sweet.

Cloud Security Moves to Runtime.

Cloud security's biggest problem is that it was built as an extension of on-premises technologies. Security teams are accountable but not in charge of the cloud, piles of alerts are simply useless, and a new type of scale challenges arise: The average enterprise has 500,000 containers (50 times more than endpoints!).

After years of securing: code, configurations, posture, and whatnot, organizations **miss cloud attacks**. Cloud adopters have everything - aside from what's needed.

Sweet Security delivers security teams critical insights on active cloud risks so they can stop cloud attacks, **now**.

Cloud Security You Can't Ignore

Sweet delivers the first unified runtime security platform for the cloud.

It puts a stop to cloud attacks, helping security teams focus on business critical cloud risks.

Sweet utilizes a patent-pending, eBPF-based sensor that performs deep security profiling, establishing a unique baseline for normal and anomalous behaviors.

It looks into core elements to identify active cloud risks before, during, and after an attack has unfolded.

Key Features

Before

Runtime Vulnerability Management

Drop CVEs to address by 99% with runtime insights on loaded packages and more

Before

Runtime NHIs Management

Track non-human identities in transit and unveil unmanaged secrets

During

Runtime Detection

Automatically detect even zero-day attacks all across workloads. Get a full attack story.

After

Runtime Response

Cut investigation time from **days to minutes!** Attain full Assessment and enforce proactive remediation

Post Analysis

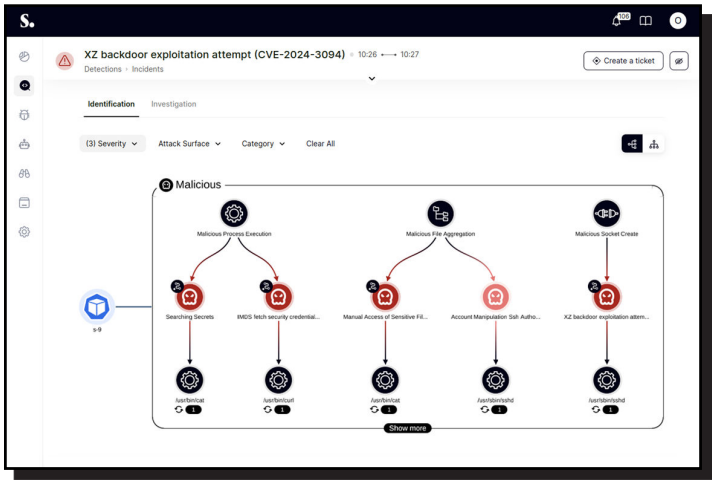
Expedite investigation on potential expansion with a detailed Impact Prediction analysis

sweet.

The Cloud Runtime Security Suite

Sweet leverages an eBPF-based sensor to attain cloud-native cluster visibility and stream key application data and business logic to its servers. It uses its innovative framework to profile workload behavior anomalies and contextualize it with traditional threat graphs and TTPs.

Sweet's security profiling paired with strong Layer 7 capabilities allow its solution to cut through cloud security's noise. Security teams can now focus on business-critical risks, based on its unique cloud footprint.



Key Benefits

Maximal Certainty

Never miss an incident. Sweet's behavioral baseline and unique L7 capabilities uncover every anomaly, providing real time proof of malicious activity.

Minimal Noise

Sweet reduces alert noise to nearly zero, delivering bulletproof findings on critical risks you cannot ignore.

Sweet and Lean

Sweet's eBPF-based sensor keeps installation under 5 minutes and CPU consumption very low - up to 0.5% from a single core.

About Us

Dror Kashti
CEO

Eyal Fisher
CPO

Orel Ben-Ishay
VP R&D

TLV

30 Employees

$40M A

Backed by:

evolution EQUITY PARTNERS

Munich RE
Munich Re Ventures

GLILOT CAPITAL PARTNERS

CYBERARK
The Identity Security Company

+20 World-Class Security Experts