WHITE PAPER

AZURE PIM VS. BEYONDTRUST PAM

Comparing Azure Privileged Identity Management (PIM) to BeyondTrust Privileged Access Management (PAM)

BeyondTrust

TABLE OF CONTENTS

1 Introduction

Security teams who seek to meaningfully reduce their organization's attack surface by better controlling privileged access in their environment are faced with an increasingly more complex and decentralized IT infrastructure. Any decision on which tool, or tools, are best fit to tackle this problem must be balanced by the ever-expanding scope and types of privileged accounts that need to be managed.

The scale of managing the exploding universe of privileges requires an integrated approach, instead of relying on a stack of niche tools, each only helping to manage a slice of the privilege problem.

Many organizations are quickly adopting and migrating their infrastructure to cloud providers, such as Microsoft's Azure. However, in most cases, native toolsets offered by cloud providers provide only basic controls and incremental amounts of risk reduction around the cloud's privileged access problems. The native toolsets are not designed to fully and adequately solve the core problems inherent to unmanaged privileged access. And, these tools only help address a small slice of the Azure privilege problem itself, while providing no coverage across the rest of an organization's privilege universe.

This document reviews and compares the privilege management capabilities of Azure Privileged Identity Management (PIM), which provides some basic functionality, to BeyondTrust Privileged Access Management (PAM), which is recognized by Gartner, Forrester, and KuppingerCole analysts as a PAM leader and offering a complete solution.

> *The scale of managing the exploding universe of privileges requires an integrated approach, instead of relying on a stack of niche tools, each only helping to manage a slice of the privilege problem.*

2 Azure Privileged Identity Management (PIM)

Designed as a feature in Microsoft's cloud directory services, Azure Active Directory, Azure PIM adds enhanced control and auditing in front of Azure AD's more sensitive roles and resources, as well as other Azure components, such as Office 365.

As part of Microsoft's Premium P2 or EMS E5 licenses, Azure Active Directory customers can enable the optional features of Privileged Identity Management for Azure AD services. The PIM tool specifically pertains to Azure AD roles and does not extend to other platforms outside of Azure. For other infrastructure, such as the workstation environment, Microsoft continues to recommend existing tools such as the Local Administrator Password Solution (LAPS) that rely on on-premises Active Directory infrastructure. (Note that LAPs itself is a very basic tool, learn more at "What Does Microsoft Local Administrator Password Solution Really Do?").

The PIM tool specifically pertains to Azure AD roles and does not extend to other platforms outside of Azure.

With Azure PIM, direct or standing access to your more sensitive Azure AD roles can be restricted, and time-based or approval-based workflows may be implemented. Users may request access to roles, such as the Global Administrator role, and be granted approval for a configurable period of time, after which the privilege is removed. All requests and approvals are logged, and 'access reviews' can be conducted to better identify who requires access to certain roles based on their activity over a time period. In this model, Microsoft contends that Azure AD PIM replaces the traditional network security perimeter of access to privileged roles with the identity layer.

From Microsoft's documentation, the Azure PIM tool has the following primary use cases:

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit

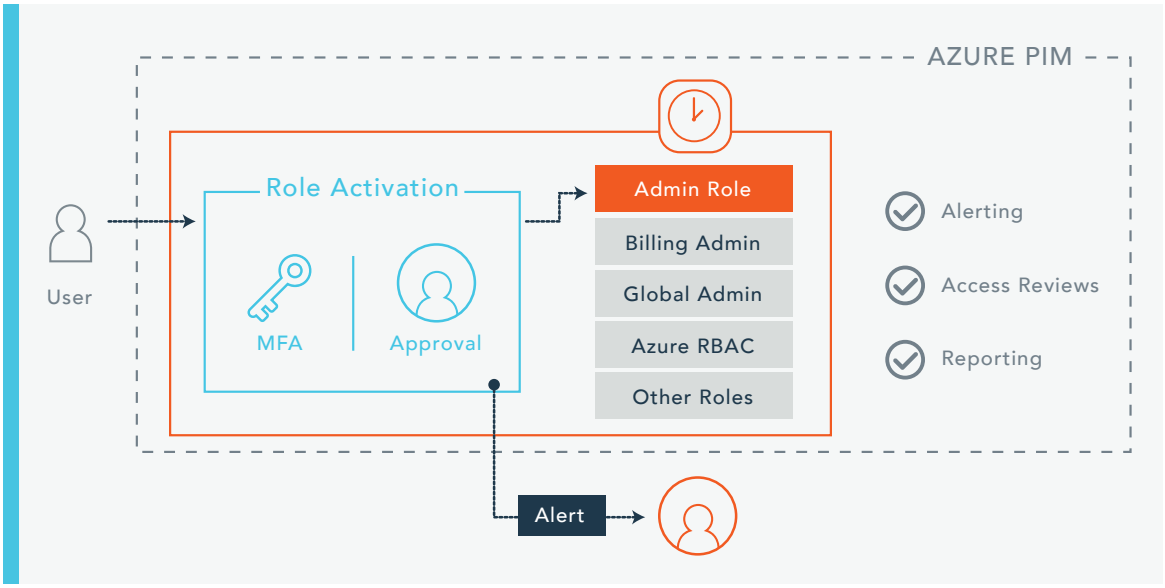
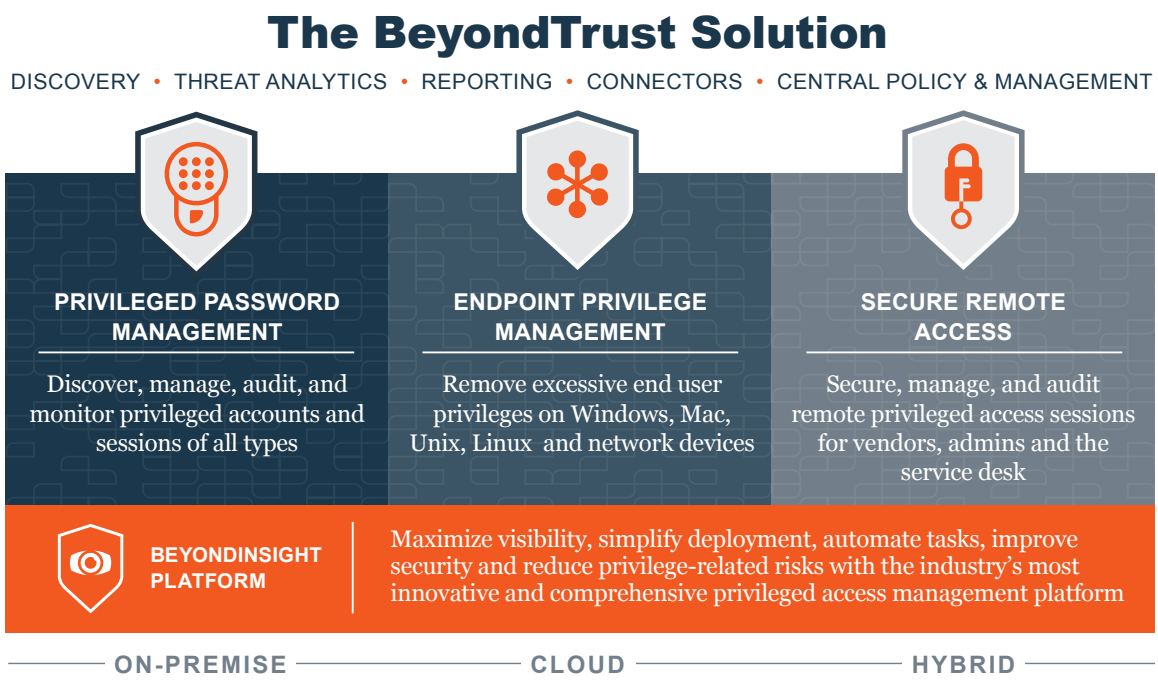


Figure 1: "How PIM Works." Azure PIM in a simple flow-diagram; at the time a user needs to step-up their access within Azure AD to an eligible role, they must follow MFA and gain approval. They're then given either short or long-term access.

3 BeyondTrust Privileged Access Management

Our comprehensive privileged access management portfolio of integrated solutions enables you to tackle privileged access management starting from your chosen areas of highest risk, whether on the workstation side, server estate, or both.

BeyondTrust PAM solutions include Endpoint Privilege Management, Privileged Password Management, and Secure Remote Access.



Overview By Solution

Endpoint Privilege Management allows you quickly and easily remove Local Administrator Rights (LARs) across Windows, macOS, and Linux/Unix devices without the associated impact to end user productivity. The solution was designed to start and stay simple throughout deployment, distilling a once-complex process into an easy-to-follow and proven methodology. By removing rights from user and instead assigning it to specific applications, this solution drastically reduces risk by eliminating the largest and, often, highest-risk pool of privileged accounts that exists in many environments - Local Administrators.

Privileged Password Management secures and manages the privileged accounts that remain after successfully eliminating LARs, namely your 'keys to the kingdom' accounts such as Domain Administrators, Linux/Unix root accounts, workstation administrators, SaaS or cloud accounts, etc. The solution is designed to address as many different types of privileged accounts on as many different platforms as exists across your organization: legacy IT systems, workstations, servers, SaaS/IaaS/PaaS platforms, Linux/Unix devices such as firewalls or switches, etc. By providing privileged password and session management in one solution, all your organizations' most sensitive privileged access requirements are met.

Secure Remote Access doesn't leave securing remote control of your organization's assets to only the identity of the person making the connection; it secures the connection itself. Our remote access solution allows you to safely provide remote connectivity to privileged resources across even the most decentralized networks, all without a VPN being necessary. Secure Remote Access mitigates the risk associated with 3rd parties, vendors, and even internal users who would like to connect from a device that may be compromised, by ensuring those devices have no ability to spread through that open connection.

Primary Use Cases By Solution

Endpoint Privilege Management

- Quickly and easily eliminates Local Administrator Privileges across the end-user estate for Windows, macOS, and Linux/Unix workstations and servers
- Ensures users remain productive, with customizable end-user messaging and an experience appropriate to their role
- Enforces an easy-to-manage application whitelist and/or blacklist to further reduce risk of malware infection
- Proactively reduces exposure to advanced fileless malware through context-aware application whitelisting (trusted application protection)
- Works offline and supports a distributed, remote workforce

Privileged Password Management

- Minimizes the risk of your privileged accounts from being compromised by vaulting and rotating passwords/SSH keys on a schedule and after every use
- Utilizes credential injection so that end users never see the password
- Integrates with existing identity providers and MFA platforms
- Provides secure, audited management of break glass Administrator accounts that doesn't require putting passwords down on paper
- Ensures a full and detailed audit record of every session involving privileged access
- Locks down management of Azure/O365 Global Administrator roles by restricting network traffic to only the solution itself
- Requires approval, notification, or ITSM workflows when accessing particularly sensitive assets
- Works across a huge variety of systems and account types, not just a single platform

Secure Remote Access

- Secures network architecture where all traffic is encrypted via HTTPS. No port-forwarding or firewall reconfigurations are necessary
- Provides access to untrusted third parties, giving them only the right level of access into your environment, mitigating the threat of a potentially infected system spreading laterally
- Offers an intuitive and powerful web, thick client, and iOS/Android interface
- Provides detailed audit records and alerting, as well as integration into identity providers (such as Azure) with built-in MFA
- Provides access to web pages such as the Azure or Office 365 portal through a locked-down chromium browser that supports automatic web credential injection and logs session recordings
- Securely injects managed credentials into remote access sessions, applications, and web pages to add additional abstraction layers between the user and privileged secrets

4 Capability Comparison

BeyondTrust PAM	Azure PIM
FEATURES	
• Most comprehensive PAM feature set. Eliminates majority of admins using Endpoint Privilege Management and securely manages remaining privileged accounts with Privileged Password Management • Eliminates standing/persistent administrator access across all platforms • Deploys in hours and days, not weeks or months • Minimizes impact to users and IT administrators, while achieving security goals	• Specific to Azure AD / Office 365 accounts as well as certain 3rd party web applications • No session management capabilities • Not applicable to Local Administrator (LAR) accounts on Windows, macOS, or *Nix • Not applicable to most other platforms, such as Linux/Unix, database, thick-client applications, etc. • Requires Azure AD and Azure AD managed devices when using PIM to delegate Device Administrator role • Does not eliminate standing administrators across all platforms • Conditional Access policies can limit suspicious logins. Needs extensive configuration, and doesn't apply restrictions after the user successfully authenticates, only at the point of authentication

3 Capability Comparison Continued

BeyondTrust PAM	Azure PIM
SECURITY	
• Endpoint Privilege Management ensures the user runs from the safety of a standard user account. Pass-the-hash (PTH) and Token Hijack attacks are mitigated • Trusted Application Protection proactively prevents fileless malware through commonly manipulated tools, such as the Office suite, Adobe Reader, and web browsers • Privileged Password Management ensures privileged accounts are rotated on a schedule as well as after every use, so that any compromised credential is quickly invalidated • Session management hides the credentials from the user and forces all traffic to be routed through our password solution's secure proxy • Secure Remote Access extends access to Azure or internal resources without a VPN and without adding risk • Reports are detailed with video and text-based logging of all activity and processes that are launched, ensuring a complete and immutable audit record	• Reporting is specific to logins and approvals granted within the system, not activity within privileged sessions • Conditional access polices (part of Azure AD) are specific to the point of authentication, not what happens after (user activity) • 'Device Administrator' role applies to all devices, not subgroups – a user has admin access to all end-user devices simultaneously • Just-in-time and time-bound access is often used improperly; many users require such frequent access to privileged roles that the time expiry becomes forever! • Microsoft recommends two break glass Global Administrator accounts need to be managed separately from any MFA or other controls provided by Azure PIM
PASSWORD VAULTING	
• Full-featured password management and rotation capabilities for both human and non-human identities across a large number of platforms • Credential injection abstracts secrets from the user so that they're not used in other tools • Endpoint Privilege Management reduces the need for many privileged accounts to exist in the first place – why rotate a password when you can eliminate the risk entirely!	• No password vaulting capabilities • LAPS (legacy password management solution) requires on-premises Active Directory and a network connection to Domain Controllers

3 Capability Comparison Continued

BeyondTrust PAM	Azure PIM
INTEGRATIONS	
• Open integration framework • Integrates with major ITSM, SSO, MFA, SIEM, Threat Intelligence, and IDAM (via SCIM) tools	• SCIM identity provisioning protocol
DEPLOYMENT	
• Flexible deployment options across the product portfolio, including SaaS and on-prem models • Does not require Azure AD	• Requires Azure AD Premium P2, or E5 licenses • Only deployed through Azure AD

Questions to Ask

Completeness of Coverage

- How does the tool work for non-Azure or Azure AD-based services, such as SSH into Linux devices?
- Does the tool address the entire environment to your satisfaction, or are there gaps?
- Does the tool manage service accounts and application-to-application accounts (non-human identities)?

Security

- How do you address Local Administrator Privileges across your workstation and server environments?
- How do you protect against Device Administrator accounts being compromised and opening the door to the entire Azure-managed environment?
- Is a 'Device Administrator' role that allows designated users to have admin access across all Azure AD-joined devices acceptable?
- How will you safely and securely manage the credentials of the Microsoft recommended Global Administrator break glass accounts?
- As Azure PIM only secures access at the identity layer, do you still see risk in users connecting to internal networks from external or unmanaged devices that may be compromised?
- What tools would they then use to facilitate the connection, and can you verify their authenticity and any security gaps those tools may introduce?
- Are these privileged identities separate from the users' normal identities? Is anything preventing them from using the same passwords on both accounts, as users tend to do?

Reporting & Auditing

- Are lists of logon event details and reports on privileged roles within Azure AD enough to satisfy auditing requirements?
- Does the tool/solution provide full session recordings, audit logs of privileged activity, and more granular command/privilege management within user sessions?

Ease of Administration

- Who will be tasked with managing requests for access and how much resource overhead will this place on your security team?
- Could credential rotation and injection mitigate the risk of standing administrator privileges being granted, as the users would never have 'standing', unfettered access to privileged account credentials?

5

Reduce Risk Effectively & Enable User Productivity with PAM

For threat actors—whether internal or external—waging an attack on your environment, the highest priority is to gain elevated privileges as early as possible. Privileged access that is not effectively managed—especially when users are provisioned with administrator-level access on their workstation—provides the attacker with easy shortcuts to compromising your environment and moving laterally within it.

Leaving IT admins with unfettered and unmanaged access to your organization's most sensitive resources is a proven recipe for recurring breach events and audit fails. Across the desktop environment, the need to keep users happy and productive—especially technical or VIP users such as doctors, developers, technicians, and engineers—forces many IT organizations to provide users with a full administrator account on their desktop or laptop. Similarly, in the server estate, sysadmins consistently perform functions that require high-privileged accounts. In an effort to keep these extremely technical users flexible, they are often provisioned with standing/persistent administrative access to the resources under their control. All of these risks are unjustifiable and can be resolved with the right privileged access controls.

Privileged access management means many different things to different organizations and often represents itself as a journey.

When considering an investment into tools that solve these problems, it is especially important to balance cost and complexity against efficacy, and the ability of the tool to deliver across the entire scope of your environment.

When considering an investment into tools that solve these problems, it is especially important to balance cost and complexity against efficacy, and the ability of the tool to deliver across the entire scope of your environment.

BeyondTrust delivers the industry's most complete and flexible PAM platform. Our PAM platform is comprised of three integrated solutions that can manage your entire universe of privileges—whether it Azure, AWS, Google, on-premise, Unix, Linux, Windows, macOS, human, machine, insider, or vendor. And, we can manage and report on these privileges in a unified way that integrates with the rest of your IT and security infrastructure—including IAM, ITSM, SIEM, and more.

Learn more at beyondtrust.com/solutions.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

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 78 of the Fortune 100, and a global partner network.

beyondtrust.com

2020_09_ENG