Meeting the New Security Realities with Behavioral Attack Detection

Highlights

Company: PDX, Inc.

Industry: Healthcare Technology

Location: Ft. Worth, Texas

Partner: Secure Data Solutions

Secure Data played an instrumental role in the selection and deployment of the Magna platform following its model of "Simplify, Secure, Sustain."

About the Customer

PDX and its suite of products and services give pharmacies the ability to process prescriptions, manage reconciliation and adjudication, store and give authorized caregivers and patients access to healthcare records through traditional computer methods as well as mobile applications, provide medication therapy management, improve patient outcomes with clinical disease management, offer store-based mail order, and many more options that keep pharmacies competitive and compliant with industry needs and standards.

> **"LightCyber shows us what we really need to look at. The needle is an actionable thing, not just another piece of straw."**
>
> - John Woods, Vice President of Information Security, PDX

The nature of security has changed dramatically over the past several years. Daily headlines of major data breaches discovered far too late are the norm, and thousands of cases of the theft of intellectual property and other corporate secrets go unreported or announced. Attacks are targeted and carefully planned by criminal organizations in a way that can go undetected for months or even longer.

Proactive Security Roadmap

John Woods, Vice President of Information Security, and his team understood these changes and set a course to proactively evolve their security before anything could impair the business of PDX or tarnish the company's reputation and trust it has from its customers. They wanted visibility to be able to see the operational activities of a potential attacker to stop them early before theft or damage could occur.

"I strongly believe that pattern-based anti-virus is a thing of the past," said Woods. "It's like the rotary dial phone—it will still work, but not as well."

"You would be foolish to think that you are not going to be breached," said Woods. "You'd be foolish to think it's okay to be breached and you will just deal with it when it happens. There are a huge number of companies that go out of business because of a breach, or they are damaged beyond what they could easily repair."

"I was looking for something that would give me visibility based on anomalies and tell me when things were going wrong—when I had a potential breach," explains Woods. "I wanted to see where it was in the breach process so that I could react to it appropriately, based on what was happening."

"I needed to cover all the shortcomings of preventative security," said Woods.

Searching for the Right Product

Woods and his team considered 15 different products but eliminated most of them once they cut through generic terms and marketing claims for detection or behavioral analytics. They ended up evaluating four products in their network, "dropping them in to see what they could find."

One solution lacked sufficient network visibility and any endpoint visibility at all; it really just offered a user perspective which was not enough to see malicious behavior—such as an attacker at work—on the network. Another seemed to have good network coverage, but no endpoint perspective. It had a "slick, sci-fi" looking user interface but was complex and cumbersome while not clearly showing attacker activity.

The clear choice was the LightCyber Magna Behavioral Attack Detection platform. Magna caught malicious activity not seen by other solutions, including a keylogger in operation.

In fact, the team was "disgusted" with the amount of malicious software that was invisible to the existing security tools. "I was horribly upset at my existing vendors for not finding so many bad actors that penetrated the network." Only Magna found these.

After a "soak time" of a few weeks profiling all users and devices on the network, Magna produced the fewest number of alerts with the highest level of accuracy and actionability.

LIGHTCYBER
CLOSING THE BREACH DETECTION GAP

> **That's what LightCyber does–it catches the mole or spy at work.**

Key Challenges

- Needed to protect privacy and security of patient data
- Wanted increased visibility so they could quickly pinpoint and stop potential breaches
- Needed to cover the shortcomings of preventative security systems

Key Results

- Magna caught malicious activity not seen by other security solutions, with the fewest number of alerts with a high level of accuracy and efficiency
- Gave them the confidence to know with a high level of certainty that attacks were not successful
- Lowered security costs by freeing up resources and enabling fast responses

> **With Magna the alert is real.**

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.

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

The Power of Assurance

One of the most important functions of Magna is to determine whether there might be an attacker at work on the network. One time, when the company was under a heavy load of intrusion attempts, Woods turned to one of the security professionals on his team and asked if he was sure that one of the attempts wasn't successful and an attacker got in. The analyst said that before having LightCyber Magna, it would be impossible to answer that question. Now, they had the confidence of knowing with a high level of certainty.

"One of my primary jobs is to keep the company out of newspaper headlines in a negative light," said Woods. LightCyber Magna "gives me a lot of power to accomplish my mission." If an attacker possibly circumvented preventative security, Magna can find them through their operational activity.

Protecting Health Care Data

With the marked increase in data breaches among health care organizations and the recognized value of patient data, the PDX team wanted to be aggressive in the way they detect and respond to potential threats to prevent any potential of a network attack leading to a breach. Maintaining customer and patient privacy and security is paramount, particularly as PDX runs groundbreaking services such as the RX.com Electronic Pharmacy Record (EPR), a real-time information service that provides access to almost two billion prescription records of nearly 94 million patients. EPR helps pharmacies offer better, more integrated healthcare though real-time, chain-wide Drug Utilization Reviews (DUR) and the exchange of demographic, prescription, third party, and clinical data across all pharmacies within the chain. Intra-chain EPR is also available to pharmacies that want to participate in the sharing of clinical data between chains. The service provides compliance with the applicable Health Information Technology mandates legislated by the HITECH provisions of the American Recovery and Reinvestment Act (ARRA) of 2009.

Lower Cost and Efficiency; Real Visibility

Cost and team efficiency have significant impact on the overall security effectiveness an organization can achieve. "Cost is not just the price of a product or service," reflects Woods. "Cost encompasses what is required to run the technology and get work done. If I have to look across 15 tools to see what's going on and the extent of the issue, that is going to be costly and slow. Having Magna allows me to use a single tool to see what's going on. If something happens, I see it in one place and can respond to it quickly."

"It's expensive and inefficient to have to dig through a massive mound of data to find the proverbial needle in the haystack," said Woods. "Magna provides automated investigation that frees up our resources and enables a fast response. We don't have to do all the research we used to do to find out what and where the problem is and how bad it might be. I get that automatically."

"With Magna the alert is real," said Woods. "In security you get a lot of alert blindness—you get so much data coming at you it's difficult to see which are real issues. Other solutions provide a lot of generalized pings that are really not actionable. LightCyber shows us what we really need to look at. The needle is an actionable thing, not just another piece of straw."

Invaluable Support from Secure Data Solutions

The PDX team received invaluable support from Secure Data Solutions in making their selection and implementation of LightCyber Magna. Secure Data helped determine what was most important and how that fit with the vision and roadmap Woods had established. "The starting issue is how quickly can you see an important security event," said Rob Anderson, partner and chief operating officer, Secure Data Solutions, Inc. "You need to be able to detect, contain, report and remediate a threat wiht speed and precision." Woods felt that the Secure Data professionals were a part of his own team.

Castle Walls and Moats are Outdated

Traditional security tries to be preventative and focused on keeping attackers out of the network. Woods knows that this approach can no longer be counted on to be completely effective.

"The walls and moat of the castle is like the firewall and IPS," says Woods. "The guards on the walls are like anti-virus and endpoint security. But the trouble with this model is that you can't detect the spy or mole who is now inside the castle and is about to stab the king and steal the crown. That's what LightCyber does—it catches the mole or spy at work."

LIGHTCYBER