sweet.

Sweet for CloudSec & DevSecOps

From misconfigurations to runtime reality. Get ahead of what's truly risky.

Runtime Context DevSecOps Can Trust

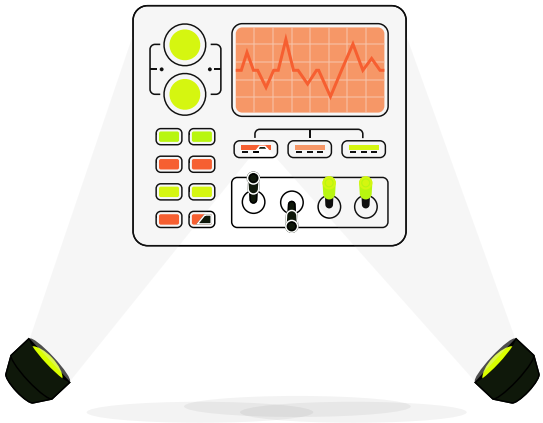
Break down siloes between security and development. Sweet unites both teams around shared runtime context, so when security flags a risk, it comes with the evidence developers need to act quickly. No false alarms. No blockers.

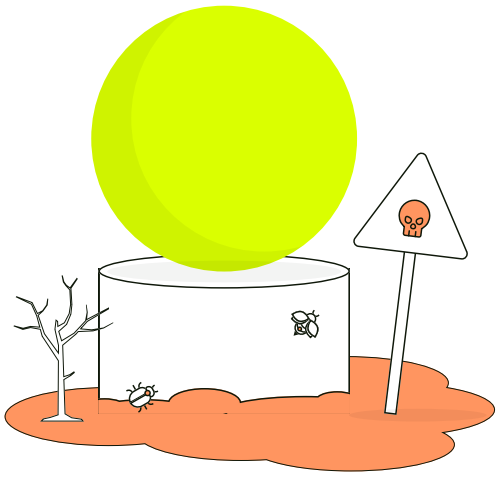
- **CSPM**
- **Toxic Combinations**
- **Attack Path Analysis**
- **Container & Kubernetes Security**
- **Identities Security**
- **Network Connections**
- **Topology & Asset Management**
- **Compliance Management**

Know Which Misconfigurations Are Dangerous

CSPM with runtime context, not just config snapshots.
With Sweet's real-time monitoring, you'll see:

- Which misconfigurations are exposed to the internet or have cross-account access
- When a misconfiguration occurred, with complete context on what role/identity caused the change
- Which roles or identities are used actively, not just over-permissioned
- Where vulnerabilities exist in running workloads (containers, EC2, serverless)
- Which workloads are both misconfigured and under active threat





Prevent Breaches by Surfacing Toxic Combinations Before They're Exploited

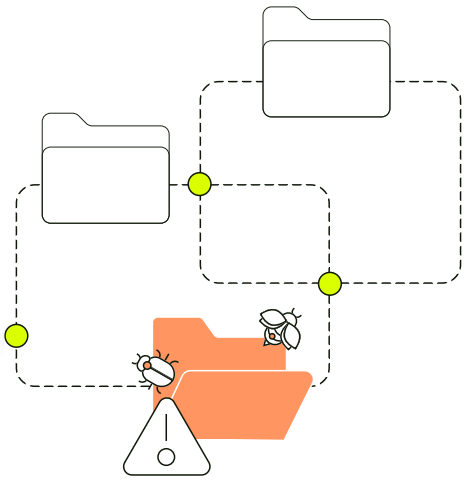
Real breaches don't come from one misstep; they come from the wrong things lining up. Sweet identifies toxic combinations that should never coexist, such as:

- A vulnerable container + exposed secret on disk
- A privileged IAM role + usage from unusual location or service
- Which roles or identities are used actively, not just over-permissioned
- An API receiving sensitive data + no authentication + cross-account usage
- A public-facing workload + CVE executed in runtime + outbound connection

Address Identity and Vulnerability Risks That Actually Matter

Get the context you need to focus on real risks, not theoretical CVEs, including:

- Vulnerabilities running in production and exposed to traffic
- Packages reachable via API endpoints or auth flaws
- Unusual role assumptions and identity chaining
- Shadow or inactive high-privilege accounts
- Public, cross-account, and lateral movement paths



Built for Complex Cloud Environments

Whether you're in one AWS account or managing dozens across orgs, Sweet supports:

Multi-account, multi-region visibility

Cross-account session tracing

Context-aware baselining (e.g., flag access outside business hours or regions)

Support for EC2, EKS, Fargate, and hybrid workloads.

AWS

Cross-account session tracing	EKS
Self managed Kubernetes	Any self managed Kubernetes
Virtual Machines	ECS2
Container Management Service	ECS
Serverless Compute for Containers	AWS Fargate

Private Cloud

Managed Kubernetes	Any K8S
Self managed Kubernetes	Any self managed Kubernetes
Virtual Machines	Any virtual machine (Linux based, see details below)

Azure

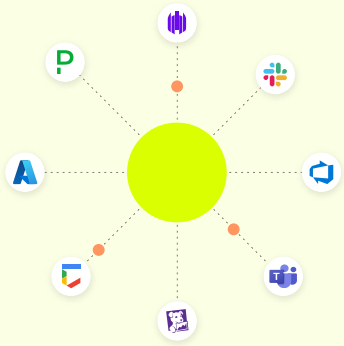
Managed Kubernetes	AKS
Self managed Kubernetes	Any self managed Kubernetes
Virtual Machines	Azure Virtual Machine

Google Cloud Platform

Managed Kubernetes	GKE
Self managed Kubernetes	Any self managed Kubernetes
Virtual Machines	Google Compute Engine

Integrations

Sweet offers SOC, IR, DevSecOps, and AppSec teams a wide array of integrations across SIEMs, SOARs, alerting and ticketing systems.



Detect threats in real time. Take action faster.