DAZZ.

The Dazz Unified Remediation Platform

Security and development teams are facing pressure to not only detect security issues faster than before, but to show evidence that they are fixing them. Increased executive and regulatory scrutiny, an ever-growing attack surface, and faster cyber attacks are all making remediation a pressing security issue. Yet with data fragmented across multiple environments, technologies, and detection tools, today's fragmented and manual processes to prioritize and fix vulnerabilities are too complex and slow to keep pace with the business.

We unify data for remediation

The Dazz Unified Remediation Platform gives security and development teams one remediation solution for everything developed and run in code, clouds, applications, and infrastructure. The Dazz Unified Remediation Platform aggregates data from a plethora of detection technologies, correlates and prioritizes related issues, traces back to root causes, and delivers a contextual remediation plan in order to measurably reduce exposure.

With Dazz, you can finally answer critical questions, such as:

- Do we have exploitable secrets in code in production?
- Do we have shadow pipelines?
- How many alerts are false positives and duplicates?
- Which vulnerabilities should we prioritize, based on business risk?
- How do we discover and fix the root cause of the issue?
- Who is the developer responsible for fixing this vulnerable artifact?
- What context is available for the owner to fix the issue as fast as possible?

Discover

Understand every resource and application developed an run across code, clouds, applications, and infrastructure.

Reduce

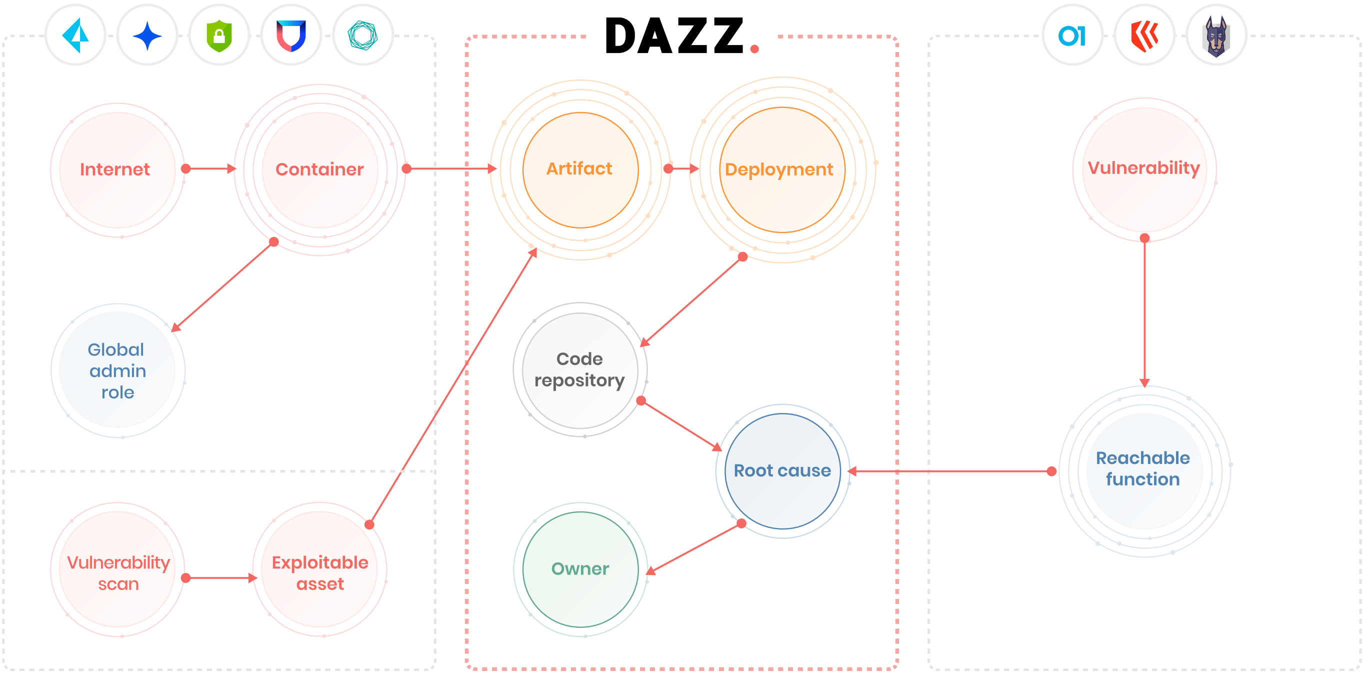
Clean up the noise: deduplicate alerts and prioritize CVEs, misconfigurations, and secrets in code based on their unique root causes, then automatically find owners.

Fix

Use both assistive and automatic remediation actions in a dev-friendly workflow to rapidly fix critical issues.

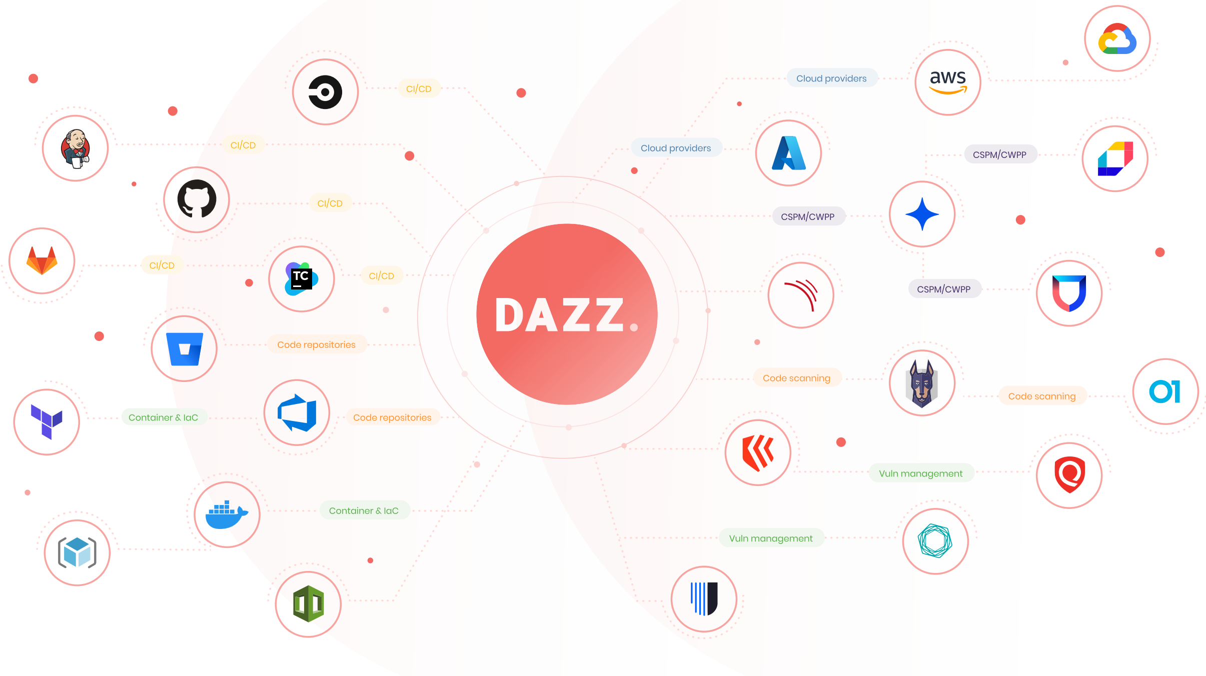
How it works

The Dazz Unified Remediation Platform connects to detection tools and technologies to trace issues back to root causes. Dazz has patent-pending root cause analysis technology that uniquely analyzes data to backtrack each security issue to where it originates. For instance, the Dazz solution understands which specific cloud resource caused the security issue being seen in a cloud security tool and traces the cloud resource back to the specific pipeline that was used to deploy it. By fully examining pipelines, we are able to understand which vulnerable artifact was deployed, and what triggered its build. Furthermore, by connecting to the source code, we are able to analyze the specific commit and developer that applied the change and ultimately provide context on the root cause for fast, efficient remediation.



Connect your existing security tools

The Dazz Unified Remediation Platform easily connects into environments via read-only APIs to quickly aggregate relevant data. Dazz's rich API catalog is platform agnostic and allows organizations to seamlessly integrate best-of-breed detection tools rather than compromise on quality with one or two vendors. The platform currently supports a wide variety of integrations across cloud IaaS providers, CI/CD and source code management platforms, cloud native application protection platforms (CNAPP), AppSec solutions, vulnerability assessment solutions, API security, and data security platforms.

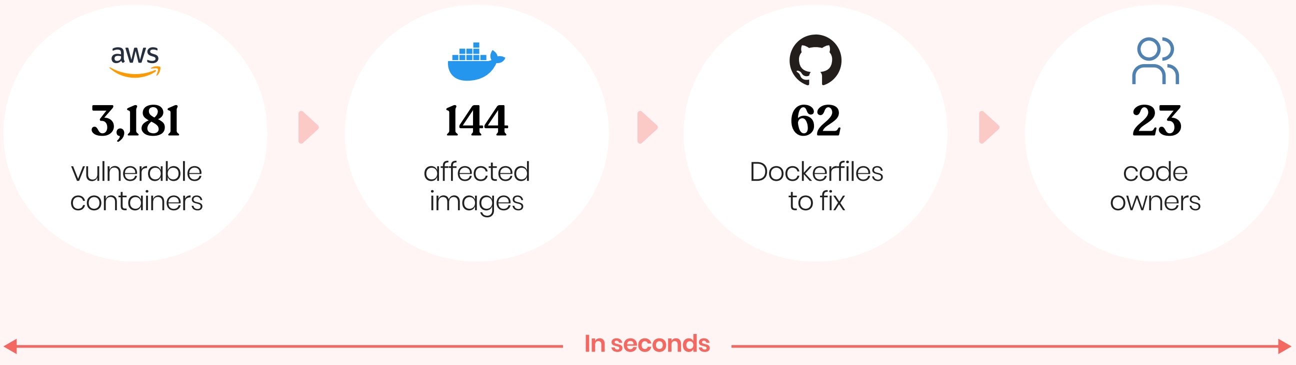


Reduce risk in minutes, not months

Dazz simplifies and automates the otherwise cumbersome process of remediating security issues across cloud, code, applications, and infrastructure. Our unique root cause analysis enables effective and swift remediation of groups of security issues at the root cause. Dazz customers prioritize the most critical root causes instead of chasing a never-ending alert backlog. In doing so, they are able to shrink their exposure window by reducing the mean-time-to-remediate (MTTR) from weeks to minutes, and communicating the right fixes instead of throwing problems over the fence to developers.

Case study: Fortune 500 financial services

One of our customers, a Fortune 500 financial company, purchased the Dazz Remediation Cloud only a few weeks before the infamous Log4j incident back in 2021.
With simple API-based integration, the team connected the Dazz Unified Remediation Platform to GitLab, so it could discover and map all of the organization's code-to-production development pipelines. Within minutes, the Dazz solution showed which security tools were in use, and reduced thousands of alerts in production to only several key root causes that actually needed to be fixed.
The Dazz Unified Remediation Platform also identified the owners who should fix every root cause and auto-generated developer-friendly fixes, allowing developers to take corrective action quickly.
The outcome was that over 3,000 containers were fixed in four days. Now that the team is using Dazz for all vulnerabilities, they were able to cut mean-time-to-remediation (MTTR) by more than 90 percent and close the risk window of un-remediated vulnerabilities from weeks to four days.



Want to learn more?

To learn more about Dazz, please visit our website at www.dazz.io. You can request a demo or meeting at contact@dazz.io. We would love to hear from you!