BeyondTrust

Your path to effective Privileged Access Management & Identity Security should be straightforward.

> **Start here.**

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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

No identities—human or machine—are more imperative to secure than those with privileged access to systems, data, applications, and other sensitive resources.

Beyond that, PAM is also essential for protecting your entire identity infrastructure, including your backend IAM/IGA tools themselves.

Today, privileges 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 also grappling not just with more identities, but with more complex ones as well.

> What hasn't changed is that cybercriminals covet privileges/privileged access because it can expedite entry into 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. This warrants the need for identity security of all accounts.

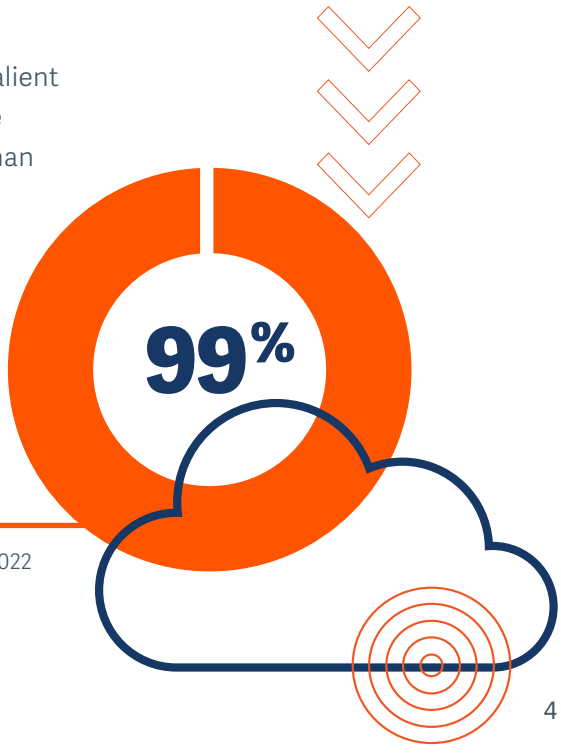
While many breaches can still be prevented by simple security fundamentals, attackers are rapidly advancing in agility beyond just simple automation. Machine Learning (M/L) and Artificial Intelligence (AI) are changing the game, vastly enhancing attacker toolsets and empowering human-operated attacks.

Generative AI is in its nascent stage, but already is helping attackers speed up their workflows while becoming more targeted and sophisticated—for instance, by utilizing multi-step social engineering exploits to impersonate identities and their attributes. And of course, it's just as important for organizations to protect their own AI and M/L data from being stolen or poisoned.

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

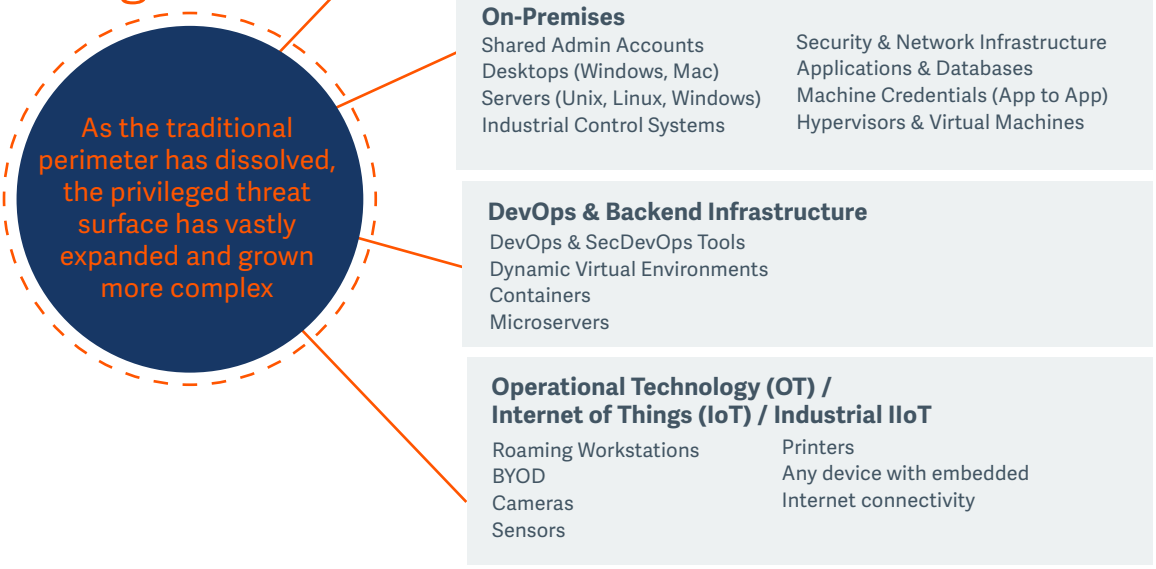
While the attack surface continues to expand and evolve, the most salient part of the story is how privileges continue to proliferate and become exposed in new ways. Identities are under attack from more angles than ever before.

>>> In **99% of pentesting cases** conducted by IBM's X-Force Red, **cloud identities were found to be over-privileged**, enabling the pentesters to quickly compromise client cloud environments.



SOURCE: IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022

The Attack Surface is Expanding



Identity-Based Security Challenges
At a Glance

More Cloud, Multicloud, and Bring Your Own Cloud (BYOC)
40,000+ types of cloud permissions to manage[1]

More Vulnerabilities
540% increase in cloud vulnerabilities over the past 6 years[2]
159% increase in Azure and Dynamics 365 vulnerabilities in 2022[3]

More Remote Access
76% of cloud accounts for sale on the dark web are for RDP access[4]

More Identities (human, machine, etc.)
98% of security professionals say the number of identities are increasing, primarily driven by cloud adoption, third-party relationships, and machine identities

More Privileges
95% of machine identities are overprivileged[5]
In **99% of pentesting cases**, cloud identities were found to be over-privileged[6]

More Connectedness to Everything
93% of OT security pros say their organizations had at least one OT system intrusion incident in the last 12 months; 78% had 3+; **61% of the intrusions impacted OT systems**[7]

More Identity-based incidents and breaches
90% of security professionals said they experienced an identity-related incident in the past year[8]

1. 2023 State of Cloud Permissions Risks Report. Microsoft Security. March 2023.
2. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022.
3. Microsoft Vulnerabilities Report. BeyondTrust. March 2023.
4. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022.
5. Gartner. Innovation Insight for CIEM, June 2021.
6. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022
7. 2022 State of Operational Technology and Cybersecurity Report. Fortinet. June 2022.
8. IDSA 2023 Trends in Securing Digital Identities. May 30, 2023

Attackers are using smarter tools. So should you.

PAM stands at the core of identity security.

Today, effective security against privilege and other identity-based threats requires blending preventative and detective capabilities. Thus, today's complete PAM solution should not only prevent threats, but also provide intelligent detection capabilities as well. To use an analogy of home security—it's no longer about using just locks and key codes, but smart motion sensors, too.

Where do you start?

Controlling, monitoring, and auditing privileges and privileged access—for employees, vendors, systems, applications, IoT, and everything else that touches your IT environments—is essential for protecting against both external and internal threat vectors, and for meeting a growing list of compliance requirements.

But where do *you* start?

Is remote access the biggest area of risk? Or are privileged credentials? What about end-user machines? Perhaps the Linux servers where your sensitive data and operations, including your own AI, is hosted? And once you've started, how do you know what areas to focus on next?

This PAM Buyer's Guide will help you answer just that – where to begin your privileged access management (PAM) project, how to progress to a better security posture, and what business outcomes to expect. We will start with the PAM basics that will mitigate most risks. Then, we'll delve into other significant use cases, finishing with emerging use cases you should know.

Our experience over many thousands of deployments has shown that there is a fairly typical path most customers follow, but 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**
Manual processes for managing privileged passwords, including spreadsheets or physical safes		Automated password and session management of all privileged accounts
Most users have administrator access on their machines		Rules-based least privilege implemented organization-wide, on all systems and machines
Lack of auditing and control over root accounts and 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 access		Granular, flexible control ensures remote access is extended only to the required resources for authorized vendors and employees
No singular, clear picture of threats or what to do about them		Complete visibility over identities and attack paths to proactively mitigate threats
Disorganized and chaotic directory services infrastructure, with multiple logons required and inconsistent policy 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
Impeded user productivity and 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**

Evolving beyond the basics to improve 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 & Next-Generation Identity & Access Security

By evolving your PAM and identity security capabilities, you not only reduce the threat surface, eliminate security gaps, improve your response capabilities to attacks, and make compliance and cyber insurance qualification easier—you also deter many attackers who seek to exploit the easiest prey.

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

1. **Improve** Accountability and Control Over Privileged Identities, Accounts, and Passwords
2. **Secure** Remote Access for Employees, Vendors, Contractors, and Infrastructure
3. **Implement** Least Privilege and Application Control for Windows and macOS
4. **Implement** Least Privilege and Audit Access Across Unix and Linux Servers and Desktops
5. **Streamline** Identity Management and Security by Integrating Unix and Linux into Windows
6. **Gain** Visibility and Threat Intelligence on All Identities to Proactively Mitigate Risk

The 6 Key Steps *for* Complete Privilege Management

This section of the white paper 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 activity 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 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 privileged access management solution, **keep in mind these business requirements**, as they will help you articulate the value of this program to those higher 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, 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 capabilities to meet the PAM use cases of tomorrow?

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

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 any file needed to start and maintain DevOps systems, such as JSON and XML files. According to Forrester Research, these privileged credentials are implicated in 80% of data breaches[9].

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 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. Even some 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 administrator productivity, workflows, and processes?

9. The Forrester Wave™: Privileged Identity Management, Q4 2020

Goal

An automated, comprehensive solution to seamlessly discover the ever-expanding list of privileged accounts and credential types in your environment (both human and non-human), place those accounts and credentials under management, and satisfy auditor requests.

Such a solution will eliminate some privileged attack vectors outright while mitigating many others, thus drastically reducing enterprise security exposures. This requires a purpose-built enterprise password management or privileged credential management solution that can automate each phase of the password lifecycle consistently 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 unmatched 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, eliminating embedded credentials in scripts and code.

Real-Time Session Management
Log and monitor all privileged credential activity and sessions for compliance and forensic review.

Advanced Auditing & Forensics
Leverage extensive privilege and credential analytics to simplify compliance, benchmark tracking, and more.

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 may be able to scale to manage tens of thousands, or even hundreds of thousands of privileged user credentials. Fewer still can also manage high numbers of SSH keys or secrets used by non-human users. If it is important to you to monitor and manage all privileged sessions (and it should be), understand that only a couple elite vendors can monitor/manage hundreds of thousands of concurrent sessions. Only BeyondTrust delivers all these capabilities and meets the enterprise needs of scale across the board and across any environment.

How adverse are you to security complexity, solution overlap, and security vendor redundancies?
As Gartner noted in its Magic Quadrant for PAM, many security vendors sell various components of privileged account and credential management separately—each with their own distinct management console. Of course, there are also niche security vendors that offer standalone capabilities for SSH key management, application password management, or secrets management.

BeyondTrust provides a single, complete solution to manage, monitor, and audit all types of privileged credentials in a centralized and unified way.

If utilizing other leading vendors, this would require purchasing up to six different solutions!

"This is the first time we have ever implemented a security product that made the end user's job so much easier. Our building managers previously managed dozens of different credentials for staff and vendors. Password Safe centrally manages every credential, so they now have only one password for them, one password for vendors, and one password for their staff."

Curtis Jack, Manager of Technical Engineering,
Oxford Properties Group

KEY STEP

2

Secure Remote Access for Employees, Vendors, Contractors, and Infrastructure

Remote access pathways have long been weak points for most organizations. Today's era of elevated remote work and distributed workforces provides ample opportunity for attackers. Researchers have consistently found that between 50-80% of ransomware attacks gain an initial foothold by exploiting Remote Desktop Protocol (RDP)[10]. According to an IBM X-Force Report, 76% of cloud accounts for sale enable RDP access[10].

Third-party vendors and internal employees alike (including cloud ops engineers, developers, and other distributed workers) need the right level of access to effectively do their jobs. IT admins need the ability to effectively manage, grant, and elevate privileges.

Organizations often lack visibility into what vendors and remote workers are doing when they access their network. VPNs provide far too much access for what is usually required, putting networks and identities at risk. Most other remote access solutions also share similar weaknesses to VPNs, including:

- All-or-nothing access, with a lack of granular security settings
- No visibility into or record of user activity—meaning no audit trails
- A lack of support across diverse operating systems and use cases

With these shortcomings, a single compromised account can quickly and easily take down your entire network.

When you consider the scale of your organization and the security risk of dozens or hundreds of third parties on your network, it's plainly apparent how critical this deficiency is.

With so many remote access points—and typically sub-optimal visibility, auditing, and security controls over this access—it's just a matter of time before a weak link across the remote access surface is compromised via an employee or a third-party vendor.

10. IBM Security, 2022 IBM Security X-Force Cloud Threat Landscape Report, 2022

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

Goal

Eliminate "all-or-nothing" remote access for vendors and other remote workers by implementing granular, role-based access to specific systems with defined session parameters. Allow vendors or internal users access to specific systems, for an allotted time, for specific applications or purposes. Administrators can approve or deny access requests from anywhere and for any device across major platforms.

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.

Privileged Remote Access facilitates the remote access users need while ensuring sensitive data is protected and compliance mandates (PCI, HIPAA, ISO, GDPR, etc.) are satisfied.

You can deploy the Privileged Remote Access solution on-premises via a hardened physical or virtual appliance, or through a secure cloud. Provision access to and from machinery, laptops, mobile devices, and operational technology (OT) endpoints.

This solution 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.

The cloud solution can manage over 5,000 Windows credentials and can store up to 10,000. For more comprehensive credential management capabilities, **Privileged Remote Access seamlessly 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 known credentials.

Infrastructure Access
Empower your cloud developers and DevOps engineers with no-hassle secure connectivity, authentication, and auditability across infrastructure.

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

Note that BeyondTrust is the only Privileged Access Management or identity security vendor with mature capabilities for extending privileged access security best practices to vendors, other third parties, and remote workers, all in one solution.

Our closest competitors have only recently started to begin building these essential PAM capabilities.

"With BeyondTrust's Privileged Remote Access solution, we can make sure that access to any part of our infrastructure is impossible unless we say so... We can enforce a policy of least privilege by giving just the right level of access needed for their role; plus, the ability to schedule when vendors have access to which systems and for how long."

Curtis Jack, Manager of Technical Engineering,
Oxford Properties Group

KEY STEP

3

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 least privilege. How? By eliminating local admin rights on end-user machines. If you have Windows servers, least privilege also requires establishing proper privileged access for your various Administrator accounts, including Network, Microsoft Exchanges Active Directory, Database, Developers, Help Desk, IT Staff/Power Users, and others.

With a least privilege approach, users only receive permissions to the systems, applications, and data they need based on their current role. Rather than having privileges enabled and always on (and thus, always ripe for misuse or abuse), privileges are only elevated on an as-needed basis. By defaulting most users to standard users and only elevating privileges as needed, you drastically reduce the threat surface, sharply curtail your susceptibility to lateral movement, and minimize the risk of successful phishing and ransomware threats. By tightly controlling and auditing admin access, you help guarantee your most sensitive company assets are protected.

Relying on native and ad hoc in-house toolsets to restrict or enable end-user privileges is onerous and time consuming. Moreover, although users should not be granted local administrator or power user privileges in the first place, sometimes certain applications require elevated privileges to run.

"Historically, 75% of critical Microsoft vulnerabilities could have been mitigated by removing admin rights."

Microsoft Vulnerabilities Report 2023, **BeyondTrust**

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

Goal

Efficiently eliminate local admin rights across Windows and macOS systems, tightly control and audit admin access to servers and sensitive systems, and enforce granular control over applications—all without hindering end-user productivity. Enterprise endpoint privilege management solutions need to be able to remove end-user privileges while automating rules-based technology to elevate application privileges—without ever elevating user privileges themselves.

Solution

BeyondTrust Privilege Management for Windows and Mac enforces least privilege and simplifies compliance across physical and virtual Microsoft Windows desktops, servers, and macOS desktops while also improving end-user productivity.

Top 3 Use Cases

Zero Trust Security Across Windows & Mac
Remove local admin rights and enforce true least privilege across Windows and macOS desktops and servers.

Attack & Fileless Threat Protection
Reduce your cyberattack surface and protect against malware, ransomware, and phishing attacks.

Audit & Compliance Assurance
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 will require a complex service arrangement, while others can show a demonstrable risk reduction and decrease help desk tickets in just 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 unified solution that can enforce least privilege and application control best practices across all your endpoints – Windows, Unix, Linux, macOS, ICS, SCADA, IoT, and network devices included?

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

The solution provides a strong ROI by closing identity and access security gaps, reducing security-related help desk tickets, and expediting the path towards meeting compliance objectives.

Out-of-the-box Quick Start policies honed from thousands of deployments enable organizations to make leaps in risk reduction, fast. The solution's unique Trusted Application Protection capability (Windows only) even stops tricky fileless attacks by leveraging built-in, context-based controls to catch bad scripts, infected attachments, and control child processes and DLLs.

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

"We've got a team of six engineers who manage the entire desktop and mobile estate, so we needed something that was really going to empower them to get the job done in as quick and efficient a way as we can. Using Privilege Management for Windows and Mac really opened doors to allow us to do that. "

Ryan Powell, Operations & Response Centre Manager,
University of Derby

KEY STEP

4 Implement Least Privilege and Audit Access Across Unix and Linux Servers and Desktops

Business-critical, Tier-1 applications running on Unix and Linux 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 may be necessary for IT administrators to do their jobs. Unfortunately, this practice presents significant security risks stemming from intentional, accidental, or indirect misuse of privileges.

Native, open source, and ad hoc tools are often used to "get by." But in server environments with even modest complexity, you end up paying a high price for these "free" tools in several ways. Some shortcomings of sudo and other basic tools include:

- Deficiencies in oversight, forensics, and auditing, including a lack of file integrity monitoring, log securing, or the ability to record sessions and keystrokes for audits.
- Serious gaps in security. These tools don't account for activity inside scripts and third-party applications, leaving shortcuts to unapproved applications. Native OS tools also lack the ability to delegate authorization without disclosing passwords.
- Administrative complexity and lack of scalability. Policies typically need to be managed on each individual server when using sudo or other basic tools.
- Lack of enterprise support.
- No efficient migration path away from sudo, if it is being used.

With sudo and other tools, it's virtually impossible to maintain best-practice security and compliance in all but the most primitive 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 visibility and control over all privileged activities across Unix and Linux, consistent enforcement of least privilege, efficient delegation of Unix and Linux privileges, and authorization—all without disclosing passwords for root or other accounts. Gain the ability to either do away with sudo outright—or make the most of sudo by layering on enterprise capabilities that resolve security and auditing deficiencies to make administration simpler and less error-prone.

Solution

BeyondTrust Privilege Management for Unix & Linux is the leading solution for Unix and Linux privileged access security. This solution helps you achieve control over Unix/Linux root account privileges with centralized analytics, reporting, and keystroke logging. Use it to reduce risk and achieve compliance faster than with native tools or sudo.

Top 3 Use Cases

Root Access Control
Apply fine-grained privilege elevation rules to execute only specific tasks or commands.

Activity Tracking & Auditing
Protect against unauthorized changes to files, scripts, and directories with advanced auditing of all user activity.

Real-Time Session Monitoring
Detect suspicious user, account, and asset activity in real time with monitoring of all logs and sessions.

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

Other Considerations

Do you also have Windows servers and desktop endpoints? Would you prefer having one vendor and platform to implement PAM across all your endpoints?

Is it important for you to have the ability to enable single sign-on (SSO) across your heterogeneous infrastructure and unify policy management across Unix, Linux, macOS, and Windows?

If improving PAM coverage and reducing complexity is important to you, there are only a couple vendors that can meet your needs.

By enabling just-in-time privilege management (and thereby eliminating persistent privileged access), Privilege Management for Unix & Linux sharply limits the time an account possesses elevated privileges and access rights.

This drastically 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 a low total cost of ownership (TCO) compared to alternatives. This is achieved by centralizing the privileged account management under a single pane of glass, drastically reducing the time and effort needed to achieve security and audit objectives.

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.

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

Ryan Powell, Operations & Response Centre Manager,
University of Derby

5 Streamline Identity Management and Security by Integrating Unix and Linux into Windows

Once you have greater control over privileged access in Unix and Linux environments, the next logical step is to bring those systems under consistent management, policy, and single sign-on. Unix and Linux have traditionally been managed as standalone systems – each a silo with its own set of users, groups, access control policies, configuration files, and passwords to remember. Managing a heterogeneous environment containing these silos – in addition to the Microsoft environment – leads to inconsistent administration for IT, unnecessary complexity for end users, and added risk to the business.

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

Goal

Centralized authentication for Windows, Unix, and Linux environments that reduces the risks and complexities of managing a heterogeneous environment. Improve efficiencies by reducing the number of logins (and the resulting help desk calls when they are forgotten) and the number of different systems, configurations, and policies to manage. This requires an Active Directory Bridging solution to streamline management of user identities.

Solution

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

By centralizing the management of logins and configurations and leveraging your Windows Active Directory infrastructure, BeyondTrust AD Bridge expedites your achievement of identity security and audit objectives while boosting productivity for users and server administrators.

Top 3 Use Cases

Unified Management of Identities
Apply fine-grained privilege elevation rules to execute only specific tasks or commands.

Auditing & Compliance
Provide audit details to compliance teams, and centrally manage group policies.

Enhanced Unix / Linux Security
Expand single sign-on (SSO), file sharing, and security policies and control access to non-Windows 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**

6 Gain Visibility and Threat Intelligence on All Identities to Proactively Mitigate Risk

Organizations are struggling to protect themselves in large part due to two trends. The first is that the size of digital estates and attack surfaces are increasing, while their threat visibility is decreasing. The second is the rapid explosion of human and machine identities and the proliferation of new access paths to critical systems and data that has left most security teams with poor visibility into threats and other security exposures.

Many organizations today use more than two dozen systems to manage identities and access rights, adding another layer of complexity and further expanding the attack surface. What's more, many of these IAM/IGA systems themselves are ripe targets for attack.

When the identity management system itself becomes compromised, it then becomes a simple exercise for an attacker to infiltrate the environment at great scale.

On the other hand, IT and security professionals are already overloaded with vulnerability and threat data. Unfortunately, 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. 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. AI-driven attacks are already proving more evasive and harder to pinpoint.

Organizations lack a centralized view of identities, accounts, and privileged access across their IT estate. Generally, more fractured and siloed visibility translates into:

- Heightened risk of solutions not integrating or communicating well with each other, resulting in downtime, security gaps, and frustration.
- Persistently higher administrative burden.
- Delayed orchestration in response to threats.
- Inability to satisfy auditors or address forensic requests in a timely manner, if at all.
- Security risks to the identity infrastructure itself.

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

Goal

A holistic, intelligent view of all identities and access across your entire multicloud and on-premises estate —all to gain a clearer picture of risks. Benefit from the ability to see new attack paths that were previously undetectable in a siloed environment. Promote identity hygiene with actionable recommendations before they become a threat. Detect identity-based threats and proactively respond. Accelerate threat investigations and get results quicker. Understand complex attack chains, attack paths, and the blast radius of compromised identities and accounts. Marshall the intelligence needed to orchestrate the optimal response to a threat or breach.

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, privileges, and access — revealing their exact impact on your security posture.

Identity Security Insights ushers in groundbreaking levels of identity and threat intelligence to the BeyondTrust portfolio, and makes all BeyondTrust products and connected solutions significantly more intelligent and powerful.

Get intelligent, actionable analytics your teams can leverage to immediately improve your security posture and eliminate potentially dangerous backdoors and weak spots.

Identity Security Insights combines with other BeyondTrust solutions and third-party data sources (including Okta and Azure Active Directory) to leverage correlated data of users, accounts, and privileges, while also unlocking powerful ITDR capabilities. Apply guided recommendations driven by holistic identity intel, rated by importance, to ensure least privilege access. No other solution provides as comprehensive a view into privilege and identity-based weaknesses, while also identifying the privileges that open attack paths and present backdoors to sensitive assets.

This solution 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.

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 threat surface.

Nearly every emerging technology with the power to transform IT comes with security challenges, such as how to manage identity and authentication models and privileges. These present the types of 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 touch on several important areas that have emerged in recent years that can present unique challenges.

Specialized Identity & Access Security and Business Cases for PAM

In this section, learn how 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

DevOps

Most organizations today have adopted DevOps practices. Yet, security is often an afterthought, or even a casualty, of the speed and tools (often open source) used within 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 gaps.

Some common DevOps security gaps 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 privileges across the DevOps landscape.
- Sharing of secrets.
- Vulnerabilities, misconfigurations, and other weaknesses in containers.

While it's clear that security 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 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 DevOp and CI/CD environments:

- Inventories and auto-onboards all DevOps assets and automated workflows for increased visibility and support for audit and compliance.
- Finds, secures, and centrally manages the use of all hardcoded 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 deploy, configure, and remediate production issues on machines and images.
- Applies application control to ensure 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 dev, 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 while maintaining peak development agility.

Operational Technology, IoT, and Non-Traditional Endpoints

Internet of Things (IoT) has gone mainstream in enterprises. Other non-traditional endpoints are also pervasive across most organizations today.

These endpoints often lack basic security features, frequently have default and hardcoded or embedded credentials, may have firmware that is difficult to patch or update, and carry with them many 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. Additionally, many ICS vendors now use standard IT technologies within their solutions, making them more accessible to attacks.

Legacy tools typically lack the ability to uncover, onboard, and securely manage diverse device types and their access—let alone at scale. This results in dangerous security exposures scattered across OT and IT environments. Mirai and other botnets, which caused widespread disruption and brought some businesses to a standstill, are just the tip of what can occur from lapses in security for IoT devices. Compromises of OT systems could lead to catastrophic damage to infrastructure and jeopardize many human lives.

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

BeyondTrust was first-to-market with a PAM solution to offer granular command control and audit over privileged user activity on network, IoT, and OT (ICS, SCADA, etc.) 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 improving 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 for all endpoints and access.
- 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 any SSH or Telnet device.
- Supports the Purdue Model and zero trust.

Moreover, BeyondTrust lets you implement our technologies in any order, which is often needed for OT environments.

" The majority of the systems within the buildings being accessed are not traditional IT systems. They are building control systems, like smart elevators, surveillance systems, and HVAC units, where it is not possible to install antivirus software. We recognize that privileged access management is one of the most important tenets of a modern cybersecurity program and a must-have for a zero trust architecture and robust BYOD security framework."

Curtis Jack, Manager of Technical Engineering,
Oxford Properties Group

Robotic Process Automation

Robotic process automation (RPA) is a fast-emerging and evolving method of using software robots to eliminate 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 or hardcode credentials in order to quickly establish connections for automation.

BeyondTrust can extend Privileged Access Management best practices to your Robotic Process Automation implementation.

BeyondTrust PAM capabilities for improving RPA security:

- Scans, identifies, profiles, dynamically categorizes, and auto-onboards all assets that may be included in an RPA workflow, and supporting resources.
- Enforces best practices for password management, including eliminating hardcoded or embedded RPA credentials, and secures the organization from automated exploitation via an extensive, RPA-compatible API.
- Ensures that passwords can be automatically reset after RPA usage to ensure the security of the workflow.
- Enforces least privilege and granular control across RPA processes, toolsets, and workflows.
- Locks down access 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 their qualification criteria, increased rates, and even dropped coverage for many organizations. This comes largely in response to a surge in costly cyberattacks and ransom payouts.

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 laptops and desktops and enforces least privilege.
- 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 for an extra layer of security for remote access.
- Provides blended protection to block or mitigate ransomware attacks.

LEARN MORE

Addressing cyber insurance requirements and getting the best rates with BeyondTrust:

Download: Cybersecurity Insurance Checklist
Visit: Cyber Insurance Solutions & Education Hub

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

Zero Trust

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

Zero trust principles and architectures aim to eliminate persistent trust, enforce continuous authentication, least privilege, and adaptive access control, and apply segmentation and microsegmentation for 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 any threats to the network.

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 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.
- 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 for accounts.
- Applies least privilege controls to right-size access for every identity and account—human, application, machine, employee, vendor, etc.
- 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.
- 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

Learn more about how BeyondTrust addresses zero trust:

Learn how to bridge NIST zero trust principles to real-world privileged access management (PAM) and secure remote access product capabilities. Learn practical implementation steps and architectures.

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

Watch: Oxford Properties Group - Creating a Zero Trust Cyber Security Strategy for Multiple Sites

Visit: Solutions to Operationalize Zero Trust & 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

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 solution offering, 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, the completeness of our solution, our technological innovation and vision, and our centralized management platform.

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

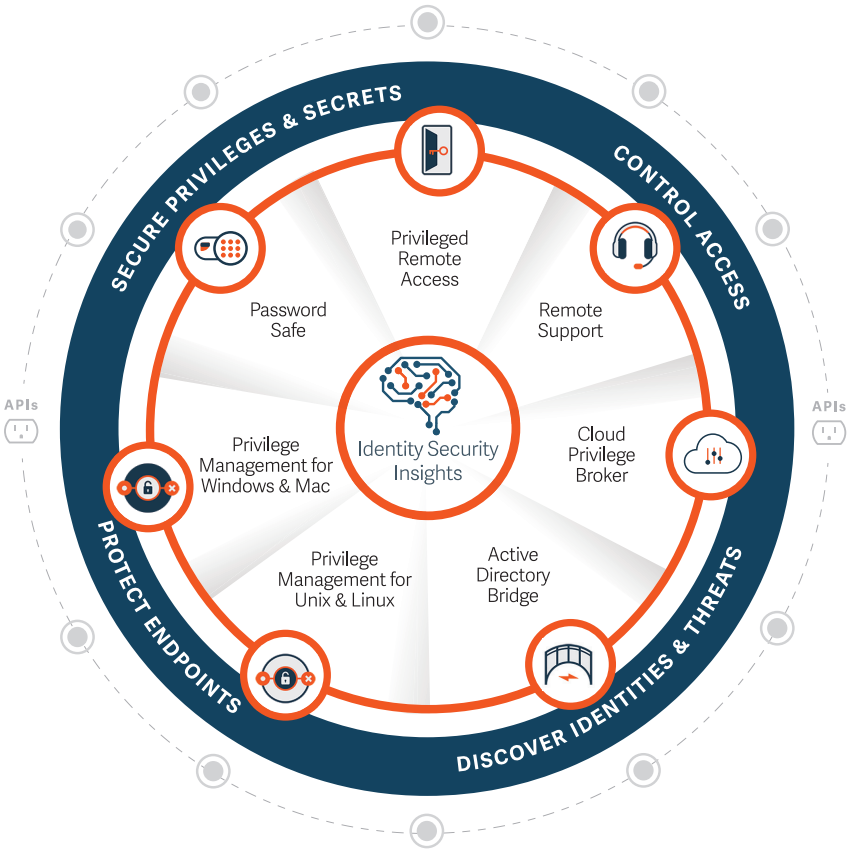
BeyondTrust uniquely blends three disciplines together — PAM, CIEM, & ITDR — to help organizations holistically strengthen their Identity Security and account for every plane of privilege.

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 at once, or to phase in capabilities over time at your own pace. While you can start with a password vault (Password Safe), you don't have to. You could just as easily start with Privileged Remote Access, AD Bridge, or Privilege Management for Windows & macOS or Unix & Linux.

We also give you the choice of deployment model that best suits your needs— cloud, virtual or on-premises appliances.

No PAM vendor provides more deployment options.

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



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

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

BeyondTrust is also committed to delivering digital accessibility, and we take proactive steps to ensure that our products adhere to the standards of the Web Content Accessibility Guidelines (WCAG) 2.0 level AA via a third-party audit and internal training.

Intelligent UX 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 across 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:

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

Minimizes 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.

Improves 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 and leverage internal user feedback, in conjunction with external user feedback, to continually improve the UX.

Unique Features to 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

For instance, starting a privileged session with BeyondTrust is faster and simpler than with competitor tools, and ensures the most robust security and auditing controls are in place.

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

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

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.

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

"Security needs to be seamless, just a part of the normal flow. It shouldn't stop a user in their tracks. For security to stick, it needs to be designed effectively, or else you'll inadvertently introduce even more risk."

Angela Duggan, VP of User Experience,
BeyondTrust

LEARN MORE

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 PAM & Identity Security

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 and has pioneered many of the must-have PAM capabilities that have come to define today's PAM space. **And we're not stopping.**

Our remote access security solutions for insiders and vendors were launched years ahead of alternative offerings. It's probably because we supported remote work and work-from-anywhere (WFA) for our employees well before it became commonplace.

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.

Some BeyondTrust innovations, many of them patented, include:

- 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.
- First to integrate robust remote access security that truly extends PAM and identity security best practices to vendors and remote workers.
- First to offer a true integrated platform for all core PAM use cases across every major platform (Windows, macOS, Unix, Linux).
- First PAM solution to provide granular command control and audit overprivileged user activity on network, IoT, ICS, and SCADA devices—providing coverage over all endpoints.

BeyondTrust is first-to-market with many major innovations for Unix/Linux privileged access management, including:

- Advanced audit and control (ACA) technology that audits activities inside scripts, controls file and folder access (even for root), and blocks malicious and compromised binaries.
- Registry Name Services, 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.
- File integrity monitoring, which ensures that the 'things' you allow to be elevated, and the processes that perform the elevation, have not been compromised.
- First PAM platform to be available on the AWS Marketplace, first available on the Microsoft Azure Marketplace, and first available on Google Cloud.
- First privileged access management (PAM) solution to be enabled for complete Managed Service Provider (MSP) deployments—whether on-premises or cloud.

BeyondTrust is the first (and only) product vendor to combine traditional PAM with CIEM and ITDR for holistic visibility, prevention, detection, and remediation capabilities 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.

Today, BeyondTrust continues to trailblaze with our expansive vision and roadmap.

We're aggressively pushing to solve emerging and future customer needs with the launch of our groundbreaking Identity Security Insights solution, as well as enhancements to our existing solutions, so they're always best-of-class in features, capabilities, and usability.

Differentiator 4: Integrations and Interoperability

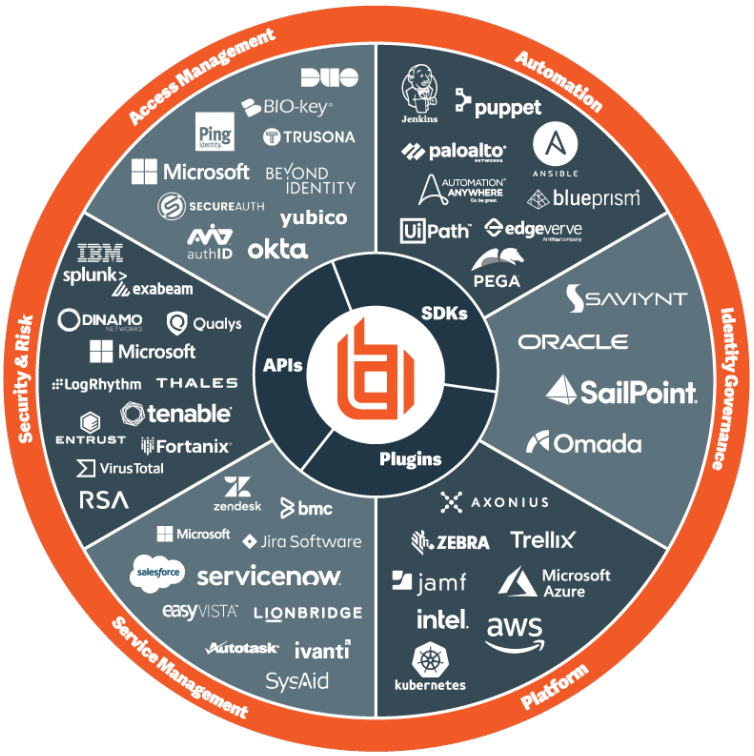
BeyondTrust's solutions and platform are elegantly architected to make integrations with important third-party tools as seamless and as complementary as possible. The last thing we think you need is another siloed security point solution.

BeyondTrust empowers you with a holistic understanding of the modern 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.



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.

2022 Gartner® Magic Quadrant™ for Privileged Access Management
2023 KuppingerCole Leadership Compass: Privileged Access Management
The Forrester Wave™: Privileged Identity Management, Q4 2020

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.

We have received the distinction of Gartner Peer Insights Customers' Choice for Privileged Access Management for the past two years running.

You can check what our customers have to say about us on the Gartner Peer Insights platform, where we have 450+ five-star verified customer reviews.

Differentiator 6:
Proven BeyondTrust Experience & Global Presence

More than 20,000 customers rely on BeyondTrust solutions, which are backed by our 1,500+ employees across 20+ countries and an extensive global partner network.

We understand that each of our customers has unique needs and requirements, and with over 1000+ 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 both security and compliance 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

55
Market Leading NPS Score

95%
CSAT for Customer Experience

"We love working with BeyondTrust for their strong focus on ensuring customer success and satisfaction."

Senior Manager of Authentication Services,
Manufacturing Industry Customer
Gartner Peer Insights

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 annually recognized as one of the top places to work. Fortune Magazine and Great Place to Work rank us as the "#22 Best Workplace in Technology (Large)."

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

Recent Recognition of Beyondtrust Exceptional Workplace Culture and Employee Experience

Inc. Magazine Best Workplaces 2022
Fortune Magazine Best Workplaces in Technology™ 2022
Fortune Magazine Best Workplaces for Women™ 2022
Fortune Magazine Best Workplaces for Parents™ 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.

Let's be honest—not every aspect of PAM and identity security 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 and Identity Security Journey

This paper has defined the capabilities required of a complete privileged access management solution. This solution goes well beyond traditional PAM to incorporate the CIEM and ITDR capabilities necessary to survive in a world with proliferating planes of privileges, commonplace remote access, and sophisticated, rapid-fire attacks, such as those leveraging AI.

BeyondTrust is ready to be your trusted advisor on your PAM journey. We have the experience and expertise 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 PAM 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?

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 Privileged Access Management use cases. Our comprehensive solution includes substantive capabilities no other vendor delivers. Our next-generation capabilities extend your line-of-site 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 offerings enable you to handle today's threat scenarios and prepare for tomorrow's possibilities.
- You can choose from the deployment model that best suits your needs – including cloud, virtual, or on-premises appliances. No other PAM vendor provides more choices.
- Because we put you first and don't charge extra for capabilities that we believe are essential, BeyondTrust maximizes your security ROI.
- We empower and support our people so that, together, we can all be successful.

Achieve Your Security Goals with BeyondTrust

Prevent Breaches

- Reduce the attack surface
- Prevent ransomware attacks
- Protect privileged access and remove admin rights
- Eliminate excessive privileges
- Secure critical applications and implement application control

Gain Efficiencies

- Simplify IT workflows
- Automate privileged tasks
- Integrate with existing ecosystem
- Leverage existing investments

Attain Compliance

- Enforce least privilege
- Meet regulatory, zero trust, and data privacy requirements
- Deliver granular permissions
- Monitor and record all privileged activity
- Leverage a centralized audit trail

Enable & Protect Business

- Gain visibility over all privileged and remote access
- Eliminate VPN for privileged users
- Implement just-in-time access controls
- Enable help desk and remote support diagnostics and troubleshooting

BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BeyondTrust protects all privileged identities, access, and endpoints across your IT environment from security threats while creating a superior user experience and operational efficiencies. With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 75 of the Fortune 100, and a global partner network.

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 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 (Azure AD, etc.); social media accounts; machine accounts; DevOps secrets; API keys; and robotic process automation (RPA) credentials. This also includes 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 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 embedded or hard-coded credentials in files, applications, scripts, and other code.	✔		
Automates the rotation of passwords, SSH keys, and other secrets according to a defined schedule, including after each use for the most sensitive accounts, or for accounts facing heightened security 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.	✔		
Provides granular access control.	✔		
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 additional third-party tools or Java for session management—utilizes native tools (MSTSC, PuTTY) instead.	✔		
Enables true least privilege by enabling a security model of just-enough access and just-in-time access.	✔		
Features a modern, uncluttered user interface (HTML5) for end users that simplifies adoption and administration.	✔		
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 that includes session monitoring/management – no requirement for multiple/different interfaces, or to be charged separately for each.	✔		
Enables privileged task automation to reduce risk by automating multistep, repetitive tasks.	✔		
Provides comprehensive reporting and analytics for 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 Privileged Remote Access Capabilities

	BeyondTrust	Vendor A	Vendor B
Enforces least privilege by giving authorized users just-enough access to complete activities just-in-time for remote sessions.	✔		
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.	✔		
Leverages industry standards,like SAML and RADIUS, to integrate with any MFA tool.	✔		

Top Windows & macOS Privilege Management Capabilities

	BeyondTrust	Vendor A	Vendor B
Implements true least privilege by removing standing local administrative rights across desktop and server users while enabling dynamic, just-in-time elevation of privileges for specific applications and tasks.	✔		
Provides powerful 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.	✔		
Sets policies via Active Directory Group Policy and Web Services with support for air-gapped systems and non-domain assets.	✔		
Eliminates unauthorized software installations, workarounds, or 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.	✔		
Allows for granular control over the access and permissions of APIs, extending the principle of least privilege to API accounts.	✔		
Provides a technique for using real domain or local privileges when required.	✔		
Centralizes management, policy, reporting, and analytics into one streamlined solution.	✔		
Integrates with identity security, ITSM, SIEM, and other privilege management tools to enhance and embed into the existing security tech stack, improving workflows and allowing for a more comprehensive understanding of risk.	✔		

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 just-in-time administration (JIT) with the ability to assign dynamic privileges to accounts and assets, while ensuring identities only have the appropriate privileges when necessary and for a limited amount of time.	✔		
Exercises granular control and audit over applications, commands, files, and scripts – protecting against malicious threats as much as against innocent errors.	✔		
Records and indexes all sessions for quick discovery during audits.	✔		
Adaptively enforces full keystroke logging for the most sensitive sessions.	✔		
Provides a clear view and clean audit trail into who is doing what — and where.	✔		
Consolidates audit logs and centralizes reporting across all server domains.	✔		
Supports Pluggable Authentication Module to enable utilization of industry-standard authentication systems.	✔		
Offers a powerful and flexible policy language to provide a migration path away from sudo.	✔		
Provisions and de-provisions privileges transparently, ensuring compliance satisfaction.	✔		
Includes file integrity monitoring to protect critical files and binaries from tampering.	✔		
Offers REST API for easier integration with third-party products.	✔		
Has extensive support for many Unix and Linux platforms.	✔		
Integrates all policies, roles, and log data via a web-based console.	✔		
Leverages an integrated data warehouse and threat analytics across the privilege landscape.	✔		
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
Features a single sign-on for any enterprise application that supports Kerberos or LDAP.	✔		
Provides a single, familiar toolset to manage both Windows and Unix/Linux systems (ex: Active Directory users and computers, ADUC).	✔		
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.	✔		
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.	✔		
Provides a pluggable framework with an interface similar to Microsoft's Management Console on Linux.	✔		
Supports a wide range of Unix and Linux platforms, including CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, SUSE, RedHat, Solaris, Ubuntu, and architectures such as x86_64, SPARC, PPC, PPCLE, and s390.	✔		
Supports compliance with SOX, PCI, HIPAA, and other regulations.	✔		
Leverages industry standards, like SAML and RADIUS, to integrate with any MFA tool.	✔		

Top Identity Security Visibility and Threat Intelligence Capabilities	BeyondTrust	Vendor A	Vendor B
Provides a centralized, holistic lens of identities and access across your multicloud and on-premises estate.	✔		
Provides a clear, easy-to-understand picture of the accounts, privileges, and access associated with each identity.	✔		
Identifies problematic privileges and multicloud entitlements and helps you right-size them.	✔		
Identifies potential security misconfigurations and assists in proactively mitigating them.	✔		
Identifies overprivileged and high-risk privileged 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.	✔		
Illuminates and makes sense of identity-based risk, including the potential blast radius of each account and identity—enabling you to take decisive action.	✔		
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 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.	✔		