Contrast SECURITY

What you need to know about

Application Security observability

Definition

Application Security (AppSec) observability is the security blueprint extracted directly from your running software.

Security teams can:

- Automatically generate an architectural blueprint that reveals an application's attack surface.
- See which security defenses are in place or missing, like authentication and access controls.
- Take security decisions that instantly reduce the application risk.

Application architects and product owners can:

- Instantly generate architecture blueprints for each application.
- See all the connections that each route makes.
- See all the dangers on each route.
- Make decisions that improve the security of each application they own.

What's the difference between security monitoring and security observability?

According to Splunk, security monitoring is the catch-all name for the process of detecting threats and managing security incidents.

Security Monitoring v. Security Observability

Phase 1.
Acquiring and analyzing logs, data and indicators of security threats.

Phase 2.
Responding with security risk remediation actions.

Contrast Security defines AppSec observability as the capability to watch live the running software and directly observe the exact routes, calls, dangers and defenses of each application.

It is a way to watch and reveal all application and application programming interface (API) activities in multiple directions, including:

- Attack surface
- Defenses
- Dangerous methods and outbound calls to API endpoints
- System interactions
- Database
- Connections and file system interactions

Why don't many enterprises have good AppSec observability?

Security is a decade behind software engineering. We are just starting to transform the work of security the way that DevOps (and powerful DevOps tools) transformed software development.

According to a 2024 report,

88%

of organizations mentioned the increasing complexity of their technology stack.

This makes it ever more challenging to track and gain end-to-end observability.

Another report found that

97%

of firms grapple with visibility into their apps, leading to potential vulnerabilities.

According to Deloitte insights,

79%

of organizations acknowledge an asset visibility gap.

This leads to three times more incidents.

Traditional AppSec testing tools, like Static Analysis Security Testing (SAST) and Dynamic Application Security Testing (DAST), adopt an outside-in approach.

This means that they lack true application context that can only be observed at application runtime and can only be obtained by instrumenting security from within.

What happens when enterprises lack proper security observability?

In short, nothing good.

According to Google:

Close to 100 zero-day vulnerabilities were exploited in the wild in 2023, which is 50 percent more than in 2022.

The 2024 Verizon Data Breach Investigations Report found that:

Breaches caused by exploited vulnerabilities rose by 180% year over year.

What can AppSec observability provide?

Always-on monitoring in both test and production environments to easily spot and address exploitable vulnerabilities.

Visibility into the blueprint of each application, its routes, connections, dataflows, dangers and defenses.

Never-before-seen accuracy of security improvements and risk mitigation.

6 key use cases for Runtime Security observability for web applications

01 Early threat detection:

Monitor your digital infrastructure in real time so you can spot potential threats before they happen.

02 Vulnerability triage/risk prioritization:

Quickly detect vulnerabilities as they manifest in the operational environment.

03 Threat modeling:

Continuously update and refine threat scenarios based on live application behavior.

04 Incident response and forensics:

Collect and analyze detailed runtime data to trace back security incidents and understand attack vectors.

05 Targeted penetration testing:

Focus penetration efforts where they are most needed, based on live data.

06 Dynamic runtime SBOMs:

Create dynamic Software Bills of Materials (SBOMs) to ensure you have an accurate, always-on view of your software inventory.

See the benefits of improved AppSec observability for yourself.

Schedule a demo

Contrast SECURITY

All rights reserved. ©2024 Contrast Security, Inc.

contrastsecurity.com