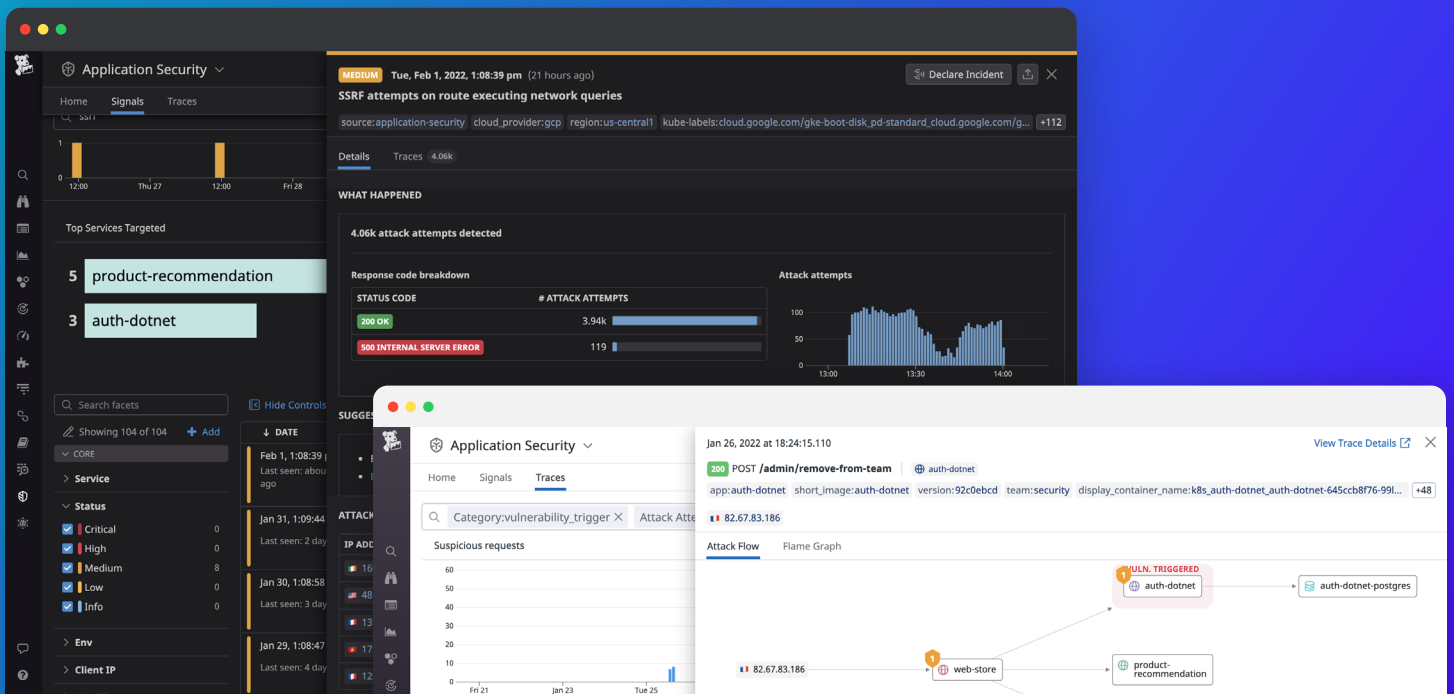
# Application Security BETA

Secure your web-applications and APIs, from the network to down to the code

DATADOG




## Introduction

Every company is increasingly a software company, but every company—large and small—struggles to secure their software. The status quo is expensive and complex: secure coding practices, code reviews, security testing that slow down development, periodic vulnerability scans and pentests, and protections at the network/edge. Those who have the resources to deploy this complex set of solutions still **struggle to scale** them and **keep up with engineering** — especially as software teams accelerate their release cycles, move to complex distributed systems and microservices. In the modern software era, unscalable and piecemeal approaches to application security are as sufficient as a screen door on a submarine.

Attackers will go down the easiest path, and applications are increasingly the fat, soft underbelly for security. **Insecure apps put customers data and company infrastructure at risk.**

## Problems with traditional Application Security solutions

Companies that have started their Application Security journey typically face a couple of challenges.

- **Not all vulnerabilities can be identified and fixed before code reaches production:** Application Security Testing solutions demand a lot of internal security resources to triage findings that are often false positives. Companies typically have to make trade-offs about where they roll them out or how frequently they run them, leading to a gap in coverage. And even when vulnerabilities are found, the fix is not always prioritized.
- **Targeted attacks bypass the perimeter monitoring layers:** Web-Application Firewalls are rarely tuned to adapt to the context of the application it's meant to protect. It's more often than not permissive and easy to bypass for anyone skilled. As a result, companies don't have visibility on attacks that actually matter & cannot take efficient actions to remediate threats targeting APIs and microservices.

## Secure your web-applications and APIs, from the network to down to the code

The shift from traditional monolithic architectures to microservices has enabled organizations to increase agility and scalability. However, the **growing complexity of these distributed applications introduces a whole array of code-level security risks and vulnerabilities** that traditional security solutions like intrusion detection systems and firewalls fail to catch.

Meanwhile, observability solutions brought DevOps high quality & quality insights about how distributed systems behave. **Datadog Application Security uniquely combines security and observability data** to provide teams with higher fidelity and more actionable security insights, unifying Developers, Security and Operations on a single platform. This helps teams **decrease the mean-time-to-detect and mean-time to respond to threats** reducing the likelihood of breaches.

Thanks to Datadog Application Security, you can now:

### GET ALERTED WHEN THREATS TARGET WEB-APP & API BUSINESS-LOGIC

- **Out-of-the-box detection of OWASP attacks** like Server-Side-Request Forgery (SSRF), SQL Injections, Cross-Site-Scripting (XSS) and more.
- Automated aggregation of attacks into Security Signals **when attention & action is required.**
- Notification in their own tools through hundreds of integrations.
- Criticality of Security Signals set thanks to the **runtime execution context** from the Distributed Traces.

### ASSESS HOW DEEP ATTACK GO AND REMEDIATE, FROM NETWORK TO CODE

- Identification of **attacks that trigger code-level vulnerabilities** (available for SQL Injections today and more soon).
- Deep **observability capabilities** in how applications and APIs reacted to attacks & full context of the distributed trace to understand the end-to-end **attack flow**.
- Pivot to errors, associated stack traces or even source code to **collaborate cross-functionally** and fix potential vulnerabilities.

### RECONSTRUCT THE ATTACK VECTOR ACROSS THE STACK WITH THE CLOUD SECURITY PLATFORM

Attackers now focus the weakest link across the full cloud stack: applications, workloads, infrastructure. Swiveling chairs across many security point solutions wastes precious time during investigation. Datadog Application Security is **fully integrated in the Datadog Cloud Security Platform** helping teams decrease their mean-time-to-detect threats.

## Get started in minutes with the Datadog Unified library


Datadog Application Security leverages the unified Datadog Library that is already deployed in any service leveraging Datadog APM. No additional component to deploy. See the documentation for additional information.


DATADOG