

IronScales Secured The Email For A Global Retailer

ORVIS®

Challenges

- No IT staff in stores and many untrained users
- Phishing number one threat vector
- Users experiencing “banner fatigue”
- Legacy email security unable to spot sophisticated threats

Solution

- IRONSCALES- the AI-driven, self-learning email security platform
- Phishing training and simulation platform

Results (Weekly)

- Of 351 active phishing incidents, 92.3% were automatically remediated by IRONSCALES
- In a single week, IRONSCALES inspected 277,000 emails, found 4,000 to be suspicious, and grouped 372 incidents, with only one false positive
- Click rate down to 1.5%
- False positives less than 1%

“As a retailer, we have a large number of locations far from the corporate HQ. The farther you are from the headquarters, the looser things can become from a cybersecurity perspective. Around October, these ‘looser’ environments double in size as we hire new people for the holiday season. I was looking to enhance our email threat detection capabilities while driving an improved user experience for staff.”

JOE MINIERI, CISO AT THE ORVIS COMPANY

About Orvis

Orvis is a family-owned retailer, specializing in fly fishing gear, hunting equipment, sporting goods, and men’s and women’s clothing. Founded in 1856, the Vermont headquartered business now has around a hundred stores across the US and UK, along with a major e-commerce presence. Joe Minieri is the Chief Information Security Officer (CISO) at Orvis and is responsible for cybersecurity as well as fraud and loss prevention.

The Problem

Phishing is still the number one threat vector¹ for cyber attacks and present in 90% of breaches². In retail, the median click rate for malicious emails is said to be nearly 11%, giving attackers plenty of opportunities to hijack employees’ inboxes, steal corporate and customer data, and deploy ransomware. The challenge was amplified by the large number of new and temporary Orvis store employees that may not be on staff long enough to receive security awareness training. If just one of these workers falls for just one malicious email it could have serious repercussions for their employer. Orvis doesn’t deploy IT staff to individual stores and relies on service providers to augment IT & security on the ground. The key for the company was to reduce cyber risk by enhancing its email security capabilities. Prior to deploying IRONSCALES, Orvis used a legacy signature detection technology. The former solution did an adequate job with catching common threats but could not identify or stop advanced phishing attacks.



“We got to the end of deployment and were successfully detecting and quarantining malicious emails, I realized that we’d never even put any whitelisting in place. We don’t have any email that comes into the environment that hasn’t at least been inspected by IRONSCALES, which was one of the biggest things I wanted to do here. I’m very happy with it.”

JOE MINIERI, CISO AT THE ORVIS COMPANY

The original solution also relied heavily on whitelist functionality to filter emails—a setup which meant many messages weren’t scanned at all before being allowed through. On the user awareness side, the original solution could only produce a generic warning banner indicating the email originated from outside the company. The early warning banners were ineffective, as employees simply started ignoring them over time.

Orvis was therefore looking for a more agile, intelligent email security solution capable of detecting and stopping sophisticated threats in real time while offering greater capabilities to improve end user awareness of potential email threats.

Solution

Orvis began working with IRONSCALES at the start of 2021 following a proof-of-value test in November 2020. IRONSCALES’ AI-powered technology is designed to detect and remediate in real-time advanced email threats like BEC, credential harvesting and account takeover. Also featured are dynamic warning banners which only notify users when there’s a potential threat—overcoming the challenge of banner fatigue. Deployment couldn’t have been simpler: the solution was put in place alongside the company’s previous email security product with no impact on IT or end users. After fine-tuning IRONSCALES to minimize spam without blocking legitimate mail, Minieri was delighted with the end result.

Alongside the email protection comes IRONSCALES’ phishing simulation and training capabilities. Orvis has already begun testing staff with several simulation exercises, and couples this with awareness bulletins to reinforce lessons learned.

Outcomes

Since deploying IRONSCALES, Orvis has experienced improved ease of management, stronger threat protection (with extremely low false positive rates) and enhanced user awareness. Minieri can access notifications and manage email incidents with ease via an iPhone app while IRONSCALES automatically blocks and resolves over 90% of issues, providing simple-to-view threat data via an intuitive UI. Similar email threats, common with polymorphic phishing email attacks, are grouped together into an incident, making it easier for Orvis to clean up and manage them afterwards.

Most importantly, IRONSCALES is blocking more malicious and spam emails than the previous solution, and Orvis has had no infected PCs in the past year. On the training side, users are responding positively to Minieri’s phishing simulations and follow-up emails. The click rate for phishing is now down to an impressive 1.5%.

Solution Brief: Solution Name Here





I recommend IRONSCALES all the time. The thing that gets people really excited, especially the end users, is the smart banners.”

JOE MINIERI, CISO AT THE ORVIS COMPANY

IRONSCALES has definitely increased productivity and saved us time and money. Our end users are exposed to fewer malicious emails, so it is less likely that they will make a mistake. The phishing simulation and security awareness training equip that user to make the right decision if they do encounter a malicious email.”

JOE MINIERI, CISO AT THE ORVIS COMPANY

Looking Ahead

Going forward, Orvis continues to tweak the IRONSCALES platform to further reduce the number of suspicious emails that must be manually checked by IT. The firm is also keen to plan more regular simulation exercises—to keep the threat of phishing at the forefront of employees’ minds.

About IRONSCALES

Every day criminals launch billions of new phishing attacks. No company is immune. Legacy solutions can’t keep up & cloud providers struggle to stop advanced attacks with native controls. IRONSCALES’ powerfully simple email security solution helps you fight back fast and keeps your company safe in today’s cloud-first world. Incubated inside the world’s top venture program for cybersecurity and founded by alumni of the Israeli Defense Forces’ elite Intelligence Technology unit, we offer security professionals an AI-driven, self-learning email security platform that provides a comprehensive solution to proactively fight phishing attacks.

¹ <https://securityintelligence.com/series/ibm-x-force-threat-intelligence-index-2020/>

² <https://www.graphus.ai/blog/verizon-says-phishing-still-drives-90-of-cybersecurity-breaches/>

www.srccybersolutions.com | +91 120 232 0960 / 1 | sales@srccybersolutions.com   

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide NexGen, Highly Automated and User-Friendly solutions in partnership with IRONSCALES with the POWER OF NOW for Comprehensive NexGen Email Security, THREATX for NexGen WAAP (WAFF++) with an Attack-Centric approach and Cyber Security Training with Project Ares by CIRCADENCE CORPORATION for Online Simulation based Cyber Security Training.

ARPR Case Study

