



Case Study:

# NATIONAL UNIVERSITY OF HEALTH SCIENCES

A Multilayered Security Approach  
to Defend Against Cyberattacks

Founded in 1906, the National University of Health Sciences (NUHS) is a leader in career training for health care. They are a part of a growing field of integrative medicine, balancing healing arts and science with patient-centered care.





## The Challenge

NUHS with its dual locations (Lombard, Ill. and St. Petersburg, Fla.) connects a diverse population of staff, students and prospective students through their network. While most of the network users are located in the United States, NUHS also draws many international prospective students. As a long-time client, NUHS and Elevation have held regular meetings to review NUHS' IT security posture.

Cybersecurity threats are constantly evolving and a student email migration project revealed that NUHS needed additional security to stay on top of bad actor attempts in real time across multiple systems. It was time to implement additional tools designed to complement and strengthen NUHS' cybersecurity suite of solutions.



## The Solution

Elevation recommended a multilayered cybersecurity plan to deter bad actors in real time. This included deploying a proven HIPAA and GLBA compliant SIEM/SOC solution into NUHS' network. The change in strategy increased NUHS' defenses and now includes the ability to proactively hunt for, identify and neutralize lurking threats.

Additional cybersecurity measures were added later, such as incident escalation procedures and multifactor authentication to enhance this comprehensive, multilayered approach.







## The Results

NUHS' now receives an alert notification as soon as a data abnormality is detected in real time. This early alert has already saved NUHS twice from phishing attacks attempting to compromise an employee's credentials.

In comparison, prior to implementing the SIEM/SOC solution, there was an incident where an employee's email account was compromised due to a phishing attack and it took three weeks before this breach was identified.

Today, NUHS and their Elevelty vCIO meet quarterly to discuss data trends and evaluate if adjustments to their alert thresholds are necessary. These meetings are key to ensuring that NUHS is well-protected from cyberthreats both now and into the future.



*As an administrator, it makes me feel more comfortable knowing what's happening in my system and that we have defenses in place that notify us of potential system breaches, in real time.*



**Ron Mensching**  
Vice President, Business Services



Elevity offers fully managed technology services for small and mid-sized businesses, as well as co-managed technology services for larger companies whose IT departments need an extra hand. We encourage you to contact us and discuss what new technology solutions we can bring to your business.

[CONTACT US](#)

