



Global Fortune 500 Healthcare Uses Ocean to Protect From Targeted Attacks and Cut SoC Overhead

Nov, 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 global healthcare organization with 120,000 employees, partnered with Ocean to address critical gaps in their Microsoft E5 defenses and eliminate unsustainable SOC overhead. Despite significant investment in Microsoft security and automation tools including SOAR, the organization continued experiencing:

- SOC analysts spend 40% of their time reviewing emails that ultimately prove to be benign
- 2,000—3,000 phishing reports weekly, with over 90% ultimately identified as safe or spam
- Quarantine backlogs disrupt business operations and frustrate executives
- Targeted attacks bypass Microsoft defenses, including BEC, phishing emails from abused third parties (e.g., DocuSign), QR codes embedded in PDFs, and fake conversation histories

Ocean's deployment delivered immediate operational transformation and measurable risk reduction, generating a **460% ROI** in the first year.



Transforming Email Defense and SOC Efficiency with Ocean

Industry: Healthcare

Employees: 120,000 employees (150K inboxes)

Current Defense: Microsoft E5

4,800

Threats bypassing Microsoft
& detected monthly

AI SoC Analyst

45,000

SOC/IT hours
saved annually (22 FTEs)

3,000

Legitimate emails auto-
released from E5 quarantine

Microsoft isn't enough

Despite Microsoft E5 and SOAR automations, targeted threats continued reaching inboxes.

The fundamental limitation: Analysts could not trust static policies or automated verdicts. Tightening policies led to an increased volume of legitimate business emails being misclassified and blocked. With over 90% of reported emails ultimately benign, the SOC still had to manually verify each one, spending 15–24 minutes per email. The superficial analysis provided by SOAR solutions could not definitively confirm email safety.

Meanwhile, Microsoft's quarantine created a separate crisis: the Office 365 team was buried in manual release requests, causing delays to legitimate business traffic and frustrating executives who demanded immediate action. Critical threats like BEC attacks, QR codes embedded in PDFs, and emails with fake conversation history consistently slipped through.

Ocean's contextual understanding

Ocean was deployed alongside Microsoft to block missed attacks and assume full responsibility for user-reported email triage and quarantine processing, applying its agentic AI reasoning engine to every email.

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

Immediate business impact

Ocean's Agentic Email Security transformed SOC operations within weeks. Each month, it processed 8,640 user-reported phishing emails—automatically releasing benign messages and escalating only the 4% confirmed as malicious. The platform also handled ~3,500 quarantine release requests, blocking 17% of malicious emails that users attempted to un-quarantine. Response times dropped to under one minute, delivering a white-glove experience that increased employee engagement.

On threat detection, Ocean identified approximately 4,800 threats bypassing Microsoft monthly and prevented over 50 targeted BEC and spear-phishing attacks.

The result: Over 96% reduction in email security workload - ~45,000 analyst hours saved annually, equivalent to 22 FTEs, while eliminating targeted email attacks.



SOC Perspective

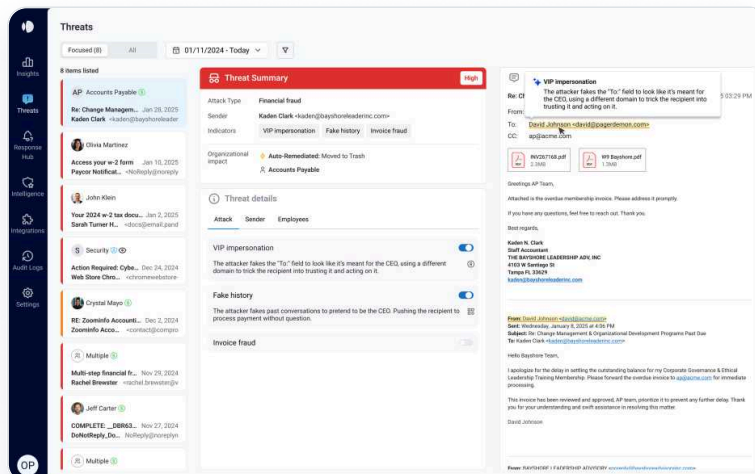
“We knew we had a problem, our time was going to emails that didn't matter. Ocean didn't just reduce that burden, it eliminated it. The automations alone justified the investment by getting executives their legitimate emails instantly while stopping the bad ones. Our team can focus on meaningful work now, instead of chasing email reviews”

Head of Global Cyber Security Operations and Incident Response

Bottom Line

Ocean delivers a 4.5× ROI, detecting 4,800 targeted threats per month that bypassed E5, including 50+ BEC and spear-phishing attacks prevented. At the same time, Ocean automatically released 3,000 legitimate emails per month and processed 8,460 phishing reports monthly, returning 45,000 SOC/IT hours to meaningful security work and streamlining business communications.

About Ocean



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](#).