

Secure AI Transformation

Laying the foundation for Secure AI with Deloitte, Google Cloud, and Wiz

As AI accelerates both threat discovery and new attack surfaces, the window between vulnerability and exploitation has compressed from months to hours. Traditional security models can't keep pace with the growing gap between identifying a vulnerability and remediating it.

The inflection point: scaling AI, scaling risk



Shadow AI proliferation

Unsanctioned AI tools bypassing security controls can create invisible attack vectors.



Data hemorrhage

Sensitive data can leak through prompts, fine-tuning datasets, and model outputs without detection.



New AI attack surface

AI workloads introduce novel attack surfaces that existing security solutions were never built to prevent or detect.



Operational blind spots

Fragmented tooling and unscalable security programs lead to lack of unified AI visibility and control.

Achieve Secure AI Transformation

Deloitte's **Secure AI Transformation** solution is a foundational step for organizations building secure AI capabilities. It unites Deloitte's strategic advisory and cyber AI blueprint framework with Google Cloud's AI-native security infrastructure and Wiz's AI Application Protection Platform.

This integrated approach builds security directly into your AI platforms from the ground up, moving beyond reactive controls. Through strategic assessments and foundational safeguards, the solution helps you to proactively mitigate compounding AI risks, build systemic resilience, and rapidly accelerate AI security maturity, positioning security as a trusted enabler for secure business growth from the outset.

1 IN 5 BREACHES
INCLUDED SHADOW AI¹

43% OF EMPLOYEES
SHARE CONFIDENTIAL
DATA WITH AI²

73% OF ORGS
CITE PRIVACY AND SECURITY
AS TOP AI ADOPTION
CONCERNS³

Deloitte's cyber AI blueprint

Deloitte leverages its **cyber AI blueprint framework** to integrate Google Cloud's advanced AI and security tools with Wiz's comprehensive AI Security platform, assisting clients to proactively address emerging AI risks and establish secure AI operations, while providing organizations with potential benefits, including:

Accelerated,
confidence-driven
AI Innovation

Visibility and
proactive risk
management
(AI security posture
management/AI-SPM)

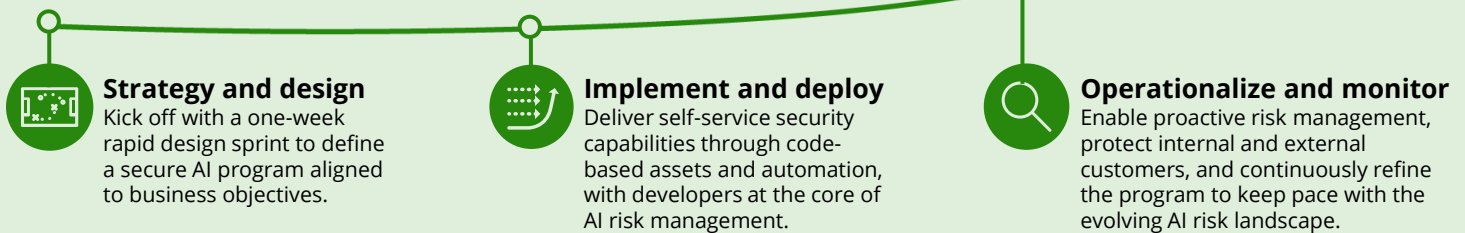
Reduced complexity
and lower costs
(tool consolidation)

Enterprise-grade
governance and
compliance

Seamless
scalability

How to engage

A mature, secure AI program integrates development, operations, and security by adopting a shift-left approach that helps protect Generative AI and agentic AI workloads in the cloud while supporting continuous compliance.



Bridging the gap with Deloitte, Google Cloud, and Wiz

Accelerate your digital transformation with the combined power of Deloitte's strategic experience, Google Cloud's scalable infrastructure, and Wiz's industry-leading cloud and AI security.

Deloitte.

Leverages **deep industry and cyber risk experience** to integrate technologies, transform your security operating model, and translate technical risks into clear business outcomes.

Google Cloud

Provides a **secure, scalable, and AI-ready cloud infrastructure**, offering advanced compute capacity and AI models for cyber defense.

WIZ

Delivers **visibility into your entire cloud and AI stack**, from code to cloud to runtime, allowing you to prioritize the risks that matter most.

CONTACT OUR TEAM



Mark Nicholson

Principal, Lead Alliance Partner,
Google Cyber
Deloitte & Touche LLP
manicholson@deloitte.com



Kristin Robbins

Managing Director, Cyber Lead
Deloitte & Touche LLP
kr Robbins@deloitte.com



Aaron Brown

Partner, Cyber
Deloitte & Touche LLP
aaronbrown@deloitte.com



Max Lechner

Sales Engineer, Google Cyber
Deloitte & Touche LLP
mlechner@deloitte.com



Abhi Kulkarni

Technology Fellow, Cyber
Deloitte & Touche LLP
akulkarni9@deloitte.com



Chris Trollo

Senior Manager, VP Executive
Deloitte & Touche LLP
ctrollo@deloitte.com



Melissa Hartman

Manager, Google Cyber Alliance
Deloitte Consulting LLP
mehartman@deloitte.com

Sources:

1. 2025 IBM data breach report.
<https://www.ibm.com/reports/data-breach>
2. <https://www.staysafeonline.org/articles/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-2025>
3. <https://www.deloitte.com/content/dam/assets-zone3/us/en/docs/services/consulting/2026/state-of-ai-2026.pdf>

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, 'Deloitte' means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services and Deloitte Consulting LLP, which provides strategy, operations, technology, systems, outsourcing and human capital consulting services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.