Understand the True Privilege™ of your accounts across your enterprise with Identity Security Insights Connectors

Organizations are approaching the identity security and privilege challenge incompletely because they are overlooking the Paths to Privilege™ attackers are exploiting. When a seemingly unimportant account can be the keys to your entire environment, you need to have full visibility and proactive information about every account.

With Identity Security Insights connectors, BeyondTrust maximizes your visibility into the true privilege of your accounts and identities beyond simply enumerating Microsoft Active Directory groups. The more connectors you configure, the more you can extensively map your organization's landscape and link identities across multiple applications. This comprehensive connectivity provides a clear view of the True Privileges™ (both known and hidden) across your environment, helping you prioritize security where it matters most, with highly-tuned detections and recommendations to secure your environment.

The more connectors you configure, the more you can extensively map your organization's landscape and link identities across multiple applications.

Here's where we currently connect:

Microsoft Active Directory

okta

PingOne®

aws

Azure

Google Cloud

GitHub

Insights Collector

Password Safe Cloud

Remote Support

Privilege Remote Access

Privilege Management Cloud

Common Paths to Privilege

Vulnerable human & machine accounts

Exposed secrets (passwords, API keys, certificates)

Identity infrastructure misconfiguration

Remote access (VPNs & lack of zero trust)

Excessive privileges

What is a Connector?

Identity Security Insights connectors are out-of-the-box, read-only APIs that ingest identity data from all the identity sources across your entire identity fabric, whether on-prem, cloud service providers, or SaaS solutions — including additional BeyondTrust platform solutions — for analysis by Identity Security Insights. Think of it as gathering all the pieces of your identity puzzle that are made up by your inventory data, configuration state, auditing, and event data.

How easy is it to set up?

It can usually be done within an hour.
For more details, please visit the Knowledge Base.

For more information about connectors and how to further integrate detections and recommendations into your ServiceNow, Azure Sentinel, Slack, and many more tools in your ecosystem via Webhooks, please check our documents website or contact our sales team at sales@beyondtrust.com.