ALWAYS LEADING

Hospital Improves the Health of Its Cloud Security

HIGHLIGHTS

Customer

- A nonprofit specialty hospital offering long-term care for patients in and around Chicago

Industry

- Healthcare

Customer Environment

- A variety of on-premise products, along with secure cloud investments that included SECaaS and vCISO services
- The customer wanted to further strengthen their security posture in the cloud

Key Challenges

- The addition of security monitoring, incident response and triage, as well as forensics services to assist in the detection, response, and remediation of an attack
- The customer's AWS cloud environment achieved a higher level of protection, helping critical data and applications stay safe from bad actors

CUSTOMER

Founded in 1987, this nonprofit specialty hospital has locations in Chicago and the surrounding area. They focus on providing acute, long-term compassionate care for patients with prolonged and severe illnesses.

ENVIRONMENT

The customer had solutions from a wide variety of vendors within their on-premises IT environment, plus a significant number of "as a service" solutions in the cloud through AWS. Sentinel was also providing the customer with a number of different services, including Colocation Services, Managed Services for their DR site, Advisory Services, as well as Fortis by Sentinel offerings Virtual Chief Information Security Officer (vCISO) and Security as a Service (SECaaS).

CHALLENGE

As a healthcare organization that consistently deals with private medical records and other extremely sensitive data, the security of their environment remains a top priority. The customer sought to advance the protection services for their cloud to ensure the most robust detection and response possible in the event of an attack.

SOLUTION

The customer signed up for Fortis by Sentinel ActiveDefense Monitoring, designed to provide 24x7x365 threat protection. It maintained a close eye on nearly every portion of the cuistomer's AWS cloud environment, making it easier to detect suspicious activity, issue alerts, mitigate significant threats, and achieve compliance. Fortis also began to handle Incident Response for the customer, alerting them to high priority security events and delivering triage support and expert guidance should an attack occur. Lastly the customer added Fortis Forensics Services, where a team of highly certified investigators gather and preserve evidence of compromise making it easier to understand how an intruder gained access to their environment, the actions taken once inside, and what can be done to prevent such incidents from happening again.

RESULTS

As an AWS partner responsible for other cloud solutions, the Fortis by Sentinel team already had deep roots in the environment, which made the addition of advanced monitoring, incident response, and forensics services a very simple and streamlined process. The new solutions strengthened the customer's security posture even further, and most importantly gave them peace of mind that their highly sensitive data would remain safe in the event of a sophisticated attack.