sweet.

Datasheet 2025

Cloud Native **Detection and Response**

Sweet Security provides the next generation of cloud protection with its supercharged Cloud Native Detection and Response platform that synchronizes runtime insights from cloud applications, infrastructure, and workloads - in a single pane of glass.

Trusted by

Phoenix · tripledot · Fireblocks · SafeBreach · FIREBOLT · hippo · kaltura

The Challenge in Detecting Cloud Attacks

Security teams are too slow to respond to cloud attacks because they lack real-time context and visibility. Add to this the challenges of tool sprawl, soaring cloud security costs, and overwhelming volumes of false positives, and it becomes clear that security teams are stretched thin. Many are forced to make hard decisions about which cloud breaches they can realistically defend against.

How We Do It

At Sweet Security, we address the complexities of cloud attack detection through our advanced, cloud-native architecture. Our unique multi-layered detection and response combines and cross-correlates data from:

- **Cloud Infrastructure:** We extract actionable insights from cloud logs and APIs, allowing for a comprehensive understanding of infrastructure events and changes.
- **Containers /Workloads:** Our eBPF sensor continuously monitors your containers and workloads, providing deep visibility into the processes and events happening in your environment.
- **Applications:** Utilizing network and Layer 7 analysis via our eBPF sensor, we scrutinize API calls and application behaviors, identifying vulnerabilities and malicious activities.

Sweet Security's Cloud Native Detection and Response

Functionality	Description
Supercharged Detection and Response	Detect real-time threats in seconds and drop MTTR to 5 minutes. Get a unified attack view with insights correlated across cloud infrastructure, workloads and applications.
Unified Cloud Visibility	Understand your environment with real-time insights into connections, assets, and key production elements. Sweet maps runtime activities and dependencies, helping you monitor critical interactions and maintain control across your cloud.
Vulnerability Management	Identify exploitable vulnerabilities across your environment and detect real-time exploitation attempts. Prioritize vulnerabilities based on execution status, criticality, and exposure.
Identity Threat Detection and Response	Detect, investigate, and respond to identity-based threats by monitoring credentials, access patterns, and privilege misuse across your environment.

Key Benefits

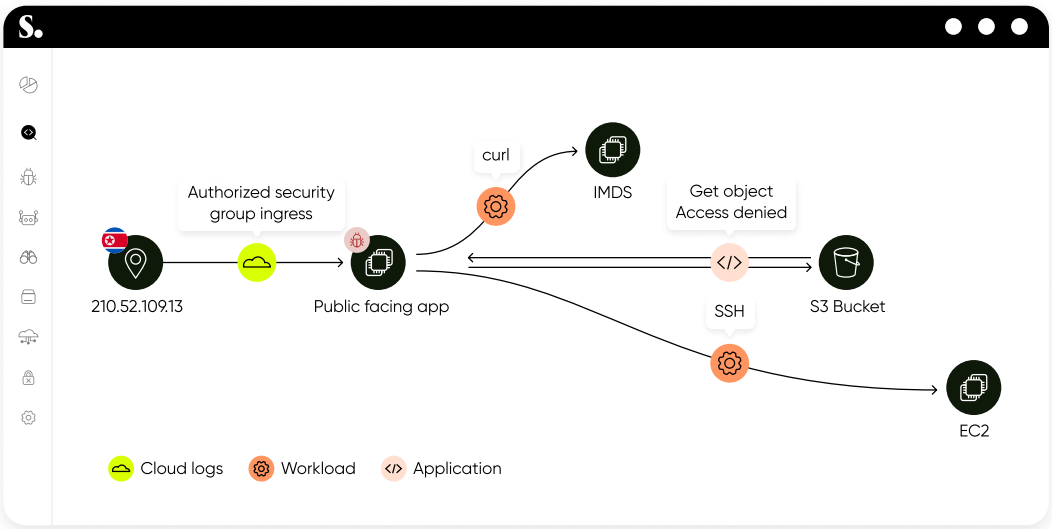
Reduce MTTR by 90%: Accelerate your mean time to respond (MTTR) through automated threat detection and rapid remediation processes, minimizing the impact of incidents.

Reduce tool sprawl: Simplify your security stack and enhance your detection capabilities by integrating multiple detection tools (ADR, CWPP, CDR, NDR + VM) into a single, cohesive solution.

Enhance SecOps Efficiency by 300%: Focus on what matters most and work with the right contributor to resolve incidents and vulnerabilities.

Reduce Costs by 80%: Lower operational costs by consolidating multiple security tools and reducing the need for extensive personnel resources.

Unified Cloud Detection & Response



This integrated approach provides:

- Multi-layered detection across infra, workloads, and apps - so you don't need to choose what attacks to be protected against.
- Agile response capabilities including automatically isolating compromised workloads, terminating processes, or simply sending an alert to the right remediator.
- Unparalleled visibility into the cloud environment, what it includes, and how it behaves.

Why Sweet

30+ out-of-the-box integrations with SIEM, SOAR, notification and ticketing systems, and more.

Non-intrusive eBPF sensor
Deep, real-time visibility without performance penalties or risks to your servers.

Rust for safety and efficiency
Low footprint, memory safety and unparalleled speed.

Built for modern cloud-native apps
Unlike lift-and-shift solutions that adapted existing capabilities without understanding the dynamic nature of the cloud.

About Sweet

Sweet Security is the leading provider of Cloud Native Detection and Response solutions. Powered by comprehensive threat intelligence and behavioral analytics, Sweet's unified platform correlates data from multiple layers—including application, workload, and cloud infrastructure—to deliver cloud native threat detection and response and complete visibility. By analyzing baseline behaviors across different entities, Sweet aims to reduce false positives and ensure faster and more accurate threat identification and remediation. Our identity-centric approach, combined with AI-powered capabilities, facilitates rapid detection and response, helping organizations hit a benchmark of 2-5 min MTTR for all incidents.