Anti-Phishing Requires A Three-Pronged Strategy: **technical controls, end-user controls and process automation.**

IRONSCALES
World's 1st *Automated Phishing* Prevention, Detection & Response Platform

Executive Summary

Email phishing remains the most commonly exploited attack vector despite many organizations making significant financial investments in phishing awareness training, DMARC and gateway-level email security tools. According to research from CyberDB, 156 million phishing emails are sent out every day and email users receive up to 20 phishing emails each month.

This whitepaper explores how modern phishing techniques, such as business email compromise (BEC), ransomware, spear-phishing and advanced persistent threats (APTs) are meticulously designed to defeat traditional email security approaches and how IRONSCALES' advanced threat protection platform is uniquely built to addresses the contemporary techniques of phishers.

Key Takeaways

After reading this whitepaper, CISOs, SOC teams and IT security professionals will have an understanding for how IRONSCALES' anti-email phishing platform:

1. Detects and responds to phishing emails that bypass traditional email security, minimizing risk, workplace disruption and ensuring business continuity.
2. Reduces SOC workload burden by combining automation, orchestration and rapid response into a repeatable workflow.
3. Closes the gap between end-users and technology by creating a human-centric feedback loop that strengthens detection and response of suspect emails.
4. Decentralizes intelligence by anonymously leveraging user-led email threat sharing of emerging phishing campaigns.
5. Is deployed on-premises, via the cloud or as a hybrid and seamlessly integrates natively into O365 or G Suite as a standalone platform or as a complement to email security tools already in use.

Why is Email Phishing Still so Successful?

1. Sender impersonation is very easy, as the email protocol was not designed to truly authenticate sender identity.

2. Efforts like DMARC to authenticate domains are not granular enough to authenticate users and do not address all attack types.

3. The proliferation of highly-targeted phishing schemes is overwhelming to SOC and security teams, who stand no chance to detect and respond quickly enough to every attack without the proper workflow for dealing with suspect emails.

4. Gaps in email security exist because humans and technology have traditionally operated in silos, leaving gapping vulnerabilities for phishing attacks to exploit.

5. Most implemented secure email gateways (SEGs) are not designed with post-delivery detection and remediation techniques, costing incident responders and email admins time while also reducing the feedback loop from end users.

IRONSCALES analyzed data of more than 2 million mailboxes across four continents to better understand trends in email phishing, attacker patterns, phishing tools & techniques, and hacker preferences. In total, more than 7,500 human verified attacks that bypassed other counter measures like SEG were evaluated. Of those attacks:

- **For every 5 brand spoofed attacks** (Like Paypal or DHL) identified by email filters, approximately 20 spear-phishing attacks bypassed the safeguard of email filters and went undetected into the mailbox.
- **One-third (33%)** of attacks targeted just one mailbox.
- **Almost 95% of email phishing attacks** were highly-targeted campaigns, with the majority impersonating internal communications teams or individuals (i.e. CEO fraud).

Vulnerabilities of Existing Email Security Tools

1. Humans are not prompted with indicators of compromise to detect attacks missed by technical controls, leaving gaps in dealing with suspicious emails.
2. There is no post email-delivery threat detection that is supported by an automated workflow consisting of threat analysis and rapid response, costing incident responders and email admins valuable time.
3. A lack of real-time user-lead email threat intelligence (both human and machine) to mitigate and resolve emerging phishing campaigns.
4. Tools are not easy to use, unified, integrated and orchestrated into a single platform.
5. End-users are not integrated into most email security workflows, which reduces the feedback loop from end users.

The Email Threat Landscape is Changing

IRONSCALES has developed the world's first multi-layered anti-phishing platform to automatically prevent, detect and respond rapidly to today's advanced phishing threats. The platform combines human intelligence with advanced machine learning to help organizations limit risk from specific phishing attacks, including those with:

Malicious Attachments
(malware and ransomware)

URL's in email body or attachment
(malware, credential theft or ransomware)

Business Email Compromise (BEC)
(Spoofing & Impersonation)

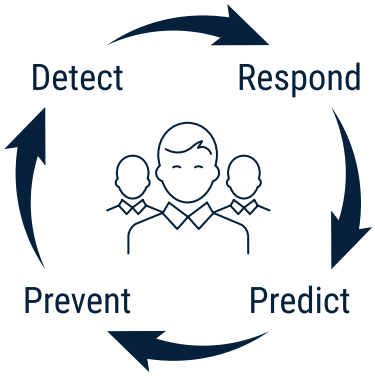
Reduce Risk with Multi-Layered Human Centric Threat Protection

Anti-phishing requires a three-pronged strategy: technical controls, end-user controls and process automation.

> *"Use technical controls to block as many phishing attacks as possible. But make users an active part of the defense strategy."* ----- Gartner

A best practice of email security is to always assume one control will always fail and that another is prepared to cover for it. IRONSCALES has built the world's first multi-layered platform to detect, prevent and respond to phishing attacks at any stage (pre and post-delivery) in the form of rapid incident response.

The IRONSCALES platform combines human centric detection, mailbox intelligence, user-led anonymous intelligence sharing and rapid response inside of an automated, adaptive and repeatable workflow.



The Layers of the IRONSCALES Platform

Layer 1: Attack Simulation and Awareness Training

IronSchool

IronSchool is a customized micro-learning method to help employees to think and act as a virtual SOC response team members, becoming proactive against malware attacks. Our gamified, interactive micro-learning method is customized to each employee based on an initial assessment of users phishing recognition and classification skills.

Layer 2: Advanced Malware and URL/Link Protection

IronShield

IronShield is a cloud-based email protection module that helps protect organizations from zero-day malware and phishing websites by providing real-time protection against all inbound emails, using various multi AV and Sandbox engines.

Layer 3: Advanced Protection Against Business Email Compromise (BEC)

IronSights

IronSights prevents email spoofing and impersonation attacks in real-time by combining smart fingerprinting with trusted relationships to determine what is normal user behavior and communication habits. Using machine learning algorithms, IronSights continuously studies every employee's inbox to detect anomalies based on a first-of-its-kind sender fingerprint technology, which can identify the authenticity of a sender based on both email data and metadata extracted from previously trusted communications.

Layer 4: Automated Email Phishing Investigation, Orchestration & Response

IronTraps

IronTraps streamlines phishing incident response by conducting email phishing investigation, threat intelligence gathering (forensics), orchestration and rapid response automatically or at the click of a button. This process eliminates the need for an army of highly trained SOC or security analysts to manually deal with the continuous growth of daily reported email threats incidents, reducing the time from detection to remediation from weeks or months to just seconds.

Layer 5: An AI-Driven Virtual Security Analyst

Themis

Themis is an AI-driven virtual security analyst that helps security teams determine a verdict on suspicious email incidents in real-time. By mimicking security analyst's decision-making criteria, Themis can predict with high-confidence the legitimacy of any suspicious email, improving the efficiency of email phishing classification and expediting the resolution of confirmed phishing threats.

Layer 6: Automated & Collaborative Phishing Campaign Detection

Federation

Federation offers real-time human verified actionable collaboration, integrated with automated incident response, as a means to better prepare and respond to new attacks before they target other employees' or other companies' inboxes. By decentralizing and distributing threat intelligence automatically, companies around the world can implement proactive phishing protection to defend against unknown threats that have already been verified by other security experts within the Federation community.

IRONSCALES Anti-Phishing Platform VS. Secure Email Gateways

● YES ● NO ○ PARTIAL

	IRONSCALES	Microsoft ATP	Proofpoint	Symantec	Cisco	Mimecast
Advanced Anti-phishing Threat Detection						
Mailbox-level Behavioral Analysis	●	●	●	●	●	●
Domain Lookalike Detection	●	●	●	●	●	●
Display Name Impersonation	●	●	●	●	●	●
Direct Spoof (Exact Impersonation)	●	○	●	●	●	●
Dynamic Trusted Sender List	●	●	●	●	●	●
In-Mail Anti-Phishing Banner Alerts	●	●	●	●	●	●
Phishing Reporting Add-on for OWA/Outlook/Gmail clients	●	●	●	○	●	●
Actionable Phishing Reports	●	●	●	●	●	●
Malware Protection						
URL/Link/Attachment Inspection	●	●	●	●	●	●
Multi Anti-Virus Scanning	●	●	●	●	●	●
File Sandboxing	●	●	○	●	●	●
Forensics						
Automated Spam Handling	●	●	●	●	●	●
Reporter Reputation Scoring	●	●	●	●	●	●
Orchestrated Suspicious Email Analysis	●	●	●	●	●	●
Advanced Polymorphic Email Detection	●	●	●	●	●	●
Affected Mailboxes Real-Time Report	●	●	○	●	●	●
Automatic Email Clustering	●	●	●	●	●	●
Post-Delivery Remediation						
1-Click or Automatic Remediation	●	○	○	●	●	●
Automated Workflow Triggering	●	●	●	●	●	●
Intelligence						
Real-Time, Human Verified, Intelligence Sharing	●	●	●	●	●	●
Cross-Organization Sharing	●	●	●	●	●	●
Awareness & Training						
Enterprise Grade Phishing Simulation and Training Platform	●	●	●	●	●	●
Deployment						
No Mx Records Changes - 2 Click Deployment	●	●	●	●	●	●
Cloud Deployment	●	●	●	●	●	●
On Prem	●	●	●	●	●	●
Hybrid	●	●	●	●	●	●
Cloud-native Google Apps / Office 365 Support	●	●	●	●	●	●

Get Started with IRONSCALES

For more information, including on-demand videos, demo requests and product sheets, or to get started with the IRONSCALES' advanced phishing threat protection platform, visit www.ironscales.com

For sales or partner program questions, please email Adam Hofeler at adam@ironscales.com

About IRONSCALES

IRONSCALES is the leader in advanced phishing threat protection, combining human intelligence with machine learning to automatically prevent, detect and respond to advanced email phishing threats. By combining technical and end-user controls into one integrated, automated & multi-layered platform, IRONSCALES drastically reduces the workload burden of SOC and security teams while expediting the time from phishing attack discovery to enterprise-wide remediation from hours, weeks or months to just seconds. Headquartered in Tel Aviv, IRONSCALES was incubated at the 8200 EISP, the top program for cybersecurity ventures, founded by alumni of the Israel Defense Forces' elite Intelligence Technology unit.

www.ironscales.com

@ironscales

ironscales

Why IRONSCALES

- Forbes named IRONSCALES 1 of 25 Machine Learning Startups To Watch in 2018
- Named Top Innovator in Markets and Markets Spear Phishing Market Report
- Themis Named by CRN as a Hot Cybersecurity Product Announced At Black Hat2018
- Gartner Market Guide for Secure Email Gateways – IRONSCALES noted for Advanced Threat Defense Capabilities
- Citi & Microsoft Accelerator Participants