BeyondTrust

The CISO's Guide to Addressing Critical Gaps in Identity Security through PAM Modernization

Securing identities for humans, machines, and AI

BeyondTrust

TABLE OF CONTENTS

Executive Summary

Chief Information Security Officers (CISOs) are under constant pressure to enable the business to innovate safely and move faster. Enterprises are expanding cloud deployments and adopting new toolsets and processes—many of which are underpinned by novel, fast-evolving technologies powered by SaaS and AI.

One of the most significant of these challenges is a cresting new wave of shadow AI, hidden outside the purview of known technology procurements. This wave is driven by employees throughout the organization using new AI toolsets (both paid for and free) to enhance productivity. When employees use personal accounts or credit cards to access these tools, they often operate outside of security's view, creating unmanaged identities with access to sensitive corporate data. This extends to a new class of non-human identities, such as AI agents, which may be granted privileges to act autonomously within the environment, creating novel and unpredictable security vulnerabilities.

Security Needs to Scale with Rapidly Growing AI Risks

82% of organizations already use AI agents

23% reported their AI agents have been tricked into revealing access credentials

80% of companies say their AI agents have taken unintended actions, including:

- Accessing unauthorized systems or resources (39%)
- Accessing or sharing sensitive or inappropriate data (31% and 33%)
- Downloading sensitive content (32%)

Source: AI agents: The new attack surface. Dimension Research (commissioned by SailPoint). May 2025.

Every new toolset, server, application, and user identity (human or machine) has the potential to expand the attack surface. Yet, with current security tooling and architectures, it's highly difficult, if not impossible, for CISOs and their teams to identify and gauge these emergent risks, let alone effectively prioritize and mitigate them. This risk blindness can slow organizations down in assessing and adopting new technologies with the potential to accelerate business. It can also lead to dangerous gaps and breaches if those technologies are implemented without proper guardrails.

Why Identity Security and PAM Modernization Matter More than Ever

While organizations have mature programs for traditional vulnerability management, they lack similar maturity in approaching identity-based vulnerabilities that are proliferating alongside the growth of identities (human, machine, agentic AI, etc.), entitlements, and escalation pathways. These in adequately managed identities, and their escalation pathways, represent a significant blind spot in every organization.

Securing privileged access is a core CISO responsibility, as accounts with elevated permissions are prime targets for malicious actors. The BeyondTrust Phantom Labs™ research team compiled data from our Identity Security Risk Assessment engagements across a wide range of industries, reporting in August 2025 on the following findings:

- Dormant service accounts with privilege in over 70% of environments.
- Overly permissive Entra Service Principals that created direct pathways to Global Admin privileges, exposing entire Microsoft 365 environments to potential takeover.
- Credentials reused across multiple service accounts by human admins, enabling a single compromised password to compromise numerous non-human accounts.
- Low-privileged users that could escalate to administrative access across Active Directory, Entra, AWS, Okta, and GitHub through hidden privilege escalation paths built on configuration oversights, federation, and synchronization.
- AD Service accounts that bridged on-premises and cloud environments with Active Directory accounts holding privileged Entra roles, that led to cross-platform attack vectors.
- Ineffective GitHub repository access management, leading to uncontrolled secret access and unauthorized access to sensitive code, often accessible through personal GitHub accounts.

Ultimately, these issues stem from a visibility challenge. While a multitude of security vendors are approaching this problem from a variety of angles, most are only addressing fractional components of the underlying issue.

We believe this core identity security problem is best solved by an approach rooted in privileged access management (PAM)—one that builds on foundational controls with a modern set of cloud-native capabilities architected for the velocity and scale of AI-driven digital transformation.

The CISO's Guide to Addressing Critical Gaps in Identity Security through PAM Modernization shows how BeyondTrust gives you the platform and framework for reducing risk and securely enabling your organization in an exciting new frontier of innovation and opportunity.

Key areas covered in this guide include:

- The emerging identity-based risks from shadow AI and hybrid cloud sprawl.
- How a modern PAM approach provides unified visibility and intelligent remediation.
- Critical use cases for risk reduction, compliance, and incident response.

Supercharging Security and Productivity

A modern PAM approach is designed to connect the dots and enhance foundational PAM controls (password vaulting, secrets management, session monitoring, basic entitlement management, etc.) with the intelligence and automation that today's identity security demands. It addresses gaps missed or inadequately addressed by other security toolsets.

A modern PAM approach recognizes that, to be effective, security must go hand-in-hand with productivity, and empower businesses to forge ahead with confidence. With that said, while it may require sophisticated technology under the hood, the experience for users and administrators should be simplified, allowing for fast ROI and minimizing ongoing maintenance.

BeyondTrust's modern PAM approach provides significant and measurable value across the critical use cases and strategic priorities that matter most to security leaders:

- **Risk reduction:** Minimizing the attack surface and blast radius of attacks
- **Accelerated incident response:** Reducing dwell time—the time from detection to remediation
- **Compliance:** Simplifying audits and ensuring continuous readiness
- **Business enablement:** Enabling secure adoption of new technologies and processes

How BeyondTrust Addresses Key Identity Security Challenges

Here are a few key use cases where BeyondTrust's Modern PAM solution significantly advances identity security:

Use Case 1:

Achieve Unified Visibility Across Hybrid Environments

To address risks from shadow AI and sprawling cloud services, CISOs need a single, correlated view of all identity activity. BeyondTrust's Modern PAM solution extends visibility beyond traditional on-premises systems into multicloud and SaaS applications. By integrating and analyzing data from all these sources, CISOs can answer questions like, "Which employees are using unvetted AI tools with corporate identities?" and "Which data are these applications accessing?". This enriched context is vital for understanding the relationships between users, entitlements, and resources across the entire ecosystem.

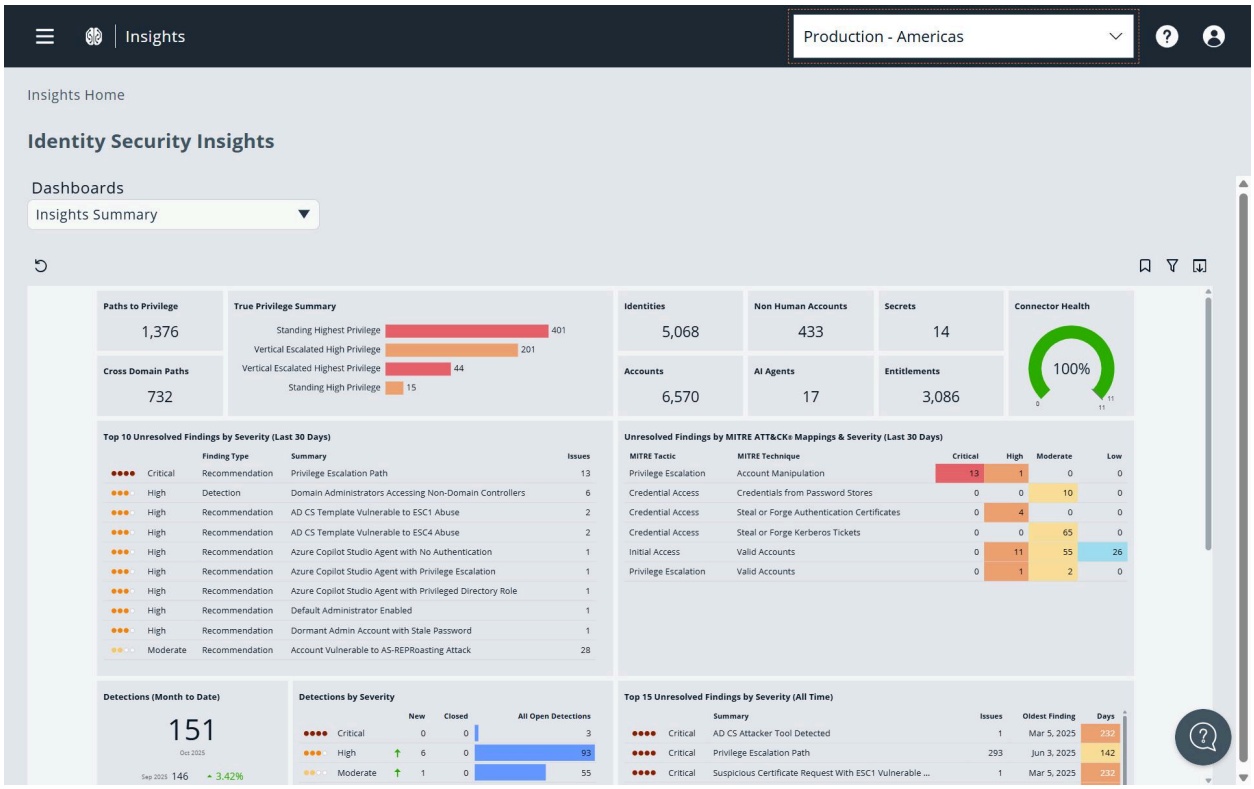

Figure 1: A consolidated view of privilege paths, unresolved findings, identity risks, and provider-based detections, provided by BeyondTrust Identity Security Insights®.

Use Case 2:
Detect Emerging Threats with Behavioral Analytics

Simply logging privileged sessions is no longer sufficient. Today, agentic AI can operate autonomously and rapidly with privilege, and attackers are leveraging advanced techniques that are easily masked as 'normal' user behavior.

Modern PAM incorporates advanced behavioral analytics to understand the context and intent over time. By analyzing patterns and deviations from normal behavior, the system can distinguish between legitimate administrative tasks and malicious activity. This is key to detecting subtle threats like session hijacking, Kerberoasting attacks, or anomalous activity from a compromised AI agent.

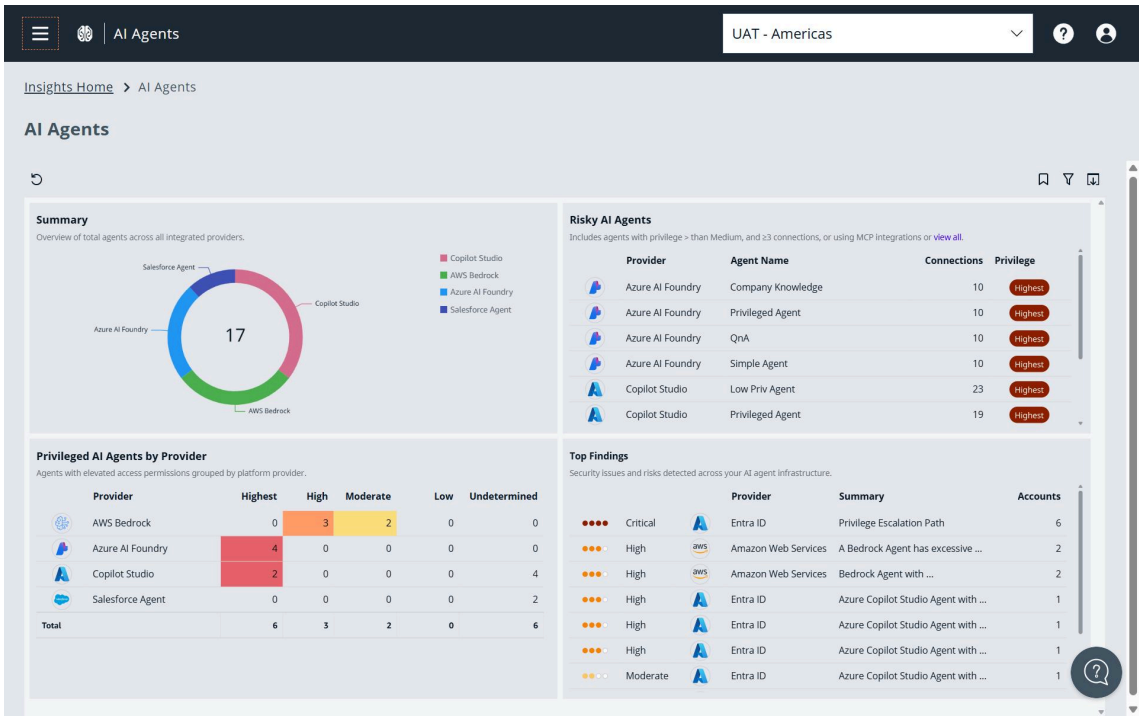

Figure 2: Identity Security Insights provides an overview of AI agent activity and associated risks across multiple platforms.

Use Case 3:
Secure Cloud Identities and Entitlements

Legacy controls weren't designed for the complexity of the cloud. IBM's X-Force has reported that cloud account credentials make up 90% of cloud assets for sale on the dark web, making it easy for threat actors to simply buy their way in.

Our modern PAM capabilities provide the granular visibility needed to secure cloud-native identities, ephemeral roles, and complex entitlements. This enables your team to uncover and mitigate risks like privilege escalation pathways within cloud applications, standing privileges, and excessive entitlements. It ensures cloud resources receive the same level of protection as on-premises identities.

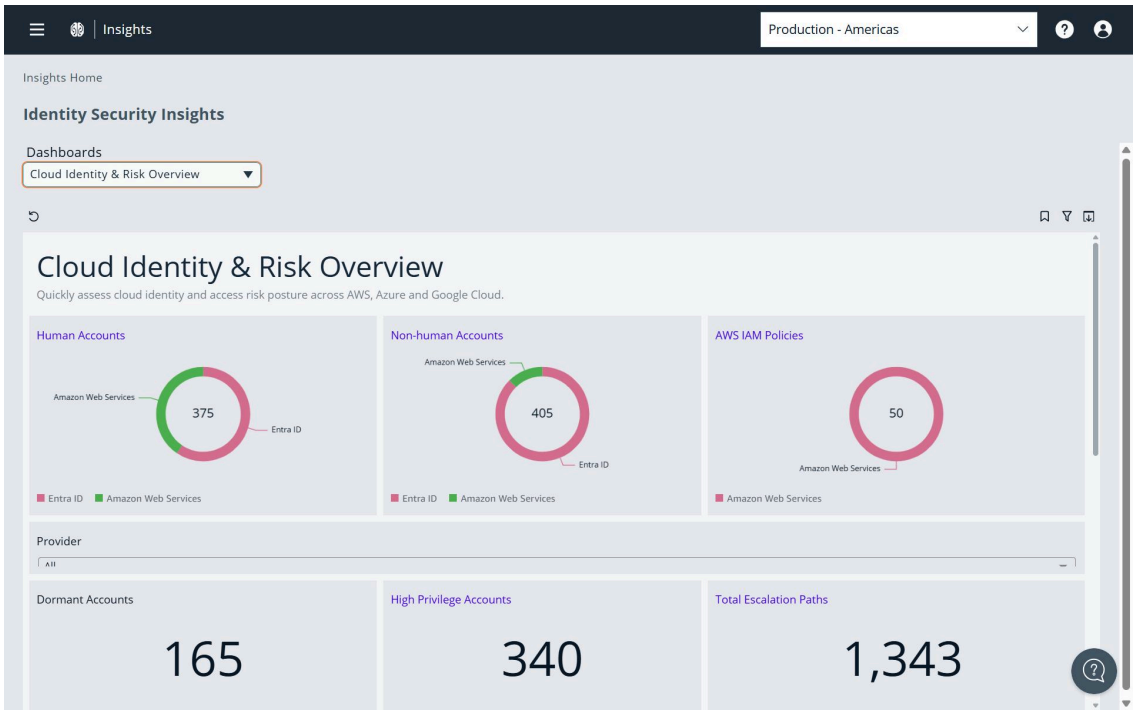

Figure 3: Identity Security Insights provides a centralized view of identity and access risks across AWS, Azure, and Google Cloud, enabling organizations to quickly identify exposure and prioritize risk mitigation.

Use Case 4:
Eliminate Excessive Privileges

In a dynamic environment, "privilege creep" creates a massive risk. Modern PAM champions the use of just-in-time (JIT) access to ensure users only get the access they need for the finite moments they need it. Instead of granting permanent admin rights, users get temporary, scoped privileges that auto-expire after the task is complete. This enforces a true least-privilege model and reduces the number of exploitable accounts in an environment.

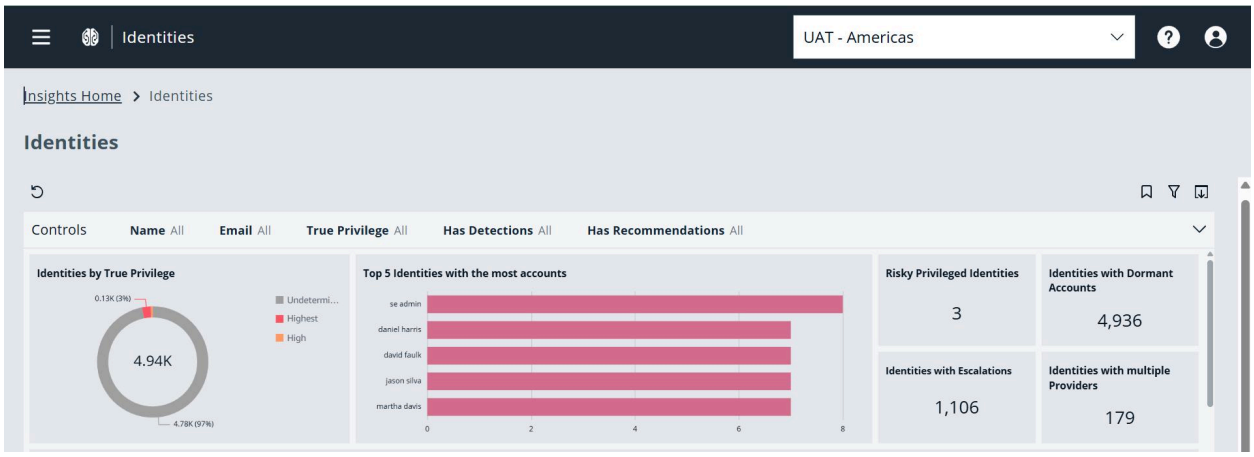

Figure 4: Identity Security Insights provides a comprehensive snapshot of identity access governance, highlighting the critical relationship between user privilege and security risk.

Use Case 5:
Simplify Management for Better Scalability

Juggling many different siloed tools is a significant resource drain in terms of time and money. We integrate these functions into one platform that simplifies deployment, streamlines management, unifies reporting, consolidates role-based access, and provides enhanced scalability. This reduces operational overhead and frees up your team to focus on mitigating risk rather than managing multiple, disparate solutions.

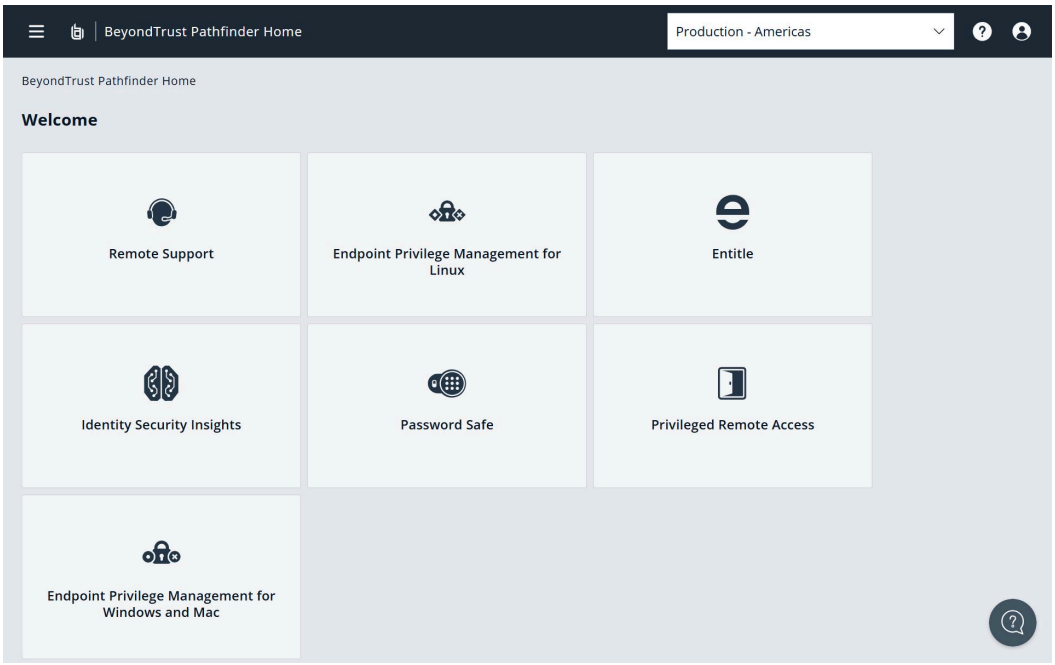

Figure 5: The BeyondTrust Pathfinder Platform unifies visibility and risk intelligence across all identities and assets, enabling organizations to discover, assess, and secure hidden pathways attackers could exploit—from one console.

The Modern PAM Toolkit in Action

The BeyondTrust Pathfinder Platform provides a cohesive management console across the entire BeyondTrust product portfolio, enabling shared intelligence and rapid response. This unified platform also includes three products that make up the core of BeyondTrust's modern PAM approach:

- **Identity Security Insights®:** Your intelligence engine and command center for risk-based prioritization. Identity Security Insights continuously discovers and analyzes identities, privileges, and escalation pathways across an environment, including on-premises systems, cloud platforms, hybrid environments, and SaaS applications. This deep visibility across human, machine, and agentic AI identities—and their pathways through your environment—enables you to proactively identify and prioritize security risks based on real-time data, actual usage patterns, and potential business impact.
- **Entitle:** The enforcement arm for achieving a reduced attack surface through the elimination of standing privileges. Entitle eliminates dangerous, always-on admin accounts by replacing them with just-in-time access. This limits the potential for lateral movement by attackers. When a user needs elevated access, they are granted a temporary, specific permission, which is auto-revoked when the task is done, improving both security and operational efficiency.
- **Privileged Remote Access:** The solution for secure, auditable remote access across IT and OT. Unlike VPNs, it provides secure, session-based access for employees, third-party vendors, and remote teams—without exposing the entire network. Every session is fully audited and monitored, giving you complete control and accountability for remote activity.

With Pathfinder, you can manage these modern PAM capabilities, together with BeyondTrust's foundational PAM capabilities, for a holistic approach to securing identities, privileges, and escalation pathways. Foundational PAM capabilities within the platform are provided by the following BeyondTrust products:

- **Password Safe:** A comprehensive solution for managing privileged accounts, passwords, keys, and secrets for people, machines, and AI agents. It centralizes the secure management and oversight of these accounts and credentials to ensure proper hygiene and minimize risk from common identity-based attack methods.
- **Endpoint Privilege Management:** The solution for enforcing least privilege across endpoints and applications to dramatically reduce cyber risk against malware, insider attacks, and other threats. The solution removes admin rights across Windows, macOS, Unix, Linux, IoT devices, and more to drive toward zero trust, while preserving productivity and improving operational performance.
- **Active Directory Bridge:** Your solution for streamlined identity management and access control across Windows, Linux, and Unix. This product extends Microsoft AD authentication, SSO capabilities, and Group Policy configuration management to Linux and Unix systems.

In addition, BeyondTrust Pathfinder also integrates our Remote Support solution, which supercharges service desk productivity, while also providing best-in-class security that can help organizations meet the most rigorous requirements across enterprise environments.

Value Propositions for the CISO: Addressing Critical Priorities

PAM modernization provides tangible value across the strategic priorities that matter most to your peers:

Holistic Risk Reduction and Improved Security Posture

Modern PAM capabilities enable CISOs to proactively identify and mitigate potential risks before they can be exploited. According to Microsoft Security, the average organization has 351 exploitable attack paths that threat actors can leverage to reach high-value assets. BeyondTrust Identity Security Insights monitors user behavior to detect entitlement creep, and flags potential misconfigurations. By implementing the principle of least privilege and JIT access via BeyondTrust Entitle, organizations can substantially reduce standing privileges, condense their attack surface, limit the blast radius of an incident, and enable a zero trust security posture.

Demonstrate Compliance and Achieve Audit Readiness

Modern PAM simplifies the process of maintaining compliance with regulations like GDPR, HIPAA, SOC 2, and PCI DSS. Entitle's granular access controls ensure users only get the minimum necessary permissions to perform their tasks, directly aligning with the principle of least privilege.

Identity Security Insights provides centralized visibility and comprehensive reporting capabilities to generate detailed audit trails for all privileged activity. This enables a state of continuous audit-readiness, reducing the burden and cost of compliance.

Faster Incident Response and Reduced Breach Impact

In the event of a security incident, fast and effective containment is critical. A modern PAM approach enhances incident response by providing real-time alerts. For example, Identity Security Insights can detect deviations from normal user behavior that may indicate a compromised account.

Privileged Remote Access allows security teams to access affected systems for faster investigation and remediation, while Entitle's just-in-time controls restrict lateral movement to reduce overall impact and cost of a breach.

Justify Security Investments and Communicate Risk to the Board

CISOs must effectively communicate the organization's risk posture in the language of the board of directors: risk, metrics, and ROI. Modern PAM provides quantifiable data to do just that. By highlighting tangible results—such as a demonstrable reduction in standing privileged accounts achieved with Entitle, or an improved compliance posture shown by Identity Security Insights—CISOs can effectively communicate the value of their security investment. Statistics on cloud breaches and excessive privileges are also powerful tools to justify the need for a modern PAM solution and secure board-level buy-in.

Maturing and Modernizing Your Identity Security Approach

To enable business innovation in the age of AI, CISOs must manage the explosion of identity-based risks that come with it. Foundational PAM controls are more important than ever, but they must be augmented to address the new frontier of shadow IT, AI agents, and complex cloud environments. Modernizing your approach to PAM provides this critical evolution, delivering the visibility, context, and dynamic control needed while safeguarding the organization's most valuable assets and its reputation.

Free Identity Security Risk Assessment

Gain an Attacker's Eye View of Your Identity Attack Surface

- Reveal account misconfigurations, overprivileged accounts, unused accounts, stale passwords, and other potential identity-based backdoors
- Understand the True Privilege™ of your environment and the hidden paths that could be used to escalate access or cross domains
- Receive prescriptive recommendations to improve your security hygiene
- Benefit from unrivaled insights to guide your identity security strategy

Start here: https://www.beyondtrust.com/assessment

Contact BeyondTrust today to get started with modernizing your PAM and Identity Security approach to reduce organizational risk, streamline compliance, and enhance operational performance: https://www.beyondtrust.com/contact

Additional Resources

- A PAM Maturity Model (guide)
- Buyer's Guide for Complete PAM (guide)
- Guide to Identity Security Defense in Depth (guide)
- How to Detect Session Hijacking Before It's Too Late: A Data Science Approach (research blog)
- From Heuristics to Histograms: Reinventing Kerberoasting Detections (research blog)
- "Evil VM": From Guest Compromise to Entra Admin In 9 Easy Steps (research blog)
- A Guide to Using Longitudinal Data Analysis for Improved Identity Threat Detection (research blog)
- Entra ID App Escalations: Attacks & Defenses (research blog)

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.**