BeyondTrust's Password Safe, Privileged Remote Access, Remote Support, Identity Security Insights, PathFinder Overview

Seema Kalwani

seemakalwani@gmail.com
Security Engineer, IL, USA

Abstract

The article provides overview covering different privilege capabilities from BeyondTrust bridging gaps across identity security deployments. Password safe architecture, usage, features and use cases are illustrated. Other products including Privileged remote access and remote support are discussed. Identity security insights showing data at an individual and organization level is covered. Lastly, PathFinder is talked about that has the capability to unite all the above solutions and discover risk pathways.

Keywords: BeyondTrust, Password Safe, Pathfinder, Identity security insights, Remote Support, Privilege Remote Access

I. INTRODUCTION TO BEYONDTRUST

BeyondTrust's true privilege capability bridges a critical and widespread gap across identity security deployments. Organizations can expand PAM controls beyond just directly privileged accounts to also cover how human and non-human identities access privilege, finding vulnerable paths to be hardened and much more. This article will present different product offerings of BeyondTrust available:

1) *Beyond Safe Password Safe*
2) *Privileged Remote Access*
3) *Remote Support*
4) *Identity Security Insights*
5) *PathFinder*

II. BEYOND SAFE PASSWORD SAFE

Privileged credentials unlock access to the most critical IT assets and can create severe levels of risk if compromised or misused. Beyond Safe password safe enables complete visibility and control over privileged credentials to safe guard sensitive information from unauthorized access and preventing the breaches. The exponential growth of privileged accounts is largely driven by the demands of digital transformation project and the expansion of remote work forces. This complexity makes it more challenging to identify, secure or manage the credentials that enable privileged access. Thus, increasing the need for resources and undermining the security posture. Unified credential and session management allows for complete accountability and control of privileged account access. It is easy to gain full visibility over the privileged management landscape with robust discovery and automating capabilities, leveraging flexible

deployment option to reduce complexity, cost and empower the team by single integrated platform for ease of management.

It offers deep integrated capabilities reducing the risk of compromised privileged credentials. Storing credential for human and non-human capabilities eliminating hard coded application credentials, record and monitor privileged sessions in real time. Visualize privilege related risk via centralized management platform, leveraging existing investments with comprehensive portfolio of out of the box integrations. It offers a cost-effective, comprehensive credential and session management solution. It closes security gaps and simplifies deployments across on-premises, cloud and devops environments and meets the most demanding scalability and performance needs.

A. Core Features

1) Automated Discovery & Onboarding

Scan, identify, and profile applications and assets (including SSH keys) with auto-onboarding of privileged, shared, and service accounts—all while automating repetitive tasks.

2) Credential & Password Management

Secure and control access to privileged credentials (privileged passwords, DevOps secrets, and SSH keys), and automate password rotation.

3) Secrets Management

Secure and control access to secrets used in DevOps tools, workflows, and CI/CD processes in a fully auditable, controlled environment.

4) Application Password Management

Control scripts, files, code, and embedded keys. Eliminate hard-coded credentials. Define and automate controlled access using REST APIs.

5) Extensible API

Automate for scale by integrating with an extensive set of enterprise tools and systems to orchestrate PAM enterprise-wide.

6) Privileged Session Management

Log and monitor all privileged credential activity, account activity, and sessions for compliance and forensic review.

7) Employee Account Security

Apply enterprise-scale visibility and audit support to employee password management with the Workforce Passwords capability.

8) Just-in-Time Access Control

Advance zero trust with just-in-time context. Simplify access requests by considering the day, date, time, and location a user accesses resources.

B. Featured Use Cases

1) Credential, Key, & Secrets Management

Automatically discover and onboard accounts and secure and manage all credentials, keys, and secrets--even employee business passwords. Store, manage, and rotate privileged passwords and eliminate embedded credentials.

2) Real-Time Session Management

Log and monitor all privileged credential activity and sessions for compliance and forensic review, including session metadata.

3) Advanced Auditing & Forensics

Leverage extensive privilege and credential analytics to simplify compliance, benchmark tracking, and more.

4) Discover, Onboard, & Manage Cloud Assets & Privileged Identities

The first step in gaining control over cloud assets is discovery. BeyondTrust Password Safe performs continuous discovery and inventory of assets across cloud, physical, and virtual environments.

Discovery in the cloud includes all online and offline instances, devices, servers, virtual machines, identities, users, accounts, credentials, and privilege-related risks (default passwords, etc.).

After discovery, Password Safe auto-onboards all assets, allowing you to bring privileged accounts under centralized management. You can even integrate with existing identity providers, cloud identity stores (i.e. Azure Active Directory), and MFA platforms.

C. Architecture of BeyondTrust Password Safe Cloud

1) Infrastructure

Password Safe Cloud is hosted within Microsoft Azure. A Password Safe Cloud deployment consists of:

a) Management Console

Beyond Trust Cloud hosted management console and Password Safe user portal

b) Resource Brokers

- An on-prem agent deployed in the customers network facilitating the necessary local functions for password and session management
- Authentication against local AD/LDAP services
- Asset and account discovery
- Credential management

Session proxy

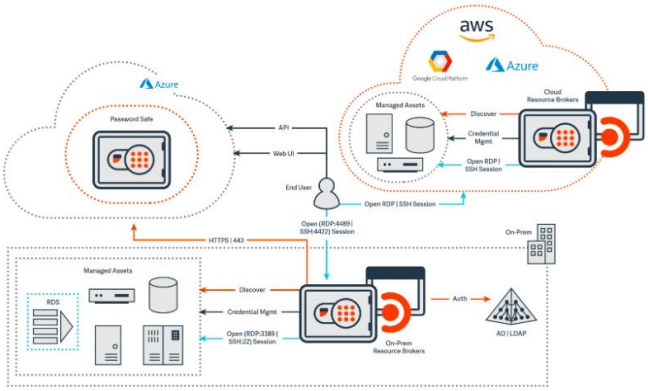

Fig. 1. Beyond Trust Password Safe architecture taken from Beyond Trust documents

D. Benefits

1) Reduce Security Risks for IT & Cloud

Password Safe combines Privileged Account and Session Management (PASM) + Secrets Management capabilities in one solution. Protect human and machine privileged identities, and network, against account hijacking, credential re-use attacks, exposed hardcoded passwords, lateral movement, privilege escalation attacks, and more.

Minimize the risks associated with privileged credential compromise by onboarding privileged accounts and credentials and safeguarding access to privileged account passwords and DevOps secrets, including certificates, API keys, tokens, and SSH keys.

2) *Gain full control over system and application access through live session management.*
Administrators can record, lock, and document suspicious behavior, with the ability to lock or terminate sessions.

3) *Minimize Operational Complexity*
Leverage discovery-driven dynamic policy, smart rules, and just-in-time access control features to ease the IT workload.
Automate manual responsibilities, like onboarding, credential storage, and privilege approval, to reduce administrative overhead and ensure no system is left unmanaged.

III. PRIVILEGED REMOTE ACCESS

Today most organizations need to provide remote network access to everyone from business users, IT administrators, data center teams, third part vendors. However recent data breaches have exposed vulnerabilities in common remote access tools and taken advantage of back door, firewall settings. How to give legitimate users the access they need to be protective while keeping attackers out. Most commercial remote access are unable to provide granular access to specific systems and taking all or nothing approach can frustrate users, alert auditors and open doors for malicious activity. Without a flexible solution one cannot fix the gap between security and productivity.

Fig. 2. Betond Trust Remote access bridges the gap between security and productivity. From Beyond Trust documents

With BeyondTrust, one gets unmatched visibility and control to remote access for employees, contractors and third party vendors. Secure remote access to all servers, managed desktops, point of sale systems as well as SSH and Telnet devices.

1) Define which endpoints and servers the users can access and when they can access them.
2) Protect the access by controlling and monitoring sessions via a secure agent or using standard protocols for RDP, VNC web and SSH connections.
3) Require notifications and authorizations for all privileged access connections.
4) Enable agentless remote access without VPN Tunnelling, forwarding or firewall configuration changes
5) Integrate with change management, password management and SIEM solutions
6) Single flexible solution, simplifies deployments and ensures maximum scalability while empowering remote workers to be productive

A. *Core features*

1) *Secure Remote Access*

Connect securely, seamlessly, and from anywhere to critical IT systems, cloud applications, and OT systems—no VPN required.

2) *Privileged Access Control*

Enforce least privilege and just-in-time access by giving users the exact level of remote access they need — and only for the finite moments needed.

3) *Streamlined Authentication*

Drive productivity and protect systems with MFA, passwordless authentication, and SAML authentication optimized for smooth onboarding and access.

4) *Session Management*

Gain full visibility and control over all actions, permissions, and more, in every privileged session. Ensure compliance is easily met with granular details of every session automatically recorded and logged.

5) *Flexible Consoles & Tools*

Maintain secure workflows with familiar tools like Putty or Azure Data Studio and increase coverage by initiating access via mobile or web consoles.

6) *Compliance & Session Auditing*

Get SOC 2 compliance-ready with audit trails, forensics, and advanced analytics using detailed session data – available in real-time or post-session.

B. *Use cases*

1) *Secure Access for Employees, Anywhere*

Maximize employee productivity and security with credential injection and secure remote access to authorized systems.

2) *Vendor Privileged Access Management (VPAM)*

Provide simple, secure remote access for trusted vendors connecting to systems, while eliminating the need for VPNs and known credentials.

3) *Kubernetes Environments*

Elevate Kubernetes environment with the assurance of just-in-time security and efficiency that only Privileged Remote Access can provide.

IV. REMOTE SUPPORT

Today's IT service desk is under pressure to support an expanded remote work force and diverse technology platforms and devices, all with limited resources. Beyond Trust Remote support empowers service desk teams with a single secure solution to resolve support and technology challenges for any device on any platform inside or outside the network. Many service desk's leverage a patch work of support tool creating inefficiencies and security risks. A comprehensive remote support solution enables faster incident resolution and higher end-user satisfaction while protecting the organization from data breaches. This feature is built to make the entire service desk more productive, efficient and secure. It speeds time to resolution providing features like chat, intelligent routing and automation. Controlling cost by consolidating to one solution, fix off-network devices such as robots, machines and any other devices that are not connected to the internet. Allows to easily manage unattended access to hundreds or thousands of systems. Stream line processes with simple, out of the box integrations with the ITSM solution such as ServiceNow. Satisfying security and compliance requirements unlike point-to-point tools like RDP, VNC or online meeting tools. Included security features allow to grant the right level of access, record all session activity, control passwords in the

Service desk with Beyond Trust vault. IT service desk teams are empowered to increase productivity, improve security and deliver a superior user experience.

A. *Core features*

1) *Remote Access Control*

Access, diagnose, and fix devices on or off the corporate network, and deliver support with thick client, browser-based, or mobile access.

2) *Jump Clients*

Facilitate unattended access to systems and bring efficiency to enterprise with mass deployments and just-in-time access.

3) *Auditing & Compliance*

Log all session activity for an unimpeachable audit trail, with real-time reporting, detailed video logs, and more.

4) *Efficiency & Scale*

Integrate with external directories to scale with infrastructure growth. Make it simple with mass installers, canned scripts, and escalation features.

5) *Customization & User Experience Controls*

Brand deployment's unique URL and client, customize portals, support invitations, watermarks, and surveys.

6) *Integrations*

Integrate Remote Support with trusted CRM, ITSM, SIEM, and password tools--or use open API to create custom integrations.

B. *Use cases*

1) *Modern Service Delivery Across the Enterprise*

Support any user, device, and system inside and outside network with a single tool, across Windows, macOS, Linux, iOS, Android, and more.

2) *Comprehensive & Secure Remote Support*

Leverage secure, attended and unattended access capabilities to troubleshoot, update, and support servers, workstations, network devices, kiosks, etc.

3) *Secure Remote Access—without a VPN*

Protect unsecure remote access pathways and attack vectors with a secure, VPN-less tool that audits every session.

V. IDENTITY SECURITY INSIGHTS

A. *Overview*

Identity Security Insights cuts through the noise, correlating data from BeyondTrust and third-party solutions to provide a single, unified view of all identities, accounts, elevated access, and paths to privilege. By detecting anomalous activity and compromised credentials in real time, you can proactively respond to threats—before they escalate. Plus, with built-in risk ratings and actionable recommendations, you can continuously reduce exposure and strengthen security posture.

Beyond Trust Identity Security Insights empowers security and IT teams with the industry's first intelligent layer of identity security analytics. The solution provides holistic, unified visibility across the entire enterprise, detects identity threats and provides proactive recommendation to protect the identity landscape and reduce the attach surface.

B. *Core features*

1) Unified Identity Insights Dashboard

Gain a complete view of identity security posture—identities, accounts, effective privileges, escalation paths, and threats—from a single lens.

2) True Privilege™ Graph

See the effective privileges of any identity, including how attackers can exploit obscure interconnections between accounts, privileges, and configurations to escalate privileges.

3) AI/ML-based Detections & Recommendations

Proactively detect the abuse of privileges and identity infrastructure. Leverage context-rich recommendations to understand and remediate risks.

4) Seamless Enterprise Security Integrations

Leverage out-of-the-box integrations with SIEM, SOAR, and ITSM for further correlation and response, or build custom integrations for extensibility.

5) Pre-built Reports with Quick Insights

Further analyze non-human accounts, effective privileges, local accounts, endpoint access, risky SSH keys, policy deviations, and trends.

6) Integrated PAM Controls

Use PAM controls like Just-in-Time access to proactively eliminate excessive privileges, block vendor and guest accounts, and enforce least privilege.

7) Quick Deployment and Results

Get up and running in less than an hour with native connectors. Gain actionable findings paired with rich context, within a day.

8) Intelligent, Cloud-Native Platform

Leverage a cloud-native, data-driven platform. Gain broad visibility, deep context, and advanced analysis to stop sophisticated identity threats.

C. *Use cases*

1) Continuous Identity Assessment and Monitoring

Assess and monitor identity security posture, including human and non-human identities, privileges, configurations, and potential paths to privileges.

2) Identity Security Posture Hardening

Proactively enhance identity security posture by understanding and addressing risks with prescriptive recommendations and integrated PAM controls.

3) Privilege Abuse & Threat Detection

Proactively detect anomalous activities such as privileged accounts under active attack, manipulation of IdP configuration, and privilege escalation.

D. *Workings of Identity Security Insights*

Identity security insights leverages connectors to BeyondTrust portfolio products to get data from password safe, privilege remote access, Privilege management and remote support. It also connects various identity providers such as Octave, Ping Identity and Azure Active Directory. It correlates all the data to give the unified view dashboard

1) Connector setup is most intuitive, setting it up is fast and easy. It can be setup in 30 minutes and can be receiving data from multiple sources.

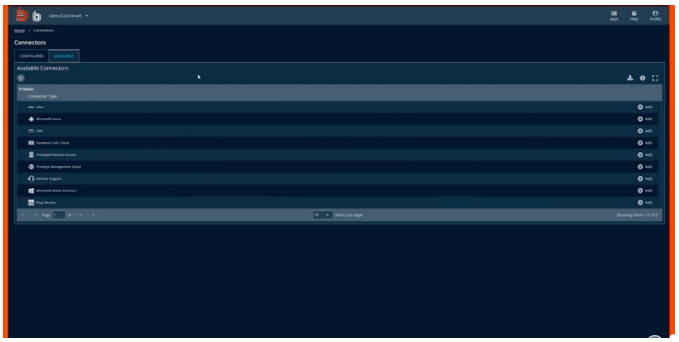

Fig. 3. Connector setup from BeyondTrust site

2) Connecting to Octave via an admin creative API token. It connects through API for all connectors. Data is access through read-only privilege. There is adherence to least modify privilege and there is no modification in the systems. Admin creates an API token, sets a name for the connector and points to the URL location and input the API token. Once collected, data can be seen in minutes.

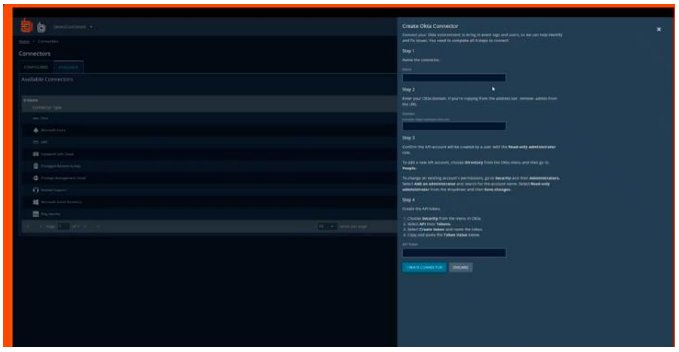

Fig. 4. Connecting to Octave via admin creative API Token from BeyondTrust site

3) In this environment 11118 accounts discovered, out of which 1174 are privileged and across the accounts we can see all key entitlements – 3000 roles and 1800 permissions. From the 11000+ total accounts are correlated into 4000+ identities.

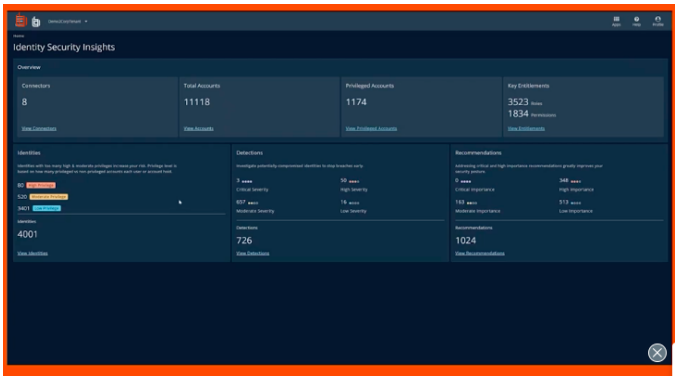

Fig. 5. Reading the environment from BeyondTrust site

4) All the accounts associated with each identity can be viewed. This is done for human and service accounts. System has identified 726 detections which are potential threats. These detections leaves the enterprise open to risk. 1024 recommendations to improve the security posture of those accounts.

5) Holistic view at an individual level. All his roles and accounts can be viewed. The status active or inactive can be viewed

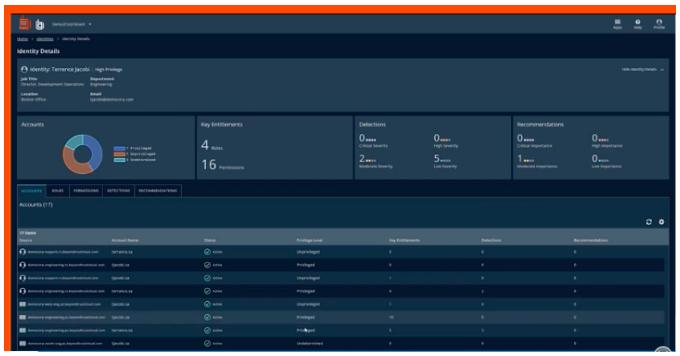

Fig. 6. Holistic view at an individual user level from BeyondTrust site

6) *User is a global administrator in Azure*

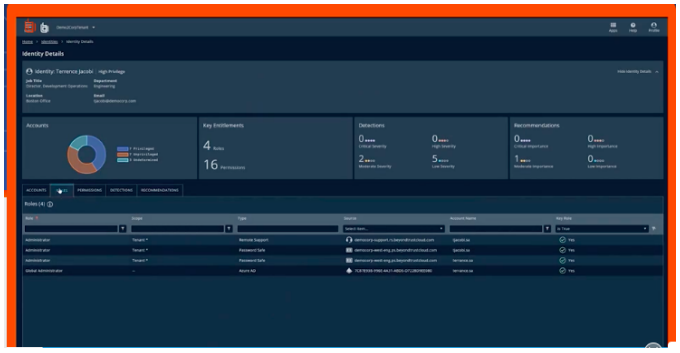

Fig. 7. Global administrator view of the user from BeyondTrust site

7) *From Beyond Trust Password Safe data we can see all his permissions across different accounts*

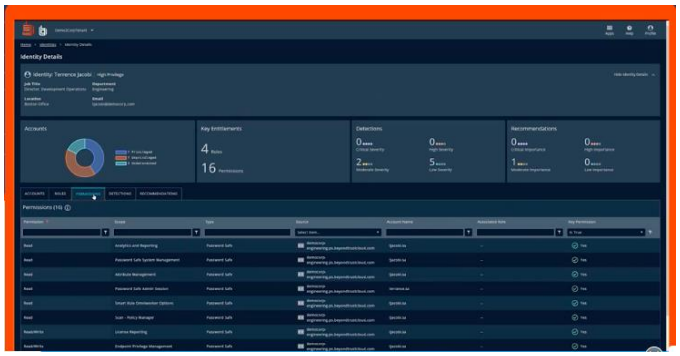

Fig. 8. A view of PasswordSafe data from BeyondTrust site

8) *Information from multiple sources to acheive the unified view of clues that can tell if the threat is underway. The detection indicator are 4 accounts that are dormant but recently been active. A partially disabled account showing a recent activity.*

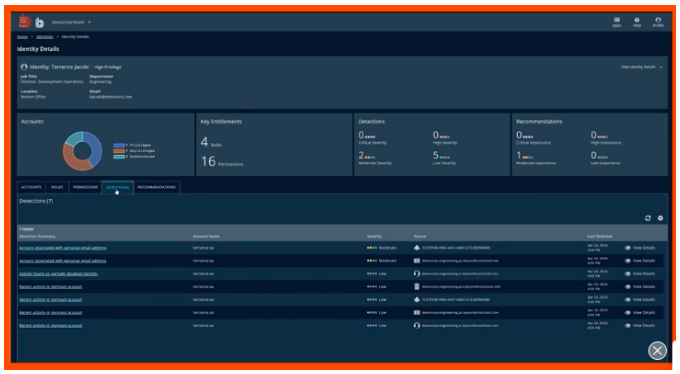

Fig. 9. A view of accounts under threat from BeyondTrust site

9) This shows the users identity might have been compromised and must be studied in detail to address the detections and activity.

E. Benefits

1) Proactively reduce attack surface Identity Security Insights gathers data across environment, using machine learning, graph theory, and rules-based techniques to surface intelligent, prescriptive recommendations.
2) Quickly identify and address identity risks such as a service account in a Domain Administrator's group, a dormant Admin account with a stale password, or a privileged account without MFA. Gain a clear understanding of both the risk and how to resolve it with clear contextualized guidance.
3) Identity Security Insights also detects potential misuse of privileges and accounts. The product enables rapid remediation by providing deep context and integrating with PAM and other toolsets to apply the effective controls.
4) Enable a proactive, extensible identity security approach
Identity Security Insights integrates seamlessly with enterprise security and incident response tools, streamlining processes for a more extensible, proactive approach to identity security. IT, security, and IAM teams can automatically receive real-time updates about critical findings, recommendations, and detections within their familiar tools. This enables faster response, improved productivity, and further data correlation for a deeper context.

VI. PATHFINDER

Identity-based threats span identities, endpoints, cloud and on-premises environments, SaaS applications, and credentials / secrets, creating a complex threat surface—with attack paths often crossing domains. Addressing these risks with a series of siloed or poorly integrated tools is not only inefficient and resource-intensive—it also leaves dangerous gaps. Attackers can exploit these gaps in security coverage and shared intelligence to gain footholds, escalate access, and execute lateral movement—all while remaining undetected.

The BeyondTrust Pathfinder Platform unites best of breed security solutions (including Password Safe) under a single login, delivering a streamlined experience that enhances operational agility, while also bringing shared, intelligent context across all products to unlock powerful synergies. With integrated Pathfinder platform, customers can benefit from the broad and deep capabilities reflected in multicategory identity security leadership, and leverage the fastest time-to-value via a unified approach to manage their entire identity attack surface.

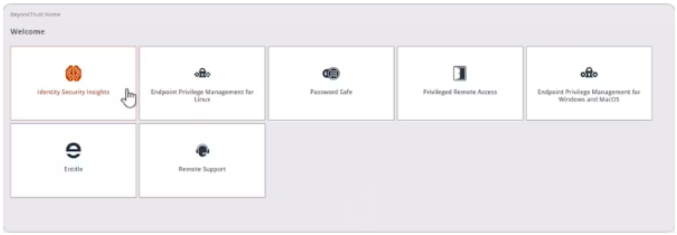

Fig. 10. Picture depicting one platform uniting best breed solutions from BeyondTrust site.

By fusing cross-domain visibility, management, and governance of identities, entitlements, and access into one AI-driven system, Pathfinder uniquely empowers organizations to:

1) Eliminate hidden risks and break down siloes across endpoints, servers, clouds, IdPs, SaaS, and databases

2) Implement just-in-time (JIT) access and enforce zero standing privilege (ZSP) and least privilege principles everywhere

3) Respond to threats, including active attacks, with speed and precision

4) Enhance operational efficiency through streamlined workflows, improved admin and end-user productivity, simplified auditing, and powerful integration synergies

A. Game-Changing Identity Security Visibility and Intelligence

Pathfinder dynamically maps and manages privilege relationships for every human, machine, and workload identity, continuously updating access paths and exposing hidden attack vectors, including identity-based misconfigurations and conflicts with least privilege principles.

Innovative True Privilege Graph capability, powered by Identity Security Insights, provides a clear, visual mapping of elevated access (entitlements, privileges, permissions, etc.) and Paths to Privilege™, including those that are indirect, hidden, and missed by other solutions.

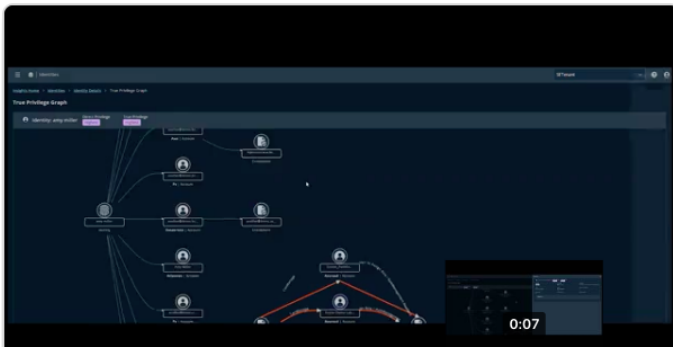

Fig. 11. Picture depicting true privilege graph capabilities from BeyondTrust site.

B. Adaptive, AI-Powered Protection

With Pathfinder, you are finally armed to instantly identify, prioritize, and act on the most impactful risks across identity estate, such as shadow admins. The platform automates escalation of detections and streamlines collaborative remediation to accelerate risk reduction.

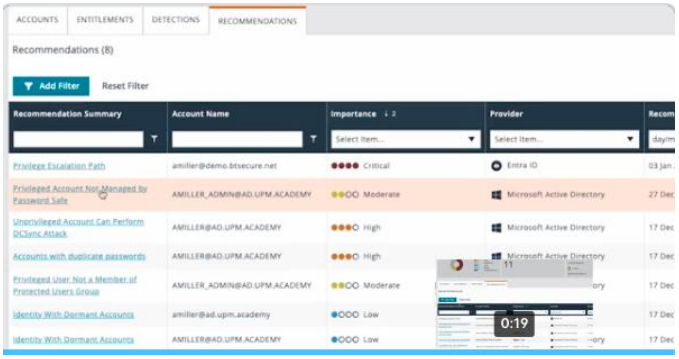

Fig. 12. Picture depicting AI powered detection and recommendation from BeyondTrust site.

Intelligently analyze privilege patterns, entitlement drift, access behaviors, anomalies, and attacks. Neutralize risks by removing standing privileges and implementing JIT access, revoking access, rotating credentials, hardening configurations, and more—from one console.

C. *One Platform, Infinite Identity Security*

Pathfinder enhances the capabilities of BeyondTrust's entire product suite. With the integrated Pathfinder Platform, customers can benefit from the broad and deep capabilities reflected in our multicategory identity security leadership, which spans Privileged Access Management (PAM), Identity Threat Detection and Response (ITDR), Cloud Identity Management, and Cloud Infrastructure Entitlement Management (CIEM).

As the focal point of identity security defense-in-depth, Pathfinder also leverages third-party connectors and deep integrations with other favorite toolsets to expand visibility, security, governance, and operational synergies

Fig. 13. Picture depicting the One Platform Identity from BeyondTrust site.

D. *Benefits*

1) *Gain Cross-Domain Visibility of Identities*

Break down identity silos to unify visibility for identities across IT and OT, from cloud to on-premises. Discover all human / nonhuman identities, privileged accounts and credentials, DevOps secrets, devices, and access—across every domain.

2) *Discover All Identity Risk Pathways*

Surface nested privileges, over-privileged identities, dormant accounts, identity misconfigurations, and other blind spots. Connect the dots across entire identity estate. Benefit from ML and AI-powered insights to prioritize the risk and blast radius of each path to privilege.

3) *Condense Identity Attack Surface and Threat Windows*

Attackers can't exploit what isn't there. Proactively remove or harden paths to privilege and reduce identity-based risks. Operationalize just-in-time access, and right-size authorization for all users, sessions, applications, machines, and endpoints to ensure least privilege and support Zero Trust.

4) *Respond to Identity Threats with Velocity and Precision*

Know the instant world changes—and when it matters. Benefit from AI-powered detections paired with easy-to-understand guidance that puts risk in clear context, and how to address it. Flex powerful PAM control plane and third-party integrations to harden security posture, stop attacks, and boost cyber resilience.

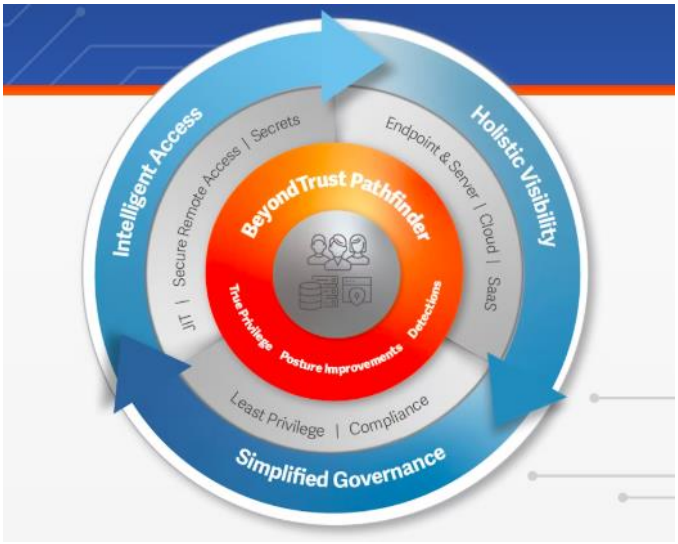

Fig. 14. Picture depicting the Holistic visibility, Intelligent access and simplified governance from BeyondTrust site.

Conclusion: **BeyondTrust has great features for detecting anomalous activity and compromised credentials in real time, proactively respond to threats in a mid-sized organization. Password Safe offers deep integrated capabilities reducing the risk of compromised privileged credentials Platform. Remote access allows unmatched visibility and control to remote access for employees, contractors and third-party vendors bridging the gap between security and productivity. BeyondTrust's comprehensive remote support solution enables faster incident resolution and higher end-user satisfaction while protecting the organization from data breaches. The Pathfinder Platform unites best of breed security solutions under a single login, delivering a streamlined experience that enhances operational agility, while also bringing shared, intelligent context across all products to unlock powerful synergies**.

REFERENCES

[1] BeyondTrust, "BeyondTrust Basics", https://www.beyondtrust.com/ (accessed Mar 21 2025)

[2] Entrust, "Partners with BeyondTrust", https://www.entrust.com/partners/directory/beyondtrust-software-inc (accessed Mar 2025)

[3] Gatner peer insights, "BeyondTrust Reviews?", https://www.gartner.com/reviews/market/privileged-access-management/vendor/beyondtrust, (accessed April 2025)

[4] BeyondTrust, "BeyondTrust Overview", https://www.youtube.com/watch?v=nwqVvNvv3Yk, Aug 2024

[5] BeyondTrust, "How BeyondTrust remote support works", https://www.youtube.com/watch?v=2gfH7ZzxqK4, August 2020.

[6] BeyondTrust. "BeyondTrust documentation", https://docs.beyondtrust.com/bips/docs/welcome-to-password-safe, March 2025