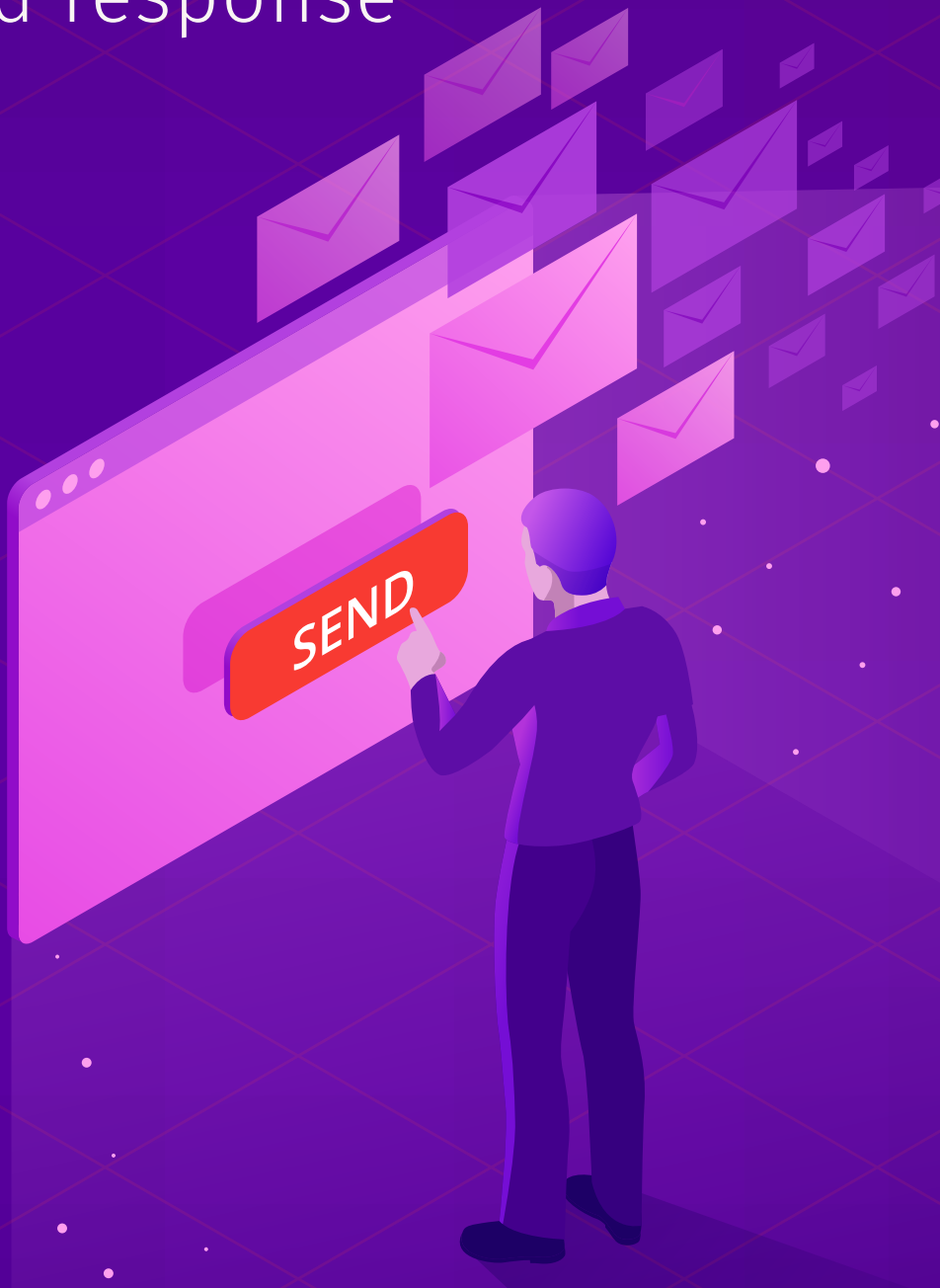
Office365 is Not Built to Defend Against Modern Real-World Email Threats

Learn why organizations that rely on cloud-email services must budget for advanced phishing prevention, detection and response



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

Executive Summary

It's hard to overestimate how fundamental email has become to initiating cyberattacks. While there are numerous ways for attackers to target organizations, email is almost-always the common denominator. Email phishing attack detection, analysis and rapid response is one of the biggest challenges email admins and security teams face today.

Did you know?

- *Phishing represents 98% of social incidents and 93% of breaches.*
- *Email continues to be the most common vector for cyber attacks (96%).*

Source: 2018 Verizon Data Breach Investigations Report (DBIR)

Microsoft has an opportunity and an incentive to solve the phishing epidemic, but based on historical results, it must become more agile and respond more rapidly to changing attacker tactics, should it want to lead here.

As Microsoft's SEG market share increases, smart attackers will specifically target Microsoft's defenses.

"Vendors that have been fully focused on this market are responding more rapidly to changing threats than vendors that offer broad portfolios of security services."
– Gartner (fighting_phishing__2020)

This presents a simple question: is the cloud email security deployed by the leading platforms, including Microsoft's Office 365 and Google's G Suite, capable of defending against the real-world threats faced by organizations and should organizations budget for advanced phishing protection?

Currently Office 365 offers no phishing protection without Advanced Threat Protection (ATP). Moreover, organizations that subscribe to ATP must contend with its weaknesses and limitations.

1. **File-less attacks:**
   Microsoft ATP's effectiveness is uncertain against Business Email Compromise (BEC).

2. **Post-email delivery incident response:**
   It is labor-intensive and unscalable, lacking automated phishing forensics and remediation of emails and without any clear indicators of compromise (IOC).

3. **Centralized threat intelligence:**
   This is limited to Microsoft's internal research, which is not done in real-time or scalable when time is of the essence.

4. **Technical controls only:**
   ATP relies heavily on AV, sandboxing, and machine learning without incorporating real-time human intelligence/end-user controls.

5. **Predictable and testable:**
   Using public information (a simple Mail Exchange MX record lookup), cybercriminals can easily test and customise phishing campaigns to suit the cloud environments that they know targets use most frequently.

According to figures from Gartner, in order to bolster protection, an estimated 40% of Microsoft Office 365 deployments will incorporate third-party tools by the end of 2018 with the figure predicted to rise to half of all deployments by 2020.

IRONSCALES Advanced Email Threat Protection Improves on ATP by Offering:

1. Superior mailbox intelligence, combining sender fingerprinting, inbox behavioral analysis and advanced mapping of trusted senders.
2. Automated Email Clustering analysis to detect polymorphic emails.
3. Advanced clawback and remediation of emails without indicators of compromise (file-less attacks), reducing IT security workload.
4. Decentralized intelligence by crowd sourcing email threat intelligence sharing of emerging phishing campaigns that is actionable.
5. Rapid response using machine learning, automation & orchestration

Defining Today's Email Threats

Contemporary phishing threats can be divided into overlapping categories, starting with significant amounts of spam, which is usually harmless, but clogs gateways and employee inboxes.

Next are more serious, but still generic threats such as ransomware and phishing attacks based on social engineering techniques.

Today, the most dangerous and fastest-growing threats to enterprises are those designed specifically to target their employees, business processes and supply chains. These include:

1. **Spear phishing and credential theft:**
   Aimed at any employee, these attacks are designed to gain a foothold in an organization by stealing credentials and gathering attack intelligence.
2. **Whaling:**
   Sometimes confused with spear-phishing, whaling targets high-value employees such as management or VIPs in a highly-personalised way.'
3. **Ransomware:**
   Today's state-of-the-art malware threat, ransomware needs only a single victim to gain a foothold in a network from where it can spread.
4. **Polymorphic attacks:**
   Polymorphism describes emails that automatically vary their properties to defeat signature-based scanning. The threat these messages pose to email security is formidable and extremely difficult to remediate.
5. **Business Email Compromise (BEC):**
   A highly-targeted attack designed to conduct financial fraud. Relying on spoofing or impersonating a co-worker or trusted third party to compromise an email system from within.

   BEC attacks can be extremely hard to detect because in most cases there is no payload (e.g. an attachment or link indicating malicious intent). The hallmark indicators of BEC are intent and urgency: "*You must to wire X dollars to Y by 15:00 today. Do not delay.*"

Defining Today's Email Threats

IRONSCALES empirical data shows that almost 95% of all email phishing attacks were highly-targeted campaigns, with the majority impersonating internal communications teams or individuals (e.g. CEO fraud). The data also revealed that 33% of attacks targeted just one mailbox.

- According to the FBI's 2017 Internet Crime Report, BEC attacks topped $676 million in losses.
- A notable recent example of BEC is provided by Italian Series A football team Lazio, which was reportedly defrauded of £2 million after being tricked into sending a transfer fee to the wrong bank account.

While these categorizations help us understand different phishing techniques, it's important not to forget that attackers can combine them into a single campaign – for example, once-opportunistic ransomware is becoming highly targeted.

The takeaway for defenders is that cybercriminals are now highly organized, willing to devote resources and time to researching their victims and planning attacks over many months. Each successful attack is simply the prelude to beginning a new one.

For every 5 brand spoofed attacks (Like Paypal or DHL) identified by spam filters, approximately 20 spear-phishing attacks bypassed the safeguard of spam filters and went undetected at the mailbox.
– IRONSCALES 2017 Trend Report

Boosting ATP capabilities with IRONSCALES

ASSUME the Phish – Defending against the multi-faceted complexity of targeted phishing attacks represents a huge challenge for any defensive system, including ATP.

However, ATP's centralized and prioritized design makes this even more challenging, which has knock-on effects for the speed at which it can respond to attacks in real-time.

This often represents the difference in survival for some companies, as many businesses, in particularly those of small and mid-size, are not built to recover from a business email compromise or ransomware attack.

According to Aberdeen report Reduce the Risk of Phishing Attacks: *It's About Time shows that on average, it only takes 82 seconds from the time a phishing email is first distributed until the first victim is hooked and by the end of the first 24 hours of phishing attacks 99% of user clicks on phishing URLs have already occurred*.

Inevitably, phishing emails will bypass ATP and arrive in the mailboxes of one or more employees, which means that it's imperative to detect and respond quickly using both mailbox anomaly detection and decentralized security intelligence that is able to scale.

IRONSCALES multi-layered approach to phishing mitigation works together with ATP, supplementing its capabilities using continuous monitoring and remediation.

ATP vs IRONSCALES
Preventing attacks before email delivery

ATP	IRONSCALES
ATP's malware prevention for malicious links & attachments offers proprietary AV and sandboxing without the option to integrate with other third-party providers.	**IRONSCALES' counters malicious links** and attachments using multiple AV and sandboxing engines from best-of-breed vendors such as Checkpoint, OPSWAT, Sndbox and others.
ATP's mailbox-level intelligence context filtering (Sender Reputation Scoring) allows customers to add up to 20 internal and external addresses they want to protect from impersonation and supported only on O365 Pro (June 2018).	**IRONSCALES' mailbox-level anomaly detection** module, IronSights, protects employees from email spoofing and impersonations attempts by dynamically learning their mailbox using fingerprint technology and studying communication habits. Using machine learning algorithms, IronSights also continuously studies every employee's inbox to detect anomalies based on both email data and metadata extracted from previously trusted communications.
	Polymorphic email threats are countered using machine-learning algorithms that cluster similarities and permutations of emails for quarantine in real time. (Polymorphic phishing emails are often sent to multiple users where at least one of the following is being changed either randomly or intentionally depending on the attack: sender name, sender address, subject Greeting, email body or signature).
Not supported on mobile devices	**Supported on all devices**

ATP vs IRONSCALES
Remediating Attacks After Email Delivery

ATP	IRONSCALES
ATP's detection of new phishing campaigns is based on centralized analysis whereby end-user reports are gathered by Microsoft analysts, leaving SOC and security teams with no visibility over user-reported phishing emails. This is not scalable, actionable or in real-time. And with phishing mitigation, time is of the essence. There is also no guaranteed SLA and security is dependent on Microsoft decisions and prioritization.	**IRONSCALES' decentralized analysis** moves phishing detection, analysis and forensics to the company in a more real-time and scalable infrastructure leveraging crowd-sourced phishing intelligence from other security sources connected to the IRONSCALES platform, which grows every month to provide unmatched detection to response time. This closes the gap between known and unknown phishing attacks.
ATP's detection using its anti-impersonation mailbox intelligence creates a 'sender map' based on the people an individual user sends to and receives from. However, this is only available for cloud-based accounts hosted entirely in Office 365.	**IRONSCALES' inbox behavioral analysis** establishes a baseline of normal communications so that the mailbox-level security can monitor every inbox individually, based on correspondence and attachment/ link interaction. IRONSCALES Inbox Behavioral Analysis establishes a baseline of normal communications so that the system builds a clearer picture of what a user and sender's "normal" email communications typically look like, flagging anomalies in real-time.

ATP vs IRONSCALES
Remediating Attacks After Email Delivery

ATP	IRONSCALES
Office 365's phishing simulation and training reporting is basic. It lacks continuous scoring of individual users, no organizational segmentation based on phishing awareness levels, and no ability to run multi-tiered phishing campaigns. There is also no feedback loop, which means employees never find out whether their report was an attack or a false positive.	**IRONSCALES simulation and training** works through continuous assessments via simulated phishing attacks, combining human intelligence that consistently trains the platform's machine learning modules to further close the gap between detection and response. In doing so, IRONSCALES has built a Human Intrusion Detection System.
	IRONSCALES' automated clustering occurs via IronTraps, our automated email phishing investigation, orchestration and response module. Using patented machine learning algorithms, IronTraps automatically clusters and finds similarities in phishing emails, preventing advanced phishing threats, such as polymorphic email attacks.
	IRONSCALES' AI-powered SOC assistant predicts threats and anomalies, with little to no input from humans. This helps to detect unknown/unverified phishing incidents automatically using AI models that continuously incorporate input from global security experts.

ATP vs IRONSCALES
Attack Response

ATP	IRONSCALES
ATP's clawback; Zero-Hour Auto-Purge (ZAP) can only clawback malware that has reached users' inboxes based on malicious content scanned by AV and sandbox solutions. Service-Level Agreements (SLAs) are undetermined. Already-delivered, malicious attachment files detection is very limited and mostly based on MD5 signatures that can be easily tampered.	**IRONSCALES' automated response** – makes it possible for a fully-automated quarantine to occur across an enterprise if an email is reported by end users or verified as malicious through other IRONSCALES modules, such as IronSights, IronShield, Federation or Themis. This automation removes harmful emails from employees' inboxes, neutralizing the threat automatically or with 1-click and in real-time. This process takes only a matter of seconds. It has proven to accelerate the time from identification to remediation from hours or weeks to seconds.
	IRONSCALES' orchestration phishing reports can be integrated with multi-AV and sandboxing solutions. All intelligence is delivered to the SOC and SIEM allowing for greater control and incident response capabilities.

Comparitive Matrix

Solution Features	IRONSCALES	ATP
Advanced Anti-phishing Threat Detection		
Domain Lookalike Detection	Yes	Yes
Display Name Impersonation	Yes	Yes
Direct Spoof (Exact Impersonation)	Yes	Partial
Dynamic Trusted Sender List	Yes	No
In-Mail Anti-Phishing Banner Alerts	Yes	Yes
Phishing Reporting Add-on for OWA/Outlook/Gmail clients	Yes	Yes
Continuous Malware Protection		
URL/Link/Attachment Inspection	Yes	Yes
Multi Anti-Virus Scanning	Yes	Yes
File Sandboxing	Yes	Yes
Forensics (Fully Automated/ No YARA Rules/ No Playbooks)		
Spam Handling	Yes	Yes
Reporter Reputation Scoring	Yes	No
Suspicious Email Clustering Analysis	Yes	No
Advanced Polymorphic Email Detection	Yes	No
Affected Mailboxes Real-Time Report	Yes	Partial
Post-Delivery Remediation		
One-click or Automatic Remediation (including non IOC emails)	Yes	No
Automated Workflow Triggering	Yes	No
Phishing Intelligence (Fully Automated)		
Real-Time, Human Verified, Intelligence Sharing	Yes	No
AI Assisted Open Incident Decision Making	Yes	No
Awareness & Training		
Enterprise Grade Phishing Simulation and Training Platform	Yes	No
Deployment		
No MX Records Changes	Yes	Yes
Two-click Deployment	Yes	Yes
On-Premises	Yes	No
Cloud-native Office 365 Support	Yes	Yes
Mobile Responsive	Yes	No

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.

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.

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.

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.

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.

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.

Start with IRONSCALES Today

Ready to enhance your phishing response strategy?
Anti-phishing requires a three-pronged strategy: technical controls, end-user controls and process automation.
Contact us for a free trial.

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
- Frost and Sullivan Technology Innovation Award: AI-powered Email Security
- Named Top Innovator in Markets and Markets Spear Phishing Market Report
- Gartner Market Guide for Secure Email Gateways – IRONSCALES noted for Advanced Threat Defense Capabilities
- Citi & Microsoft Accelerator Graduates

Info Security Products Guide 2018 GLOBAL EXCELLENCE SILVER

MOST INNOVATIVE ANTI-PHISHING CYBER DEFENSE MAGAZINE 2018

CYBERSECURITY BREAKTHROUGH AWARDS

2017 SINET 16 INNOVATOR

THE CHANNEL CO. CRN EMERGING VENDORS 2018