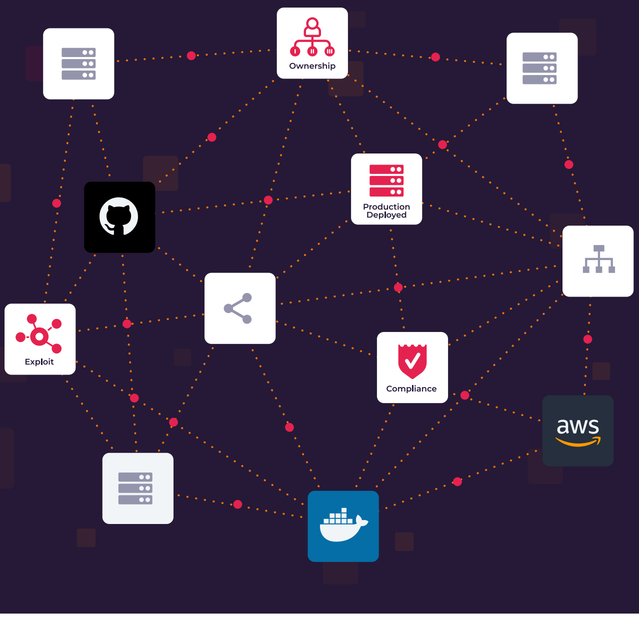
TROMZO | ASPM SOLUTIONS BRIEF

Risk-Based ASPM from Code to Cloud

Tromzo is the first risk-based ASPM (application security posture management) platform that delivers rapid remediation of security vulnerabilities from code to cloud. Security teams use Tromzo's proprietary Intelligence Graph to identify critical software assets – including ownership and lineage – and remediate the vulnerabilities that pose the greatest risk to the business.



Reduce Risk through Rapid Remediation

Tromzo accelerates remediation by building a prioritized risk view of the entire software supply chain with deep environmental and organizational context — from code to cloud. This context identifies which software assets are critical to the business, prevents risks from being introduced to those assets, and provides a roadmap for remediation including which assets are impacted, who owns them, and how to fix vulnerabilities.

Discovery Artifact Inventory & Risk Posture

Contextual software asset inventory (code repositories, software dependencies, SBOMs, containers, microservices, etc.), so you know what you have, who owns them, and which ones are important to the business.

Reduce MTTR by 60%: Turn To-Do's into How-To's

Tune out the noise and automate the remediation lifecycle so you can eliminate the manual processes of triaging, prioritizing, associating ownership, risk acceptance, and compliance workflows.

Achieve a Data-Driven Security Program

Understand the security posture for every team with SLA compliance, MTTR, and other custom KPIs, so you can drive risk remediation and accountability across the organization.

Why Tromzo?

- Gain visibility of software assets with associated ownership.
- Ensure security scan coverage for all business critical assets.
- Save time by automating manual triaging and vulnerability tracking.
- Reduce MTTR by over 60% for issues that truly matter.
- Designed by security practitioners for security practitioners, and backed by more than 25 CISOs.
- We know what you're going through, and we know what needs to be done. So we did it...

What Makes Us Awesome?!

Code to Cloud Context
Single source of truth to identify every software artifact and its risk based on business context.

Asset Ownership
True understanding of who is building and deploying which artifacts, and who owns the risk.

Security Guardrails
Pre-built and customizable security policies in CI/CD to influence developer behavior.

Automated Triaging & Prioritization
Automatically eliminate noise from many scanners, and only prioritize the few important issues based on the code to cloud context.

Developer Workflow Integration
Streamline remediation within existing developer tooling. They'll thank you for it.

Flexible Dashboards
Pre-built and customizable dashboards for data driven insights to all stakeholders.

Integrations
Tromzo partners with leading technology vendors to create a single source of truth for all software assets so application and product security teams know what risks are being introduced by the code being built. Any new integration guaranteed in five business days.

aws SYNOPSYS O1

A small subset of our integrations

About Tromzo
Code and cloud infrastructure are deployed faster than they can be secured, resulting in unmanageable risk. Existing security tools lack the business context to accurately identify and assess risk. Even when vulnerabilities are prioritized by severity, security teams don't know what software assets are critical, who owns them, or how to reduce year-long remediation timelines.

Unlike other security tools that are designed to help reduce noise or simply prioritize by severity, the Tromzo ASPM platform accelerates mean-time-to-resolution from many months to just a few days. Tromzo easily integrates with existing dev tools, security solutions, and cloud platforms to gain the context necessary to quickly remediate critical vulnerabilities.