CASE STUDY

Keelings

INDUSTRY	HEADQUARTERS	EMPLOYEES	MAIL STACK	DEPLOYED
Fresh produce	Dublin, Ireland	2,700+	M365 + Mimecast	January 2026

Company Intro

Keelings is a 100% Irish-owned, third-generation family business that has been growing, sourcing, and distributing fresh produce since 1926. The company farms over 3,000 hectares across Ireland, Costa Rica, and Brazil, sources from 46 countries, and supplies more than 1,000 customers worldwide, with operations spanning **fresh fruit, vegetables, flowers, and ERP software solutions**.

The Problem

Keelings' IT security stack relied on Mimecast as a gateway filter, and it did that job well, catching bulk spam and known threats before they reached employee inboxes. But a different class of attack was getting through, and those were the ones that mattered most. CEO impersonation emails were reaching employee inboxes. On at least four separate occasions, well-crafted messages impersonating the chief executive led to gift voucher purchases.

The incident response process highlighted the gap. When a suspicious email was reported, the team had to manually search gateway logs, identify every recipient, send individual warnings, and hope people deleted the message. The rise of AI-generated phishing made the problem worse: the old giveaway signs were disappearing. Keelings needed something that could learn and adapt, not just match patterns.

Warwick Botwright evaluated four vendors alongside Mimecast's own advanced offering. Concerns over a journal-based, mirrored-mail architecture ruled out a key finalist. IRONSCALES connected via API in minutes and, during a read-only proof of concept, flagged a live CEO impersonation email. That single moment validated the investment.

> ***"It's about as close to 'set it and forget it' as you can get, especially compared to the daily management a traditional gateway requires with all its rules and policies."***

Warwick Botwright
Group Head of IT Infrastructure, Security and Operations, Keelings

The Solution

IRONSCALES went active in January 2026, deployed alongside Mimecast with no changes to mail flow. The API-based integration connected directly to Microsoft 365, giving the platform visibility into every mailbox without adding routing complexity or a new point of failure. From the moment of connection, Adaptive AI began building behavioral profiles for every mailbox user, learning who they communicate with so it could flag the anomalies the gateway was missing.

Challenges

- **CEO impersonation attacks bypassed the SEG** on multiple occasions, resulting in gift voucher fraud that even security-aware staff missed.
- **Manual, time-consuming incident response:** search gateway logs, identify recipients, email warnings individually, hope they comply.
- **A rule-based SEG required constant tuning** and offered no adaptive intelligence against AI-generated threats.

Solution

- **IRONSCALES cloud email security** deployed alongside Mimecast as an AI-powered post-delivery protection layer.
- **API-based integration with Microsoft 365**, with no mail flow changes and no additional hops.
- **Adaptive AI (Themis)** for automated detection and remediation.
- **IRONSCALES report phishing button** deployed to all Outlook users.

Results (First 90 Days)

- **3.5M emails monitored;** 584 email attacks automatically remediated.
- **20 VIP targets actively attacked** with 114 dedicated BEC and phishing attempts.
- **742 exact display name impersonation** attempts caught.
- **76.1K spam emails detected and removed** after enabling adaptive filtering.
- **224% increase in threat visibility** vs. prior 90-day period.

The team ran IRONSCALES in read-only mode during the proof of concept, then transitioned to active remediation. When they flipped the switch, not a single employee noticed. No complaints, no disruption, no pushback. The daily quarantine digest replaced what had been a manual process of chasing down recipients one by one.

Messages that users used to open, evaluate, and delete manually, roughly 30 to 35 per day in some cases, were now handled automatically. What used to take 20 minutes of someone's day now takes 15 seconds scanning a single summary email.

On February 5, the team enabled adaptive spam filtering. Detection volume jumped from near-zero to over 7,500 emails per week, then stabilized as the models tuned to Keelings' mail patterns. The report phishing button, deployed across all Outlook installations, drew 65 organic employee reports in the first 90 days with no formal training.

Keelings

"When we activated it, nobody noticed across the business. We activated banners, sent communications. No negative feedback. And that's quite refreshing."

Warwick Botwright
Group Head of IT Infrastructure, Security and Operations, Keelings

The Outcome

In its first 90 days, IRONSCALES reshaped email security at Keelings:

- **Threat Visibility:** 3.5 million emails monitored and 584 attacks automatically remediated, a 224% increase over the prior 90-day period.
- **Impersonation Caught:** 1,235 mailbox anomalies identified, including 742 exact display name impersonation attempts, the technique behind prior gift voucher fraud.
- **VIP Protection:** 20 employees flagged as VIP targets were actively attacked with 114 dedicated BEC and phishing attempts.
- **Zero Tuning:** no rule tuning, no policy updates, no constant feeding and watering.
- **Reversible Remediation:** 1,500 copies of a misreported HR notification removed and instantly restored, with no user disruption.
- **Organic Adoption:** 65 employee phishing reports in 90 days with no training or awareness campaign.

Compared to segment peers, Keelings faces 37% more phishing attempts, validating the decision to add dedicated AI protection beyond the SEG. The agentic SOC engine resolves the majority of incidents automatically, escalating only what requires human judgment.

90-DAY METRICS

3.5M	584	76.1K	+224%
EMAILS MONITORED	ATTACKS REMEDIATED	SPAM REMOVED	THREAT VISIBILITY

"

It's so reversible on any mistake you make. Nobody notices, because it just drops straight back into people's mailboxes.

Warwick Botwright
Group Head of IT Infrastructure, Security and Operations, Keelings

Learn more about Keelings at www.keelings.com