BeyondTrust

Strengthening Cloud Identity Security: AWS and BeyondTrust's Integrated Approach

BeyondTrust

TABLE OF CONTENTS

Introduction

Accelerate Cloud Adoption and Expansion with Confidence

The cloud is an engine and platform providing seemingly infinite potential for innovation. It empowers organizations with speed, elasticity, and scale, so they can launch services faster, meet global markets where they are, and embark on continuous digital transformation. With AWS, organizations everywhere are modernizing applications, streamlining operations, and rapidly responding to evolving customer needs.

However, to fully reap these benefits, organizations must ensure security is incorporated by design. For many organizations, striking the right balance between leveraging opportunities in the cloud, while minimizing cloud risks, continues to represent a fundamental challenge. This is where the collaboration between BeyondTrust and AWS provides value. Together, they help customers adopt cloud services with enhanced security features—implementing identity and access controls, addressing Paths to Privilege™, and helping protect sensitive resources. Through this partnership, organizations of all sizes can implement security controls from the start, supporting their digital transformation, while helping improve productivity.

In this guide, discover the power of the joint approach, and how you can unlock the benefits.

Defining Identity Security for the Cloud

What is identity security? Ask a dozen cybersecurity professionals and a dozen Identity and Access Management (IAM) practitioners and you may arrive at two dozen different answers. The truth is, not even the analyst community can agree on a single definition for identity security. So, for the purposes of this guide, we provide you with the most common definition and the appropriate use cases, as applied to the cloud.

Identity security is the practice of implementing protection measures for digital identities—both human and non-human (machine)—and managing access to systems, applications, and data. It focuses on helping ensure the right individuals have the appropriate access to the designated resources when needed.

The goal of identity security practices is to reduce unintended access and address potential risks based on activity patterns. Identity security combines multiple established disciplines and practices, such as Identity and Access Management (IAM), Privileged Access Management (PAM), Cloud Infrastructure Entitlement Management (CIEM), Identity Detection Threat and Response (ITDR), authentication, access management, and continuous monitoring. These capabilities help protect identities across cloud, on-premises, and hybrid environments.

Identity security plays a critical role in defending against modern cybersecurity risks like identity-based attacks, credential theft, and lateral movement, including some risks that crisscross domains.

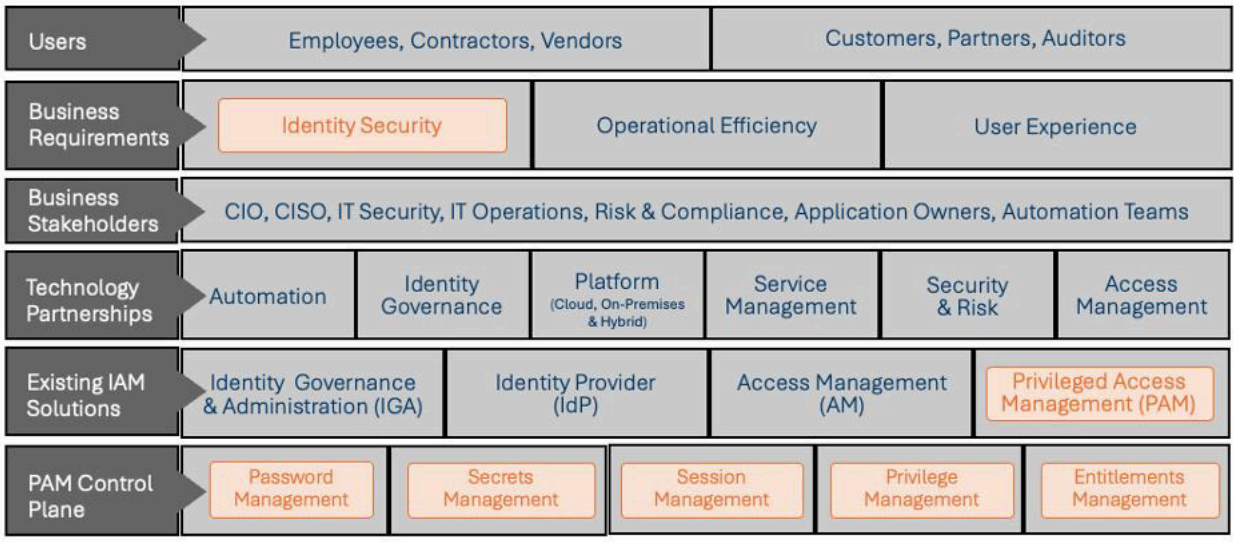

Figure 1: An illustration of the importance of identity security to corporate environments, and relationship to modern PAM deployments.

6 Essential Identity Security Controls for Cloud Environments

With the above identity security definition in mind, here are six key ways identity security controls can help address core challenges in cloud environments:

1 Just in Time (JIT) Access

Standing access (persistent, 24/7 privileges) proliferates across cloud and SaaS environments. This means entitlement, permission, or privilege is always in an active state that is ready for use or abuse. Yet, many of these risky standing permissions are rarely, if ever, needed and sit unused.

A JIT access model limits elevated access to the exact moment it's needed, and nothing more. It helps decrease the scope of potential unintended access by reducing standing privileges that could be exposed to unauthorized users.

A JIT implementation helps ensure users and systems receive precise permissions only when required, and only for the finite moments needed, potentially reducing periods of elevated risk and supporting efforts to enhance security postures. JIT access is designed to support the implementation of a least privilege model and zero trust principles across the cloud.

2 Secure Remote Access (SRA)

Just as with privilege, remote access is a vector in almost every attack. Cloud environments multiply the potentially insecure remote pathways that can give attackers a foothold. In fact, 76% of cloud accounts sold on the dark web have RDP access.

A modern secure remote access approach adheres to zero trust network access (ZTNA) principles and enables employees, contractors, and vendors to connect to critical systems from anywhere, without compromising security. These solutions essentially extend PAM best practices to anywhere, and enforce least privilege, robust authentication, and session monitoring to minimize risk.

By implementing access controls and audit capabilities, organizations can help protect data, support compliance efforts, and decrease the scope of potential unintended access in an increasingly remote work environment. This approach can reduce reliance on legacy technologies like VPN or VDI.

Password Management

Unmanaged credentials can present a direct route into your cloud environment. Attackers increasingly leverage legitimate user credentials to gain access into victim environments. One prominent research study found that cloud account credentials alone make up 90% of for-sale cloud assets on the dark web.

Password management enables teams to manage and secure these valuable credentials by generating, vaulting, and protecting strong, unique passwords for every account. It minimizes risk, prevents unauthorized access, and strengthens digital defenses. And no credentials are more important to manage than those for privileged accounts. Modern enterprise password managers automate this process, simplifying security for users and reducing human error.

Secrets Management

Unauthorized users may take advantage of DevOps environments hosted in the cloud, seeking and exploiting hardcoded secrets hidden within code. Exposed secrets, such as API keys and certificates across systems and applications, can be used to gain unauthorized access to critical systems. 70% of organizations have unencrypted secrets in code repositories, making it a common pathway that can be used to gain a foothold in cloud environments.

While conceptually similar to password management as described above, secrets management often benefits from specialized tools designed for the rapid pace and dynamic nature of DevOps, CI/CD pipelines, and cloud environments. Ideally, such solutions provide centralized visibility to gain control over secrets sprawl, a common problem that presents high risk to organizations. Secrets management helps support access control processes so that authorized users and non-human identities can access secrets through just-in-time provisioning principles.

Implementing effective secrets management can help decrease the scope of potential unintended access, support risk reduction from internal users, and enhance protection against supply chain risks—all working together to help defend an organization's critical digital resources.

Cloud Entitlements Management

Excessive entitlements present a widespread challenge across the cloud, creating multiple layers of permissions that can increase the scope of potential unintended access. Unauthorized users may utilize excessive entitlements to gain initial access or expand their reach within the environment. Despite these potential risks, many organizations may unintentionally configure excessive privileges as default settings.

Entitlements management helps organizations by controlling access to specific resources, ensuring appropriate users receive suitable permissions only when needed, aligning with a JIT access model. It supports organizations by reducing excessive privileges, decreasing risks from internal users, and containing potential security events. Entitlements management strengthens critical systems protection, enables least privilege practices, and supports compliance requirements with 'need to know' access and permission controls.

Identity Threat Detection and Response (ITDR)

Organizations today often manage multiple complex systems and diverse identity stores. This can create separate silos that may not intercommunicate effectively, potentially leading to identify-based security risks—especially those that span across different domains.

Identity Threat Detection and Response (ITDR) is a discipline that provides a comprehensive approach to identify and address identity-based security risks across cloud, hybrid, and on-premises environments. ITDR pairs proactive controls for identity-based hardening (such as identifying and remediating unmanaged privileged accounts, orphaned accounts, multi-factor authentication gaps, and persistent access) with detection and response capabilities.

ITDR solutions aim to provide continual monitoring, behavior analytics, and automated responses to suspicious access patterns. This holistic approach helps reduce lateral movement and potential security incidents. When used alongside cloud-native security tools, ITDR supports zero trust principles by helping ensure only verified users and devices access sensitive resources across hybrid and multicloud infrastructures.

When selecting a vendor for these use cases, consider one with deep understanding of cloud security who collaborates closely with the cloud provider to address identity and privileged access security challenges that could affect an environment. Look for a vendor with a strong partnership with the cloud provider and integrated cloud security models in their solutions. A robust partnership, such as between AWS Security and BeyondTrust, can help you manage security and compliance efficiently, minimizing potential gaps between the two vendor technologies. **Read on to learn more about this true partnership.**

AWS Security

AWS provides cloud services for private cloud environments, as well as a platform for delivering new solutions. When developing new solutions, AWS recommends following established guidelines for security, compliance, access control, and hardening. Many of these security controls can be designed into a vendor's AWS cloud offering and produce automated reporting that demonstrates compliance with regional regulations, regardless of data residency and runtime.

This process is part of the AWS Competency Program. The program validates partner expertise in building software or delivering services across industries, use cases, and workloads.

Among the competencies offered is the AWS Security Competency. AWS Partners with the Security Competency have demonstrated deep technical expertise with security on AWS and proven customer success in securing the cloud journey with their software and service offerings. BeyondTrust achieved this competency in April 2024, enabling the implementation of AWS security best practices combined with BeyondTrust's specialized identity security features and use cases.

BeyondTrust and the Pathfinder Platform

BeyondTrust is a global, multi-discipline identity security solutions leader. The BeyondTrust Pathfinder Platform empowers organizations with a cohesive, one-console approach for addressing critical identity security challenges and use cases. Pathfinder is hosted as a SaaS solution on AWS and implements AWS security best practices in its design, architecture, and compliance reporting capabilities.

As a platform that integrates BeyondTrust's products into a single console with shared intelligence, Pathfinder offers an advanced vehicle for the six essential identity security areas described earlier in this paper, and more. Key cloud and hybrid security capabilities include:

- **Holistic Identity Risk Visibility** across clouds and domains, with a visual mapping of True Privileges™, which includes all possible escalation pathways of identities.
- **Password Management**, for automatically discovering, vaulting, and managing every privileged credential—both human and non-human.
- **Secrets Management**, for securing and controlling access to secrets used in DevOps tools, workflows, and CI/CD processes.
- **JIT Access & Least Privilege Management**, with automated permissions management and self-serve workflows to ensure access is fine-grained and time-bound.
- **Secure Remote Access**, for applying robust security controls to all remote access and eliminating the need for VPNs, while also supercharging IT productivity.

- **Cloud Infrastructure Entitlement Management**, with flexible identity security controls for managing identities and entitlements in cloud environments.
- **Identity Threat Detection and Response**, with a view of all accounts, privileges, paths to privilege, and access levels for rapid detection and response to risks.

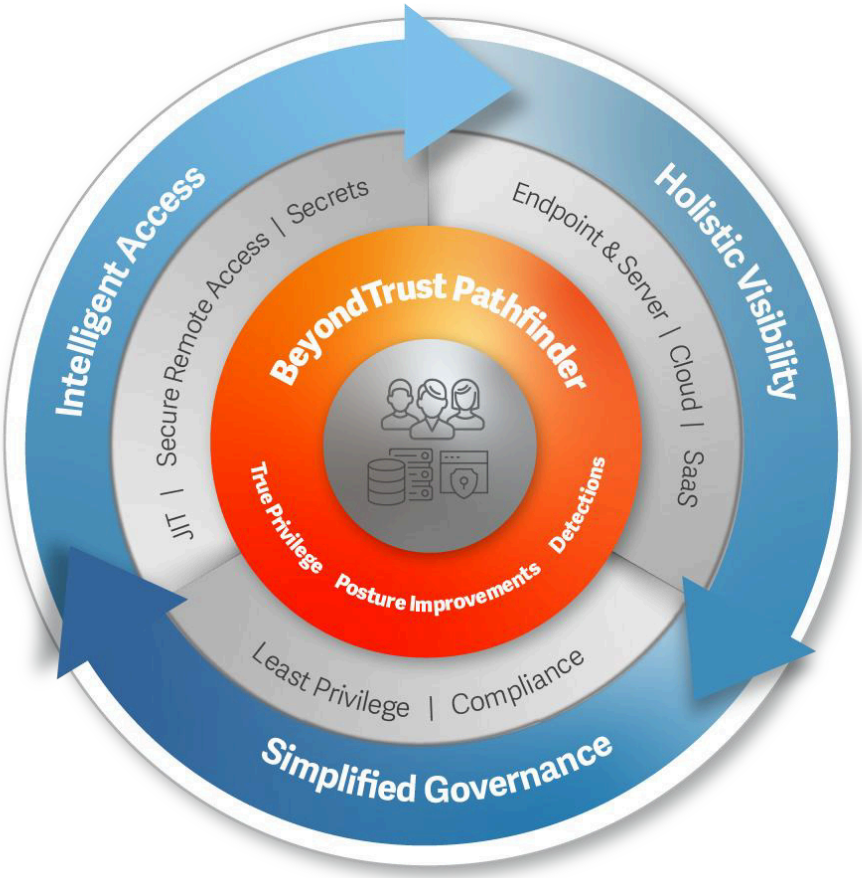

Figure 2: The BeyondTrust Pathfinder Platform—a modern, unified platform for identity security

With Pathfinder, organizations can also leverage AI/ML and key integrations to find, manage, and protect the Paths to Privilege™ that are most dangerous to organizations in the cloud today. With BeyondTrust Pathfinder, organizations are empowered to continuously know, prioritize, and manage the most impactful identity security risks across their heterogeneous environments.

As discussed earlier, PAM is a core component in any identity security strategy, helping reduce potential risks through privilege management and enhanced access controls.

Pathfinder extends PAM capabilities across the entire identity ecosystem. By combining preventative controls with advanced detection capabilities and privilege path discovery, the platform offers a comprehensive approach to help identify potential identity security gaps, decrease the scope of exposure, and support least privilege implementation. The BeyondTrust solution is designed to address the use cases defined in this guide for identity security, while implementing AWS recommended security best practices.

The Pathfinder platform delivers additional capabilities that help organizations reduce identity-based risks and prioritize the most impactful remediations, all in one place.

This includes:

True Privilege™ Graph and Continuous Risk Assessment: Visual privilege mapping provides detailed and context-rich visibility into identities (human, machine, and workload), entitlements, and privilege escalation paths across cloud, hybrid, and on-premises environments.

The Pathfinder platform uses advanced capabilities to provide deep analysis, helping organizations identify and address the true privilege of identities.

Unlike static, role-based access models, BeyondTrust Pathfinder maps privilege relationships dynamically, regularly updating access pathways and helping identify potential security risks. This includes indirect permissions, deviations from least privilege principles, and identity-based misconfigurations. These BeyondTrust capabilities help organizations to accurately measure the impact of security risks and implement proactive measures.

> "BeyondTrust's solution has impacted our business by giving us peace of mind around the security of our customers' data and also giving us a very robust audit trail to ensure the integrity of that at all times, and allowing us to put in the appropriate safeguards to ensure we're always in front of any potential security vulnerabilities."
>
> **— Shane Carden, CIO, Behavox**

Pragmatic AI-Powered Security: The Pathfinder platform simplifies identity security and empowers organizations of all sizes to implement advanced capabilities.

The Pathfinder platform's AI capabilities extend beyond basic alert generation by helping automate detection escalation, and supporting efficient risk remediation. These features assist customers in analyzing privilege patterns, entitlement changes, and access behaviors. This approach helps organizations proactively decrease their scope of potential exposure by identifying and addressing risks related to excessive privileges, configuration issues, and undocumented privilege paths.

> "Our workflows were highly inefficient and there was a lot of friction and frustration. But BeyondTrust changed that with Identity Security Insights, and we are able to tailor our alert settings. This way, it significantly reduces unnecessary alerts. There's more accurate threat detection which reduces our false positive rate and Insights, powered by AI and Machine Learning, adapts to my inputs. It learns from how I process detections and recommendations. It's continuously evolving alongside my business."
>
> **— Anna Essex, Sr. Security Analyst, Polsinelli**

Adaptive Just-in-Time (JIT) Access: The Pathfinder platform helps decrease the scope of potential exposure by managing unnecessary privileges and enabling access only when needed, for specific durations, while supporting operational agility. Building from foundational PAM, Pathfinder enhances adaptive JIT access capabilities, which use identity risk context to enable dynamic, conditional access decisions. These features are designed to help reduce the impact of security incidents.

Unlike alternative solutions that can only apply just-in-time access controls across a few select environments, the Pathfinder platform applies JIT controls across the entire identity estate to get control over entitlement sprawl and eliminate standing privileges.

> "Employees do the maximum using minimum permissions. [Billie] has embraced JIT access as a standard practice and now experiences a notable reduction in standing permissions. The task of reviewing user access has become manageable, thanks to [BeyondTrust] Entitle's system which efficiently supports a modern tech stack on a large scale."
>
> **— BeyondTrust Customer at Billie**

Security and Scalability with the AWS & BeyondTrust Partnership

When a cloud provider and a security solutions vendor partner to deliver enhanced security features, customers benefit the most. AWS and BeyondTrust aim to provide:

- A comprehensive platform approach to SaaS identity security, designed with security and compliance best practices reviewed by both AWS and BeyondTrust.
- Support for global compliance efforts, with automated reporting capabilities to help demonstrate adherence to regional requirements. The solution is designed to require minimal changes at deployment to support local data sovereignty regulations.
- Enhanced security features in the design, including compliance controls, change management, access controls, encryption capabilities, and data segmentation for backend operations and management. These features are intended to help reduce the likelihood of the identity security solution itself becoming a potential area of concern.

Conclusion

When addressing identity-based security challenges, implementing technology designed to help protect against modern IT security risks is important. It's also crucial to consider how this technology, as part of your supply chain, can be implemented to help minimize potential security concerns.

When cloud service providers and SaaS vendors collaborate to offer solutions that address contemporary security challenges and incorporate cloud security and compliance best practices, organizations can benefit from this approach of integrating security considerations early in the design process.

AWS and BeyondTrust aim to support this objective for Identity Security, working to provide enhanced protection against potential identity-related security risks.

To license BeyondTrust solutions from AWS, please visit the AWS Marketplace.

Learn More

- Premier Bankcard AWS Case Study
- Texas A&M University Case Study
- GigaOm CIEM Radar Report
- PAM Buyers Guide
- KuppingerCole ITDR Report
- Entitle SC Award

About BeyondTrust

BeyondTrust is the global cybersecurity 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 AWS Security

AWS implements a shared responsibility model where AWS helps maintain "security of the cloud," protecting the infrastructure that runs AWS services, while customers and partners like BeyondTrust implement "security controls in the cloud," including identity management, data protection, and application security. BeyondTrust builds upon AWS's enhanced security features by integrating with AWS services and implementing AWS security best practices. This approach helps organizations to achieve comprehensive identity security controls while leveraging AWS's global infrastructure.

Learn more at **aws.amazon.com**