observable networks

Observable Networks is now a part of Cisco.

Case Study

Regional Healthcare Provider Improves Security Efforts with Observable Networks

"Observable's alerts give us a very specific, targeted approach for dealing with potential threats. This is so valuable because the alerts allow us to make better use of our staff and resources to address specific issues."

-Director,
Information Services,
Regional Healthcare Provider

ABOUT THE ORGANIZATION

This prominent regional healthcare provider is consistently recognized for clinical excellence and strong patient satisfaction scores. The 500-bed, not-for-profit hospital offers a full range of inpatient and outpatient care from one hospital plus a network of more than 20 offsite locations.

CHALLENGES

- Protecting patient records and other sensitive healthcare data
- Identifying potential issues quickly – without time-consuming efforts required to pore through extensive audit logs
- Complying with HIPAA and other security regulations

SOLUTION

Dynamic Endpoint Modeling

BENEFITS

- Improved visibility into the entire network of endpoint devices to acutely understand their normal behaviors
- Gained real-time, actionable alerts to potential indicators of compromise and hostile changes in endpoint behavior
- Improved compliance with HIPAA and other regulations with dynamic modeling and behavioral history
- Reduced the time associated with monitoring security issues, so staff could focus on proactive security measures

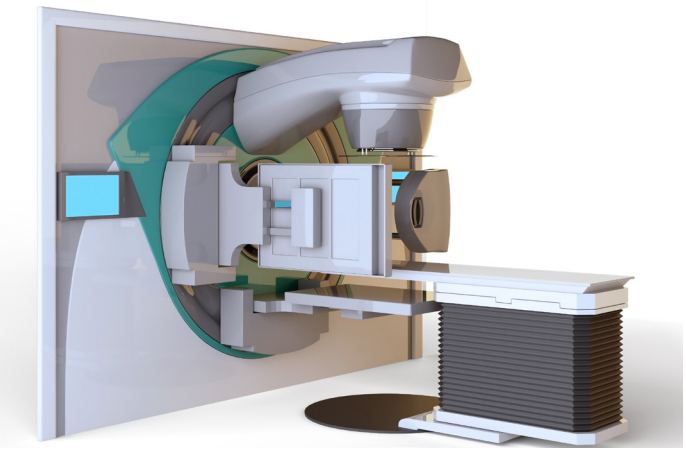
Conventional security methods fall short

While IT security is always at the top of any organization's priority list, protecting data is especially critical in healthcare. Failure is simply not an option: Hospitals and healthcare organizations must safeguard patient records and other sensitive information. If they don't, they risk significant penalties and fines from non-compliance as well as the loss of their reputations.

This regional healthcare provider faces all these same challenges, yet it must continue to protect its network at an affordable cost and with limited headcount. Additionally, its overall security approach must address emerging trends such as increasing levels of encryption, bring your own device (BYOD), and IT and medical device proliferation, which includes many specialized medical endpoint devices, such as cardiac, radiography, mammography, and point-of-care technologies.

To add to the challenge, software agents or other security technologies are limited on many of these endpoints as mandated by FDA regulations. As a result, it is difficult to monitor and protect these devices, a fact that presents significant challenges to traditional network security methods – and can potentially expose the organization to additional risk.

Additionally, conventional security programs attempt to align with security and compliance initiatives as part of larger annual audits. Once a year, independent auditors visit the hospital, review log files, examine configurations, run tests, and attempt to assess overall vulnerability. Yet such a "rearview" approach can't identify potential issues in enough time to take appropriate action – before it's too late.



"The biggest benefit of the Observable solution is that it gives us focused, actionable alerts so we can act immediately."

-Director,
Information Services,
Regional Healthcare Provider

Implementing a more effective solution

After reviewing many competitive solutions, this healthcare organization selected Observable Networks and its Dynamic Endpoint Modeling solution. Dynamic Endpoint Modeling monitors all of its endpoint devices, including FDA-regulated systems. More, the solution learns and continuously analyzes each device's "normal" behavior, so if it ever acts abnormally, IT staff will be alerted quickly to the potential source of compromise.

"Dynamic Endpoint Modeling gives us real-time, actionable alerts," says the director of information services. "This lets our staff quickly understand when a device is acting outside its normal behavior without spending a lot of time reviewing log files or other fragmented reporting tools."

For example, the Observable solution helps the organization model the activities of its vendor community so the IT team can understand normal vendor activities and quickly highlight any abnormalities, whether they are related to vendor access, changes in device behavior, or other potential indicators of compromise.

"Dynamic Endpoint Modeling gives us visibility into our devices, but it also helps us monitor the behavior and activities of all of our vendors," explains the director of information services. "Since this has been a point of entry for many organizations breaches in the past, this is a significant advantage."

Improved security and compliance

In healthcare, complying with industry regulations is a significant effort and one that affects security. For example, HIPAA and Meaningful Use guidelines require healthcare providers to demonstrate how they use technology to create secure environments. Additionally, healthcare organizations have to document all aspects of their security programs to comply with specific regulations such as the HIPAA Omnibus Act.

For this healthcare organization, achieving compliance could be a challenge, especially considering that it has so many regulated medical endpoints as well as employee-owned devices on the network. "We really don't have the ability to update these devices with traditional security methods, such as antivirus or other agent software technologies," says the director of IT services.

All of this has changed with Dynamic Endpoint Modeling. Now, the organization has complete visibility of its environment including encrypted networks, which is a significant advantage over other tools that simply can't provide insight into encrypted network activity.

"All device behavior is modeled, continuously analyzed, and reported along with alerts or examples of abnormal behavior, including where encrypted traffic is present," explains the organization's director of information services. "This is a significant improvement over previous processes where we had to look back, gather log files from various systems, and attempt to piece all of the data together. With Dynamic Endpoint Modeling, device behavioral history, incident history, and any example of malicious activity are all readily available. It's a continuous learning process. We are finding opportunities in real time, investigating, and creating system-wide improvements much more frequently."

Complete visibility. Complete control.

The organization is pleased with the results Dynamic Endpoint Modeling has delivered. "It's similar to the way individuals now manage their own health and wellness as opposed to relying on an annual check-up," says the director of information services.

"The Observable solution helps us continuously monitor our network and quickly tell the difference between normal device behavior and potentially more serious behavioral abnormalities. Before we implemented Dynamic Endpoint Modeling, it was a challenge to uncover or identify potential security concerns, especially identifying these proactively. But now we believe we have the tools that we can leverage to create a much more secure environment for our organizational and most importantly, our patients' data."

observable networks

Observable Networks is now a part of Cisco.

Observable Networks is a privately held company headquartered in St. Louis, MO.

For more information or to start a free trial visit our website at **www.observable.net.**