GAVS

CASE STUDY

Cybersecurity Solutions for End-to-End Protection

for one of the Busiest Safety Net Hospitals in New York

Client Overview

The customer is the largest voluntary, not-for-profit health and teaching hospital system serving South and Central Bronx, servicing more than one million outpatients and 141,000 emergency visits each year.

The Business Situation

As part of their digital transformation initiatives, the customer required comprehensive cybersecurity solutions to proactively protect their high-risk legacy landscape that included 4,500+ endpoints, 500+ servers, 500+ network & security devices, 100+ applications, and 4500+ users (employees, vendors, contractors). Their needs included – among others, implementation of Multi-Factor Authentication (MFA), a highly secure business-class email & collaboration solution, extended endpoint protection, and Artificial Intelligence (AI) based network protection.

The Solution

With extensive expertise and rich experience in cybersecurity and data protection solutions for the healthcare domain, GAVS took an integrated approach to providing cybersecurity with AI-based security solutions focused on preventing intrusion, minimizing risk, and increasing resilience. Given below are the different security solution components:

- 24x7 SOC operations for threat monitoring, detection, and prevention
- Security Incident Triage and Response
- AI-based network solution, by partnering with Darktrace
- Collaboration with H-ISAC for real-time Cyber Information Sharing
- Automated Cyber Threat Intelligence and Threat Hunting
- Vulnerability detection in devices, IoT, and clinical applications
- Secure-By-Design: Microsoft Exchange to O365 Migration
  - Microsoft Exchange Online Protection, Advanced Threat Protection
  - Self-Service Password Reset (SSPR) with MFA for authentication
  - Cloud App Security for proactive risk mitigation for cloud services
  - AIP for encryption, to restrict ePHI content access
  - HIPAA compliant collaboration with SharePoint, OneDrive, Forms
  - Secure texting platform for desktops, mobile devices using Teams
- Adaptive, flexible MFA (Windows, Apple, Chrome OS) after assessment
  - Secured SSO access to applications
  - Hybrid cloud-based, on-premise solution for classic, emerging tech
  - Extensive API integration with Syslog and SIEM
  - Enhanced compliance and governance
- Strict adherence to HIPAA and state guidelines like the NY SHIELD Act
- Periodical 3rd party audits for vendor adherence to HIPAA/HITRUST
- ZIF™ enabled security functionalities:
  - Thwarting of phishing emails
  - Automation of the following: blocking of cyber attacks; incident response for Command & Control, data exfiltration, and ransomware; incident response in servers through auto scaling capability; repeatable security processes

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

Challenges

- High-risk legacy IT landscape
- Undetected vulnerabilities across end user, business, IT environments
- Lack of visibility into threat landscape
- Reactive approach to cybersecurity and data protection

Solution Highlights

- 24x7 SOC, Managed Detection & Response-MDR
- AI-based cyber defense solution, Darktrace
- Automated Cyber Threat Intelligence, Hunting
- Vulnerability detection, remediation in devices
- ZIF™ for automation of repeatable processes, threat blocking, and incident response
- Tightly integrated MFA solution with secured SSO access to applications
- Exchange Hybrid solution with advanced security features for access and collaboration
- Periodic audits to ensure regulatory compliance

Solution Outcomes

- 360° protection for the enterprise with multi-pronged AI-led solutions
- Expanded IOCs to proactively block nation/state sponsored & healthcare/HDO specific attacks
- Increased ability to predict threat landscape & scale security initiatives
- Highly secure communication, collaboration between clinicians
- Comprehensive MFA solution to include employees, vendors, contractors, partners
- Protection from identify theft, breaches, weak passwords, phishing attacks through MFA
- Enhanced regulatory compliance, governance, risk management