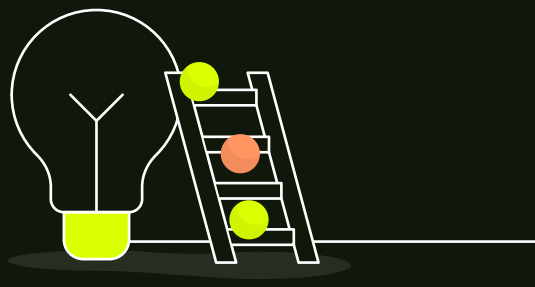
sweet.



Engageli Case Study

Scaling Secure Learning Without Compromising Performance

Company size	Vertical	Environments
50-60 employees	**EdTech**	**Hybrid**

Key need

- **Runtime protection**
- **Compliance evidence**
- **Vulnerability re-prioritization**

Cloud Security unlocked

- **ZERO impact on production scalability and cost**
- **97% reduction of time spent on audits (30 days to 1 day)**

About Engageli

Engageli is redefining the virtual classroom experience. Unlike traditional video conferencing tools that mimic meetings, Engageli creates an immersive learning environment that brings back the feeling of a real classroom. The platform supports a wide range of institutions across K–12, higher education, and corporate training, including large organizations. By leveraging AI, Engageli helps educators predict student success, measure teaching effectiveness, and offer administrators deep visibility into the learning journey.

The Challenge: Visibility, Compliance, and Zero Performance Tradeoffs

Engageli needed deeper visibility into their environment to detect and respond to real threats—not just scan for surface-level issues. They had been relying on agentless solutions that could inventory resources but lacked the context and depth to reveal true risk.

However, as a real-time education platform, Engageli must guarantee an uninterrupted experience for every student, in every session. With over **1 million hours of video streamed per week** and **350,000 active students,** even the slightest performance degradation can impact learning outcomes.

That made adopting real-time, deep observability tools a challenge. Any runtime protection had to be non-invasive, lightweight, and carefully designed to avoid remediation actions that might interfere with live workloads.

"No glitch can take place. We need the highest level of performance ALL the time because students are learning on here ALL the time."

Matan Yemini
VP of R&D at Engageli

Engageli's security needs were further complicated by its hybrid infrastructure running on both AWS and Oracle, and the frequent audits and compliance requirements specific to the education sector.

"My concern is compliance and making sure every quarter, we can meet those compliance and industry regulation requirements. Because of the education sector, it's frequent and a real pain."

To solve these challenges, Engageli needed a security solution that delivered real-time visibility and threat detection, but without putting performance at risk. They also wanted to simplify their operations by consolidating signals, reducing manual audit prep, and improving their overall cloud posture.
And Sweet Security checked all the boxes.

Sweet's Lean and Clean Sensor to the Rescue

Sweet's sensor was designed specifically for modern cloud-native environments. Built on eBPF, it runs efficiently at the kernel level to capture rich runtime data without slowing down applications or interrupting workloads. This gave Engageli the confidence to deploy real-time observability without sacrificing user experience.

"Sweet Security's lean sensor is perfectly aligned with our needs. It lets us stay fast and responsive while strengthening our security," said Matan Yemeni. "For us, having something lightweight was critical. Security couldn't come at the cost of performance, especially with students learning on the platform around the clock."

With runtime visibility from Sweet's Linux-based agent, Engageli now monitors both AWS and Oracle environments, including workloads that were previously underserved. Just as importantly, the team can detect issues in real time without triggering automated responses that might impact critical services.

"It's comfortable for me. I get the two things I need, visibility and response."

Compliance Audits: From 30 Days to 1 Day

Sweet has completely transformed how Engageli handles audits. "We were spending weeks justifying why certain CVEs were not addressed, even when those vulnerabilities posed no real risk at runtime."

Sweet provides real-time evidence to show why certain CVEs do not pose an active risk. For example, if a vulnerability is present but the associated code is never loaded or executed, Sweet generates runtime-backed proof that satisfies auditors. What once required combing through over 300 lines of vulnerabilities now takes minutes.

"Previously I needed 30 days to answer an audit. Now it takes me one day", states Matan.

The platform integrates directly with compliance automation tools like Vanta, allowing Engageli to centralize posture data and streamline quarterly reviews. Security and compliance are no longer a burden that slows the team down.

A Single Source of Truth for DevSecOps

Sweet's runtime agent delivers visibility, detects misconfigurations, API exposures, and workload risks in one centralized dashboard. Sweet also provided the team control. If an issue was related to images, configurations, or infrastructure, they could resolve it internally. Yet, when deeper action was required, Sweet helped them prioritize and assign ownership to the right member of R&D.

Vulnerability Management with Runtime Context

Sweet surfaces only the vulnerabilities that matter most. Instead of chasing every CVE, Engageli uses runtime insight to understand which vulnerabilities are actually exploitable. This is essential in a small company where security is not a dedicated role. Each developer takes on some responsibility for security.

> "Security posture in a small company is not an official job. So having the platform be that security guy for us is awesome."

Engageli ♥ Sweet

By combining deep runtime visibility, audit-ready evidence, and low operational overhead, Sweet Security empowers Engageli to meet compliance requirements and secure their environments without compromising on performance. With Sweet, Engageli no longer has to choose between security and user experience. They get both.