SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

IRONSCALES
THE POWER OF NOW

OFFICE 365 ATP IS NOT BUILT TO DEFEND AGAINST MODERN REAL-WORLD EMAIL THREATS.

Executive Summary:

It's hard to overestimate how fundamental email has become as a route to attack enterprises. While there are numerous ways for attackers to target organizations, email is almost-always the common denominator.

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:

1. **File-less attacks:** BEC protections are manually configured – limited to 60 profiles

2. **Post-email delivery Incident response:** It is labor-intensive and unscalable, lacking automated phishing forensics and remediation of emails.

3. **Centralized Threat Intelligence:** This is limited to Microsoft's internal research, which is not 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.

Did you know?

- Phishing was the most used threat action variety representing 22% of data breaches and was the second most seen threat action in all incidents

- Email links were the number one vector used to infect endpoints with malware

- 96% of all social attacks arrive via email

- 37% of breaches used compromised credentials

Source: 2020 Verizon Data Breach Investigations Report (DBIR)

IRONSCALES Improves On ATP By Offering

1. Superior mailbox intelligence combining sender fingerprinting, inbox behavioural analysis and advanced mapping of trusted senders.

2. AI-Powered Incident Response
Prioritizes reported incidents, automating investigative analysis and automated remediation.

3. Advanced clawback/remediation of polymorphic emails and emails without indicators of compromise (file-less attacks), reducing IT security workload.

4. Federated decision-making from all the platform's users, giving you an entire virtual analyst community for real-time, actionable threat intelligence.

5. Advanced URL & Malware Protection leveraging computer vision and neural network technology, our platform goes beyond traditional solutions to detect and block visual deviations of spoofed websites and brands in real-time.

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 other malware attacks. However, for enterprises the most dangerous and fastest-growing email threat 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 on 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. Once a polymorphic email finds a way into an organization, then it can be extremely difficult to remediate, especially if the only defensive measures are from signatures and regular expressions.

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.”

While these categorizations help us understand the different phishing techniques, it’s important not to forget that attackers can combine them in 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.

> *Microsoft has an opportunity and an incentive to solve the phishing issues, but based on historical results, it must become more agile and respond more rapidly to changing attacker tactics. 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)*
>
> 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

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.

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 quickly using both mailbox anomaly detection and decentralized security intelligence that is able to scale. IRONSCALES multilayered approach to phishing mitigation works through continuous monitoring and remediation.

> *Vendor-provided signatures of phishing email attacks are much too slow to provide an effective defense.*
>
> *For example, signatures from Microsoft Advanced Threat Protection took between 6 days to more than 250 days from the time a phishing email attack was first reported, to the time a signature was made available to enterprise technical staff.*
>
> *In addition, the trend towards sophisticated, polymorphic phishing email attacks makes traditional signature-based approaches only marginally useful.*
>
> **Source: Aberdeen Research, How to Conquer Phishing, Beat the Clock**

According to Aberdeen Group, *"by the end of the first 24 hours of phishing attacks 99% of user clicks on phishing URLs have already occurred."*

- According to the FBI's 2019 Internet Crime Report BEC attacks topped $26 billion in losses since June 2016.
- A notable recent example of BEC is provided by Italian Serie A football team Lazio which was reportedly defrauded of $2 million after being tricked into sending a transfer fee to the wrong bank account.

ATP vs IRONSCALES - Preventing Attacks Before Email Delivery

- **ATP's malware prevention** for malicious links & attachments offers proprietary AV and sandboxing without the option to integrate with other third-party providers. URLs are checked against a static database. Safe Links fail when the URL is in an attachment

- **ATP's anti-spoofing detection** requires cumbersome policy configurations which are static by nature with limited employee coverage

- **ATP's anti-phishing policy & mailbox intelligence** allows customers to add up to 60 internal and external addresses they want to protect from impersonation and supported only on O365 E3 & E5. *Mailbox intelligence only for fully hosted O365 accounts. *

- **Office 365 Attack Simulator** reporting is basic. It lacks continuous scoring of individual users, no segmentation of organization based on phishing awareness levels, and no ability to run multi-tiered phishing campaigns. There is no feedback loop, which means employees never find out whether their report was an attack or a false positive.

- Not supported on mobile devices

- **IRONSCALES URL and malware protection** technology defends against credential theft and phishing malware with proprietary computer vision technology as well as multiple AV and sandboxing engines from best-of-breed vendors such as Check Point, OPSWAT, Bitdefender, Virus Total and others.

- **IRONSCALES' mailbox-level anomaly detection** module protects organizations' employees from email spoofing and impersonation attempts by dynamically learning individual mailbox behaviours using a unique fingerprinting technology and studying communication habits. Using machine learning algorithms to continuously study every employee's inbox to detect anomalies based on both email data and metadata extracted from previously trusted communications.

- **IRONSCALES simulation and training** works though continuous assessment via simulated phishing attacks. IRONSCALES combines human intelligence that continuously trains the IRONSCALES machine learning models, further closing the gap between detection and response, ultimately building a Human Intrusion Prevention System.

- Supported on all devices

ATP v IRONSCALES – Post Attack (Forensics/Investigation and Response)

- **ATP's forensic tool:** Threat Explorer only lists basic information about the attack, limiting the depth of forensics. Top malware report only shows total count of malware, with no drill down to see the actual information

- **ATP's analysis** of new phishing campaigns is centralized 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. (average time to first click is 80 seconds.)

- **IRONSCALES' AI-powered incident response** technology helps SOCs and users go on offense against attacks. Users click a single button inside their email interface to report advanced email attacks missed by technical controls such as secure email gateways (SEG) or anti-virus filters. The platform reduces manual email analysis with automation by as much as 90%, dramatically improving your SOC's efficiency and liberating them for other tasks. At the same time, the platform uses machine learning to find and cluster similar phishing emails and known attacks, preventing broader polymorphic attacks or campaigns from going undetected and unresolved.

- **IRONSCALES democratized threat protection** The global community of IT security analysts has more up-to-date security data and threat intelligence than any security vendor does. The IRONSCALES platform gives power to the people—your business's security analysts—enabling them to cut out the legacy email security vendor as the middleman. The platform spreads realtime intelligence among analysts exponentially in a democratized, distributed and collaborative manner, removing delays, scaling threat detection and remediation, and defusing malicious email campaigns.

- **IRONSCALES' AI-driven virtual security analyst (Themis)** helps security teams determine a verdict on suspicious email incidents in real-time. This helps to detect unknown/unverified phishing incidents automatically and in real-time using AI models that continuously incorporate input from our customers analysts. Themis provides security teams with a confidence level for every phishing incident and can be operated in both suggestive and responsive modes based on her built-in confidence levels and company policy. If the confidence level is high enough, Themis can automatically make and implement decisions without human intervention.

- **IRONSCALES offers the first and only mobile incident response app.** So security professionals can resolve incidents faster on the go – without the need for a keyboard!

ATP (AIR) v IRONSCALES – Post Attack Remediation

- **ATP's 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.

Admin can only search campaigns by sender and subject. It takes several hours for the data to be fully available in the logs.

ATP relies on cumbersome policy configurations with limited flexibility and scope, workflows and enforcement.

- **IRONSCALES' automated remediation** – makes it possible for a fully-automated remediation to occur company wide if an email is reported by end users or verified as malicious through other IRONSCALES sources. This automation removes harmful emails from employees' inboxes, neutralizing the threat automatically or with 1-click and in real -time. This process has proven to accelerate the time from identification to remediation from hours or weeks to just seconds.

For both security professionals and end users, we offer a cloud-based platform with push-button protection, giving you simplicity and speed for accelerated visibility and control that works at the user mailbox level.

By giving end users and security professionals the right training, tools, and intelligence in a one-click resolution from a single platform, they can work together much more effectively to hunt, log, alert, analyze and remediate phishing attacks.

Protect your organization from the inside out against any and all types of phishing attacks with...

Advanced Malware/URL Protection - Protect against zero-day malware, credential theft, and phishing websites with a real-time defence against all inbound emails, using various multi-anti-virus, visual anomaly detection and sandbox engines.

Mailbox-Level BEC Protection - Prevent email spoofing, impersonation and non-signature-based BEC attacks in real time. Check every employee's inbox for anomalies with our unique "fingerprint" technology.

AI-Powered Incident Response - Automate email phishing investigation, orchestration and response to reduce the detection of suspicious mail to just seconds. Automatically claw back and cluster bad emails at scale - instantly.

Democratized Threat Protection - Get the world's most real-time and actionable threat intelligence with more eyeballs and SOC analysts than any other solutions available, detect existing and emerging phishing threats in real time.

Virtual SOC Analyst - Our AI-powered security analyst allows your security teams to make faster decisions on suspicious emails in real time by automating the thresholds, analysis and quarantine of threats.

Personalized Simulation & Training - Simulate attacks to drive user awareness and training with a customized micro-learning method to help employees think like security analysts and identify attacks.

See how IRONSCALES compares in specific features, functionality, and capability compared to Microsoft ATP

COMPARATIVE MATRIX - IRONSCALES VS O365 ATP

Solution Features	IRONSCALES	ATP
Advanced Threat Protection		
Mailbox-level Behavioral Analysis	Yes	Yes
Domain Lookalike Detection	Yes	Yes
Display Name Impersonation	Yes	Yes
Direct Spoof (Exact Impersonation) up to 60 mailboxes	Yes	Partial
Dynamic Trusted Sender List	Yes	No
Dynamic /Contextual In-Mail Anti-Phishing Banner Alerts	Yes	No
VIP Impersonation Protection	Yes	No
NLP BEC Detection	Yes	No
Phishing Reporting Add-on for OWA/Outlook	Yes	Yes
URL/Link/Attachment Inspection	Yes	Yes
Multi Anti-Virus Scanning	Yes	Yes
File Sandboxing	Yes	Yes
Fake Login Page Detection (Computer Vision)	Yes	No
Democratized Threat Protection	Yes	No
SecOps (Fully Automated/ No YARA Rules/ No Playbooks)		
Spam Handling	Yes	No
Reporter Reputation Scoring	Yes	No
Suspicious Email Clustering Analysis	Yes	Partial
Advanced Polymorphic Email Detection	Yes	No
Automatic Email Clustering	Yes	No
Affected Mailboxes Real-Time Report	Yes	Partial
One-Click or Automatic Remediation (including non IOC emails)	Yes	No
Automated Workflow Triggering (SIEM/SOAR)	Yes	No
Virtual SOC Analyst	Yes	No
Threat Assessment		
Enterprise Grade Phishing Simulation and Training Platform	Yes	No
Phishing Emulator	Yes	No
Deployment		
No MX Records Changes	Yes	Yes
Two-Click Deployment	Yes	No
Cloud Deployment	Yes	Yes
On-Premises	Yes	No
Hybrid	Yes	No
Mobile Incident response App	Yes	No

Box 1: Customers using IRONSCALES

Healthcare: an attack adopting the style of the provider's HR department targeted 100 employees with the title 'important updates to your account'. Within five minutes, the first employee had reported the email at which point IronTraps automatically deleted the malicious email from all affected inboxes.

Financial services: A company was targeted with an email pushing a Microsoft Outlook Web Access (OWA) login page designed to steal credentials. Again, an employee reported the email as suspicious at which point IronTraps removed the email from 46 inboxes and, importantly, prevented any employee from entering credentials.

Internet of Things: Telit is a London-headquartered Internet of Things (IoT) provider, employing 1,100 people across 42 sites that found itself dissatisfied with the performance of conventional gateway filtering. Too many malicious emails were getting through this security and even when employees suspected malicious emails, SoC reporting was slow and cumbersome. This consumed SoC resources and struggled to cope with false positives. The company deployed IronTraps and IronSights to smooth this reporting burden with automated analysis and response, backed by phishing awareness training.

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.