CASE STUDY

SECURING CRITICAL INFRASTRUCTURE IN A HEIGHTENED THREAT ENVIRONMENT

INDUSTRY

Chemicals / Critical Infrastructure

CUSTOMER

North American Mining & Chemicals Processing Company (>$20B Revenue)

APPLICATION

Enterprise Mail Security & Risk-Based Screening Program

Critical infrastructure operators — particularly in the chemicals and mining sectors — face elevated risk in today's environment of geopolitical instability, activist targeting, and increased scrutiny of industrial operations.

In 2021, a newly appointed Global Head of Security at this $20B North American chemical and mining company identified a significant gap: the organization had no formal mail security program.

At the time, the Department of Homeland Security classified the chemicals sector as high-risk for mail-borne threats. While evaluating solutions, pipe bombs were discovered in a community where the company operated. Though not directed at the company, the incident reinforced a growing reality: mail can be used to disrupt operations, intimidate leadership, or cause exposure events — even when the organization itself is not the intended target.

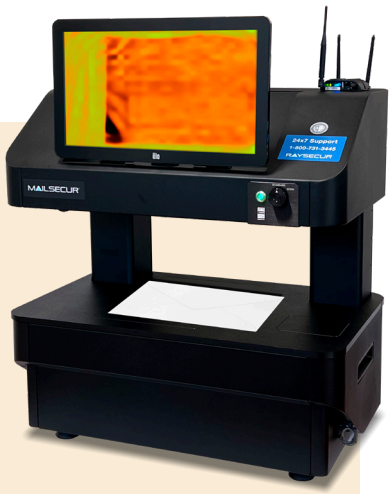
In 2026, with rising polarization, ESG-related activism, and global supply chain tensions, that reality is even more pronounced.

THE CHALLENGE: BUILDING AN ENTERPRISE MAIL SECURITY PROGRAM FROM THE GROUND UP

- A risk-based screening framework
- Standardized operating procedures across multiple sites
- DHS SAFETY Act Designated technology
- Scalable training for distributed teams
- 24/7 expert advisory support

Not all facilities carried equal risk. Some locations housed executive leadership and R&D operations. Others were manufacturing or logistics sites. The solution needed to align with differentiated risk profiles — without creating unnecessary operational burden.

And all of this had to be deployed during a period of operational disruption caused by COVID.



THE SOLUTION: RISK ASSESSMENT + 4D T-RAY SCREENING + PROTECTIVE INTELLIGENCE SUPPORT

RaySecur's security experts — including former U.S. Postal Inspectors and U.S. Army EOD specialists — conducted quantitative risk assessments across nine facilities.

- Threat perception and history
- Facility type and geographic location
- Access controls and mail flow

- Employee profile and leadership visibility
- Operational impact of a disruption

From this assessment, RaySecur developed a customized enterprise mail security SOP.

Following a 30-day pilot at headquarters, the company deployed MailSecur® across all high- and medium-risk sites.

Powered by patented 4D T-ray (terahertz) technology, MailSecur enables teams to screen unopened mail and detect anomalies consistent with powders, liquids, gels, soaked substrates, thin electronics, and other concealed threats — without opening the item.

Unlike traditional X-ray systems, MailSecur provides dynamic 4D visualization, allowing operators to rotate items and evaluate contents in real time before exposure.

Lower-risk sites implemented RaySecur's mobile screening workflow tools, providing step-by-step screening guidance, escalation protocols, and direct access to RaySecur threat experts for second opinions.

RaySecur also delivered remote and online training programs to standardize screening procedures across the enterprise.

THE OUTCOME: FROM 0% TO ENTERPRISE-WIDE PROTECTION

The company transitioned from having no formal mail screening program to a fully standardized, enterprise-wide security posture. Today, all inbound mail across the organization is screened using a risk-based protocol supported by DHS SAFETY Act Designated technology.

- 100% mail screening coverage across sites
- Standardized SOPs aligned to facility risk
- 24/7 access to military-trained threat experts
- Documented screening workflows for compliance and audit readiness

At scale, the average per-site cost of implementing a comprehensive mail security program is comparable to renting a photocopier — a modest investment relative to the operational impact of a shutdown or exposure event.

ONGOING PARTNERSHIP & PROTECTIVE INTELLIGENCE INTEGRATION

The relationship has evolved beyond technology deployment. As part of its ongoing protective intelligence posture, the company collaborates with RaySecur to refine threat models and screening best practices.

Anonymized screening data contributes to the continuous advancement of RaySecur's AI-enhanced detection capabilities.

MailSecur® is now embedded as part of the organization's broader CBRNE risk mitigation strategy — strengthening resilience against chemical, biological, radiological, explosive, dangerous goods, and hoax threats.

WHY THIS MATTERS IN 2026

For critical infrastructure operators, mail is no longer a low-risk administrative channel. It is a potential pathway for supply chain disruption, targeted intimidation, activist-driven incidents, powder hoaxes that trigger costly shutdowns, and exposure events that impact personnel safety.

This $20B chemical enterprise recognized early that proactive screening is far less costly than reactive disruption. Their approach demonstrates that mail security is not just a compliance exercise — it is a foundational component of modern protective intelligence. MailSecur® provides the capability to detect the invisible and protect critical operations before exposure occurs.

For information on how to use MailSecur to keep your people and organization safe, contact:

RAYSECUR® www.raysecur.com | 617-855-9938 | info@raysecur.com