WIZ + Deloitte.

Partner Services Success

FINANCIAL SERVICES

The Challenge

A large financial-services enterprise needed greater visibility into its multi-cloud security posture and a consistent way to manage and remediate risk across business units. While the organization had multiple security tools in place, there were challenges aligning vulnerability management, developer workflows, and regulatory compliance.
Deloitte was engaged to help the customer operationalize Wiz as a core part of their security strategy - improving governance, automation, and ownership across teams.

The Partner Approach

Deloitte led a phased implementation that combined Wiz's cloud-native visibility with structured service delivery and governance frameworks.

1. **Cloud Posture Assessment and Baseline Setup**
   - Deployed Wiz Outpost within the client's cloud boundary to ensure data residency and compliance.
   - Authored custom rule sets and technical standards for AWS and Azure environments to align with financial industry controls.
2. **Vulnerability Management Integration**
   - Consolidated infrastructure and application findings into a single ticketing system for consistent prioritization.
   - Linked Wiz with the client's CMDB to automate updates and ownership of remediation tasks.
3. **Shift-Left Enablement**
   - Developed Terraform modules and CI/CD integration so developers could run on-demand Wiz scans during code deployment.
   - Enabled application teams to detect and resolve issues earlier in the development cycle.
4. **Cloud Security Operations Runbook**
   - Built and operated Wiz-driven dashboards to track high-risk alerts and remediation progress.
   - Served as a client advocate with Wiz to map product roadmap features to the organization's requirements.

The Customer Outcome

- **Accelerated Visibility:** Wiz was fully operationalized across multi-cloud environments with real-time monitoring of compliance and vulnerabilities.
- **Reduced Risk Exposure:** Integration of Wiz into ticketing and DevSecOps pipelines reduced mean time to remediation by over 40%.
- **Improved Collaboration:** Deloitte's RACI framework established clear ownership for security findings across infrastructure, application, and risk teams.
- **Scalable Governance:** The security framework developed with Deloitte now serves as a repeatable model for future business units and cloud deployments.

Why This Worked

1. **Governance-First Approach:** Deloitte addressed compliance and data residency concerns up front through Wiz Outpost, building immediate stakeholder trust.
2. **Operational Integration:** By embedding Wiz into existing workflows (ticketing, CMDB, CI/CD), Deloitte made security part of daily operations, not an afterthought.
3. **Shift-Left Empowerment:** Developers were equipped to identify and fix vulnerabilities earlier, reducing noise and improving productivity.
4. **Defined Ownership and Accountability:** Implementing a RACI framework ensured every alert had a responsible owner, driving consistent remediation.
5. **Partner Advocacy and Collaboration:** Deloitte's close collaboration with Wiz ensured rapid feature adoption and alignment with the customer's evolving needs.

Key Takeaway

"Wiz + Partner Expertise = Operationalized Cloud Security."

By pairing Wiz's visibility and automation with Deloitte's structured deployment and governance approach, the customer achieved a scalable, compliant, and repeatable model for cloud security management.