sweet.

Sweet Security Runtime CNAPP - A Solution Brief

www.sweet.security

Sweet Simplifies Cloud Security

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.

Challenges

Lack Runtime Visibility

Traditional security tools focus on pre-deployment so runtime risks remain a blind spot.

Limited Context for Alerts

Sporadic alerts with no context lead to longer response times and more work for the team.

Hard to Prioritize Exploitation Risks

Attackers are leveraging vulnerabilities, excessive permissions, misconfigurations, shadow APIs, and more - what should be tackled first?

API Security & Visibility Gaps

Cloud-native applications rely heavily on APIs, which are often unmonitored for threats.

Sweet Solution

By adding a new "flavor" to traditional CNAPP frameworks, Sweet's CNAPP focuses on three key principles:

Runtime Monitoring

- Cloud environments need to be secured 24/7, not just periodically. Continuous runtime monitoring ensures that security teams can detect and respond to active threats in real time.

True Platform Unification

- Security should not be fragmented within a platform. Sweet Security correlates data across cloud, workloads, applications, networks, and user/machine identities to provide holistic, unified detection and response.

Application-Layered Security Focus

- The application layer is a prime target for attackers. Sweet Security integrates application visibility into the same framework as cloud visibility, ensuring that both security and development teams have the context they need to protect cloud-native applications.

With this approach, **Sweet Security has built a CNAPP that protects against modern cloud attacks**— one that doesn't just shut down attacks, but prevents them in real time with zero performance impact.

What Makes Sweet Different

5 → 1
No Tool Sprawl
Reduce tool count from 5>>1

300% ↑
SOC Efficiency
Increase SecOps team efficiency by 300%

80% ↓
Cloud Sec Costs
Drop security costs by 80%

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

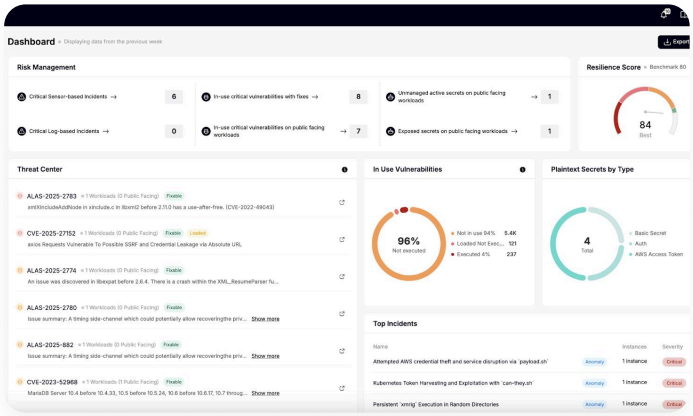
Key Capabilities

Features

- Full-Stack Runtime Monitoring
- Runtime CSPM
- Unified Detection and Response (CDR, CWPP, ADR in One)
- Cloud Visibility
- Vulnerability Management
- Identity & Secrets Security
- API Security
- Data Security

Monitor Your Could Environment 24/7

Sweet provides boots-on-the-ground eBPF sensors for real-time detection of runtime signals. 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 data to provide deeper visibility and complete context.

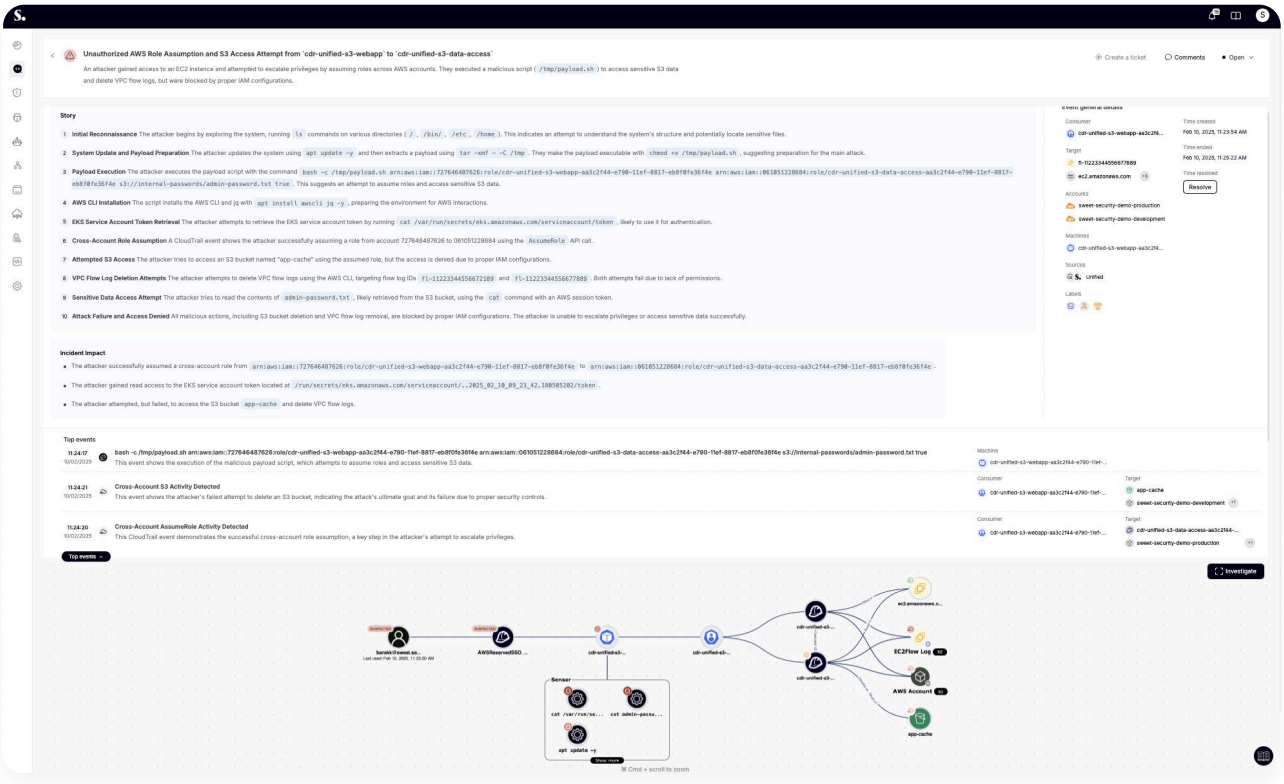


Detect & Respond to Threats with a MTTR of 2-5 Minutes

Sweet's LLM-driven detection and response combines Cloud Detection and Response (CDR), Cloud Workload Protection Platform (CWP), and Application Detection and Response (ADR) into one cohesive platform.
This means security teams can detect real-time threats in seconds as all the pieces of a lateral attack are available in a single pane of glass.

Key Highlights:

- **LLM-powered Detections and Investigations:** Sweet identifies known TTPs and zero-day attacks in a mere 30 seconds, leveraging LLMs to spot anomalies within cloud activity sessions. In addition, Sweet's LLM provides a comprehensive story of every incident and lists every action taken by the attacker. This story helps security analysts understand if the incident is a false positive, what team or team member needs to investigate, and what's the urgency of the incident.
- **Unified Attack Views:** Sweet's unified attack view correlates insights from across the cloud infrastructure, workloads, and applications, ensuring defenders have a complete picture to quickly identify, investigate, and mitigate threats.
- **AI Response Playbooks:** Respond to attacks with complete confidence with an AI playbook that adapts to the specific context of each incident.
- **Manual or Automated Responses:** Shut down attacks as they unfold by manually or automatically terminating malicious processes.

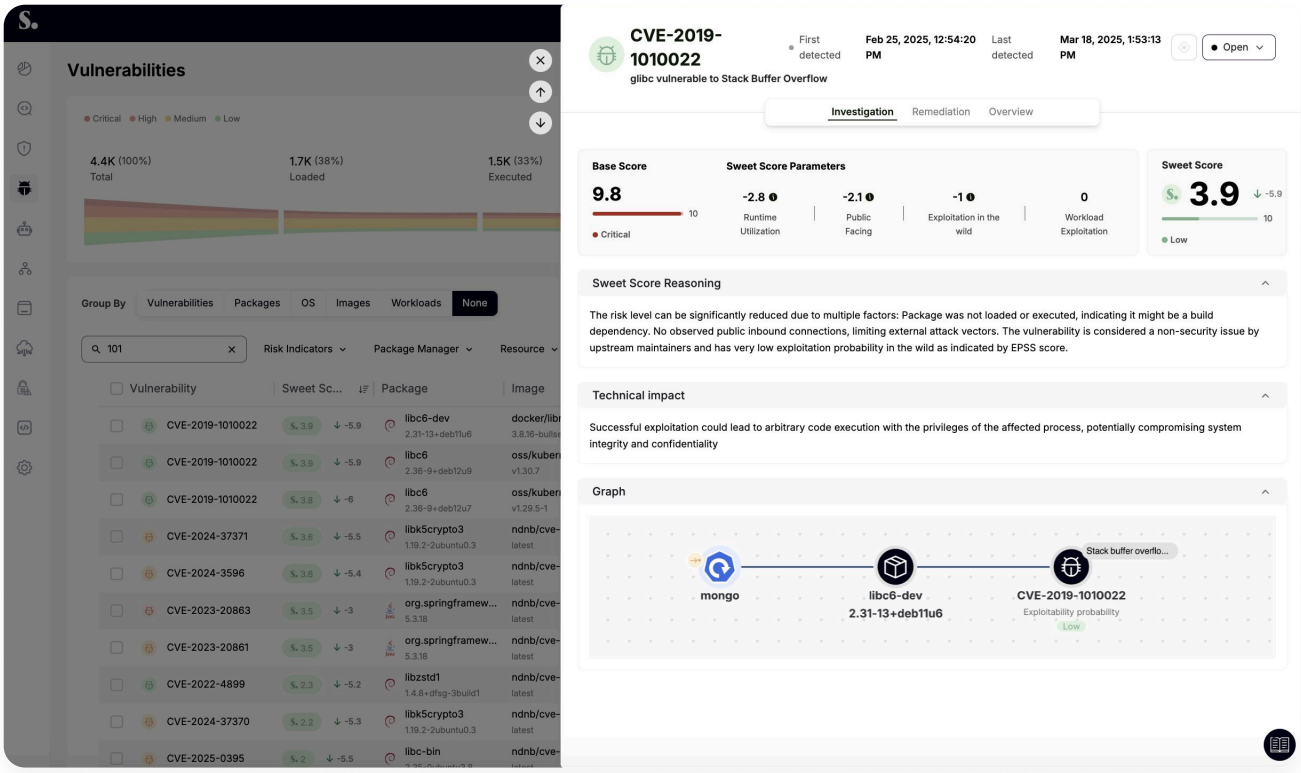


Reduce Risk and Prioritize CVEs According to Runtime Context

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.

Key Highlights:

- **CVE Prioritization Based on Runtime & LLM Analysis -** Evaluate vulnerabilities based on runtime factors, including whether the vulnerability is loaded into memory, actively executed, its exploitability potential, and whether it is public-facing.
- **Supply Chain Risk Management -** Identify and mitigate harmful packages associated with third-party dependencies before exploitation.
- **Pinpointing of Executed Vulnerable Functions -** Identifies vulnerable functions that are actually executed at runtime.
- **Software Bill of Materials (SBOM) -** A comprehensive inventory of packages and dependencies that includes both vulnerable and non-vulnerable components.
- **Image Scanning for Vulnerabilities -** Sweet's image ad-hoc scanning extends vulnerability management from the runtime phase to the registry phases so teams can identify vulnerabilities in an image before it enters the CI/CD pipeline, in addition to verifying that patched images are free of known vulnerabilities before pushing them to production.



Detect and Prioritize Toxic Combinations & Runtime Misconfigurations

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.

Key Highlights:

- **Posture Management:** Detect misconfigurations instantly, establish a behavioral baseline to differentiate normal activity from anomalies, and dynamically adapt your security posture in real-time.
- **Toxic Combination Assessment:** Get a unified view of toxic combinations by cross-correlating misconfigurations, exposed assets, and over-permissive access. Examples include identifying exposed APIs tied to vulnerable IAM roles, assessing lateral movement risks through East-West traffic analysis, and more.
- **Compliance Management:** Continuously check compliance against frameworks like HIPAA, GDPR, the CIS Kubernetes Benchmark, NIST, SOC 2, ISO 27001, and more, offering pre-built compliance rules for quick policy adherence, and issuing alerts for configuration drifts to enable timely corrections.

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. This enables teams to monitor critical interactions and maintain control over how data and workloads flow within their environment.

Key Highlights:

- **Topology Mapping:** Map hybrid and multi-cloud environments, offering both bird's-eye and worm's-eye views to understand runtime communications, dependencies, hierarchy, and structure.
- **Asset Inventory:** Sweet catalogs your environment in real-time by tracking clusters, networks, databases, compute types, and any other cloud resources the moment they spin up.
- **Network Insights:** Detect unauthorized ports, suspicious connections, and communication with malicious IPs and domains.

Manage and Protect Your 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. Our solution helps protect these critical communication channels, ensuring that they are secure against both known and unknown threats.

Identify Compromised or Mismanaged Identities and 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.

Key Highlights:

- **Identity Threat Detection and Response (ITDR):** Enables rapid detection of anomalies such as privilege escalation, credential abuse, and suspicious login patterns, allowing security teams to respond immediately and prevent further exploitation.
- **Runtime Insights:** Monitor identity usage, permissions, and privileged statuses to enhance security, including:
  - **Privilege Adjustments** for reducing over-permissioned identities based on actual usage patterns.
  - **Secret and Identity Management** for deleting unused or dormant secrets and identities to minimize attack surfaces.
  - **Non-Human Identity Management** for securing service accounts, tokens, and API keys to ensure safe operations.
  - **Human Identity Monitoring** for detecting unauthorized access attempts, unusual privilege escalations, and irregular usage patterns.

Track Data in Motion to Prevent Exfiltration

Sweet focuses on securing data in motion, ensuring that sensitive information is protected as it moves across your cloud environment. This allows security teams to pinpoint where data may be exposed to unauthorized access or manipulation. With Sweet, you can be confident that your data is protected, regardless of where it resides or how it moves within your cloud environment.

Supported Architectures & Deployment

Cloud Platforms	• **AWS:** Full support for services like EC2, Fargate, and ECS. • **Google Cloud:** Integration with Compute Engine and GKE. • **Azure:** Coverage for Azure Virtual Machines and AKS. • **Private Cloud:** Supports any private Kubernetes environment.
Orchestration and Containerization	• **Managed Kubernetes:** EKS, GKE, AKS. • **Self-Managed Kubernetes:** Any Kubernetes version >= 1.20. • **Container Management Services:** ECS, Azure Container Apps. • **Serverless Compute for Containers:** AWS Fargate
Virtual Machines	• **Virtual Machines:** Linux-based (amd64/arm64) with kernel >= 5.10.

Sweet's lightweight eBPF sensor can be deployed as a privileged pod, sidecar container, or Lambda layer, depending on your environment. It's optimized to trace only relevant system calls and runtime events, ensuring minimal impact on application performance. Additionally, updates are seamless, with automatic remote fetching of configurations and features to keep everything running smoothly.

Runtime Event Collection

Captures processes, file accesses, network traffic, and memory usage.

Baseline and Deviation Analysis

Establishes normal behavior and identifies anomalies.

MITRE Classification

Tags events using MITRE ATT&CK framework for standardized threat analysis.

IOC and TTP Detection

Continuously updated from external security vendors.

Trusted by

Phoenix tripledot Fireblocks SafeBreach FIREBOLT hippo kaltura engageli AutoFi