

Mail Security Success Stories

RaySecur is trusted to protect major companies in virtually all industries.



4 of the 5 most valuable companies in the world use **MailSecur**.

The security teams of 6 of the 10 wealthiest people use **MailSecur**, too.

Here are just a few examples.

ONE OF THOSE FIVE MOST VALUABLE COMPANIES, a tech company with over \$100B in revenue, was using X-ray scanners. They closed a major gap in their mail security with **MailSecur**.

"There is no way that I can see the powders that MailSecur is showing on my X-ray system."
– Director of Global Security Operations Center and Mail Center, Executive Protection

A GLOBAL STOCK EXCHANGE implemented **MailSecur** to assure that its operations on three continents would never be disrupted.

"The safety and ease of use are two of the key reasons why we deployed these systems across our critical sites."
– Global Security Director, International Stock Exchange

ONE OF THE BEST-KNOWN FINANCIAL SERVICES COMPANIES IN THE WORLD with over \$20B in revenue protects its offices and personnel globally with **RaySecur**.

"MailSecur quickly proved that it could detect threats that our third-party firm couldn't with their off-site X-ray scanners."
– Director, Global Security Operations

A \$5B GLOBAL CLOUD SERVICE PROVIDER uses **MailSecur** to help keep its operations up 24/7/365.

"The safety and ease of use of RaySecur's scanners are two of the key reasons why we deployed these systems across four of our critical sites in North America this year. Adding this layer of screening also allows us to comply with the recommendations made by Homeland Security..."
– Shipping and Receiving Manager

A LEADING SOCIAL MEDIA PLATFORM with over 500 million users chose **MailSecur** for their executive protection program.

"The trial period has been successful, and we feel this is a critical layer to our risk mitigation strategy supporting our Senior Leadership Team."
– Senior Manager, Executive Protection

A MANUFACTURER OF BUSINESS EQUIPMENT with over \$7B in revenue bolstered its security with **MailSecur**.

“RaySecur’s technology has permitted us to stay compliant with proper mail handling procedures and helps prevent mail threats from entering our organization.”

– Manager, Physical Security

AN AEROSPACE AND DEFENSE MANUFACTURER with over 100,000 employees chose **MailSecur** to help protect one of its most critical sites.

“RaySecur’s technology fills a critical gap in mail security not addressed by X-ray systems.”

– Site Lead

A MAJOR 2020 U.S. PRESIDENTIAL CANDIDATE was facing threats to himself, his family, and staff. His security team used **MailSecur** to keep them all safer.

“I did feel a lot more secure and I got a lot more confident in trusting what I saw because MailSecur was so easy to use.”

– Staffer in charge of handling the daily mail.

ADDITIONAL MAILSECUR USE ACROSS INDUSTRY LEADERS...

The security team of a **FORTUNE 100 MANUFACTURER** needed to create a mail security program from scratch when the company split. They chose **MailSecur** for their headquarters and are now specifying it for all new facilities. **RaySecur’s** mail security experts helped them create a new Standard Operating Procedure.

ONE OF THE FOUR FEDERAL CRIME LABS in the U.S. has access to every possible type of security technology, but their own personnel didn’t know if packages were potentially dangerous to open. Adding **MailSecur** to their tech arsenal closed the mail security gap for them and made their lab personnel safer.

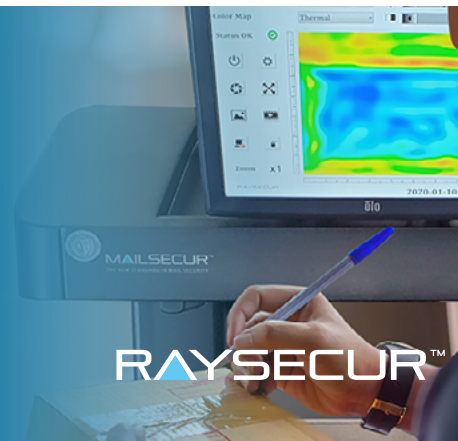
A G8 LEADER faced constant threats. Their security team added **MailSecur** to their already impressive array of security technologies to keep the leader – and team – safer.

A \$20 BILLION CHEMICAL COMPANY with over 20,000 employees chose **RaySecur** for its first-ever mail security program. **RaySecur** mail security experts helped them develop a company-wide Standard Operating Procedure and implement **MailSecur** at the high-risk locations.

The staff of **ONE OF THE FIVE LARGEST HEDGE FUNDS IN THE WORLD** was open to mail-borne threats arriving via delivery of Amazon packages and items from their internal “Craigslist”. The firm closed the security gap with **MailSecur**.

AND MANY, MANY MORE.

Leading Tech Company Using X-Ray Scanners Faced a Major Gap in their Mail Security



MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY
Tech

CUSTOMER
One of the largest
tech companies in
the world

CHALLENGE
Their existing
X-ray scanners
miss most common
mail threats.

*“There is no way that I can see the
powders that MailSecur is showing
on my X-ray system.”*

**Director of Global Security
Operations Center and Mail Center, Executive Protection**

CHALLENGE

MailSecur is used by 4 of the 5 most valuable companies in the world and this is one of them, with revenue well north of \$100 billion annually. Given its size and industry prominence, its current (and former) executives are some of the best-known business leaders and face the regular threats that that level of visibility provokes.

The company was using X-ray mail scanners, swab detectors, and downdraft tables to inspect items headed to the C-suite, but they knew that even that impressive arsenal of security technology could not detect all of the potential threats; specifically, they couldn't detect powders or liquids, the most likely mail threats today. These systems require high-trained specialists, are hard to scale, and often have false positives. Individual mail security employees have a Duty of Care and they wanted to arm them with more knowledge before they opened an item. And they wanted a Department of Homeland Security Safety Act Designated technology that could scale to many locations.

SOLUTION

The company closed the remaining mail security gap in their sophisticated executive protection program by adding **MailSecur** scanners into their screening regimen. They also asked **RaySecur** mail security experts to review and consult on their entire mail security process, so **RaySecur's** team traveled to their headquarters to meet with them and conduct the evaluation.



This led to **RaySecur's** security experts contributing to the company-wide mail security Standard Operating Procedures. And **RaySecur's EODSecur** service provides on-call expertise when they need it, eliminating the need for expensive experts on staff.

With its quick setup and training, **MailSecur** was easy to add to their security program, and is portable and scalable. **MailSecur** needed none of the extra, expensive shielding or certification that the company's X-ray mail scanners had, took up little room, and could be plugged into a standard office electrical outlet. Employees were using it in less than an hour.

As the first mail scanner to be designated as a Qualified Anti-Terrorism Technology (QATT), **MailSecur** also met that requirement.

OUTCOME

The EP team appreciates how MailSecur closes the security gap before they need to open a suspicious item. The team also continues to keep their mail security knowledge up to date by attending **RaySecur's** quarterly webinars for customers.

The company is looking at expanding the mail security program globally to all their locations. They knew from the start that they needed a scalable solution, that mail security shouldn't just be for the privileged few but for everyone. With the ease of implementing **RaySecur's** Five Pillars approach including hardware, training, and 24/7 **EODSecur** support, the company's security team is able to implement enterprise-wide coverage.

How a Global Stock Exchange Protects Mail Rooms on Four Continents

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Finance & Banking

CUSTOMER

Global Stock
Exchange

CHALLENGE

Protecting
Worldwide Trading
Desk Operations

“The safety and ease of use are two of the key reasons why we deployed these systems across our critical sites.”

Global Security Director, International Stock Exchange

CHALLENGE

With their high profiles and the possibility to make – or lose – a fortune in an instant, it’s not surprising that stock exchanges routinely face major security threats. Operating in North America, Europe, and Asia, this exchange received two significant mail-borne threats in less than six months, both exposing risks to critical infrastructure. They knew that a facility evacuation would have an enormous impact on their business and brand.

They operated a fragmented security program with five types of equipment in various locations, and some sites completely unprotected. Though the exchange used X-ray scanners, they were expensive to scale, especially in Europe and Asia where regulatory bodies are tightening the requirements on radioactive sources. And they were unable to detect threatening powders and liquids – their most common threat. Their security program was managed by exception. They needed a system to detect all CBRNE threats that was safe to use.

SOLUTION

RaySecur’s security experts completed a risk assessment for the exchange, ratings sites as low-, medium-, or high-risk based on location, number of employees, threat level, vulnerability, type of facility, and other factors consistent with US DHS guidelines. From this assessment the stock exchange recognized the significant security gap posed by their mail stream.



To quickly seal that gap, **RaySecur** provided **MailSecur** scanners that could be up and running in a matter of minutes in their offices worldwide and would detect not just powders and liquids but the full range of CBRNE threats. A significant advantage for global deployments is the safety of the **MailSecur** scanner itself, also requiring no special licenses or radiation permits, unlike X-ray. This is especially important in Japan, and other countries with strict radiation permitting requirements. Given the success of the solution, a **MailSecur** scanner is now standard equipment as the exchange opens new offices around the world.

OUTCOME

Since deploying **RaySecur's** solutions, this customer has detected and prevented several major security incidents and has avoided costly or embarrassing external responses. Most importantly, international trading operations have not been disrupted due to mail threats.

Thanks to the risk assessment provided by **RaySecur's** security experts, the customer replaced covert mail security procedures with overt operations. Their people in every department are now aware of ongoing mail screening processes, significantly reducing the risk of an inside threat. This saves time, effort, and money for security and facilities teams, which are now free to focus on external threats. The result is a stronger, more effective global security program to protect all key international sites, not just a select few.

How One of the Best-Known Financial Services Companies in the World Protects Offices and Personnel Globally

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Finance & Banking

CUSTOMER

Global Financial
Services Company
> \$10B Revenue

CHALLENGE

Protecting against
both internal and
external threats to
their operation

“MailSecur quickly proved that it could detect threats that our third-party firm couldn’t with their off-site X-ray scanners.”

Director, Global Security Operations.

CHALLENGE

The company is one of the best-known financial services brands in the world. It operates globally in a sector – Banking – that the Department of Homeland Security considers to be one of the high-risk industries for mail threats. As always, where there’s money there’s someone trying to figure out a way to get at it, whether by theft, extortion, or other means. And with multiple offices worldwide, the potential risks were both internal and external.

The X-ray mail scanners operated off-site by their third-party mail screeners were simply not up to detecting the most common physical threats and hoaxes received in the mail today. In particular, common “white powder” hoaxes and legitimate threats whether drugs, explosives, or dangerous chemical compounds (such as anthrax and ricin) typically go undetected with X-ray scanners. Off-site screening adds logistical complexities and delays in the receipt of mail. And their vendor was not able to protect all of their sites globally.

It was also important to them that any new device not sit on their network or otherwise open up a potential hole in their cybersecurity.



SOLUTION

The company security personnel knew that they needed to button up security globally. Initially, since millimeter wave imaging is a new technology, they bought two units to test **MailSecur**. They quickly gained confidence in the **MailSecur** units and deployed them to nearly two dozen offices worldwide. With their small profile and safe millimeter wave technology, the **MailSecur** units could go through customs without delay and be setup in a matter of minutes without the costly permits and licenses required for X-ray scanners. Setup also did not require any IT support since MailSecur has its own SIM card and did not need to be connected to the company network - an added benefit for the company's cybersecurity. And since they are intuitive and easy to use, their operators were quickly comfortable and proficient in operating them.

OUTCOME

It wasn't long before the company reported the detection of a major internal incident: 1.5 pounds of cocaine had been sent between offices via inter-office mail. Their third-party mail screeners had scanned the package off-site, found nothing, flagged it as safe, and sent it on to the second office where their internal people using **MailSecur** spotted the cocaine. This validated their switch to **MailSecur**: they now had the technology that – unlike X-ray scanners – could detect the most common threats, and they eliminated the additional cost, delays, and logistical complexity of using an off-site third-party mail screener.

As the company has had to reconfigure and move offices during the COVID pandemic, they have easily moved their **MailSecur** units to new locations and countries, too.

\$5B Global Cloud Service Provider Faces Threats Worldwide

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY
Technology

CUSTOMER
Cloud service provider with dozens of facilities globally > \$5B Revenue

CHALLENGE
Scaling up a new mail security program across multiple data centers.

*“The safety and ease of use of **RaySecur**’s scanners are two of the key reasons why we deployed these systems across four of our critical sites in North America this year. Adding this layer of screening also allows us to comply with the recommendations made by Homeland Security...”*

Shipping and Receiving Manager

CHALLENGE

Like any cloud service provider, this \$5B-plus company puts a top priority on uptime of its data centers. They have very high, “six-nines plus” standards. *Just an hour* of downtime in a major center can cost over \$1 million. They are very careful about the location of their centers (taking into account such factors as weather and geologic stability), having redundant power systems, multiple layers of backup – and outstanding mail security.

Cloud providers have a unique mail security challenge. They may be providing services to thousands of companies in dozens of industries, but they are not aware of everything that their customers are doing online – nor could they be. Third parties, though, may be intensely aware of the end user’s activities, may be greatly offended by some, and may (absurdly) blame the cloud provider for them. If a customer is in the news, some people will track down where they are hosted, and the hosting company can be at risk. They also have challenges from people entering and exiting the data center. A USB key or other data storage device can be used to take a huge amount of data out of the facilities.

And while the IT people may think that their greatest security threats are online, they in fact face equally serious physical security challenges. This company has over 60 sites globally, including data centers, offices, and agents, each with a different security profile. People carrying items (with data) in and out could be as significant of a risk as threats coming through the mail, but they did not have a policy for controlling those entrances and exits.



SOLUTION

Employing our Five Pillars approach, **RaySecur**'s security experts worked with the customer's security and facilities leads to develop a global Mail Security Standard Operating Procedure (SOP) to meet the cloud provider's unique requirements. The **RaySecur** team, composed of former US Federal Postal Inspectors and military threat experts supported the customer in implementing a holistic risk scoring approach for all of their sites. Based on this enterprise risk assessment and implementation plan, the customer initially installed **MailSecur** scanners in the four facilities at highest risk in North America, with a roll-out plan for additional deployments across the enterprise. Medium-risk sites are using **RaySecur**'s **MailSecur Connect** mobile app to implement and enforce standard mail security processes and procedures at satellite sites and ensure all employees are following proper screening procedures. They are also receiving in-depth mail security training from **RaySecur**, and **RaySecur** provides 24/7/365 **EODSecur** support when incidents arise.

RaySecur's security plan also included a new carry-in/carry-out policy. Now people are required to leave jackets and other personal items in an entry closet and items are scanned in **MailSecur** as people come and go, just like their inbound and outbound mail.

OUTCOME

Now the cloud provider is using **MailSecur** to scan mail and personal items being brought in or out. Company security personnel are expert at detecting potentially harmful physical items whether they come in via the mail or on a person, and with **MailSecur Connect** they can identify items from potentially high-risk individuals. They have 24/7 access to **RaySecur**'s **EODSecur** support when a suspicious item is detected.

At less than the cost of a photocopier for each site, the company is providing a whole new level of uptime assurance for their customers. **RaySecur** is helping them provide six-nines plus uptime across tens of thousands of systems. Mail security is not a cost; it is contributing to the company's core source of revenue.

Pete for America Case Study

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Politics

CUSTOMER

A major U.S.
presidential
campaign

CHALLENGE

Keeping the
candidate, staff,
and his family safe
from mail threats

“I did feel a lot more secure and I got a lot more confident in trusting what I saw because MailSecur was so easy to use.”

Lia Rocchino

Risk Management and Vetting Associate for Pete for America

Famous people – including presidential contenders – generate a lot of passion, pro and con. So it’s not surprising that they, their families, offices and staff receive a lot of unexpected items through the mail. Some are fun, like a cake or a funny t-shirt. Others are, or initially appear to be, more sinister.

CHALLENGE

Senator Bernie Sanders had two campaign offices shut down due to mail threats in just September, 2019.


The 2020 U.S. presidential campaign of Pete Buttigieg received so many verbal and written threats that they decided they needed to do something to keep their staff and the mayor’s family safe. After contracting with a third-party executive protection firm, the firm directed them to **MailSecur** given the system’s ease of deployment and high level of effectiveness in screening and detecting mail threats.



SOLUTION

Based on the recommendations of their executive protection firm, the Pete for America Campaign chose to use **MailSecur** from **RaySecur** to scan each day’s incoming mail. With **MailSecur** they could “see inside” mail with real-time, 3D video and detect potential threats before the item was opened.

MailSecur was set up in Mayor Pete’s South Bend headquarters in a few minutes. It took up little space and required no special shielding or certification. The campaign had all the mail from their South Bend field office and Pete Buttigieg’s family members sent to the headquarters for screening before being returned to them to be opened. Combined with the headquarter’s mail, it only took about an hour a day to screen it all with **MailSecur**.



Did they assign a seasoned security veteran with years of experience to handle the mail screening? No, they assigned a young campaign staffer with no security experience. The **MailSecur** training was so thorough, and it was so easy to use, that – combined with 24/7 **RaySecur** expert EOD* support – within just a few weeks she was quite comfortable running the mail screening and flagging suspect items. She could recognize “typical” mail items routinely sent into headquarters like campaign buttons, lapel pins, and other promotional items. And despite many threats, nothing was identified that required closing the office.

“The training was pretty great,” said Lia Rocchino, Risk Management and Vetting Associate for Pete for America. “I felt prepared for a lot of the things that I was going to see. I felt pretty good at recognizing items just from the training. It only took a couple weeks of checking with **RaySecur** on a couple objects to recognize items.”

“It worked a lot faster and a lot smoother than I had anticipated. I anticipated that it would be harder to use. I did feel a lot more secure and I got a lot more confident in trusting what I saw because **MailSecur** was so easy to use.”

For a person new to mail screening, a few items stood out. “Baseball caps look really weird,” Lia said. And the unusual shape of a folded-up gift t-shirt raised a few eyebrows. But she could share the suspicious images and video with **RaySecur**’s 24/7 EOD support in real-time. Over the course of the campaign she contacted **RaySecur** support several times whenever she saw something abnormal in the mail for an expert second opinion.

“And working with **RaySecur** was a lot smoother than I thought it would be, which was really, really helpful.”

OUTCOME

In this case, the client had a need to quickly set up a comprehensive mail security program for a high-profile political figure where none had previously existed. **MailSecur** eliminated the need for costly and time-consuming radiation permitting required for X-ray scanners and was set up and running in the campaign headquarters in minutes.

MailSecur’s real-time 3D video imaging of the contents inside packages and envelopes made it very easy for a campaign staffer with no previous security or mail screening experience to quickly get up to speed on how to use the system. More importantly, the staffer was able to quickly identify suspicious items and rely on **RaySecur**’s EOD remote support to provide an expert second opinion in real-time for keeping the campaign safe, and out of the news cycle, with no shut-downs for mail security threats.

**RaySecur’s Explosive Ordnance Disposal (EOD) technicians are Navy EOD School graduates with a minimum of 8 years active duty service in a Team Leader role.*

Fortune 500 Manufacturer Security Team Left in the Lurch When Company Split



MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Manufacturing

CUSTOMER

Fortune 100
manufacturer with
over \$50 billion in
revenue

CHALLENGE

Quickly developing
a comprehensive
mail security
program

The X-ray mail scanner was lost in the divorce and being in a new headquarters didn't make matters any easier

CHALLENGE

This is a major company that went through a corporate split. They were in a new building with all new employees, but their X-ray mail scanner – and accompanying security procedures – had gone with the other half of the firm. They now had little or no mail security. And they knew that just acquiring a new X-ray scanner would still leave them vulnerable to small quantities of powders and liquids – the most common mail-borne threats today – which X-ray scanners can't detect.

To complicate things even more, their security was split between two layers of contractors: one for the facilities management and one for mailroom operations. This is not unusual in Fortune 500 companies; there is often the need to coordinate between many parties.

SOLUTION

The company was starting from scratch in its new headquarters; this actually can be a great opportunity to create the optimal mail security program. **RaySecur** security experts worked with the team to quickly develop mail security Standard Operating Procedures (SOP) that included processes, training, and technology for the entire organization. A **MailSecur** scanner was placed in a central location in the new headquarters that was convenient to both the offices and the loading dock. Due to **MailSecur's** ease of use, the **RaySecur** team trained the subcontractors on how to operate it in under an hour.



OUTCOME

The new mail security program effectively closed gaps in executive protection for the C-suite and general mail security for their new headquarters building.

The security team was so impressed with **MailSecur** that they now specify it for all new facilities and are implementing a plan for roll-out of the program to existing sites globally. The EP team continues their close collaboration with **RaySecur**. They regularly attend **RaySecur** quarterly security webinars to stay up to date on the latest threats and also receive **RaySecur's** monthly threat updates.

One of the Four Major National Crime Labs Faced a Constant Barrage of Mail-Borne Threats

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Law Enforcement

CUSTOMER

National
Law Enforcement
Crime Lab

CHALLENGE

Increasing security
for lab personnel
while they dealt
with potentially
dangerous materials

National crime lab thwarts daily arrival of mail-borne threats with MailSecur.

CHALLENGE

One of the most sophisticated law enforcement labs in the country had used every possible mail screening technology – except **MailSecur**. As a result, their mailroom personnel were unnecessarily faced with threats. Crazyes were regularly sending in threats that mailroom employees had to clear and open before directing it to the lab or administrative personnel.

Their X-ray mail scanners couldn't detect the most common threats: powders that often came in letters. Mailroom personnel were frequently exposed to potentially dangerous substances in letters and packages that they had no choice but to open.

SOLUTION

The agency procured a **MailSecur** mail scanner that was capable of detecting even small amounts of powders and liquids. Due to its small footprint and need for only a standard power outlet, **MailSecur** was up and running in a matter of minutes, and it took less than an hour to train the mailroom personnel on how to operate it.

The mailroom personnel like that **MailSecur** provides real-time video imaging. They can move the item around and rotate it to see if powders or other materials are moving about. Even a few grains of powder or drops of liquid are easily detected. And **MailSecur** can detect the items that X-ray scanners do, too, like pipe bombs.



OUTCOME

Now 100% of incoming letters and packages are screened in **MailSecur** before opening. The mail security gap is closed and the team leader feels that her people are safer and able to identify threats before they go beyond the mailroom.

G8 World Leader's Security Team Adds MailSecur to Its Arsenal of Security Tech

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Government

CUSTOMER

The security team
of a G8
world leader

CHALLENGE

Every piece of
mail sent to the
leaders of a major
democracy must be
safely opened

The G8 leader's security team has cut annual shutdowns due to mail-borne threats from 80 to zero.

CHALLENGE

Leaders of the world's major democracies are in uniquely vulnerable positions: they are highly visible, at any given time at least 40% of their electorate thinks that they're doing a lousy job, and their security teams have to open every piece of mail sent to them. The passage of a single, controversial bill can set off a whole new round of threats. World leaders have been sent everything from ricin to mail bombs. This G8 leader's team was no different, and in addition to protecting the leader they needed to protect the other ministers, too, without unduly endangering themselves personally.

Of course, they already had a sophisticated mail security program in place, and almost every conceivable type of screening equipment. But threats were still making it through because they lacked the unique ability of **MailSecur's** millimeter wave technology to detect tiny amounts of powders and liquids in an item as small as an envelope.

Following the passage of controversial legislation, this leader's security team was inundated with powder threats - hoaxes and legitimate threats such as cocaine, fentanyl, arsenic, chlorine, and sugar. This uptick in threats, which were undetected by the team's conventional screening technologies, resulted in disruptions to security operations over 80 times in one year.



SOLUTION

The security team quickly added **MailSecur** to their mail inspection routine. With its small footprint and safe mmWave technology, it was up and running in minutes and the team only needed about half an hour of training. While their X-ray mail scanner could still provide insights into the contents of very large boxes, they couldn't detect liquids and powders. **MailSecur** provided a superior view into the contents of the other 95% of mail items. Security team members now can rotate items and view their contents dynamically and record the video and images for sharing with other security team members and as evidence. They also take advantage of **MailSecur**'s integrated metal and radiation detectors to identify additional threats.

The team now feels far more secure before opening suspicious items on a downdraft table.

OUTCOME

The G8 leader's security team has cut annual shutdowns due to mail-borne threats from 80 to zero.

The security team is more effective and safer. They maintain a close relationship with **RaySecur**'s security experts. They are contributing sample images of real threats for **RaySecur** to use in the development of our AI models and will continue to collaborate on new products and capabilities.

MailSecur is now the G8 leader security team's standard for mail screening.

\$20B Chemical Company Chooses RaySecur for Its First-Ever Mail Security Program



MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY
Chemicals

CUSTOMER
North American
mining and
chemicals
processing
company with
>\$20B Revenue

CHALLENGE
Scaling up
a new mail
security program

A new global security head wanted to plug a major security gap in their mail program

CHALLENGE

This chemical and mining company has over \$20B in annual revenue and over 20,000 employees in locations across North America. The U.S. Department of Homeland Security defines chemicals as a high-risk industry for mail threats but the company didn't have a mail security program; their new head of global security knew that they needed one. While they were considering the purchase of **MailSecur** units, pipe bombs were discovered in one of the towns in which they operate. While not targeting the company, this reinforced the urgent need for a comprehensive mail security program.

The global security head was looking for a company that could provide a comprehensive solution including best practices, technology, and training. They wanted technology that had been Designated by the Department of Homeland Security under the SAFETY Act. They were concerned about the potentially heavy lift of rolling out a mail security program across the enterprise – and even more so when COVID hit.

SOLUTION

The **RaySecur** security experts, who include former U.S. Postal Inspectors and U.S. Army EOD threat experts, undertook a risk assessment of nine of the company's sites and developed a custom mail security Standard Operating Procedure (SOP). While the chemicals industry may be high-risk, the global security head did not feel that all of his sites were at equal risk. In developing the SOP, RaySecur security experts scored the sites based on a set of quantitative metrics, accounting for such factors as perceived threat, location, type of facility, access controls, number of employees, risk profile of employees on site, and similar criteria.



In parallel with the risk assessment, the customer conducted a 30-day pilot of the **MailSecur** scanner at their headquarters. Based on the successful pilot and results of the risk assessment, **MailSecur** scanners were deployed across all of their high and medium risk sites. Low-risk sites are using **RaySecur's** mobile **MailSecur Connect** app which walks all employees through the steps of visual and tactile screening, flags potentially high risk items, and ensures proper screening procedures are being followed at all sites. Most importantly, the app provides direct access back to **RaySecur's** threat experts should any employees require an expert second opinion when screening mail, regardless of whether they are using the **MailSecur** scanner. **RaySecur** also provided comprehensive, remote mail security training for their mailroom personnel via web meetings and our online courses.

OUTCOME

The chemical company now has a standardized mail security program across all locations, moving from 0% protection to 100% protection. They are in compliance with DHS mail security guidelines, scanning all of their mail for chemical, biological, radiological, explosive, dangerous goods, and hoax letters with a DHS Safety Act Designated technology. The **RaySecur** program provides them with 24/7 access to military-trained security experts to provide advice should an incident occur. Given their enterprise-wide rollout, the average cost of the program per site to implement a comprehensive mail security program is comparable to the price of renting a photocopier.

One of the Largest Hedge Funds Needs to Keep Their Hard-Charging Employees Safe

RAYSECUR™

MAILSECUR™
THE STANDARD IN MAIL SECURITY

INDUSTRY

Finance

CUSTOMER

Global Top Five
Hedge Fund

CHALLENGE

Keeping employees
secure in a large
campus with many
items coming in
every day

Traders and others in this high-risk industry spend a lot of time on site

CHALLENGE

Like employees at tech companies with a campus that becomes a second home, the traders and others working at this top-tier hedge fund spend a lot of time in the office and on the trading floor. And the Department of Homeland Security considers them to be a high-risk target for mail-borne attacks.

Keeping traders happy often means deskside delivery of personal shopping and e-commerce items to the office, and they even have an “internal Craigslist”. The company wants people to feel safe on site, but it poses a significant security challenge because the campus is quite large, yet all critical infrastructure is centralized.

The company had a nascent mail security program with visual and tactile inspections but no technology that could see into letters and packages.

SOLUTION

The company acquired a **MailSecur** scanner as their first-line mail screening technology. With **MailSecur** they could be up and running quickly and with no changes to their offices; their staff was trained in less than an hour. **MailSecur** satisfied their need for a DHS Designated technology under the SAFETY Act, which not only provided validation for the technology but limitations to their potential liability in the case of an incident.



Now they have much greater insight into the contents of a piece of mail and eliminate the vast majority of threats since 95% of threats come in small letters and packages that **MailSecur** can “see inside” of. Ultimately, they also acquired an X-ray mail scanner for inspection of the few large boxes, like some of those in their internal Craigslist exchange that don’t meet their chain of custody verification.

RaySecur security experts consulted to the company on their program, visited the campus to assess the mail workflow and mail screening program, and reviewed the company’s mail security standard operating procedures. They were alert to the potential of mail threats sent by insiders – disgruntled employees or others close to the company – and helped the company put in place measures to close those gaps in their mail security program.

OUTCOME

While some security people think that they should keep all of their efforts covert, this program is highly visible so as to discourage employees from attempting to send a mail-borne threat. Each piece of scanned mail is now stamped with the red “**MailSecur** Screened” stamp so people will know that the program is active – similar to the TSA pamphlets placed inside inspected luggage. Employees now know that their arriving mail and packages are safe, providing both peace of mind and yet another highly-valued benefit.



Members of the security team subscribe to **RaySecur’s** monthly threat alerts and routinely participate in **RaySecur’s** quarterly webinars so they can keep up with the latest developments in mail security.



www.raysecur.com | [617-855-9938](tel:617-855-9938) | info@raysecur.com