IDENTITY & ACCESS MANAGEMENT:
SECURING THE NATION'S INFRASTRUCTURE

CLIENT CHALLENGES

On average, before an organization discovers their network has been breached or compromised, over 100 days will pass. At that point, it may be too late.

Often, the major weakness in networks is passwords, accounting for 80% of hacking-related breaches.

Using multi-factor authentication (MFA) requires two or more factors of verification, and makes a big difference. In fact, using two or more authentication factors reduces the risk of compromise by 99.9%.

Our client, a global leader in the freight transportation industry and a critical part of the U.S. infrastructure, needed to implement multi-factor authentication on more than 100,000 IoT devices, as well as train more than 43,000 employees.

SPERO SOLUTIONS

In partnership with the client, Spero developed a customized project plan centered around a blue team of 20 cybersecurity specialists to implement the project across their network of employees and devices.

Our project team worked on-call rotations 24/7/365, supporting the infrastructure security and incident response of their network and operations.

The Spero account managers worked hand-inhand with the client's cybersecurity team, Network Operations team and Service Desk to coordinate workflow, adjust staff to meet their response needs and deliver results on time.

SPERO RESULTS

Multi-factor authentication and training for all 100,000+ devices and 43,000+ employees was completed on time, and Spero was rewarded with taking on full support of their Mobility Service team.

We provided 20 consultants for the project and managed that team internally.

Every one of our consultants is still with our client today – two years later. In addition, several of our consultants have been promoted into lead roles.

This is yet another example of the superior quality of candidates we recruit and provide to our clients.

SPERO
NATIVE AMERICAN OWNED