WIZ + Deloitte.

Partner Services Success

HEALTHCARE

The Challenge

A large U.S.-based healthcare organization was using multiple CSPM tools – including Azure Policies, Microsoft Defender for Cloud, and Wiz – to assess cloud security posture.

However, the customer faced several challenges:

- **Duplicative efforts and overlapping controls** across different platforms
- **Fragmented visibility** into cloud risk
- **Conflicting or unclear ownership** of preventative vs. detective policies
- **Inefficient alert routing,** slowing remediation
- **Compliance monitoring gaps** caused by inconsistent workflows

The customer needed a unified, strategic coexistence model that would maximize the value of each technology while reducing operational inefficiencies.

The Partner Approach

Deloitte led the design and implementation of a coexistence strategy to streamline cloud security posture management and clarify policy ownership across platforms.

1. **Preventative Policies & Corrective Policies Strategy**
    a. Developed a coexistence model to maximize the strengths of Azure Policies, Microsoft Defender, and Wiz.
    b. Recommended using Azure Policies for preventative controls (deny/block) and using Wiz for monitoring, corrective, and remediation-focused controls.
    c. Ensured Wiz was not generating redundant Azure Policies, reducing unnecessary operational workload.
2. **Wiz Integration & Workflow Automation**
    a. Leveraged Wiz out-of-the-box policies and introduced additional custom Wiz policies where necessary.
    b. Integrated Wiz with ServiceNow (SNOW) to automatically generate incident tickets for the appropriate security and infrastructure teams.
    c. Routed high-priority alerts to Splunk for real-time visibility by the central response team.
3. **Workflow & Exception Handling**
    a. Defined and automated alerting workflows to streamline remediation processes.
    b. Introduced governance processes for exception management to ensure consistent handling of compliance violations.

The Outcome

Deloitte's coexistence strategy delivered measurable improvements across efficiency, risk management, and security operations:

- **Maximized value of all CSPM technologies** by clearly dividing responsibilities between Azure and Wiz.
- **Enhanced compliance posture** through automated alert routing, exception processes, and consistent remediation workflows.
- **Improved visibility** across cloud environments by consolidating reporting and ensuring stakeholders received timely updates.
- **Faster response times** thanks to SNOW and Splunk integrations that created clear escalation paths for high-risk alerts.
- **Reduced duplication and operational overhead**, eliminating redundant policies and manual processes.

Why This Worked

1. **Clear Segmentation of Responsibilities:** Deloitte helped the customer avoid overlapping controls by clearly defining which platform owned preventative vs. detective controls.
2. **Leveraging Strengths of Each Technology:** Maximizing Azure Policies for prevention and Wiz for detection/remediation ensured optimal usage of both toolsets.
3. **Integrated Workflows, Not Standalone Tools:** By connecting Wiz with SNOW and Splunk, Deloitte ensured cloud security data flowed directly into the customer's existing operational systems.
4. **Governance + Automation:** Automated alerting and defined exception-handling processes allowed teams to act quickly and consistently.
5. **Flexible Policy Architecture:** A blend of OOTB and custom Wiz policies supported both broad coverage and organization-specific requirements.

Key Takeaway

The combination of Wiz's real-time visibility and Deloitte's structured policy and workflow strategy enabled the customer to operate with stronger compliance, faster remediation, and clearer ownership across security teams.