Kaltura Adds LightCyber to Advance Security and Protect Resources

Preventing Network Blindness

Highlights

Company: Kaltura

Industry: Video Technology

Location: New York

About the Customer

Headquartered in New York, Kaltura is the leading video technology provider. Its mission is to power any video experience. A recognized leader in the OTT TV (Over the Top TV), OVP (Online Video Platform), EdVP (Education Video Platform) and EVP (Enterprise Video Platform) markets, Kaltura has emerged as the fastest growing video platform, and as the one with the widest use-case and appeal. Kaltura is deployed globally in thousands of enterprises, media companies, service providers and educational institutions and engages hundreds of millions of viewers at home, in work, and at school. The company is committed to its core values of openness, flexibility, and collaboration, and is the initiator and backer of the world's leading open-source video-management project, which is home to more than 120,000 community members.

> **"Now it's very easy to understand what is going on inside the network, giving us the ability to detect malicious or just risky behaviors."**
>
> - Elad Avrahami, Chief Information Security Officer, Kaltura

The Need

The reality today is that motivated attackers can get into any network. Zero day attacks are becoming the norm, and there are always vulnerabilities with increasingly sophisticated spear phishing and social engineering. At the same time, in an age of BYOD or really bring-your-own-anything, employees have the power to do things on the network that may serve a valuable business purpose that also introduces significant security risks. Alternatively, in certain conditions, an employee or contractor with network privileges could become rogue and seek to steal or damage assets.

Most companies face the real possibility that attackers can gain access to valuable assets and steal or damage them without being detected until it is far too late. Traditional security is generally blind to the operational activities of an attacker inside a network, or so ineffective that any indication of an active attack is buried under hundreds or thousands of security alerts mostly dominated by false positives.

Why LightCyber Magna

Kaltura conducted a trial of the LightCyber Magna™ platform for Behavioral Attack Detection™. It had considered advanced threat solutions, such as FireEye, but understood that they were "still blind" to real attacker activities inside the network. Endpoint solutions could catch known threats but had difficulty with zero day attacks and could not see into the network to discern activities there. Log solutions provided some insight but suffered from excessive false positive alerts.

During the evaluation, the Kaltura team instantly began to see what was happening on their network in greater detail than ever before. Even during the typical soak period of the first few weeks when Magna learns the good behaviors for all users and devices, Kaltura gained insight. Recalls Avrahami, "Right away we could see the difference between an administrator and non-administrator. In fact, just the ability to know who are the administrators—something self-learned by Magna—put us in a much stronger position. Now it's very easy to understand what is going on inside the network, giving us the ability to detect malicious or just risky behaviors."

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP

Key Challenges

- Worried about zero-day attacks and how to prevent subsequent damage
- Understood that attackers can break into any network, and that now the challenge is how quickly can you find them?
- Wanted new level of visibility for what was going on in the network

Key Results

- Instantly saw what was going on in the network
- High accuracy with only 7-10 alerts per week
- Set-up was easy

The Results

The Power of Knowing

Network attacks might occur infrequently, but, unlike most enterprises and organizations today, Kaltura has the ability to know whether or not an active attack is in underway and to stop it quickly. “If something were going on inside, we would know it,” explains Avrahami.

Policy Violations

Magna detected the use of P2P file transfer within the organization, which was a violation of company policy. Employees had good intentions for using P2P but didn’t realize they were violating policy or creating a security risk. The security group was able to shut down the use of P2P and educate the employees involved.

Smarter Security

As a result of the visibility and insight provided by Magna, the security team has been able to set better security policies and web proxy controls, as well as help in knowing how to plan and evolve their security infrastructure. One decision involved whether to add other web gateway tools and how to prioritize their security investments.

Other Findings

Magna alerted about a large file upload to China that contained information about the company’s CEO. The team immediately investigated and verified that it was a legitimate activity involved with the launch of a new office. “Nonetheless, the visibility was great, and it is exactly what we would want to know,” said Avrahami. In addition, Magna routinely finds Trojans and viruses that were missed by perimeter security, and this is a great bonus in addition to identifying real attack activities.

About LightCyber

LightCyber is a leading provider of Active Breach Detection solutions that accurately detect active cyber attacks that have circumvented traditional threat prevention systems. The LightCyber Magna platform is the first security product to simultaneously profile both network traffic and endpoint state in order to accurately detect compromised user accounts and devices early in the attack lifecycle, and to enable security operators to remediate breaches and stop attacks before real damage is done. Founded in 2011 and led by world-class cyber security experts, the company’s products have been successfully deployed by top-tier customers around the world in the financial, legal, telecom, government, media and technology sectors.

> **“There are a lot of best practices in security, and it is hard to follow them all, especially when things are always changing, admits Avrahami. Visibility from Magna enables us to know what are the urgent issues that need immediate attention to reduce the attack surface or curtail malicious or risky activities. We can know immediately if there are strong indications of an attack, so we can protect our assets and keep our reputation unblemished.”**
>
> -Elad Avrahami, Chief Information Security Officer, Kaltura

LIGHTCYBER
5050 El Camino, Suite 226
Los Altos, CA 94022
Ph: (844) 560-7976
www.lightcyber.com

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP