BeyondTrust

Your path to effective Privileged Access Management should be straightforward.

› **Start here.**

Buyer's Guide *for* Complete

Privileged Access Management (PAM)

TABLE OF CONTENTS

How to Use This Buyer's Guide

Today, privileges are built into operating systems, file systems, applications, databases, hypervisors, cloud management platforms, DevOps tools, robotic automation processes, and more. Cybercriminals covet privileges/privileged access because it can expedite access to an organization's most sensitive targets. With privileged credentials and access in their clutches, a cyberattacker or piece of malware essentially becomes an "insider".

The Attack Surface is Expanding

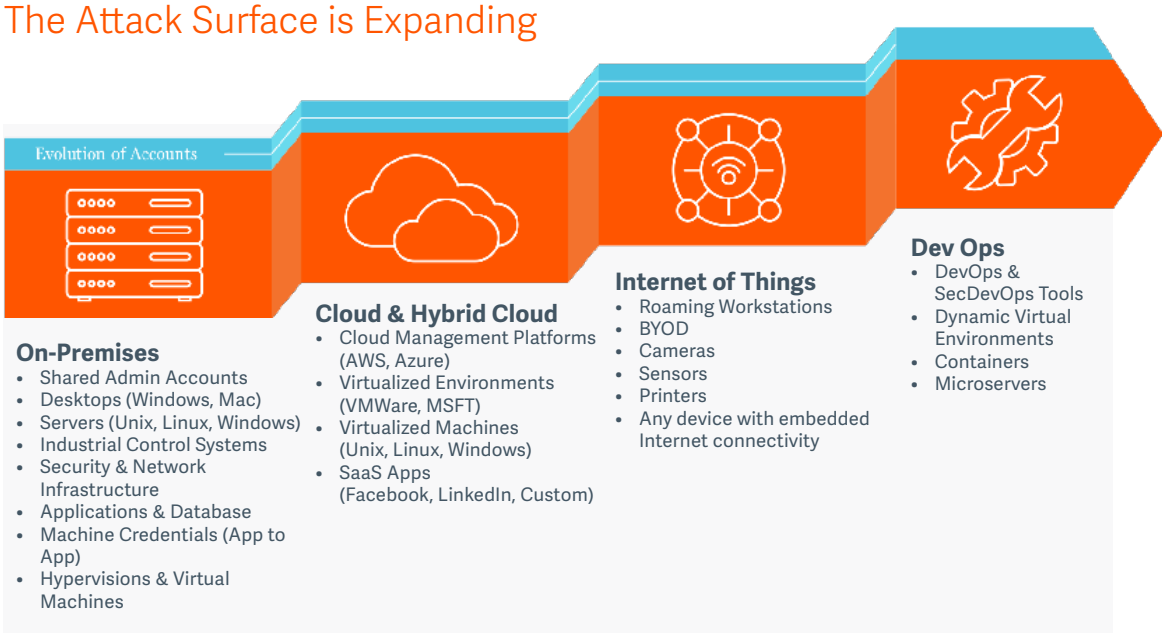

FIGURE 1: As the traditional perimeter has dissolved, the privileged threat surface has vastly expanded and grown more complex.

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 Unix the biggest area of risk? Or are privileged credentials? What about end-user machines? 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 delve into the other significant use cases, and finish with emerging and edge use cases.

Our experience over many thousands of deployments has shown that there is a fairly typical path that most customers follow, but, ultimately, your next steps with PAM are a risk-based decision based on the needs of your organization. With the right vendors and partners, your path to effective privileged access management should be straightforward.

Privilege Problems for Environments Without PAM	→	PAM End-State 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		Integrated threat analytics to improve decision-making
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**

FIGURE 2: 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

By evolving your PAM capabilities, you not only reduce the threat surface, eliminate security gaps, improve your response capabilities to attacks, and make compliance easier, you also deter many attackers, who are still largely opportunistic in seeking to exploit the easiest prey.

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

7 Steps for Complete Privilege Management

This section of the white paper identifies seven core areas for privileged access management, presenting the key capabilities you should seek across each of these areas.

Each core area, when implemented, will give you greater control and accountability over the accounts, assets, users, systems, and activity that comprise your privilege 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 of these areas you implement, the more PAM synergies you will see, and the more impactful the reduction in enterprise risk and the operational improvements.

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 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 re-deploy 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? If it only works well as a standalone/point solution, it's probably only a stopgap versus a long-term solution. On the other hand, if the solution has synergies with your existing security solutions, it will also help you maximize existing investments.
- **Longevity** – Will the solution vendor grow with you or even pull you towards growth through security enablement? Is the vendor resourced to evolve capabilities and deepen feature-richness to meet the PAM use cases of tomorrow?

01

Improve Accountability & Control Over Privileged Passwords

The most logical starting point for gaining greater control over privileges is improving accountability over privileged credentials. According to Forrester Research, privileged credentials are implicated in 80% of data breaches.

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

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

How do organizations ensure security and accountability over all the different types of credentials that allow privileged access—without disrupting administrator productivity or other workflows and processes?

Goal: An automated, comprehensive solution to seamlessly discover the ever-expanding list of privileged accounts/credential types (both human and non-human) in your environment, place those accounts/credentials under management, and satisfy auditor requests that they are adequately managed. Such a solution will outright eliminate some privileged attack vectors, while mitigating many others, helping to drastically reduce enterprise security exposures. This requires a purpose-built enterprise password management/privileged credential management solution that can automate each phase of the password lifecycle consistent with your security policies.

Top Privileged Credential Management Capabilities

- ☐ **Performs full network scanning, discovery, and profiling** with auto-onboarding of privileged accounts of all types (shared admin, user, application, and service accounts, SSH keys, database accounts, cloud and social media accounts, machine, DevOps, robotic process automation credentials—including by third-parties/vendors.
- ☐ **Illuminates where and how privileged passwords are being used,** revealing security blind spots and malpractice (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-prem, etc.), directory, hardware device, application, services/daemons, firewalls, routers, etc.
- ☐ **Centralizes, secures, and encrypts all privileged credentials** in a tamper-proof safe/vault. (Ideally the solution supports industry-standard encryption algorithms, such as AES 256.)**Builds**
- ☐ **permission sets dynamically** according to data from scans.
- ☐ **Implements API calls** to eliminate embedded/hard-coded credentials in files, applications, scripts, and other code.
- ☐ **Automates rotation of password, SSH keys, and other secrets** according to a defined schedule, including after each use for the most sensitive accounts, or for those accounts facing heightened security risk or compromise.
- ☐ **Enforces your privileged password management policy,** such as 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 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.
- ☐ **Has 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 checkout.
- ☐ **Leverages an integrated data warehouse** and threat analytics across the privilege landscape.
- ☐ **Provides one, unified, comprehensive solution** to manage human (privileged users) and non-person (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.
- ☐ **Flexible deployment options:** hardware appliances, virtual appliances, or software

Other considerations: How important is scale? Do you have just a few thousand privileged credentials, or many hundreds of thousands? 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. And, if it is important to you (it should be) to monitor and manage all privileged sessions, understand that just a couple, elite vendors can monitor/manage hundreds of thousands of concurrent sessions. And, only BeyondTrust delivers all of these capabilities and meets the enterprise needs of scale across the board and across any environment.

Another consideration - how adverse are you to security complexity, solution overlap, and security vendor redundancies? On average, organizations use four different methods for privileged credential management. As Gartner noted in its Magic Quadrant for PAM, many security vendors sell various components of privileged credential management separately—each with their own management console. Of course, there are also niche security vendors that may offer standalone capabilities for SSH key management or 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. For some of the other leading vendors, this will require purchasing up to six different solutions!

Solution: BeyondTrust Password Safe unifies privileged password and privileged session management, providing comprehensive discovery, management, auditing, and monitoring for any privileged account/credential—human, application, machine, etc., effectively reducing the risk of privilege credentials misuse and addressing compliance requirements. The solution provides unmatched threat analytics (such as correlating anomalous privileged user behavior, and third-party data to determine threat criticality) and reporting.

02

Implement Least Privilege & Application Control For Windows & Mac

Once privileged credentials and accounts are being consistently discovered, onboarded, and managed, the next step to complete privileged access management is implementing least privilege on end-user machines by eliminating local admin rights. If you have Windows servers, you also want to dial in the proper privileged access for your various Administrator accounts (Network, Microsoft Exchanges Active Directory, Database, Developers, Help Desk, IT Staff/Power Users, etc.).

> From 2015 -2020, 75% of Critical Microsoft vulnerabilities could have been mitigated by removing admin rights.
>
> **MICROSOFT VULNERABILITIES REPORT 2022, BEYONDTRUST**

With a least-privilege approach, users receive permissions only to the systems, applications, and data they need based on their current role. Rather than having privileges enabled and always-on, thus always ripe for misuse or abuse, the 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 the ability for lateral movement, and minimize the risk of threats, such as phishing and ransomware, to land and expand. By tightly controlling and auditing admin access, you also ensure your most sensitive assets are protected.

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

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/permissions?

Goal: The ability to 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. This requires enterprise endpoint privilege management solutions that remove end-user privileges, while automating rules-based technology to elevate application privileges—without ever elevating user privileges.

Top Windows & Mac Least-Privilege Capabilities

- ☐ **Defaults all desktop and server users to standard privileges,** while enabling elevated privileges for specific applications and tasks—without requiring administrative credentials.
- ☐ **Layers on powerful application control** to implement trust-based application whitelisting, with the flexibility to set both broad and granular rules.
- ☐ **Enforces restrictions** on software installation, usage, and OS configuration changes.
- ☐ **Eliminates the need for end users to require two accounts.**
- ☐ **Enforces least-privilege decisions** for applications dynamically based on the application's real-time vulnerability risk.
- ☐ **Matches applications to rules automatically** based on asset-based policies; Leverages smart rules for alerting and grouping of devices and events.
- ☐ **Monitors sessions, captures screens, and logs keystrokes** during privileged access.
- ☐ **Audits and reports on changes** to critical policy, system, application and data files, eliminating unauthorized software installs, workarounds, or gaps that could lead to exploit.
- ☐ **Provides a technique** for using real domain or local privileges when required.
- ☐ **Enables true least privilege** by enabling a security model of just-enough access and just-in-time access.
- ☐ **Provides a single, unimpeachable audit trail** of all user activity that speeds forensics and simplifies compliance.
- ☐ **Centralizes management, policy, reporting, and analytics.**
- ☐ **Integrates with other privilege management modules** to achieve comprehensive privileged access management.
- ☐ **Leverages an integrated data warehouse** and analytics across the privilege landscape.
- ☐ **Analyzes user behavior** by collecting, storing, and indexing keystroke logs, session recordings, and other privileged events.
- ☐ **Sets policies** via Active Directory Group Policy, Web Services, or McAfee ePO, with support for air-gapped systems and non-domain assets.

Other considerations: How important is the solution's time-to-value for you? Some solutions will require a complex services arrangement, while others can show a demonstrable risk reduction and slash help desk tickets in just weeks.

Another consideration – do you have a Unix/Linux server estate, or non-traditional endpoints that touch your network? Many vendors that offer Windows least privilege capabilities lack similar capabilities for Unix, Linux, and macOS, let alone non-traditional endpoints. Wouldn't you rather have one unified solution that could enforce least privilege and application control best-practices across all your endpoints – Windows, Unix, Linux, Mac, ICS, SCADA, IoT, network devices, etc.? BeyondTrust is the only vendor that can meet all of these needs.

Solution: BeyondTrust Privilege Management for Windows and Mac (part of BeyondTrust Endpoint Privilege Management) enforces least-privilege access and simplifies compliance across physical and virtual Microsoft Windows desktops and servers and macOS desktops—and is completely invisible and frictionless to the end user. The solution provides a strong ROI by closing security gaps, improving operational efficiency by reducing security-related help desk tickets, and expediting the path to compliance objectives. Additionally, the solution can be more quickly implemented than competitor solutions, while also offering deeper capabilities, and providing a quick time-to-value.

03

Secure Remote Access for Vendors & Employees

Remote access pathways represent the weakest links for most organizations—and cybercriminals know it.

IT administrators, insiders, and third-party vendors need privileged access to do their jobs effectively; they also need the ability to elevate privileges. Organizations often lack visibility into what vendors are doing when they access their network. VPNs provide far too much access than is usually required. Most other remote access solutions also share similar pitfalls as VPN, including:

- Lack of granular security settings
- Inability to provide a comprehensive audit trail
- Lack of support across diverse operating systems and use cases

> 93% of respondents say they have suffered a direct cybersecurity breach because of weaknesses in their supply chain.
>
> **MANAGING CYBER RISK ACROSS THE EXTENDED VENDOR ECOSYSTEM, BLUE VOYANT. 2021**

These are all serious shortcomings. And when you consider the scale of the problem, it's plainly apparent how critical this deficiency is. As the published research from BeyondTrust's Privileged Access Threat Study found, on average, organizations have 182 third-party vendors logging into their systems/networks, in a typical week. 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 in across the remote access surface is compromised—either via an employee or a third-party vendor.

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

Goal: Eliminate "all or nothing" remote access for vendors by implementing granular, role-based access to specific systems and 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 any device, to anywhere and across major platforms.

Top Privileged Remote Access Capabilities

- ☐ **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. (Includes accounts with MFA enabled during a Web Jump Access session).
- ☐ **Creates an audit trail** to provide visibility into vendor activity on your network, as well as meet compliance mandates, by controlling the access pathways into IT networks used by vendors.
- ☐ **Manages privileged access to business assets** that leverage web-based management consoles, including IaaS servers, hypervisor environments, and web-based configuration interfaces for core network infrastructure.
- ☐ **Integrates with existing tools** such as SIEM, Change Management, SCIM, and Password Management.
- ☐ **Provides seamless, out-of-the-box integrations** with ITSM, SIEM, and SCIM as well as other common business software solutions.
- ☐ **Leverages TouchID/FaceID** for authentication into the privileged remote access mobile console.
- ☐ **Leverages industry standards** like SAML and RADIUS to integrate with any Multi-Factor Authentication (MFA) tool

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 employees, contractors, and third-party vendors—without a VPN. Privileged Remote Access helps organizations protect sensitive data and meet compliance mandates. (PCI, HIPAA, ISO, GDPR, etc.). You can deploy the Privileged Remote Access solution on-premises via a hardened physical or virtual appliance, or through a secure cloud. The solution also has a credential management vault, that protects privileged credentials with discovery, management, rotation, auditing, and monitoring for privileged accounts – from local or domain shared administrator, to a user's personal admin account – even SSH keys, cloud, and social media accounts. The cloud-ready vault SaaS solution can manage over 5,000 Windows credentials and can store up to 10,000.

Note that BeyondTrust is the only PAM vendor with mature capabilities for extending privileged access security best practices to vendors, other third parties, and remote workers. Our closest competitors are only recently starting to play catch up in building these important capabilities.

04

Implement Least Privilege & Audit Access Across Unix & Linux Server Environments

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

Having root passwords, superuser status, or other elevated privileges is important for IT admins 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. For instance, some dangerous, or at least onerous, shortcomings of sudo and other basic tools include:

- Unsettling deficiencies in oversight, forensics, and auditing: lack of file integrity monitoring, log securing, or the ability to record sessions and keystrokes for audits
- Serious gaps in security: For instance, these tools don't account for activity inside scripts and third-party applications, leaving a shortcut 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
- Don't offer an 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/Linux environments are far too high.

Goal: 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 without disclosing passwords for root or other accounts. 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, and make administration simpler and less prone to error.

Top Unix & Linux Server Privilege Management Capabilities

- ☐ **Enforces least privilege** and eliminates use of Root.
- ☐ **Enables just-in-time administration (JIT),** which is the ability to assign dynamic privileges to accounts and assets to ensure 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.
- ☐ **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.
- ☐ **Consolidates audit logs** and centralizes reporting across all your 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 from sudo.
- ☐ **Provisions/de-provisions privileges transparently,** helping to ensure compliance.
- ☐ **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.

Other considerations: Do you also have Windows servers and desktop endpoints? Would you prefer one vendor and platform to implement PAM across all your endpoints, or are you fine relying on different vendors and management consoles for different OS. Also, is it important for you to be able to enable single sign on 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.

Solution: BeyondTrust Privilege Management for Unix & Linux (part of BeyondTrust Endpoint Privilege Management) is the gold-standard solution for Unix/Linux privileged access security. The solution helps you achieve control over Unix/Linux root account privileges with centralized analytics and reporting, and keystroke logging. With it, you can reduce risk and achieve compliance faster than with native tools or sudo. By enabling just-in-time privilege management (thereby eliminating persistent privileged access), it sharply limits the time an account possesses elevated privileges and access rights to drastically reduce the window of vulnerability during which time a threat actor can exploit account privileges. While this is by far the industry's most powerful Unix/Linux PAM solution, it provides a low total cost of ownership (TCO) compared to alternatives due to centralizing the management of privileged accounts under a

single pane of glass and taking less time to achieve security and audit objectives. Privilege Management for Unix & Linux can increase the security, accountability, and productivity for users and server administrators, without the risk of open
source sudo.

05

Leverage User, Asset & Application-Level Risk to Make Better Privilege Decisions

Once privileged credentials are under management, and end users have the privileges they need to perform their jobs – and nothing more – you can progress to leveraging real-time vulnerability data to make better-informed privilege elevation decisions. For instance, if an application is running with a vulnerability, should you permit it access to perform a highly sensitive operation? The answer may vary based on the unique contextual factors in your environment. For this to be actionable, it requires the ability to do at least three things:

1. Know where the vulnerability exists
2. Understand how the risk changes depending on what assets the vulnerable application interacts with and what privileges it elevates – and where all these scenarios fall within your risk appetite
3. The ability to orchestrate a response, in real-time, that is consistent with your policies and risk appetite

But how do you accomplish this at the enormous scale most organizations would demand?

Goal: Seamless integration of automated privilege elevation/delegation capabilities with vulnerability, risk, and threat intelligence to make smarter privileged access decisions.

Top Capabilities for Making Privilege Elevation/Delegation Actions Based on Real-Time Risk

- ☐ **Assesses real-time threat levels** to the user, requested asset, and the application launched.
- ☐ **Takes runtime actions for applications and processes** based on the rules and policies that you create (i.e. allow privilege escalation, remove administrative permissions, or prevent an application from launching).
- ☐ **Uncovers emerging risks** by identifying and reporting on the types of activities that might be at risk.
- ☐ **Enables advanced privilege elevation and delegation workflows** to undertake remedial measures that proactively eliminate the potential threats, such as session termination or heightened logging, auditing, and review for the privileged session.

Solution: BeyondTrust's Endpoint Privilege Management (includes Privilege Management for Windows & Mac, and Privilege Management for Unix & Linux products) and BeyondInsight work together in an integrated fashion to automatically scan applications for vulnerabilities at runtime – triggering alerts, reducing application privileges, or preventing launch altogether based on policy. BeyondInsight is the industry's most innovative and comprehensive privileged access management platform. It provides a holistic view of privileged vulnerabilities that provide doors into an environment, as well as the privileges that present corridors to sensitive assets. By centralizing risk and threat intelligence, BeyondInsight helps provide a "universal" awareness and enforcement approach to privilege management.

06

Unify & Centralize Privilege Management, Policy, Reporting & Threat Analytics Under a Single Pane of Glass

It's no secret that IT and security professionals are overloaded with privilege, vulnerability, and attack information. Unfortunately, advanced persistent threats (APTs) often go undetected because traditional security analytics solutions are unable to correlate diverse data to discern 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.

Generally, the more point tools you have—each with different administrative interfaces and built with different code—translates into:

- Heightened risk that your solutions won't integrate or communicate well with each other – resulting in downtime, security gaps, and frustration
- Steeper learning curves for your administrators
- Persistently higher administrative burden
- Delayed orchestration in response to threats

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 view of risk with advanced threat analytics that enables IT and security professionals to rapidly identify data breach threats—whether sophisticated or typical. This includes the ability to pinpoint specific, high-risk users and assets by correlating low-level privilege, vulnerability, and threat data from a variety of third-party solutions.

Top Management & Threat Analytics Capabilities

- ☐ **Groups, assesses, & reports on assets** by IP range, naming convention, OS, domain, applications, business function, Active Directory, and more.
- ☐ **Enables rapid orchestration of security response** to stop or mitigate threats.
- ☐ **Enables import from Active Directory** or to set custom permissions.
- ☐ **Correlates low-level data** from a variety of leading third-party solutions to uncover critical threats.
- ☐ **Correlates system activity** against a constantly updated malware database.
- ☐ **Reports on compliance,** benchmarks, threat analytics, what-if scenarios, resource requirements, and more.
- ☐ **Presents, sorts, and filters historical data** for multiple perspectives.
- ☐ **Locates network (local & remote),** web, mobile, cloud and virtual assets, as well as privileged accounts.
- ☐ **Profiles IP, DNS, OS,** Mac address, users, accounts, password ages, ports, services, software, processes, hardware, event logs, etc.
- ☐ **Provides workflows, ticketing, and notifications** to coordinate IT and security teams.
- ☐ **Shares data** with leading SIEM, GRC, NMS, and help desk solutions.

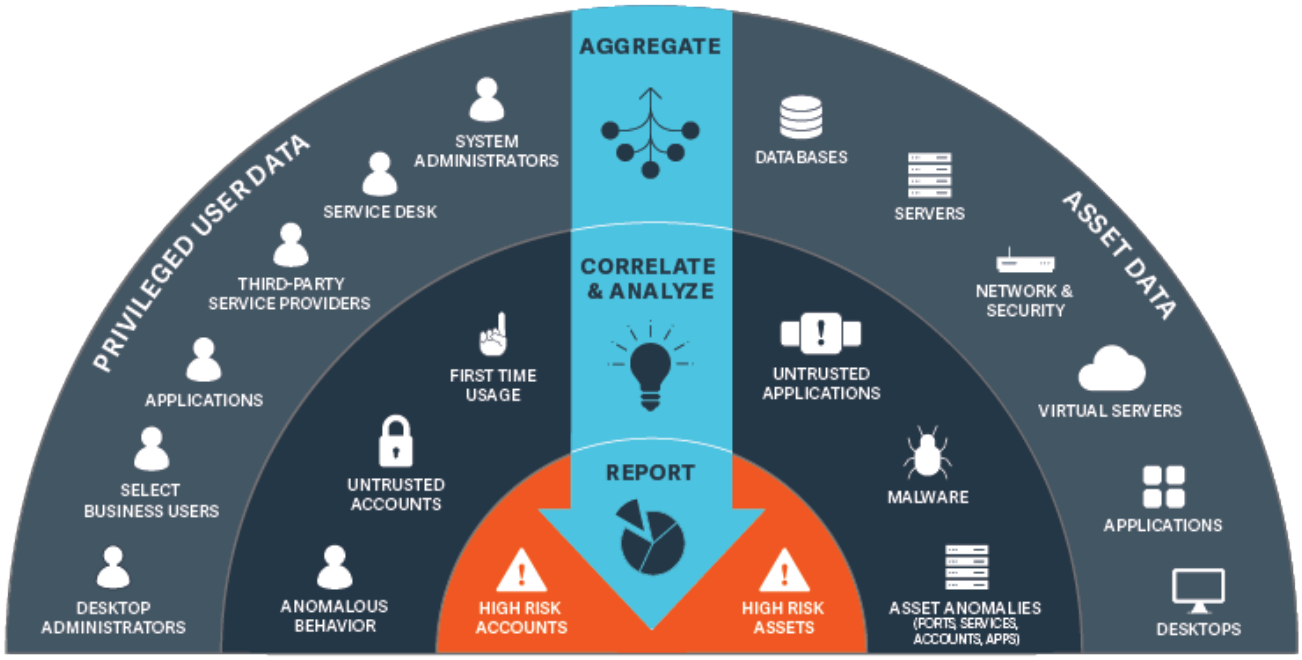

FIGURE 3: Integrated threat analytics and management for privileges and external vulnerabilities

Solution: BeyondTrust privileged access management solutions are unified and centralized via our BeyondInsight platform, enabling centralized management and policy control. BeyondInsight provides integrated capabilities such as asset discovery, profiling, smart groups, threat analytics, reporting, and connectors to third-party systems. BeyondInsight empowers IT and security teams with a single, contextual lens through which to view and address privilege risk.

07

Integrate Unix, Linux & MacOS 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, Linux, and macOS 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 that contains these silos – plus the Microsoft environment – leads to inconsistent administration for IT, unnecessary complexity for end users, and 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, Linux, and macOS environments to reduce the risk and complexity of managing a heterogeneous environment. Improved efficiencies by reducing the number of logins (and the accordant 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.

Top Active Directory Bridge Capabilities

- ☐ **Single sign-on** for any enterprise application that supports Kerberos or LDAP.
- ☐ **A single, familiar tool set** 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, Linux, and macOS, consolidating various password files, NIS and LDAP repositories into Active Directory and removing the need to manage user accounts separately.
- ☐ **Does not require Active Directory schema modifications** to add Linux, Unix, or macOS systems to the network.
- ☐ **Provides a pluggable framework** with an interface similar to Microsoft's Management Console on Linux or macOS (Full support for Apple's Workgroup Manager application would allow for seamless management and control of macOS system settings.).
- ☐ **Supports a wide range of Unix, Linux, and macOS platforms** (CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, Suse, RedHat, Solaris, Ubuntu, etc.).
- ☐ **Supports compliance with SOX, PCI, HIPAA,** and other regulations.
- ☐ **Works as part of a broad privileged access management solution family.**

Solution: BeyondTrust AD Bridge (part of BeyondTrust's Endpoint Privilege Management solution) extends Microsoft Active Directory's Kerberos authentication, single sign-on, and Group Policy configuration management capabilities to Unix, Linux, and Mac systems to improve efficiency, simplify compliance, and reduce risk. By centralizing the management of logins and configurations and allowing you to leverage your Windows Active Directory infrastructure, BeyondTrust AD Bridge expedites your achievement of security and audit objectives, while boosting productivity for users and server administrators.

PAM for Emerging & Edge Use Cases

By executing well on the proceeding 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.

The BeyondTrust PAM platform has a flexible design that enables it to adapt to your evolving needs and tomorrow's challenges. While there are many edge use cases BeyondTrust solutions can meet that are not covered in this paper, let's briefly touch on three important areas that have emerged in recent years that can present unique challenges.

DevOps

Most organizations today have adopted DevOps practices. Yet, security is often an afterthought, or even a casualty, of the speed and tools—which are often open-source—used in DevOps environments.

While DevOps achieves condensed development cycles through automation, and frequently, leveraging the scale of the cloud, the downside is that it can also "automate insecurity", creating massive security, compliance and operational gaps. Some common DevOps risks include:

- Insecure 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?

Solution: BeyondTrust PAM solutions reduce risks throughout the IT supply chain by improving visibility and control over secrets, admin privileges, and system configurations and vulnerabilities. By uniting these capabilities across on-prem, virtual, cloud, and DevOps use cases, IT organizations can achieve their agility goals without burdensome processes. BeyondTrust DevOps Secrets Safe enables secure, centralized management and auditing of secrets and other privileged credentials used by applications, tools, and other non-human identities. The solution enables IT, security, and DevOps teams to drive peak agility while controlling credentials and other secrets used across the CI/CD toolchain, including passwords, keys, certificates, applications, and other automated processes. BeyondTrust EndPoint Privilege Management enforces least privilege and application control throughout your entire environment. Working together, BeyondTrust solutions giving you full PAM coverage across your DevOps landscape:

- Inventories all DevOps assets.
- Finds, secures, and centrally manages the use of all hardcoded passwords and shared secrets (including developer access to source code, DevOps tools, scripts, test servers, and production builds)
- Enforces least privilege - granting only required permissions to appropriately build machines and images, and deploy, configure, and remediate production issues on machines and images
- Enforces boundaries between dev, test, and production systems
- Unites all features into a single platform for management

Non-traditional endpoints (IoT / IIoT, ICS, SCADA, and network devices)

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, the devices were never actually designed with 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 protect their mission-critical functions and to ensure the safety of the surrounding communities and the 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 have typically lacked the ability to uncover, onboard, and securely manage all of these diverse device types—let alone at scale. The result is many dangerous security exposures sprawled across the IT environment. Mirai and other botnets, which caused widespread disruption and brought some businesses to a standstill, are just the tip of what can result lapses in security for IoT devices. Compromises of ICS and SCADA devices could lead to catastrophic damage to infrastructure and put many human lives in jeopardy.

How can organizations consistently account for and secure—at tremendous scale—the ever-increasing number of non-traditional endpoints, from IoT / industrial IoT (IIoT) devices, SCADA, ICS, and even common network devices (routers, switches, firewalls)?

BeyondTrust was first-to-market with a PAM solution to offer granular command control and audit over privileged user activity on network, IoT, ICS. and SCADA devices, adding this capability to the BeyondTrust privileged access management platform and providing coverage over all endpoints. With BeyondTrust's integrated PAM suite, you can extend PAM best practices to these non-traditional endpoints. Our platform:

- Discovers and onboards all devices for management
- Enforces password management best practices, such as eliminating embedded/hardcoded credentials and securing credentials in a centralized, tamper-proof vault
- Applies fine-grained least privilege control, allowing you to control what commands users can run
- 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

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 other IT resources. However, RPA security controls are often inadequate. For instance, RPA toolsets typically have excessive rights, and embed, or hardcode, credentials in order to establish connections for automation.

BeyondTrust can extend best PAM practices to your RPA implementation. For instance, the BeyondTrust PAM platform integrated with DevOps Secrets Safe and Endpoint Privilege Management:

- 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 only authorized applications

What Sets BeyondTrust Apart

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 diversity of available 3rd party integrations, and the fact that we are a proven leader and innovator with a decades long-history of innovation. Only BeyondTrust offers a universal privilege management approach that secures every user, session, and endpoint across your entire privilege universe.

DIFFERENTIATOR #1:

Breadth, Depth, & Flexibility of Our PAM Platform

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions available in the market. In its 2018 Magic Quadrant for Privileged Access Management, research firm Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

From establishing and enforcing true least privilege on Windows, Mac, Unix, and Linux systems; to automating password and session management; to securing remote access for employees and third-parties, to integrating Unix, Linux, and macOS systems with Microsoft Active Directory; to auditing user and administrator activity, BeyondTrust unifies these capabilities into a single, integrated platform that acts as a central policy manager and primary reporting interface.

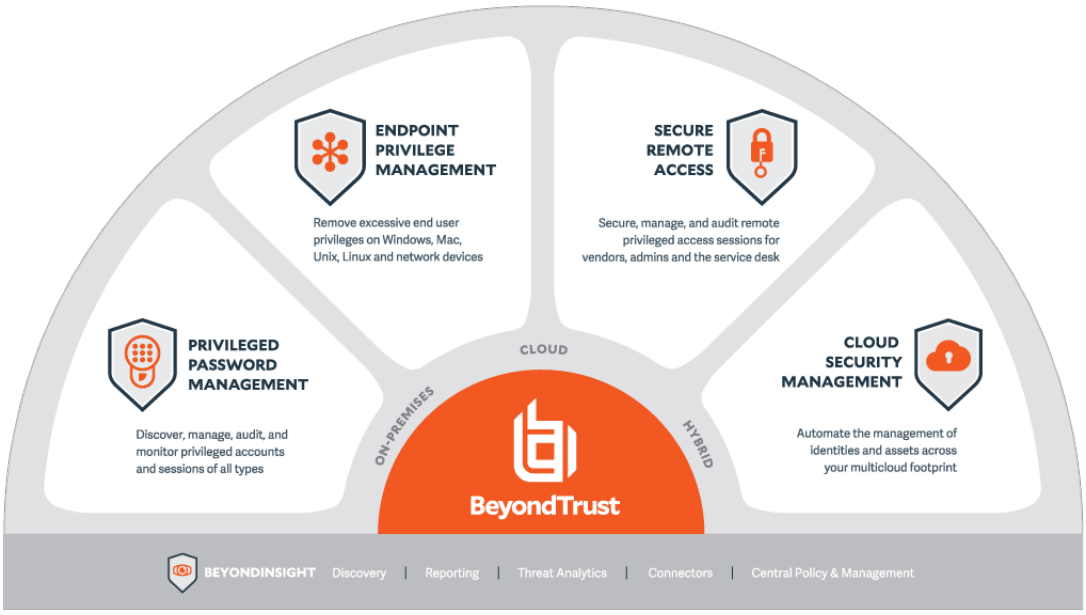

FIGURE 4: The BeyondTrust Platform

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.

DIFFERENTIATOR #2:

Security Innovator - Revolutionizing PAM

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

Some BeyondTrust PAM 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 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 over privileged user activity on network, IoT, ICS, and SCADA devices—providing coverage over all endpoints
- 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 tampered binaries
  - » Registry Name Services, which provides 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-prem or cloud

And today, BeyondTrust continues to revolutionize PAM, with the most expansive vision and roadmap. We're aggressively pushing to solve emerging and future customer needs with enhancements to our solutions so they're always best-of-class in features, capabilities, and usability—and so that our platform always covers the most PAM use cases.

DIFFERENTIATOR #3:

Integrations & Interoperability with Third-Party Solutions to Maximize Your Security Investments

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

BeyondTrust enables you to have a holistic understanding of the modern threat landscape across both internal and external risk. Our solutions incorporate relevant security data – available exploits, risky privileged activity, vulnerable systems and applications, compliance requirements, mitigations etc. – to help our customers drive more informed security decisions. The BeyondTrust Platform can integrate with next-generation firewalls (Palo Alto Networks, etc.) and SIEMs to correlate risks and make smarter decisions.

BeyondTrust also has integrations with many different identity access management (Okta, Onelogin, Savyint, etc.) and identity governance solutions (Sailpoint, etc.). For instance, our System for Cross-domain Identity Management (SCIM) integration with SailPoint enables organizations to effectively manage user access for both privileged and non-privileged identities and to leverage SSO. IT organizations benefit from full visibility into, not only role assignments and user access, but also all users and ongoing role changes.

Our integrations with various Service Desk platforms (ServiceNow, Cherwell Software, etc.) help strengthen security and improve productivity of IT help desks.

We are also proud to have been recognized by McAfee as their Security Innovation Alliance (SIA) partner of the year for two consecutive year (2018 & 2017), selected from 150 SIA partners. We have certified integrations for BeyondTrust Password Safe and Endpoint Privilege Management with McAfee solutions to enable organizations to better control risk and eliminate threats.

Ecosystem Integration

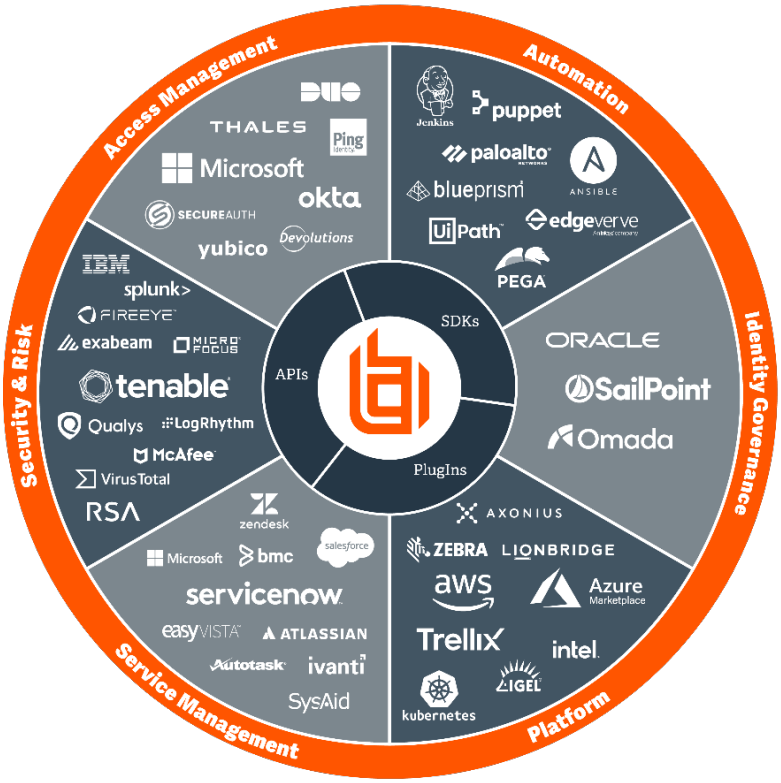

FIGURE 5: Sample of BeyondTrust Third-Party Technology Integrations

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

DIFFERENTIATOR #4:

Recognized PAM Leader

What do the top analysts have to say about PAM? BeyondTrust has been recognized as a Leader in Privileged Access Management in the most recent independent research analyst reports by Gartner, Forrester Research, and KuppingerCole. BeyondTrust stands out for our unsurpassed breadth of PAM use cases covered, completeness of our solution, technology innovation and vision, and centralized management platform.

We also received the distinction of Gartner Peer Insights Customers' Choice for Privileged Access Management. You can read **over 500 verified BeyondTrust customer reviews** on the Gartner Peer Insights site here.

Gartner peerinsights customers' choice™

DIFFERENTIATOR #5:

Proven Experience & Global Presence

More than 20k customers across 80+ companies rely on BeyondTrust solutions, which are backed by our 1300+ employees across 20+ countries and an extensive global partner network. With many thousands of successful deployments across diverse industries and use cases to satisfy both security and compliance regulatory requirements across the globe, BeyondTrust has the best team to help you accomplish your PAM goals.

Next Steps in Your PAM Journey

This paper has defined the capabilities required of a complete privileged access management solution.

Why should you partner with BeyondTrust?

- As the *only PAM vendor with a true platform*, BeyondTrust adds tremendous value to customers – from centralized management and policy, to integrated reporting and threat analytics. The result? Less cost, less complexity, and fewer gaps from using siloed tools.
- BeyondTrust is the *only PAM vendor to address all PAM use cases*. Our comprehensive PAM solution includes capabilities that no other vendor delivers, such as built-in Privileged Remote Access for insiders and vendors, and file integrity monitoring. A comprehensive solution reduces complexity and speeds time-to-value.
- The breadth of our solutions and flexibility of our platform enable you to handle today's threat scenarios and prepare for tomorrow's possibilities.
- Choose from the deployment model that best suits your needs – on-prem, private cloud, or SaaS – no PAM vendor provides more choices.
- Because we put you first and *don't price gouge for capabilities that we believe are essential*, BeyondTrust maximizes your security ROI.

Summary of Core BeyondTrust PAM Capabilities & Benefits

Discovers, onboards, and securely manages privileged credentials—for human and non-human accounts across diverse IT environments.

Manages and monitors all privileged sessions (including pausing and/or terminating suspicious sessions in real-time), and audits and reports on all privileged activities—even those for third-party (vendor) access.

Controls privilege elevation and delegation, and enforce least privilege across all endpoints (Windows, Mac, Unix, Linux), ICS, SCADA, and network devices, etc. BeyondTrust enables you to elevate application access—without elevating the user.

Enforces just-in-time access: This ensures privileged accounts are not always sitting in a privilege-active state, thereby dramatically reducing the threat window.

Securely addresses the broadest range of secure remote access use cases. From extending PAM best practices to and securing remote access for vendors and remote workers, to providing industry-leading remote support solutions that are a fixture of IT service management and internal help desks—no other IT security vendor can help you address secure remote access in all its forms as holistically as can BeyondTrust.

Consistently authenticates users across heterogeneous environments by extending AD's Kerberos authentication and single sign-on capabilities across platforms (Windows, macOS, Unix, Linux, etc.).

Enables better privilege decisions by accounting for real-time vulnerability status: Leverage patented technology to automatically scan applications for vulnerabilities at runtime, enabling IT and security teams to enforce quarantine, reduce application privileges, or prevent the launch of an application.

Provides holistic reporting and threat analytics: Gain deep analytics and reporting for multiple stakeholders, ensuring that all teams have the information and views they need to effectively manage user, application, and asset risk, and prove compliance.

Provides deep integrations with third-party technologies: Realize risk management synergies, improved visibility, smarter context, and better operational performance.

Key Benefits of BeyondTrust PAM Solutions

- Mitigates both external threats (malware, hacker, etc.) and insider threats
- Ensures accountability through session monitoring and recording, keystroke logging, and real-time auditing
- Protects you across your entire IT environment—on-premise, cloud, hybrid, DevOps infrastructures
- Enables informed, actionable IT risk management decisions from meaningful data gleaned via context-aware security intelligence, including asset, user, and account privilege information
- Simplifies your path to passing audits, compliance with government and industry mandates, and fulfilling other reporting requirements
- Enables your workforce and partners to be secure and productive
- Allows you to confidently embrace new technologies and business initiatives

ABOUT 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.

beyondtrust.com

APPENDIX:
YOUR PAM BUYER'S GUIDE TEMPLATE

Top Privileged Credential Management Capabilities	BeyondTrust	Vendor A	Vendor B
Performs full network scanning, discovery, and profiling with auto-onboarding of privileged accounts of all types (shared admin, user, application, and service accounts, SSH keys, database accounts, cloud and social media accounts, machine, DevOps, robotic process automation credentials—including by third-parties/vendors.	✓		
Illuminates where and how privileged passwords are being used, revealing security blind spots and malpractice (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-prem, etc.), directory, hardware device, application, services/daemons, firewalls, routers, etc.	✓		
Centralizes, secures, and encrypts all privileged credentials in a tamper-proof safe/vault. (Ideally the solution supports industry-standard encryption algorithms, such as AES 256).	✓		
Builds permission sets dynamically according to data from scans.	✓		
Implements API calls to eliminate embedded/hard-coded credentials in files, applications, scripts, and other code.	✓		
Automates rotation of password, SSH keys, and other secrets according to a defined schedule, including after each use for the most sensitive accounts, or for those accounts facing heightened security risk or compromise.	✓		
Enforces your privileged password management policy, such as 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.	✓		

Continued on next page...

Top Privileged Credential Management Capabilities	BeyondTrust	Vendor A	Vendor B
Provides granular access control.	✓		
Enables 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.	✓		
Has 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 checkout.	✓		
Leverages an integrated data warehouse and threat analytics across the privilege landscape.	✓		
Provides one, unified, comprehensive solution to manage human (privileged users) and non-person (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.	✓		
Flexible deployment options: hardware appliances, virtual appliances, or software.	✓		

Top Windows & Mac Least-Privilege Capabilities	BeyondTrust	Vendor A	Vendor B
Defaults all desktop and server users to standard privileges, while enabling elevated privileges for specific applications and tasks—without requiring administrative credentials.	✓		
Layers on powerful application control to implement trust-based application allow and block lists, with the flexibility to set both broad and granular rules.	✓		
Enforces restrictions on software installation, usage, and OS configuration changes.	✓		
Eliminates the need for end users to require two accounts.	✓		
Deploys overnight with out-of-the-box high-to-low flex QuickStart policies.	✓		
Matches applications to rules automatically based on asset-based policies; Leverages smart rules for alerting and grouping of devices and events.	✓		
Uses pre-built templates to stop attacks involving trusted apps, catching bad scripts and infected email attachments immediately.	✓		
Audits and reports on changes to critical policy, system, application and data files, eliminating unauthorized software installs, workarounds, or gaps that could lead to exploit.	✓		
Provides a technique for using real domain or local privileges when required.	✓		
Enables true least privilege by enabling a security model of just-enough access and just-in-time access.	✓		
Provides a single, unimpeachable audit trail of all user activity that speeds forensics and simplifies compliance.	✓		
Centralizes management, policy, reporting, and analytics.	✓		
Integrates with other privilege management modules to achieve comprehensive privileged access management.	✓		

Continued on next page...

Top Windows & Mac Least-Privilege Capabilities	BeyondTrust	Vendor A	Vendor B
Leverages an integrated data warehouse and analytics across the privilege landscape.	✓		
Sets policies via Active Directory Group Policy, Web Services, or McAfee ePO, with support for air-gapped systems and non-domain assets.	✓		

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. (Includes accounts with MFA enabled during a Web Jump Access session).	✓		
Creates an audit trail to provide visibility into vendor activity on your network, as well as meet compliance mandates, by controlling the access pathways into IT networks used by vendors.	✓		
Manages privileged access to business assets that leverage web-based management consoles, including IaaS servers, hypervisor environments, and web-based configuration interfaces for core network infrastructure.	✓		
Integrates with existing tools such as SIEM, Change Management, SCIM, and Password Management.	✓		

Continued on next page...

Top Privileged Remote Access Capabilities	BeyondTrust	Vendor A	Vendor B
Provides seamless, out-of-the-box integrations with ITSM, SIEM, and SCIM as well as other common business software solutions.	✓		
Leverages TouchID/FaceID for authentication into the privileged remote access mobile console.	✓		
Leverages industry standards like SAML and RADIUS to integrate with any Multi-Factor Authentication (MFA) tool	✓		

Top Unix & Linux Server Privilege Management Capabilities	BeyondTrust	Vendor A	Vendor B
Enforces least privilege and eliminates use of Root.	✓		
Enables just-in-time administration (JIT), which is the ability to assign dynamic privileges to accounts and assets to ensure 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.	✓		
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.	✓		
Consolidates audit logs and centralizes reporting across all your server domains.	✓		
Supports Pluggable Authentication Module to enable utilization of industry-standard authentication systems.	✓		

Continued on next page...

Top Unix & Linux Server Privilege Management Capabilities	BeyondTrust	Vendor A	Vendor B
Offers a powerful and flexible policy language to provide a migration path from sudo.	✓		
Provisions/de-provisions privileges transparently, helping to ensure compliance.	✓		
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.	✓		

Top Capabilities for Making Privilege Elevation/ Delegation Actions Based on Real-Time Risk	BeyondTrust	Vendor A	Vendor B
Assesses real-time threat levels to the user, requested asset, and the application launched.	✓		
Takes runtime actions for applications and processes based on the rules and policies that you create (i.e. allow privilege escalation, remove administrative permissions, or prevent an application from launching).	✓		
Uncovers emerging risks by identifying and reporting on the types of activities that might be at risk.	✓		
Enables advanced privilege elevation and delegation workflows to undertake remedial measures that proactively eliminate the potential threats, such as session termination or heightened logging, auditing, and review for the privileged session.	✓		

Top Management & Threat Analytics Capabilities	BeyondTrust	Vendor A	Vendor B
Groups, assesses, & reports on assets by IP range, naming convention, OS, domain, applications, business function, Active Directory, and more.	✓		
Enables rapid orchestration of security response to stop or mitigate threats.	✓		
Enables import from Active Directory or to set custom permissions.	✓		
Correlates low-level data from a variety of leading third-party solutions to uncover critical threats.	✓		
Correlates system activity against a constantly updated malware database.	✓		
Reports on compliance, benchmarks, threat analytics, what-if scenarios, resource requirements, and more.	✓		
Presents, sorts, and filters historical data for multiple perspectives.	✓		
Locates network (local & remote), web, mobile, cloud and virtual assets, as well as privileged accounts.	✓		
Profiles IP, DNS, OS, Mac address, users, accounts, password ages, ports, services, software, processes, hardware, event logs, etc.	✓		
Provides workflows, ticketing, and notifications to coordinate IT and security teams.	✓		
Shares data with leading SIEM, GRC, NMS, and help desk solutions.	✓		

Top Active Directory Bridge Capabilities	BeyondTrust	Vendor A	Vendor B
Single sign-on for any enterprise application that supports Kerberos or LDAP.	✓		
A single, familiar tool set 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, Linux, and macOS, consolidating various password files, NIS and LDAP repositories into Active Directory and removing the need to manage user accounts separately.	✓		
Does not require Active Directory schema modifications to add Linux, Unix, or macOS systems to the network.	✓		
Provides a pluggable framework with an interface similar to Microsoft's Management Console on Linux or macOS (Full support for Apple's Workgroup Manager application would allow for seamless management and control of macOS settings.).	✓		
Supports a wide range of Unix, Linux, and Mac platforms (CentOS, Debian, Fedora, FreeBSD, HP-UX, IBM AIX, Oracle Enterprise Linux, Suse, RedHat, Solaris, Ubuntu, etc.).	✓		
Supports compliance with SOX, PCI, HIPAA, and other regulations.	✓		
Works as part of a broad privileged access management solution family.	✓		