



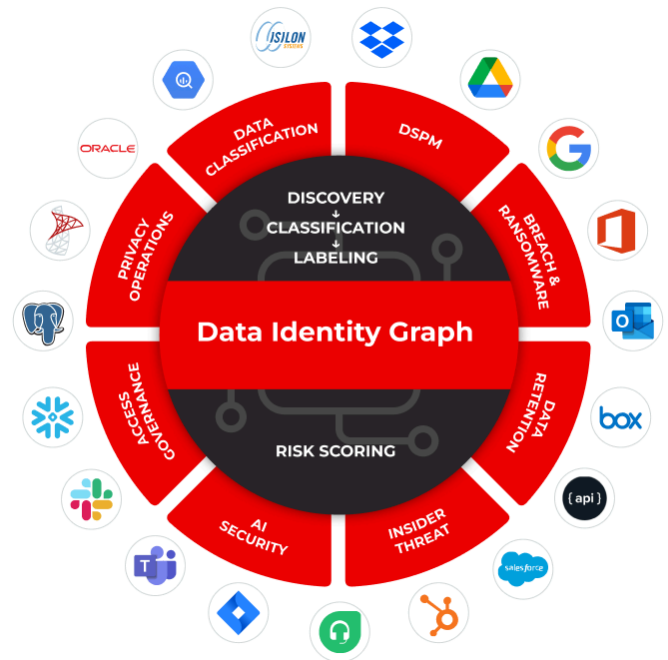
AI Security

See AI risk in real time. Protect sensitive data by governing GenAI and Copilot with confidence.



Govern AI data risk before it spreads

Lightbeam Data Identity Graph links every prompt, file, and user to real entitlements, so you know who saw what and why. Capture Copilot prompts and responses, classify sensitive content, and act in seconds: revoke access, quarantine files, or disable accounts with an audit trail. Risk Scores surface hotspots. UEBA and Ransomware Protection detect spikes and contain impact. Govern AI use across cloud, SaaS, and On-Prem without adding tools.



"Lightbeam offered granular control and unique insights into our sensitive data, mapping it to identities, something no other solution matched."

David Hanna, IT Security, Veridian Credit Union

90%

Reduction in manual data security and privacy operations

75%

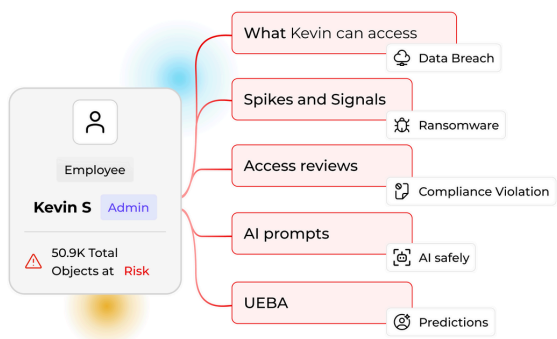
Faster remediation of risky data access

80%

Less time needed to prepare audit reports

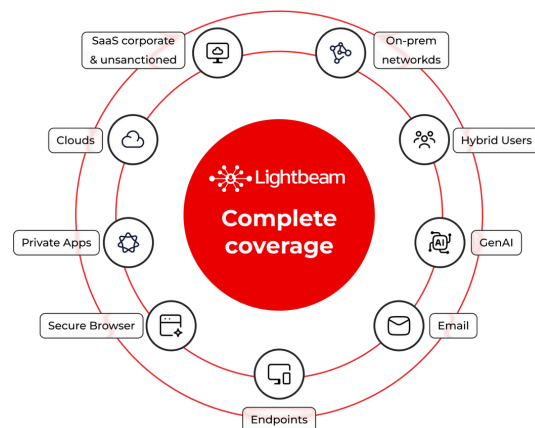
Shadow AI blind spots

Unknown or unsanctioned AI tools surface sensitive data without oversight. Lightbeam finds activity, ties it to identities, and lets you shut it fast.



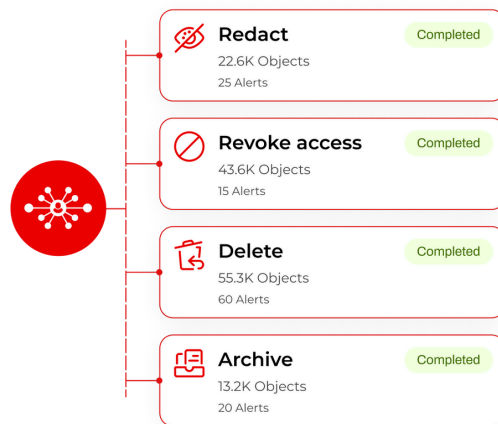
Cut excessive AI access

Limit what AI can access, surface, retain across cloud, SaaS, and On-Prem. Automate least-privilege revocation before oversharing becomes a breach.



Build an AI audit trail

Track every prompt, file, and identity touched by AI. Replay conversations, label content, and export evidence that shows who accessed what and when.



Data Visibility

Know **WHAT** data you have across Cloud, SaaS and On-prem apps.



Data Identity

See **WHOSE** data you have, **WHERE** (customers, employees, vendors).



Data Access

Enforce policies around **WHO** should have access to **WHOSE** data.

Try Lightbeam for free

Is your business poised for global expansion? Schedule your consultation and start your journey toward global success.

✉ info@lightbeam.ai

☎ +1 (650) 224 8706

🌐 www.lightbeam.ai