Wood County Hospital Gets Proactive on Security Threats

RAPID IDENTIFICATION AND RESPONSE TO RANSOMWARE ATTACK

REDUCED ALERT FATIGUE WITH MACHINE LEARNING

GREATER VALUE AT LESS THAN HALF THE PRICE OF COMPETING SOLUTIONS

EXECUTIVE SUMMARY In order to strengthen their cybersecurity stance and get ahead of unknown threats, Wood County Hospital added real-time network traffic analytics from ExtraHop to their security infrastructure. Not only did they immediately detect and stop a ransomware attempt using real-time visibility, but the security team can now detect and remediate threats faster, protecting patient and hospital data.

THE BEGINNING

Wood County Hospital has served the patients of Wood County, Ohio, since 1951. Over the years, its operation has expanded to include the main hospital, off-site medical offices, and eight clinics supported by over 700 clinical, administrative, and IT staff. The hospital is committed to providing the highest quality care and patient experience.

For the IT team at Wood County, this means delivering consistent application and infrastructure performance. It also means ensuring that these systems, as well as patient data, are protected from increasingly sophisticated and rapidly evolving threats, including ransomware.

For CIO Joanne White, security is a top priority. The hospital already had a sophisticated security framework in place, including IDS, IPS, firewalls, and SIEM. While these tools helped protect the perimeter and alerted on potential threats, alert fatigue, coupled with lack of visibility into threats inside the network, left Wood County with a crucial gap.

THE TRANSFORMATION

Seeking to gain critical visibility and improve the signal-to-noise ratio regarding potential threats, White began evaluating network traffic analysis (NTA) technologies, which combine rule-based detection, machine learning, and other advanced analytics to detect and alert on suspicious activities on the network.

Apples to Apples

After considering several options, White decided to evaluate ExtraHop and another NTA vendor. ExtraHop, recommended by several of White's peers at the College of Healthcare Information Management Executives (CHIME), supported many healthcare industry-specific applications and protocols out of the box.

The alternate solution came with a much-hyped user interface and machine-learning claims but was relatively unknown among White's peers. One of the few healthcare organizations to have used it decided to shut the solution down after a year due to escalating costs and complexity.

Unexpected Connections

As the evaluation kicked off, one clear difference emerged: ExtraHop surfaced concrete insight via dashboards and analytics right out of the box without requiring any customization.

Case in point, ExtraHop alerted White to a device that was unexpectedly communicating with over 100 workstations using an unauthorized Universal Plug-and-Play (UPnP) service. Known as a malware attack vector for DDoS and bypassing firewalls, UPnP had been specifically disabled – or so they thought. After seeing this, White was able to take action and quickly quarantine the host.

While the other solution could provide some information about which machines the workstation was communicating with, it didn't delineate the protocols and devices making those communications.

THE BENEFITS

HALF THE PRICE, DOUBLE THE VALUE

The big shock came when White compared the final pricing quotes from both vendors. ExtraHop, a solution that was broadly applicable to the entire IT team, offering visibility into application and infrastructure performance, was less than half the cost of the competing NTA solution. By that time, White had also realized that the level of customization required for the competing solution would have necessitated bringing in a full-time specialist –at a cost of over $70,000 per year.

NEUTRALIZING RANSOMWARE

With ExtraHop deployed, it didn't take long for White and her team to start reaping the benefits. Within days, a hospital employee reported seeing a message that looked like ransomware. Sure enough, ExtraHop had already started alerting on the threat – a new strain of ransomware known as CryptFlle2. With the information ExtraHop provided, the team was able to quickly identify and quarantine the infected machine, neutralizing the threat before it could impact Wood County's operations.

> "Without ExtraHop, the investigation would have taken days or weeks, exposing the hospital to potentially catastrophic risk. Even the FBI was impressed when they found out how quickly we identified and contained the threat!

JOANNE WHITE, CIO
WOOD COUNTY HOSPITAL

Staying Ahead of the Security Experts

Like many organizations, Wood County Hospital takes a hybrid approach to security, leveraging both internally-managed systems as well as a managed security service provider (MSSP) to provide additional layers of detection and prevention.

Two weeks after Wood County detected and thwarted the ransomware attack with ExtraHop, they got a call from their MSSP notifying them that ransomware was detected on one of their machines.

"We were thinking to ourselves, 'not again!' Then we looked at the data," says White. "As it turned out, the ransomware that the MSSP alerted us to was the very same thing we'd uncovered and resolved with ExtraHop two weeks prior. It took them that long to detect the issue. If we'd relied on them for ransomware prevention, we'd be in a very different position right now."

Moreover, the information provided by the MSSP lacked the detail and context required to remediate the situation. Without ExtraHop, the Wood County team would have spent days or even weeks sorting through log files to achieve the same outcome.

Find more ExtraHop customer stories at

WWW.EXTRAHOP.COM/CUSTOMERS/STORIES

ExtraHop