WIZ + escape

Executive summary of the integration

As cloud adoption accelerates and application environments grow more complex, understanding what's exposed—and mitigating risks—across the full spectrum, from code to the cloud, has become essential. Escape and Wiz bring together two unique strengths: Wiz excels at identifying cloud infrastructure vulnerabilities, while Escape focuses on the application layer to uncover risks such as API exposures, sensitive data leaks, and business logic flaws with its DAST. Together, Escape and Wiz help customers understand the full context, assign clear ownership, and empower security and development teams to work smarter, faster, and more confidently to integrate security into applications early in the development lifecycle.

Market challenge

For many organizations, the challenge isn't running a scan but understanding the full application and cloud context and determining ownership of infrastructure at risk. With the complexity of modern apps, identifying vulnerabilities at the business logic level and mapping them can take months. Without clear context & ownership, security teams face delays and struggle to engage development teams in building security early in the lifecycle.

Benefits of the integration

- **Practical Code-to-Cloud Security:** Large organizations often struggle to bridge application-level exposures with cloud infrastructure insights. Now, they can correlate both from Escape & Wiz, track them back to the same responsible teams, and reduce friction between dev, ops, and security.
- **Immediate Assignment:** If Escape finds a user associated with the Wiz application, the moment Escape's DAST finds a security issue that's also a Wiz issue, you know exactly which team needs to address it. No more guesswork, no more rummaging through outdated confluence pages or domain registries.
- **Reduced Operational Overhead:** Security Engineers spend less time "hunting" for who owns what and how to prioritize your API and Web App risks. Instead, they can devote their energy to actually securing the organization.
- **Acceleration of Remediation:** When ownership data is at your fingertips, the gap between detection and remediation shrinks from weeks or months to days or even hours. This empowers you to confidently integrate security into applications early in the development lifecycle.
- **One Unified View:** All vulnerabilities and CWEs—from exposed S3 buckets to API logic flaws—flow into a single Wiz interface. This "single pane of glass" eliminates information silos and drastically reduces the likelihood of serious issues slipping through the cracks.

The better together story

With the number and complexity of modern cloud-native applications increasing, securing them has become critical for organizations. Escape's integration with Wiz provides a unified solution for the security of modern cloud-native applications from code to cloud. Escape ingests network exposure data from Wiz, identifies whether an asset is exposed and what type of application it is, and maps it to code repositories and owners. Once resources are linked, Escape runs large-scale DAST scans to uncover business logic vulnerabilities, API misconfigurations, and sensitive data leaks. Each newly identified CWE finding and corresponding remediation are fed back into the Wiz and automatically enriched with available project ownership data, merging both infrastructure and application-level insights into a single, unified view. By consolidating findings into one seamless workflow, organizations gain end-to-end visibility across all environments, prioritize threats with full cloud context, and enhance security—without slowing development speed.

Use case overview, challenge and solution

Use case

Secure cloud-native APIs, SPAs, and microservices, even at the business logic level. Organizations with large or rapidly scaling technology stacks need a solution that not only identifies but also helps resolve threats without compromising development speed.

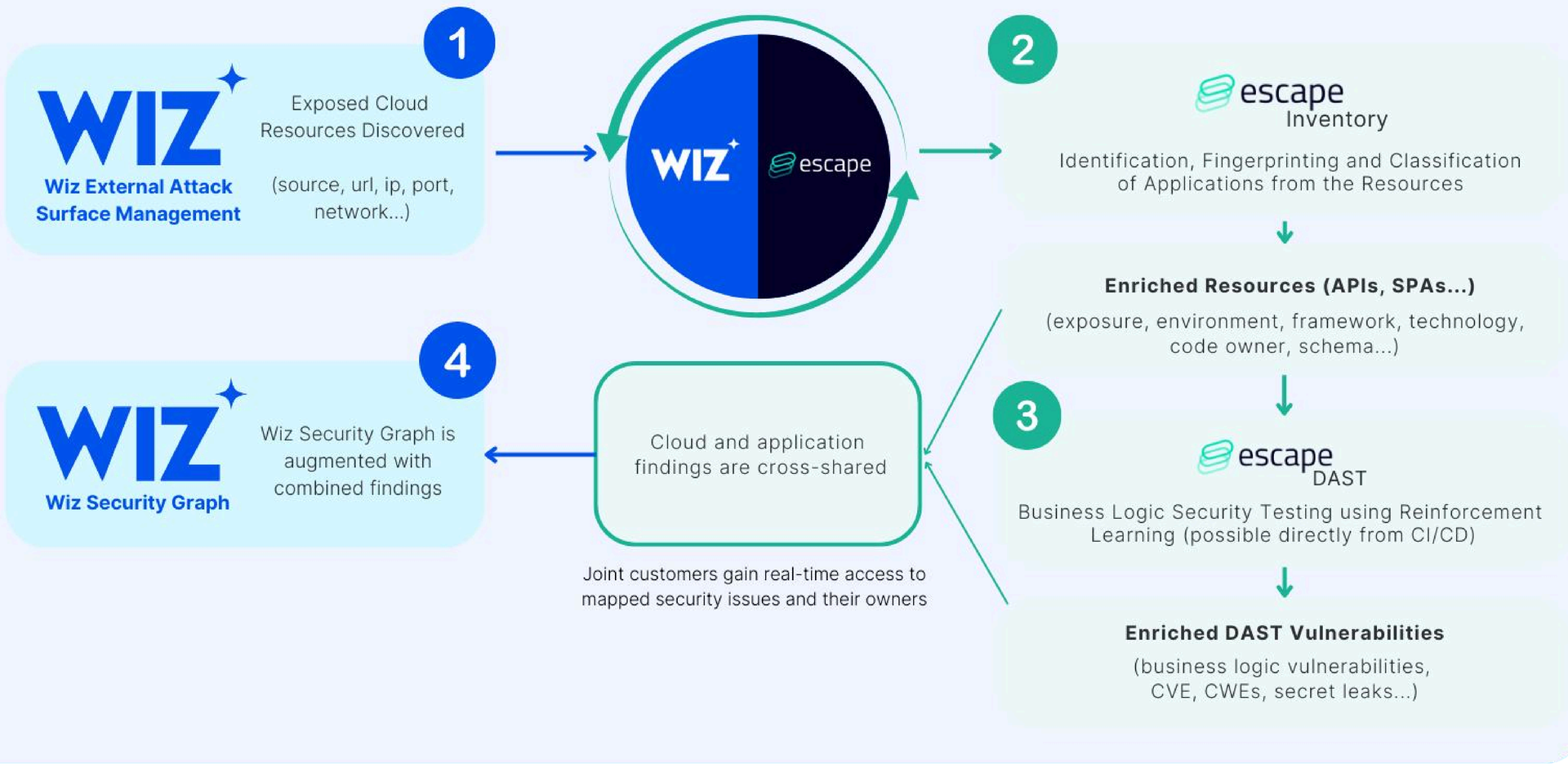
Challenge

Modern applications are becoming increasingly complex and are often prime targets for attackers. With hundreds (or even thousands) of APIs and SPAs, finding business logic vulnerabilities and mapping resources to the right stakeholders for remediation can be time-consuming. Security teams often struggle to connect application-level vulnerability findings with cloud infrastructure insights, spending valuable time figuring out ownership and how to prioritize API and web app risks.

Solution: Enhanced Vulnerability Data with Contrast Security

Escape's integration with Wiz empowers organizations to secure modern applications by combining Escape's large-scale DAST scanning with Wiz's agentless inventory, misconfiguration detection, and dynamic exposure scanning. Using previously ingested and enriched Wiz resources, Escape DAST identifies business logic vulnerabilities, API misconfigurations, and sensitive data leaks, then feeds these findings—including CWE classifications and remediations—directly into Wiz. This integration enriches security teams with valuable context and ownership data, enabling them to prioritize and remediate vulnerabilities more effectively. With this unified solution, organizations can detect risks quickly, gain clear ownership insights, and confidently embed security early in the development lifecycle.

Unified Security for Modern Cloud-native Applications



About Wiz

Wiz is on a mission to transform cloud security for customers – which include 45% of the Fortune 100 – by empowering them to embrace a new cloud operating model. Its Cloud Native Application Protection Platform (CNAPP) delivers full-stack visibility, accurate risk prioritization, and enhanced business agility. The result? More context with less noise, so that security teams can focus their time on what matters most.

About Escape

Escape helps 2000+ security teams worldwide discover and secure all modern applications—APIs, Single-Page Apps, and Microservices, without the need for complex setup or network changes. With Escape, you can document your applications in minutes, run DAST scans at the business logic level at scale and in CI/CD, and reduce developer remediation overhead with code fixes tailored to each development framework.