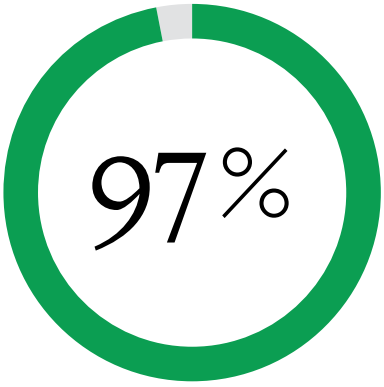
Contrast SECURITY

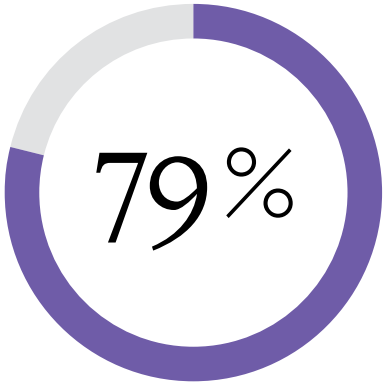
Illuminate Your Application Security

Unveiling Security Observability for Real-time Insights

In today's fast-paced, interconnected digital landscape, Application Security/application programming interface (API) security faces multiple challenges. While technological advancements have greatly expanded possibilities, they've also increased complexity and obscured visibility.



of firms grapple with visibility into their apps, leading to potential vulnerabilities.
State of Cloud-Native Security 2022



of organizations acknowledge an asset visibility gap, leading to 3× more incidents. Humans may soon be overwhelmed by the sheer volume, sophistication and difficulty of detecting cyberattacks.
Deloitte Insights

Modern AppSec environments are constantly evolving, creating a nebula of threats. Product development teams are left to deal with the shortcomings of traditional security tools. Given the increasingly hostile threat environment, it's crucial to bridge the existing disconnect between developers and security teams so they can get a more granular view to better understand risk and mitigation.

It's not merely about securing anymore — it's about achieving crystal-clear observability.

Introducing Security Observability

Security Observability approaches the problem differently. It aims to give your security and development teams deep, real-time insights into your application's architecture, behavior and risk. No more navigating blind. Observe real-time application interactions, understand their heartbeats and uncover hidden risks.

It's not just about detecting threats — it's about blocking attacks and addressing them proactively, ensuring your application's security remains uncompromised.

Runtime security isn't an afterthought with Security Observability; it's a core component. By delivering real-time visibility into the behavior of your applications and APIs while they're in operation, potential threats are detected and neutralized before they can cause significant damage.

- **Pen Testing Intelligence:** Provide real-time information most relevant to pen testers to allow them to target their efforts on a resource-by-resource level.
- **Threat Modeling Empowerment:** Discover how Security Observability enables threat modeling with precise, up-to-date information, ensuring your defenses are robust and adaptive.
- **Dynamic SBOMs:** Learn how you can create Software Bills of Materials (SBOMs) anywhere, anytime, incorporating real-time changes and ensuring you always have an accurate view of your software inventory.
- **Contextual Vulnerability Prioritization:** Understand how we empower your teams to prioritize vulnerabilities with more profound context, making your response proactive and effective.
- **Incident Response Efficiency:** See how Security Observability aids in responding to incidents rapidly and more efficiently, reducing potential damage.

Examples of data include:

- **Outbound Calls:** Detecting outbound calls to other API endpoints gives you an expanded view of your system interactions with internal and external services.
- **Database Connections:** Gain visibility into all your database connections, identifying potential threats before they become vulnerabilities.
- **File System Interactions:** Monitor file system interactions, ensuring expected system interactions at the machine level.
- **Type/Protocol of Endpoint:** Understand the nature and protocol of each endpoint in your system, providing a comprehensive view of your application network.