Identity Security Insights 24.02

What's New Documentation

Release Date – February 06, 2024

BeyondTrust Identity Security Insights helps you safeguard your entire identity estate with granular visibility and control over your identity security posture and identity-related threats. It leverages machine learning to automatically correlate and contextualize your identity data across your entire identity estate. This approach ensures a holistic understanding of your identity security posture, empowering you to identify, detect, and respond to threats swiftly and effectively.

With Identity Security Insights, your teams have a single source of truth to:

- Discover identities, accounts, and privileges across your entire identity – on-premises, cloud, and SaaS environments. Gain a unified view of your identities and related risks across your identity infrastructure like Microsoft Active Directory, Microsoft Entra ID, Okta, cloud service providers, and BeyondTrust products.
- Gain proactive recommendations to improve your identity security hygiene, e.g., discover poorly protected privilege, eliminate privilege escalation oaths, and fix identity configuration issues that could lead to a breach.
- Detect threats such as abuse of privilege and identity infrastructure.

Release Highlights

Webhook integrations enable enhanced efficiency and faster response to threats.

Don't just detect threats, act on them instantly! Leverage webhook integration APIs in BeyondTrust Identity Security Insights to directly send detections and recommendations to your preferred incident response tools, whether it's ticketing systems, Slack, or Teams. Streamline your workflows and ensure immediate threat response through better collaboration and faster actions. Webhooks can now be configured through the **Integrations** menu in Identity Security Insights.

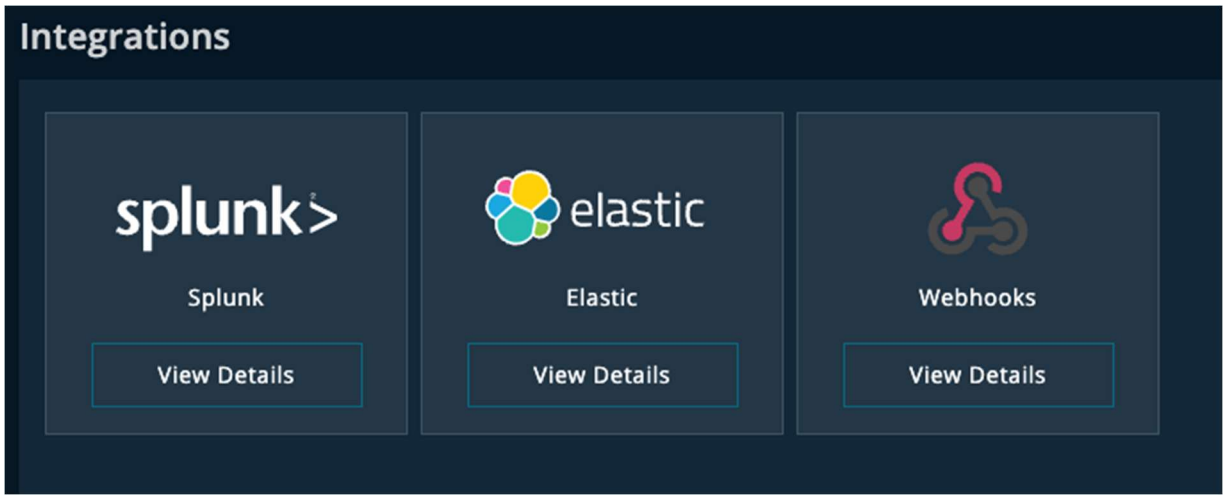

Figure 1 – Webhooks integration tile

Uncover hidden threats with advanced filtering based on complex expressions.

BeyondTrust Identity Security Insights empowers you with advanced search capabilities that let you tailor account displays based on complex filter expressions. But there's more. We understand the critical need to identify potential gaps in specific ways. For example, quickly identify privileged Entra ID accounts not managed by Password Safe. That is why we enable users to leverage the powerful "Does not contain" operator when filtering for labels. Now, you can filter for accounts that "Does not contain" the label "Password Safe managed" to gain easy visibility into accounts outside of your traditional PAM controls, potentially harboring hidden security risks.

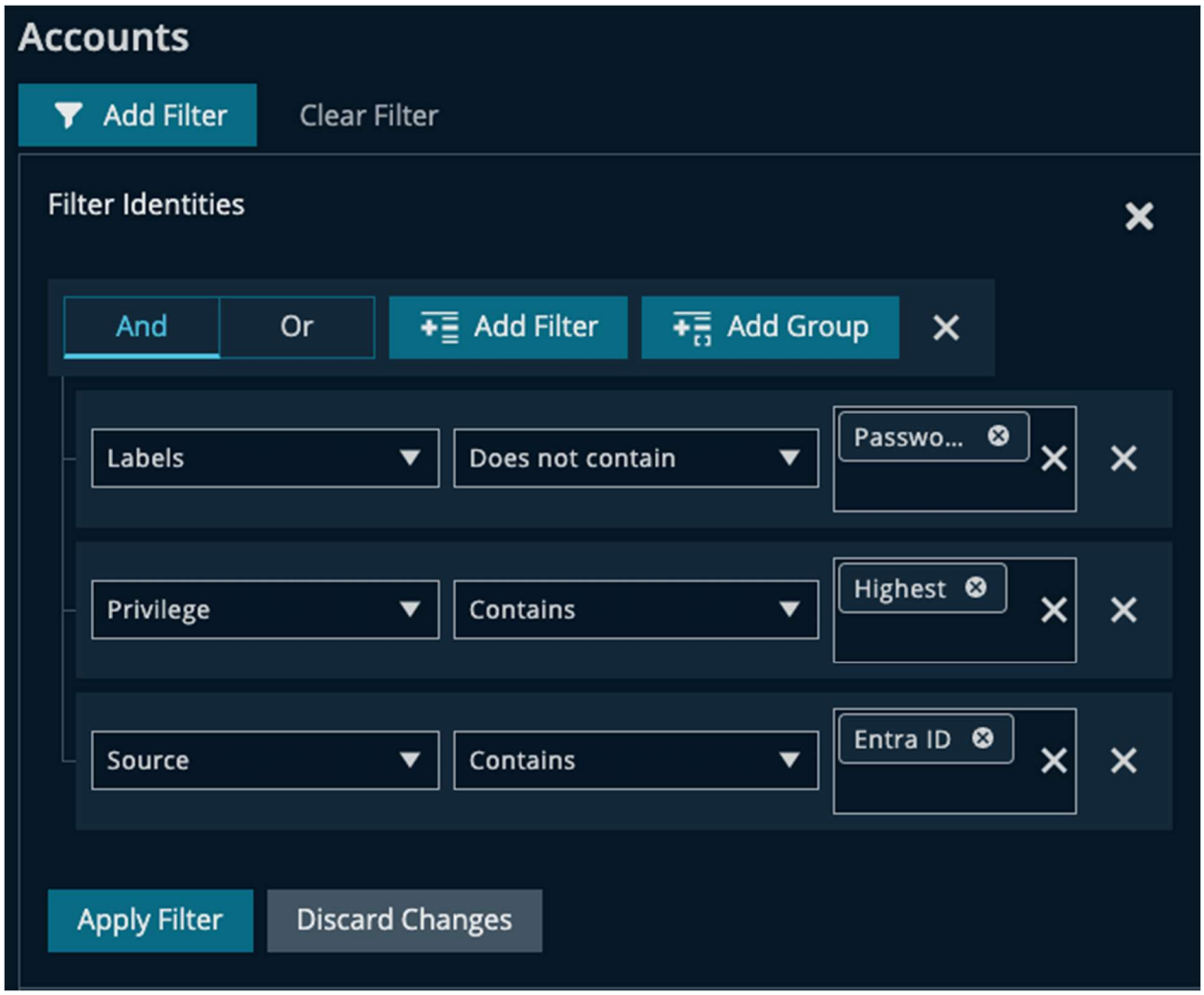

Figure 2 – New advanced filter

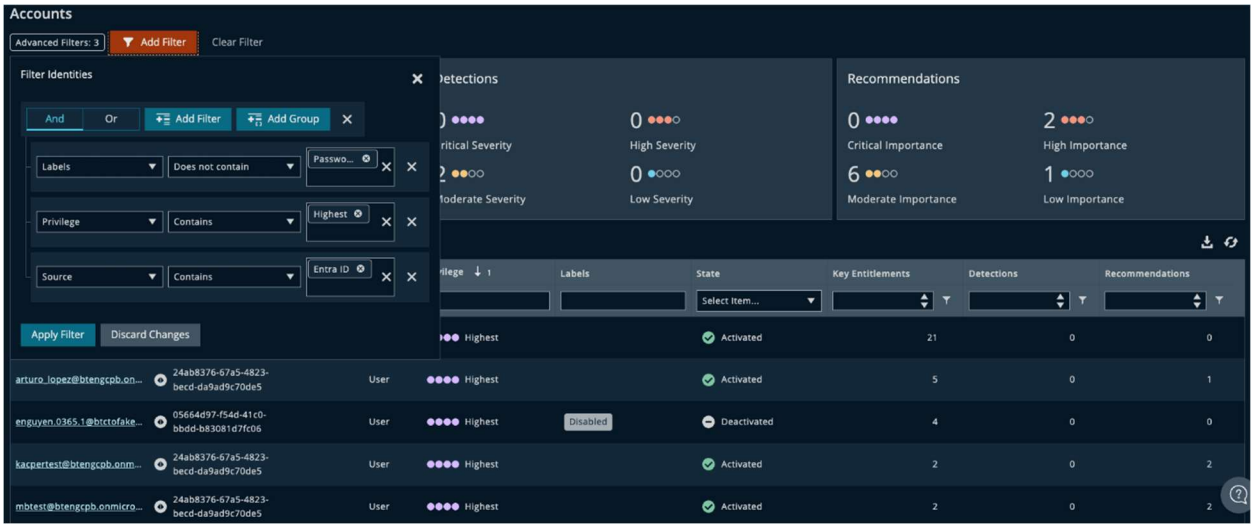

Figure 3 – Complex filter expression

New detections help stay ahead of evolving threats.

BeyondTrust is committed to empowering you with the latest threat detections to combat an ever-evolving threat landscape. In this latest update, we have a powerful set of new detections aimed at:

- **Protecting unmanaged highly privileged accounts**: For example, our detections can pinpoint highly privileged accounts that are not managed by Password Safe currently under brute force attack and do not have MFA enabled, so you protect them with Password Safe. Password Safe can help you only if have locked your privileged accounts under Password Safe.
- **Monitoring BeyondTrust products for malicious activities**: For example, identifying and monitoring against suspicious API access or user logins from malicious IPs across BeyondTrust Privileged Remote Access and Password Safe. Our malicious IP classification is based on our in-house machine learning models, achieving higher accuracy and detection rates compared to industry players.
- **Exposing hidden escalation paths**: For example, we uncover potentially exploitable, sophisticated privilege escalation paths within Active Directory, including those involving Group Policy Object ownership.

About BeyondTrust

BeyondTrust is the worldwide leader in intelligent identity and access security, empowering organizations to protect identities, stop threats, and deliver dynamic access to empower and secure a work-from-anywhere world. Our integrated products and platform offer the industry's most advanced privileged access management (PAM) solution, enabling organizations to quickly shrink their attack surface across traditional, cloud, and hybrid environments.

BeyondTrust protects all privileged identities, access, and endpoints across your IT environment from security threats, while creating a superior user experience and operational efficiencies. 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 75 of the Fortune 100, and a global partner network. Learn more at www.beyondtrust.com.