BeyondTrust

Buyer's Guide for Complete Privileged Access Management (PAM)

Modern PAM + Foundational PAM:
You need both for a complete approach.

Your path to effective PAM should be straightforward.

Start Here

BeyondTrust

TABLE OF CONTENTS

EXECUTIVE SUMMARY

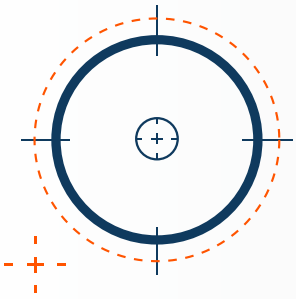
Identity is the new perimeter — and privileged access management (PAM) is the keystone of modern identity security.

Traditionally, no identities—human or non-human—have been more imperative to secure than those with privileged access to systems, data, applications, and other sensitive resources. Yet, the security calculus is not so straightforward today.

In modern environments, an ostensibly low-privilege user could have a hidden or indirect Path to Privilege™ through group memberships, misconfigurations, or overlooked cloud permissions. And these paths could traverse different domains.

To effectively protect identities, today's PAM must expand visibility, protection, and control beyond just directly privileged accounts to also cover how human and non-human identities access privilege. This entails clearly understanding and addressing True Privilege™, which encompasses all the entitlements and escalation pathways of an identity / identities.

Today, entitlements (privileges, rights, and permissions) are built into operating systems, file systems, applications, databases, hypervisors, cloud management platforms, DevOps tools, robotic automation processes, and more. The expansion of remote work and cloud means organizations are not only grappling with more identities and entitlements, but also with more complex ones as well.



What hasn't changed is that cybercriminals covet privileges / privileged access because it can expedite access to an organization's most sensitive targets.

With privileged credentials and access in their clutches, a cyberattacker or piece of malware essentially becomes an "insider."

Threat actors are also expanding their attack targets to include the very toolsets used to manage identities. In this world, PAM is essential for protecting your entire identity infrastructure, including your backend IAM / IGA tools.

While simple security fundamentals can still prevent many breaches, attackers are rapidly advancing in agility beyond just simple automation. Machine Learning (ML) and Artificial Intelligence (AI) are enhancing attacker toolsets and empowering more sophisticated human-operated attacks. And, of course, it's just as important for organizations to protect their own AI and ML data from being stolen or poisoned.

Yet, the fact remains: almost every attack today requires privileges for the initial exploit, or to laterally move within a network.

While the attack surface continues to expand and evolve, the most salient part of the story is how identities and entitlements continue to proliferate and become exposed in new ways.

The average organization has 351 exploitable attack paths threat actors can leverage to reach high-value assets.

SOURCE: 2024 State of Multicloud Security Report. Microsoft Security. May 2024.

The Attack Surface Is Expanding

As the traditional perimeter has dissolved, the privileged threat surface has vastly expanded and grown more complex.

Cloud & Hybrid Cloud

Cloud Management Platforms (AWS, Azure)
Virtualized Environments (VMware, Microsoft, Nutanix)
Virtualized Machines (Linux, Unix, Windows)
SaaS Apps (Box, Jira, Marketo, Microsoft 365, Salesforce)

On-Premises

Shared Admin Accounts
Desktops (Windows, Mac)
Servers (Linux, Unix, Windows)
Hypervisors & Virtual Machines
Security & Network Infrastructure
Applications & Databases
Machine Credentials (App to App)

DevOps & Backend Infrastructure

Containers
DevOps & SecDevOps Tools
Dynamic Virtual Environments
Microservices

Operational Technology (OT) / Internet of Things (IoT)

Building Management Systems
BYOD
Cameras
Industrial Control Systems
Printers
Roaming Workstations
Sensors
Smart Healthcare Devices (mHealth)
Any device with embedded Internet connectivity

Identity-Based Security Challenges

At a Glance

More Cloud, Multicloud, & Bring Your Own Cloud (BYOC)

Of the 51,000 different permissions (22% increase from 2022) granted to identities, only 2% are used, and 50% are considered high-risk.[1]

More Remote Access Risks

External remote services (VPNs, RDP, etc.) were the leading initial access method for breaches, **facilitating 65% of intrusions.**[2]

More Identity Misconfigurations

61% of organizations have a root user or account owner without MFA.[3]

More Identities (human, machine, etc.)

98% of security professionals say identities are increasing in number, driven by cloud adoption, third-party relationships, and machine identities.[4] Workload identities now outnumber human identities 10:1.[5]

More Privileges

50% of cloud identities are Super Admins, which are users or workloads with access to all permissions and resources.[6]

More Exposed Credentials & Secrets

Cloud account credentials comprise **90% of cloud assets** for sale on the dark web, making it easy for threat actors to take over legitimate user identities.[7]

More Connectedness to Everything

54% of pen tests on industrial environments found remote access security issues, half of which were critical or high severity.[8]

More Identity-Based Incidents & Breaches

90% of security professionals said there organization experienced an identity-related security incident in the past year.[9]

1. 2024 State of Multicloud Security Report. Microsoft Security. May 2024.
2. Sophos, It's Oh So Quiet (?): The Sophos Active Adversary Report for 1H 2024. April 2024.
3. 2024 State of Cloud Security Report. Orca Security. Feb 2024.
4. 2023 Trends in Securing Digital Identities. IDSA. May 30, 2023.
5. Microsoft Security, 2024 State of Multicloud Security Report. May 2024.
6. 2023 State of Cloud Permissions Risk Report. Microsoft Security. March 2023.
7. IBM X-Force Threat Intelligence Index 2024. IBM. April 2024.
8. 2023 OT Cybersecurity Year in Review. Dragos. Feb. 2024.
9. 2024 IDSA 20243 Trends in Securing Digital Identities. IDSA. June 2024.

Attackers are using smarter tools. So should you.

PAM stands at the core of identity security.

To address risks related to privileges and paths to privilege, a complete PAM solution should not only prevent threats, but also provide intelligent detection capabilities. To do this, a complete solution must combine both modern and foundational PAM capabilities.

Where do you start?

Controlling, monitoring, and auditing elevated access and paths to privilege for human and non-human identities—and everything that touches your IT environment—is essential for protecting against external and internal threat vectors, and for addressing a growing list of compliance requirements.

But where do YOU start?

Are hidden paths to privilege your organization's most pressing risk, or is it more specifically remote access, or privileged credentials? What about standing privileges? Perhaps it's the Linux servers where your sensitive data and operations, including your own AI, is hosted? Do you start with the most modern PAM use cases, or do you first need to focus on implementing or further maturing foundational PAM controls?

And once you've started, how do you know what areas to focus on next?

This PAM Buyer's Guide will help you confidently tackle these questions—where to begin your privileged access management (PAM) project, how to progress to a better security posture, and what business outcomes to expect.

Since most organizations have already implemented some foundational PAM controls, this guide will first introduce the PAM controls to help you quickly and efficiently address the modern risks and operational challenges organizations frequently struggle with today. Next, we'll delve into the foundational controls organizations must evolve and continue to mature to close security gaps and improve productivity. We will then cover emerging use cases you should know.

Ultimately, your next steps with PAM are a risk-based decision dependent on the needs of your organization. With the right vendors and partners, your path to effective privileged access management should be straightforward.

Privilege, Identity, & Access Problems for Environments without PAM	PAM End-State Security Goals / Best Practices
No singular, clear picture of threats or how to address them	Complete, cross-domain visibility over identities and attack paths to proactively mitigate threats
Manual processes for managing privileged passwords and secrets (use of spreadsheets, physical safes, etc.)	Automated management of privileged accounts, sessions, credentials, and secrets
Most users have administrator access on their machines	Rules-based least privilege implemented organization-wide on all systems and machines
Standing privilege is the the default provisioning model, meaning privileged access is always-on (24/7)	Standing privileges are mostly eliminated, and elevated access is provisioned just-in-time, only for the finite moments needed
Lack of auditing and control over root and other privileged accounts	Full control and accountability over privileged users on any system, eliminating root access or insufficient methods, like sudo
No session monitoring or recording of privileged use	Automatic recording of keystrokes / video / over-the-shoulder activities
Uncontrolled or "all or nothing" insider and third-party remote access	Granular, flexible control ensuring remote access is extended only to the required resources for authorized vendors and employees
Disorganized and chaotic directory services infrastructure, with multiple logons required and inconsistent policies across Windows, Unix, Linux, etc.	Single sign on (SSO) for heterogeneous systems, leveraging familiar infrastructure
Gaps in management between privileged and non-privileged identities	Seamless management of privileged and non-privileged identities for zero-gap coverage
Complete blindness—especially across the cloud and SaaS applications—of elevated access, let alone how to manage it	Automated user access reviews across multicloud and on-premises, with the ability to continuously right-size entitlements and fulfill audits
Impeded user productivity and a high volume of service desk tickets	Users are enabled to do what they need to; the help desk receives fewer tickets due to fewer security issues
VERY HIGH SECURITY RISK	**VASTLY REDUCED SECURITY RISK**

Maturing your PAM controls will improve security, auditability, and business operations. The further you make it on the continuum to the end state, the more dramatic the risk reduction, the more condensed your threat surface, and the better your security posture.

Timeless PAM Security Principles with a Modern Approach

By evolving your PAM, you not only reduce the threat surface, but also eliminate security gaps, improve your response capabilities to attacks, and make compliance and cyber insurance qualification easier.

The next section of this paper outlines a **seven-step approach** to achieving a more effective privileged access management program.

1. **Gain** fundamental visibility of all identities to successfully mitigate risk
2. **Seamlessly** operationalize just-in-time (JIT) access and right-size entitlements across clouds and SaaS
3. **Apply** zero trust access for employees, vendors, contractors, and infrastructure
4. **Improve** accountability and control over privileged identities, accounts, passwords, and secrets
5. **Implement** least privilege and application control for Windows and macOS
6. **Implement** centralized least privilege and audit access across Unix and Linux environments
7. **Streamline** identity management and security by integrating Unix and Linux into Windows directory services

The 7 Key Steps for Complete PAM

This section of our guide identifies the core areas of privileged access management, presenting the key capabilities you should seek across each of these areas to secure identities and access and meet compliance objectives.

Each core area, when implemented, will give you greater control and accountability over the identities, accounts, assets, users, systems, and activities that comprise your environment, while eliminating and mitigating many threat vectors. You can address these areas all at once or, more commonly, phase in controls for one or several areas of PAM at a time. The more areas you implement, the more complete your coverage over true privileges, the greater PAM synergies you will see, and the more impactful the reduction in enterprise risk and improvements in operations.

Throughout the process of selecting and deploying your PAM solution, **keep these business requirements in mind,** as they will help you articulate the value of this program to stakeholders in the organization:

Total cost of ownership

Does it result in time-savings (such as replacing manual processes with automation) and allow you to redeploy resources for other initiatives?

Time-to-value

How soon does it help you measurably improve security controls and dial down risk? How long will it take to achieve your end-state goals with the solution?

Integrations

How does it integrate with the rest of your security ecosystem (IAM, SIEM, SOAR, service desk, analytics)? Does it help you make better decisions on risk and have synergies with your existing security solutions?

Longevity

Will the solution vendor grow with you, or even pull you towards growth, through security enablement? Is the vendor resourced to evolve their capabilities to meet the PAM use cases of tomorrow?

KEY STEP

Gain Fundamental Visibility of All Identities to Successfully Mitigate Risk

The rapid explosion of human and machine identities, and the proliferation of new access paths (many hidden or poorly understood) to critical systems and data, has left security teams flat-footed and suffering from poor visibility into attacks and identity security exposures.

Organizations may use dozens of systems to manage identities and access rights, creating more layers of complexity and further expanding the attack surface. What's more, many IAM / IGA systems themselves are attractive targets for threat actors.

When the identity management system itself becomes compromised, it then becomes a simple exercise for an attacker to traverse the entire environment.

Advanced persistent threats (APTs) often go undetected because traditional security analytics solutions are unable to correlate diverse identity-related data (such as privileged accounts, users, assets, cloud entitlements, etc.) to detect hidden risks, such as indirect paths to privilege. Seemingly isolated events are written off as exceptions, filtered out, or lost in a sea of data. The intruder continues to traverse the network, and the damage continues to multiply. Most organizations lack a centralized view of identities, accounts, and privileged access across their diverse IT domains. This absence of cohesive, end-to-end identity visibility translates into:

- Overlooked or hidden identity vulnerabilities that present paths to privilege.
- Delayed orchestration in response to threats, and extended dwell times.
- Inability to satisfy auditors or address forensic requests in a timely manner, if at all.
- Security risks to the identity infrastructure.
- Heightened risk of solutions not integrating or communicating well with each other, resulting in downtime, security gaps, and frustration.

How do security and IT operations teams gain a clear understanding of where identity threats are coming from, prioritize them, and quickly mitigate the risks?

Goal

Gain a holistic, intelligent view of all identities and access across your entire multicloud and on-premises estate to clearly understand your risks, decrease costs, and optimize productivity. You should seek visibility into attack paths that cross domains, and manage your entire identity estate as one cohesive attack surface.

Solution

BeyondTrust Identity Security Insights leverages powerful PAM, CIEM, and ITDR capabilities to provide holistic, identity-based threat intelligence. This empowers security and IT teams with clear visibility into all identities, entitlements, and access—revealing their exact impact on your security posture.

Identity Security Insights ushers groundbreaking levels of identity and threat intelligence into the BeyondTrust portfolio. Get prioritized, actionable analytics your teams can leverage to immediately improve your security posture and eliminate potentially dangerous backdoors and weak spots.

Identity Security Insights makes all connected solutions, including other BeyondTrust solutions, significantly more intelligent and powerful.

Identity Security Insights combines with other BeyondTrust solutions and third-party data sources (including Okta, Ping Identity, GitHub, AWS, Google Cloud, and Microsoft Entra ID). The product leverages the correlated data of users, accounts, and privileges to extensively map your organization's landscape and link identities across multiple applications. You can also leverage guided recommendations to continuously harden your identity security posture and ensure least privilege access. No other solution provides as comprehensive a view into privilege and identity-based weaknesses, while also identifying the paths to privilege that open attack pathways and present backdoors to sensitive assets.

With a clear understanding of your paths to privilege and true privileges (including shadow admins, etc.), you can streamline risk reduction across your environment.

Top 3 Use Cases

Unified, Cross-Platform Visibility of True Privileges

Gain one holistic view across your multicloud and on-premises estate, and know the level of privilege an attacker could achieve if they compromised an account.

Proactive Identity Security Hygiene

Identify orphaned accounts, shadow admin, and overprivileged accounts, as well as poor identity security controls; leverage actionable recommendations to right-size privileges and mitigate risks.

AI-Driven Anomaly Identification

Zero in on anomalies—including events involving multiple identities and accounts—and accelerate threat investigations into human and non-human identity behavior.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

> "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 other BeyondTrust tools serve as a shield to protect our digital kingdom, and it has given us confidence in our security footing."
>
> **— Anna Essex, Sr. Security Analyst, Polsinelli**

KEY STEP

Seamlessly Operationalize Just-in-Time (JIT) Access and Right-Size Entitlements across Clouds and SaaS

Privileged access that is persistent (24/7 access), referred to as standing privileges, is a relic of the past. When privileges are in an always-on state, it also means they're always vulnerable to exploitation or abuse.

Attackers have learned to exploit static permissions, turning them into persistent backdoors and unchecked paths to privilege into your most sensitive systems. Traditional access management approaches leave these risks unchecked, creating a growing challenge in a world of dynamic cloud environments and ever-expanding digital estates.

Organizations often default to granting excessive permissions simply to avoid delays or to meet operational demands. Over time, this approach results in sprawling privilege creep, where permissions and paths to privilege accumulate unchecked and unrevoked.

Organizations clinging to standing privileges face daunting risks, including:

- IT teams overwhelmed by trying to provision least privilege access across clouds with legacy toolsets, leading to errors and burnout.
- Inefficient workflows, where resolving access issues consumes time better spent on strategic initiatives.
- Increased likelihood of privilege misuse, whether intentional or inadvertent.
- Heightened risk of compliance failures due to inadequate tracking and reporting of access rights.
- Amplified attack surfaces, providing intruders with more pathways to sensitive systems.

Standing privileged access overwhelms IT and DevOps teams, forcing them to choose between constant privilege management or risking over-provisioned accounts.

How can organizations effectively operationalize the shift from static access models to an adaptive, JIT access model—at scale—while keeping workers agile and productive?

Goal

Empower organizations to securely streamline access with precision, ensuring the right people access the right resources at the right time—without excessive administrative burden.

Solution

BeyondTrust Entitle combines JIT PAM and CIEM capabilities to revolutionize cloud permissions management. By implementing dynamic, least-privilege access and self-service provisioning, Entitle streamlines access control, while enhancing security. A cloud-native solution, Entitle ensures seamless scalability, smooth, multicloud integration, and instant results.

Entitle adds a critical layer of privilege defense to the BeyondTrust portfolio, extending protection from networks and endpoints to what users can actually do once logged in. With Entitle, ensure users only have the permissions they need when they need them—and nothing more. Employees can self-serve access through familiar tools, like Slack and Teams, lowering the IT / DevOps burden. Flexible no-code policy definitions enable condition-based approval workflows, while automated provisioning ensures permissions are granted and revoked seamlessly via APIs. Centralized access governance provides complete visibility, logs every action, and automates compliance tasks, including user access reviews.

Deployed in minutes, Entitle integrates with numerous cloud-based apps and infrastructure, making it an ideal solution for modern environments.

Top 3 Use Cases

Just-In-Time Access for Critical Operations

Enable secure, time-bound access to production environments and customer data, ensuring employees only have the permissions for the finite moments needed.

Accelerated Employee Access

Streamline access requests with automated workflows, reducing delays, while empowering teams to work efficiently.

Automated Access Reviews

Simplify compliance and governance with fully automated access reviews, ensuring permissions stay aligned with security policies.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

> "As a cloud-native, digital insurance company, we approach security, audit, and compliance with the bionics of automation. Using Entitle, we've implemented self-service, just-in-time provisioning that follows proper security practices."
>
> **— Jonathan Jaffe, CISO, Lemonade**

KEY STEP

Apply Zero Trust Access for Employees, Vendors, Contractors, and Infrastructure

Organizations often resort to complex systems, authentication methods, and network / VPN configurations in an attempt to provide smooth access for end users and administrators. With numerous access points and often inadequate visibility, auditing, and security controls, the likelihood of a weak link being compromised sharply increases. Considering the scale of modern organizations and the security risks associated with implementing and maintaining multiple access pathways, it's evident how critical this deficiency can be.

VPN-based access solutions introduce significant risks, creating a fragile "eggshell" layer of security that places your organization's risk posture on a single point of failure. Moreover, VPNs frequently grant excessive access beyond what is necessary, opening up paths to privilege that expose networks and identities to heightened risk.

Core issues with VPNs and traditional access methods include:

- All-or-nothing access, with a lack of granular security settings.
- No visibility into, or record of, user activity (only session activity)—meaning no behavioral audit trails.
- Protocol or application-specific access via VPN is not typically supported.

Secure access to resources doesn't have to come at the expense of efficiency and convenience.

How can organizations better control remote access for privileged users without inhibiting business agility?

Goal

Eliminate "all-or-nothing" remote system access by implementing granular, role-based access to specific systems, with defined session and application parameters. Allow contractors, vendors, or employees access to specific systems, ephemerally, for specific applications or purposes. Administrators can approve or deny access requests from anywhere, and for any device, across almost any platform.

Solution

BeyondTrust Privileged Remote Access enables security and IT professionals to securely control, manage, and audit privileged remote access to critical IT systems by authorized identities and accounts, including employees, contractors, and third-party vendors —without a VPN.

Implementing BeyondTrust's Privileged Remote Access (PRA) solution enables you to gain unified access control for your critical resources. Centralizing the management of your access pathways with BeyondTrust offers users a seamless experience across all major platforms. Privileged Remote Access facilitates the remote access users need, while ensuring sensitive data is protected and compliance mandates are satisfied.

You can deploy the Privileged Remote Access solution on-premises via a virtual appliance, or through a secure SaaS solution, which has achieved FedRAMP certification. Provision access to and from servers, laptops, mobile devices, and operational technology (OT) endpoints. Privileged Remote Access also features a credential management vault that protects privileged credentials with discovery, management, rotation, auditing, and monitoring for privileged accounts—from a local or domain-shared administrator, to a user's personal admin account—including SSH keys, cloud, and social media accounts.

For more comprehensive credential management capabilities, Privileged Remote Access integrates with BeyondTrust Password Safe. These products can be bundled for the industry's best valued and most powerful total PASM offering.

Top 3 Use Cases

Secure Access for Employees, Anywhere

Maximize employee productivity and security with credential injection and secure remote access to authorized systems.

Vendor Privileged Access Management (VPAM)

Provide simple, secure remote access for trusted vendors connecting to your systems, while eliminating the need for VPNs and the distribution of sensitive credentials.

Kubernetes Environments

Elevate your Kubernetes environment with the assurance of just-in-time security and efficiency only Privileged Remote Access can provide.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

> "BeyondTrust was among those topping the Gartner rankings and validated all of our use cases. While other PAM vendors could also check some boxes, BeyondTrust's Privileged Remote Access solution also offers the benefit of being extremely simple to use and deploy."
>
> **— Benjamin Serre, Global CTO, MANE**

BeyondTrust provides the world's most mature and complete set of capabilities for extending privileged access security best practices to vendors, other third parties, and remote workers—all in one solution.

KEY STEP

Improve Accountability and Control Over Privileged Identities, Accounts, Passwords, and Secrets

The most logical starting point for gaining greater control over privileges is improving accountability over privileged identities, their accounts, and credentials. Privileged credentials include privileged account passwords, secrets for DevOps and CI/CD toolsets, SSH keys, certificates, and more.

Admins commonly share passwords, which makes it nearly impossible to get a clean audit trail. Many systems, applications, and devices (IoT, network devices, etc.) have embedded or hardcoded passwords, exposing opportunities for misuse. Passwords and/or secrets are needed for application-to-application and application-to-database access. Privileged credentials are rapidly generated when new cloud or virtual instances are spun up. The list goes on.

Manual privileged credential management measures (discovery, rotation, propagation, enforcement of best security practices) are notoriously unreliable, complex, time-consuming, and impractical to scale. Many best practices—like eliminating and centrally managing some types of embedded passwords—are virtually impossible to adhere to without enterprise tools.

How do organizations ensure security and accountability over all the different types of credentials that allow privileged access—but without disrupting end-user productivity, workflows, and processes?

Goal

Seamless discovery of the ever-expanding list of privileged account and credential types in your environment (both human and non-human), placement of those accounts and credentials under management, and satisfaction of auditor requests—all via a comprehensive, automated solution.

Such a solution will eliminate numerous privileged attack vectors outright, while mitigating many others, to drastically reduce enterprise security exposures. This requires a purpose-built enterprise password management or privileged credential management solution that can automate each phase of the password and secrets lifecycle, consistent with your security policies.

Solution

BeyondTrust Password Safe unifies management of privileged identities, accounts, passwords, SSH keys, API keys, DevOps secrets, privileged sessions, and more—in one product.

Password Safe provides **comprehensive auto-discovery, management, auditing, and monitoring** for any privileged account or credential—human, application, machine, etc.—substantially reducing the risk of privileged credential misuse, and addressing common compliance requirements.

The solution provides valuable threat analytics (such as correlating anomalous privileged user behavior and third-party data to determine threat criticality), advanced reporting, and unmatched enterprise scalability.

Top 3 Use Cases

Credential, Key, & Secrets Management

Automatically discover and onboard accounts; store, manage, and rotate privileged passwords and secrets, eliminating embedded credentials in scripts and code via a secure API.

Real-Time Session Management

Log, monitor, and record all privileged credential and session activity in real-time for compliance and forensic review.

Advanced Auditing & Forensics

Leverage extensive privilege and credential analytics to simplify compliance, benchmark tracking, training, and audit reviews.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

Other Considerations

How important is scale? Do you have just a few thousand privileged credentials, or hundreds of thousands?

Only a handful of PAM solutions can scale to manage tens of thousands, or even hundreds of thousands, of privileged user credentials and concurrent sessions. Fewer still can also manage high numbers of SSH keys or secrets used by non-human users. BeyondTrust not only delivers all these capabilities, but also meets the enterprise needs of scale.

How adverse are you to security complexity, solution overlap, and security vendor redundancies?

Many security vendors sell various components of privileged account and credential management separately—each with their own distinct management console. There are also niche security vendors that offer standalone capabilities for SSH key management, application password management, or DevOps secrets management. BeyondTrust delivers all these capabilities in one robust solution.

But, what about all those other application passwords used by employees?

Yes, BeyondTrust Password Safe is a great tool to secure employee passwords for enterprise applications, too. While privileged credentials pose the most risk, the line between privileged / unprivileged is becoming increasingly blurred in modern environments.

Employees across your organization need access to dozens, or even hundreds, of applications to perform their roles, and often, this involves sensitive levels of access and data. Password Safe offers a Workforce Passwords module that provides enterprise-grade security for passwords used by your employees, helping you further extend important paths to privilege protection across your organization. Employees can use Password Safe to quickly store business application credentials they need for their daily work, using familiar experiences like folder storage and browser plugins. The capability also provides full auditing and reporting support, including granular tracking of identity, credential, and application access activity.

BeyondTrust provides a single, complete solution to manage, monitor, and audit all types of privileged credentials in a centralized and unified way, while also enabling non-privileged users with a simple, secure means to store their enterprise application passwords.

> "Trying to change passwords on a service account—an account used to run an application behind the scenes—used to be a nightmare. People don't always remember where passwords are, and changing them could break things and create big headaches for many people. Sometimes, fixing that situation meant restoring everything to the moment before changing the password, which could again lead to lost work... Password Safe would make the whole process more efficient, eliminating the need for duplicate work, easing collaboration between departments, and helping decrease audit findings."
>
> **— David Lokke, Senior Systems Administrator, Premier Bankcard**

KEY STEP

5 Implement Least Privilege and Application Control for Windows and macOS

Once privileged credentials and accounts are being consistently discovered, onboarded, and managed, the next step to attaining complete privileged access management is implementing endpoint least privilege. How? By eliminating local admin rights on end-user machines and ensuring privileges are granted only to the application, task, or command when needed, and for only as long as needed.

As servers remain prime targets for attackers, eliminating standing privileges for Windows servers is crucial to establishing appropriate access for critical administrator roles, including across network, Active Directory, database, developers, Help Desk, and IT staff.

> **"Removing local admin rights and controlling execution has historically mitigated 75% of Microsoft's critical vulnerabilities."**
>
> **— 2024 Microsoft Vulnerabilities Report, BeyondTrust, April 2024**

With that said, managing privileges through static policies or ad hoc toolsets is inefficient and lacks the scalability required for modern IT environments.

How do IT organizations reduce the risks of users having excessive privileges without inhibiting their productivity or overburdening the help desk with requests for privileges?

Goal

Efficiently eliminate local admin rights across Windows (desktop and servers) and macOS systems, tightly control and audit the use of privileges on servers and sensitive systems, and enforce granular control over applications—all without hindering end-user productivity. To achieve this, enterprise endpoint privilege management solutions must support just-in-time (JIT) access and remove end-user privileges, while automating rules-based technology to elevate application permissions—without ever elevating privileges to users themselves.

Rather than having privileges enabled and always on (and thus vulnerable to potential misuse or abuse), JIT access elevates privileges only for the finite moments required, dramatically reducing the threat surface, sharply curtailing susceptibility to lateral movement, and minimizing the risk of successful phishing and ransomware threats. Sensitive systems and data remain protected, while users have the flexibility to perform critical tasks without permanently elevated privileges.

Solution

BeyondTrust Endpoint Privilege Management (EPM) for Windows and Mac enforces least privilege and simplifies compliance across Microsoft Windows workstations and servers, as well as macOS workstations, while improving end-user productivity.

BeyondTrust Endpoint Privilege Management for Windows and Mac ensures users are granted permissions only as needed to specific applications and tasks. The product implements JIT application access to streamline workflows by enabling task-based privilege elevation, ensuring application permissions are granted precisely as needed. JIT admin access allows organizations to grant temporary admin privileges for critical tasks, improving compliance, strengthening security, and maintaining operational efficiency, while minimizing disruptions to workflows.

Top 3 Use Cases

Zero Trust Endpoint Security & Advanced Threat Protection

Remove local admin rights, enforce least privilege across Windows and macOS endpoints, and control privileges to effectively block threats like malware, ransomware, phishing, insider attacks, and living off the land attacks.

Streamlined Exception Handling with JIT Access

Enable secure, just-in-time access, improving user experience, reducing downtime, and always maintaining least privilege.

Comprehensive Audit & Compliance Management

Quickly address compliance and cyber insurance requirements with a single, unimpeachable audit trail of all privileged actions.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

Other Considerations

How important is the solution's time-to-value for you?

Some solutions demand complex service arrangements. Other solutions deliver rapid time-to-value by demonstrating risk reduction and decreasing help desk tickets within days or weeks.

Do you have a Unix or Linux server estate, or other non-traditional endpoints that touch your network?

Many vendors offering Windows privilege management capabilities lack similar capabilities for Unix, Linux, and macOS, let alone non-traditional endpoints. Wouldn't you rather have one solution vendor that can enforce least privilege and application control best practices across all your endpoints?

BeyondTrust is the only vendor that delivers complete privilege management across your entire estate.

BeyondTrust's Endpoint Privileged Management for Windows and Mac solution provides a strong ROI by enforcing least privilege and removing standing privilege—an integral part of your zero trust strategy.

Out-of-the-box QuickStart policies honed from thousands of deployments enable organizations to improve security posture, quickly. The solution's unique Trusted Application Protection capability (Windows only) even stops attacks via commonly exploited production software by leveraging built-in, context-based controls to catch bad scripts, spot infected attachments, and control child processes and DLLs.

Endpoint Privilege Management for Windows and Mac can be implemented faster than competitor solutions, while also offering deeper capabilities—providing a swift time-to-value from the moment it enters your teams' hands.

> "BeyondTrust Endpoint Privilege Management really is a perfect solution. Not only does it implement least privilege, protect, and monitor our privileged accounts, it also allows us to maintain compliance with several regulations, which is hugely beneficial to us... [The] solution has considerably improved our organization's security processes and reduced errors, while also helping us directly address compliance demands... Competitor solutions were bulky and had difficult processes to set up and apply. BeyondTrust Endpoint Privilege Management seamlessly integrated with our internal process and created an exceptional outcome."
>
> **— Vikas Vijaywargiya, CIO, Zensar**

KEY STEP

Implement Centralized Least Privilege and Audit Access Across Unix and Linux Servers

Business-critical, Tier-1 applications running on Linux and Unix servers are prime targets for cyberattackers. Privileged user credentials for these resources can provide access to ecommerce data, ERP systems with employee data, customer information, and sensitive financial data.

Having root passwords, superuser status, or other elevated privileges is necessary for IT administrators to do their jobs. But the exponential growth of (particularly Linux) endpoints has made securing these systems a significant challenge, especially with the continued reliance on tools like sudo. While useful for IT administrators to perform critical tasks, sudo's lack of centralized management, deficiencies in audit capabilities, and lack of robust security controls creates significant risks. These shortcomings can leave organizations vulnerable to insider threats, misconfigurations, compliance failures, and more.

Native tools and ad hoc solutions fall short in several areas:

- Limited oversight and forensics, with no central audit trail or session recording.
- Security gaps, leaving unapproved applications and activities unchecked.
- Inefficient scalability, requiring policy management on each individual server.
- A lack of enterprise-grade support.

With sudo and other tools, it's virtually impossible to maintain best-practice security and compliance in all but the most basic of IT environments. And, simply put, the stakes of inadequate privileged access controls in your Unix and Linux environments are far too high.

Goal

Gain comprehensive visibility and control over all privileged activities across Unix and Linux environments, with consistent enforcement of least privilege and efficient delegation of privileges and authorizations—all without ever disclosing passwords for root or other accounts. Move beyond the limitations of sudo. Replace sudo entirely with centralized, enterprise-grade capabilities, or enhance it to resolve security, scalability, and auditing deficiencies.

Solution

BeyondTrust Endpoint Privilege Management for Unix and Linux is the leading solution for securing privileged access, enforcing least privilege, and centrally managing root account privileges for Unix and Linux. With advanced analytics and reporting, it reduces risk, streamlines compliance, and addresses the limitations of native tools and sudo, all while simplifying administration.

Top 3 Use Cases

Root Access Control

Enforce least privilege to execute only specific tasks or commands.

Comprehensive Activity Auditing

Log all user activity to protect against unauthorized changes to files, scripts, directories, and applications, and to address compliance.

Eliminate Standing Privileges

Achieve true least privilege and minimize threat windows by removing standing privileges and granting as-needed access.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

Other Considerations

Do you also have Windows and macOS endpoints (workstations, servers, etc.) in your environment?

If improving PAM coverage and reducing complexity is important to you, there are only a few vendors that can meet your needs. BeyondTrust provides full, best-in-class privilege management coverage across your entire endpoint estate—Linux, Unix, Windows, macOS, non-traditional endpoints, and more.

Endpoint Privilege Management for Unix & Linux increases the security, accountability, and productivity of all users and server administrators, without the risks posed by open-source sudo.

By enabling just-in-time privilege management, and thereby striving toward a zero standing privilege (ZSP) state, Endpoint Privilege Management for Unix and Linux sharply limits the time during which an account possesses elevated privileges and access rights. This dramatically reduces the window of vulnerability when a threat actor can exploit account privileges. While this is by far the industry's most powerful Unix / Linux PAM solution, it also offers faster ROI compared to alternatives. This is achieved by centralizing privileged account management under a single plane of control, significantly reducing the time and effort needed to achieve security and audit objectives.

> "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 and Linux."
>
> **— Chad Erbe, Sr. Staff Engineer, ServiceNow**

KEY STEP

7 Streamline Identity Management and Security by Integrating Unix and Linux into Microsoft Directory Services

After gaining control over privileged access in Unix and Linux environments, the next step to achieving consistent management and policy enforcement across systems is to implement SSO for authentication into those environments. Traditionally, however, Unix and Linux have functioned as isolated silos, each with unique users, groups, and access control policies. This fragmentation leads to administrative inefficiencies, inconsistent policy enforcement, and increased security risks when managing a mixed environment alongside Windows systems.

So, how do IT organizations manage policy and authentication consistently across diverse platforms and provide a streamlined user experience that reduces administration time and errors?

Goal

Centralized authentication across Windows, Linux, and Unix environments mitigates the risks of shared or unmanaged credentials, while simplifying the complexities of managing a diverse infrastructure. Simplify operations by minimizing the need for multiple logins, reducing forgotten-password help desk calls, and unifying disparate systems, configurations, and policies. This requires a solution that bridges Active Directory or Entra ID with Unix and Linux, streamlining identity management and enforcing consistent security policies across platforms.

Solution

BeyondTrust Active Directory (AD) Bridge streamlines identity management and access control across your hybrid environment by extending Microsoft Active Directory or Entra ID authentication, SSO capabilities, and Group Policy configuration to Unix and Linux systems.

By centralizing the management of logins and leveraging configurations through your Windows Active Directory infrastructure, BeyondTrust AD Bridge accelerates identity security and compliance goals, while boosting productivity for both end users and server administrators.

Top 3 Use Cases

Unified Management of Identities

Eliminate complexity with a single, familiar toolset to manage digital identities across your Windows, Unix, and Linux systems.

Auditing & Compliance

Provide detailed audits to compliance teams and manage group policies from a central interface.

Enhanced Unix / Linux Security

Enable SSO, enforce consistent security policies, and control access to Unix / Linux systems.

For a comprehensive capabilities checklist, view Appendix 2: Your PAM Buyer's Guide Worksheet

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

By executing well on the preceding steps, you will address most of your PAM needs, eliminate or mitigate many privileged threat vectors, and vastly reduce your attack surface.

Nearly every emerging technology with the power to transform IT comes with security challenges and gaps that savvy attackers seek out and exploit.

While there are many edge use cases BeyondTrust solutions can meet that are not covered in this paper, let's briefly explore several important areas that can present unique challenges, and how BeyondTrust directly addresses them.

Specialized Business Cases for PAM

In this section, we take a closer look at key ways BeyondTrust helps you address:

- DevOps security
- Security for Operational Technology (OT) and non-traditional endpoints
- Security for Robotic Process Automation (RPA)
- Cyber insurance qualification
- Enablement of zero trust
- Protection against deepfakes

DevOps Security

Most organizations have adopted DevOps practices. Yet, despite the rise in prominence of DevSecOps, security is often still an afterthought, or even a casualty, of the speed and tools used across DevOps environments.

While DevOps achieves condensed development cycles through automation, and leverages the scale of the cloud, the downside is that it can also "automate insecurity," creating massive security, compliance, and operational problems.

Some common DevOps security issues include:

- Unsecure code, hardcoded passwords, and other privilege exposures.
- Scripts or vulnerabilities in CI/CD tools—such as Ansible, Chef, or Puppet—could deploy malware or sabotage code.
- Excessive provisioning of entitlements across the DevOps landscape.
- Sharing of secrets across users and control planes.
- Vulnerabilities, misconfigurations, and other weaknesses in containers and other cloud services.

While security clearly needs to be built into DevOps, how do you do so without hampering speed and agility?

BeyondTrust solutions reduce DevOps and CI/CD-related risks by improving visibility and control over identities, secrets and APIs, admin privileges, and system configurations.

By uniting these capabilities across on-premises, virtual, cloud, and DevOps use cases, IT organizations can achieve their agility goals without burdensome processes.

BeyondTrust PAM capabilities for securing DevOps and CI/CD environments:

- Inventories and auto-onboards all DevOps assets and automated workflows.
- Finds, secures, and centrally manages the use of passwords, secrets, keys, and certificates. This includes developer access to source code, DevOps tools or applications, scripts, test servers, and production builds, thereby eliminating a common threat vector frequently exploited by attackers.
- Enforces least privilege—granting only required permissions, and only for the finite moments needed—to appropriately build machines and images, and to deploy, configure, and remediate production issues on machines and images.
- Applies application control to ensure the use of only the right tools, and only within the right context, thereby limiting the chances of lateral movement should an attacker gain access.
- Enforces boundaries between development, test, and production systems.
- Manages and audits all privileged sessions, delivering much-needed visibility for security teams, as well as audit and compliance support.

Working together, BeyondTrust solutions give you full PAM coverage across your DevOps landscape, enabling your teams to stay secure, gain visibility and control over entitlements and paths to privilege, and maintain peak development agility.

Security for Operational Technology, IoT, and Non-Traditional Endpoints

OT, IoT, and other non-traditional endpoints are pervasive today.

These endpoints often lack basic security features, have default and hardcoded credentials, and may have firmware that is difficult to patch or update, among other risks. Frequently, these devices and systems were never actually designed with the intention of being connected to the corporate network. Industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems—which were traditionally 'air-gapped' to safeguard their mission-critical functions, while ensuring the safety of the surrounding communities and environment—are increasingly connected and exposed due to these architectural flaws. Additionally, many ICS vendors now use standard IT technologies within their solutions, making them more accessible to attacks.

Architectures like the Purdue Model have been developed to address these concerns, but in many cases, the relevant changes in architecture would significantly impact an organization. In addition, legacy tools typically lack the ability to uncover, onboard, and securely manage diverse device types and their access—let alone at scale.

This all results in dangerous security exposures scattered across OT and IT environments. Compromises of OT systems could lead to catastrophic damage to infrastructure, and even jeopardize many human lives.

How can organizations consistently account for and secure the ever-increasing number of non-traditional endpoints, including OT / IoT devices, SCADA, ICS, and even common network devices, such as routers, switches, and firewalls?

BeyondTrust was first-to-market with a PAM solution offering granular command control and auditing over privileged user activity on network, IoT, and OT devices. With BeyondTrust, you can extend PAM best practices and zero trust security principles to OT systems and non-traditional endpoints.

BeyondTrust PAM capabilities for hardening OT security:

- Discovers and onboards all devices for management.
- Enforces credential management best practices, such as eliminating embedded / hardcoded credentials and securing credentials in a centralized, tamper-proof vault.
- Removes admin rights and applies fine-grained least privilege control.
- Secures remote access (for employees, vendors, to / between systems, etc.), with a robust, VPN-less solution that also layers on MFA.
- Enables segmentation and microsegmentation to isolate networks and resources.
- Monitors and records sessions to provide a complete audit trail of user activity.
- Analyzes behavior to detect suspicious user activity.
- Supports multiple protocols, including RDP, HTTPs, SSH, Telnet, and application protocol tunneling.
- Enables the Purdue Model and zero trust architectures.

Learn more about BeyondTrust OT security solutions.

Security for Robotic Process Automation

Robotic process automation (RPA) eliminates mundane and routine tasks that would otherwise burden IT resources.

However, native RPA security controls are often inadequate. For instance, RPA toolsets typically have excessive rights, and embed credentials to quickly establish connections for automation.

BeyondTrust can extend PAM best practices to your RPA implementation.

BeyondTrust PAM capabilities for improving RPA security:

- Scans, identifies, profiles, dynamically categorizes, and auto-onboards all assets and supporting resources that may be included in an RPA workflow.
- Enforces best practices for password management, including eliminating hardcoded / embedded RPA credentials, and secures the organization from automated exploitation via an extensive, RPA-compatible API.
- Ensures passwords can be automatically reset after RPA usage to safeguard the security of the workflow.
- Implements least privilege and granular control across RPA processes, toolsets, and workflows.
- Locks down and provides access control to authorized applications only.
- Integrates with and supports a wide range of RPA tools (Blue Prism, UiPath, Pega, etc.).

Cyber Insurance Qualification

In recent years, cyber insurers have tightened qualification criteria, increased rates, and even dropped coverage for many organizations. This comes largely in response to a surge in costly cyberattacks and ransomware claims.

Cyber insurance companies and underwriters recognize that privileged access management controls provide foundational security for every organization, prevent many cyberattacks outright, and significantly minimize the damage of any potential breach.

BeyondTrust Privileged Access Management can help you qualify for cyber insurance and get the best rates, while drastically reducing your cyber risk.

PAM solutions provide must-have capabilities, including least privilege enforcement, privileged account and credential management, and remote access security—all common criteria for cyber insurance approval.

BeyondTrust can help you confidently address the following common security criteria required for cyber insurance qualification:

- Removes local admin rights on user workstations and enforces least privilege across all endpoints.
- Ensures human and non-human accounts (including service accounts) always abide by least privilege.
- Protects, monitors, and audits employee and vendor remote access, also ensuring credentials used for remote access are managed and secured.
- Implements MFA as an extra layer of security for remote access.
- Uncovers and remediates attacks and indicators of compromise (IoCs).
- Provides blended protection to block or mitigate ransomware attacks.

Addressing cyber insurance requirements and getting the best rates with BeyondTrust:
Download: Cyber Insurance Compliance Checklist
Visit: Cyber Insurance Solutions & Education Hub

BeyondTrust's blended ransomware protection:
Visit: Ransomware Protection Solutions & Education Hub

Enablement of Zero Trust

The need for zero trust has surged in response to increased IT decentralization, remote work, and network perimeter erosion.

Zero trust principles and architectures aim to eliminate persistent trust. This entails enforcing continuous authentication, least privilege, and adaptive access control, and applying segmentation and microsegmentation to create secure access. A key zero trust goal is to always have visibility into who is doing what, and why, and to ensure that you can control or limit the blast radius of any threats to the network when an incident occurs.

BeyondTrust solutions support the smart, practical implementation of NIST's zero trust security model—**without disrupting day-to-day business processes.**

BeyondTrust solutions help enable NIST's seven core tenets of zero trust by working relentlessly to identify and secure every privileged user (human, non-human, employee, vendor), asset, and session across your digital estate. Control the who, what, when, why, and where of access. Implement BeyondTrust zero trust security controls to reduce your attack surface, minimize threat windows, and improve protection against ransomware, malware, advanced persistent threats, insider threats, and more.

BeyondTrust capabilities for advancing zero trust:

- Discovers, inventories, and intelligently groups all privileged assets to eliminate blind spots, illuminate shadow IT, and control access points.
- Illuminates identities, entitlements, and paths to privilege across domains, providing intelligent context on how to eliminate excess access and mitigate threats.
- Applies least privilege controls to right-size access for every identity and account—human, application, machine, employee, vendor, etc.
- Continuously enforces adaptive and just-in-time access controls based on context.
- Manages and enforces credential security best practices for all privileged passwords, secrets, and keys.
- Implements segmentation and microsegmentation to isolate various assets, resources, and users to restrict lateral movement.
- Secures remote access with granular least privilege and adaptive capabilities well beyond that of VPNs, RDP, and other common remote access technologies.

- Secures access to control planes (cloud, virtual, DevOps) and sensitive applications and data.
- Continuously monitors, manages, and audits every privileged session.
- Simplifies secure management of identities and zero trust implementation enterprise-wide by extending Microsoft Active Directory (AD) authentication, SSO, and Group Policy Configuration Management to Unix and Linux.

Learn more about how BeyondTrust addresses zero trust:

Learn how to bridge NIST zero trust principles to real-world privileged access management (PAM) product capabilities.
Download: Advancing Zero Trust with Privileged Access Management (PAM)

Learn how BeyondTrust solutions map to and enable the 7 core tenets of the NIST zero trust model, how common PAM use cases enable the core tenets of the NIST zero trust model, and more.
Download: Mapping BeyondTrust Capabilities to NIST Zero Trust (SP 800-207)

Learn about successful implementations from customer stories:

Watch: Investec's Journey to Zero Trust, from Theory to Practice
Visit: Zero Trust Solutions & Education Hub

> "The interactions between the products in the [BeyondTrust] suite have been brilliantly and carefully orchestrated in a way that we are maximizing our chance of getting as far down the Zero Trust road as we possibly can given the state of the products in the security market."
>
> **— Brandon Haberfeld, Global Head of Platform Security, Investec**

Protection Against Deepfakes

In recent years, deepfake technology has taken impersonation to new levels, amplifying the threat of social engineering and other identity-based attacks.

Over the course of a deepfake attack, a threat actor may try to persuade a targeted user to share their password or sensitive data, bypass or remove security controls, download malware, or perform some other action, such as transferring money. While deepfake attacks are disturbing and sometimes outright shocking, existing identity security technologies, combined with strong policies, can help break multiple phases of the attack chain to prevent or mitigate the impact.

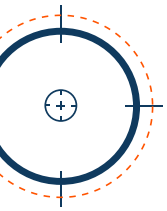
BeyondTrust capabilities for deepfake protection:

- Identifies identity security misconfigurations that could allow account hijacking (lack of MFA on privileged accounts, etc.), privilege escalation, or unwanted lateral movement (excess privileges, etc.).
- Provides identity-based detections across domains to zero in on anomalous behavior.
- Enables robust privileged session management and auditing, including the ability to pause or terminate suspicious sessions.
- Removes admin rights and enforces least privilege, so even if a user is tricked, the impact of what they are persuaded into wrongly doing can be limited.
- Supports enforcement of privilege separation and separation of duties to minimize the privileges that can be exercised by any single identity or user.

Each of these BeyondTrust capabilities is highly effective in protecting against deepfake-powered and other types of social engineering attacks, providing critical protection for your identity security program.

Why select a single vendor to achieve complete privileged access management?

We believe our differentiation in the PAM market lies in the breadth and depth of our platform that covers both foundational and modern use cases, the ease-of-use of our products, the diversity of available third-party integrations, our proven, decades-long history of leadership and innovation, and our people.



The BeyondTrust Difference

Differentiator 1:
Breadth, Depth, and Flexibility of Our PAM Solution

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions available in the market. BeyondTrust stands out for our unsurpassed depth and breadth of PAM use cases covered, technological innovation and vision, and our modern, centralized management platform: **Pathfinder**, which empowers organizations to holistically see, understand, and address true privileges.

We cover it all—Windows, macOS, Unix, Linux, cloud, on-premises, hybrid, human (employee and vendor), and machine.

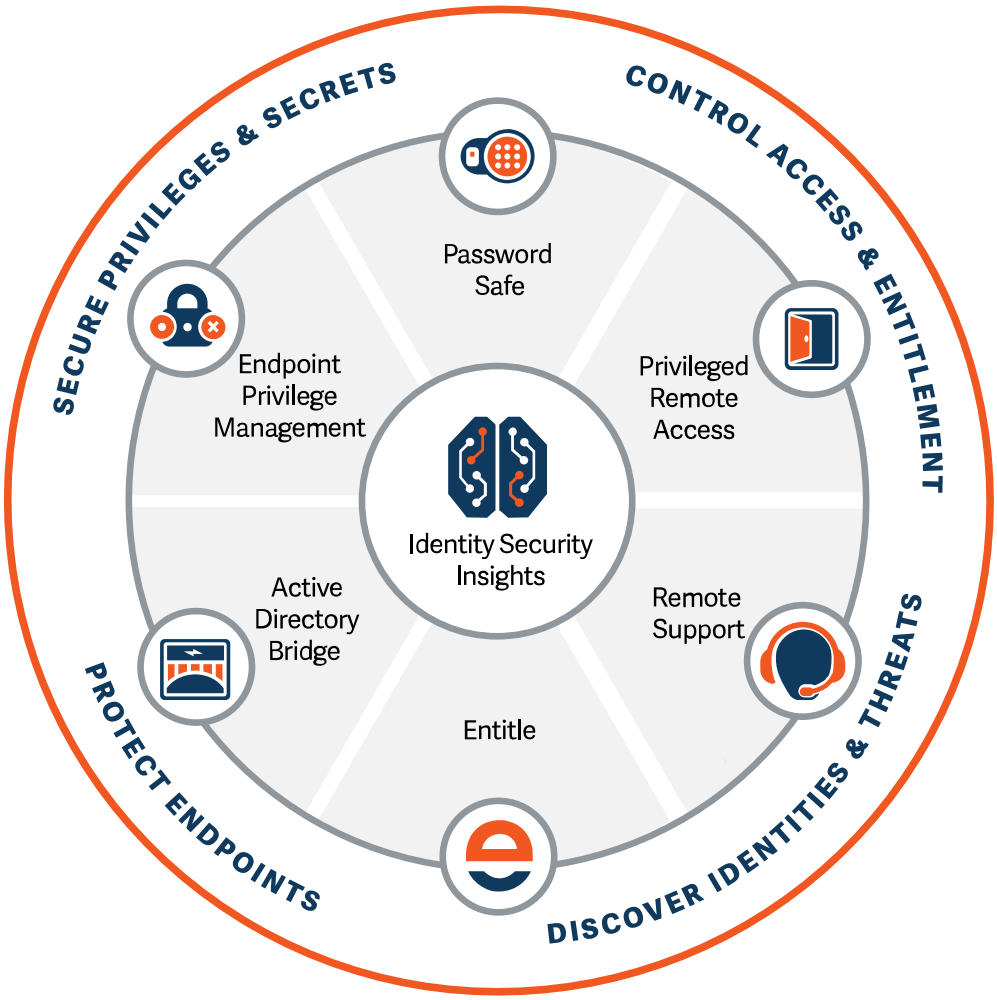
Together, our platform and complete approach to PAM delivers holistic visibility, simplified management, and intelligent protection.

BeyondTrust blends three disciplines—PAM, CIEM & ITDR—to help organizations holistically strengthen their identity security.

Unlike other PAM vendors, BeyondTrust doesn't force you to do privileged access management our way. With BeyondTrust's extensible platform, you have the option to roll out a complete set of PAM capabilities all at once, or to phase in capabilities over time at your own pace. You can start with modern PAM use cases, or by maturing foundational PAM capabilities. With BeyondTrust, it's always your choice.

We also give you the choice of deployment model that best suits your needs.

Whichever product or deployment model you begin with, you will immediately start reducing risk and improving administration.



CLOUD | HYBRID | ON-PREMISES | OT

Differentiator 2:
Intelligent UX Unleashes Productivity Gains and Accelerates Time-to-Value

We make PAM easier and work better. BeyondTrust accomplishes this through a focus both on UX and on delivering productivity-unlocking features that delight our customers and enable them to make rapid leaps in security and operational efficiencies.

We are also committed to advancing digital accessibility and are collaborating with a trusted third-party accessibility partner to take proactive steps toward aligning our products with the Web Content Accessibility Guidelines (WCAG) 2.2 Level AA standards.

Intelligent UX that Facilitates Ease-of-Use and Good Security

Each quarter, in conjunction with the NPS survey, our UX team collects standardized usability scores for our products. These scores are collected using a modified version of the Post-Study System Usability Questionnaire (PSSUQ), an assessment tool that has consistently demonstrated effectiveness hundreds of times in well-respected scholarly literature throughout the past 35 years.

Our surveying efforts have shown a truly world-class level of usability across our products and help guide us in continuing to improve BeyondTrust products.

We design our products in adherence to the following three principles of good UX:

Remove friction
Less friction means the user is more likely to adopt the product and use it effectively. We understand it's human nature for people (users) to tend to avoid what's difficult. You don't want people avoiding security practices!

Minimize human errors
Human error remains a leading cause of IT security incidents, especially in the cloud. If the experience of the product or service is properly designed, it removes the potential for errors to occur. In contrast, if the experience is confusing or doesn't give clear feedback to the user, it's much more likely for the user to introduce an error or miss something critical.

Improve speed
The better the user experience, the more likely the important, critical, or urgent information is quickly surfaced. This means less "hunting" or investigation is needed by the user.

We also use our own products at BeyondTrust throughout our infrastructure and leverage internal user feedback, as well as external user feedback, to continually improve UX.

Unique Features that Accelerate Time-to-Value and Boost Productivity

One benefit of PAM done right that surprises many of our customers is that it:

- Improves the productivity of the admins using our tools.
- Enables the secure productivity of workers, including third-party vendors.
- Enhances operational efficiencies across the enterprise.

Here are some examples of such features across our products:

Identity Security Insights connectors ingest identity data from all your identity sources, giving you the most holistic, centralized picture of your identity attack surface, and how to manage it, in just minutes or hours.

Entitle boosts productivity for end-users and admins with features like self-service access requests, permission bundling, and decentralized approval workflows, delivering fast, secure, and time-limited access to resources—without the typical provisioning delays.

Privileged Remote Access empowers users to initiate a privileged session faster and more simply than with competitor tools, while ensuring the most robust security and auditing controls are in place.

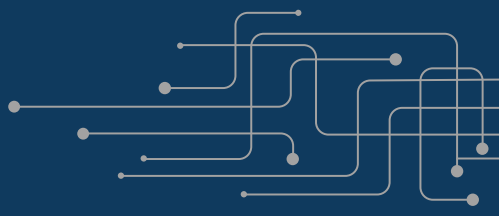
Password Safe enables organizations to auto-discover, onboard, and enforce security best practices across all types of privileged accounts and credentials (passwords, keys, secrets, etc.) with Smart Rules, our market-leading automation.

Endpoint Privilege Management for Windows and Mac provides Quick Start Templates that enable organizations to apply least privilege controls in minutes or hours, rather than weeks or months.

Endpoint Privilege Management for Unix and Linux not only provides far more security and auditing control than sudo and other tools, but it also offers powerful centralized management capabilities that make it far easier to use, especially at scale.

We also do not require professional services for upgrades, and do not void a support agreement if professional services are not used.

BeyondTrust and UX:
Blog: How to Leverage UX to Defragment Your Security Solution
Blog: Good User Experience Leads to Good Security
Blog: BeyondTrust's Commitment to Digital Accessibility



Differentiator 3:
Security Innovator - Revolutionizing & Reinventing PAM

BeyondTrust is recognized by analysts as a PAM leader—not just for our product excellence and solution completeness, but also for our innovation. We believe the recognition is well-earned. BeyondTrust has a decades-long history of innovation, pioneering many foundational, must-have PAM capabilities that have come to define today's PAM space. And we're not stopping.

Modern PAM Innovations Transforming the Industry

Today, BeyondTrust continues to provide innovative, industry-leading capabilities that are re-defining PAM to cover an expanded swathe of modern identity security challenges. In fact, in 2024, industry experts recognized BeyondTrust as a Leader across three important identity security domains: PAM, identity threat detection and response (ITDR), and cloud identity management. BeyondTrust's multicategory identity security approach combines these three important areas in a powerful, unified platform to address privilege and paths to privilege.

Privileged Remote Access: While remote privileged access management (RPAM) is now gaining wide recognition as an essential PAM capability, BeyondTrust's remote access security solutions for employees and vendors were launched years ahead of alternative offerings. We were first to offer robust remote access security that truly extended PAM and identity security best practices to vendors and remote workers, empowering our customers with a secure, work-from-anywhere (WFA) approach. Other vendors are still trying to catch up as we continue to make our secure remote access capabilities even more robust and easy to use for a modern, borderless workforce.

JIT Access and Multicloud Permissions Management: BeyondTrust has also taken an innovative approach to solve the increasingly widespread challenges organizations are facing due to standing privileges and cloud entitlements sprawl. The 2024 SC Awards crowned BeyondTrust Entitle as the winner of the Best Identity Management Solution category for what SC staff called the product's "groundbreaking approach to managing permissions and addressing the risks associated with excessive privileges in modern cloud environments."

In the award announcement, SC staff also wrote, *"Notably, Entitle has enabled companies to reduce IT workloads by up to 85%, while also drastically cutting down excessive permissions in production environments by over 90%. The platform's ease of implementation is a further highlight. Entitle can be deployed and configured in just a few hours, a remarkable feat compared to the lengthy setup times of legacy IAM systems."*

Cross-Domain Identity Visualization and Risk Intelligence: In 2023, BeyondTrust launched Identity Security Insights, which completely broke the mold of existing market solutions to set a new bar for approaching and solving for modern identity security challenges. It enables customers to accurately and holistically assess and improve their identity security posture with radically reduced time and effort.

The product immediately introduced unparalleled identity and access visibility across cloud, SaaS, and on-premises, as well as game-changing capabilities for understanding and contextualizing identity-based risks. Customers not only gain clear intelligence into entitlements and access, but also into paths to privilege. The product provides AI-powered detections and alerts on in-progress attacks that other solutions miss. Identity Security Insights makes BeyondTrust PAM and other security solutions far more intelligent, and through webhooks and other integrations, helps operationalize ITDR.

Some other BeyondTrust innovations, many of them patented, include:

- An ML-driven IP abuse scoring method that aggregates existing vendor risk scores and proprietary event data across multiple sources, providing ground-breaking improvements in detecting, contexualizing, and prioritizing identity-based risks across domains.
- First to provide holistic visualization of an enterprise's entire identity fabric across on-premises, cloud, and SaaS infrastructures—all through a single solution that not only illuminates direct entitlements of identities, but also indirect and hidden paths to privilege, putting risk in context.
- First to provide a Microsoft Windows least privilege solution.
- First to provide an Apple macOS least privilege solution.
- First endpoint privilege management solution to introduce an intelligent anti-tamper mechanism that can protect our least privilege software and configuration settings against modification from elevated processes, while still allowing the solution to be administered by true system administrators.
- File integrity monitoring (Unix / Linux), which ensures the 'things' you allow to be elevated, and the processes that perform the elevation, haven't been compromised.

- Advanced audit and control (ACA) technology (Unix / Linux) that audits activities inside scripts, controls file and folder access (even for root), and blocks malicious and compromised binaries.
- Registry Name Services (Unix / Linux), which provide advanced failover and load-balancing automatically, centralized role-based management, and the ability to form groups of clients that share configuration or policy based on role or business organization.

BeyondTrust is the first product vendor to combine foundational PAM with CIEM and ITDR for cohesive visibility, prevention, detection, and remediation across a hybrid computing, work-from-anywhere world.

We are also the first PAM solution to provide enterprise-grade credential management with DevOps secrets management in one tool, and at no additional cost to customers.

Our trailblazing Pathfinder platform provides the most complete and cohesive way to find, understand, and control true privileges.

Today, BeyondTrust continues to trailblaze with our expansive vision to address Paths to Privilege, and our PAM Modernization roadmap.

We're aggressively pushing to solve emerging and future customer needs, as well as innovating enhancements to our existing solutions, so they're always best-of-class in features, capabilities, and usability.

Differentiator 4:

Integrations and Interoperability

BeyondTrust's solutions and platform are elegantly architected to integrate with your current security and infrastructure solutions so you can maximize your existing investments and processes. The last thing we think you need is another siloed security point solution.

BeyondTrust empowers you with a holistic understanding of the identity threat landscape across both external and internal risks. Our solutions incorporate relevant security data—including available exploits, risky privileged activity, vulnerable systems and applications, compliance requirements, and mitigations—to help our customers drive better-informed security decisions. BeyondTrust solutions also capture important information that can be shared with your other IT and security tools and systems.

Ecosystem Integration

Sample of BeyondTrust third-party technology integrations

You can learn more about our rich technology partner ecosystem on our Technology Alliances page.

"One of the best things about working within the BeyondTrust ecosystem is that every solution is compatible with everything else. Once we realized we could integrate Password Safe with Remote Support, we shaved 30–45 seconds off every support call. Over time, that adds up."

— David Hart, IT Division Manager - Customer Service, City of Dothan

"We were looking for solutions that not only provided ease of use and ease of management, which we found in the BeyondTrust solution(s), but the integration of the multitudes of different solutions that BeyondTrust provides gave us the ability to integrate seamlessly through those different solutions."

— David Tyburski, CISO, Wynn Resorts

"Our [Insights] integration with the SIEM solution, Splunk, helps streamline the remediation of detections and recommendations. BeyondTrust webhooks connect with various applications in our environment, greatly expanding our automation capabilities, which is something I'm particularly passionate about."

— Anna Essex, Sr Security Analyst, Polsinelli

Differentiator 5:

Recognized PAM Leader by Analysts, Chosen by Customers

What do the top analysts have to say about Privileged Access Management?

BeyondTrust has been recognized as a Leader in Privileged Access Management and Privileged Identity Management in the most recent independent research analyst reports by Gartner®, Forrester Research, and KuppingerCole.

2024 Gartner® Magic Quadrant™ for Privileged Access Management
2024 KuppingerCole Leadership Compass: Privileged Access Management
The Forrester Wave™: Privileged Identity Management, Q4 2023

20,000 customers across 100+ countries choose BeyondTrust.

Year after year, the top industry analysts recognize us as a PAM Leader. But we are even more proud of the recognition heaped on us from our customers.

Additionally, BeyondTrust was named a 2024 Gartner® Peer Insights™ Customers' Choice for Remote Desktop Software.

You can check what our customers have to say about us on the Gartner Peer Insights platform, where we have 550+ five-star verified customer reviews.

You can also check out more BeyondTrust case studies on our own site, here.

Differentiator 6:

Proven BeyondTrust Experience & Global Presence

More than 20,000 customers in 100+ countries rely on BeyondTrust solutions, which are backed by our 1,600+ employees across 24 countries, and an extensive global partner network.

We understand each of our customers has unique needs and requirements, and with over 1,500+ partners globally, we have the network and expertise to provide tailored solutions to meet those needs. We are intentional about partnering with the organizations that possess the right capabilities, expertise, and experienced track record to ensure we are providing our customers with the best solutions and experience.

With thousands of successful deployments across diverse industries and use cases to satisfy security, compliance, and regulatory requirements across the globe, BeyondTrust has the strongest team to help you accomplish your PAM and identity security goals.

75%
of Fortune 100

95%
Gross Retention Rate

65
Market Leading NPS Score

94%
CSAT for Customer Experience

> "Over and above the expertise we would expect from a software vendor, BeyondTrust has provided us with hands-on support and helped us to think beyond this project towards future developments."
>
> **— Benjamin Serre, Global CTO, MANE**

Differentiator 7:
Our People

Yes, we are recommended by analysts and customers. But BeyondTrust is also recommended by our employees, who drive the success of our company every day.

BeyondTrust is continually recognized and recommended by our employees for providing an outstanding work environment. We are consistently recognized as one of the top places to work.

97%

of employees at BeyondTrust say it is a great place to work

VS.

57%

of employees at a typical US-based company

SOURCE
Great Places to Work®
Global Employee Engagement Study

Recognition of BeyondTrust for Exceptional Workplace Culture and Employee Experience

Inc. Magazine Best Workplaces 2023
Fortune Magazine Best Workplaces in Technology™ 2023
Fortune Magazine Best Workplaces for Millennials™ 2023
Fortune Magazine Best Workplaces for Parents™ 2022
Fortune Magazine Best Workplaces for Women™ 2022
Great Place to Work® Best Workplaces in Tech™ UK 2022
Nova Scotia's Top Employer 2022, by Mediacorp Canada Inc.

The cultivation of a healthy, productive, and empowering work environment sets the foundation for our success. It's reflected in the high-quality products we bring to market, our continued innovations, and the high satisfaction of our customers, as evidenced in surveys, third-party review sites, and more.

"Everybody tries to sell you the world and then gives you a little bit. BeyondTrust is different. They have given us more than we even knew was possible."

— Tommy Green, VP of Information Systems & Technology, Amoco

"BeyondTrust pushes us to be better... From sales to support to engineering, BeyondTrust has always extended dedicated care and attention to our projects."

— David Lokke, Senior Systems Administrator, PREMIER Bankcard

"We put ourselves in a long-term position for success, implementing BeyondTrust really allowed us to give that access in a way that was much more secure for our employees and for outside agencies."

— Logan McDonald, IT Systems Analyst, Town of Truckee

Let's be honest—not every aspect of PAM will be easy.

Your environment and priorities are likely evolving. And for digital enterprises, there is never a moment in the day when cyber risk is not present and threat actors are not honing their wares.

BeyondTrust is your trusted partner.

Our people are ready to help you make sense of this environment and show you how you can best achieve your objectives.

Next Steps in Your PAM Journey

This paper has defined the capabilities required of a complete PAM platform that will help your organization build critical cyber resilience, effectively address privileged access and paths to privilege, and defend against sophisticated, identity-based attacks.

BeyondTrust is ready to be your trusted advisor on your PAM journey. We have the experience and expertise to help you make sense of how PAM solutions and capabilities can deliver on your business needs.

In the Appendix of this paper, we have two templates for you. The first template can help you make the internal business case for PAM. Use it to create alignment within your organization, as well as with your privileged access management vendor. This can help expedite internal approvals of a PAM project and get you on the right path. The second template will help you assess PAM vendors, including BeyondTrust, side-by-side across important privileged access management capabilities.

Why should you partner with BeyondTrust? Your success is our priority!

BeyondTrust adds tremendous value to customers with our integrated solution set. The result? Less cost, less complexity, and fewer gaps from using siloed tools.

- BeyondTrust is the only product vendor to address all PAM use cases—foundational + modern. Our comprehensive solution includes substantive capabilities no other vendor delivers. Our next-generation capabilities extend your line-of-sight to privileged threat pathways and identity-based attack chains, beyond what other solutions can provide.
- The breadth of our solutions and the flexibility of our approach enables you to handle today's threat scenarios and prepare for tomorrow's possibilities—no matter how your environment evolves.
- You can choose from the deployment model that best suits your needs—including cloud, virtual, or on-premises.
- Because we put you first and don't charge extra for capabilities we believe are essential, BeyondTrust maximizes your security ROI.
- With Success Included, BeyondTrust University offers complimentary, self-paced eLearning to empower system administrators with the skills to deploy and manage our products using industry best practices. We also offer instructor-led training, labs, certifications, and other training options. Learn more.
- We empower and support our people so, together, we can all be successful!

Achieve Your Security Goals with BeyondTrust

Protect the Organization

- Eliminate identity and privilege blind spots.
- Manage privileged credentials and secrets.
- Right-size all access.
- Secure a borderless workforce.
- Protect critical applications.
- Reduce the threat surface and blast radius of attacks.

Gain Efficiencies

- Leverage a true, modern platform approach.
- Automate privileged tasks.
- Achieve least privilege with least friction.
- Simplify IT workflows.
- Integrate with existing ecosystems.
- Leverage existing investments.

Attain Compliance

- Monitor and record all privileged activity.
- Leverage a centralized audit trail.
- Meet regulatory, zero trust, data privacy, and cyber insurance requirements.

Always get better with BeyondTrust. Contact us today to get started.

BeyondTrust

BeyondTrust is the global cybersecurity leader protecting Paths to Privilege™ with an identity-centric approach. We are leading the charge in transforming identity security and are trusted by 20,000 customers, including 75 of the Fortune 100, and our global ecosystem of partners.

Learn more at www.beyondtrust.com

Appendix 1: Business Case for PAM Worksheet Template

What metrics are we trying to improve / change with this project? (quantifying success)	
Why are we pursuing this outcome now and not before?	
What broader business strategy is this initiative tied to? (security, compliance, cyber insurance, zero trust, operational excellence, etc.)	
What management KPI does this project support?	
Which business unit is driving this program / project?	
How is this security risk being graded in terms of level of operational risk? (negligible, low, medium, high, severe, very severe)	
How is this security risk being graded in terms of inherent probability? (very unlikely, unlikely, likely, very likely, almost certain, certain)	
What is the specific/measurable business result making the change will deliver?	
Cost of inaction—what are we losing by not acting on this problem? (measuring risk & impact)	
How is this initiative being funded?	
What solutions are being considered?	
What decision-making governance process will this project follow?	
Description of compelling pressures / timeline of action?	
Risks to this project? (internal, external)	
What metrics are we trying to improve / change with this project? (quantifying success)	

Appendix 2: Your PAM Buyer's Guide Worksheet Template

Top Identity Security Visibility and Threat Intelligence Capabilities	BeyondTrust	Vendor A	Vendor B
Presents a centralized, holistic lens of identities and access across all your cloud and on-premises domains. This includes a clear, easy-to-understand picture of the accounts, privileges, and access associated with each identity.	✓		
Ensures continuous visibility across every user, device, and application interaction, supporting auditing and compliance.	✓		
Provides real-time insights into identity and activity that intelligently puts risk in clear context, enabling proactive detection of anomalies and threats.	✓		
Identifies problematic paths to privilege and cloud entitlements, nested permissions, and identity security misconfigurations, and assists in proactively mitigating them to improve hygiene.	✓		
Identifies overprivileged and high-risk accounts, inactive and orphaned accounts, partially revoked identities, and other security issues.	✓		
Detects and alerts on suspicious activities, including events involving multiple identities and accounts.	✓		
Correlates low-level data from a variety of leading third-party solutions to pinpoint high-risk users and assets, and identifies critical threats.	✓		
Integrates with other solutions, including PAM technologies, to unlock ITDR capabilities, enabling a rapid orchestration of security response to stop or mitigate threats.	✓		
Reports on compliance, benchmarks, threat analytics, what-if scenarios, and more.	✓		

Top Just-in-Time Access and CIEM Capabilities	BeyondTrust	Vendor A	Vendor B
Provides self-service access requests that integrate with MS Teams and Slack, meeting users where they are to simplify adoption.	✓		
Automates provisioning and de-provisioning of roles and permissions across applications, eliminating the need for manual processes.	✓		
Offers flexible approval workflows with conditions like on-call schedules, group membership, and time duration, with approvals automated or from peers, managers, or resource owners.	✓		
Bundles various permissions and roles across multiple applications into a single access request, simplifying user experiences and enhancing admin control.	✓		
Implements lifecycle permission management to grant and revoke access automatically based on attributes and group membership, removing the need for repeated access requests.	✓		
Delivers out-of-the-box integrations with popular IaaS and SaaS platforms to fit seamlessly into modern cloud environments.	✓		
Visualizes all cloud permissions and roles associated with any identity, providing complete access clarity across the organization.	✓		
Centralizes user access reviews for compliance, with automated evidence collection, templates, delegation, and reporting.	✓		
Integrates with PAM solutions to unify all temporary access management and eliminate standing privileges.	✓		

Top Privileged Remote Access Capabilities	BeyondTrust	Vendor A	Vendor B
Enforces least privilege for remote sessions by giving authorized users just-enough access to complete activities just-in-time.	✓		
Controls and monitors sessions using standard protocols for RDP, VNC, HTTP/S, and SSH connections.	✓		
Enables granular access to specific systems, improving security and eliminating "all-or-nothing" access.	✓		
Enables the user to inject credentials directly into the access session; the user never needs to know or see the credential (including accounts with MFA enabled during a Web Jump Access session).	✓		
Creates an audit trail to provide visibility into vendor activity on your network and meet compliance mandates by controlling the access pathways into IT networks used by vendors.	✓		
Manages privileged access to infrastructure and business assets that leverage web-based management consoles, including IaaS servers, hypervisor environments, and web-based configuration interfaces for core network infrastructure.	✓		
Provides seamless, out-of-the-box integrations with ITSM, SIEM, SCIM, and Password Management, as well as other common business software solutions.	✓		
Enables MFA and alternative authentication methods, such as TouchID or FaceID.	✓		

Top Privileged Identity, Account, and Credential Management Capabilities	BeyondTrust	Vendor A	Vendor B
Performs full network and cloud discovery and profiling with auto-onboarding of privileged identities and accounts of all types—including shared admin, user, application, and service accounts; SSH keys, database accounts; cloud identities and accounts (Entra ID, AWS, GCP, etc.); social media accounts; machine accounts; DevOps secrets; API keys; and RPA credentials. This also covers vendor identities and accounts.	✓		
Illuminates where and how privileged passwords are being used, revealing security blind spots and malpractice—including default, shared and/or embedded passwords, use of the same admin account across multiple service accounts, reuse of SSH keys across multiple servers, etc.).	✓		
Manages and audits access to employees' business applications, with secure folders and a browser plugin to auto-fill usernames and workforce passwords.	✓		
Manages credentials across every platform (Windows, Unix, Linux, Cloud, on-premises, etc.), directory, hardware device, application, service/daemon, firewall, router, and more.	✓		
Centralizes, secures, and encrypts all privileged credentials in a tamper-proof safe or vault. Ideally, the solution supports industry-standard encryption algorithms, such as AES 256.	✓		
Builds permission sets dynamically according to data retrieved from scans.	✓		
Implements API calls to eliminate hard-coded credentials in files, applications, scripts, and other code.	✓		
Automates rotation or expiration of passwords, SSH keys, and other secrets according to a defined schedule, including after each use for the most sensitive accounts, or in response to heightened risk or compromise.	✓		
Enforces your privileged password management policy—including password complexity, uniqueness (different passwords per asset, account, etc.), expiration, rotation, check-in and check-out, elimination of default passwords, and other rules.	✓		
Automates workflows across the entire password management lifecycle.	✓		
Enables better security for SSO and never reveals the password to the end user.	✓		
Performs rigorous session monitoring and management to ensure a clean audit of all privileged activity, and to immediately pause or stop suspicious sessions until a determination can be made regarding legitimacy.	✓		
Requires no third-party tools or Java for session management—utilizes native tools (MSTSC, PuTTY, etc.)	✓		
Enables true least privilege by enabling a security model of just-enough access and just-in-time access.	✓		
Leverages industry standards, like SAML and RADIUS, to integrate with any MFA solution.	✓		
Provides break-glass options for password check-out in the event of an emergency.	✓		
Leverages an integrated data warehouse and threat analytics across the privilege landscape.	✓		
Provides one unified, comprehensive solution to manage human (privileged users) and non-human (application, machine, service account, etc.) identities, and perform session monitoring/management.	✓		
Enables privileged task automation to reduce risk by automating multistep, repetitive tasks.	✓		
Provides comprehensive reporting and analytics for the SOC team and executive visibility into the management of privileged credentials.	✓		
Delivers enterprise-grade audit and compliance support by providing clear and distinct audit trails for all activities involving credentials under management.	✓		

Top Windows & macOS Privilege Management Capabilities	BeyondTrust	Vendor A	Vendor A
Implements true least privilege by removing standing local administrative rights across Windows and Mac desktops and Windows servers, while enabling dynamic, just-in-time elevation of privileges for specific applications and tasks.	✓		
Provides powerful yet pragmatic application control, enabling management of which applications users can install or run, with the flexibility to set both broad and granular rules through a non-resource-intensive operational process.	✓		
Enforces policy-based restrictions on software installation, usage, and OS configuration changes.	✓		
Support for macOS is not an afterthought, but a robust capability within the product itself.	✓		
Eliminates unauthorized software installations, workarounds, and gaps that could lead to exploitation.	✓		
Reports on privileged user behavior, including applications installed or run, system and configuration changes, as well as changes to critical policy or data files.	✓		
Provides a single, unimpeachable audit trail of all user activity that simplifies compliance and streamlines forensic investigations.	✓		
Simplifies operations by eliminating the need for end users to require two accounts.	✓		
Delivers an extensible end-user experience, including seamless elevation, blocking of unapproved activities, or enforcing MFA / requiring self-justification / requiring designated approver.	✓		
Provides JIT application or admin access for exception handling use cases.	✓		
Centralizes management, policy, reporting, and analytics into one streamlined solution.	✓		
Integrates with identity security, ITSM, SIEM, and other tools to enhance and embed into the existing security tech stack, improving workflows and allowing for a more comprehensive understanding of risk.	✓		
Provides a mature and complete set of APIs and webhooks for customized workflows and automation with your other toolsets.	✓		

Top Unix and Linux Privilege Management Capabilities	BeyondTrust	Vendor A	Vendor B
Enforces least privilege and eliminates use of root without hindering user productivity.	✓		
Enables JIT administration, with the ability to assign dynamic privileges to accounts and assets, while ensuring identities only have the appropriate privileges for the finite duration necessary.	✓		
Exercises granular control and audit over applications, commands, files, and scripts—protecting against malicious threats as much as against innocent errors.	✓		
Centralizes policy creation, management, and approval in one location that is separate from the endpoints requesting elevated privileges.	✓		
Records and indexes all sessions for quick discovery during audits.	✓		
Consolidates audit logs and centralizes reporting across all server domains.	✓		
Offers a powerful and flexible policy language to provide a migration path away from sudo.	✓		
Provisions and de-provisions privileges transparently, ensuring compliance satisfaction.	✓		
Offers REST API for easier integration with third-party products.	✓		
Supports many Unix and Linux platforms.	✓		
Integrates all policies, roles, and log data via a web-based console.	✓		
Integrates with identity security, ITSM, SIEM, and other privilege management products to improve workflows, better understand risk, and implement context-based privilege elevation and delegation decisions.	✓		

Top Active Directory Bridge Capabilities	BeyondTrust	Vendor A	Vendor B
Allows users to use their Active Directory credentials to gain access to Unix and Linux, consolidating various password files, NIS, and LDAP repositories into Active Directory, and removing the need to manage user accounts separately.	✓		
Enables the use of AD Group Policy Objects to manage privileges on Unix and Linux systems.	✓		
Provides integration with Linux and Unix services via PAM and Kerberos (Samba, NFS, Apache, etc.).	✓		
Adds Linux or Unix systems to the network without requiring Active Directory schema modifications.	✓		
Supports a wide range of Unix and Linux platforms (including CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, SUSE, RedHat, Solaris, and Ubuntu) and architectures such as x86_64, SPARC, PPC, PPCLE, and s390.	✓		