ALERT LOGIC™

CASE STUDY

Alert Logic Helps Iodine Software Secure In-patient Healthcare Data and Meet Compliance Mandates

Iodine is an enterprise AI company dedicated to using its one of a kind technology to solve hard, evergreen challenges inherent in US hospitals—such as automating complex clinical tasks to scale hospitals' most valuable resources, generating insights, and ultimately empowering intelligent care. Powered by approximately 20-percent of all inpatient admissions in the United States, Iodine's clinical machine-learning engine, Cognitive ML, constantly ingests the patient record to generate real-time, clinically-informed, unique predictive insights. With this access to massive amounts of data comes an equally critical responsibility to ensure it is secure, confidential, and complying with regulations.

CHALLENGE

As a rapidly growing company, Iodine quickly recognized they could be an attractive target for a breach. As their peers in the healthcare industry suffered debilitating and embarrassing breaches, Iodine realized they needed continuous monitoring to provide the best protection for their client data. Their four-member IT department shared responsibilities between technical operations and information security. According to Cheng Zhou, Director of Site Reliability Engineering, Iodine Software, "Given our size, there was no way we could build a 24/7 security operations center (SOC) ourselves, nor the algorithms and expertise necessary to inspect all the data. Building it in-house would take away time that we could otherwise invest in engineering solutions for our scalability, which is more aligned to our core business."

iodine

About

Location: Austin, US

Industry: Healthcare Tech

Company Size: 140+

Business Impact

- Continuous monitoring and triaging by Alert Logic's 24/7 SOC allow Iodine to focus on **scaling their business**
- Iodine **gained the HITRUST certification** for their systems much faster with Alert Logic
- Alert Logic enables Iodine to easily prove **compliance with regulations**

SOLUTION

When Iodine realized they needed outside help, they led an extensive evaluation exercise and ultimately chose Alert Logic because of the completeness of the solution. Rather than protect a portion of their IT estate, they deployed Alert Logic MDR Professional across their entire enterprise spanning their AWS instances and on-premises data centers. This gave Iodine the ability to identify their most vulnerable assets and deploy their scant resources to address them. Zhou added, "We now run vulnerability scans far more frequently than we used to with our old vulnerability scanning tool."

Iodine also leverages the ability to search across all the logs that have been ingested into the system. Zhou elaborated, "Because of the duration of retention that we get with Alert Logic, not only are we able to use that as part of our security apparatus, but it also forms part of our compliance solution because we are able to assert that we can store logs for as long as needed by the regulators and auditors."

Alert Logic's response capability is key for Iodine because incidents are validated, triaged, and assigned a severity level by the Alert Logic SOC team. Iodine is notified on the high and critical incidents that need immediate action. Zhou explained, "We're able to confidently rely on Alert Logic's assertation of criticality, so when there are low priority incidents, we can be relatively certain that there isn't a monster hiding behind there." Zhou also shared that he was impressed by the quick response times and the depth of understanding of the various teams with which he interacted. "Overall, we've been extremely pleased with all our interactions with the deployment, detection, and response teams," he said.

The pandemic changed where people were accessing systems, what was considered normal versus abnormal traffic, and Iodine quickly had to react to that from a security assurance and response perspective. Zhou explained, "We appreciated the ability to continue extending our support and security infrastructure to all our employees, as they were now outside the envelope of protection that our corporate offices used to offer."

> *"Alert Logic is a major component in gaining HITRUST certification for our systems, due to their capabilities like vulnerability scanning and event correlation. This would have taken us years to do without Alert Logic."*
>
> **CHENG ZHOU**
> **DIRECTOR OF SITE RELIABILITY ENGINEERING, IODINE SOFTWARE**

> *"Our current team would have to be twice the size to be able to give ourselves the kind of coverage that we're getting with Alert Logic."*
>
> **CHENG ZHOU**
> **DIRECTOR OF SITE RELIABILITY ENGINEERING, IODINE SOFTWARE**

SUMMARY

Iodine always knew that AWS was part of their company's infrastructure future due to the flexibility and the speed of reactivity. They were cognizant of the fact that some organizations had made several missteps while moving to AWS, and they didn't want to do the same. They would not consider moving their production workloads into AWS without the protection of Alert Logic. Zhou shared, "A big part of our go forward strategy in moving and migrating customers to AWS was to be able to offer that envelope of protection that we got by combining Alert Logic with AWS."

In the end, Alert Logic has delivered peace of mind to the Iodine staff focused on securing their data and critical business systems. Zhou concluded, "While it's hard to put a price tag on it, it's really priceless to sleep well at night, knowing that there is somebody watching over our environment."