BeyondTrust and Beyond Identity Partner for Zero Trust PAM

Strong authentication for the administrator and the device they are using to access privileged accounts is a foundational underpinning of zero trust.

Overview

BeyondTrust and Beyond Identity have teamed up to deliver integrations that advance zero trust for the most sensitive accounts at every enterprise. The combined solution integrates Beyond Identity's unphishable, passwordless multi-factor authentication (MFA) with BeyondTrust's Endpoint Privilege Management Cloud and Privileged Password Management solutions, ensuring that only authorized users and secure devices can gain privileged access to critical systems.

Key Benefits:

- ✓ Implement strong, unphishable MFA and policy-based access controls to ensure high-trust authentication for admin accounts
- ✓ Ensures only devices that meet the company's security policy have access to admin accounts
- ✓ Establish identity before privileged actions on an endpoint are allowed using a frictionless step-up authentication
- ✓ Create a zero-trust PAM architecture - don't trust the user until they pass a high-assurance authentication and don't trust their device unless it meets security policies

Privileged Password Management Integration

The combined solution ensures that all privileged account access requests include a very strong passwordless and unphishable MFA challenge–ensuring that only trusted administrators, using authorized and secure devices gain access to the most important accounts.

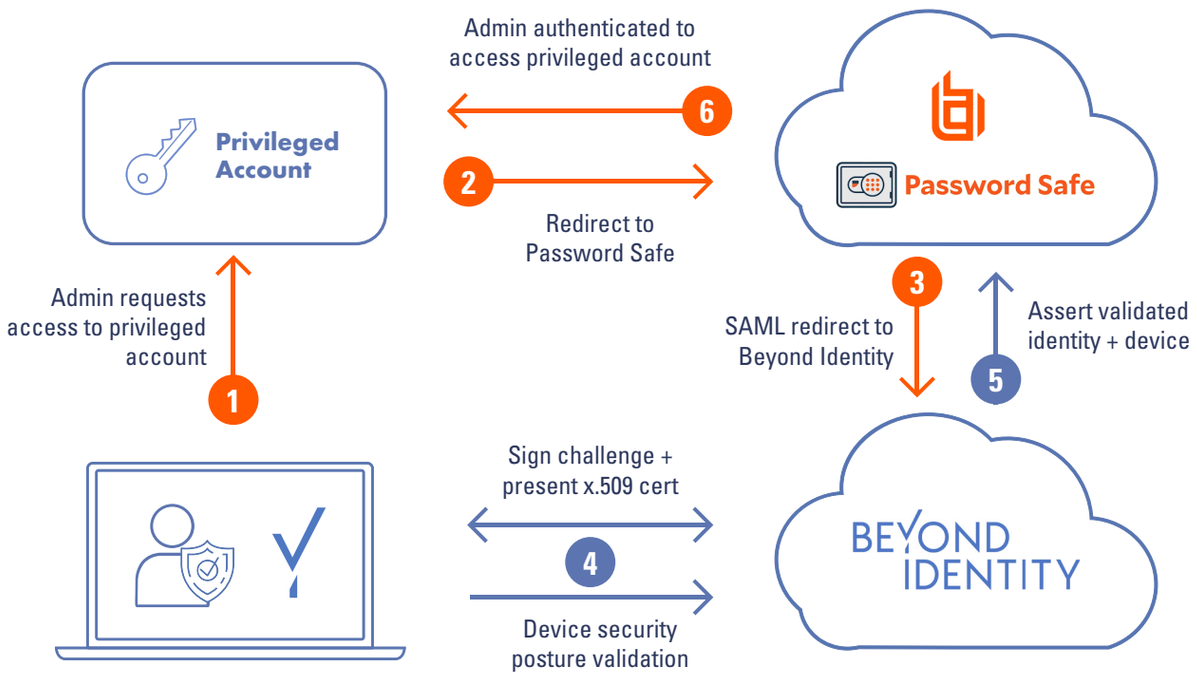
BeyondTrust Password Management

(Password Safe and DevOps Secrets Safe)

- **Continuous Discovery:** Automatically identify and manage privileged accounts
- **Secure SSH Key Management:** Automatically rotate SSH keys according to a defined schedule and enforce granular access control and workflow.
- **Real-Time Session Monitoring:** Fully integrated session recording and visibility into privileged user account behavior
- **Just-in-Time Access Control:** Evaluate just-in-time context and simplify access requests by considering the days, dates, times, and locations of user access

Beyond Identity's Secure Workforce

- **Passwordless Authentication to Password Safe:** If access to the BeyondTrust Password Management tools is vulnerable, the very purpose of the Password Safe is rendered obsolete. Removing passwords defends against the number one attack vector for unauthorized access.
- **Device Trust:** Beyond Identity cryptographically ties identity to device, and scans the device's security posture at every authentication event to ensure it complies with company policy.
- **User Experience:** Beyond Identity is inherently multi-factor, and doesn't require a second device.



Endpoint Privilege Management (EPM) Integration

When a user with limited rights needs to run a command, access an application that requires elevated rights, or run an executable on their endpoint, organizations need to have a method to elevate those privileges securely and seamlessly. The BeyondTrust integration with Beyond Identity facilitates this privilege management by providing the following benefits:

BeyondTrust Endpoint Privilege Management Cloud (EPM)

- **Enforce Least Privilege and JIT Provisioning:** Prevent threat actors from breaching endpoints by removing the privileges needed to compromise a host endpoint - in this case by running an executable that may contain malware.
- **Leverage Seamless Application Control:** Deliver trust-based application whitelisting
- **Cloud Deployment:** Same high availability, security, access, and scalability of an on-prem offering, while removing the overhead of managing infrastructure.
- **Privileged Threat Analytics:** Correlate user behavior against asset vulnerability data and security intelligence from best-of-breed security solutions

Beyond Identity's Secure Workforce

- **Remove Passwords:** Eliminate passwords as an authentication factor, which immediately closes a security gap for step-up authentication (i.e. threat actors can't phish your password to circumvent the EPM step-up).
- **Inspect and Trust the Device:** Leveraging public-private key cryptography, Beyond Identity binds the user identity with the device, and inspects the security posture of the device, ensuring that escalating privileges are allowed on an authorized and secure device.
- **Remove Friction:** Beyond Identity is inherently multi-factor, and doesn't require a second device. So your employees can get back to work, and you can rest assured that your environment is secure.