CrowdStrike Falcon® + BeyondTrust Pathfinder Platform Integrations Close the Prevention-Detection Gap

BeyondTrust identity and privilege intelligence, now inside CrowdStrike Falcon

Attackers increasingly gain enterprise access using legitimate, compromised credentials rather than malware. BeyondTrust Phantom Labs® research found that roughly 75% of modern attack paths exploit identity relationships rather than software vulnerabilities alone.[1] Yet ISPM, ITDR, and PAM signals often sit in disconnected tools, leaving detection without enforcement or enforcement without context.

The joint integrations bring identity and privilege intelligence from the BeyondTrust Pathfinder Platform directly into CrowdStrike Falcon. By correlating identity relationships, privilege exposure, and Falcon threat telemetry across human, non-human, and AI agent identities, security teams can uncover attack paths earlier and respond faster.

[1] Phantom Labs® Research Index. BeyondTrust. August 2026.

Key Outcomes

- **Reveal Attack Paths Before They're Exploited** Privilege and identity relationship mapping uncovers escalation paths, dormant accounts, and excessive permissions across human, non-human, and AI agent identities.
- **Accelerate Identity Threat Investigation** Privilege and blast-radius context enriches Falcon detections, helping analysts triage identity and endpoint threats without switching tools.
- **Correlate Risk Without Changing Workflows** BeyondTrust data flows in through Falcon Data Connectors, giving joint customers one correlated view of privilege risk and threat activity.

Joint Integrations

BeyondTrust Identity Security Insights®: Correlate Falcon detections with identity relationships, effective privileges, dormant accounts, shadow admins, and blast-radius context. Coming soon: AI Agent – Identity Security Insights Connector: Inventory AI agents and their privileges, identify over-permissioned agents, and correlate agent activity with Falcon detections.

BeyondTrust Endpoint Privilege Management: Integrate privilege elevations, blocked-execution events, and JIT approval workflows into Falcon, with decisions informed by CrowdStrike app risk scores.

BeyondTrust Password Safe®: Enrich Falcon with privileged credential activity, checkout events, and session context.

BeyondTrust Privileged Remote Access: Stream configuration changes, authentications, session activity, and recorded-session context into Falcon for deeper privileged access visibility.