sweet.

Kaltura Secures Their CloudTV **with Sweet's Cloud Native Detection & Response**

kaltura

Company size	Vertical	Environments
500+ employees	**Media**	**Multi-cloud**

Key need

- **Precise threat detection**
- **Runtime protection**

Cloud Security unlocked

- **MTTD & MTTR reduced by 90%**
- **ZERO impact on production scalability and cost**

About Kaltura

Kaltura is a video technology company that offers cloud-based solutions for creating, managing, and distributing video content. Known for its flexibility and scalability, Kaltura helps organizations enhance engagement through customized video workflows and integrations.

Kaltura, a leading provider of video technology, operates a massive, multi-cloud infrastructure spanning AWS, Azure, and Google Cloud. Their CloudTV platform is used by millions of customers globally, providing seamless and high-quality video experiences for real-time streaming, content delivery, and interactive media services. The CloudTV environment is critical to Kaltura's business, with a 24/7 operational need to ensure minimal latency and zero disruption to users. With this high-stakes environment, securing CloudTV became a complex challenge that required real-time protections without compromising the performance or scalability that Kaltura's customers demand.

The Challenge: Balancing Runtime Security with Performance

Kaltura's team needed a security solution that could provide granular runtime visibility into their multi-cloud environment, detecting real-time threats that could span across the application, container/workload, and infrastructure layers. However, their primary challenge was ensuring this comprehensive security without introducing performance overhead. Given the sensitive nature of their CloudTV platform, traditional security solutions were not an option.

> As Shai Sivan, CISO at Kaltura, explained, "The very nature of our environment makes implementing a traditional runtime security solution extremely difficult. An agent-based solution was simply not an option for us, as any performance impact would directly affect our customers' experience. We needed a solution that wouldn't require security to come at the expense of performance."

So in order to boost the integrity of their CloudTV service, Kaltura set out to find a cloud security solution that could:

1. Detect sophisticated attacks in real time — enabling Kaltura to respond to potential threats before they escalate and affect customers.

2. Operate with minimal resource consumption — ensuring the solution would not disrupt the performance of their production environment.

The Solution: Sweet's Cloud Native Detection and Response

Sweet's Cloud Native Detection and Response platform was the perfect fit for Kaltura's needs. As the only solution on the market to integrate multiple forms of detection across application, workload, and cloud infrastructure layers, Sweet was able to provide Kaltura with a way to identify incidents before they escalated into a full-on breach.

In addition to its extensive detection capabilities, Sweet's solution leverages an extremely lean eBPF sensor—a small, resource-efficient module that runs with minimal impact on system performance. This sensor requires only 50 MB of RAM and 0.20% CPU per node, making it virtually invisible in Kaltura's environment.

Unlike traditional agent-based security solutions, Sweet's eBPF sensor operates invisibly while still providing the ability to monitor detailed, real-time activities within the environment. This includes tracking network connections, file system access, and system calls to detect any suspicious behavior or unauthorized activity without burdening the system with excessive resource consumption.

Shai Sivan commented on why Sweet was the ideal solution: "We knew we needed a solution that could provide deep visibility and protection, but without impacting our production environment. Sweet's eBPF-based approach was the game changer. It's so lean and efficient that we could implement it without worrying about performance degradation."

Red Team Testing: Real-World Attack Detection with Sweet

To validate the effectiveness of Sweet's platform, Kaltura's red team conducted a series of simulated attacks. These tests were designed to replicate zero-day, multi-layered attacks that would target vulnerabilities in their cloud environment.

Attack Simulation:

The red team started by exploiting a code injection vulnerability in a PHP page, uploading a malicious file through a web vulnerability. Once inside, they escalated privileges using a known kernel vulnerability (specifically, a policy kit vulnerability in older Linux systems). The team then used the vulnerability to perform further exploitation, including creating a cronjob to resist detection and maintain persistence.

How Sweet Detected the Attack:

Sweet detected the attack in real time, identifying not just the main attack vector, but also the sub-processes behind the attack. Specifically, Sweet pinpointed the use of the "dash" sub-process of PHP, which is a lesser-known technique used by attackers to execute commands in the environment. The ability to see these sub-processes provided Kaltura with the precise context they needed to stop the attack quickly and identify the vulnerability that had been exploited.

Key Insight:

Sweet didn't just detect the end result of the attack but also the methods used to execute it, which is a critical aspect of modern threat detection and intelligence. This deep, contextual visibility into both the attack and the processes behind it gave Kaltura a major advantage in understanding and mitigating the attack.

> As Shai Sivan explained: "What really impressed us was Sweet's ability to detect not just the attack itself but the sub-processes involved. In the attack we simulated, Sweet detected a dash process executing in the background —something most tools would have missed. That's the level of visibility and depth we were looking for."

Business Value: Reduced MTTD and MTTR by 90%

By implementing Sweet's Cloud Native Detection and Response platform, Kaltura achieved significant improvements in both Mean Time to Detection (MTTD) and Mean Time to Response (MTTR)—two key metrics in cloud security.

With Sweet's ability to detect sophisticated attacks in real time, Kaltura's security team was able to identify and respond 90% faster than with previous tools. This reduction in detection and response times ensures that Kaltura remains one step ahead of adversaries, minimizing the impact of any potential security breach and maintaining the flawless user experience their customers depend on.

> As Shai Sivan noted: "Sweet has fundamentally changed how we respond to security threats. The reduction in MTTD and MTTR by 90% means we can handle threats immediately, preventing any impact on our users. This is exactly what we need to stay ahead of attackers and keep our service running flawlessly."

Conclusion:

Why Sweet was the Perfect Solution for Kaltura

Kaltura's unique needs—granular and real-time security, minimal impact on performance, and scalability across a multi-cloud environment—were met perfectly by Sweet's Cloud Native Detection and Response platform. By using Sweet's lean eBPF sensor, Kaltura has achieved comprehensive protection for its CloudTV environment while maintaining the speed, scalability, and reliability that its customers want.

With Sweet, Kaltura has ensured that their cloud-native platform remains secure, high-performing, and ready to handle the evolving security challenges of the modern media landscape.