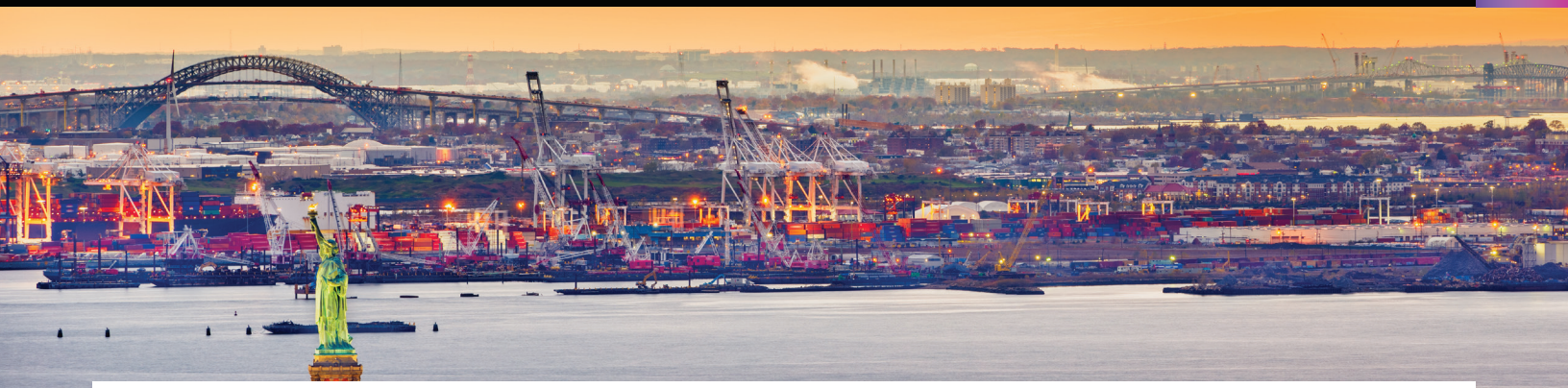

CASE STUDY

The Path to Enhanced Cyber Risk Management – Port Authority of New York and New Jersey (PANYNJ) and Claroty

Introduction

As one of the largest transportation agencies in the United States, the Port Authority of New York and New Jersey (PANYNJ) manages a vast network of critical infrastructure. This includes several major international airports, multiple bridges and tunnels, a major maritime port complex, an extensive commuter train system, a major bus terminal, and the World Trade Center complex. At its busiest time of the year, PANYNJ can serve upwards of six million people in a single day. To securely support that multifaceted infrastructure, an extensive collection of Operational Technology (OT) systems is embedded in a complex architecture that demands a vigorous risk management program. Ranging from behind-the-scenes operational systems to passenger tolls and safety information systems and much more, there are hundreds of PANYNJ industrial control systems, composed of thousands of assets.

PORT AUTHORITY NY NJ

The Port Authority of New York and New Jersey, (PANYNJ) is a joint venture between the U.S. states of New York and New Jersey, established in 1921 through an interstate compact authorized by the United States Congress. The Port Authority oversees much of the regional transportation infrastructure, including bridges, tunnels, airports, and seaports, within the geographical jurisdiction of the Port of New York and New Jersey.

Cybersecurity Challenges

The emergent OT threat environment, coupled with unexamined vulnerabilities in the Agency's OT architecture, created a new sense of urgency to identify, isolate, and manage their OT cyber risks. The challenge became clear and immediate: design, then either buy, or build an OT-specific security platform that would support multiple program initiatives for securing this technology environment.

The Agency began utilizing a laborious and time-consuming manual system-specific OT risk assessment process. The results were startling—they revealed that PANYNJ was already experiencing multiple OT cyber incidents. Ranging from malware infiltrations to abnormal OT data traffic patterns and even unauthorized system access attempts, these discoveries highlighted the susceptibility of the existing OT defenses and illustrated the difficulty of securing and supervising both interconnected and standalone OT systems and devices.

Moreover, the convergence trend of IT and OT systems adds an additional layer of technical complexity because visibility into system configurations and OT asset behavior can be obscured. Underpinning these technical and security risk factors were new and wide-ranging regulatory requirements emerging from the federal government that are based on the NIST Cyber Security Framework.

The mission was clear: protect their vast system from potential breaches that could disrupt services and pose risks to security and safety.

Embracing Claroty

To address these challenges, the PANYNJ embarked on a comprehensive search for a versatile platform specifically designed and engineered for OT and able to handle complex challenges like the convergence of IT and OT. Their "wish list" was extensive—a platform that not only provides robust threat detection, vulnerability management, and secure remote access but can also be extended to other areas of the NIST CSF collection of 108 cybersecurity controls that the PANYNJ was measured against in previous external risk assessments.

> "In order to determine the features, functionalities, and flexibility of OT network monitoring platforms, we selected several competitor vendors and distributed a detailed Data Request that included 265 questions in seven distinct functional and technical areas. Only three responded with answers to nearly all 265 technical questions- this enabled our internal stakeholders to precisely measure what each vendor might do for us, and no one else came close to the Claroty responses."
>
> – JOHN BALLENTINE, OT CYBERSECURITY PROGRAM LEAD, PANYNJ.

After an exhaustive analysis of the three Data Request Responses and completing vigorous- and comparative proofs-of-concept with the three responding vendors, Claroty emerged as the clear choice for PANYNJ. The Agency established that Claroty would seamlessly integrate with PANYNJ's existing environment, such as the IT security program and the Cybersecurity Operations Center (CSOC).

Implementation and Current Usage

Given the breadth and depth of the PANYNJ OT environment, the initial implementation of Claroty is nearly complete after two years, with the bulk of most critical systems onboarded in the first 8-10 months. The process began with training PANYNJ's cybersecurity teams to optimize the use of Claroty's features and capabilities. The present-day sequence of onboarding OT systems onto Claroty has become fairly standardized, with the main operation being to fine-tune the output from Claroty's technical analysis of the traffic it is capturing.

Today, Claroty plays a vital and pivotal role in PANYNJ's overall OT cyber risk management strategy. It continues to provide real-time threat detection to OT networks and the interaction between IT-OT networks, maintaining their integrity while ensuring system availability. Leveraging Claroty allows PANYNJ to understand the communication patterns of their OT assets, monitoring not just for security breaches but also for unusual behaviors that can reveal threat activity and even operational disruptions from a variety of causes.

Moreover, as Claroty continues to evolve and add new features to its suite, PANYNJ is poised to benefit from these enhancements, thereby further strengthening its security and operational conditions.

> "Claroty has acted as a real partner, focusing on our unique challenges and creating working teams that have adapted the product to better align with our program goals, especially our threat management strategies."
>
> — JOHN BALLENTINE

Conclusion

With the assistance of a tailored and adaptable enterprise-grade solution like Claroty, PANYNJ has successfully designed, procured, engineered, deployed, and consequently achieved, maintained, and enhanced its OT risk management position by ensuring safer and more resilient critical infrastructural services.

Going forward, PANYNJ recommends that organizations operating in similar scenarios embrace digital transformation securely by opting for robust, comprehensive platforms that provide visibility, control, and protection for their ICS networks.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.