TROMZO

WHITEPAPER

Build or Buy?

Application Security Posture Management (ASPM)

What is ASPM and Why is it Important?

Application Security Posture Management (ASPM) Platforms are quickly becoming more prominent in cybersecurity – even Gartner released research on this rapidly-growing sector.

Today, companies are deploying cloud and code assets faster than they can be secured. Security teams often don't even have visibility into these assets, making them much more vulnerable to risk. Whatsmore, once vulnerabilities are discovered, remediation takes many months as it is still a manual process to understand what software assets are impacted, who owns those assets, or how to fix the issues.

ASPM solutions are designed to address these issues and improve risk management in three key ways:

UNDERSTANDING RISK:
discover and aggregate vulnerabilities, reduce noise, and identify/ prioritize real risk

REMEDIATING RISK:
accelerate remediation through automated triage – what is impacted, who owns it, how to fix it

COMMUNICATING RISK:
measure risk over time across environments, applications, and teams

Without ASPM, security teams are burdened with manual and time-consuming processes, longer and complex remediation timelines, and, ultimately, greater risk.

Build or Buy?

The promise and value of ASPM is self-evident. Now security teams are left with an important decision to make: "Should we build or buy an ASPM?"

Why Companies Consider "Build"

The pain that ASPM addresses is so great that most large security organizations have already started building ASPM features whether they know it or not. A script here, some automation there, and a few custom integrations with JIRA and Slack later and it's easy to flirt with the idea of a homegrown solution.

There is also a very slippery slope of assumptions like "nobody understands our apps and environments like we do" or "I'm sure no vendor would have considered our particular use case" that have launched many inhouse ASPM projects. However, homegrown ASPM projects take longer to build, have limited features and capabilities, and have a higher total cost of ownership (TCO) compared to the ASPM solutions on the market today. Let's better understand why that is the case.

Why Companies Ultimately Choose "Buy"

Development of ASPM features begins out of necessity, but when security teams look at the full sets of features and desired outcomes it is clear why they tend to buy a complete ASPM platform instead of building, maintaining, and supporting their own homegrown solution.

Faster-Time-To-Value

The ultimate purpose of ASPM solutions is to reduce risk. This outcome is often achieved while also delivering additional benefits like reduced noise from scanners (e.g. SAST, DAST, SCA), less time spent triaging vulnerabilities, and better visibility into risk. Many ASPM platforms can start delivering value within just a couple of weeks. Vendor-based solutions already have years of development into their platform with many deep integrations with tools that exist in your tech stack.

Building an ASPM from scratch is often focused on a symptom (e.g. time spent triaging vulnerabilities), not the overall goal of reducing risk. And most security teams don't have a full team of product managers, UX designers, frontend developers, backend developers, QA/testing, etc. available to work on the homegrown solution. The end result is an under-staffed and under-resourced project that takes many months to even begin chipping at the challenges ASPM solves.

Rich and Flexible Features (& Avoid Lock-in!)

ASPM vendors have large development teams to bring a broad and rich set of features to customers. Most ASPM vendors integrate with dozens and dozens of cloud platforms, code repositories, and security tools so you can futureproof your application security and work with whatever tools you want across code to cloud.

For homegrown ASPM solutions, features and integrations are limited and ad hoc. Offering feature parity across cloud environments and security stacks is also impractical. Building an in-house ASPM can create lock-in to your existing stack. Migrating to another cloud or changing security tools may deprecate the homegrown solution or require months of refactoring to adjust to the environment. Additionally, homegrown projects are usually managed by just a couple people. If they ever go on extended leave or decide to part ways with the company, the project will fail.

Buying ASPM gives you the need-to-have and the nice-to-have features out-of-the-box, and gives you the same capabilities across every code to cloud environment.

Lower Total Cost of Ownership (TCO)

The final reason why most organizations choose to buy an ASPM solution instead of building one themselves is because it is a lot less expensive.

Homegrown ASPM solutions cost millions of dollars to build, maintain, and support. As mentioned above, most security teams don't even have product managers, UX designers, frontend developers, or backend developers to dedicate to the project. Existing resources will be fragmented to build a minimum viable product. Ultimately, the in-house project will take much more time to deliver value, be less flexible and feature rich, and cost significantly more than today's modern ASPM solution.

TROMZO

What is Tromzo?

Tromzo doesn't just reduce noise, we accelerate remediation by discovering critical assets,identifying asset ownership, and providing details on how to resolve vulnerabilities.

Learn More