GAVS

CASE STUDY

Robust Security and Resilience
for Leading Healthcare Insurer

Client Overview

The client is one of the fastest growing not-for-profit managed care organizations in the U.S. - a provider-sponsored health insurance company, serving more than 1.2 million members in New York.

The Business Situation

As part of digital transformation initiatives, the client upgraded their core technology platforms to accelerate growth of their business. However, they faced several challenges due to the high-risk IT environment that had many unidentified security vulnerabilities. Securing their applications and infrastructure had become critical. They had an immediate need to secure their IT infrastructure that included 2,000+ endpoints, 500+ servers, and 200+ networks.

The Solution

With extensive expertise and rich experience in cyber security and data protection solutions for the healthcare domain, GAVS provided round-the-clock remote SOC (Security Operations Center) with threat hunting, and other solutions to bolster the client's security posture. Given below are the different solution components:

- 24x7 security operations support through a remote-based dedicated SOC
  - 2000+ endpoints, 500+ servers, 200+ networks
- Continuous monitoring, detection, and remediation of security vulnerabilities in applications, systems, networks, and end-user devices
- Quick detection and proactive alerting enabling immediate remediation
- Threat hunting for investigation on alerts triggered by security tools
- Increased control on application usage and user actions
- Splunk SIEM fine-tuned for user behavior analysis

Challenges

- High-risk environment due to unidentified security vulnerabilities
- Lack of visibility into threat landscape
- Reactive approach to cyber security and data protection

Solution Highlights

- 24x7 remote SOC, with threat hunting
- Continuous monitoring and proactive remediation of vulnerabilities
- SIEM fine-tuned for user behavior analysis
- Increased control on application usage and user actions

Solution Outcomes

- Highly secure end user, business, and IT environments
- 360° view of digital estate to help tackle emerging threats quickly
- 300% acceleration of security incident discovery
- Discovery of several security weaknesses not identified by previous vendor
- 35% reduction in false positives from SIEM and FIM
- Drastic reduction in security incident response time through validation against past occurrences
- Substantial improvement in client's security posture, infosec maturity
- Business assurance through effective triage of numerous incident trails, utility installations

To find out how GAVS can help your organization, please visit **www.gavstech.com**