Kontext, einschließlich der Identität und Rolle des Anfragestellers
- Der Status und die Anmeldedaten des anfordernden Geräts
- Die Sensibilität der IT-Ressource

Zero-Trust-Referenzarchitektur

Hier ein Beispiel für eine ZTA gemäß NIST SP 1800-35B, die auf mehrere Sicherheitsdisziplinen angewendet wird:



Die wichtigsten Komponenten einer ZTA im oben aufgeführten Architektur-Diagramm:

- **Policy-Engine (PE):** Die PE übernimmt die endgültige Entscheidung bezüglich Gewährung, Verweigerung oder Widerruf des Zugriffs auf eine IT-Ressource für einen bestimmten Benutzer. Die PE berechnet die Vertrauensbewertungen/Vertrauensstufen und die endgültigen Zugriffsentscheidungen basierend auf den Unternehmensrichtlinien und Informationen von unterstützenden Komponenten. Die PE führt den Vertrauensalgorithmus aus, um jede empfangene Ressourcenanfrage zu evaluieren.
- **Policy-Administrator (PA):** Der PA führt die Richtlinienentscheidung der PE aus, indem er Befehle an den PEP sendet, um den Kommunikationspfad zwischen Benutzer und IT-Ressource aufzubauen und zu beenden. Er generiert alle sitzungsspezifischen Authentifizierungs- und Autorisierungstoken oder Anmeldedaten, die vom betreffenden Benutzer für den Zugriff auf die Unternehmensressource verwendet werden.
- **Policy Enforcement Point (PEP):** Der PEP bewacht die Vertrauenszone, in der eine oder mehrere Unternehmensressourcen gehostet werden. Er sorgt für das Aktivieren, Überwachen und schließlich Beenden von Verbindungen zwischen Benutzern und Unternehmensressourcen. Er arbeitet auf der Grundlage von Befehlen, die von der PA empfangen werden.

Weitere wichtige Definitionen:

- **Policy Decision Point (PDP):** PE und PA bilden zusammen den PDP, der die Entscheidung trifft, ob ein Benutzer Zugriff auf eine Ressource erhält oder nicht.
- **Policy Information Point (PIP):** Der PIP liefert telemetrische und andere Daten, damit der PDP fundierte Zugriffsentscheidungen treffen kann. Dazu zählen PAM, EDR und identitätsbasierte Bedrohungs- und Reaktionslösungen.
- **Benutzer:** Ein Endbenutzer, eine Anwendung oder eine sonstige maschinelle Anwendung, die Informationen von IT-Ressourcen anfordert.
- **Das Gateway:** Für das Aktivieren, Überwachen und Beenden der Verbindung zwischen Benutzer oder Anwendung und der Ressource über den Agenten zuständig, damit sämtliche Aktivitäten beurteilt und dokumentiert werden können.

Zero-Trust-Segmentierung

Als bewährtes Sicherheitsverfahren sollten Netzwerk- und Zugriffskontrollen für herkömmliche On-Premise-Ressourcen konfiguriert, geprüft und überwacht werden, um unbefugte Zugriffe zu verhindern. In vielen modernen Umgebungen wurden diese Sicherheitskontrollen jedoch gelockert oder entfernt, um verschiedenste Anwendungsfälle zu unterstützen – von Hybrid-Cloud-Umgebungen über Remote-Mitarbeiter bis zu Lösungen, die mehrere Standorte und Netzwerke umfassen. Dies bedeutet nicht, dass die Sicherheitskontrollen komplett fehlen, sondern vielmehr, dass Ausnahmen eingerichtet wurden, um zusätzliche geschäftliche Anwendungsfälle zu ermöglichen, und dass die zusätzlichen Risiken hingenommen werden. Diese „Aufweichung“ der Umgebung läuft dem Zero-Trust-Modell zuwider und setzt in vielen Fällen auf statische Anmeldedaten oder Secrets, damit verschiedene Lösungen miteinander interagieren können. So wird mit einem Kompromiss an einem Standort die gesamte Umgebung gefährdet.

Zur Zero-Trust-Umsetzung und gleichzeitigen Unterstützung von neueren Anwendungsfällen muss ein neuer Perimeter eingerichtet werden. Dafür ist ein zonenbasierter Ansatz erforderlich, mit dem eine sichere Umgrenzung geschaffen wird. Der Zugriff auf dessen „Enklave" sowie auf die darin befindlichen IT-Ressourcen sollte stark eingeschränkt werden.

Der umgrenzte Bereich ist vergleichbar mit einem Netzwerkperimeter innerhalb eines ungesicherten Netzwerks, in dem die Eindämmung samt Sicherheitskontrollen integriert ist.

Gateway-Segmentierung

Ein Gateway-Enklavenmodell richtet einen granular segmentierten Perimeter mit IT-Assets ein, auf die nur über einen geschlossenen und überwachten Netzwerkpfad zugegriffen werden kann. Während IT-Ressourcen innerhalb der Enklave über gelockerte Sicherheitskontrollen verfügen können, welche die betrieblichen Geschäftsanforderungen erfüllen, werden sie bei Aktivitäten von außen dennoch auf unangemessenes Verhalten überwacht. Es handelt sich also um ein vertrauenswürdiges Mini-Netzwerk innerhalb eines anderen Netzwerks.

Der Zugriff auf den umgrenzten Bereich erfordert Sicherheitskontrollen, die über einen als Bastion-Host gesicherten Rechner oder eingeschränkte Netzwerktunnel- und Routing-Kontrollen hinausgehen. Für eine Netzwerksegmentierung ist dies entscheidend.

Weitere notwendige Voraussetzungen für die Umsetzung von Zero-Trust-Funktionalität innerhalb einer Enklave:

- Eine externe Ressource setzt die Richtlinie und Verwaltung des gesamten Zugriffs um.
- Der Zugriff wird von einer logischen Engine vermittelt, welche die Richtlinien und Attribute verarbeitet, um Zugriffe zu bestimmen oder einzuschränken.
- Jeder Zugriff wird vollständig dokumentiert – von der Autorisierung bis zur kompletten Sitzungsverwaltung und -aufzeichnung.
- Sessions werden zur Erledigung von Aufgaben auf Verhaltensaktivität überwacht, von Beginn bis zu erforderlichen Seitwärtsbewegungen. Auf unangemessene Aktivitäten kann in Echtzeit reagiert werden.
- Der Zugang ist dabei begrenzt und sollte über Workflows wie Just-in-Time-Zugriff erfolgen, einschließlich zeitbegrenzter Konnektivität und Integration in ITSM- und andere Change-Management-Lösungen.
- Sitzungen oder Datenverbindungen mit der Enklave werden nur über die Steuerungsebene verarbeitet. Mit anderen Worten: Sämtliche lateralen Bewegungen im segmentierten Bereich sollten mithilfe herkömmlicher Netzwerk- und Zugriffskontrollen verhindert werden. Die Enklave sollte wie ein gesichertes Netzwerksegment fungieren, das vollständig abgeschottet ist und keine Hintertüren aufweist.

Der Erfolg dieses Modells basiert auf der richtigen Balance zwischen all diesen Anforderungen. Autorisierte Benutzer und Anwendungen müssen eine Sitzung initiieren, die verifiziert und mit der Gateway-Enklave verbunden werden kann. Sitzungsüberwachung, Credential Injection und Least Privilege müssen angewendet werden, um Sicherheits- und Compliance-Bedenken eines Unternehmens auszuräumen und die Zero-Trust-Ziele erfüllen zu können.

Ressourcen-Segmentierung

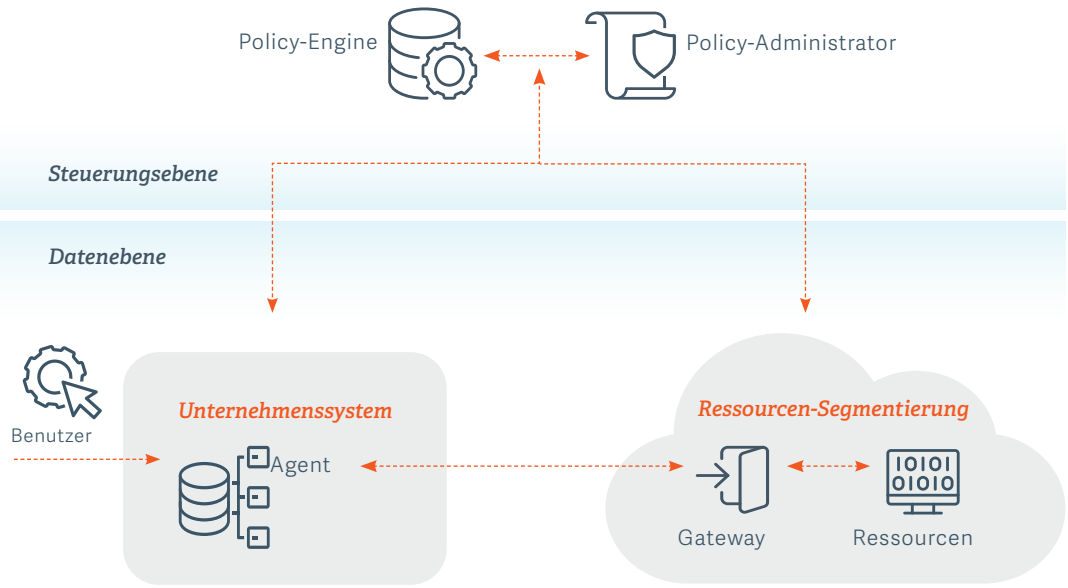
Eine Ressourcen-Enklave ist eine Variation einer Netzwerkzone oder eines VLANs. Es handelt sich um eine Sammlung von IT-Ressourcen (IT-Assets) (Anwendungen, Betriebssysteme, Netzwerkgeräte, Datenbanken usw.) mit einem gehärteten Perimeter zur Abgrenzung. Anstatt eines Perimeters als breiter Netzwerkzone werden kritische IT-Ressourcen innerhalb der Ressourcen-Enklave nur für einen bestimmten Zweck isoliert. Im Prinzip handelt es sich bei einer Ressourcen-Enklave um eine gesicherte Netzwerkzone mit begrenztem externen Zugriff, die vollständig segmentiert ist. Jeder Zugriff muss über ein Gateway erfolgen, wie von der Gateway-Enklave vorgeschrieben. Im Wesentlichen definiert eine Gateway-Enklave den Pfad für einen sicheren Zugriff, und die Ressourcen-Enklave definiert die eingebundenen IT-Ressourcen.

In jeder Organisation gibt es potenziell Dutzende oder Hunderte von Ressourcen-Enklaven, die durch herkömmliche Zugriffskontrolllisten und Netzwerkzugriffshärtung gesichert werden. Hierbei handelt es sich um eine Erweiterung des Mikrosegmentierungskonzepts für einzelne Implementierungen, um geschäftliche oder technologische Anforderungen zu erfüllen. Eine Ressourcen-Enklave kann an Legacy-Systeme angepasst werden, und die Architektur muss mit Zero Trust kompatibel sein – entweder nativ oder unter Verwendung einer Gateway-Enklave.

Daher verlassen sich Ressourcen innerhalb der Enklave auf herkömmliche Modelle zur Sicherheitskontrolle und wehren Bedrohungen (d. h. unangemessene laterale Bewegungen) nicht notwendigerweise innerhalb der Enklave selbst ab, es sei denn, die Konnektivität wird komplett überwacht. So werden zum Beispiel Bedrohungen, die nur von lateralen Bewegungen ausgehen, nur zwischen Benutzern und zwischen den Ressourcen-Enklaven abgewehrt.

Grundsätzlich müssen alle Sitzungen und die Konnektivität erzwingbar sein, egal, ob der Benutzer oder die Anwendung im Büro oder an einem externen Standort aktiv ist. Mit diesem Paradigma kann eine Zero-Trust-Architektur (ZTA) eine wesentliche Rolle bei der Bewältigung der Herausforderungen von Legacy-Netzwerken einnehmen, wenn ein breiter Netzwerk-Perimeter nicht mehr für die Durchsetzung von Sicherheitsmaßnahmen verwendet wird.

Das folgende Diagramm zeigt eine vereinfachte NIST-basierte Zero-Trust-Architektur für eine sichere Gateway-Enklave:



In einer reinen Zero-Trust-Umgebung können das Gateway und die Ressourcen-Enklave auf einem einzelnen IT-Asset vorhanden sein, so dass die Anwendung ordnungsgemäß eingeschränkt ist. Dies ist zwar das Ziel, aber für viele Unternehmen, die Zero Trust zum ersten Mal umsetzen, nicht realistisch. Das Konzept einer Enklave kann je nach IT-Ressource und IT-Asset, die im Rahmen einer Zero-Trust-Initiative implementiert werden, nach oben oder unten skaliert werden.

Privileged Access Management (PAM) ist die Grundlage für Zero Trust

Privileged Access Management (PAM) besteht aus Cybersicherheitsstrategien und -technologien, mit denen Kontrolle über erweiterte („privilegierte“) Zugriffe und Berechtigungen für Benutzer, Konten, Vorgänge und Systeme in einer IT-Umgebung ausgeübt wird. Anwendungsfälle reichen u. a. von der Durchsetzung des Least-Privilege-Prinzips über die Verwaltung privilegierter Konten/Anmeldedaten bis hin zur Sicherung des gesamten privilegierten Remote-Zugriffs. PAM ist eine grundlegende Sicherheitskontrollmaßnahme, die unter das Identitäts- und Zugriffsmanagement (IAM) fällt.

„Die Mehrheit der Systeme innerhalb der Gebäude, auf die zugegriffen wird, sind keine klassischen IT-Systeme. Dabei handelt es sich um Gebäudesteuerungssysteme wie intelligente Aufzüge, Überwachungssysteme und Klimaanlagen, bei denen es nicht möglich ist, Antivirensoftware zu installieren. Wir sind uns bewusst, dass die Verwaltung privilegierter Zugriffe einer der wichtigsten Bestandteile eines modernen Cybersicherheitsprogramms sowie ein Muss für eine Zero-Trust-Architektur und ein robustes BYOD-Sicherheitssystem ist."

Curtis Jack, Leiter Technical Engineering, Oxford Properties Group

Fallstudie lesen

Heutzutage müssen Unternehmen und öffentliche Einrichtungen wesentlich mehr privilegierte Konten sichern und viel mehr Remote-, Hybrid- und dezentralisierte Netzwerke unterstützen als in den vergangenen Jahren – viele davon werden nicht einmal als privilegierte Konten von Administratoren oder Systembesitzern betrachtet.

Wir arbeiten mit mehr Tools, Benutzern und Rechnern, die einen privilegierten Zugriff benötigen, als je zuvor. IT-Ressourcen und privilegierte Konten können in großem Umfang in Cloud-Umgebungen bereitgestellt werden. Allerdings können auch vorübergehend bereitgestellte Ressourcen eine Angriffsfläche bieten und müssen daher durch Sicherheitsmaßnahmen geschützt werden.

IT-Ressourcen, die Authentifizierung, Berechtigungen und Zugriff erfordern, befinden sich zunehmend außerhalb der Corporate Governance. Das kann andere, nicht vertrauenswürdige Ressourcen oder Identitäten, Konten und Prozesse umfassen. An diesem Punkt setzt das Konzept der Datenebene an, und diese gilt es zu verwalten.

Eine Zero-Trust-Architektur (ZTA) adressiert die Herausforderungen moderner Privileged-Access-Sicherheit. Eine ZTA setzt granulare, sichere und autorisierte Zugriffe für Remote-Mitarbeiter und Partner in Nähe der IT-Ressourcen – sei es lokal oder in der Cloud – auf Grundlage der festgelegten Zugriffsrichtlinien einer Organisation durch.

Durch die granulare Umsetzung von Privileged Access Management (PAM) kann Zero Trust sicherstellen, dass jeder Zugriff verwaltet und dokumentiert wird, um angemessenes Verhalten ungeachtet von Größe und Design einer Enklave zu gewährleisten. Aktuell ist dies eine besonders wichtige Herausforderung, die Unternehmen lösen müssen, um gesetzliche Compliance-Anforderungen und Voraussetzungen für Cyberversicherungen erfüllen zu können.

ZTA mit BeyondTrust Privileged Access Management (PAM)

Wie vom NIST (SP 800-207) vorgesehen, vermeidet ein Zero-Trust-Sicherheitsmodell uneingeschränktes Vertrauen und setzt eine kontinuierliche Authentifizierung, das Least-Privilege-Prinzip und adaptive Zugriffskontrollen durch. Diese Strategie umfasst zudem die Segmentierung und Mikrosegmentierung für sicheren Zugriff. Bei einem Zero-Trust-Ansatz geht es um konstante Transparenz und Kontrolle darüber, wer was in Ihrem Netzwerk ausführt. Dies sind alles Kernfunktionen, die moderne Privileged Access Management (PAM)-Lösungen, wie von BeyondTrust, abdecken.

„Die Wechselwirkungen zwischen den Produkten in der Suite [von BeyondTrust] sind so perfekt und durchdacht aufeinander abgestimmt, dass wir unsere Möglichkeiten bei der Durchsetzung von Zero-Trust-Vorgaben maximieren können."

Brandon Haberfeld, Globaler Leiter Plattformsicherheit, Investec

Fallstudie lesen

BeyondTrust Privileged-Access-Management-Lösungen unterstützen die durchdachte, praktische Umsetzung des Zero-Trust-Sicherheitsmodells des NIST – ohne Unterbrechung der Geschäftsprozesse. Unsere Lösungen stellen sicher, dass alle privilegierten Zugriffe und Berechtigungen kontinuierlich überprüft werden und Least-Privilege-Zugriffe auf Just-in-Time-Basis bereitgestellt und sofort nach Abschluss einer Aufgabe, nach Änderung des Kontexts oder nach Ablauf einer bestimmten Zeitspanne widerrufen werden.

Mit BeyondTrust können Sie mit den dringendsten PAM-Anwendungsfällen in Ihrem Unternehmen beginnen und im Laufe der Zeit nahtlos die verbleibenden Anwendungsfälle angehen. Jeder Anwendungsfall bietet nach erfolgreicher Umsetzung eine verbesserte Kontrolle und Verantwortlichkeit über die Konten, IT-Assets, Benutzer, Systeme und Aktivitäten, die Ihre privilegierte IT-Umgebung betreffen, und entschärft zugleich mehrere Bedrohungsvektoren. Darüber hinaus bietet BeyondTrust zentralisierte Sicherheitskontrollen für den privilegierten Zugriff in Ihrer heterogenen Umgebung — On-Premises, Cloud/Multi-Cloud (AWS, Azure usw.), Windows, macOS, Unix, Linux etc. Kein anderer Anbieter bietet eine so tiefgreifende und umfassende Kontrolle über privilegierte Zugriffe.

Je mehr Anwendungsfälle Sie bearbeiten, desto mehr PAM-Synergien entstehen, und desto mehr Unternehmensrisiken können Sie verringern, Betriebsabläufe optimieren und Zero-Trust-Ziele erreichen.

Auf hohem Niveau bietet BeyondTrust PAM die folgenden Funktionen für On-Premise- und Cloud-Umgebungen:

- Erkennung, Integration und Katalogisierung aller privilegierten Identitäten, Konten und IT-Assets.
- Durchsetzung adaptiver Zugriffe und kontinuierliche Authentifizierung, um sicherzustellen, dass alle Geräte, Benutzer und Konten ein hohes Vertrauen in ihre tatsächliche Identität haben. Mit anderen Worten: Über eine positive Authentifizierung hinausgehend sind sie wirklich, wer sie vorgeben zu sein.
- Richtige Dimensionierung für privilegierte Zugriffe und Berechtigungen durch Anwendung des Least-Privilege-Prinzips, einschließlich Just-in-Time-Zugriff, auf alle Sitzungen, Endpunkte und Anwendungen.
- Sicherer Remote-Zugriff auf Sitzungen und vertrauenswürdige Anwendungen nach dem Least-Privilege-Prinzip für Anbieter, Mitarbeiter und Servicedesks.
- Segmentierung und Mikrosegmentierung zur Isolierung von IT-Assets und Benutzern sowie zur Vermeidung von lateralen Bewegungen.

- Überwachung und Verwaltung jeder privilegierten Sitzung für kontinuierliche Transparenz und Kontrolle darüber, wer was und warum tut, sodass verdächtiges Verhalten zum sofortigen Entzug von Berechtigungen und Zugriffen führt.
- Erweiterung der Microsoft® Active Directory-Authentifizierung, Single Sign-On-Funktionen und des Gruppenrichtlinien-Konfigurationsmanagements für Unix- und Linux-Systeme sowie vereinfachte und sichere Verwaltung von Identitäten und unternehmensweite Zero-Trust-Implementierung unabhängig von Betriebssystem oder Anwendung.

Tabelle: Wie BeyondTrust PAM in die NIST-Zero-Trust-Architektur passt

		NIST-Kernkonzepte für ZTA			
		Policy-Engine (PE)	**Policy-Administrator (PA)**	**Policy Enforcement Point (PEP)**	**Gateway**
BeyondTrust-Lösungen	**Password Safe**	Verwaltungsfunktionen für das Secrets-Management sowie rollen- und attributbasierte Zugriffsmodelle, die vom Policy-Administrator definiert werden. Die Policy-Engine von BeyondTrust Password Safe entscheidet anhand einer Vielzahl von Kriterien über die Verfügbarkeit des Zugriffs und zeichnet einen privilegierten Zugriff selbst dann auf, wenn er vorübergehend ist.	Erstellung, Aktualisierung und Verwaltung der Richtlinie für Endbenutzer und maschinelle Identitäten, um Zugriff zu gewähren und eine privilegierte Sitzung zu automatisieren. Der Zugriff auf die Ressourcen-Enklave wird dem Policy-Administrator gewährt und kann über die BeyondInsight-Konsole von BeyondTrust verwaltet werden.		Gateway-Implementierung: 1. Eine BeyondTrust-Appliance als Worker-Knoten bei der lokalen Installation von Password Safe, unabhängig davon, ob ein Internetzugang vorhanden ist. 2. Ein Resource Broker bei der Verwendung von Password Safe für die On-Premise-Verwaltung von IT-Assets (bevorzugt). Das Gateway antwortet auf eine privilegierte Zugriffsanforderung für eine Sitzung oder Anwendung über eine vertrauenswürdige Policy-Engine. Dies ist für Zero Trust ausschlaggebend, da einem Benutzer niemals direkter Zugriff auf eine Ressource gewährt wird, wie das bei der Verwendung eines nativen Betriebssystemprotokolls der Fall ist. Die gesamte Konnektivität wird vom Agenten verwaltet und überwacht, und lediglich die Sitzungsaktivität (Bildschirm, Terminal oder Webseite) wird für den anfordernden Benutzer bereitgestellt.

	NIST-Kernkonzepte für ZTA			
	Policy-Engine (PE)	**Policy-Administrator (PA)**	**Policy Enforcement Point (PEP)**	**Gateway**
Privileged Remote Access	Verwaltungsfunktionen für den Remote-Zugriff sowie rollen- und attributbasierte Zugriffsmodelle, die vom Policy-Administrator definiert werden. BeyondTrust Secure Remote Access kann IT-Assets und Benutzer unabhängig vom Perimeter in jeder Netzwerkzone verwalten, solange ein Internetzugang verfügbar ist.	Erstellung, Aktualisierung und Verwaltung der Richtlinie für Endbenutzer, um Zugriff zu gewähren und den Remote-Zugriff auf Anwendungen zu automatisieren. Das ist die Grundlage für Zero Trust. Der Zugriff auf die IT-Ressource oder Anwendung wird dem Policy-Administrator gewährt und kann über die Secure-Remote-Access-Konsole von BeyondTrust verwaltet werden.	Implementierung über Secure Remote Access Jump Client. Er reagiert auf Remote-Access-Anfragen für eine Sitzung oder Anwendung über eine vertrauenswürdige Policy-Engine oder einen Zwischenproxy, also Jump Point. Einem Benutzer wird niemals direkter Zugriff auf eine Ressource gewährt, wie das bei der Nutzung eines nativen Betriebssystem-Protokolls der Fall ist. Die gesamte Konnektivität wird verwaltet und überwacht, und lediglich die Sitzungsaktivität (Bildschirm, Terminal oder Webseite) wird für den anfordernden Benutzer bereitgestellt.	
Privilege Management für Windows/Mac und Unix/Linux	Verwaltungsfunktionen für die Regeln, Richtlinien und Protokoll-Engine für den Least-Privilege-Endpunktzugriff sowie die rollen- und attributbasierte Zugriffsmodelle, die vom Policy-Administrator definiert werden.	Der Web-Policy-Administrator erstellt, aktualisiert und verwaltet die Richtlinie für Endbenutzer, gewährt Zugriff und automatisiert den Zugriff auf Anwendungen. Das ist die Grundlage für Zero Trust. Der Zugriff auf die IT-Ressource oder Anwendung wird dem Policy-Administrator gewährt und kann über die Windows- und Mac-Schnittstelle von BeyondTrust Privilege Management (bei Bereitstellung über die Cloud) verwaltet werden.	Der Policy Enforcement Point ist der auf Windows-, macOS-, Unix- und Linux-Endpunkten installierte Least-Privilege-Client. Bei Windows und macOS initiiert er privilegierte Anwendungen und führt die Anwendungssteuerung für den Benutzer oder die Anwendung auf den Endpunkten durch. Der Policy Enforcement Point vergleicht die Anwendungsausführungsanfrage anhand definierter Richtlinien und startet (oder verweigert) die Anwendung mit den entsprechenden Privilegien, ohne privilegierte Anmeldedaten zu verwenden. Diese Funktion ist für Zero Trust von grundlegender Bedeutung, da Anwendungen oder Benutzer niemals Administratorrechte erhalten, sondern eine Anwendung nur mit den erforderlichen Berechtigungen ausgeführt wird. Unter Unix/Linux werden Befehle auf dem Host für den Benutzer oder die Anwendung initiiert — ohne dass sich der Endbenutzer tatsächlich anmeldet – und gibt die Ergebnisse für den Endbenutzer transparent wieder.	

Privileged Password Management

Die digitale Transformation führt zu einer Ausweitung von privilegierten Konten und Zugriffen

Unternehmen verzeichnen eine explosionsartige Zunahme privilegierter Konten (Benutzer, Anwendungen, Rechner usw.), die verwaltet werden müssen.
Diese privilegierten Konten unterstützen On-Premises-Technologien, die Cloud, Hybrid-Umgebungen und viele der SaaS-, IaaS- und PaaS-Lösungen, mit denen ein modernes Unternehmen arbeitet.

Privilegierte Anmeldedaten und andere Secrets müssen mithilfe eines Modells verwaltet werden, das moderne Umgebungen unterstützt. Der Zugriff auf Passwörter und Secrets erfolgt über digitale Identitäten (menschlich und maschinell), ob lokal oder in der Cloud oder von einem Anbieter, Lieferanten oder Lösungsanbieter lizenziert.

Sicherer, adaptiver privilegierter Zugriff und Überwachung mit Privileged Password Management

Privileged Password Management (oder auch Privileged Account and Session Management) bietet einen optimalen Weg, den Zugriff auf vertrauliche IT-Ressourcen zu gestalten und an aktuelle Herausforderungen anzupassen. Die Umsetzung umfasst, wie bereits beschrieben, ein Zero-Trust-Modell mit Gateway-Enklaven.

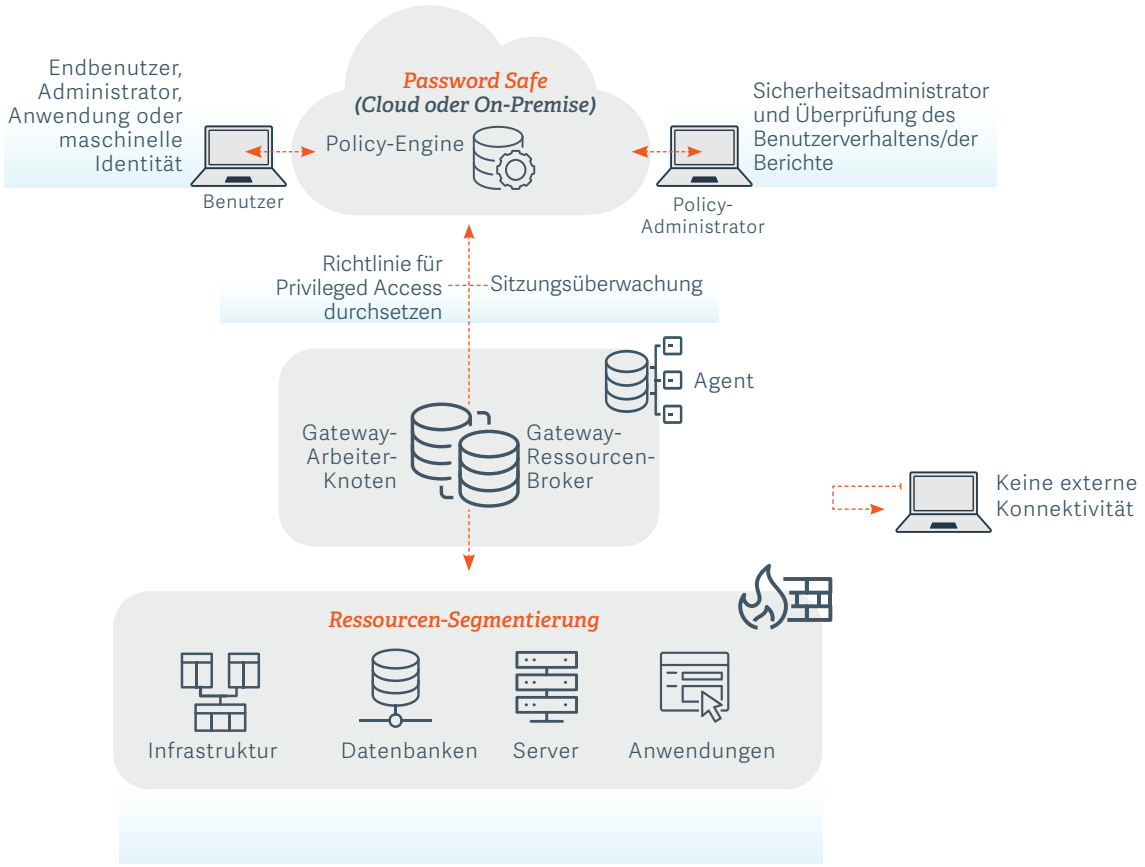
Die BeyondTrust-Lösung für privilegiertes Passwort-Management, Password Safe, stellt sicher, dass Ihre IT-Ressourcen verwaltet und vor potenziell unangemessenen Verbindungsaktivitäten geschützt sowie alle in einer Enklave enthaltenen IT-Ressourcen im Rahmen eines Zero-Trust-Modells ausgeführt werden. Das bedeutet, dass Endbenutzer oder maschinelle Identitäten niemals privilegierte Direktsitzungen aufbauen können, sondern der Zugang nur über ein Gateway vermittelt wird. Alle Sitzungsaktivitäten werden vollständig überwacht. Das gilt unabhängig vom Perimeter für jeden Standort, an dem sich eine Ressourcen-Enklave befindet.

Die wichtigsten Zero-Trust-Anwendungsfälle mit Password Safe:

- Sicheres Speichern und Abrufen von Passwörtern, Anmeldedaten und anderen Secrets für den Zugriff auf menschliche und maschinelle Identitäten.
- Automatisches Rotieren von Passwörtern auf Basis von Workflows, Zeitplänen und bedarfsgesteuerter Verwendung der IT-Ressourcen sowie Bereitstellung einer funktionsreichen API zur weiteren Automatisierung.
- Bereitstellung eines Verlaufsdatensatzes für Passwörter und Secrets beim Zugriff auf Backups, Momentaufnahmen virtueller Maschinen und Disaster-Recovery-Umgebungen.
- Vollständiges Session-Management, einschließlich Überwachung, Aufzeichnung, Wiedergabe und Analyse von Sitzungen sowohl in Echtzeit als auch chronologisch für Compliance-Audits, Forensik und Schulungszwecke.
- Zugriffsfreigabe ausschließlich über sichere Gateway-Technologie, um laterale Bewegungen zu verhindern oder zu überwachen, Brokerzugriff über vertrauliche Komponenten zu ermöglichen und eine geeignete Zugriffsrichtlinie aufzulisten und durchzusetzen.
- Privilegierte Passwort-Management-Architektur für bestehende Umgebungen mit minimaler Verteilung.

Auf Basis der in diesem Whitepaper beschriebenen Konzeption können sämtliche Anwendungsfälle von BeyondTrust Password Safe über Least-Privilege- und Just-in-Time-Zugriff erfolgen, inklusive Integration in ITSM-Lösungen und Bereitstellung in einer Zero-Trust-Enklave mit den damit verbundenen Vorteilen bei IT-Verwaltung und Zugriffssteuerung.

Password-Safe-Architektur für ein segmentiertes Zero-Trust-Modell



Im obigen Diagramm ist das Unternehmenssystem die Password Safe-Konsole oder die REST API zur Unterstützung der Automatisierung und maschinellen Konten. Beachtenswert ist auch, dass die Rolle des Agenten eng mit der Richtlinien-Engine verknüpft ist. Sein Zweck besteht darin, Kennwörter oder Secrets vom verschlüsselten Passworttresor an die Benutzer weiterzugeben sowie Kontrollen und Rotationen bei den verwalteten IT-Ressourcen durchzuführen. Dazu gehören der Zugriff auf bisherige Passwörter und Secrets sowie Entscheidungen der Policy-Engine, einschließlich der Zugriffsdauer.

Bei einem softwaredefinierten Perimeter kann schon eine partielle Implementierung dieses Modells das privilegierte Passwort-Management verbessern. Diese IT-Architektur ist wesentlich sicherer als ein unbeschränkter Zugriff auf IT-Ressourcen von überall aus mit statischen Anmeldedaten; insbesondere bei Ein-Faktor-Authentifizierung von Passwörtern oder Secrets und Wiederverwendung in veralteten Lösungen.

Secure Remote Access

Eine moderne Arbeitsumgebung birgt jede Menge Risiken bei Remote-Zugriffen

Als bewährtes Sicherheitsverfahren sollten native Fernzugriffsprotokolle der vom Unternehmen ausgegebenen Computergeräte deaktiviert werden. Leider findet diese Sicherheitsmaßnahme in vielen Umgebungen (insbesondere bei Benutzern, die im Homeoffice arbeiten) keine Anwendung, und Remote-Geräte könnten über unzureichend gesicherte Remote-Zugriffspfade auf Unternehmensressourcen zugreifen.

Die Gründe zur Aktivierung von Protokollen wie RDP, SSH und VNC sind seit längerem ein Konfliktpunkt zwischen den Teams für Informationstechnologie und Informationssicherheit. Zum einen gibt es einen Bedarf an kostengünstiger Remote-Access-Technologie, die vom Betriebssystem nativ unterstützt wird. Das wird im Regelfall von der IT aufgrund fehlender Sicherheitserfahrung oder aufgrund von Budgetbeschränkungen befürwortet. Sicherheits- und Compliance-Teams sehen hingegen die damit verbundenen Schwachstellen, wurmfähige Exploits und das Fehlen von Audits und sicherem Netzwerk-Routing nativer Protokolle.

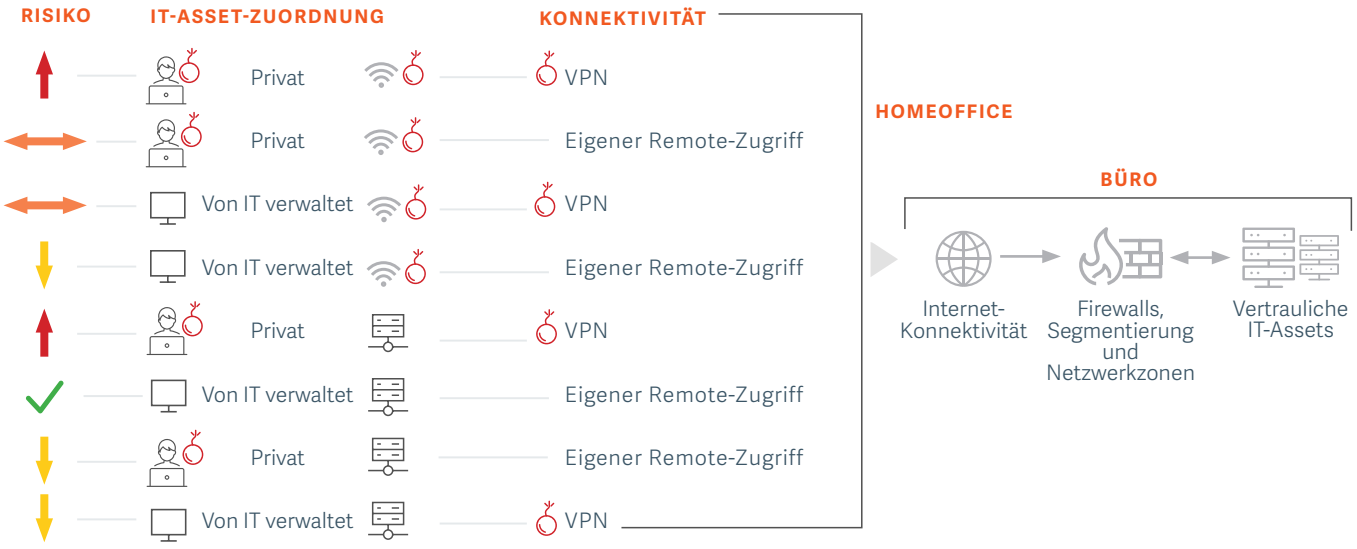
Beide Ansätze müssen ausbalanciert werden. Autorisierte Benutzer müssen auf jedem Gerät, überall und protokollunabhängig eine sichere Remote-Access-Sitzung initiieren. Darüber hinaus müssen die Sitzungsüberwachung, Credential Injection sowie Least Privilege angewendet werden, um die Sicherheits- und Compliance-Bedenken eines Unternehmens auszuräumen. Diese Funktionen müssen vorhanden sein, egal, ob der Mitarbeiter im Büro oder an einem Remote-Standort arbeitet. Dies gilt insbesondere dann, wenn die Remote-Sitzung lediglich eine Anwendung und keine Terminal-basierte Remote-Session unterstützt.

Wie kann ein Benutzer eine Anwendung ohne VPN (Virtual Private Network) verwenden und die Grundsätze von Zero Trust erfüllen? Secure Remote Access mit Zero-Trust-Umsetzung kann dieses Problem für Anwendungen lösen und auch herkömmliche Herausforderungen beim Protokoll-Routing überwinden.

Wie eine Zero-Trust-Architektur Protokoll-Herausforderungen bei nativem Remote-Zugriff überwinden kann

Eine ZTA kann bei der Überwindung von Protokoll-Herausforderungen bei nativem Remote-Zugriff eine wesentliche Rolle spielen. Eine Zero-Trust-Implementierung beim Remote-Zugriff kann in nahezu jeder Umgebung eingesetzt werden und einen Just-in-Time-Workflow (JIT) mit Zero Standing Privileges (ZSP) ermöglichen, was bedeutet, dass es keine Konten mit ständig aktivierten Berechtigungen gibt.

Das folgende Diagramm veranschaulicht die Risiken, die sich aus Remote-Arbeit in einer dezentralen, perimeterlosen Umgebung ergeben, und spiegelt die Kombination aus IT-Assets, Konnektivität, Fernzugriffstechnologie und den Hauptstandorten wider, an denen ein Bedrohungsakteur eine Umgebung infiltrieren kann.
Darüber hinaus können Anwendungen basierend auf normaler Konnektivität extern oder mit einer Remote-Sitzung arbeiten. Zum Schutz sämtlicher Aktivitäten muss die Konnektivität selbst gesichert werden und der gesamte Zugriff nur über eine sichere Remote-Access-Technologie erfolgen.



In der obigen Grafik stellt jede „Bedrohung“ ein Risiko dar:

- Drei Bedrohungen: Nicht hinnehmbares, kritisches Risiko
- Zwei Bedrohungen: Mittleres Niveau eines hinnehmbaren Risikos
- Eine Bedrohung: Geringes Risiko für Remote-Zugriff
- Keine Bedrohungen: Bestes Szenario für akzeptable Remote-Konnektivität

Die Verwendung eines privaten Geräts mit einem vom Unternehmen ausgegebenen VPN-Client stellt immer ein kritisches Risiko dar, unabhängig davon, ob es sich um eine kabelgebundene oder drahtlose Verbindung handelt. Das liegt daran, dass private Geräte nicht verwaltet werden und das Unternehmen keine Kontrolle darüber hat, wie sie verwendet, aktualisiert oder betrieben werden – auch was die Installation anderer Software oder Malware betrifft.

In dezentralen Umgebungen gibt es folgende Bedrohungen beim Zugriff auf vertrauliche, interne IT-Ressourcen:

1. Private oder BYOD-Hardware (Bring Your Own Device), die nicht verwaltet, nicht aktualisiert und von mehreren Benutzern verwendet wird oder das Ende ihrer Lebensdauer erreicht hat und anderweitig anfällig für Phishing oder Malware ist. Darüber hinaus sind BYOD-Benutzer in der Regel selbst lokale Administratoren, was das Risiko noch erhöht.

2. Unsichere Heimnetzwerke, die auf einer WLAN-Konnektivität basieren und bei denen die Verbindung potenziell unsicher oder das Passwort schwach ist, sind aufgrund einer gemeinsamen SSID oder unzureichender Verschlüsselung offen für Man-in-the-Middle-Angriffe. Außerdem können andere Geräte das drahtlose Netzwerk kompromittieren oder die Kommunikation überwachen. Dazu zählen privilegierte Konten außerhalb der Corporate Governance in Heimnetzwerken, die auf einfache SaaS-Lösungen zugreifen.

3. VPN-Technologie, die in der Regel Split-Tunneling verwendet und niemals auf privaten Geräten installiert werden sollte, könnte die Kommunikation kompromittieren und über Schwachstellen im Heimnetzwerk Seitwärtsbewegungen im Unternehmensnetz begünstigen. VPN-Technologie, die nur auf Netzwerkebene ausgeführt wird, kann Remote-Sitzungen oder -Anwendungen nicht überwachen. Und in der Regel benötigen Remote-Benutzer lediglich Zugriff auf Anwendungen (Anwendungsebene) für ein bestimmtes Programm oder eine Sitzung.

Behebung von Remote-Zugriff-Risiken mit Zero Trust

Bedrohungen können mit einer Kombination aus Zero Trust, IT-verwalteten Geräten, IT-Governance und Privileged Access Management behoben werden, wenn herkömmliche Technologien allein zu einem nicht hinnehmbaren Risiko führen könnten.

- **Von der IT verwaltet** – IT-verwaltete Sicherheitskontrollen zur Risikobewertung, einschließlich Kerndisziplinen für das Schwachstellen- und Patch-Management.
- **Konnektivität** – Minimierung von Netzwerkrisiken mit einer kabelgebundenen Verbindung anstelle unbekannter drahtloser Konnektivität.
- **Privileged Access Management** – Remote-Access-Sitzungen werden rollenbezogen auf der Anwendungsebene initiiert, wobei eine Verschleierung der Anmeldedaten erfolgt. Dadurch entfällt die Notwendigkeit von Datenverkehr auf der Netzwerkebene pro Anwendung und Benutzer. Die Erhöhung von Berechtigungen wird lokal und im gesamten Netzwerk streng kontrolliert, wobei auch lokale Admin-Zugangsdaten und Administratorrechte für Endbenutzer entfallen.
- **IT-Governance** – Dokumentation aller privilegierten Aktivitäten zur Einhaltung von IT-Compliance-Vorgaben, einschließlich des Benutzerverhaltens von Benutzern beim Remote-Zugriff.
- **Zero Trust** – Durch die Implementierung einer Cloud-basierten Verwaltungsarchitektur für alle Fernzugriffssitzungen wird Zero Trust und eine strenge Anwendungskontrolle durchgesetzt. Damit wird das Zero-Trust-Konzept sowie das Least-Privilege-Prinzip auf alle Sitzungen angewendet, unabhängig von ihrem Ursprung oder Ziel. Auf diese Weise können Risiken vollständig gemindert werden, indem niemals Root- oder Administratorrechte außerhalb des erweiterten Perimeters oder für den Endbenutzer offengelegt werden.

Diese Kombination aus Technologien und Strategien funktioniert, weil nicht nur das Quellgerät geschützt, sondern auch Netzwerkrisiken minimiert werden – durch:

- Verwendung einer Kabelverbindung
- Strenge Kontrolle von Remote-Zugriffen
- Kein Protokoll-Routing wie SSH
- Aufzeichnung aller Sitzungsaktivitäten zur Compliance- und Verhaltensanalyse

Und durch die Anwendung des Zero-Trust-Konzepts mit Least Privilege wird sichergestellt, dass die Risiken vollständig gemindert werden können, indem niemals Root- oder Administratorrechte außerhalb des Perimeters offengelegt werden. Mit VPNs ist das ohne Privilege-Management-Lösungen nicht möglich.

Erweiterung von PAM- und Zero-Trust-Kontrollen über den Perimeter hinaus mit BeyondTrust Privileged Remote Access

VPNs können Risiken innerhalb eines definierten Perimeters oder einer Enklave nicht effektiv verwalten. Damit Zero Trust funktioniert, müssen Netzwerk und Umgebung vor der Implementierung einer ZTA gesichert werden.

BeyondTrust Privileged Remote Access ist für die Verwaltung von Sitzungen konzipiert und kann – nach einigen Grundüberlegungen – mit einem Zero-Trust-Modell implementiert werden. Die Lösung erweitert Best-Practice-Empfehlungen für Privileged Access Management über den Perimeter hinaus.
Privileged Remote Access ermöglicht Unternehmen die Anwendung von Least Privilege und effizienten Audit-Kontrollen bei sämtlichen Remote-Zugriffen, die von Mitarbeitern, Anbietern und Servicedesks ausgehen. Benutzer können schnell und sicher auf jedes Remote-System zugreifen, das auf einer beliebigen Plattform und an jedem beliebigen Standort läuft sowie den integrierten Passworttresor nutzen, um privilegierte Anmeldedaten zu erfassen, einzubinden und zu verwalten. BeyondTrust Privileged Remote Access bietet granulare Least-Privilege-Kontrolle, die mit VPNs und vielen anderen gängigen Remote-Access-Technologien nicht realisierbar ist.

Für den Fall, dass native Protokolle oder native Tools gewünscht werden, bietet BeyondTrust auch Infrastruktur-Zugriffsmanagement-Funktionen über die Privileged-Remote-Access-Lösung. Diese Fähigkeit kombiniert native Workflows, Zero-Trust-Prinzipien (wie JIT und ZSP) und einen umfassenden Audit-Pfad.

Für Techniker, wie Entwickler und Cloud-Ops-Ingenieure, ist die Verwendung von VPNs ein notwendiges Übel (und manchmal sind mehrere VPNs in unterschiedlichen Umgebungen erforderlich). Zwar sind VPNs verschlüsselt und allgemein sicher, aber sie bieten einen breiteren Zugriff, als normalerweise benötigt wird. Aus Workflow-Perspektive muss der Benutzer daran denken, welches VPN für jedes spezifische Gerät verwendet werden soll, und er muss auch die Anmeldedaten für das jeweilige System kennen.

Mit Privileged Remote Access kann der Benutzer eine einzige Konsole und native Tools (z. B. SQL, SSH und RDP) nutzen, Anmeldedaten aus einem sicheren Passworttresor einfügen und für jede Sitzung einen vollständigen (und konsolidierten) Audit-Pfad generieren. Diese Methodik bietet den Benutzern den gewünschten Workflow für die Verwaltung der gesamten Infrastruktur und gibt dem Unternehmen die nötige Sicherheit bei Audits.

Die wichtigsten Privileged-Remote-Access-Anwendungsfälle für Zero Trust:

- Anwendung des Least-Privilege-Prinzips und robuste Audit-Kontrollen bei allen Fernzugriffen durch Mitarbeiter, Drittanbieter, Auftragnehmer und Servicedesk-Mitarbeiter.
- IT-Verwaltung und automatische Einbindung von Anmeldeinformationen in Remote-Sitzungen und -Anwendungen, die Endbenutzer nicht einsehen können, um sie angemessen nutzen zu können (Integration mit BeyondTrust Password Safe für eine noch umfassendere Verwaltung privilegierter Anmeldedaten).
- Sicherung des Infrastrukturzugangs – Implementierung eines sicheren Jump-Servers mit Multi-Faktor-Authentifizierung, adaptiver Autorisierung und Sitzungsüberwachung für Administratorkonsolen. Dies gilt auch für Zugriffe über vertrauenswürdige Netzwerkzonen hinweg.

- Zugriff auf Webseiten wie das Azure- oder Microsoft-365-Portal durch einen gesicherten und eingebetteten Chromium-Browser.
- Einhaltung von Grenzen zwischen Entwicklungs-, Test- und Produktionssystemen für bewährte SecDevOps-Verfahren.
- Mikrosegmentierung auf Anwendungsebene, die Benutzer daran hindert, Anwendungen und andere Ressourcen auszuführen, für die sie nicht autorisiert sind.

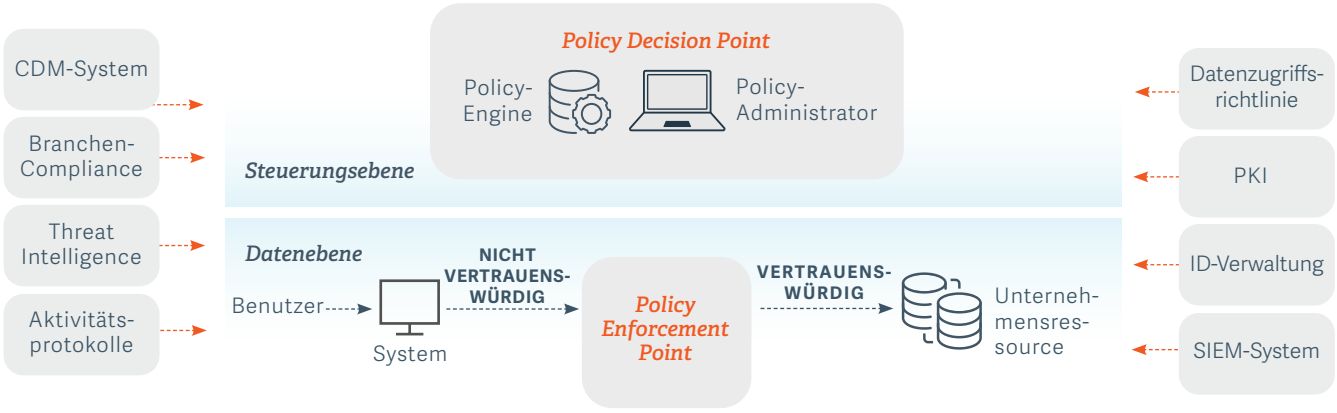
Privileged Remote Access bietet gegenüber VPN folgende Vorteile.

So schneiden die Funktionen von BeyondTrust Privileged Remote Access im Vergleich zu einem typischen VPN ab:

VPNs und BeyondTrust Privileged Remote Access im Vergleich

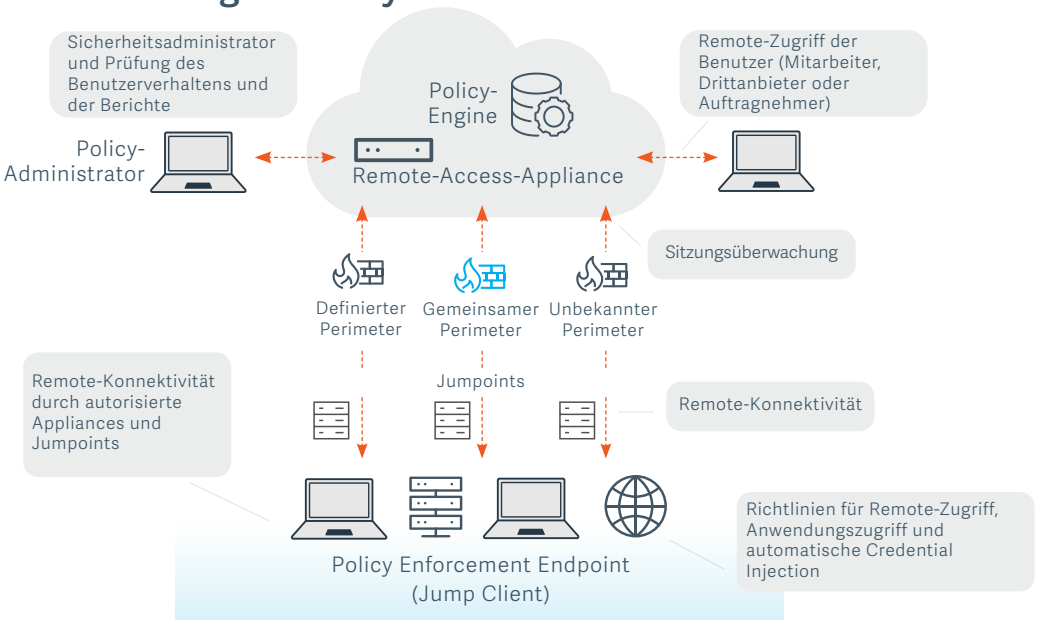
FUNKTION	VPN	BeyondTrust
Remote-Zugriff	●	●
Sichere Konnektivität	●	●
Zugriff auf der Netzwerkschicht (Protokoll-Tunneling)	●	●
Verschlüsselter Datenverkehr	●	●
Virtualisierung der Anwendungsschicht		●
Remote Desktop		●
RDP-Zugriff per Proxy		●
VNC-Zugriff per Proxy		●
SSH-Zugriff per Proxy		●
Überwachung von Anwendungssitzungen		●
Aufzeichnung von Anwendungssitzungen		●
Just-in-Time-Zugriff		●
Zero-Trust-Architektur		●
Privileged-Access-Management-Integration (PAM-Integration)		●
Sichere BYOT		●
ITSM-Integration		●
Passwortverwaltung und Speicherung von Anmeldedaten		●
Cloud- oder On-Premise-Bereitstellung (physische oder virtuelle Appliance)		●
Zugriff ohne Agent		●
Umfassende Unterstützung gängiger Betriebssysteme und Plattformen		●
Verhinderung von Seitwärtsbewegungen im Netzwerk		●
Audit-Trail und Sitzungsberichte		●

Das folgende Diagramm zeigt eine vereinfachte NIST-basierte Zero-Trust-Architektur für Remote-Zugriff:



Auf der Grundlage dieses Konzepts sollten alle Remote-Sitzungen das Least-Privilege-Prinzip und Just-in-Time-Zugriff befolgen, in ITSM-Lösungen integrierbar sein und einer Zero-Trust-Architektur für Richtlinien und Verwaltung folgen, um bewährte Sicherheitsverfahren einzuhalten.

Das folgende Diagramm zeigt, wie dies in alltäglichen Abläufen mit der Privileged-Remote-Access-Technologie von BeyondTrust und Zero Trust funktioniert:



Kein direkter Zugriff auf IT-Assets durch Remote-Benutzer.
Durchsetzung von Zero-Trust-Richtlinien durch Policy-Engine, Netzwerk-Routing und dedizierte Remote-Access-Clients.

Bei einem softwaredefinierten Perimeter kann schon eine partielle Implementierung dieses Modells die IT-Sicherheit verbessern. Diese Architektur bietet wesentlich mehr Sicherheit, als einem Heimcomputer mit VPN-Zugriff in Ihrer Umgebung zu erlauben, Administrationsfunktionen auszuführen.

Endpoint Privilege Management

Windows- und macOS-Benutzer haben zu weit gefasste Zugriffsprivilegien

Für nahezu alle Unternehmen ist die einfachste Möglichkeit, die Kontrolle über ihre Windows- und macOS-Endgeräte zu übernehmen, das Least-Privilege-Prinzip zu implementieren und Endbenutzern die dauerhaften lokalen Administratorrechte zu entziehen. Leider setzen viele Unternehmen diese so wichtige Sicherheitsmaßnahme nicht vollständig um und sind daher anfällig für Cyberangriffe jeglicher Art.

Zur erfolgreichen Implementierung des Least-Privilege-Prinzips müssen Organisationen eine Lösung finden, die folgende Ziele miteinander verbindet:

- **Produktivität:** Für viele der Aufgaben, die Endbenutzer im Alltag erledigen müssen, sind Administratorrechte erforderlich, wie beispielsweise für das Installieren von Anwendungen oder Ändern von Systemeinstellungen. Werden die Administratorrechte ohne eine passende Enterprise-Lösung entzogen, kann die Produktivität stark beeinträchtigt werden.
- **Sicherheit:** Das Unternehmen muss sämtliche lokalen Administratorrechte entfernen und vorgeben, welche Anwendungen von verschiedenen Endbenutzergruppen installiert oder ausgeführt werden können, und einschränken, welche Aufgaben Endbenutzer auf ihren Endpunkten ausführen können, um die Angriffsfläche zu reduzieren.

Diese Ziele unterstreichen die Bedeutung einer Zero-Trust-Architektur für das Endpoint Privilege Management, insbesondere mit Blick auf flexible moderne Arbeitsumgebungen. Mit der richtigen Endpoint-Privilege-Management-Lösung als Teil einer Zero-Trust-Architektur können Büro- und Homeoffice-Umgebungen berücksichtigt und die Lücke zwischen der Verwaltung von Privilegien und von Anwendungen geschlossen werden – bei gleichzeitig strenger IT-Governance über die Authentifizierung.

Aufbau einer ZTA mit BeyondTrust Privilege Management für Windows & Mac

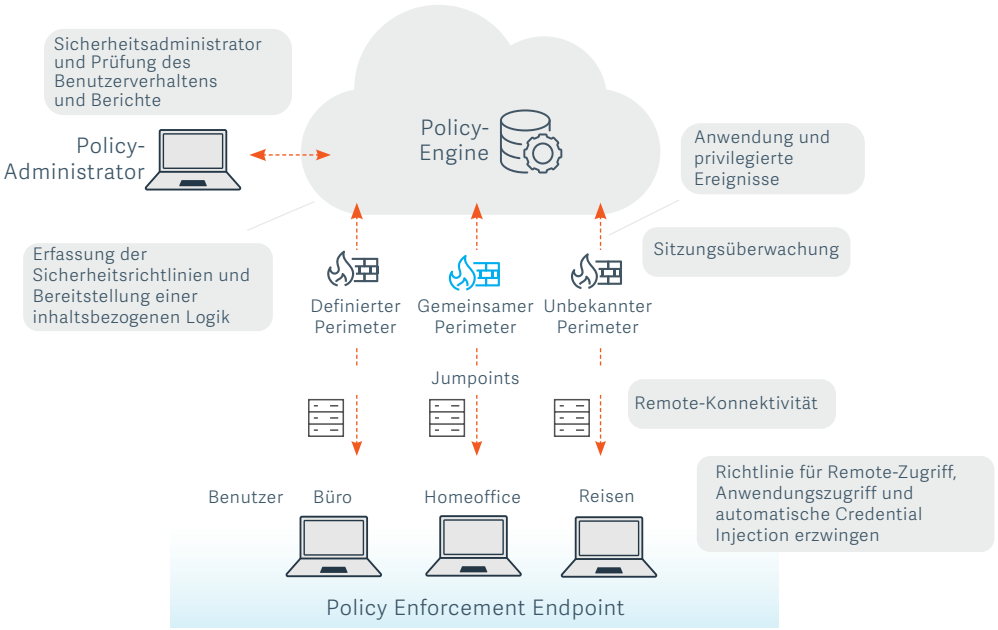
BeyondTrust **Privilege Management für Windows & Mac** erfüllt beide Ziele, die eine erfolgreiche Endpoint-Privilege-Management-Lösung abdecken muss.
Die Lösung hebt zu weit gefasste Administratorrechte auf und wendet eine moderne Anwendungskontrolle an, während die Rechte der Endbenutzer dynamisch erhöht und genau zum richtigen Zeitpunkt zugeführt werden, ohne die Produktivität einzuschränken.

Privilege Management für Windows & Mac bietet folgende Anwendungsfälle für Zero Trust:

- Zero-Trust-Sicherheit durch Entfernen nicht notwendiger Administratorrechte und dauerhafter Privilegien.
- Anwendung einer granularen Anwendungskontrolle und Durchsetzung der geringsten Privilegien für Anwendungen, Webbrowser, IT-Systeme und andere IT-Ressourcen, indem Benutzern der erforderliche Zugriff zum richtigen Zeitpunkt gewährt wird.
- Abwehr von Angriffen, die vertrauenswürdige Anwendungen wie Office, Adobe oder Webbrowser ausnutzen, indem sie integrierte, kontextbasierte Sicherheitsmaßnahmen anwenden.
- Drastische Reduzierung der Cyberangriffsfläche und Schutz vor Malware, Ransomware und Phishing-Angriffen.
- Bereitstellung eines einzigen Prüfpfads für alle Benutzeraktivitäten mit Grafik-Dashboards und Reporting.

Zusammen bilden Privilege Management für Windows & Mac, Privilege Management für Unix & Linux (im folgenden Abschnitt behandelt) und **Active Directory Bridge** die Endpoint-Privilege-Management-Lösung von BeyondTrust. Die Lösung kombiniert Least-Privilege-Management und Anwendungskontrolle, um die Angriffsfläche für Endpunkte zu minimieren und unerwünschte Seitwärtsbewegungen in Ihrer gesamten heterogenen Umgebung zu verhindern.

Beachten Sie dieses Diagramm zu Privilege Management für Windows & Mac gemäß NIST-ZTA:



Keine lokalen oder vertrauenswürdigen Remote-Verwaltungsprivilegien für Benutzer. Anwendungen werden für erhöhte Rechte als vertrauenswürdig eingestuft oder geblockt.

Eine Neugestaltung, eine erneute Bereitstellung oder eine Modernisierung Ihres Endpunkt-Sicherheitsmodells können Sie mit dem Zero-Trust-Modell, dem Least-Privilege-Prinzip und der Applikationskontrolle erreichen. Dieses Modell erfüllt alle NIST-Zero-Trust-Anforderungen und ermöglicht bei der Endpunkt-Privilegienverwaltung auch die Implementierung von zusätzlichen Sicherheitsmodellen, wie z. B. Just-in-Time-Zugriff.

In dieser IT-Architektur befindet sich die gesamte Enklave auf dem Endpunkt und stellt damit den idealen Zustand für eine Zero-Trust-Architektur und -Segmentierung dar.

Privilegien-Risiken unter Unix und Linux gefährden vertrauliche Daten und IT-Assets

Unix- und Linux-Administratoren nutzen selten, oder gar nicht, die Tastatur direkt hinter ihrem IT-Asset – falls überhaupt eine angeschlossen ist. Das ist bei Arbeiten in der Cloud fast immer der Fall.

Administrator- oder sogar Root-Zugriff wird Einzelpersonen gewährt. Diese Person verwendet Remote-Access-Technologien und Protokolle wie SSH zur Erfüllung einer Aufgabe. Erfolgt die Verwaltung in Unix und Linux in erster Linie aus der Ferne, stellt sich die Frage, auf welchem Weg die Remote-Verwaltung erfolgt. Arbeiten Benutzer lokal innerhalb eines vertrauenswürdigen Netzwerks oder wählen sie sich per Remote-Zugriff vom Homeoffice oder vom Sofa aus ein? Wenn man bedenkt, dass jede Fernzugriffssitzung eine Privileged-Remote-Access-Verbindung ist, da der Zugriff von jemandem aus der Ferne gewährt wird, dann sind Tastatur und Maus nicht einmal in der Nähe des Rechners.

Heutzutage erweitern unsichere Netzwerke von Benutzern, die von zu Hause aus arbeiten – oder von einem beliebigen Standort aus – unsere IT-Perimeter. Infolgedessen gibt es neue Angriffsvektoren und potenzielle Probleme bei der Einhaltung von Vorschriften, die es zu lösen gilt. Für die Unix- und Linux-Administration ist das ein inakzeptables Risiko, da die sensibelsten Daten und Anwendungen eines Unternehmens sich in der Regel auf diesen geschäftskritischen Plattformen befinden.

Alle Verbindungen hängen von sicheren Anmeldedaten ab, die dem Least-Privilege-Modell, Just-in-Time-Zugriff und Einmalauthentifizierung folgen (sollten).

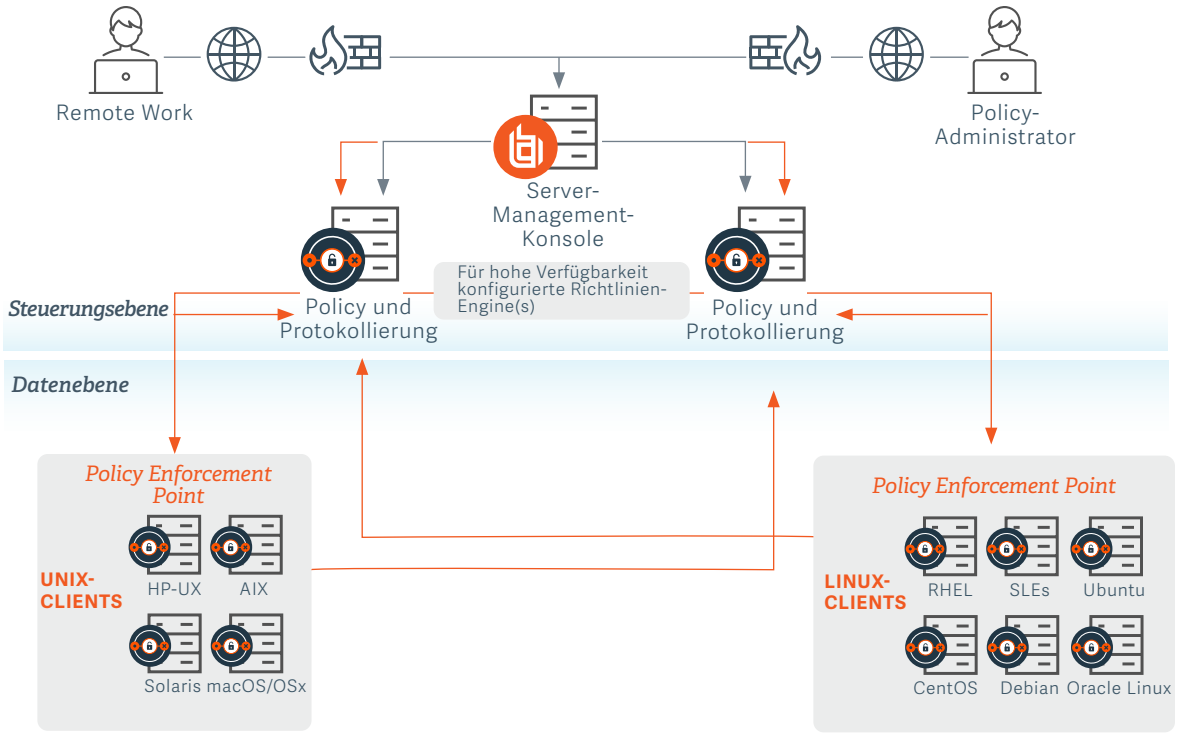
Aktivierung einer ZTA für Ihren Serverbestand mit BeyondTrust Privilege Management für Unix & Linux

BeyondTrust Privilege Management für Unix & Linux ermöglicht Unternehmen die granulare Kontrolle privilegierter Zugriffe, die Einhaltung von IT-Compliance-Anforderungen und die Reduzierung von Cyberrisiken. Die Lösung wendet Faktoren wie Uhrzeit, Datum, Standort und Schwachstellenstatus von Anwendungen oder IT-Assets an, um eine fundiertere Entscheidungsfindung bezüglich der Heraufsetzung von Privilegien zu ermöglichen. Die Lösung erweitert die Möglichkeiten weit über sudo hinaus – mit zentraler Administration, Sitzungsüberwachung und -verwaltung, Überwachung der Dateiintegrität und leistungsstarker Produktivitätssteigerung.

Privilege Management für Unix & Linux bietet folgende Anwendungsfälle für Zero Trust:

- Entfernen von Administratorrechten und Durchsetzung des Least-Privilege-Prinzips auf allen Unix-/Linux-Endpunkten.
- Benutzern wird das sichere Ausführen bestimmter Befehle und Sitzungen aus der Ferne ermöglicht – ohne Anmeldung als Administrator oder Root-Benutzer.
- Annäherung an einen ZSP-Zustand (Zero Standing Privilege) durch dynamisches Just-in-Time-Heraufsetzen von Berechtigungen für Prozesse oder Anwendungen, aber nicht für Endbenutzer.
- Erzwungene Trennung von Aufgaben und Privilegien, um mit einem Konto oder Prozess verbundene Berechtigungen einzuschränken.

Beachten Sie dieses Diagramm zu Privilege Management für Unix & Linux gemäß NIST-ZTA:



Durchgängige Zero-Trust-Sicherheitsmaßnahmen unter Windows, Unix und Linux mit AD Bridging

BeyondTrust Active Directory (AD) Bridge ist Teil der Endpoint-Privilege-Management-Lösung und unterstützt und vereinfacht die Zero-Trust-Strategie bei Unix-/Linux-Geräten. Zugleich hilft sie Unternehmen, gesetzliche Vorschriften einzuhalten.

BeyondTrust AD Bridge bietet zentrale Authentifizierung in Unix- und Linux-Umgebungen, indem die Kerberos-Authentifizierung von Microsoft Active Directory sowie Single Sign-On erweitert werden. Benutzer nutzen ihre AD-Anmeldedaten für den nahtlosen Zugriff auf Unix- und Linux-Systeme.

Unternehmen können für durchgängige Richtlinien und Kontrollen im gesamten Unternehmen sorgen, indem sie die nativen Gruppenrichtlinien-Verwaltungstools um Einstellungen für Unix und Linux erweitern und Benutzer von Desktops auf Remote-Geräte oder zwischen Systemen umleiten, ohne dass eine erneute Eingabe der Anmeldedaten erforderlich ist. Die Nutzung von Microsoft-Gruppenrichtlinien auf anderen Plattformen als Windows ermöglicht außerdem eine zentrale Konfigurationsverwaltung, wodurch das Risiko und die Komplexität der Verwaltung einer heterogenen Umgebung reduziert werden.

In der Vergangenheit war es für Sicherheitsadministratoren schwierig, NIST und andere Richtlinien im gesamten Unternehmen zu konvertieren, anzuwenden, durchzusetzen und zu überprüfen. Mit AD Bridge lassen sich die NIST-Einstellungen automatisch zuordnen und auf die Rechner anwenden – unabhängig davon, ob sie sich vor Ort oder in der Cloud befinden. NIST-Einstellungen lassen sich mithilfe von Active-Directory-GPOs (Gruppenrichtlinienobjekten) erzwingen. Wenn also versucht wird, diese Einstellungen zu ändern – selbst von root – werden sie sofort erneut angewendet und eine Warnung wird generiert, die auf einen Richtlinienverstoß hinweist. Diese Warnung kann an Ihr SIEM weitergeleitet werden, z. B. an Elasticsearch, das standardmäßig in AD Bridge integriert ist.

Privilege Management für AD Bridge bietet folgende Anwendungsfälle für Zero Trust:

- Bereitstellung eines einzigen, vertrauten Toolsets zur Verwaltung von Windows- und Unix-/Linux-Systemen.
- Zentrales Management von Gruppenrichtlinien.
- Bereitstellung präziser Audit-Detailinformationen für Audit- und Compliance-Teams.
- Erweiterung von Single Sign-On (SSO) und Filesharing-Funktionen sowie Zugriffskontrolle auf Nicht-Windows-Systeme.

Überlegungen zum Zero-Trust-Design

Technische Altlasten und Legacy-Systeme

Legacy-Anwendungen, -Infrastrukturen und -Betriebssysteme sind sicherlich nicht Zero-Trust-geeignet. Sie verfolgen kein Least-Privilege-Konzept, erschweren die Anwendungskontrolle und haben keine Modelle für die Ausweitung von Rechten oder Authentifizierung, die dynamische Änderungen auf Grundlage der kontextabhängigen Nutzung zulassen. Sie haben weder ein Konzept für Remote-Mitarbeiter noch für moderne Netzwerkarchitekturen – geschweige denn für die Cloud. Sie sind auf direkte Netzwerkkonnektivität angewiesen, und es fehlen ihnen Funktionen zur Überwachung von Sitzungen oder lateralen Bewegungen. Ihre Sicherheit ist höchstwahrscheinlich stark netzwerkabhängig.

Die Umgestaltung, Neukodierung und erneute Bereitstellung interner Anwendungen ist mitunter teuer und könnte zu Betriebsunterbrechungen führen. Nur eine ernsthafte geschäftliche Notwendigkeit kann derartige Maßnahmen rechtfertigen. Vorhandene Anwendungen mit Sicherheitskontrollen zu versehen, um sie Zero-Trust-geeignet zu machen, ist nicht immer möglich. Wahrscheinlich sieht die Spezifikation Ihrer vorhandenen Anwendungen keine Möglichkeit für solche Verbindungsmodelle vor, und ihr Code eignet sich nicht für den Betrieb in einem Ressourcen-Enklaven-Modell gemäß NIST.

Erwägen Sie je nach Architektur Ihrer eigenen oder bisherigen Drittanwendung deshalb Folgendes:

- Zero Trust und privilegierte Passwortverwaltung als Mechanismus für jede verwaltete Sitzung, bei der die Konnektivität überwacht und verwaltet werden sollte.
- Zero Trust mit Endpoint Privilege Management als Mechanismus für die Heraufsetzung der Privilegien von Remote-Mitarbeitern, Least Privilege und Anwendungskontrolle.

- Zero Trust mit Privileged Access Management als Mechanismus für die Authentifizierung von Remote-Mitarbeitern, Least Privilege und Sitzungsüberwachung.
- Zero Trust mit Secure Remote Access als Mechanismus für die Konnektivität von Remote-Mitarbeitern.

Dieser Ansatz ermöglicht die Implementierung von Zero-Trust-Kontrollen und die Stärkung Ihrer Sicherheitslage ohne vorhandene Systeme umschreiben zu müssen.

Jede Zero-Trust-Implementierung erfordert mehrere Ebenen oder einen Wrapper-Ansatz für die Nutzung von Altsystemen. Ein reiner Zero-Trust-Ansatz muss jedoch alle IT-Ressourcen – ungeachtet von deren Standort – im Rahmen dieser Konzepte umfassen. Alternativen:

- Protokollierung von Remote-Sitzungsaktivitäten, Aufzeichnung interaktiver Bildschirmsitzungen und Überwachung der Ereignisse, um potenziell schädliches Verhalten zu erkennen. Hierbei handelt es sich um eine teilweise Implementierung von Zero Trust mit Secure Remote Access, die zur Minderung von Risiken in bestimmten Umgebungen ausreichen könnte. Dies ist eine wichtige Überlegung, wenn eine einzelne Remote-Sitzung im Hintergrund mit mehreren Systemen interagieren kann, die nicht verwaltet werden, und somit einen hohen Wert für Bedrohungsakteure darstellen.
- Protokollierung privilegierter Aktivitäten, Erfassung von Prozessstarts und Überwachung der Ereignisse, um potenziell böswilliges Verhalten aufzudecken. Hierbei handelt es sich um eine teilweise Implementierung von Zero Trust mit Privileged Access Management, die zur Minderung von Risiken bei Remote-Anwendungen in bestimmten Umgebungen ausreichen könnte.
- Protokollierung von Bildschirmaktivitäten, Erfassung von Prozessstarts, Aufzeichnung von Tastenanschlägen und Überwachung der Protokolle, um potenziell böswilliges Verhalten aufzudecken. Hierbei handelt es sich um eine teilweise Implementierung von Zero Trust mit Privileged Access Management. In Verbindung mit gut definierten Zugriffskontrolllisten reicht die Implementierung aus, um die Risiken des Remote-Zugriffs auf Ihre Unix- und Linux-Ressourcen von praktisch jedem Standort aus verwalten, überwachen und mindern zu können.

Peer-to-Peer-Technologien

Wenn Sie der Meinung sind, Ihr Unternehmen verwendet keine Peer-to-Peer-Netzwerktechnologie (P2P), sind Sie womöglich nicht mit den Standardeinstellungen in Windows 10 vertraut. Seit 2015 nutzt Windows 10 eine Peer-to-Peer-Technologie für die Weitergabe von Windows-Updates unter Peer-Systemen, um Internet-Bandbreite zu sparen. Manche Unternehmen deaktivieren diese Funktion – andere wiederum wissen gar nicht, dass sie existiert.

Dadurch entsteht ein Risiko für privilegierte Seitwärtsbewegungen zwischen Systemen. Obwohl für diese Funktion keine kritischen Schwachstellen oder Angriffe aufgetreten sind, stellt sie eine Kommunikation dar, die dem Zero-Trust-Modell genauso zuwiderläuft wie ein E-Mail-Server, der mit jedem E-Mail-Client des Endbenutzers kommunizieren muss. Es sollten keine unautorisierten seitlichen Bewegungen möglich sein – nicht einmal innerhalb eines spezifizierten Mikroperimeters.

Arbeiten Remote-Mitarbeiter zudem mit Protokollen wie ZigBee oder anderen Mesh-Netzwerktechnologien für IoT, werden Sie feststellen, dass ihre Funktionsweise nicht mit Zero Trust kompatibel ist. Sie erfordern Peer-to-Peer-Kommunikation, aber das Vertrauensmodell basiert ausschließlich auf Schlüsseln oder Passwörtern ohne dynamische Modelle für Authentifizierungsmodifikationen.

Erwägen Sie also folgende Punkte:

1. Es ist nicht praktikabel, eine Ressourcen-Enklave für die gesamte Installation zu errichten. Ressourcen-Enklaven sollten klar definiert und so klein wie möglich sein. Sie erfordern Peer-to-Peer-Kommunikation, aber das Vertrauensmodell basiert ausschließlich auf Schlüsseln oder Passwörtern ohne dynamische Modelle für die Authentifizierung beim Gateway-Zugriff. Sie können mit einem privilegierten Passwort-Manager verwaltet werden, jedoch nicht in einer Zero-Trust-Architektur.

Wenn Sie sich also für Zero Trust und Privileged Password Management entscheiden, sollten Sie in Erwägung ziehen, Ihre Ressourcen so zu härten, dass ein Enklaven-Modell möglich ist und unangemessene Netzwerkkommunikation innerhalb dieser definierten Enklave unterbunden wird.

Auch wenn es Ausnahmen für die Kommunikation innerhalb der Enklave gibt, endet der Perimeter konzeptionell bei der Sammlung von Ressourcen. Externer Zugriff sollte durch Privileged Password Management über ein Gateway erfolgen.

2. Wenn Sie sich also für Zero Trust und Privileged Access Management entscheiden, sollten Sie in Erwägung ziehen, Ihr Endpunkt-Sicherheitsmodell so zu härten, dass unangemessene Netzwerkkommunikation innerhalb des gleichen Subnetzes, in dem sich die Quelle oder das Ziel befinden, unterbunden wird. Es mag Ausnahmen für Geräte wie lokale Drucker geben, aber der Perimeter endet konzeptionell bei den Geräten selbst, die durch Anwendungen und Privilegien definiert werden, und der Remote-Zugriff steuert nur die Verbindung von Punkt zu Punkt.

3. Prüfen Sie, ob Ihre Unix- und Linux-Umgebung ähnliche Technologien einsetzt, über P2P verfügt oder Mesh-Netzwerktechnologien aktiviert hat – auch für die Richtlinien- oder Netzwerkverwaltung. Dies wäre ein großes Hindernis bei der Einführung eines vertrauenswürdigen Remote-Zugriffsparameters, da es immer in irgendeiner Form zu lateralen Bewegungen kommen wird.

Zusammenarbeit mit BeyondTrust bei Ihrem Zero-Trust-Projekt

Organisationen aus dem öffentlichen und privaten Sektor arbeiten weltweit mit BeyondTrust zusammen, um Zero-Trust-Sicherheitsgrundsätze und -architekturen zu implementieren.

Zusätzliche Ressourcen

FALLSTUDIE Umsetzung von Zero Trust am Beispiel von Investec: Von der Theorie zur Praxis

FALLSTUDIE Wie die Oxford Properties Group mit BeyondTrust eine Zero-Trust-Architektur erstellte

WHITEPAPER Mapping BeyondTrust Capabilities to NIST Zero Trust (SP 800-207)
Dieses Whitepaper befasst sich im Detail mit den sieben Grundsätzen von Zero Trust und zeigt auf, wie BeyondTrust Sie dabei unterstützen kann, ihr Unternehmen an diesen Grundsätzen auszurichten. In der Fallstudie werden die BeyondTrust-PAM-Anwendungsfälle den Zero-Trust-Grundsätzen detailliert zugeordnet.

Wenn Sie Ihr Zero-Trust-Projekt mit BeyondTrust besprechen möchten, können Sie sich gerne an uns wenden.

Über BeyondTrust

Die BeyondTrust-Plattform

ÜBER BEYONDTRUST

BeyondTrust ist globaler Marktführer für intelligenten Identitäts- und Zugriffsschutz und ermöglicht Organisationen digitale Identitäten zu schützen, Bedrohungen aufzuhalten sowie sicheren Fernzugriff auf IT-Ressourcen für das ortsunabhängige Arbeiten von überall auf der Welt bereitzustellen. Das integrierte Produkt- und Plattformangebot stellt die branchenweit fortschrittlichste PAM-Lösung (Privileged Access Management) bereit, mit der Unternehmen ihre Angriffsfläche in traditionellen, Cloud- und Hybrid-Umgebungen reduzieren.

BeyondTrust-Lösungen basieren auf kontinuierlichen Innovationen und lassen sich einfach implementieren, verwalten und skalieren. Mit einem globalen Partnernetzwerk unterstützt BeyondTrust über 20.000 Kunden, zu denen 75 Prozent der Fortune-100-Unternehmen zählen. Weitere Informationen unter **beyondtrust.com/de.**