

# Identity Security Insights 24.03

What's New Documentation

Release Date – February 29, 2024

BeyondTrust Identity Security Insights helps you safeguard your entire identity estate with granular visibility and control over your identity posture and identity-related threats. It leverages artificial intelligence and 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 estate – on-premises, cloud, and SaaS environments.
- Gain a unified view of identities and related risks across identity ecosystem, including Microsoft Active Directory, Microsoft Entra ID, Okta, cloud service providers, and BeyondTrust products.
- Eliminate identity risks like poorly protected privilege, privilege escalation paths, and identity misconfigurations with prescriptive recommendations.
- Detect identity-driven threats such as abuse of privilege and identity and access infrastructure.
- Leverage in-built PAM products to take swift actions to block access, enforce the principle of least privilege, and remediate other identity-driven threats. Use the findings to enhance privilege management processes and achieve a secure identity posture that is resistant to modern attacks.

## Release Highlights

See across multiple clouds. Unify your identity landscape.

Identity Security Insights now shines a light across your multi cloud environment with three new connectors for AWS Organizations and Identity Centers, Google Cloud, and GitHub, presenting a unified view of your entire cloud landscape. Unmask every identity and understand their access to critical services and applications. Gain clear visibility into the powerful entitlements granting administrator privileges and identify potential identity-related risks lurking within your environment.

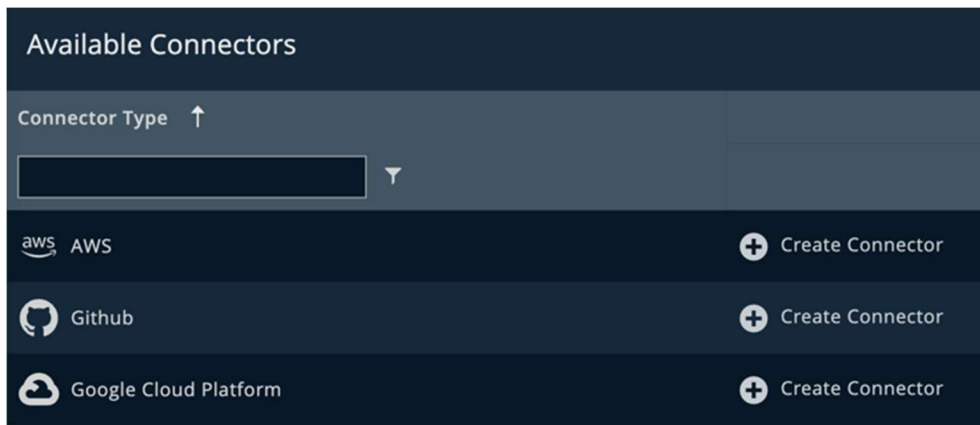
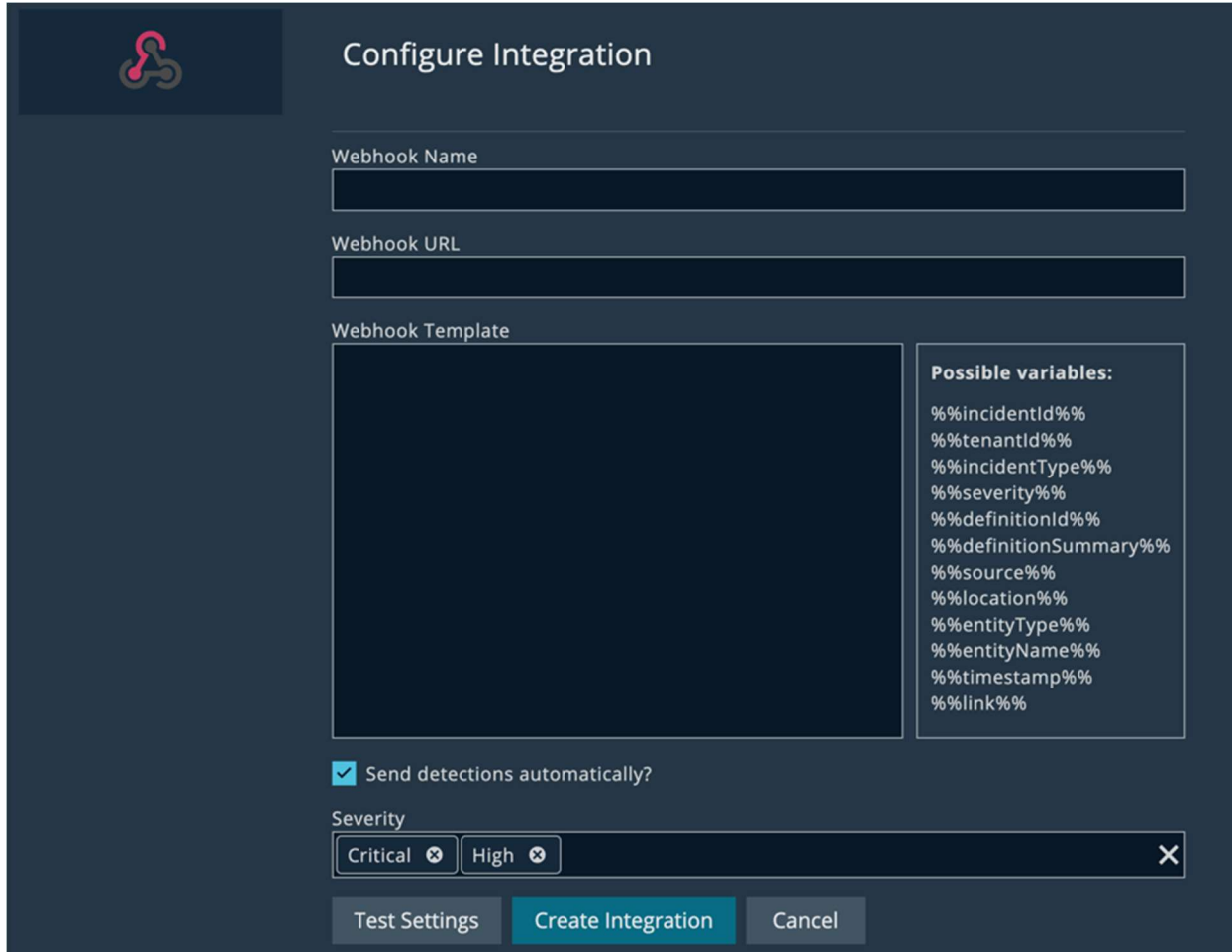


Figure 1 – New connectors

## Streamline threat detection and response with automated Webhook integration.

Identity Security Insights now automatically sends detections to your preferred incident response tools, thanks to enhanced Webhook capabilities. Simply choose your preferred tool, be it a ticketing system, Slack, or Teams, and configure automatic alerts for specific detection severity. No more manually chasing down threats – high and critical alerts will automatically land in your preferred channel, allowing for immediate response and mitigation.



The screenshot shows a dark-themed 'Configure Integration' window. At the top left is a logo with three interlocking rings. The title 'Configure Integration' is centered at the top. Below the title are three input fields: 'Webhook Name', 'Webhook URL', and 'Webhook Template'. To the right of the 'Webhook Template' field is a box titled 'Possible variables:' containing a list of variables: %%incidentId%%, %%tenantId%%, %%incidentType%%, %%severity%%, %%definitionId%%, %%definitionSummary%%, %%source%%, %%location%%, %%entityType%%, %%entityName%%, %%timestamp%%, and %%link%%. Below these fields is a checked checkbox labeled 'Send detections automatically?'. Underneath is a 'Severity' dropdown menu with 'Critical' and 'High' selected. At the bottom are three buttons: 'Test Settings', 'Create Integration', and 'Cancel'.

Figure 2 – Automated detection alerts with Webhook integrations

## Say goodbye to click fatigue. Streamline updates and save time with bulk actions.

Updating the status of individual detections and recommendations can feel like an endless click-fest, especially if the update status is the same. Identity Security Insights now enables you to update multiple detections or recommendations with powerful bulk actions. Simply select multiple detections or recommendations, choose the desired status update, and watch as your changes apply instantly.



New detections, recommendations, and visibility to help protect identities and privileges, including Cloud Infrastructure Entitlement Management (CIEM)\*.

---

BeyondTrust provides a unified identity security platform for all teams, including IAM and SOC, offering granular visibility, threat detection, and prescriptive recommendations to address identity security gaps across your entire IT landscape – on-premises, multicloud, and SaaS. Here are the latest updates:

**Gain unified threat-aware entitlement visibility. Identify and eliminate the riskiest privileges.**

Discover all key entitlements across your multicloud environments, including those that can grant an account a higher level of privileges or access. Identity Security Insights surfaces multiple types of entitlements such as applications that identities can access, group memberships, roles, and individual permissions, in a unified view. Filter and prioritize entitlements based on your unique risk tolerance and security needs. For example, you might want to identify entitlements that grant excessive privileges, are dormant, under brute-force attack, not managed by BeyondTrust Password Safe, and lack multi-factor authentication (MFA). These are potentially risky or under attack privileges that warrant closer scrutiny. With threat-aware context, you can effectively prioritize your greatest threats based on your own criteria and make informed decisions about eliminating unnecessary or risky privileges and implementing stronger policy controls.

**Find significant outlier privilege assignments.**

Identity Security Insights uses AI/ML-based analytics to analyze standing privileges and identifies significant outliers as compared to role-based expectations, departmental norms, and overall trends against the broader dataset in your environment. When we find assignments that are both significant and unusual, we recommend you check that they are intentional. You can take actions to reduce privilege creep and ensure standard permissions by job role and detect when attackers add backdoor privilege to unusual accounts.

**Discover environments with unusual and sweeping privileges.**

An excessive number of sweeping privileges, like global admins in Azure or domain admins in Active Directory, can introduce significant security risks. Identify environments where such excessive privileges are allocated and mitigate risks by limiting the number of such accounts. We provide prescriptive recommendations to right size privileges and retain only a small set of tightly controlled accounts with admin privileges.

**Detect vendor or guest accounts with risky or suspicious privilege.**

Managing access for external accounts like vendor users and guest accounts can be challenging. These accounts are granted privileges to access your systems and applications but can pose a significant threat if not carefully monitored and controlled. If you are a BeyondTrust customer, we pay particular attention to privileges assigned to your external accounts such as Azure guest accounts or BeyondTrust Privileged Accounts. We flag external accounts with significant or suspicious privilege. We enable you to easily filter and explore permissions assigned specifically to external accounts, to identify potentially risky assignments that are outside of your risk tolerance or policy.

**Detect suspicious or unnecessary Azure service principal and application privilege, including foreign application privilege.**

Azure service principals play a vital role in automating tasks and managing access within your Azure environment. Granting excessive or unnecessary privileges can create significant security vulnerabilities. We enable you to browse and filter privileges assigned to service principals across all your Azure environments. We provide recommendations to check specific service principal that is permissive or suspicious, including excessive privilege assigned to service principals that can be accessed from another tenant – a significant part of the recent Microsoft breach.



**Detect Azure service principal manipulation.**

Identity Security Insights helps you proactively detect suspicious manipulations of Azure service principals, similar to those observed in [recent breach](#).

**Detect suspicious privilege manipulation.**

Identity Security Insights detects when attackers manipulate accounts and privileges, as we have seen in the case of Okta Support breach.

**Detect more Active Directory privilege escalation paths.**

Attackers can exploit hidden pathways within Active Directory to escalate privileges. Identity Security Insights continues to add rich detections to identify privilege escalation paths within Active Directory, delving deep to identify vulnerabilities such as unconstrained delegation on computer objects, and misconfigurations and inconsistencies.

**Detect overly permissive AWS policies and permission grants, as well as unused or unrotated credentials, and significant AWS principals not properly protected by posture controls like MFA.**

Identity Security Insights helps you strengthen your AWS security posture by detecting overly permissive policies and grant, unused or unrotated credentials, and inadequate posture controls.

\* **CIEM:** Managing multicloud permissions is challenging due to the complex and dynamic nature of the cloud, and inconsistent cloud provider approaches and services, each with its own definition of identity, access, and authorization systems. The rapid explosion of identities, especially machine identities and granular service accounts, have only made matters worse, making traditional approaches inadequate. BeyondTrust Cloud Infrastructure Entitlement Management (CIEM) capabilities can help you manage cloud access risks through discovery, threat- and context-aware visibility, and controls to manage the risk of over privileged accounts across your multicloud environments.

## 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](http://www.beyondtrust.com).