

# Real-time URL and Malware Protection

Identify and respond to modern attacks at scale



of malware  
is delivered  
by email



Increasingly sophisticated email attacks like credential harvesting are becoming more common and are able to trick unsuspecting users on a regular basis. Outdated email security technologies can't keep up, leaving companies exposed.

## Detect Email Threats That Bypass Your SEG

Secure Email Gateways (SEGs) rely on signatures of known threats to perform detection. Polymorphic variants make it nearly impossible for these older technologies to identify every possible attack. Our service protects in the mailbox with a combination of sandboxing, multiple anti-virus engines and proprietary, real-time threat intelligence.

“With banners, warnings and intuitive self-management, it's easy to prove that IRONSCALES is protecting our company... and to easily demonstrate that our email security system is secure.

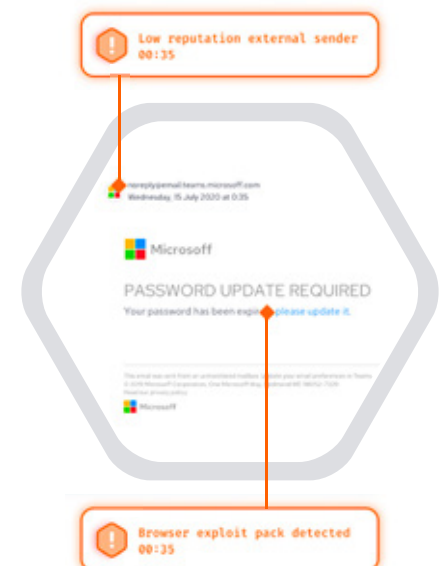
NEIL STEIN, SVP OF TECHNOLOGY SERVICES  
AT ORTHOCAROLINA

## The Challenge

Email security is the biggest challenge your company is facing. Modern email threats are designed to bypass legacy technologies like Security Email Gateways (SEGs). Modern criminals are using a combination of bad links and fake login pages to lure victims into giving up their user credentials and other personal details.

## The Solution

A new approach to email security that leverages AI/ML and computer vision is needed to defend against today's highly sophisticated types of email attacks. IRONSCALES' mailbox-level protection incorporates sandboxing, multiple anti-virus (AV) engines, computer vision, AI/ML, proprietary real-time threat intelligence and input from our user Community to defend against polymorphic email attacks.



## Protect against advanced URL attacks

Leveraging computer vision and neural network technology, our platform goes beyond traditional solutions to detect and block spoofed websites and brands in real-time. Our URL and malware protection technology defends against credential theft and phishing malware with:

- Real-time identity profiling and scoring of internal and external senders
- Continuous monitoring of communication patterns to detect anomalies
- Computer vision and deep learning to block fake login pages in real-time

## Comprehensive Malware Protection

We deliver sandbox and antivirus integrations out of the box that can complement or replace your existing protection engines. We offer a single dashboard that details results of URL and link monitoring that supports detection, analysis and remediation.

## Proactive Ransomware Prevention

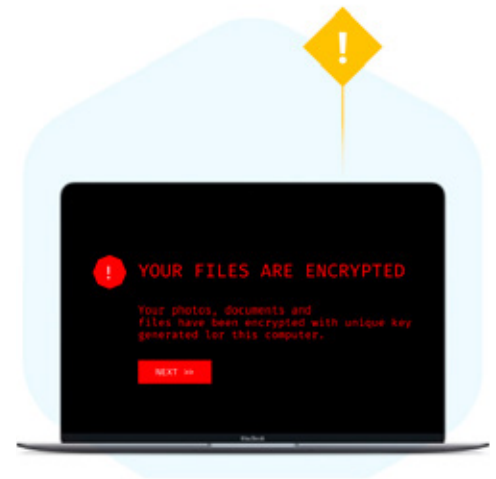
Ransomware attacks constantly evolve in order to slip past legacy defenses. Attackers may even delay the execution of weaponized links or remain dormant in your network, just watching and waiting for the right moment to strike. Continuous monitoring of your inboxes is the only true path to protection. We combine behavioral analysis with ongoing, automated inspections of links and attachments to anticipate and prevent future attacks.

### Why choose IRONSCALES?

1. We are fast to deploy, simple to manage and highly effective in stopping all types of email attacks
2. We deliver email security in the mailbox and defend against modern email threats
3. We integrate both email security and awareness training into a single offering

“Since implementation a year and a half ago, IRONSCALES has reduced the amount of phishing emails getting through our email security systems by 99%.

STEPHANIE MCKEE,  
DIRECTOR OF TECHNOLOGY  
ENGAGEMENT AT APPARO



[www.srccybersolutions.com](http://www.srccybersolutions.com) | +91 120 232 0960 / 1 | [sales@srccybersolutions.com](mailto:sales@srccybersolutions.com)



## ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

