Gigamon Utilizes Magna for Detection of Network Attacks and Security Events

Highlights

Company: Gigamon
Industry: Network & Security
Location: Silicon Valley

The Need

Gigamon has layers of well-configured world-class preventative security in place. Its conservative policies, training and procedures are designed to repel security threats and safeguard company intellectual property, customer and corporate data, infrastructure and employees. Still, the specter of a data breach looms heavily, as it does for most companies.

It's also important to be able to thwart a potential malicious act or unintentional compromise from employees or contractors. With the industry average dwell times of six or seven months, bad actors have the ability to stealthily go about their tasks without fear of being discovered until they have long completed their goals. The Gigamon IT team wants to know if an attack or risky behavior has occurred and then immediately respond to it.

Moving From Prevention to Detection

"Security used to be about preventing malware," said Marshall Wolf, senior director of IT, Gigamon. "Now it is all about admitting that every network could be breached. That means you have to able to detect an attacker on your network. It's more about visibility and figuring out exactly what's happening on the network, and this is precisely what LightCyber Magna provides to us."

> **"We need tools that can slap us across the face and tell us what's going on. Now we don't have to go looking for security events. LightCyber delivers those to us."**
>
> - Marshall Wolf
> Senior Director of IT
> Gigamon

Team Efficiency is Critical

Like other companies, one impediment Gigamon faced was having the ability to detect attacker activities, whether they might originate internally or externally. Another was the time and resource constraints of a small, general purpose IT team.

"A small team has to be a jack of all trades," said Wolf. "Every single person has to be a help desk analyst or available to change out a server, administer a VM, or focus on security. You are doing 10 things at once. We need tools that can slap us across the face and tell us what's going on. Now we don't have to go looking for security events. LightCyber delivers those to us."

Risky Business

"The ability to see what's going on around our network and tie it to endpoints is invaluable," said Wolf. "Many times it's not even malicious. People in a company can get very creative, and sometimes it will bring issues that could undermine our

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP

Key Challenges

- Find network attackers that have circumvented preventative security, including those that have compromised a user account or computing device.
- Offload much of the investigative work, increasing the efficiency of a small, general-purpose IT team.
- Produce a small number of highly relevant alerts that will not overwhelm the team with a flood of false positives.
- Support a best-in-class security infrastructure.

Key Results

- Complete visibility of all security events, including internal and external attacks as well as risky behavior.
- Fully automated, highly accurate alerts with complete contextual information enabling the security operations team to efficiently identify attacks and remediate quickly.
- Leverages Magna's intuitive dashboard as a centerpiece of the SOC operations.

About LightCyber

LightCyber is a leading provider of Behavioral Attack Detection solutions that provide accurate and efficient security visibility into attacks that have slipped through the cracks of traditional security controls. The LightCyber Magna™ platform is the first security product to integrated user, network and endpoint context to provide security visibility into a range of attack activity. 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..

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

security or slow down the network. We're trying to be transparent with these issues. We actually display the LightCyber dashboard in an open area across from a break room where employees can see it. It's become very popular. People hang out there to see what's been caught."

Truth or Malware

"For us, the primary function of LightCyber Magna™ is to detect an active attack," said Wolf. "We want to be able to know for certain whether an attacker is present or if there are risky practices that are impairing security. Magna also gives us a bonus we hadn't counted on. It's great at finding malware that you would expect to be caught at the firewall or endpoints. Malware seems to get through in just about everyone's network. Maybe it is previously unknown malware at the time it gets into the network. It could still be unknown when Magna discovers it. We didn't expect it to point out issues with specific endpoints, but it does. That's the beauty of not relying solely on signatures or technical artifacts of known bad."

Seeing is Believing

"The Magna user interface is not super glitzy, but we weren't looking for a Star Wars interface," said Wolf. "We were looking for something that picks out malicious behaviors. Magna tells us what's important and helps us to minimize the time it takes for us to keep the network secure and healthy. It keeps our eyes on the ball. It's the most intuitive user interface and the most productive."

Great Combination with GigaSECURE

The Magna platform supports Gigamon's GigaSECURE, the industry's leading security delivery platform that simply and intelligently delivers appropriate network traffic to security tools. Magna connects directly to a Gigamon GigaVUE appliance to receive a high-fidelity copy of relevant traffic streams from across the network infrastructure. "Magna plugged right into our appliance, and everything worked great," said Wolf.

> **"Magna tells us what's important and helps us to minimize the time it takes for us to keep the network secure and healthy."**
>
> - Marshall Wolf
> Senior Director of IT
> Gigamon

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP