

Gaviota Group

118

threats contained automatically.

799

investigations automated; only 38 needed review.

24k+

inbound and 13k+ outbound emails kept clean weekly.

Gaviota Simbac is a Spanish manufacturer operating across 15+ countries, producing solar protection systems and enclosures, and relying on Darktrace to secure its decentralized global infrastructure.

Adapting to a complex and evolving threat landscape

For Sergio Soriano, Head of Systems, Communications, and Cybersecurity, safeguarding Gaviota's operations means protecting every link in a complex international supply chain. The organization's distributed workforce, remote sites, and constant data exchange make it a target for increasingly sophisticated attacks.

Phishing was one of the most persistent threats. With thousands of messages moving through the network each day, email had become the most common entry point for fraud attempts and credential theft.

One of Gaviota's ongoing challenges was user awareness. With staff working in different countries and environments, education took time — and users often clicked before thinking. Soriano needed a system that could support people in real time, catching risky actions before they turned into incidents.

“We didn't have someone watching systems around the clock,” notes Soriano. “We needed technology we could trust to act immediately.”

■ Sergio Soriano

General Manager, Information Systems Department,
Corporate Administration Division, Gaviota Group

From manual oversight to autonomous defense

Before adopting Darktrace, Gaviota relied on traditional perimeter tools and manual monitoring. The IT team handled alerts as they appeared but lacked real-time visibility across a growing infrastructure.

After learning about the solution, Soriano decided to run a free trial of Darktrace / NETWORK. The deployment process took less than an hour and demonstrated tangible value. The ability to block a single port with surgical precision — while keeping the rest of the network running — showed how Darktrace's Autonomous Response could deliver control and agility at the same time.

Encouraged by these results, Gaviota expanded its protection to Darktrace / EMAIL in 2023 and, most recently, to Darktrace / ENDPOINT. Today, the company operates a layered AI-driven defense built on visibility, automation, and continuous learning.

Stopping phishing before it reaches the inbox

With Darktrace / EMAIL, Gaviota has achieved a new level of precision in detecting and neutralizing email threats. The system uses Self-Learning AI to understand normal communication patterns for each user and spot anomalies in real time, stopping attacks before they reach employees.

For a manufacturing company operating across multiple regions, even a single missed phishing email could lead to downtime, fraud, or data compromise.

Darktrace's impact can be clearly seen across everyday email activity:

- Spam and malicious links no longer reach end users.
- Attachments flagged as potentially dangerous are automatically blocked.
- CEO-fraud and impersonation attempts are intercepted before causing disruption.

"In a single week we can receive more than 24,000 incoming emails and send over 13,000. Since implementing Darktrace, those messages are clean — no spam, no suspicious links. The system blocks everything that could pose a risk."

He also underscores the importance of protecting outbound communication. The tool identifies when users attempt to share sensitive information externally, preventing data-loss incidents that could carry financial or reputational consequences.

"We've had cases where Darktrace detected attempted data transfers and stopped them immediately, and those events helped us refine our internal security policies."

(*) Metrics are based on the customer's interview, data and sourced from its monthly Cyber AI Insights reporting.

Visibility, precision and measurable impact

At the system level, Darktrace / NETWORK provides continuous oversight of every connected device. Between August and November 2025, 118 anomalous behaviors were contained before they escalated — stopping issues that could have disrupted operations or required manual intervention.

By automating this analysis, Darktrace reduced a significant portion of manual triage work, allowing the team to spend more time on strategic initiatives rather than chasing routine alerts.

Darktrace's Cyber AI Analyst™ carried out 799 investigations on behalf of the security team, with only 38 of them being genuine incidents that required human review.

Soriano emphasizes that this balance — automation backed by human oversight — is what makes the solution so effective.

"Darktrace gives us peace of mind," he says. "We don't have to watch every alert, because we know the system will detect, investigate, and respond in seconds."

The implementation has also strengthened Gaviota's overall resilience. Darktrace supports users, reinforces internal policies, and helps the organization maintain its security posture without expanding the team — a critical advantage for a company with widely distributed operations.

Looking ahead

Gaviota continues to invest in AI-driven defenses as it expands into new markets. For Soriano, the next step is deepening the integration of Darktrace technologies across endpoints and cloud services, ensuring consistent protection across every layer of the business.

"Cybersecurity is about balance," he concludes. "You can't stop working to stay safe — you need solutions that let you do both. With Darktrace, that's what we have."



■ About Darktrace

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit www.darktrace.com.