Runtime Powered CNAPP

Sweet is a runtime powered CNAPP that unifies insights from applications, workloads, and cloud infrastructure to surface key risks, enabling teams to detect incidents and resolve threats faster.

Trusted by Phoenix tripledot Fireblocks SafeBreach FIREBOLT hippo kaltura engageli AutoFi

5 → 1
No Tool Sprawl
Consolidated and unified security for infra, workload, and cloud-native apps

96% ↓
reduction in vulnerabilities to address
Complete focus on the most critical and urgent risks across the stack

80% ↓
reduction in DevSecOps costs
Operational efficiency across security and dev teams

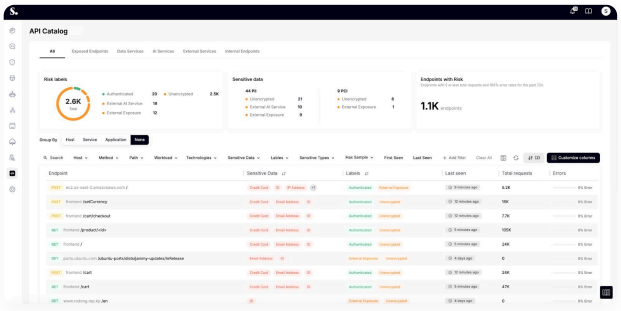
2 – 5 min
MTTR
Detect and respond to threats in minutes

Sweet Security

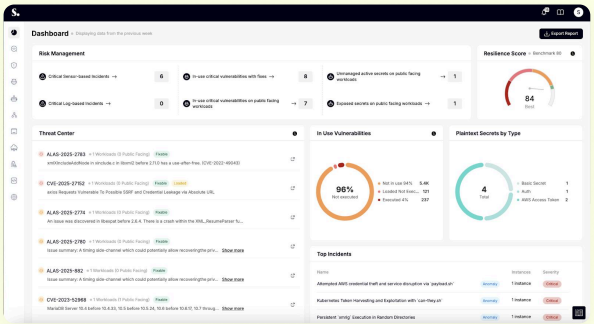
Threats to Remediate

Monitor Your Could Environment 24/7
Sweet monitors your cloud environment 24/7 through boots-on-the-ground eBPF sensors. These sensors collect telemetry and security data directly from the cloud infrastructure, workloads, containers, and serverless environments and require minimal CPU and RAM consumption. The sensor data is then correlated with real-time
cloud logs and layer 7 activity to provide deeper visibility and complete context.

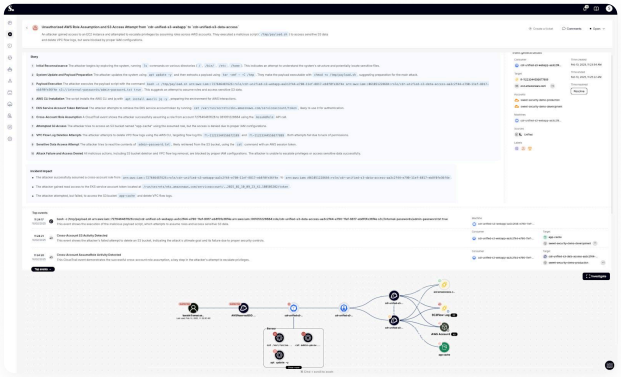
Manage and Protect Your Cloud-Native Applications
Sweet provides deep Layer 7 visibility into API traffic, enabling comprehensive application-layer threat protection. By analyzing API requests and responses, Sweet can detect common application-layer attacks such as SQL injection, cross-site scripting, and other exploits targeting APIs and microservices.



Incidents to Detect



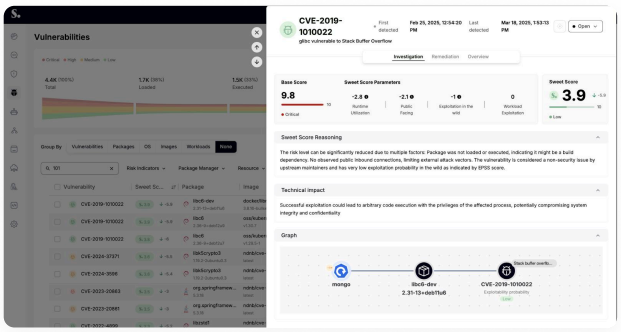
Detect & Respond to Incidents with a MTTR of 2-5 Minutes
Sweet's LLM-powered cloud detection engine identifies known TTPs and zero-day attacks across your cloud infrastructure, workloads, and applications. With AI-generated storylines of every incident and a timeline of every action taken by the attacker, investigate the incident with ease and determine if the incident is a false positive, what team or team member needs to resolve, and what's the urgency.



Threats to Remediate

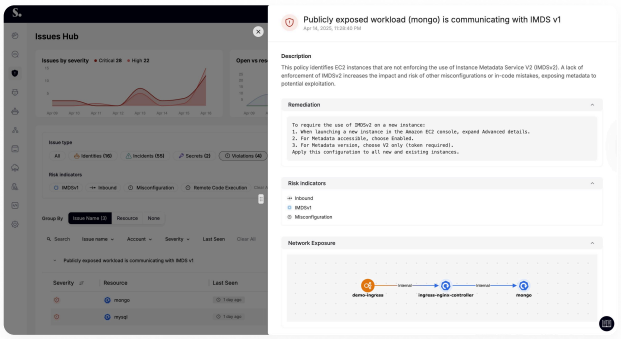
Prioritize Vulnerabilities According to Runtime Context

Sweet's vulnerability management combines runtime insights and LLM-powered analysis to assess and prioritize vulnerabilities based on the behavior of the vulnerability, in addition to the risk and impact it will have on the business.



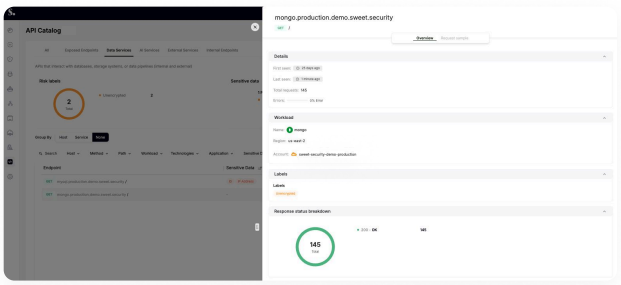
Detect and Prioritize Toxic Combinations

Sweet's Runtime CSPM & Issues Hub delivers real-time and immediate alerts on any misconfiguration or deviation from best practices, enabling proactive remediation and minimizing the risk of an attack due to the toxic combination of misconfigured resources.



Track Data in Motion to Prevent Exfiltration

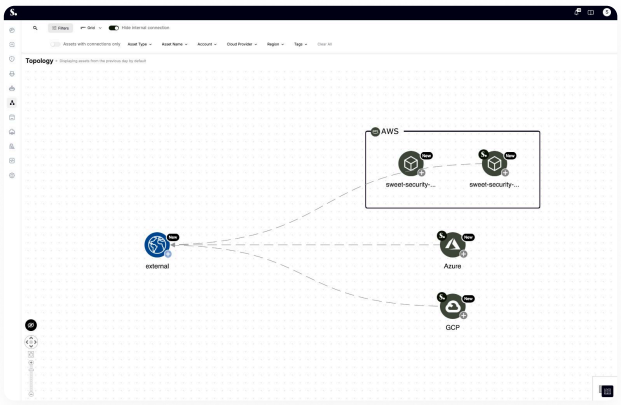
Sweet traces the origin and path of potentially malicious traffic. If an alert is triggered due to suspicious activity, Sweet maps out all connections made by the compromised service, identifying other services or external entities that may have been affected.



Incidents to Detect

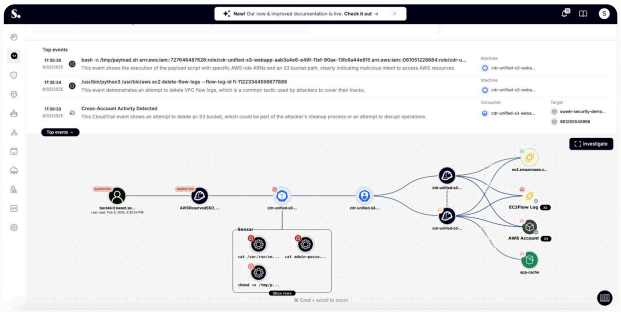
Map Your Cloud Environment

Sweet provides comprehensive, real-time visibility into your cloud environment. The platform maps runtime activities and dependencies, providing insight into how resources interact and depend on each other across your cloud infrastructure.



Identify Compromised or Mismanaged Identities & Secrets

Sweet's ITDR capability monitors and responds to identity-based threats across your cloud environment. By tracking user credentials, access patterns, and privilege misuse, Sweet helps identify potential insider threats or external attackers targeting your identities.



> "Sweet has fundamentally changed how we respond to security threats. The reduction in MTTD and MTTR by 90% means we can handle threats immediately, preventing any impact on our users. This is exactly what we need to stay ahead of attackers and keep our service running flawlessly."
>
> **Shai Sivan**
> CISO at Kaltura
>
> kaltura