White Paper

Microsoft Defender for Office 365 is not Built to Defend Against Modern Email Threats

IRONSCALES
SAFER TOGETHER

Introduction

It's hard to overestimate how email has been and remains the primary method used to attack companies and organizations of all sizes. While there are numerous ways for attackers to target organizations, email is almost-always the common denominator.

So, the question is whether or not the email security functionality available from the leading cloud platforms, including Office 365 and Google Workspace, is capable of defending against the real-world phishing threats faced by organizations and should organizations budget for advanced phishing protection?

In short, the answer is no. Currently Office 365 offers no phishing protection without having an E5 license and then deploying Defender for Office 365 (formerly known as Advanced Threat Protection (ATP)). Even with Defender for O365 deployed, companies will still face several challenges, including:

FILE-LESS ATTACKS
BEC protections are manually configured – limited to 60 profiles

POST-EMAIL DELIVERY INCIDENT RESPONSE
It is labor-intensive and unscalable, lacking automated phishing forensics and remediation of emails.

CENTRALIZED THREAT INTELLIGENCE
This is limited to Microsoft's internal research, which is not real-time or scalable when time is of the essence.

TECHNICAL CONTROLS ONLY
Defender for O365 relies heavily on Antivirus, sandboxing, and machine learning and does not incorporate real-time human intelligence/enduser controls.

PREDICTABLE AND TESTABLE
Using public information (such as a simple Mail Exchange MX record lookup), cybercriminals can easily test and customize phishing campaigns that target cloud-based email deployments.

Contents

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:

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.

WHALING

Sometimes confused with spearphishing, whaling targets high-value employees such as management or VIPs in a highly personalized way.

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.

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.

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 wire X dollars to Y by 3:00 PM 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 security teams and company leadership 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 the next one.

Defender for Office 365 vs IRONSCALES: Preventing attacks before emails are delivered to end users

- **Defender for O365's malware prevention for malicious links & attachments** offers proprietary Antivirus 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.
- **Defender for O365's anti-spoofing detection** requires cumbersome policy configurations which are static by nature with limited employee coverage.
- **Defender for O365'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 and not supported on mobile devices.
- **Office 365 Attack Simulator reporting** is very minimal. 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.

- **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 behaviors 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.

> "With banners, warnings and intuitive self-management, it's easy to prove that IRONSCALES is protecting our company. And it really is essential to have the visual tools that IRONSCALES provides to show our board and to easily demonstrate that our email security system is secure."
>
> NEIL STEIN, SVP OF TECHNOLOGY SERVICES AT ORTHOCAROLINA

Defender for Office 365 vs IRONSCALES: Preventing attacks after emails are delivered to end users

- **Defender for O365's forensic tool named "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.
- **Defender for O365'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.

> "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

- **IRONSCALES' AI-powered incident response technology** helps security teams and users go on the 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** leverages our global community of customers to provide an early warning system against zero-day attacks, and intelligence source that neither Microsoft nor any other email security provider offers today. Our platform distributes real-time 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 milliseconds by using AI models that continuously incorporate input from our customers' security teams. Themis provides our users 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 our customers' unique company policies. If the confidence level is high enough, Themis can automatically make and implement decisions without human intervention.
- IRONSCALES offers the first and only full-featured mobile incident response app. This allows our customers' tool admins to review and resolve phishing incidents while on the go – no need to be tethered to their desks!

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

Boost your email defenses by adding IRONSCALES as a second layer of protection behind Defender for Office 365

Defender for Office 365 is basically the same as other Secure Email Gateway technologies: great at stopping spam but terrible at finding and eliminating advanced phishing attacks like BEC, Account Takeover (ATO) and VIP impersonation. Companies who have made the investment in Defender for O365 can add IRONSCALES as a second layer focused on catching everything that gets through.

IRONSCALES
SAFER TOGETHER

IRONSCALES is a self-learning email security platform that can predict, detect and respond to email threats within seconds.

Email threats are growing exponentially and morphing at scale. Each day, billions of new, increasingly sophisticated phishing attacks and launched globally. Legacy technologies like security email gateways (SEGs) have been shown to allow up to 25% of incoming phishing attacks through to their intended targets.

With IRONSCALES, you and your organization are Safer Together because of the following:

- Advanced malware/URL protection
- Mailbox-level Business Email Compromise (BEC) protection
- AI-powered Incident Response
- Democratized real-time threat detection
- A virtual security analyst
- Gamified, personalized simulation and training

To learn more, please visit **www.ironscales.com** today!