deepwatch™

CUSTOMER SUCCESS STORY

Deepwatch Partners with Ezer Group to Save Healthcare Organization Millions of Dollars

"We have given them the experience of having a full blown SOC for a third of what they thought they were going to have to spend."

- Justin Smith, CEO, Ezer Group

OVERVIEW

Deepwatch Helps Healthcare Organization Reduce The Frequency of Alerts

Deepwatch partnered with a healthcare organization to optimize their detection capabilities, significantly lowering the number of escalations, reducing their overall alert volume, and improving the noted true positive rates of their notifications.

Working with Ezer Group as the key partner, Deepwatch was able to greatly improve the customer's managed detection and response capabilities delivered through their Splunk investment, improving visibility into the organization's threat environment and significantly enhancing their cyber resilience.

CHALLENGE

Low Fidelity, High Volume Alerting

As a global organization delivering workforce education and training solutions to various healthcare organizations and providers, the customer faced significant challenges with the high volume of their alerts, many of which were false positives. Having a significantly complex security environment, the customer required specific customizations to achieve their goals while successfully delivering their unique compliance requirements and compensating controls.

Initial efforts to implement their solution resulted in significant challenges in dealing with the resulting alert volume and investigative workload, depriving the team of the precious time needed to identify and resolve the critical threats to the business.

When seeking a managed security provider, the customer struggled to find one that offered not only the necessary Splunk expertise but also the flexibility needed to effectively address their existing security team's obligations.

To overcome these challenges, the customer partnered with Ezer Group to identify a provider to assist with their alert volume, Splunk management, and regulatory requirements using their existing technology stack.

ENTERPRISE DETAILS

Industry: Healthcare

Services: Healthcare Enablement Solutions

Employees: 1,000

Security Team Size: 5

Deepwatch Partners: Ezer Group

deepwatch™

CYBER OUTCOMES

The Deepwatch solution led to several key cyber resilient outcomes for the customer, including:

- Platform stabilization and optimization
- Improved visibility into complex security environments
- Significant reduction in alert volume through increased fidelity
- Greatly expanded capabilities for their existing SOC staff
- An overall improvement to the organization's security program effectiveness

"The biggest change has been the reduction in the number of alerts, going from 17,000 to 8 in 90 days."

- Justin Smith, CEO, Ezer Group

Deepwatch was pivotal in the customer's successful cyber outcomes, saving them approximately three days a week of combing through alerts and improving their SOC team's efficiency, saving millions of dollars that can now be reallocated to other areas of their business. As a result, the customer was able to begin discussing expanding their SOC to include additional peer companies.

"This has been really instrumental for them in not only increasing their security posture, but also reducing the amount of noise they had coming and the workload associated."

- Justin Smith, CEO, Ezer Group

SOLUTION

Human-led, Splunk Expertise Tailored to Unique Challenges

Deepwatch experts implemented a tailored strategy to extend the capabilities of the company's existing team, optimize their Splunk instance, and achieve high fidelity and actionable alerting. This approach continues to support the company's current investments and compliance requirements

"With their level of customization, Deepwatch was able to catch alerts that other organizations were not catching."

- Gus Chiarello, COO, Ezer Group

Deepwatch improves actionable alerting and extends response capability speed, expertise, and coverage with a solution that includes:

- Transparent Managed Detection & Response capabilities based on the Splunk platform
- Integrated SOAR, automation, ticketing, and reporting capabilities
- 24/7/365 real-time actionable alerting and response coverage
- Access to world-class Splunk expertise
- Increased awareness and incident investigation leveraging the Deepwatch Adversary Threat Intelligence team

The Deepwatch partnership enabled the customer to optimize their existing environment, deriving maximum value from their current investments. The value of the partnership was further extended by augmenting their existing security team with Deepwatch Experts, avoiding the human resource spend required to build a larger internal SOC.

CUSTOMER TESTIMONIAL

"The combination of time saved, resources freed up, and how fast things got up and running once the solution was completely implemented was key."

- Deepwatch Customer, Healthcare Industry

deepwatch™

ABOUT DEEPWATCH

Deepwatch® is the pioneer of AI- and human-driven cyber resilience. By combining AI, security data, intelligence, and human expertise, the Deepwatch Platform helps organizations reduce risk through early and precise threat detection and remediation.

CONTACT US

GET STARTED

4030 W Boy Scout Blvd. Suite 550
Tampa, FL 33607

www.deepwatch.com