

# Cloud Runtime Protection with Sweet Security

## Product Highlight: Vulnerability Management

Today, security teams are frustrated with blindspots and noise caused by traditional cloud application security solutions. **"Shift left" approaches are not enough** to handle all the modifications made to applications daily and the high amount of uncontextualized static insights coming from traditional solutions.

Sweet's cloud runtime protection solution secures running applications in your cloud environment. By monitoring cloud and application runtime data, paired with advanced non-human identification and L7 capabilities, **Sweet enables proactive threat detection and response, vulnerability management, and non-human identity management.** Its comprehensive profiling capabilities empower teams to cut through the noise and deliver actionable recommendations on critical, real-time risks.



Sweet facilitates effective risk management, prioritizing vulnerabilities and non-human identities based on their business impact and security threat levels.

### With Sweet, you can:

#### 1 **Prioritize risks**

Evaluate vulnerabilities according to critical criteria—such as whether they are loaded into the applications memory, are executed, public-facing, exploitable, or fixable—so you can focus on threats that actually matter.

#### 2 **Pinpoint the root cause**

Find the root cause for each vulnerability (in as deep as the image layer) in order to tackle the root as soon as possible and fix multiple vulnerabilities at once.

#### 3 **Validate fixes**

Leverage ad-hoc scanning of images before they are deployed to ensure all vulnerabilities were addressed.

#### 4 **Adhere to regulations**

List out all your active vulnerabilities as an SBOM so you can adhere to compliance and regional regulations.



**Leverage runtime insights to manage vulnerabilities with confidence.**

- ✓ **Reduce CVEs by 94%**
- ✓ **Limit operational noise**
- ✓ **Automate remediation actions**

Sweet’s holistic approach to vulnerability management goes beyond traditional methods, seamlessly integrating visibility, risk management, and proactive hardening within a unified platform. By continuously monitoring runtime application behavior and correlating it with cloud infrastructure activities, we empower organizations to make real-time adjustments based on actual usage and emerging threats.

This enables security teams to enforce policies and application hardening best practices effectively, while also **reducing the overall vulnerability burden by 94%**. Our advanced technology not only protects against immediate risks but also establishes a comprehensive framework that allows teams to understand the intricate relationships between applications, infrastructure, and identities, ensuring robust protection against sophisticated attacks.

## About Sweet

Founded in 2022 by military veterans from the IDF’s intelligence unit, Sweet’s team comprises cyber security experts with over 20 years of experience and a breadth of knowledge within threat intelligence. Our all-in-one cloud runtime protection platform provides unparalleled security for running applications in your cloud environment.

By focusing on the relationships between application, infrastructure, compute, and identity components, Sweet provides a wide range of solutions to protect, detect, and respond to any and all attacks.