Identity Security Insights 23.11

What's New Documentation

Release Date – November 07, 2023

BeyondTrust Identity Security Insights is a powerful solution that helps you protect your organization from identity-driven threats. It leverages machine learning to automatically correlate and contextualize your identity data across on-premises and multicloud environments. This enables you to gain a holistic understanding of your unique identity security posture, and helps you to identify, detect, and respond to threats quickly and effectively.

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

- Identify your greatest identity-driven risks early.
- Gain proactive recommendations to improve your overall security posture.
- Detect threats such as lateral movement and privilege escalation.

Release Highlights

Granular visibility into Ping One identities and entitlements helps reduce risks.

BeyondTrust provides holistic visibility into Ping One identities, entitlements, and accounts, eliminating the need to sort through multiple systems. This gives you a clear understanding of how and which identities are accessing applications, helping you to reduce risks and improve overall security posture.

New detections help detect incidents like Okta Support breach.

BeyondTrust consistently introduces new detections and recommendations that empower our customers in countering emerging threats and proactively addressing hygiene concerns. In this latest release cycle, we've rolled out a new set of detections focused on identifying suspicious activities around Okta admin account. Read our blogs to understand how Identity Security Insights can help detect incidents like Okta Support breach and Okta identity attacks. For a complete list of new detections and recommendations in this release, please refer to the release notes.

Identity Security Insights integrated with Elastic SIEM to deliver additional value.

Security Information and Event Management, or SIEM, allows organizations to collect and analyze a broad range of log and event data to quickly locate and respond to potential security threats. Identity Security Insights can help SIEM users to improve detection and incident response with additional identity-driven context and information.

BeyondTrust Identity Security Insights is now seamlessly integrated with Elastic SIEM. When activated, BeyondTrust provides fresh detections and recommendations directly to your Elastic SIEM so your security teams can access additional insights for effective triage and investigation.

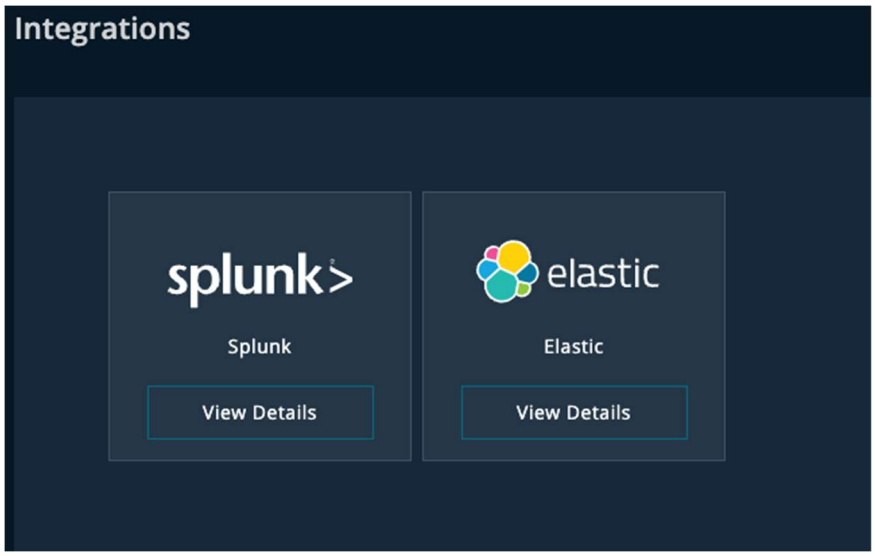

Figure 1 – Elastic SIEM connector now available

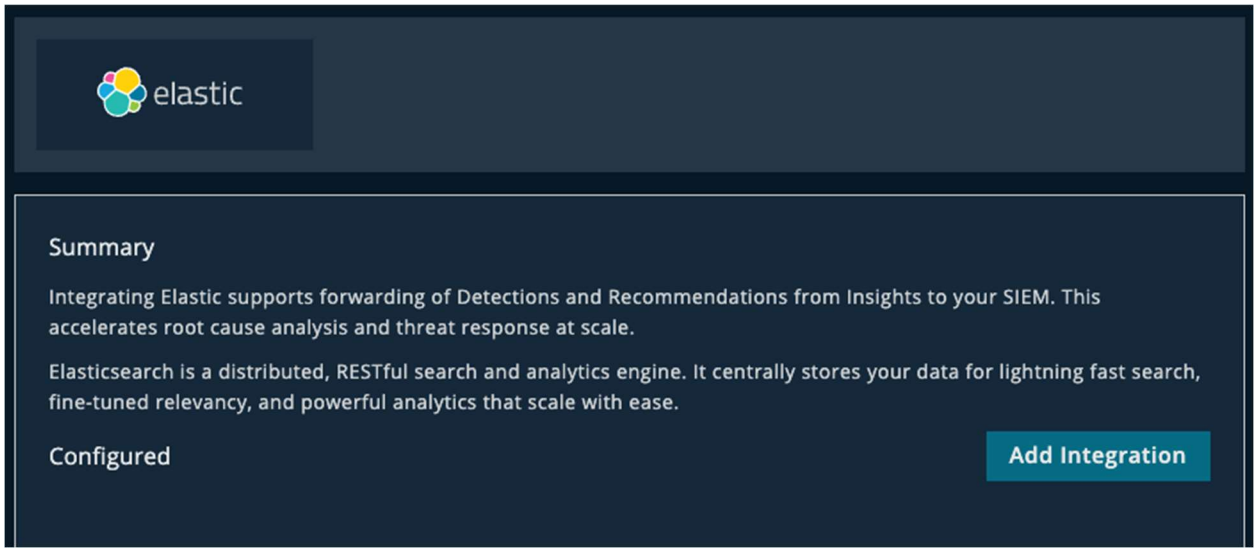

Figure 2 – Integration details for Elastic SIEM connector

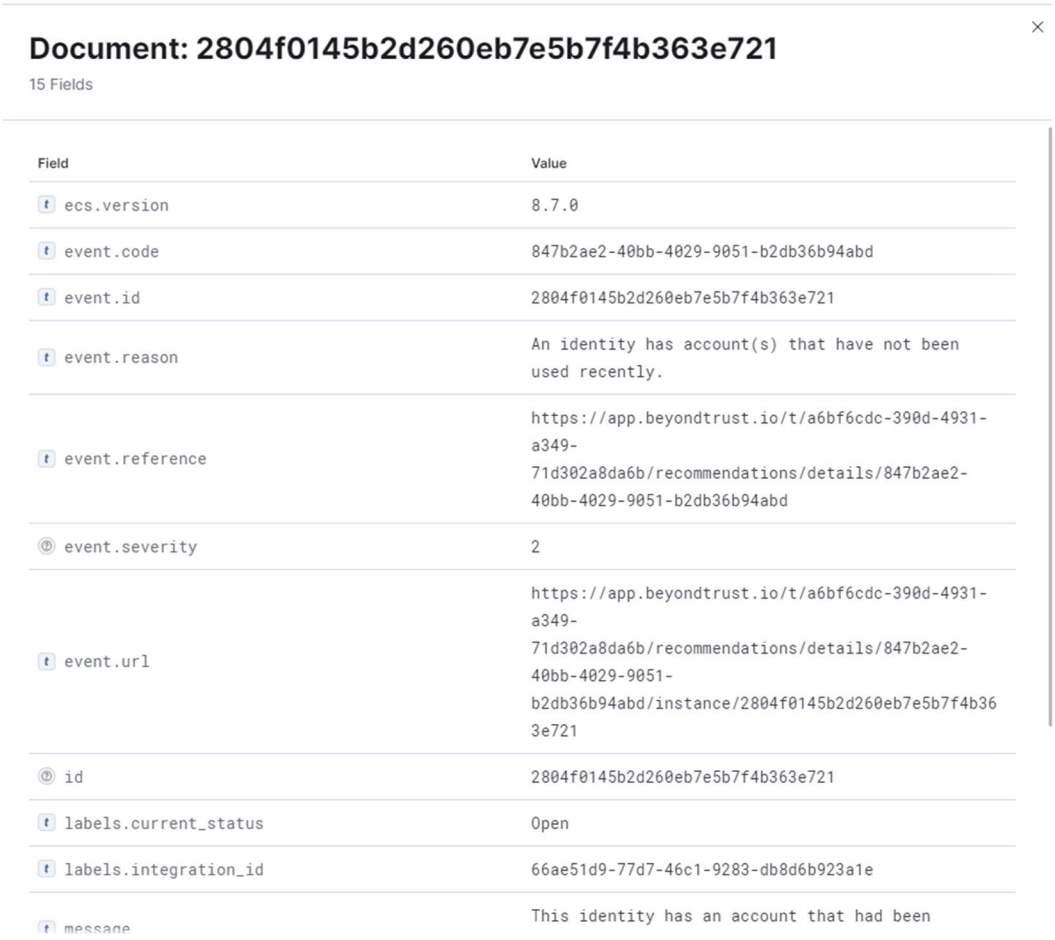

Figure 3 – Example of ECS-formatted Incident forwarded by BeyondTrust Identity Security Insights

CSV export for detections and recommendations makes it easier to share data.

You can now export detections and recommendations directly from the grid view to a CSV file while preserving your applied filters. This makes it easier for your teams to share and analyze critical data about your environment.

UI enhancements drive simplicity and flexibility for users.

We have introduced a new “Summary” tab within the “Entitlement Overview” view, where entitlements are organized by rolling up accounts by roles. This makes it simpler for you to quickly access your most relevant entitlements, eliminating the need to navigate through extensive results spread across multiple pages. If you prefer the flat user-centric view of entitlements, it is still available under the “Details” tab.

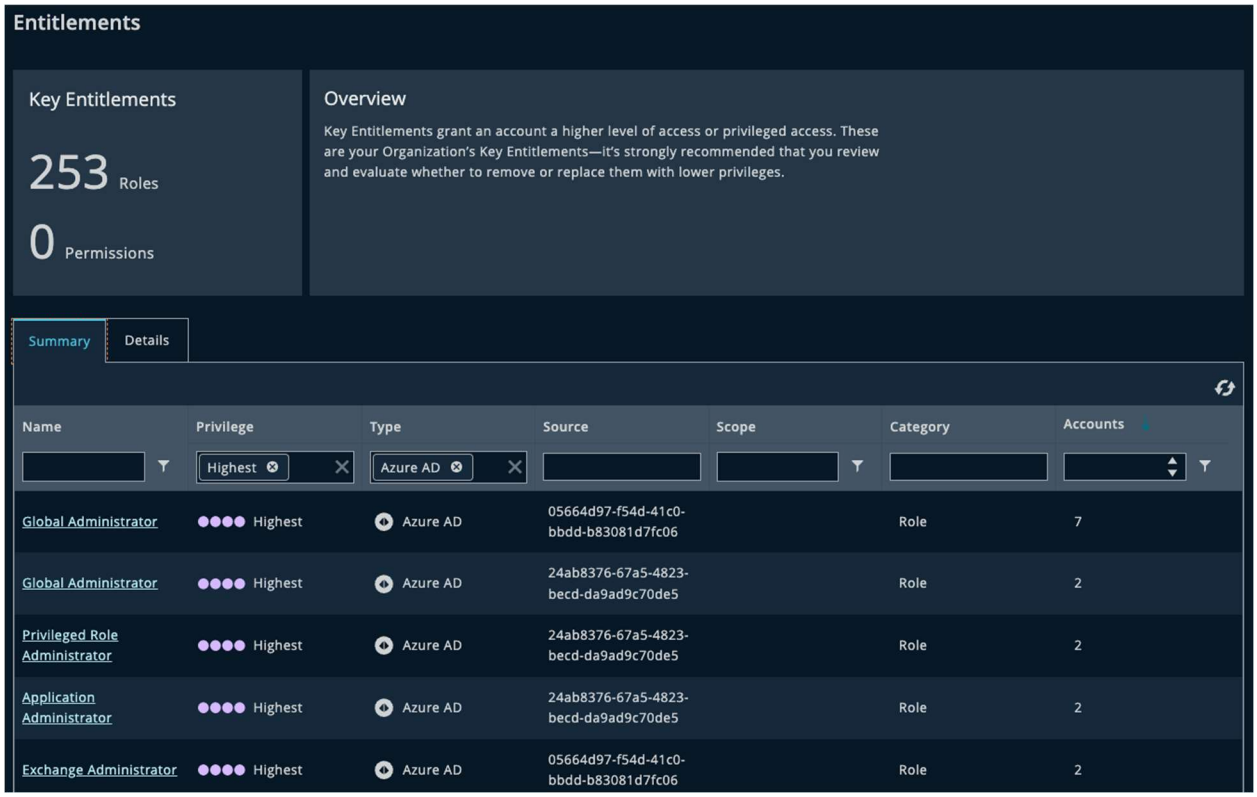

Figure 4 – Example of Summary tab

New platform invites for administrators to improve onboarding experience.

Your admins will now receive redesigned platform invitation emails that includes more context and relevant information as compared to previous versions. This improvement is aimed at minimizing the likelihood of administrators classifying these emails as spam, and ultimately, ensuring a smoother onboarding experience.

A new “Warning” status monitors connector health, preventing failures.

We have added a “Warning” status, highlighted in yellow, to help customers monitor connector health. This status signifies that the connector is operational and actively ingesting data, though with the possibility of partial or occasional failures. Previously, we had a green “Connected” status and a red “Failed” status. The new status addresses the intermediate state, meaning that the connector is not performing optimally. This provides customers with additional context and opportunity to resolve any issues before the connector experiences complete failure.

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.