Healthcare Organization Deploys Powerful Adaptive Detection Fabric to Stop Threats and Protect Patient Data

The Customer

This healthcare organization is a nationally top-ranked hospital and is internationally recognized in several fields of research. It has an extensive medical staff of over 250 healthcare providers.

The Challenge

Malware attacks had become a sizable problem. The hospital experienced several outbreaks across the entire network and noticed substantial command and control traffic. The attacks progressed beyond endpoints and servers to include MDM Android and iPhones as well. Their existing solution was not able to secure the entire network.

The hospital IT security team knew they needed greater visibility into the malware and the attack vectors before a breach compromised the hospital and, perhaps, cost someone their life. The customer decided to evaluate Cyphort's Adaptive Detection Fabric (ADF) specifically to detect and contain advanced threats that bypass their first line of defense.

Solution Requirements

To defend the hospital and still allow the ease and efficiency of doing business across a large healthcare community, the hospital IT security team specifically required visibility and rapid detection across their entire network including Mac OSX machines. The key requirements included:

- **Rapid detection of advanced malware and zero-day attacks** – Detection of malware needed to be fast with immediate notification of zero-day threats. They wanted North/South visibility but also visibility into East/West lateral spread as well as to see incidents and infections when they happened, how they happened and what vectors they took.
- **Identification of the risk** – With the vast amount of threat activities, from adware to advanced persistent threats, and the extended network of endpoints, the team needed a precise understanding of the real level of risk they faced. Cyphort's SmartCore™ software contained advanced threat detection and mitigation features that determined which users were impacted by threats and their severity, giving the hospital the much-needed verification and actionable intelligence to remediate threats quickly.
- **Rapid integration with existing infrastructure** – Integration with existing enforcement infrastructure, e.g. firewalls, secure Web gateways and intrusion prevention systems, was key to the cost-effectiveness, and the speed of implementation and threat mitigation the hospital needed. ADF's native integration with Palo Alto Networks enabled the hospital to provide rapid threat containment and mitigation using their existing perimeter security infrastructure. Most importantly, Cyphort's ADF solution fit into their existing security infrastructure including SIEM and provided controls to better meet HIPAA and PCI compliance.

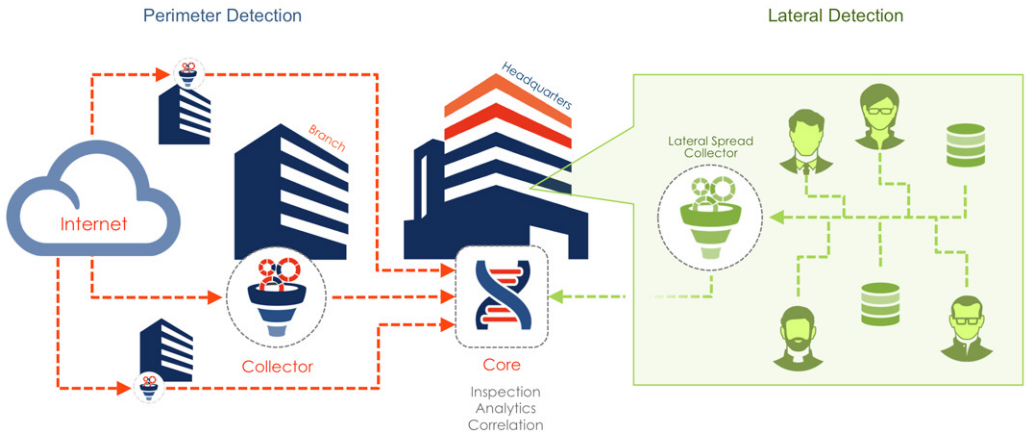
"Early on Cyphort's Adaptive Detection Fabric proved its value in our battle against malware. We're getting a lot more granular visibility into endpoints and infections allowing us to respond quicker."

–Security Team Lead

Malware attacks had become a sizable problem. The hospital IT security team needed visibility into the malware and attack vectors before the breach compromised the hospital or possibly threaten someone's life.

ADF provided East/ West and North/South visibility into endpoints and infections—allowing the hospital to respond to threats with speed and efficiency.

To learn more details about the results and benefits this customer experienced, call us at 1.408.841.4665 or email Cyphort at info@cyphort.com.



ADF uses an Open API architecture that seamlessly integrates with existing security infrastructure. ADF is designed to close the detection and mitigation gap across a diverse and distributed organization.

Results & Benefits

By deploying Cyphort's ADF solution, the hospital IT security team had broader and more granular visibility into the threats and infections attacking the network. The hospital is now able to defend a vast network of different endpoints and servers with fast, prioritized mitigation. Even with a large number of endpoint devices, ADF provides the team with visibility to better meet HIPAA and PCI compliance.

The hospital seamlessly integrated ADF with Palo Alto Networks (PAN) Next Generation Firewalls for threat containment and to block detected command and control activity. The hospital also tied ADF into their SIEM which accessed SmartCore's threat intelligence feeds and syslog to give the hospital clarity into what was taking place on their network.

About Cyphort

Cyphort, Inc. is a network security company providing mid- and large-size enterprise customers with the innovative Adaptive Detection Fabric, a scalable software solution designed to integrate with existing security tools to discover and contain the advanced threats that bypass the first line of security defense in an organization. Based in Santa Clara, California, the company was founded in 2011 and distributes its software through direct sales and channel partners across North America and international markets. Learn more at www.cyphort.com.

CYPHORT

5451 Great America Pkwy, Suite 225, Santa Clara, CA 95054 | P 1.408.841.4665 | F 1.408.540.1299 | info@cyphort.com
Sales/Customer Support P 1.855.862.5927 | F 1.408.540.1299 | support@cyphort.com