

## Security Solutions

Trace3's Security Solutions team leverages decades of combined experience in the field to address our client's most pressing security challenges. This expertise helps make Trace3 one of the most trusted partners in the emerging technology and security space.

Client ("Client") seeks Trace3's assistance to support the enhancement of their security posture by implementing Wiz within their Cloud Service Provider environment.

### SUMMARY OF SERVICE

Trace3 will deliver a Wiz Cloud Implementation to a single Cloud Service Provider (CSP) to deploy, configure, and operationalize Wiz's Cloud-Native Application Protection Platform (CNAPP). This engagement provides a structured and validated deployment across Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWPP), and Cloud Infrastructure Entitlement Management (CIEM) capabilities. The engagement, which is delivered in up to **one-hundred (100) hours**, includes:

- Connecting a client CSP environment via Wiz Cloud Connectors and validating ingestion
- Establishing secure access and role-based governance integrated with Client's identity platform
- Configuring projects, dashboards, scanners, and workflows aligned to business requirements
- Integrate with ticketing/chat tools and building automation for prioritized issue routing
- Delivering knowledge transfer and optionally, documentation and runbooks to enable effective day-to-day operations post-engagement

### METHODOLOGY

#### Kick-Off and Project Initiation

- **Kick-Off Call:** Trace3 will conduct a structured kick-off session to define the project scope, timelines, roles, and success criteria. During this call, Trace3 will also confirm CSP accounts, regions, and any data residency requirements to ensure alignment from the start.
- **Documentation Review:** The Trace3 team will review any existing architecture diagrams, IAM/IdP configurations, tagging standards, and/or CI/CD pipelines to establish a baseline understanding of Client's environment.

#### Current State Discovery

- **Discovery Workshop:** Trace3 will facilitate a collaborative workshop to map stakeholder goals, current environments, ticketing processes, security tools, access control models, regulatory requirements, and external integrations. The outcome is a shared understanding of Client's current state and the inputs required for a successful Wiz deployment.
- **Action Plan:** Based on discovery inputs, Trace3 will develop a Deployment Workbook and Acceptance Test Plan tailored to Client's environment. Trace3 will create and confirm onboarding stories that align with Client's organization's requirements and priorities.

## Security Solutions

Trace3's Security Solutions team leverages decades of combined experience in the field to address our client's most pressing security challenges. This expertise helps make Trace3 one of the most trusted partners in the emerging technology and security space.

### Deployment & Configuration

Deployment and Configuration establishes the core Wiz platform components and aligns them to Client's environment and security requirements. The goal is to configure access, connectivity, projects, scanners, and integrations so Client's organization has a secure and operational baseline deployment of Wiz.

### Access & RBAC

- Configure enterprise SSO (SAML/OIDC).
- Map IdP groups to least-privilege Wiz roles (global and project-scoped).
- Provision auditable service accounts with narrowly scoped API permissions, secret rotation, and optional IP whitelisting.

### Cloud Connector

- Deploy Wiz Cloud Connector via CloudFormation in management or target accounts.
- Scope to the full Organization or selected accounts/regions per policy.
- Verify status (Active), confirm data ingestion, record role ARN/stack ID.
- Establish recurring rescan and health-check cadence.

### Projects & Dashboards

- Model a folder to project hierarchy aligned to business units and environments.
- Apply resource scopes, ownership, and risk profiles.
- Configure boards and widgets (Security Score, MTTR, Top Issues, WQL views).
- Define reporting cadence.

### Scanners & Tuning

- Select encrypted-disk strategy: CMK sharing or snapshot/volume tuning where required.
- Optionally enable non-OS disk scanning capabilities
- Standardize tag inheritance and exclusion tags.
- Configure compute instance sampling with priority on active hosts.

### Integrations & Automation

- Configure up to two integrations (e.g., Jira/ServiceNow + Slack/Teams) using secure per-integration service accounts.
- Build automation rules to route Critical/High issues by project/severity with SLAs.
- Validate workflows through test runs and optionally enable curated exports (e.g., S3/Snowflake) for analytics.

## Security Solutions

Trace3's Security Solutions team leverages decades of combined experience in the field to address our client's most pressing security challenges. This expertise helps make Trace3 one of the most trusted partners in the emerging technology and security space.



### Validation and Outcome

The Validation and Outcome stage ensures that all components of the Wiz deployment are functioning as intended and aligned with the Client organization's requirements. By validating each configured element, Trace3 will confirm the system is stable, secure, and ready for production use. Execute Acceptance Test Plan will confirm:

- Connector health and ingestion.
- Access controls and role mappings.
- Dashboards, boards, and reporting outputs.
- Automation workflows and integration triggers.
- Document exceptions, remediations, and next steps.

### Knowledge Transfer

Knowledge Transfer is designed to equip Client's team with the knowledge and tools to operate Wiz effectively. The objective is to transfer expertise on the deployed architecture, configuration, and ongoing management processes so Client's staff can manage Wiz independently. Participants will gain both practical guidance and best practices for long-term success. Trace3 will facilitate a one-day session (up to 10 participants) covering:

- Wiz architecture and configurations.
- Connector lifecycle management.
- System health triage workflows.
- Project/Role-Based Access Control best practices.
- Recommended operational runbooks and next steps.

### Close-Out and Project Handoff

Trace3 will host an up to two-hour close-out meeting with project participants to deliver a Trace3 presentation summarizing the outcomes, lessons learned, and prioritized roadmap.

## Security Solutions

Trace3's Security Solutions team leverages decades of combined experience in the field to address our client's most pressing security challenges. This expertise helps make ACME one of the most trusted partners in the emerging technology and security space.

Phase	Overview
<b>Kick-Off &amp; Project Initiation</b>	Conduct a structured kick-off to define scope, timelines, roles, and success criteria while confirming CSP accounts, regions, and data residency requirements. Review existing architecture, IAM/IdP details, tagging standards, and workflows to establish a baseline understanding.
<b>Current State Discovery</b>	Facilitate a discovery workshop to capture stakeholder goals, environments, ticketing, tools, and compliance needs. Develop a Deployment Workbook and Acceptance Test Plan while creating onboarding stories aligned to requirements.
<b>Deployment &amp; Configuration - Access &amp; RBAC</b>	Configure enterprise SSO (SAML/OIDC) and map IdP groups to least-privilege roles. Provision service accounts with narrowly scoped API permissions, secrets rotation, and optional IP allow listing.
<b>Deployment &amp; Configuration - Cloud Connector</b>	Deploy Wiz Cloud Connector(s) in management or target accounts, scoped to the organization or specific regions. Validate ingestion, record role ARNs, and establish recurring health checks.
<b>Deployment &amp; Configuration - Projects &amp; Dashboards</b>	Build a project hierarchy aligned to business units and environments. Configure boards, widgets, and reporting cadences to provide clear visibility into risks and ownership.
<b>Deployment &amp; Configuration - Scanners &amp; Tuning</b>	Configure encrypted-disk scanning strategies, enable optional workloads, and tune exclusions. Standardize tag inheritance and optimize compute instance sampling for efficiency.
<b>Deployment &amp; Configuration - Integrations &amp; Automation</b>	Configure up to two integrations (e.g., Jira/ServiceNow, Slack/Teams) and establish event-driven automation rules. Validate workflows for routing high-priority issues and enable curated exports if required.
<b>Validation &amp; Outcome</b>	Execute the Acceptance Test Plan to confirm connector health, RBAC, dashboards, and integrations. Document exceptions, remediations, and next steps to ensure readiness.
<b>Knowledge Transfer</b>	Deliver a one-day knowledge transfer session for up to 10 participants covering Wiz architecture, lifecycle operations, and best practices. Provide guidance on ongoing operations and adoption.
<b>Close-Out &amp; Project Handoff</b>	Host an up to two-hour close-out meeting with participants and present outcomes, lessons learned, and operational guidance. Ensure smooth transition to operations without requiring additional documentation.