

Solution Brief

# Business Email Compromise Protection

Prevent and Detect BEC in the mailbox



The FBI estimates that there have been over \$26 Billion in losses from BEC just since 2016. Legacy email security technologies aren't built to stop these kinds of attacks and the criminals know it.

## Unique fingerprinting technology helps you to see and act

Our hybrid human intelligence (HI) and machine learning (AI) solution works in real-time to answer a simple, yet very complicated question: Who is sending what?

## Go beyond DMARC




By examining the sender's IP address, historical communications, and other metadata, IRONSCALES develops an individualized fingerprint for each sender. Our solution also inspects DMARC implementation, Sender Policy Framework (SPF), and Domain Keys Identified Mail (DKIM) to round out each sender's fingerprint. Only then can you determine the sender's true identity, the content, and context of the communication. IRONSCALES authenticates all emails and automatically flags suspicious emails. End-users can make smarter and quicker decisions regarding emails with one-click.

## The Challenge

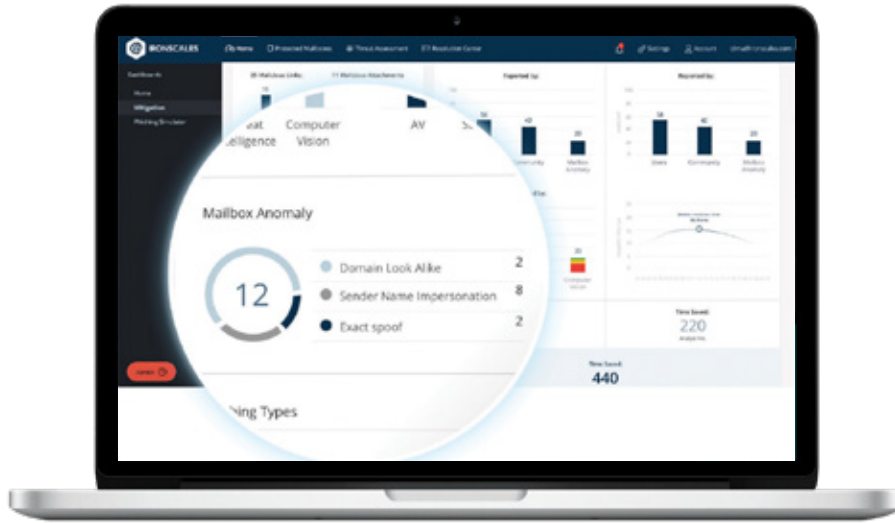
Email is insecure by default. Unfortunately, even newer protocols like DMARC don't go deep enough to confirm users' identities, email content, or links. Secure email gateways (SEGs) struggle to protect against business email compromise (BEC) attacks. SEGs do not operate at the mailbox-level and cannot review previous communications for sender recipient anomalies, but rather rely heavily on lists of known malicious email domains to filter emails.

## The Solution

IRONSCALES' powerfully simple email security solution helps you fight back fast and keeps your company safe in today's cloud-first world.

-  Unique fingerprinting technology helps you to see and act
-  We go beyond DMARC to provide true protection against BEC
-  Our solution identifies and stops non-signature-based threats





“People used to send me emails all the time asking ‘Should I open this?’ With IRONSCALES this doesn’t happen anymore. The solution is a huge time saver.”

IT MANAGER, FINANCIAL SERVICES COMPANY

## Identify And Stop Non-Signature-Based Threats

Our platform leverages patented machine learning algorithms and deep scans at the mailbox-level to identify advanced threats. These capabilities, combined with ongoing user behavioral analysis (people, relationships, and end-user behavior) helps to combat against impersonation and spoofing proactively.

### 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



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

## 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.

