

Identity-Aware Data Security with Forcepoint and BeyondTrust

Correlate identity risk with sensitive data insights to reduce business risk faster

Challenge:

- › Identity risk and data risk live in separate tools, creating visibility gaps
- › Security teams spend valuable time manually correlating alerts and access data
- › Investigations are delayed by fragmented workflows and multiple handoffs
- › Organizations struggle to prioritize risk based on actual business impact

Solutions:

- › BeyondTrust identifies risky identities, excessive privileges and compromised accounts
- › Forcepoint discovers and classifies sensitive data, and who accesses it
- › Together, they correlate identity risk with data exposure insights to prioritize and reduce risk faster

Outcome:

- › Organizations gain a clearer view of business risk, accelerate investigations and reduce exposure risk before it becomes a security incident

As identity-based attacks continue to rise, security teams face a growing challenge: understanding whether a risky identity (person, service account or other entity with system access) can reach sensitive information. Organizations invest heavily in both identity security and data security. Yet these disciplines often operate independently, leaving security teams without an answer to a critical question:

Which risky identities can access sensitive data, and what is the potential business impact?

Identity security solutions can flag risky identities, excessive privileges and compromised credentials. **Data security** solutions can discover sensitive information and map access permissions. But when these risks remain disconnected, security teams must manually correlate information, slowing investigations, delaying remediation or even missing risk entirely.

Forcepoint and BeyondTrust help organizations bridge this gap by connecting identity risk with sensitive data exposure. Together, they provide a unified view of who is risky, what sensitive data they can access and how organizations can reduce that exposure before it leads to a breach.



Joint Use Cases

Identify Risky Identities with Access to Sensitive Data

Security teams often know which identities are risky and where sensitive data resides but struggle to connect those insights.

BeyondTrust flags identities exhibiting risky behavior, excessive privilege or signs of compromise. Forcepoint provides visibility into sensitive data and the identities that can access it. Together, they reveal which risky identities pose the greatest potential for harm to the organization.

Business value:

- Focus on the highest security risks that matter most
- Reduce manual investigation effort
- Improve prioritization of security resources

See the Blast Radius of a Risky Identity

Not every risky identity presents the same level of threat. Understanding potential business impact requires visibility into the sensitive data that identity can access.

BeyondTrust identifies the risky identity, while Forcepoint reveals the volume, type and sensitivity of the data accessible to that identity. Together, they help organizations understand the potential consequences of a compromised account.

Business value:

- Prioritize high-impact incidents faster
- Improve risk assessment and decision-making
- Focus investigations where exposure is greatest

Accelerate Security Investigations

Security investigations often require analysts to assemble information from multiple tools before they can understand risk and determine next steps.

BeyondTrust and Forcepoint provide a correlated view of identity risk, sensitive data exposure and remediation context within a unified workflow. This reduces investigative complexity and helps teams move from detection to action faster.

Business value:

- Accelerate investigation and response times
- Improve analyst productivity
- Increase confidence in remediation decisions

Remediate Exposure Before It Becomes a Breach

Organizations frequently identify risky identities but lack an efficient way to protect data before an incident occurs.

By combining BeyondTrust's identity-risk intelligence with Forcepoint's data-access visibility, security teams can identify unnecessary access to sensitive data and take action to reduce risk, either by adjusting access permissions or moving sensitive data away from public shares. The process is fully auditable, helping organizations strengthen governance and prevent breaches.

Business value:

- Limit the attack surface
- Shorten exposure windows
- Lower the likelihood of data breaches
- Strengthen security governance

Business Outcomes

Improve Risk Prioritization

- Understand business risk through the combined lens of identity and data
- Identify the highest-priority threats faster
- Reduce manual analysis and correlation efforts

Accelerate Response

- Investigate incidents faster
- Respond with greater confidence
- Minimize delays caused by disconnected workflows

Reduce Data Exposure

- Minimize the attack surface
- Reduce exposure before incidents occur
- Strengthen overall security posture

Support Compliance and Audit Readiness

- Maintain an auditable record of identity risk, data access and remediation actions
- Support governance, compliance and security reporting requirements
- Improve accountability across security and IT teams

Joint Value

BeyondTrust answers:

What identities exhibit risky behavior?

Forcepoint answers:

What sensitive data can they access?

Together, they answer:

What are my highest risks and what actions reduce the exposure?

To learn more about Identity-Aware Data Security with Forcepoint and BeyondTrust, contact your Forcepoint or BeyondTrust representative.