BI software company finds terminated-user access and stale cloud credentials

A business intelligence software company used the IAM Risk Analyzer to surface terminated employees with live accounts and stale cloud credentials, then ran targeted access reviews to remove them.

Industry	B2B SaaS (business intelligence and analytics)
Size	~600 employees
Modules	IAM Risk Analyzer, User Access Reviews
Systems	BambooHR, Active Directory, OneLogin, AWS IAM Identity Center, GitLab, Google Workspace, Jira, SaaS management platform
Drivers	Audit evidence that terminated users no longer hold access, with an immutable decision history

Challenges before BalkanID

- A quarterly check of terminated users across applications ran in spreadsheets.
- An internal tool built on spreadsheets and dashboards covered only handful of systems, and could report problems but not fix them.
- It showed accounts disabled in single sign-on but still active in downstream apps, plus user records that were inactive or incomplete.
- Review evidence could be edited, which weakened it for auditors.

What they implemented

- IAM Risk Analyzer across HR, directory, SSO, cloud and developer platforms, with daily findings alerts to Slack and email.
- Findings for terminated employees who still hold active identities, correlated against the full HR termination history.

- Cloud credential hygiene findings, such as access keys not rotated in over 180 days and service accounts with stale credentials.
- Targeted access review campaigns on recently terminated users, routed to app owners, with an immutable decision trail.

Outcomes

- Terminated-user access detected continuously, instead of once a quarter in spreadsheets.
- Stale and long-unused cloud credentials surfaced, including a key created years earlier and unused since.
- Audit-ready review evidence replaced spreadsheet workflows, which reviewers described as "simple, straightforward."