



Healthcare Non-profit Uses Ocean to Protect Executives and Cut SoC Overhead

Oct, 2025



Executive Summary

Enterprises using Ocean Agentic Email Security gain an autonomous platform that delivers real-time protection against targeted attacks. Security teams see immediate impact: targeted attacks are stopped before users engage, SOC workload drops dramatically through automated triage and investigation, and employees are empowered with contextual AI guidance to make safer decisions every day.

Ocean's multi-agentic AI engine actively investigates emails instead of passively pattern-matching or anomaly-spotting. It correlates context, behavior, processes, identity, content, and intent across every email, attachment, and connected service to make explainable decisions in real time.

Client Overview

A 1,400-employee healthcare non-profit organization partnered with Ocean to evaluate whether AI-driven contextual analysis could strengthen email defense and reduce SOC burden. Despite deploying Cisco's Secure Email Gateway with IronPort technology under a multi-year contract, the organization continued experiencing:

- Sophisticated phishing attacks bypassing gateway filters and reaching executive inboxes
- QR code attacks exploiting Cisco's inability to analyze visual content
- Credential harvesting campaigns leveraging compromised Google Drive shares and HR impersonations
- Overwhelming SOC investigation workload from high false-positive alert volumes

The 3-week proof of concept, evaluating 45 days of historical and live email traffic, revealed a dramatic gap between pattern-based defenses and contextual AI. It provide an immediate impact on both risk reduction and operational efficiency.



Transforming Email Defense and SOC Efficiency with Ocean

Industry: Healthcare / Non-profit

Employees: 1,400

Current Defense: Microsoft + Cisco (multi-year contract)

695

Advanced threats that
bypassed Cisco

Sonar - AI SoC Analyst

1500

SOC analyst hours
saved annually

17

Executives protected from
targeted phishing

When pattern matching fails

Despite Cisco's IronPort, spear-phishing and BEC remained a persistent problem.

The fundamental limitation: Pattern-based systems cannot understand context.

Attacks leveraging QR codes, Google Drive, and HR impersonations regularly slipped through, overwhelming the SOC team with manual investigations and phishing reports.

Ocean's contextual understanding

Ocean was deployed alongside Cisco to analyze historical data and live traffic, applying its agentic AI reasoning engine to every email.

Unlike traditional pattern-matching systems, Ocean delivers true contextual understanding. It investigates every email like an expert security analyst on their best day. Rather than relying on pattern matching or statistical anomaly detection, Ocean actively gathers evidence, validates claims, and reasons through context to make decisions.

Immediate business impact

Within 3 weeks, Ocean uncovered 695 advanced threats that bypassed Cisco, out of 4,000 total threats detected.

70% of these threats reached inboxes, and 26% were engaged with (read, clicked, replied to, or attachment downloaded).

Ocean also reduced SOC triage response time to under 20 seconds per email, saving the organization over 1,500 analyst hours annually. This demonstrates the difference between a system that generates alerts and one that resolves them.

SOC Perspective

"Once we deployed Ocean, it immediately showed us what we already knew but couldn't manage with Cisco. Its contextual reasoning caught what pattern-based filters kept inconsistently missing. We thought another system would just create more noise, but it actually reduced the time we spend on email almost entirely. For us, it's the difference between a system that generates alerts and one that actually reduces risk."

CISO, Healthcare Non-Profit Organization



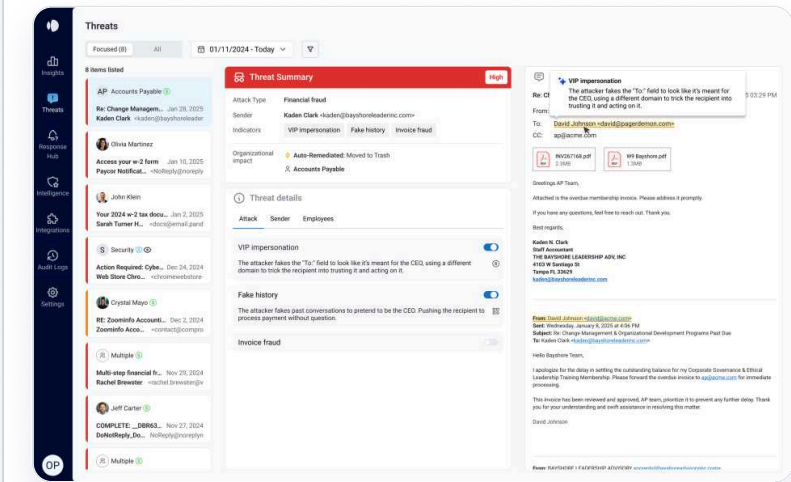
Bottom Line

In just three weeks, Ocean proved its impact. 695 sophisticated threats detected that bypassed Cisco, executive risk eliminated, and tens of analyst hours saved.

By moving from pattern matching to AI contextual understanding, Ocean empowered the SOC to achieve real risk reduction, real efficiency, and real transformation in email defense.

Ocean is now deployed in production as a second layer alongside Cisco and will become the primary email security platform within a year. Beyond threat detection, it has evolved into the company's central control point for all email operations from investigating business cases to managing workflows and accessing new functionality.

About Ocean



The screenshot displays the Ocean Threats interface. On the left, a sidebar lists various threat categories like 'Threats', 'Investigate', 'Intelligence', 'Integrations', 'Audit Logs', and 'Settings'. The main area shows a list of threats, with one selected: 'VIP Impersonation'. The detailed view on the right shows the threat's attack type (Financial Fraud), sender (Kaden Clark), and a warning that the attacker is impersonating a VIP. It also shows the threat's details, including the attack, sender, and employees involved, and a 'Threat Summary' section with a 'Threat Details' table.

Ocean's Advantage

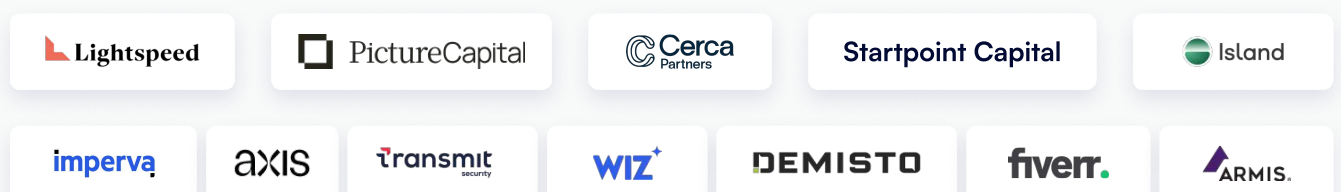
- Protection from targeted attacks
- Significant analyst time reduction
- World-class threat intelligence
- One UI, No configurations
- Integrates in seconds via API
- Read-only evaluation

The Team

Ocean is practitioner-built, combining offensive social engineering expertise with agentic AI to secure enterprise email.

Founded by Israeli Ministry of Defense veterans and backed by top VCs, Ocean brings unmatched credibility to email security.

Backed by top tier VCs and cybersecurity founders



Want to Learn More?

Schedule a short meeting to learn more via the [following link](#).