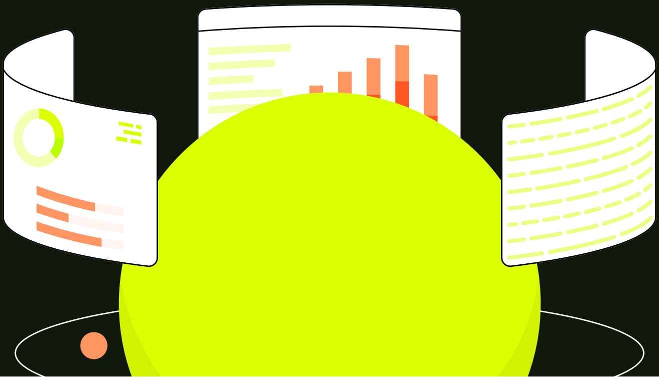
sweet.



Get Visibility into Application Risks and Threats

✓ Gain Visibility

- API Catalog
- SBOM
- Sensitive Data Classification
- “East-West” & “North-South” API Traffic Views

✓ Mitigate Risks

- DAST
- Open Source Security
- Attack Path Analysis

✓ Detect Threats

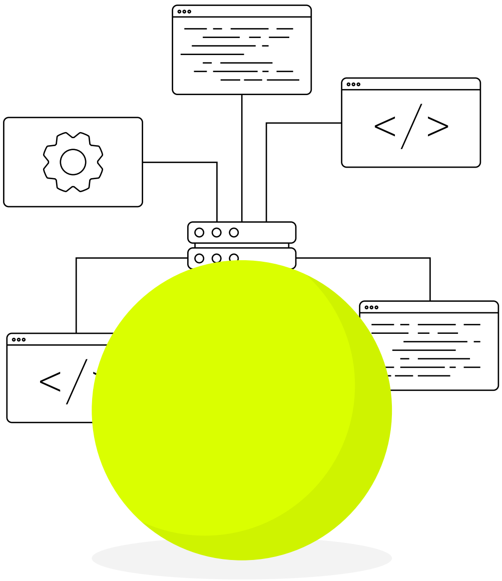
- Attack Attempts
- Supply Chain Security
- Root Cause Via Stack Trace
- Application Detection and Response (ADR)

Sweet gives AppSec teams continuous visibility into how applications behave, including what APIs are exposed, which vulnerabilities are exploitable, where sensitive data flows, and where attackers are actively probing. It’s runtime application security with built-in prioritization and response.

Get a Clear View of all Your APIs

Gain deep visibility into your APIs with organized views that simplify both troubleshooting and oversight.

- Organize APIs by individual endpoints to track request methods, error rates, and potential vulnerabilities
- View APIs as resources based on the services they expose
- Effortlessly shift between granular analysis and high-level monitoring
- Monitor East-West & North-South API traffic to understand how services communicate internally
- Map APIs to known components and dependencies via Software Bill of Materials (SBOM)



Is the workload exposed to untrusted input or L7 traffic?
Was the vulnerable function actually executed in the environment?
Does the service store secrets or process sensitive data?

Reduce Vulnerability Noise & Prioritize with Context

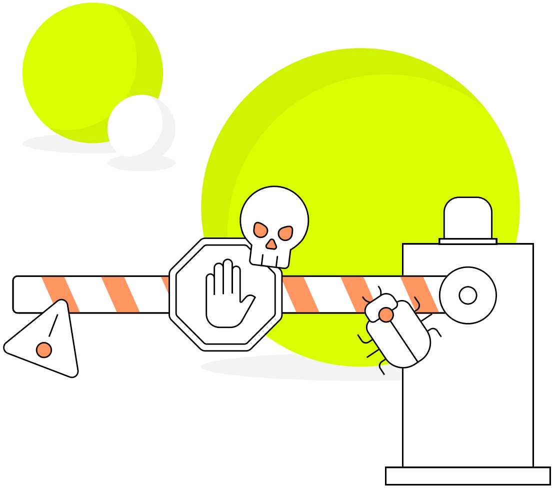
Not all vulnerabilities are equal. Sweet helps you prioritize with precision by taking into account runtime execution, exposure, contextual signals, and behavior type to calculate a dynamic AI-powered Sweet Score for every vulnerability.

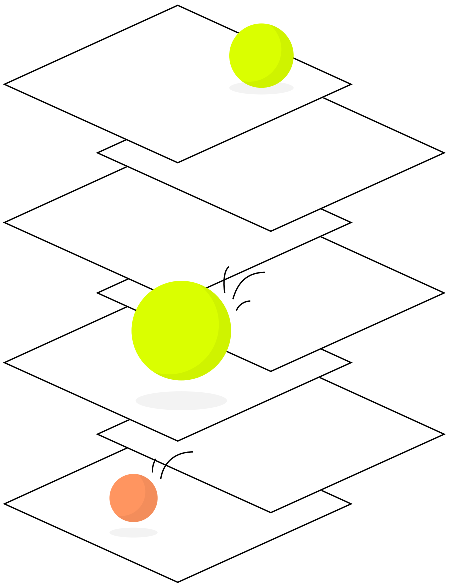
- Determine if a vulnerability is actually executed in your environment
- Assess the real exploitation preconditions and business-critical context
- Detect risky privilege escalations, public exposure, or exploitable code paths with precision
- Adjust scores intelligently for containerized apps, inbound traffic, and workload sensitivity

See the Attack Attempt Before the Breach

Most security programs focus on what happens after a breach. Sweet gives you the ability to stop attacks earlier by surfacing attempted intrusions—even the ones that didn't succeed.

- View all attack attempts across environments—successful or not
- Identify which services are being targeted, how, and by whom
- Filter by threat type (e.g., SQLi, XSS, SSRF) and status code
- Block suspicious IPs and refine defenses based on real-world reconnaissance
- Get enriched request context including full headers, payloads, OWASP/MITRE mapping, and historical timelines





Detect and Respond to Layer 7 Attacks in Real Time with ADR

See and stop application-layer (Layer 7) attacks as they happen. Sweet continuously monitors first- and third-party application behavior at runtime to detect anomalies, unauthorized activity, and signs of exploitation.

- Analyze application behavior at the package and function level
- Detect threats missed by static scans and log-based tools
- Automatically block malicious activity in real time
- Surface rich forensic context to guide investigation and response