BeyondTrust

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

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

BeyondTrust

TABLE OF CONTENTS

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.

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.	✓		

4

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.

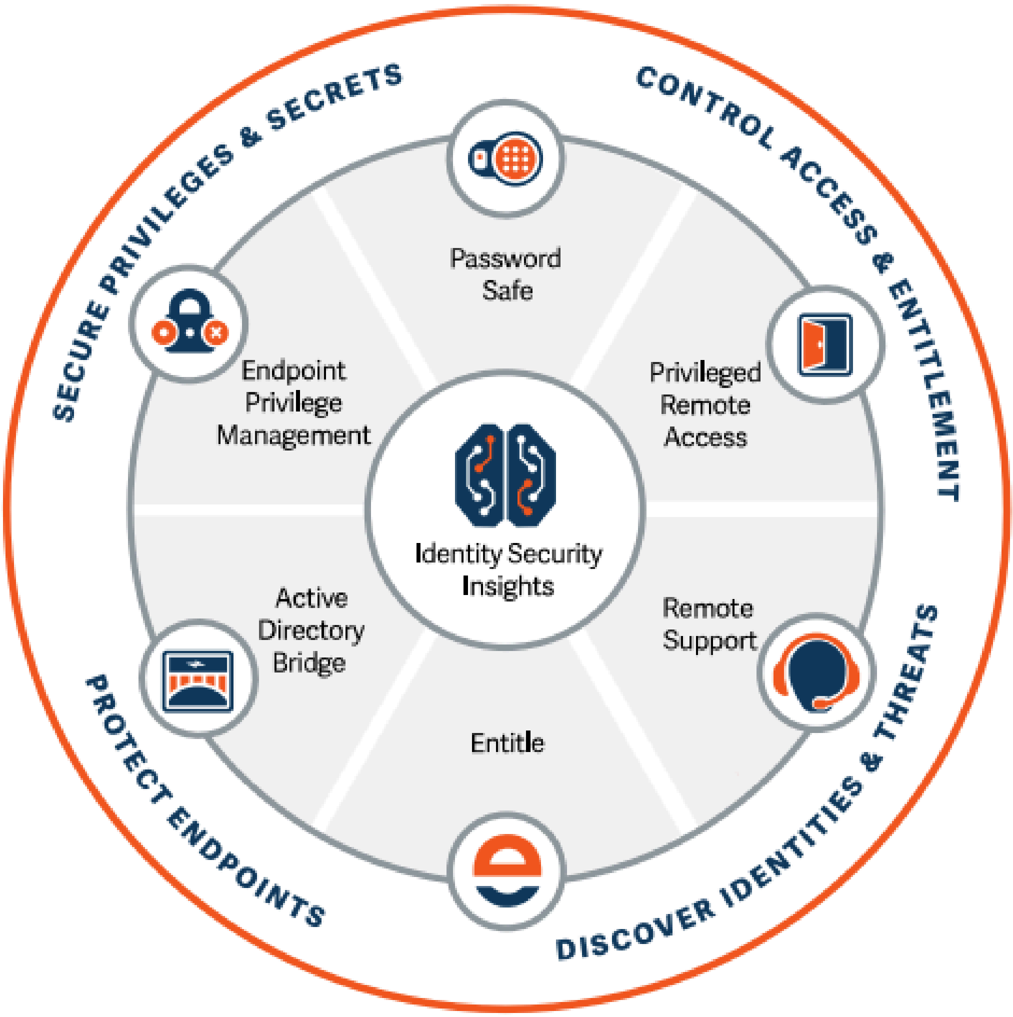
Such a solution will eliminate numerous privileged attack vectors outright, while mitigating many others, to drastically reduce enterprise security exposures. This requires a purpose-built enterprise password management or privileged credential management solution that can automate each phase of the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

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.


SECURE PRIVILEGES & SECRETS
CONTROL ACCESS & ENTITLEMENT
DISCOVER IDENTITIES & THREATS
PROTECT ENDPOINTS
Password Safe
Privileged Remote Access
Remote Support
Entitle
Active Directory Bridge
Endpoint Privilege Management
Identity Security Insights

CLOUD | HYBRID | ON-PREMISES | OT

The 7
Comp

This section of
management, p
of these areas t
compliance obj

Each core area, whe
identities, accounts
while eliminating ar
or, more commonly,
you implement, the
synergies you will s
improvements in op

Throughout the pro
requirements in mi
in the organization:

Total cost of
Does it resul
automation)

Time-to-valu
How soon do
risk? How lon

Integrations
How does it i
service desk,
synergies wit

Longevity
Will the soluti
security enab
PAM use case

BeyondTrust

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

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

o Privilege Explained

nst Microsoft,
ge that arise

OAuth
s that are
gh levels of
l Administrator

Delete Azure resources

Password reset, MFA reset

which required
ere simply over-
privileges
ud, the
stores, and

15

Get the full Buyer's Guide for Complete PAM via the link above!