CASE STUDY

Providing Security and Resilience

as an End-to-End IT Partner

Client Overview

The Jewish Board is one of the largest not-for-profit healthcare organizations in New York City, providing behavioral health & human services for over 140 years. They offer their services in over 65 facilities spread across the five boroughs of New York City.

The Business Situation

The Jewish Board is grounded on a legacy of help and relief to increasing number of individuals & families in newer ways, with IT as the business backbone. However, their IT landscape presented many challenges that impacted productivity and inhibited business growth. One of the main roadblocks was the lack of sufficient cyber security for their high-risk IT and business environments that included hundreds of servers, network devices, security devices, and thousands of endpoints. They required integrated cyber security solutions to prevent cyberattacks and increase their resilience.

The Solution

With extensive expertise and rich experience in cyber security and data protection solutions for the healthcare domain, Long 80 took an integrated approach to providing cyber security with AI-based security solutions focused on preventing intrusion, minimizing risk, and increasing resilience. Given below are the different solution components:

- Implementation of AI-based cyber defence solution, Darktrace
- TAXII & STIX based cyberthreat intelligence configured to block attacks within the Healthcare and Public Health (HPH) sector, and to block adversaries targeting the agency
- Enforcement of dual authentication mechanism
- Network infrastructure enhancements for higher redundancy & security
- Proactive detection of security issues leveraging AIOps Platform ZIF™
- Governance & compliance aligned with guidelines like HIPAA, arresting PHI leakage
- Periodic audits at regular intervals for IT security maturity
- Continuous user education & monthly phishing campaigns
- Rapid enablement of workforce during Covid-19
    - Secure mobility and telehealth with minimal disruption
    - Secure remote application access on a virtual desktop via Citrix gateway

To find out how Long 80 can help your organization, please visit **www.long-80.com**

Challenges

- Several security vulnerabilities across end user, business, and IT environments
- Lack of visibility into threat landscape
- Reactive approach to cyber security and data protection

Solution Highlights

- Implementation of Darktrace, an AI-based cyber defence solution
- TAXII & STIX based cyberthreat intelligence
- Enforcement of dual authentication mechanism
- Network infrastructure enhancements
- Implementation of AIOps Platform ZIF™
- Governance & compliance aligned with regulatory guidelines
- Periodic audits, routine phishing campaigns, continuous user education
- Rapid enablement of secure mobility during Covid-19

Solution Outcomes

- Highly secure end user, business, and IT environments
- Reduction in costs of safeguard through proactive detection and remediation
- Unified view of entire digital estate to help tackle emerging threats quickly
- Expanded IOCs to block healthcare & other adversaries
- Increased ability to predict threat landscape & scale security initiatives