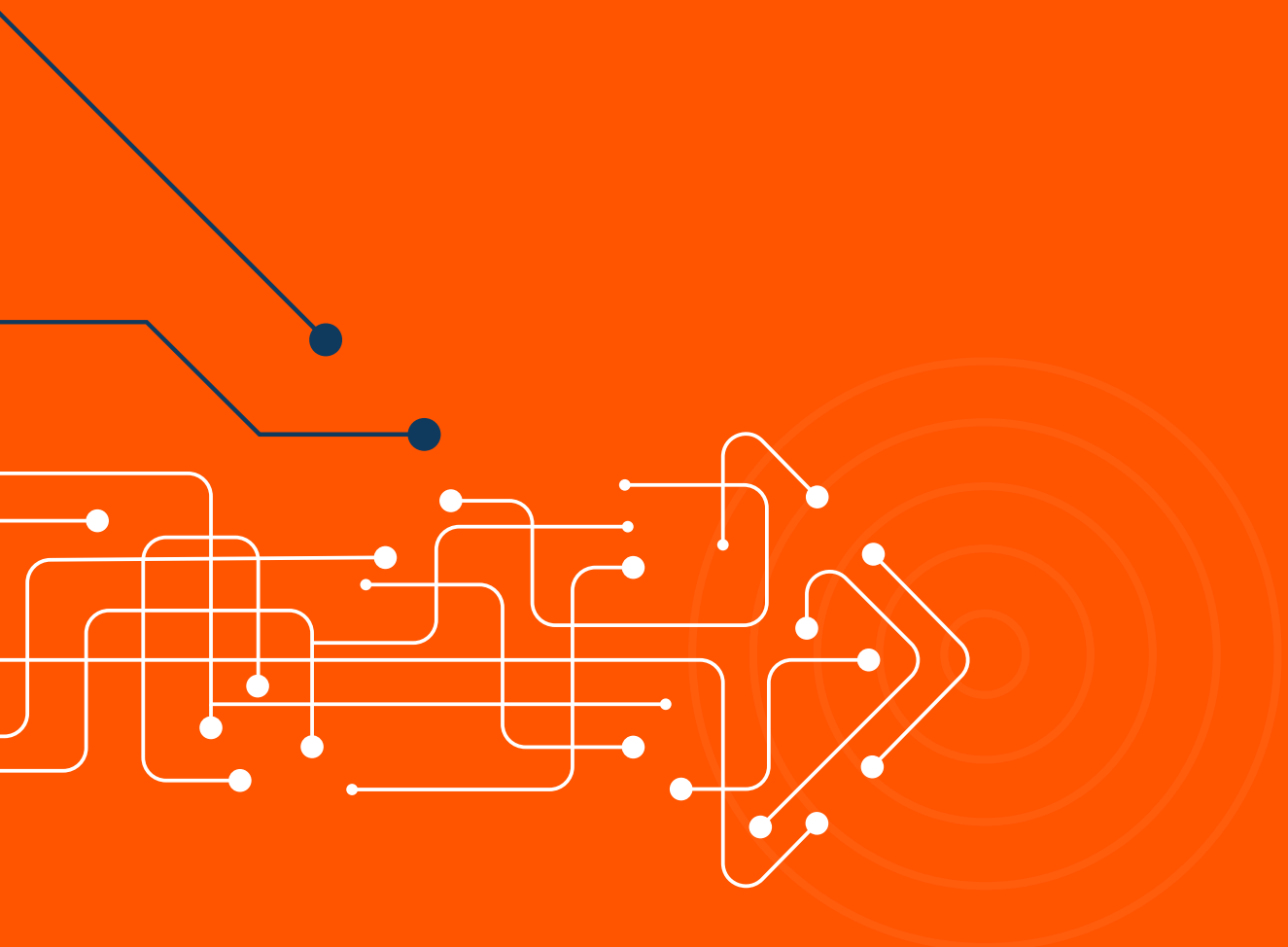
BeyondTrust

Comparing Microsoft Entra PIM vs. BeyondTrust

How Entra Privileged Identity Management (PIM) Compares to BeyondTrust's Multi-Domain PIM & Identity Security Solution



BeyondTrust

TABLE OF CONTENTS

Introduction

Security teams who seek to meaningfully reduce their organization's attack surface by better controlling identities and privileged access are faced with an increasingly complex and decentralized IT infrastructure. Any decision on which tool, or tools, are best fit to tackle this problem must be balanced by the ever-expanding scope of privileged accounts, permissions, and entitlements to be managed.

Organizations with multiple cloud providers and numerous cloud services must contend with the varied and complex permissions models each service brings. And it's not just about managing direct entitlements or privileges, but also escalation pathways that can lead to unintended elevated access. Such paths could be hidden or indirect and work across federated identity sources, yet provide a route to privilege that must be identified and addressed.

The scale of managing an exploding universe of privileges, permissions, and entitlements requires an integrated approach that spans many domains, instead of relying on a stack of niche tools, each only helping to manage a slice of the privilege problem.

In most cases, native toolsets (offered by the Microsoft ecosystem, Google Cloud, AWS, Oracle, etc.) only deliver basic controls and incremental amounts of risk reduction around privileged access and identity security problems. These native toolsets (e.g., Microsoft Entra PIM) are not designed to fully and adequately solve the core problems inherent to unmanaged privileged access and permissions sprawl. They only address a small slice of the problem itself and are typically only available within their own technologies, providing no, or immature, coverage across the rest of an organization's direct privileges and privileged pathways.

This guide reviews and compares the capabilities of Microsoft Entra Privileged Identity Management (PIM) to BeyondTrust, which is recognized as a Leader by the top industry analysts across multiple essential identity security disciplines, including:

- Privileged Identity Management (PIM)
- Privileged Access Management (PAM)
- Cloud Infrastructure Entitlement Management (CIEM)
- Identity Threat Detection and Response (ITDR)

Entra Privileged Identity Management (PIM)

Entra PIM is a feature within Microsoft's Entra ID cloud directory services. It adds enhanced control and auditing in front of Entra ID's more sensitive roles and resources, as well as other Azure and Entra components, such as Microsoft 365.

As part of Microsoft's Premium P2 or EMS E5 licenses, customers can enable the optional features of Privileged Identity Management for Entra ID services. The PIM tool is designed primarily to work within the Microsoft cloud ecosystem, such as Entra ID and Azure services.

With Entra PIM, direct or standing access to your more sensitive Entra roles can be restricted, and time-based or approval-based workflows may be implemented. Users may request access to roles, such as the Global Administrator role, and be granted approval for a configurable period of time, after which the privilege is removed.

All requests and approvals are logged, and access reviews can be conducted to better identify who requires access to certain roles based on their activity over a time period. In this model, Microsoft contends that Entra PIM replaces the traditional network security perimeter of access to privileged roles with the identity layer.

From Microsoft's documentation, the Entra PIM tool has the following primary use cases:

- Provide just-in-time (JIT) privileged access to Entra and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multifactor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need their existing roles
- Download audit history for an internal or external audit
- Prevent removal of the last active Global Administrator and Privileged Role Administrator role assignments

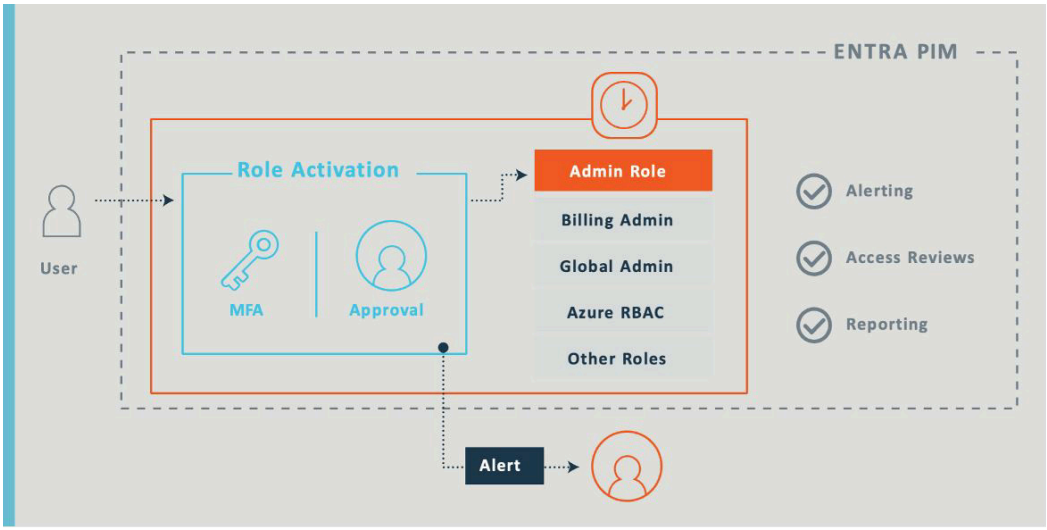


Figure 1: Entra PIM in a simple flow diagram; at the time a user needs to step up their access within Entra ID to an eligible role, they must follow MFA and gain approval. They're then given either short- or long-term access.

BeyondTrust PIM / PAM

BeyondTrust provides the world's most holistic and intelligent identity security visibility, and pairs it with the leading privileged access management (PAM) / PIM controls to mitigate identity-based risks and stop attacks. Core to our approach is a focus on True Privilege™, which encompasses all the entitlements and escalation pathways of an identity.

Read on to gain a clear understanding of how BeyondTrust takes PIM capabilities far beyond that of Entra PIM to help you enable critical identity security and business use cases across every domain—not just Microsoft environments.

Entitle

BeyondTrust Entitle offers a stronger, more adaptable, scalable, and broad-based alternative to Entra PIM. This BeyondTrust solution empowers customers to break down silos that exist between cloud providers by implementing user-friendly, JIT access for a much wider range of cloud, SaaS, and on-prem resources—not just Microsoft. Entitle not only provides PIM and Cloud Infrastructure Entitlement Management (CIEM) capabilities, but also removes limitations by enabling integrations to other critical resources, wherever they might reside (See Entitle integrations).

Entitle delivers on the core tenets of Entra's PIM offering, namely enabling customers to move towards a 'zero' or 'low' standing-privilege model, whereby privileges are requested only when needed and when appropriate, and are revoked automatically. This eliminates instances of persistent access, significantly reducing the attack surface and threat windows.

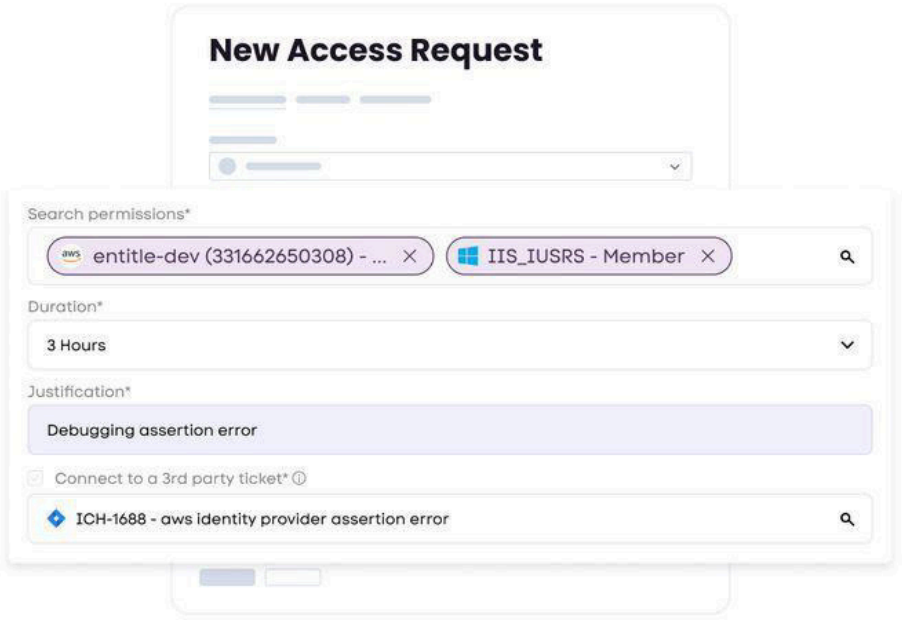


Figure 2: BeyondTrust Entitle enables teams to accept / deny access requests granularly and set access durations.

BeyondTrust Entitle extends these capabilities outside the confines of Microsoft, into other cloud providers, as well as many on-premises resources and SaaS platforms. Until recently, Microsoft offered its own CIEM solution, known as Entra Permissions Management, to extend to other cloud providers as well. But notably, this was a **separate** offering from PIM and reached End of Life (EoL) at the end of October 2025. While Defender for Cloud fills some of the use case gaps left by this solution's EoL, there is no full replacement announced as of this time.

Entitle offers both the capabilities of Entra PIM and Permissions Management, through a single layer.

Customers of Entitle receive both benefits: comprehensive JIT access flows for multicloud and on-premises resources as well as CIEM capabilities.

User-friendliness is also a key focus for the Entitle solution. We ensure that solution administrators, as well as users, find the solution **easy to adopt** by integrating where users do work, such as directly within Teams or Slack, or via our own, simplified Web UI:

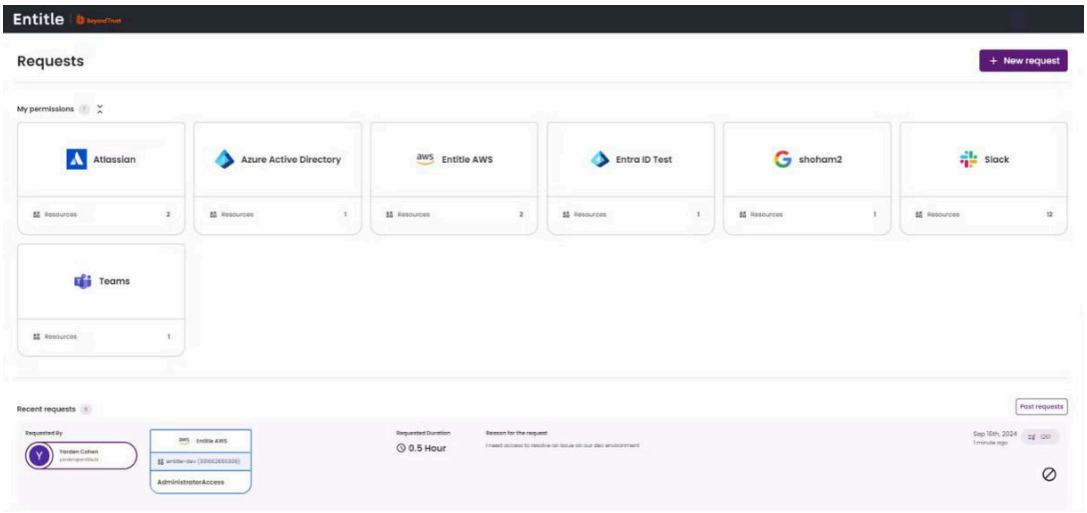


Figure 3: Entitle's interface, which displays access requests from across domains in a single dashboard.

We recognize that the world of cloud entitlements and permissions often make it a challenge for IT / Security teams to even understand which exact permissions are required for certain tasks. This is why Entitle puts a focus on 'bundling' or friendly-naming resources to ensure users are swiftly able to jump from point A to B in their search. This approach minimizes mouse clicks when privileges across multiple resources are required at the same time (e.g., a developer requiring access to workloads in AWS / Azure and repositories in GitHub, data in Datadog, etc.).

With Entitle, you can easily enforce temporary and policy-based permissions to cloud resources. It also supports regulatory compliance with frameworks such as SOX, HIPAA, and PCI-DSS by maintaining audit controls and access governance.

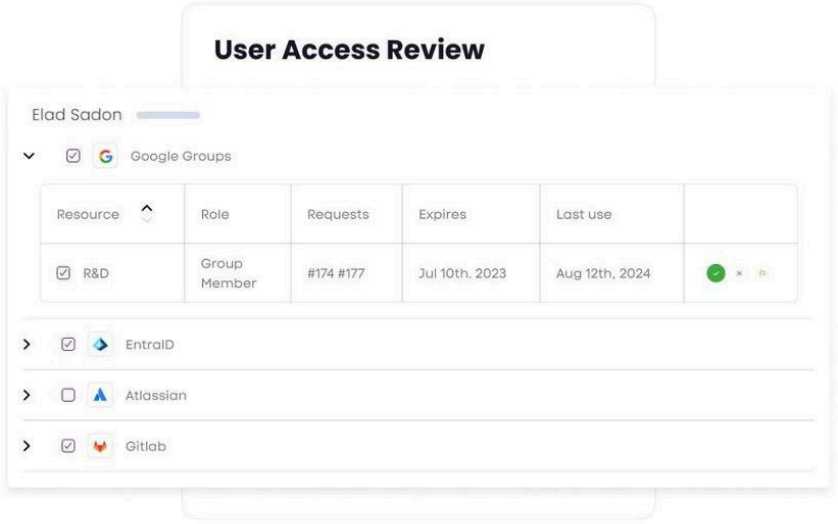


Figure 4: Entitle enables organizations to easily prove compliance via auto-generated reports on user access and entitlements.

> "Employees do the maximum using minimum permissions. [Billie] has embraced JIT access as a standard practice and now experiences a notable reduction in standing permissions. The task of reviewing user access has become manageable, thanks to Entitle's system which efficiently supports a modern tech stack on a large scale."
>
> **— Employee at Billie**

Key BeyondTrust Entitle capabilities:

1. Tracks shadow privileges granted outside of Entitle and eliminates shadow permissions across local accounts, with a centralized source of truth.
2. Identifies high-risk entitlements and takes corrective action.
3. Prevents policy drift by replacing high-risk broad entitlements with precise privileged access.
4. Bundles roles into one access request, from SharePoint folders and S3 buckets to MongoDB tables.
5. Provides users who require access to non-federated systems with a new temporary account endowed only with needed permissions.
6. Enables users to seamlessly access what they need via Teams, Slack, or Jira.
7. Simplifies compliance and forensics with an audit trail of all user activity.

At BeyondTrust, we recognize that any tool such as PIM, or even our Entitle technology, works best when integrated into an ecosystem of controls that helps you holistically reduce risk. For BeyondTrust, this includes addressing the key source of identity risk today: the ability for an attacker to identify and exploit a path to privileged access in your organization.

While Entitle provides a direct replacement for Entra PIM and related technologies, your journey in pursuit of risk reduction and business enablement does not stop at entitlement and permissions management in the cloud, given attackers will seek to exploit other avenues available to them.

This is where the full scope of BeyondTrust technologies, integrated together in our Pathfinder platform, is critical to consider.

Identity Security Insights®

BeyondTrust Identity Security Insights® correlates data from across BeyondTrust products and third-party solutions, giving you holistic visibility into identities and Paths to Privilege™. This empowers security and IT teams with clear, risk-based understanding of all identities, entitlements, and access—revealing their exact impact on your security posture. The product's True Privilege Graph visualizes privilege escalation paths across clouds and on-premises environments, providing insight into risk exposure and surfacing hidden privileges and entitlements.

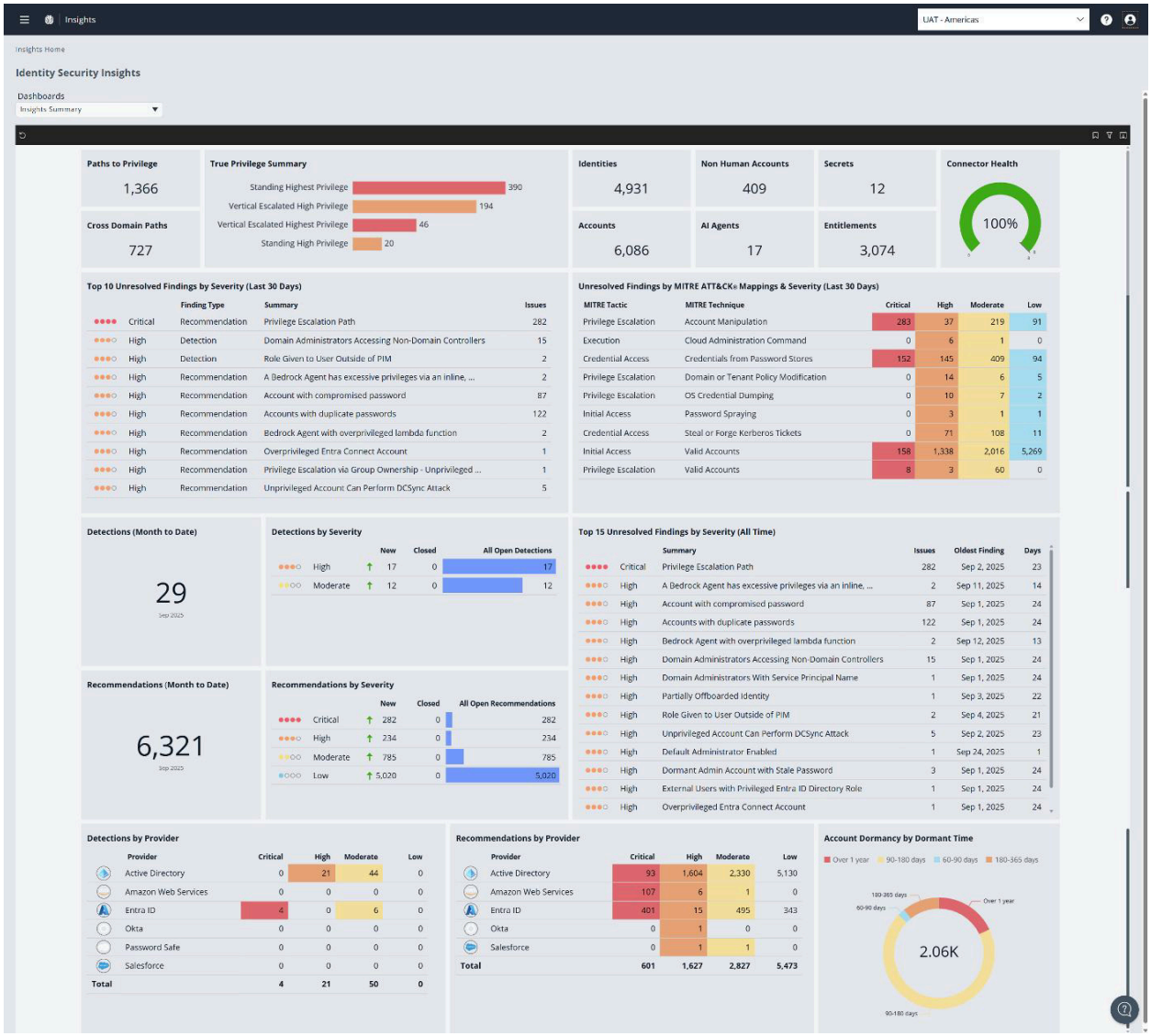


Figure 5: Identity Security Insights gives you the most complete view and understanding of your identity attack surface, and provides rich context that enables you to quickly take decisive action for mitigating risks and stopping attacks.

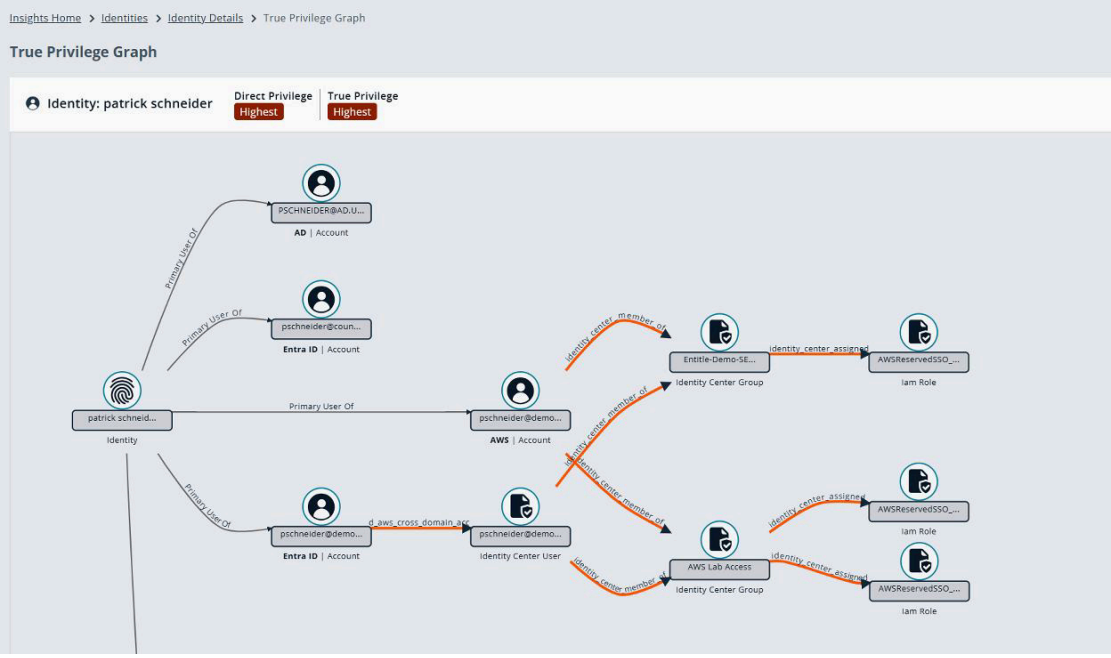


Figure 6: Identity Security Insights provides True Privilege visualization, illuminating escalation paths across cloud and on-premises environments

> "I wholeheartedly endorse Identity Security Insights as a game changer in the identity security space for organizations like ours, starting with on prem AD and then moving into a cloud-forward footing, Insights offers visibility that is unparalleled. Insights and all the other BeyondTrust tools serve as a shield to protect our digital kingdom, all our digital assets."
>
> **— Anna Essex, Sr. Security Analyst at Polsinelli**

Key BeyondTrust Identity Security Insights capabilities:

- Provides a complete view of identity security posture—identities, accounts, effective privileges, escalation paths, and threats—from a single lens.
- Illuminates how attackers can exploit obscure interconnections between accounts, privileges, entitlements, and configurations—across all your domains—to escalate access.
- Proactively detects anomalous activity, the abuse of privileges and identity infrastructure, and threats resulting from compromised human and non-human identities. Offers context-rich recommendations to understand and remediate risks.
- Integrates with BeyondTrust PAM controls, like just-in-time access, to proactively eliminate excessive privileges, harden identity security, and stop in-progress threats, such as by pausing / terminating sessions, rotating privileged passwords or secrets, etc.
- Leverages out-of-the-box integrations with SIEM, SOAR, and ITSM for further correlation and response, or build custom integrations for extensibility.
- Allows customization to fit your exact needs using REST APIs and a Terraform provider.

Endpoint Privilege Management for Windows and Mac

BeyondTrust Endpoint Privilege Management for Windows and Mac enforces least privilege and simplifies compliance across Microsoft Windows and macOS workstations and servers, while improving end-user productivity. It enables you to grant the right privilege to the right application—not the user—only when needed. The solution creates a detailed and centralized audit trail of every elevation—accessible through the solution or via integration with SIEM tools.

Prebuilt policy templates for Windows and macOS stop attacks involving trusted apps, instantly addressing bad scripts and infected email attachments. Application control, allowlists, and exception handling enable granular control over what users can install or run, and what applications can execute. Policies can also be tailored to specific roles (IT, DevOps, etc.) and delivered via AD groups, GPO, or cloud policy service.

> "I really appreciate BeyondTrust Endpoint Privilege Management because it allows us to define which applications we're okay with, which ones we're not, who we allow to install apps, who cannot, and make sure that it is all managed in as much of an automated way as possible."
>
> **— Owen Koch, Head of IAM Architecture at Vialto Partners**

Key BeyondTrust Endpoint Privilege Management for Windows and macOS capabilities:

- Enables zero trust security by removing local admin rights and eliminating standing privileges across Windows and macOS.
- Exerts control over which applications users can install or run.
- Offers advanced token elevation capabilities that allow for precise privilege customization at the Windows token level, reducing attack surfaces while supporting legacy application needs.
- Provides a single, unimpeachable audit trail of all user activity, easily accessed from a secure central console.
- Monitors end users' activity through customizable dashboards and reports.
- Provides pre-built QuickStart policy templates informed by insights from thousands of deployments.

Endpoint Privilege Management for Unix and Linux

BeyondTrust Endpoint Privilege Management for Unix and Linux secures privileged access, enforces least privilege, and centrally manages root account privileges for Linux and Unix. It reduces risk, streamlines compliance and reporting, and addresses the limitations of native tools and sudo, all while simplifying administration.

> "Rather than looking at Privilege Management for Unix/Linux like you're doing a bunch of draconian policies trying to lock everyone down, think of it more like you're enabling your users; how quickly can I get that person online, get them [access] to the things that they need to do, and let them fix the system? That's what we do with Privilege Management for Unix/Linux."
>
> **— Chad Erbe, Sr. Staff Security Engineer at ServiceNow**

Key BeyondTrust Endpoint Privilege Management for Unix and Linux capabilities:

- Controls root access and elevates privileges for standard users based on fine-grained, policy-based conditions (such as role, time of day, or task context).
- Strengthens security and simplifies management by replacing sudo with a centralized, enterprise-grade, and purpose-built solution.
- Audits and reports on changes to critical policy, system, application, and data files.
- Enables users to run specific commands and conduct sessions remotely based on rules—without logging on as admin or root.
- Captures detailed logs of all elevated activity, including command execution, policy enforcement outcomes, and full session recordings with optional keystroke logging.
- Automates tasks and seamlessly integrates with other systems and tools such as SIEM, IGA, ServiceNow, and ticketing systems.

Password Safe®

BeyondTrust Password Safe® combines privileged account / password and session management. The product discovers, manages, and audits all privileged account / privileged credential activity for humans, machines, and AI agents. It unifies management of privileged identities, accounts, passwords, SSH keys, API keys, DevOps secrets, privileged sessions, and more. Password Safe can also vault and generate employee passwords used for enterprise applications.

> "[Password Safe] now provides comprehensive identity security capabilities across the company. Security has been further strengthened by bifurcating user access rights. This means that if access to one application is compromised, it does not allow an attacker to gain access to other applications. The result is higher resilience and greater protection of assets."
>
> **— Mateen Sayyed, Regional Head of Identity & Access Management at Ninja Van**

Key BeyondTrust Password Safe capabilities:

- Minimizes the risk of your privileged accounts being compromised by vaulting and rotating passwords and SSH keys on a schedule, after every use, and / or in response to a potential exposure.
- Eliminates hard-coded credentials and brings them under management.
- Logs and monitors all privileged credential activity, account activity, and sessions for compliance and forensic review.
- Advances zero trust with just-in-time context.
- In conjunction with Privileged Remote Access, it enables credential injection so end users never see the password or secret.
- Locks down management of Entra / Microsoft 365 Global Administrator roles by restricting network traffic to only the solution itself.
- Provides secure, audited management of break-glass administrator accounts.
- Applies enterprise-scale visibility and audit support to employee password management.

Privileged Remote Access

BeyondTrust Privileged Remote Access empowers IT teams to control, manage, and audit remote access by authorized employees, contractors, and vendors—without compromising on security. Securely connect from anywhere to anywhere, no VPN required, while creating identity-secure, just-in-time access across all your enterprise environments including cloud, on premises, and OT.

> "BeyondTrust's [Privileged Remote Access] solution has impacted our business by giving us peace of mind around the security of our customers' data and also giving us a very robust audit trail to ensure the integrity of that at all times, and allowing us to put in the appropriate safeguards to ensure we're always in front of any potential security vulnerabilities."
>
> **— Shane Carden, CIO at Behavox**

Key Privileged Remote Access Capabilities:

- Implements identity-secure, zero trust access to all your enterprise environments: cloud, on-premises, and OT.
- Enforces least privilege and JIT access by giving users the exact level of access they need—and only for the finite moments needed.
- Provides access to untrusted third parties, giving them only the right level of access into your environment, mitigating the threat of a potentially infected system spreading laterally.
- Securely injects managed credentials into remote access sessions, applications, and web pages to add additional abstraction layers between the user and privileged secrets.
- Secures network architecture with fully encrypted HTTPS traffic, avoiding inbound firewall changes or port forwarding.
- Provides access to web pages (i.e. Azure or Microsoft 365 portal) through a locked-down chromium browser that supports auto-injection of credentials and logs session recordings.
- Ensures full visibility and control over all actions, permissions, etc. for all privileged sessions.
- Ensures compliance is easily met with granular details of every session automatically recorded and logged.
- Maintains secure workflows with familiar tools like Putty, RDP, or Azure Data Studio/Visual Studio Code with MSSQL extension and increases coverage by initiating access via mobile or web consoles.
- Facilitates SOC 2 compliance with audit trails, forensics, and advanced analytics using detailed session data—available in real-time and post-session.

Remote Support

BeyondTrust Remote Support enables help desk teams to quickly and securely access and fix any remote device, on any platform, with a single solution. Gain absolute visibility and control over internal and external remote access, secure connectivity to managed assets, and create a complete, unimpeachable audit trail for compliance.

Remote Support boosts service desk productivity, efficiency, and security by consolidating and standardizing help desk support with BeyondTrust. The product has a robust security architecture and can scale support and security in the most demanding enterprise environments, while providing powerful simplified administration that empowers any sized business or agency.

> "BeyondTrust Remote Support was the right product for Ariento because it achieved the cyber compliance requirements from the DoD, specific to DFARS and CMMC, in terms of our ability to service our defense contractor customers."
>
> **— Chris Rose, Partner and CEO at Ariento**

Key BeyondTrust Remote Support Capabilities:

- Supercharges the service desk with secure, least privilege access and support for any device and system, from anywhere—including Windows, macOS, Linux, Android, and iOS.
- Facilitates unattended access to systems and brings efficiency to your enterprise with mass deployments and just-in-time access.
- Logs all session activity for an unimpeachable audit trail, with real-time reporting, detailed video logs, and more.
- Integrates with external directories to scale with infrastructure growth.
- Makes admin tasks simple with mass installers, canned scripts, and escalation features.
- Integrates with your trusted CRM, ITSM, SIEM, and password tools—plus offers an open API to easily build custom integrations.

Active Directory Bridge

BeyondTrust Active Directory Bridge centralizes authentication for Unix and Linux environments by extending Microsoft AD's Kerberos authentication and single sign-on. Users can leverage their AD credentials to access Unix and Linux systems for a seamless experience.

> "Starting with AD Bridge made all the difference in speeding up the execution of our zero trust strategy at Investec."
>
> **— Brandon Haberfield, Global Head of Platform Security at Investec**

Key BeyondTrust Active Directory Bridge Capabilities:

- Extends Microsoft Active Directory or Entra ID authentication, SSO capabilities, and Group Policy configuration to Unix and Linux systems to streamline identity management.
- Enables a wide range of Unix and Linux systems, including RedHat, Solaris, Ubuntu, and others, by connecting them with Active Directory.
- Extends native group policy management capabilities to include specific group policy settings for Unix and Linux.
- Controls access to non-Windows systems by defining which users are permitted to log on to which systems via Active Directory and other policies.
- Provides non-impact, schema-less deployment to enable cross-platform management of identity and access control.

The BeyondTrust Pathfinder Platform

The **BeyondTrust Pathfinder Platform** provides a unified console with which to manage all BeyondTrust products (covered above), also enabling shared intelligence and other synergies for security, productivity, and operational efficiency. Through Pathfinder, organizations can holistically address True Privilege across their hybrid, multi-domain estate, to systematically reduce risk and proactively manage their identity attack surface.

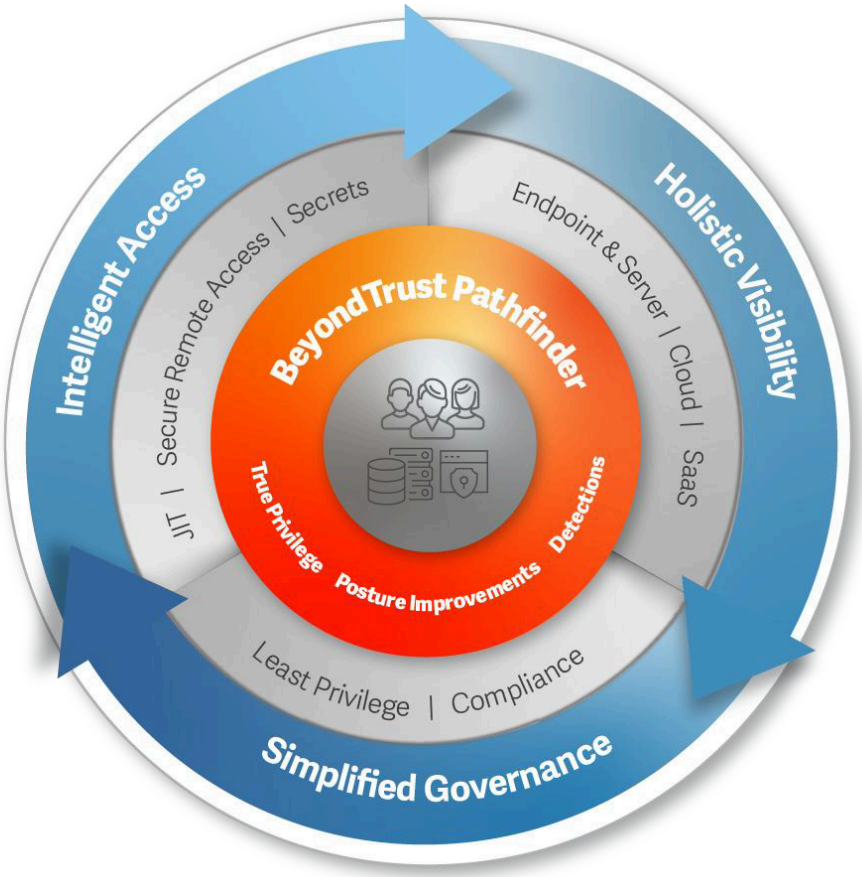


Figure 7: BeyondTrust's Pathfinder Platform, uniting BeyondTrust's entire identity security suite into a single, unified management console.

The BeyondTrust Pathfinder Platform enables you to tackle privileged access management and identity security starting from your chosen areas of highest risk, whether it be your cloud infrastructure or on-premises estate. The platform extends security governance across on-premises, AWS, Entra ID, GCP, and key DevOps tools like Terraform and GitHub. RBAC and ABAC are supported, which allow for fine-grained access policies.

With Pathfinder, organizations can ensure least privilege and PIM best practices are enforced across all endpoints and identities—including human, machine, and agentic AI.

Capability Comparison

BeyondTrust	Microsoft Entra PIM
FEATURES	
• Not confined to Microsoft or Entra, but applicable for all cloud, SaaS, and even on-premises services—'PIM, but for everything'. • Robust session monitoring and management. • Integrates directly with Teams / Slack, including approval workflows. • Approval workflows integrate with a variety of tools, such as on-call schedulers or any automation technology using webhooks. • Visualize privileges / entitlements, as well as escalation pathways, in near-real time across all cloud services using our True Privilege Graph. • Most comprehensive PIM / PAM feature set. Eliminates majority of admins using Endpoint Privilege Management and securely manages remaining privileged accounts with Password Safe. • Eliminates standing / persistent administrator access across all platforms. • Deploys in hours and days, not weeks or months. • Minimizes impact to users and IT administrators, while achieving security goals.	• Specific to Azure, Entra / Microsoft 365 accounts, as well as certain third-party web applications. • No session management capabilities. • Not applicable to Local Administrator (LAR) accounts on Windows, macOS, or *Nix. • Not applicable to most other platforms, such as Linux / Unix, databases, thick-client applications, etc. • Requires Entra ID and Azure managed devices, when using PIM to delegate Device Administrator role. • Does not eliminate standing administrators / admin rights across all platforms. • Conditional access policies can limit suspicious logins, but need extensive configuration, and don't apply restrictions after the user successfully authenticates—only at the point of authentication.

BeyondTrust	Microsoft Entra PIM
SECURITY	
• Entitle delivers zero or low-standing privilege across all cloud providers, not just Entra, and ensures privileges are revoked at the end of any session. • Endpoint Privilege Management ensures the user runs from the safety of a standard user account. Pass-the-hash (PtH) and token hijack attacks are mitigated. • Trusted Application Protection (a capability of Endpoint Privilege Management) shields commonly exploited business tools (such as Office, Acrobat, and PowerShell) from malware and misuse, even by authorized users. • Password Safe onboards and manages privileged accounts / credentials for humans and machines. It ensures privileged passwords, keys, DevOps secrets, and more are rotated on a schedule as well as after every use, so any compromised credential is quickly invalidated. • Session management obfuscates the credentials from the user and forces all traffic to be routed through our password solution's secure proxy. • Privileged Remote Access and Remote Support extend access to Azure or internal resources, without a VPN—and without added risk. • Session reports are detailed with video and text-based logging of all activity and processes that are launched, ensuring a complete and immutable audit record.	• Reporting is specific to logins and approvals granted within the system, not activity within privileged sessions. • Conditional access policies (part of Entra ID) are specific to the point of authentication, not what happens after (user activity). • 'Device Administrator' role applies to all devices, not subgroups—a user has admin access to all end-user devices simultaneously. • Just-in-time and time-bound access are often used improperly; many users require such frequent access to privileged roles that the time expiry becomes forever! • Microsoft recommends two break-glass Global Administrator accounts, which need to be managed separately from any MFA or other controls provided by Entra PIM.

BeyondTrust	Microsoft Entra PIM
PASSWORD VAULTING	
• Full-featured password management and rotation capabilities for both human and non-human identities (machines, etc.) are available across a large number of platforms. • Credential injection abstracts secrets from the user, ensuring that they aren't reused in other tools. • Endpoint Privilege Management reduces the need for many privileged accounts to exist in the first place. Why rotate a password when you can eliminate the risk entirely!	• No password vaulting capabilities.

BeyondTrust	Microsoft Entra PIM
INTEGRATIONS	
• Open integration framework. • Just-in-time access controls across across 150+ cloud app / services. • Integrates with major ITSM, SSO, MFA, SIEM, SOAR, threat intelligence, and IAM tools.	• SCIM identity provisioning protocol.

BeyondTrust	Microsoft Entra PIM
DEPLOYMENT	
• Flexible deployment options across the portfolio, including SaaS and on-prem models. • Does not require Entra.	• Requires Entra ID P2, Suite, or E5 license. • Only deployed through Entra ID.

PIM Evaluation Criteria Shortlist

Completeness of Coverage

- How does the tool work for non-Entra or Azure-based services, such as SSH into Linux devices? SaaS applications? AWS, GCP, or Oracle Cloud? At the database layer?
- Does the tool address the entire environment to your satisfaction, or are there gaps?
- Does the tool manage service accounts and application-to-application accounts (non-human identities)?

Security

- How do you address Local Administrator Privileges across your workstation and server environments?
- How do you protect against Device Administrator accounts being compromised and opening the door to the entire Entra-managed environment?
- Is a 'Device Administrator' role that allows designated users to have admin access across all Entra AD-joined devices acceptable?
- How will you safely and securely manage the credentials of the Microsoft recommended Global Administrator break-glass accounts?
- As Entra PIM only secures access at the identity layer, do you still see risk in users connecting to internal networks from external or unmanaged devices that may be compromised?
- Which tools would they then use to facilitate the connection, and can you verify their authenticity and any security gaps those tools may introduce?
- Are these privileged identities separate from the users' normal identities? Is anything preventing them from using the same passwords on both accounts, as users tend to do?

Reporting & Auditing

- Are lists of logon event details and reports on privileged roles within Entra enough to satisfy auditing requirements?
- Does the tool/solution provide full session recordings, audit logs of privileged activity, and more granular command / privilege management within user sessions?

Ease of Administration

- Who will be tasked with managing requests for access and how much resource overhead will this place on your security team?
- Could credential rotation and injection mitigate the risk of standing admin privileges being granted, as the users would never have 'standing', unfettered access to privileged account credentials?

Next Steps to Effectively Reduce Privilege Risk & Enable User Productivity

For threat actors—whether internal or external—waging an attack on your environment, the highest priority is to gain elevated access (privilege) as early as possible. Privileged access that is inadequately managed—especially when users are provisioned with administrator-level access on their workstation—provides the attacker with easy shortcuts to compromising your environment and moving laterally within it.

In addition, attackers are increasingly exploiting unknown escalation paths. These attacks may be on identities and accounts that lack direct privileges as traditionally recognized, yet still provide a pathway to escalating privilege via hidden or indirect access, misconfigurations, or other means.

Leaving any user with unfettered and unmanaged access to your organization's most sensitive resources is a proven recipe for recurring breach events and audit non-compliance. Across the desktop environment, the need to keep users happy and productive—especially technical or VIP users such as doctors, developers, technicians, and engineers—forces many IT organizations to provide users with a full administrator account on their desktop or laptop, as well as high-privileged access to the resources (i.e. cloud websites) that they might access on a day-to-day basis.

Similarly, in the server estate, sysadmins consistently perform functions that require high-privileged accounts. In an effort to keep these extremely technical users flexible, they are often provisioned with standing / persistent administrative access to the resources under their control. All these risks are unjustifiable and can be resolved with the right PIM / PAM controls.

Privileged identity management means different things to different organizations and often represents itself as a journey.

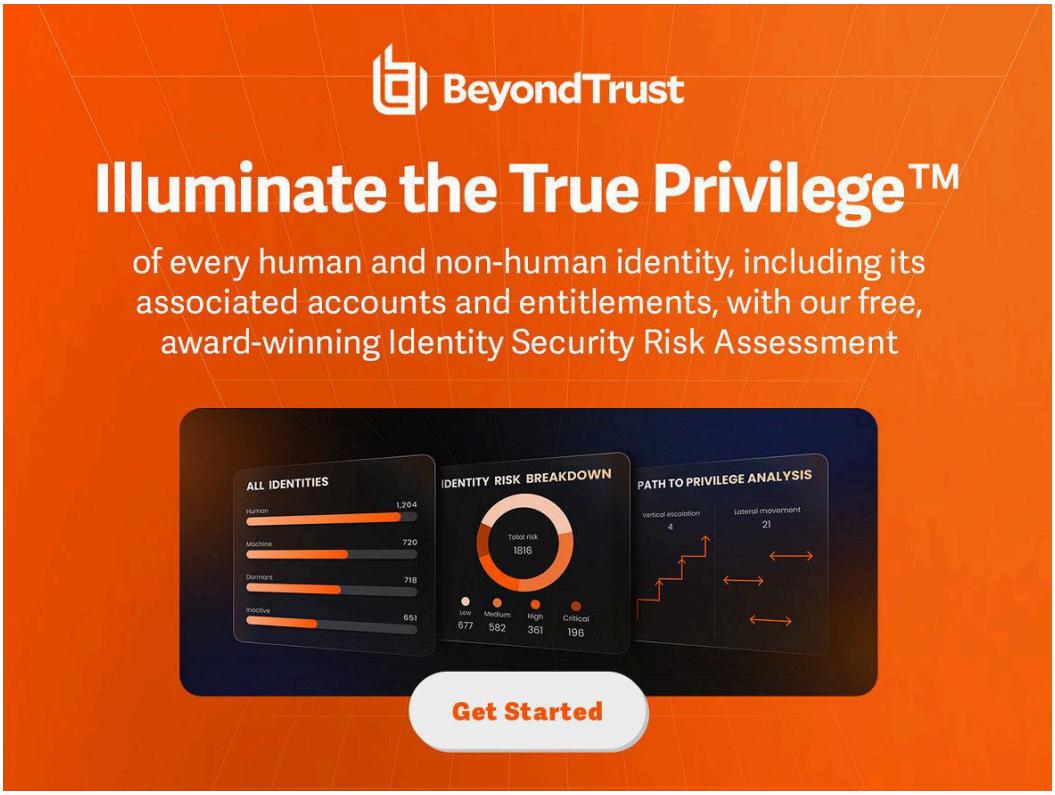
When considering an investment into tools that solve identity and privilege-centric problems, it's especially important to balance cost and complexity against efficacy, and the ability of the tool to deliver across the entire scope of your environment.

The BeyondTrust Pathfinder Platform, and our integrated suite of products, empowers teams with the most holistic protection of privilege and Paths to Privilege™, whether it's Entra, AWS, Google, on-premises, Unix, Linux, Windows, macOS, human, machine, insider, or vendor.

Additionally, we can manage and report on these privileges in a unified way that integrates with the rest of your IT and security infrastructure—including IAM, ITSM, SIEM, SOAR, and more. BeyondTrust delivers the industry's most complete and flexible approach for privileged identity management. Our single platform combines these capabilities along with CIEM, ITDR, and more—giving you the best visibility and protection against identity-based attacks, including those that may cross domains and evade other defenses.

With BeyondTrust, you are well-poised to find and defend against threats across your entire identity estate: unifying visibility across domains such as IT, OT, cloud, and on-premises.

Our team is ready to support you on your security journey. Contact us any time to start a conversation around improving your PAM controls, cloud security, and governance.



Keep Learning about PAM / PIM, CIEM, and Identity Security

- Identity Security Research Kit (a curation of reports from top analysts)
- CIEM Solutions info page
- The Guide to Identity Security Defense-in-Depth
- Buyer's Guide for Complete Privileged Access Management (PAM)
- Guide to Endpoint Privilege Management
- The CISO's Guide to Addressing Critical Gaps in Identity Security through PAM Modernization

About BeyondTrust

BeyondTrust is the global identity security leader protecting Paths to Privilege™. Our identity-centric approach goes beyond securing privileges and access, empowering organizations with the most effective solution to manage the entire identity attack surface and neutralize threats, whether from external attacks or insiders.

BeyondTrust is leading the charge in transforming identity security to prevent breaches and limit the blast radius of attacks, while creating a superior customer experience and operational efficiencies. We are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at **www.beyondtrust.com.**