CACC Cargolinx Deploys Halcyon to Reduce Ransomware Risk & Impact

COMPANY PROFILE:

CACC Cargolinx, based in Egypt, is the region's leading cargo service provider for more than 25 major airlines. By continuously innovating its import, export, and express handling offerings for Cairo's International Airports, CACC Cargolinx has built a reputation as the leading cargo service provider. With over 30 years of experience, over 54,000 square meters of terminal capacity and servicing over 24,000 flights annually, CACC Cargolinx plays a vital role in ensuring the smooth movement of cargo to and from the region. CACC Cargolinx has established a series of state-of-the-art import, export and express cargo terminals that represent a new era of advanced logistics operations in the Egyptian market. With a highly dedicated team of professionals and world-class service standards.

BUSINESS CHALLENGE:

The company's ICT Operations & Security Manager, Alaa Osama, identified the escalating threat of ransomware as a critical risk to CACC Cargolinx's operations and reputation. The rise of sophisticated ransomware attacks posed severe risks to operational continuity, customer data integrity, and financial stability. Despite having an Endpoint Detection and Response (EDR) solution, Alaa was aware of EDR limitations in addressing targeted ransomware attacks that now include data exfiltration. While CACC Cargolinx has not experienced a ransomware incident, Alaa understands the importance of a proactive cybersecurity strategy. The existing cybersecurity stack, including email security, DLP, and EDR solutions, lacked a dedicated, purpose-built ransomware prevention and mitigation tool.

HOW HALCYON SOLVED THE PROBLEM:

CACC Cargolinx evaluated the Halcyon Anti-Ransomware Platform to address their ransomware security concerns. CACC Cargolinx thoroughly tested the ability to combat the impacts of ransomware attacks and data exfiltration, before, during, and after an attack.

First, CACC Cargolinx spent time evaluating the use of finely tuned machine learning models to stop applications, files, and processes showing ransomware characteristics from executing automatically. Next, CACC Cargolinx tested Halcyon's "during an attack" capabilities verifying its ability to detect applications, files, and processes demonstrating behaviors indicative of a ransomware attack and consequently disrupting their actions in real-time. Finally, CACC Cargolinx simulated ransomware encryption actions to test the platform's ability to capture encryption key material that enables data decryption without negotiating with the attackers to obtain the decryption key.

CACC CARGOLINX

Company/Industry

- CACC Cargolinx
- Logistics, Air Cargo Handling

Challenges

- Concern with evolving ransomware threats
- Needed to close gaps left by existing security stack
- Desire to show customers their forward-leaning security posture

Solutions

- Pre-execution ransomware prevention
- Targeted ransomware behavior detection
- Mitigation of ransomware-associated data exfiltration
- In-flight encryption key capture thwarting data encryption attempts
- Seamless integration with existing security stack
- Near zero footprint and low CPU resource utilization

An important factor in CACC Cargolinx's ultimate decision to select Halcyon was the 24x7 threat monitoring included with the platform free of charge. This monitoring, completed by a team of malware reversing engineers, cryptography experts, offensive security specialists, and others with highly specialized skills, is ready to take decisive action to keep the CACC Cargolinx environment secure if an attack is detected. To date, no Halcyon customer has had to negotiate with ransomware attackers to recover any data.

"The specialized capabilities Halcyon delivers filled a critical gap in CACC Cargolinx's cybersecurity ecosystem, providing advanced protection against the rising threat of ransomware attacks," Alaa noted. He continued, "The Halcyon team demonstrated exceptional expertise during the Proof-of-Concept phase, simulating ransomware attack scenarios to ensure compatibility with CACC Cargolinx's existing tools."

"We are committed to providing the highest level of security for our customers' data and ensuring the uninterrupted flow of air freight operations," said Alaa Osama. "This new system represents a significant step forward in our cybersecurity roadmap, providing robust protection against ransomware attacks and data breaches."

In less than a month Halcyon was seamlessly deployed across the CACC Cargolinx environment, enhancing security with minimal disruption. The solution integrated effectively with the existing EDR tools, offering greater visibility and more proactive threat management. Furthermore, Halcyon boosted customer confidence by highlighting a strong security posture, positioning CACC Cargolinx as a leader in logistics cybersecurity.

BUSINESS OUTCOMES:

Since deploying Halcyon, CACC Cargolinx significantly strengthened its ransomware security, addressing a critical gap in its cybersecurity stack with proactive ransomware prevention, detection, and data loss mitigation. The lightweight Halcyon solution integrates seamlessly into daily workflows, ensuring operational continuity without disruptions. Halcyon's adoption has also bolstered customer confidence, reinforcing trust among airline partners by showing a proactive approach to cybersecurity. The smooth deployment and exceptional ongoing support enhanced user satisfaction. "As we advance in our digitalization roadmap and prepare to expand our operations, Halcyon remains a cornerstone of our robust and forward-thinking security architecture," Alaa said.

The risk of a ransomware attack disrupting your organization's normal operations has never been higher. By incorporating the Halcyon Anti-Ransomware Platform into your security framework, you get the targeted ransomware security you need to ensure your organization can withstand any ransomware attack today, tomorrow, and in the future. To see Halcyon in action, visit **halcyon.ai** and **schedule a demonstration** today!

> "As we advance in our digitalization roadmap and prepare to expand our operations, Halcyon remains a cornerstone of our robust and forward-thinking security architecture."
>
> **Alaa Osama,**
> ICT Operations & Security Manager