BeyondTrust

IN PARTNERSHIP WITH

Ping Identity

Bridging PAM, IAM, & IGA with BeyondTrust + Ping Identity

4 Use Cases for Managing, Governing, and Securing Every Identity

BeyondTrust

TABLE OF CONTENTS

Executive Summary

For years, the disciplines of Privileged Access Management (PAM), Identity and Access Management (IAM), and Identity Governance and Administration (IGA) have largely operated in silos—each tackling a single piece of identity security, such as visibility, centralized management, access, automation, account provisioning, permissions, or provisioning / deprovisioning.

Yet, precisely because these functions operate in silos, today's organizations struggle to keep up with constantly-changing user profiles and access requirements. Identities, both human and non-human (RPA bots, applications, AI agents, etc.), are proliferating at a rapid pace, while IT teams are stretched across a wider range of environments than ever before, including on-premises, multicloud, endpoints, OT, and SaaS applications. As a result, maintaining consistent identity management and security has become increasingly challenging, creating operational inefficiencies, security gaps, and auditing complexity.

Without a more unified approach to identity security, businesses are at heightened risk of identity-based threats, as bad actors target the blind spots in identity infrastructure to gain initial access and move laterally within an organization.

BeyondTrust and Ping Identity offer a combined approach to directly address this identity estate fragmentation problem. By uniting identity and privilege into a single identity security fabric, our joint customers benefit from adaptive access control for increased productivity, automated remediation, and continuous protection.

This paper highlights the underlying identity infrastructure challenges many of today's businesses face and how BeyondTrust and Ping together solve these challenges. Also, explore several key use cases your organization can implement using the BeyondTrust + Ping combined solution.

Siloed Identity Infrastructure = Your Biggest Risk

While IT teams are aware of increasing identity risk, it can be a formidable challenge to understand and eliminate threats across the entire identity lifecycle. Identities in today's environments are multiplying at breakneck speed due to the expansion of cloud environments and adoption of SaaS technologies and AI agents. In many cases, the technology is outpacing policy and governance, making it a challenge to gain full visibility into which identities are being used where, exactly what their privileges look like, and which potential attack paths they create.

Additionally, as companies scale, inconsistencies across various domains are inevitable. Identity infrastructure often varies between environments, as every SaaS technology, cloud provider, etc. tends to use a domain-specific system for managing identities. For example, Entra ID offers a privileged identity management (PIM) solution, but its functionality is confined to Microsoft technologies.

The responsibilities to keep these technologies up to date also fall on different groups within the organization, meaning that separate teams often end up managing identities and access in silos. Consequently, while organizations may have IAM, IGA, and PAM solutions deployed, each of these solutions may manage identities and operate independently. As such, each of the solutions only sees and acts on the visibility and intelligence within its own domain.

This siloed identity estate approach ultimately fails to protect against many modern threats, as attackers look to exploit indirect and hidden pathways between endpoints, servers, IdPs, cloud environments, and SaaS solutions. Rather than moving within a single domain, they exploit the various trust relationships and connections that exist between domains to move deeper into the environment.

This separation between various identity domains also makes it challenging for organizations to prove compliance. When security controls and monitoring only extend to the boundary of each specific domain, it becomes incredibly difficult to fulfill complex compliance requirements.

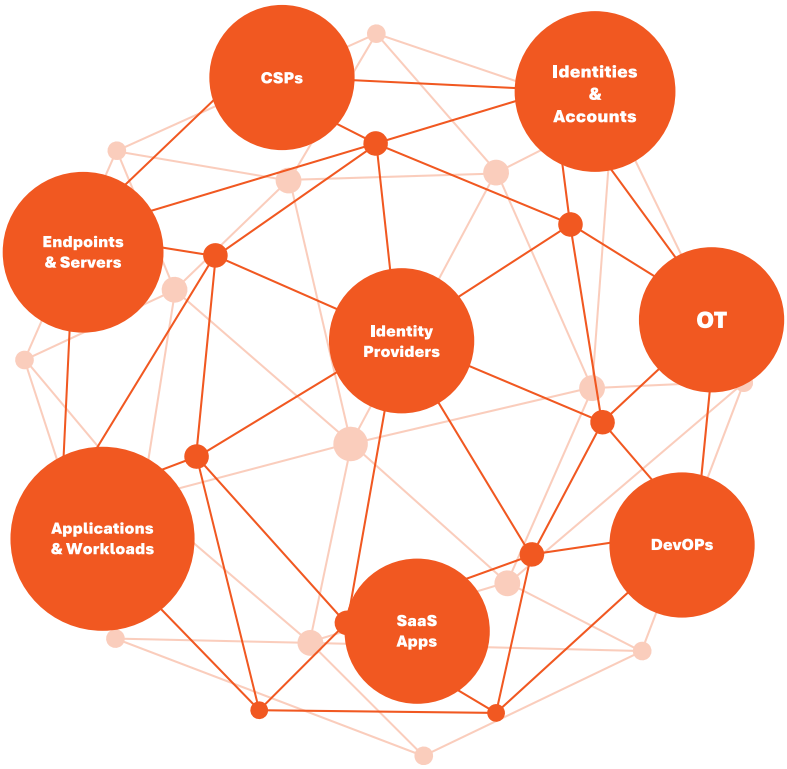
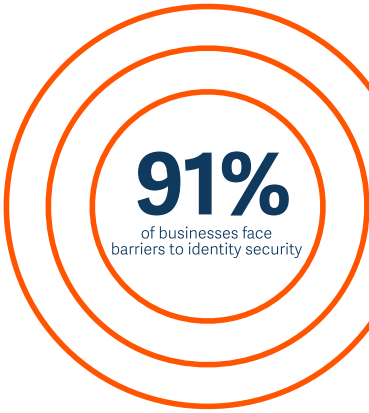


Figure 1: Enterprises and agencies must contend with a vast ecosystem of identity infrastructure and security tooling, often managed by teams that are essentially siloed from each other.

In many cases, organizations bring in additional point tools or piecemeal integrations in an attempt to better understand and defend this sprawl of identities and their associated privileges. However, this often exacerbates visibility gaps between domains and fails to provide an end-to-end vision of the entire identity lifecycle.

Additionally, piecemeal identity controls can quickly become overly restrictive and burdensome to teams. To avoid the friction that comes with overly restrictive identity controls, it's common for organizations to err on the side of over-provisioning accounts and leaving standing access. However, indefinite access to critical resources without proper lifecycle controls exponentially increases the potential for successful identity-based attacks.



According to the IDSA, 91% of businesses still face barriers to identity security, with "our technology environment is very complex" and, "identity frameworks are complicated with multiple vendors and different architectures" as the top two roadblocks.

—IDSA, 2025 Trends in Securing Digital Identities, Oct 2025.

A Unified Identity Fabric Approach

Implementing an end-to-end identity security strategy, rather than bringing in more point tools, is the key to effectively minimizing the identity attack surface, while also protecting against modern, cross-domain threats. This means taking an integrated 'identity fabric' approach to users, applications, and data—facilitating a single view of all human and non-human identities across domains.

A strong identity security program also involves operationalizing robust identity hygiene, ensuring the right users have the appropriate access to resources across the entire IT estate, particularly when it comes to heightened privileged access. Additionally, it means fulfilling security requirements, while also empowering worker productivity with seamless, just-in-time access.

BeyondTrust + Ping Identity: Strengthening End-to-End Identity Security

BeyondTrust and Ping Identity have partnered to enable a centralized approach to managing, governing, and securing all identities (privileged or non-privileged) and access pathways. Whether granting just enough access for a new employee, revoking privileges at offboarding, or detecting and responding to anomalous behavior in real time, this integrated approach strengthens identity security across the entire lifecycle.

Together, BeyondTrust and Ping Identity address three critical needs for customers:

1. **Proactive Least Privilege and Zero Standing Privilege (ZSP) Authentication** – Enforcing just-in-time (JIT) elevation and adaptive authentication to minimize the attack surface—without impacting productivity

2. **Streamlined Joiner-Mover-Leaver (JML) Processes** – Ensuring fast, accurate provisioning and deprovisioning across all systems and levels of privilege

3. **AI-Driven Detection and Response** – Automatically identifying security hygiene issues and risky behavior, then triggering workflows to suspend or terminate access

Key Business and Security Outcomes

The joint BeyondTrust + Ping Identity strategic partnership delivers a comprehensive approach to managing identity security. Together, these solutions support least privilege and Zero Trust principles, helping organizations secure their digital environments from endpoint to cloud.

As a result, customers can take advantage of significant security and business outcomes, including:

Operational Efficiency

Together, BeyondTrust and Ping enable automated JML processes such as provisioning, password management, and access requests and certification. Streamlining these processes means reducing implementation time / cost and other manual IT overhead.

Improved Agility

These solutions also speed digital transformation and cloud adoption without slowing access. With this streamlined approach, organizations can seamlessly adapt with dynamic environments, so users can get a better experience, while security remains effective and scalable. This combined approach enhances an organization's ability to automate workflows and reduces the need to juggle multiple tools. It also empowers teams to quickly identify and address security gaps, minimizing effort while accelerating response times.

Organizational Resilience

BeyondTrust and Ping's combined solution enables continuous identity verification to reduce the blast radius of attacks. Together, these solutions allow organizations to secure and control access to all privileged identities and their credentials, as well as automate password rotation. Additionally, BeyondTrust + Ping can quickly terminate or remove access to a remote session via hostname or username, if a security incident is detected.

Streamlined Compliance

The combined BeyondTrust and Ping solution simplifies the path to compliance through automated controls, evidence gathering, and built-in auditability. Every IAM and IGA activity—from provisioning to access requests to authentication—is automatically monitored and documented to meet regulatory requirements and prove compliance to auditors.

Together, BeyondTrust and Ping deliver a truly scalable identity security architecture that reduces risks, accelerates governed access, and maximizes the value of existing identity investments—without sacrificing control or productivity.

Joint Solution Use Cases

BeyondTrust and Ping Identity deliver four key use cases for our joint customers, including:

1. Govern Conditional Access and Enhance Productivity

BeyondTrust Identity Security Insights® + PingOne DaVinci; BeyondTrust Endpoint Privilege Management + Ping Identity Platform

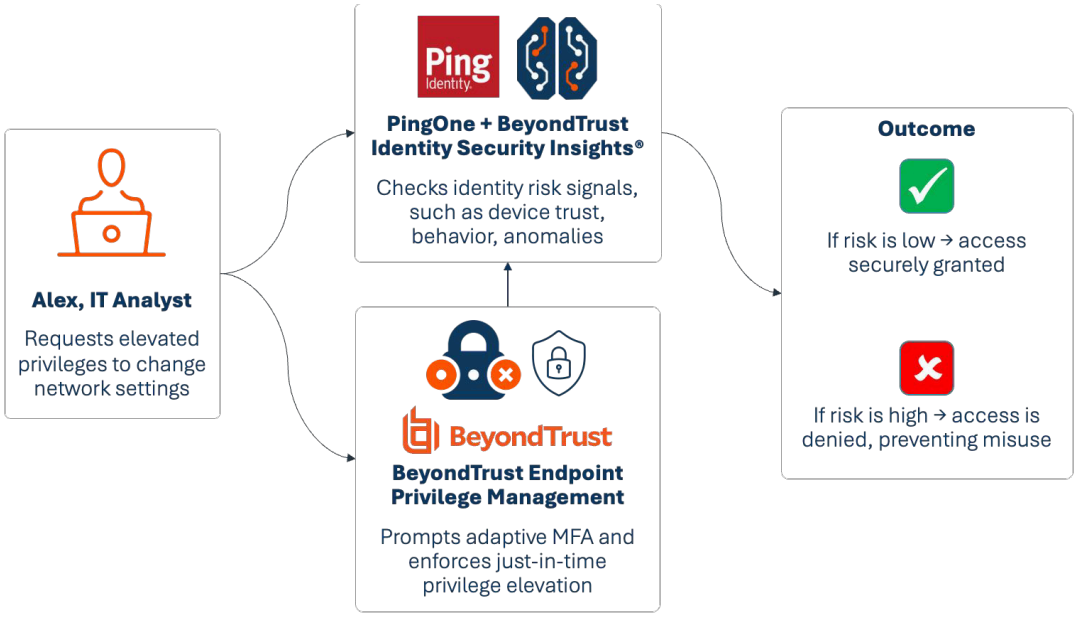


Figure 2: PingOne + BeyondTrust solutions streamline governance of conditional access. Enable additional authentication and risk checks for applications, using Ping's adaptive MFA and BeyondTrust Endpoint Privilege Management and Identity Security Insights.

Together, these solutions enable businesses to automatically enforce conditional, JIT privilege access across endpoints, cloud environments, and SaaS applications. Additionally, these powerful product combinations leverage behavioral analytics to flag and respond to risky or anomalous behavior and can take automated actions, including revoking / denying access.

BeyondTrust Identity Security Insights®

Reveal the access escalation pathways of identities—including across domains—to gain unparalleled visibility and understanding over the entire identity attack surface.

BeyondTrust Endpoint Privilege Management

Enforce least privilege dynamically, across all endpoints, without impacting productivity.

Ping Identity Platform

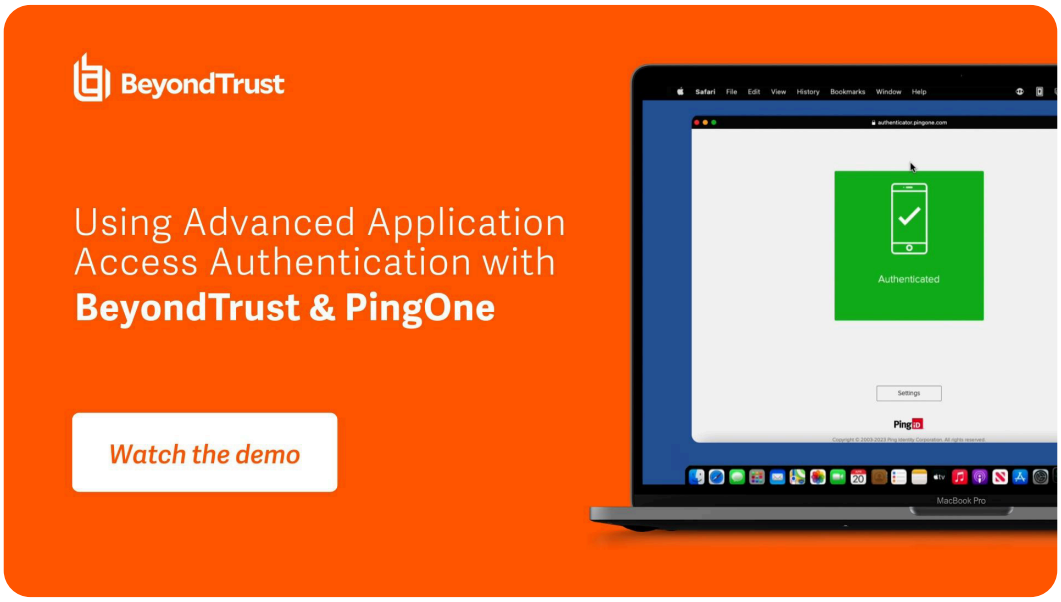
Manage user access to applications and data with controls such as single sign-on (SSO) and integrated step-up multi-factor authentication (MFA).

PingOne DaVinci

Leverage a no-code orchestration platform that enables seamless integration of identity, security, and authentication workflows across complex environments.

With the Ping Identity Platform + Endpoint Privilege Management, and Identity Security Insights + PingOne DaVinci, organizations can activate the following features and capabilities:

- **Contextual Self-Service Access:** Users can request (and admins can approve, provision, and revoke) access to SaaS applications based on real-time risk signals and business context using PingOne DaVinci and Identity Security Insights.
- **Integrated MFA & SSO:** Use SAML, OIDC, and RADIUS protocols to enforce secure, seamless access across cloud and on-prem environments.
- **Advanced Application Access Authentication:** Use Ping's biometrics, device trust, and behavioral analytics for adaptive MFA, together with BeyondTrust Endpoint Privilege Management, to facilitate additional authentication checks for applications that require admin rights.



Benefits of leveraging these joint solutions include:

- **Enhanced User Experience:** Reduce friction with seamless, secure access to applications and systems.
- **Increased Productivity:** Automate access provisioning and reduce delays in user onboarding and role changes.
- **Scalable Security:** Easily adapt to dynamic environments and evolving business needs.

By leveraging Ping Identity + BeyondTrust to govern conditional access, organizations gain smart and streamlined JIT access and MFA to applications and data. The combined solutions operationalize seamless access with risk-based controls and automate zero standing privilege enforcement across the entire IT environment. As a result, teams can boost productivity without sacrificing security.

2. Unify Identity Governance & Privileged Access Management

BeyondTrust Password Safe + Ping Advanced Identity Cloud

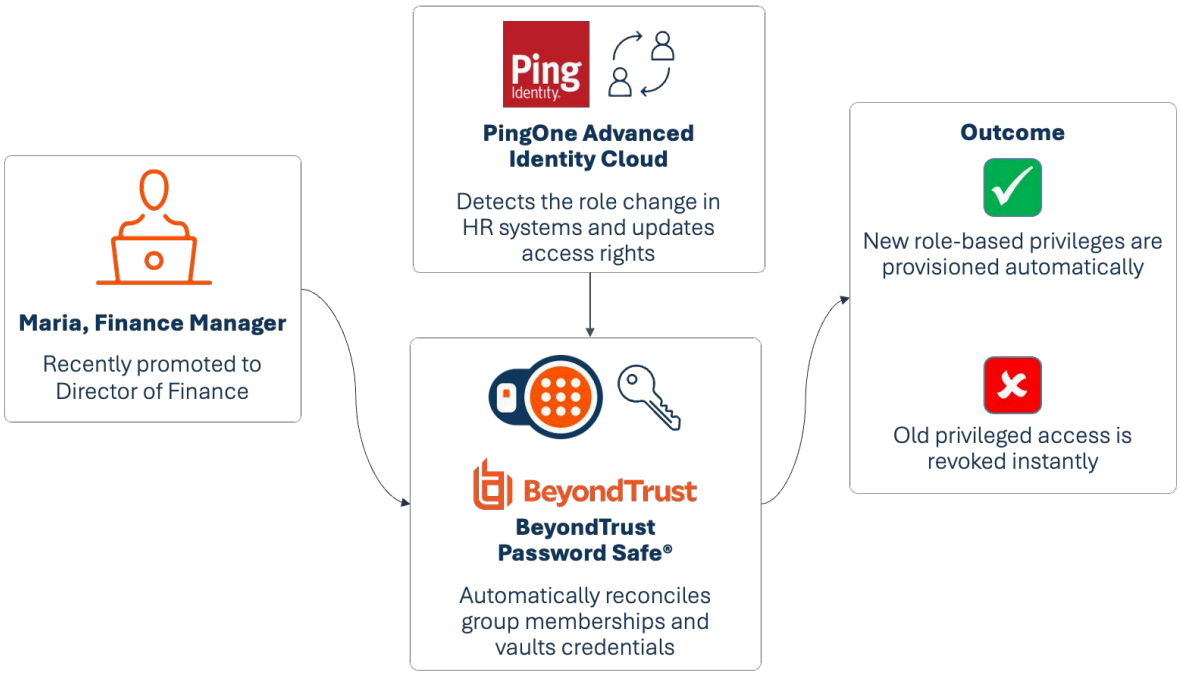


Figure 4: Approve, provision, and revoke access to SaaS applications based on real-time risk signals and business context using PingOne DaVinci, together with BeyondTrust Password Safe and Identity Security Insights. By unifying identity governance, you can ensure policy is automatically enforced, even as the environment and roles change.

Leveraging Password Safe and PingOne Advanced Identity Cloud together enables businesses to reduce access risk throughout the JML process, via dynamic provisioning and deprovisioning. Additionally, manage passwords, secrets, and keys seamlessly to lower associated risks when employees join, change roles, or leave.

With BeyondTrust Password Safe + PingOne Advanced Identity Cloud, activate the following features and capabilities:

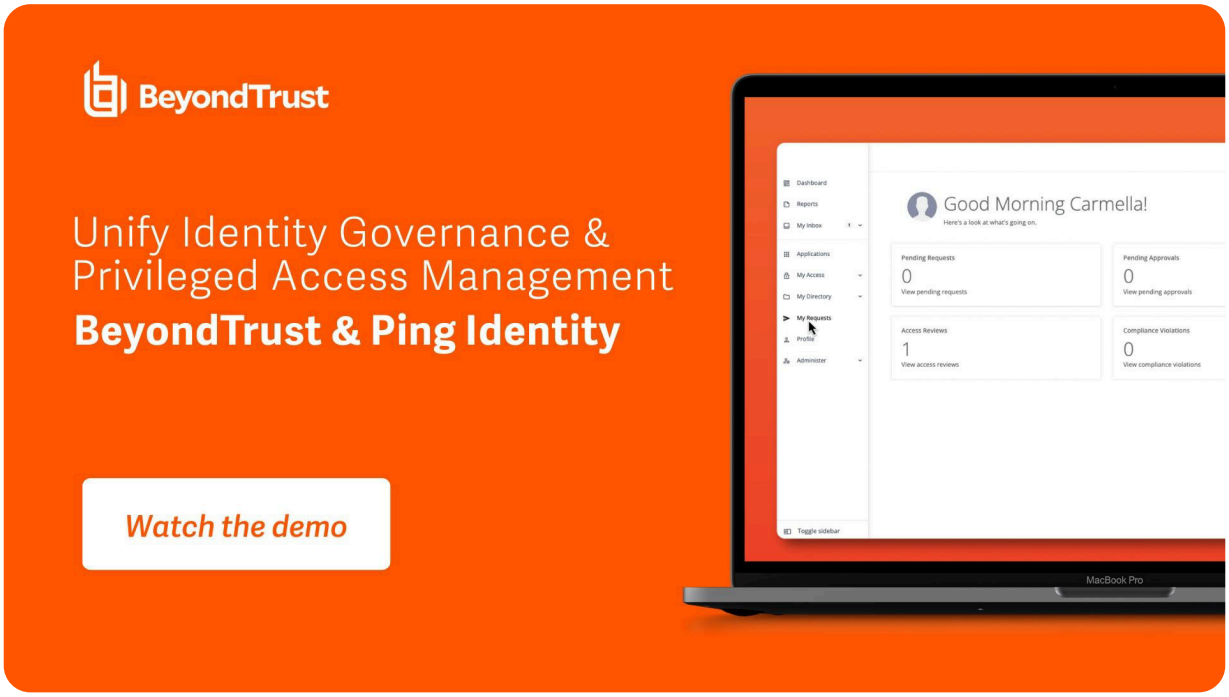
- **Visibility Across the Identity Estate:** Gain a view into ungoverned identities, unmanaged access, and questionable privileges.
- **Centralized Identity Security:** Combine PingOne Advanced Identity Cloud's identity governance capabilities with BeyondTrust's Password Safe and Identity Security Insights for full management.
- **Policy-Based Access Control:** Enforce least privilege and adaptive access policies based on user context and risk.

Password Safe®

Manage privileged accounts and the associated passwords, keys, secrets, and sessions—for people, machines, and AI agents.

PingOne Advanced Identity Cloud

Ensure every identity only has the access needed with cloud-native governance, powered by AI and machine learning, that supports enterprise-grade security and compliance.



Benefits of leveraging these products as a joint solution include:

- **Stronger Compliance:** Automate access reviews, credential management, and audit logging to meet regulatory standards.
- **Reduced Risk:** Minimize the attack surface by enforcing least privilege and monitoring privileged activity.
- **Simplified Management:** Leverage a unified dashboard and centralized view via the BeyondTrust Pathfinder Platform for managing all identities (human and non-human) and access across the enterprise.

By unifying identity governance and PAM with BeyondTrust + Ping Identity, organizations can automatically minimize access risks whenever employees join, change roles, or leave. They can also enable automated provisioning with least privilege, making compliance simple with clear audit trails.

3. Automate Threat Response & Session Termination

BeyondTrust Identity Security Insights + BeyondTrust Privileged Remote Access + PingOne DaVinci

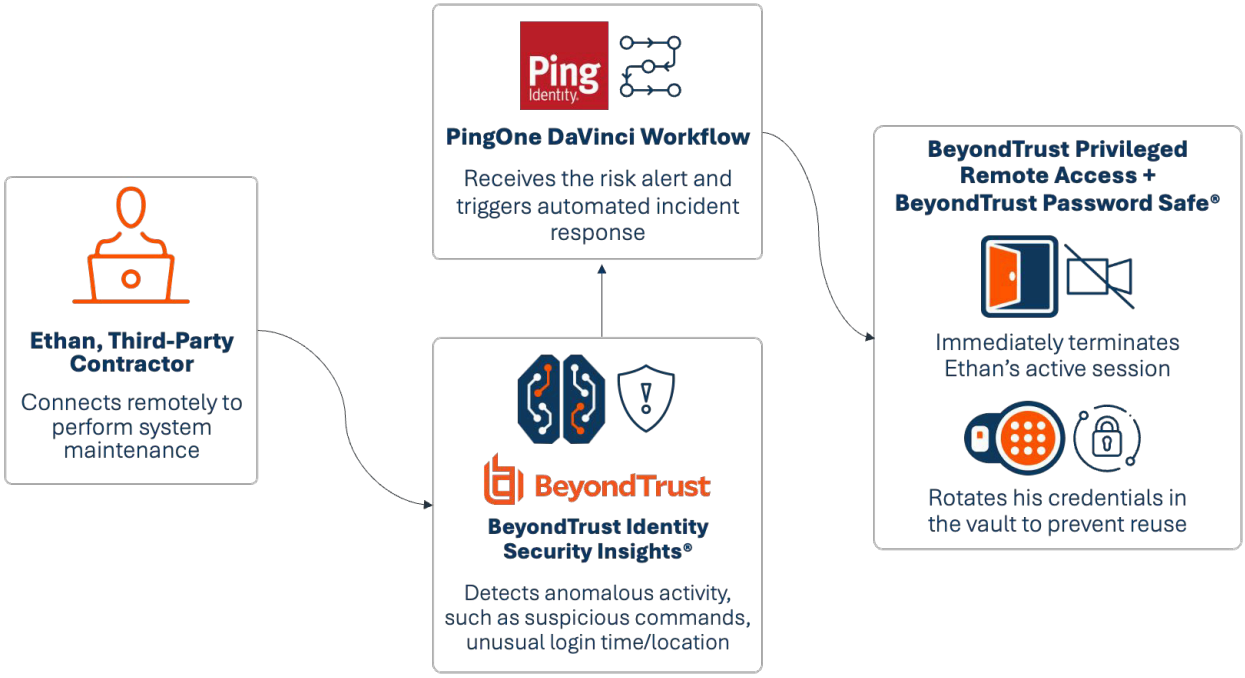


Figure 6: Enable identity threat detection and response (ITDR) capabilities by combining BeyondTrust and Ping solutions. In this example, a risk is identified, triggering an automatic workflow resulting in session termination and credential rotation to mitigate the threat.

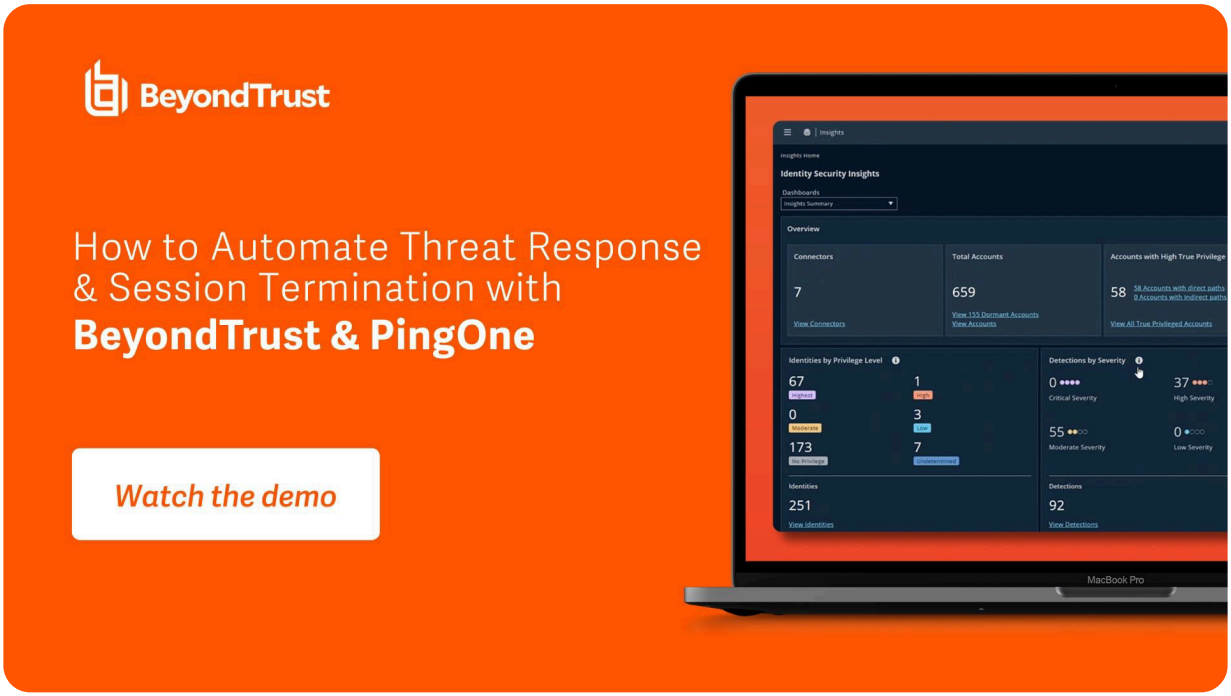
With Identity Security Insights, Privileged Remote Access, and PingOne DaVinci, scale dynamic secure access for operational technology (OT), IT, and cloud for internal teams and third parties. Plus, automatically trigger PingOne DaVinci incident response workflows, streamlining anomalous detections and privileged access termination responses for IT and third-party contractors.

With BeyondTrust's Identity Security Insights and Privileged Remote Access, combined with PingOne DaVinci, activate the following features and capabilities:

- **No-Code Orchestration:** PingOne DaVinci enables drag-and-drop workflow creation for access approvals, provisioning, and revocation.
- **Advanced Privilege Detection and Visibility:** Supports human, non-human, and machine identity trust, along with behavioral analytics.

Privileged Remote Access

Create identity-secure, just-in-time access to all your enterprise environments: cloud, on-premises, and OT.



Benefits of leveraging these joint solutions include:

- **Enhanced User Experience:** Reduce friction with seamless, secure access to applications and systems.
- **Increased Productivity:** Automate access provisioning and reduce delays in user onboarding and role changes.
- **Scalable Security:** Easily adapt to dynamic environments and evolving business needs.

With Ping + BeyondTrust for automated threat detection and session termination, businesses establish a faster, simpler process to handle security incidents and contain threats before they spread. Our joint customers benefit by not only detecting threats in real-time, but also by enforcing proactive steps to harden their identity estate, such as ending privileged access for IT staff and outside contractors when it's no longer needed.

4. Manage Non-Human Identities (AI Agents) and Protect Their Access to Resources

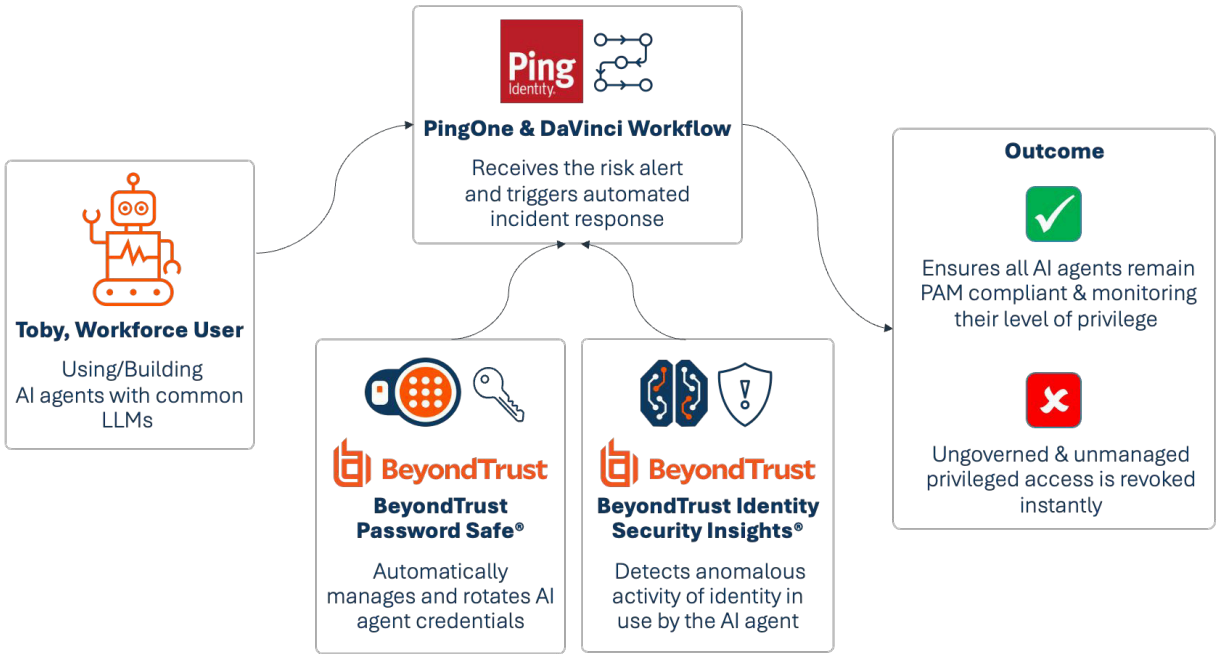


Figure 8: Together, PingOne and BeyondTrust solutions proactively protect AI agents from threats and ensure they remain compliant with PAM policies.

Organizations are increasingly adopting agentic AI to autonomously perform tasks on behalf of a user or system. But there are several identity security challenges organizations must consider when deploying AI agents, including:

- Delegation of user and system permissions to an agent
- Identification of an agent's unique identity
- Authentication of an agent
- Authorization of an agent to access protected resources and what data the agent is allowed to use and provide back to the user or system (APIs, databases, cloud services, or even other agents)
- Consent and transaction approval for the agent to act on behalf of a user or system

With the Ping Identity and BeyondTrust solutions, customers can gain control of managed AI agents (i.e. digital assistants / workers, etc.) by managing the full lifecycle of AI agents: onboarding, authenticating, authorizing, monitoring, and retiring the agents. This includes governance of the agent's access to ensure that it only has the privileges it needs, for the finite moments needed, to perform its authorized actions, within the right context.

With BeyondTrust + Ping Identity, activate the following features and capabilities to secure agentic AI:

- **Agent Identification** – Identify and classify AI agents as personal, digital assistant, or digital worker
- **Agent Detection** – Establish AI-driven sessions and tag sessions for downstream security
- **User Delegation** – Use tokens or secrets with limited scope to maintain clear accountability back to the human principal, and gain visibility into each agent's interaction with systems and other agents
- **Least Privilege Access** – Restrict agent access to only required resources, for a limited time of operation, to fulfill the authorized action
- **Agent Governance** – Monitor, analyze and revoke access of agents in real-time to prevent compromised or misbehaved agents

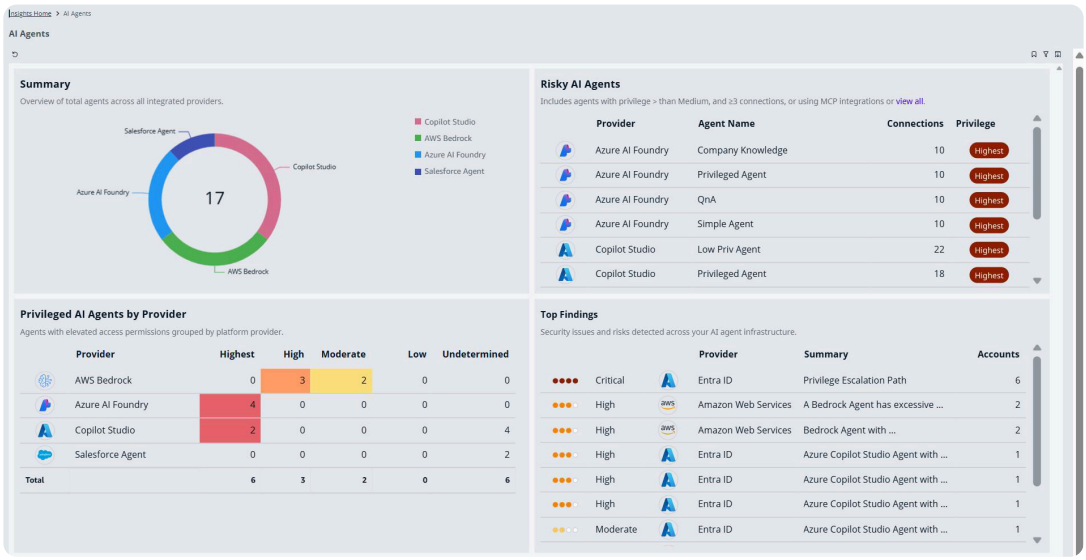


Figure 9: BeyondTrust + Ping offer visibility and governance of all AI agents, from across your entire identity estate.

Benefits of leveraging BeyondTrust + Ping Identity for protecting and managing AI agents include:

- **Eliminated Blind Spots:** Gain cross-domain visibility of your entire identity and agentic AI estate—including shadow AI—and bring it under management and oversight to reduce risk.
- **Enhanced Security:** Proactively identify and fix excessive permissions, continuously monitoring and adjusting access to reduce the attack surface and prevent breaches.
- **Improved Efficiency:** Automate the management of AI agent identities and their permissions, saving time for IT and security teams, and speeding up deployment.
- **Reduced Business Risk:** By connecting permission changes to their business impact, make smarter decisions that prevent both operational disruptions and security breaches.

With BeyondTrust + Ping, teams can secure AI agents and other non-human identities, prioritizing security for these new technologies so organizations can confidently use them to improve business operations, productivity, and innovation.

These combined solutions offer visibility of all AI agents and enable organizations to bring them under IAM / PAM control, including onboarding, offboarding, and governance.

Why Choose BeyondTrust + Ping Identity

Together, BeyondTrust and Ping Identity provide a unified identity fabric for securing all identities and access pathways. The results: new efficiencies and resilience through combining IAM + IGA + PAM into a single comprehensive approach.

As industry leaders with distinct areas of expertise, BeyondTrust and Ping Identity bring together strong PAM, IAM, and IGA, built to scale in an era of identity convergence.

BeyondTrust has been recognized by analysts across identity security disciplines, including the following recognitions:

- Leader in the 2025 Gartner® Magic Quadrant™ for PAM, for seven consecutive times
- Leader & Fast Mover in the 2025 GigaOm Radar Report for CIEM
- Leader in the 2025 Forrester Privileged Identity Management (PIM) Wave
- Leader in the 2025 KuppingerCole Enterprise Secrets Management Leadership Compass
- Leader in the 2024 KuppingerCole PAM Leadership Compass, for five consecutive times
- Leader in the 2024 KuppingerCole ITDR Leadership Compass

Ping Identity has also been recognized by analysts across identity security disciplines, including the following recognitions:

- Leader in the 2025 Gartner® Magic Quadrant™ for Access Management, for nine consecutive years
- Leader in the 2025 KuppingerCole Access Management Leadership Compass
- Leader in the 2025 KuppingerCole Policy Based Access Management Leadership Compass
- Leader in the Forrester Wave™: Customer Identity and Access Management Solutions, Q4 2024
- Leader in the 2024 KuppingerCole CIAM Leadership Compass
- Leader in the 2025 KuppingerCole Identity Fabrics Leadership Compass
- Leader in the 2024 KuppingerCole Passwordless Authentication for Consumers Leadership Compass
- Leader in the 2024 KuppingerCole Passwordless Authentication for Enterprises Leadership Compass

> "Xalient is pleased to support the integrated BeyondTrust and Ping Identity solution, which unites complementary capabilities to strengthen identity, access, and privilege security. This collaboration delivers significant value for organizations advancing Zero Trust convergence and reflects our continued commitment to enabling intelligent, identity-first security outcomes."
>
> **— David 'DJ' Morimanno, Field CTO - North America at Xalient**

Learn more about BeyondTrust and Ping Identity's approach to identity security and expansive partner ecosystem:

- Ping Identity + BeyondTrust (web page)
- The PartnerTrust Ecosystem (BeyondTrust Partner web portal)
- Nexus Partner Program (Ping Identity's Partner Program)
- BeyondTrust and Ping Identity: Unified Identity Security (solution brief)
- BeyondTrust and Ping Identity Partner to Deliver Unified Identity Security Fabric (press release)
- Availability of BeyondTrust + Ping Identity Unified Identity Security Solutions in AWS Marketplace (press release)
- Interview with Morey Haber, BeyondTrust Chief Security Advisor, on Unified Identity Fabric (video)
- Identity Security Insights and PingOne DaVinci (demo)
- IGA and PAM with BeyondTrust and Ping (demo)
- ITDR with BeyondTrust and PingOne DaVinci (demo)
- A PAM Maturity Model (whitepaper)
- The Guide to Identity Security Defense-in-Depth (whitepaper)
- Buyer's Guide for Complete Privileged Access Management (PAM) (whitepaper)
- The CISO's Guide to Addressing Critical Gaps in Identity Security through PAM Modernization (whitepaper)
- Paths to Privilege Explained (whitepaper)

About BeyondTrust

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

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

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

About Ping Identity

At Ping, we make it possible to trust every digital moment—moments with customers, employees, partners, and non-human identities. Whether you're securing millions of users, fighting sophisticated fraud, simplifying third-party access, or embracing passwordless experiences and verifiable credentials, establishing trust shouldn't slow you down. Our enterprise-grade identity platform is built for scale, speed, and flexibility—and works seamlessly with your existing tech stack across cloud, hybrid, and on-prem. We help innovators accelerate growth and confidently leverage AI—making life easier for developers, users, IT teams, and partners. With Ping, all your digital experiences start with trust.

Learn more at **www.pingidentity.com.**