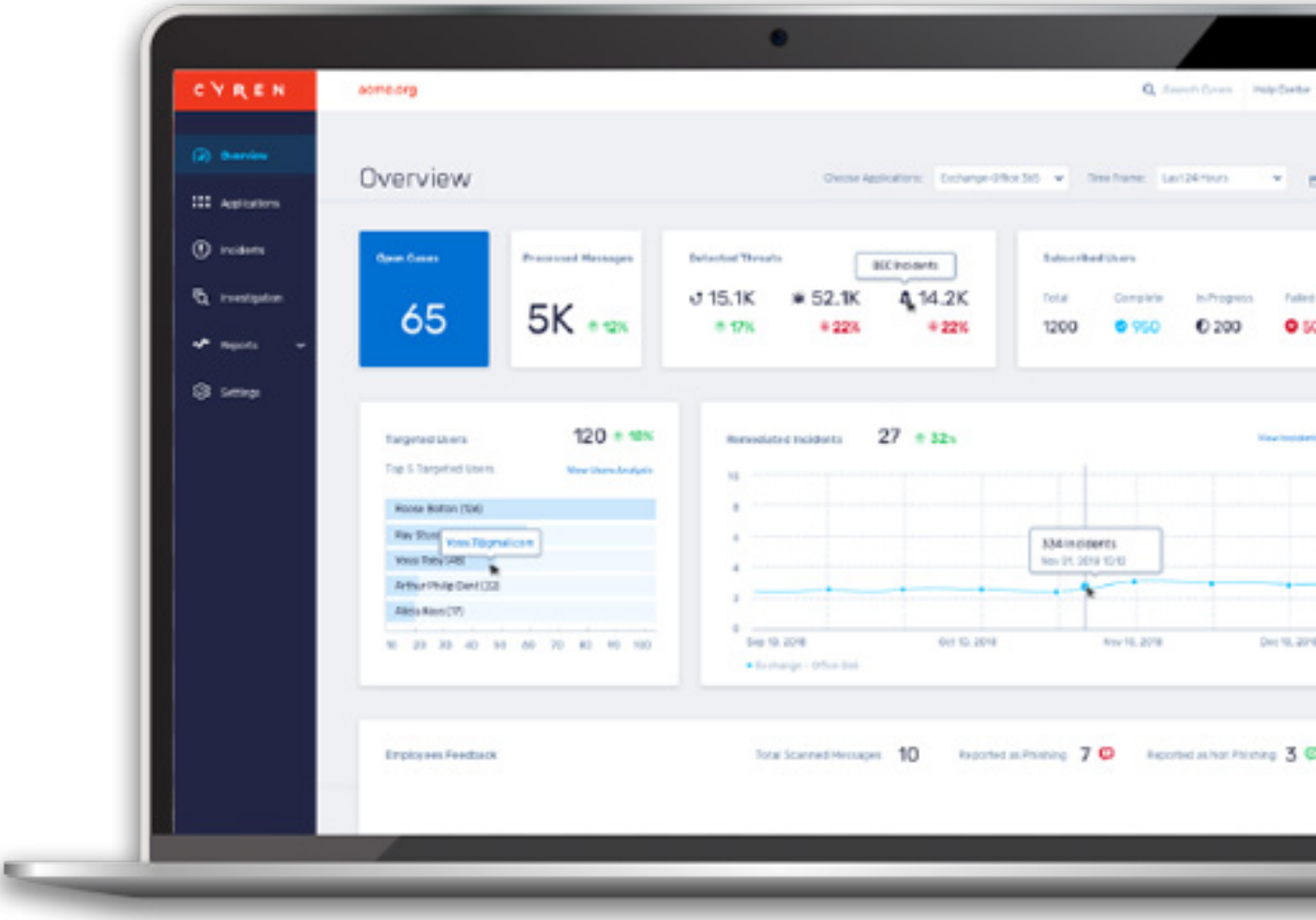
CYREN

SECURITY GUIDE

# How to Stop Evasive Phishing Attacks from Microsoft 365 Accounts



# Contents


Executive Summary . . . . . 2

Corporate Email Remains Highly Vulnerable to Cyber Threats . . . . . 4

- Gaps in the cloud . . . . . 4
- Phishing is lucrative . . . . . 4
- No experience needed . . . . . 4
- Evasive attacks avoid detection . . . . . 4

Time to Establish an IDR Layer in Corporate Email Security . . . . . 6

- IDR – Advanced, Automated and Adaptive Corporate Email Security . . . . . 7
- IDR – Reducing Business Risk . . . . . 7
- IDR – Crowd Sourcing Threat Intelligence . . . . . 7

Best Practices in IDR Implementation . . . . . 8

- Frictionless Onboarding . . . . . 8
- Automated Response and Remediation . . . . . 8
- Adaptive Threat Protection . . . . . 8
- Effective Employee Engagement . . . . . 8

Summary . . . . . 9

# Executive Summary

Cybersecurity professionals understand that no single defense will catch all cyber threats. Gartner recommends a layered and adaptive security architecture that enables a continuous cycle of "prevent-detect-respond-predict" defense. While this architecture is widely used by cybersecurity vendors, it is noticeably absent in corporate email security, particularly among Microsoft 365 users. Most organizations still rely primarily on prevention delivered by a secure email gateway (SEG) at the network perimeter.

The secure email gateways has one purpose - prevent email-borne cyberattacks from penetrating the enterprise network. But as threats increase in sophistication and number, the SEG frequently fails. Despite vendor improvements in SEG filtering and performance, too many phishing, Business Email Compromise 1 and fraud attacks get past the SEG and land in corporate mailboxes, greatly increasing business risk.

Email-borne phishing is a major problem facing organizations of all sizes, with 78% of Microsoft 365 administrators reporting security breaches with phishing as the leading cause. Experts predict that phishing attacks will increase because phishers never rest. The investment is minor; the payoff is lucrative; and it takes only one victim to breach an organization.

The rise in successful email-borne cyberattacks is driven by three main factors:

1. **First**, Microsoft 365 creates a new and attractive attack opportunity of hosted email platforms in the cloud. Adoption of Microsoft 365 is becoming ubiquitous making it a popular target for cybercriminals.

2. **Second**, Phishing, BEC and fraud attacks are more sophisticated and constantly evolving. They use evasion techniques to avoid detection by cybersecurity systems, and social engineering to create a sense of urgency that induces people to click or follow instructions.

3. **Third**, IT admins and security teams are stretched to the limit. Cybersecurity skills are in short supply. Depleted staff are bombarded on a daily basis with alerts and struggle to get ahead of the curve.

Organizations need to bolster their perimeter approach to Microsoft 365 email security. Inbox Detection and Response, or IDR, introduces a critical layer of security, right at the cloud mailbox, filling the gaps in detection and remediation left by the SEG. The SEG continues to operate as the first layer of defense, removing spam and malware threats as emails pass through it. The IDR layer operates in the mailbox, catching all the phish that got away.

This paper takes a deep dive into corporate email security to explain:

- Why Microsoft 365 email in the cloud remains highly vulnerable to cyber threats
- How Inbox Detection and Response (IDR) addresses these vulnerabilities
- Best practices in IDR Implementation

# Microsoft 365 Email Is Especially Vulnerable to Cyber Threats

The Gartner model of adaptive security architecture has been applied to many cyberattack vectors, including email security. On-premises email servers often have anti-malware and anti-phishing engines installed on them to provide regular scans and to detect newly found threats in the mailbox. When organizations migrate to cloud-hosted mailboxes, this is no longer possible. Hence, a critical gap in email security now exists.

## Gaps in the cloud

Enterprises using Microsoft 365 email platform in the cloud report a higher average incidence of successful phishing attacks than they experienced with on-premises email platforms. Users also report that native Microsoft 365 add-ons— Exchange Online Protection (EOP) and Advanced Threat Protection (ATP)—often fail to detect and isolate threats. As a result, too many phishing emails wind up in user mailboxes, where they become the users' problem.

## Phishing is lucrative

Successfully phishing an employee's Microsoft 365 credentials is lucrative. Armed with legitimate credentials, a cybercriminal can send emails from a real and recognized corporate account, opening inner doors to company data and assets. A Business Compromised Email (BEC) attack may be used to obtain information that will enable further penetration into the organization, or to extract a more immediate payback. The business risk is compounded when the compromised account has admin permissions. It is far more difficult to defend against a compromised insider than an external email attempting to impersonate an internal sender.

## No experience needed

Today, no particular expertise is needed to launch a sophisticated phishing attack. It's easy. On the Dark Web, veteran and novice cybercriminals conduct a robust business in low-cost, high-quality, and easy-to-use phishing campaigns, which can be purchased as a service or as do-it-yourself kits that contain everything needed to launch a phishing campaign. To avoid detection and assure their chances for success, sophisticated phishing campaigns utilize and array of evasion techniques. The more the criminal pays for a phishing kit or service on the Dark Web, the more evasion tactics will be included.

As the barriers to entry fall away, the volume and frequency of phishing attacks has spiraled upward, and traditional SEGs are failing to detect them. How are Secure Email Gateways failing? Typically, the SEG extracts URLs from email messages and from attachments. Standard SEGs check the URL against a list of known phishing sites. Advanced SEGs use more sophisticated detection capabilities such as "time-of-click." Predictably, these improved detection techniques have spawned further evasion tactics, making the SEG less effective.

## Evasive attacks avoid detection

Advanced Secure Email Gateways now include detection capabilities like in-line sandboxing and support authentication protocols like SPF, DKIM and DMARC[3]. Unfortunately, even advanced SEGs have a critical limitation that prevents them from detecting account-takeover attacks, spear phishing, cousin domain spoofing and unknown threats. Their insurmountable limitation is that they see the email at a single point in time and get only one pass to identify an attack. When the SEG fails to detect a threat, the email is delivered to the user mailbox and is no longer accessible to the SEG. Should a new threat be discovered post-click or post-delivery, it is too late. The email cannot be retrieved and the SEG can no longer intervene.

Let's take a closer look at how evasion tactics enable phishing and fraud emails to bypass the SEG and trick users into taking the bait.

## Evasion Tactics

Evasion tactics help bad actors avoid detection so their attacks have a better chance of success. They need to fool the SEG, the user, and other cybersecurity solutions that hunt for them on the web.

### Fooling the SEG

Activating or uploading malicious content to the target webpage only after the email has been scanned is a tactic that is not new. Advanced SEGs countered this tactic with "time-of-click" detection, which automatically rescans an email when the user clicks the link. It gives the SEG one last chance to detect a malicious URL. However, spear phishing and BEC attacks contain no URLs or attachments, so they appear harmless to the SEG. Once the tainted email has evaded the SEG, the user is the last line of defense.

For example:

*Consider a Business Email Compromise attack that gets past the SEG and succeeds in obtaining one user's login and password credentials. The attacker may simply observe his victim's email correspondence for a period of time, and then start sending messages to strategically placed employees to gain access to sensitive data that can be used to steal funds in a wire fraud attack. The SEG cannot detect this activity.*

### Fooling the user

Evasion tactics trick users as well. 50% of users click on links because social engineering creates a sense of urgency. Cousin domains are used to obfuscate URLs and create look-alike websites. Punycode attacks use foreign language characters that resemble English ones. Likewise, attackers serve up local versions of a spoofed site, so the domain looks legit, but it's not.

For example:

*Consider the employee who receives an email from one of his shadow applications, saying a security vulnerability has just been patched, so please click now to update. Not only does the counterfeit email/site look and act like the real thing, it has all the expected security trappings. Even the most vigilant, security-trained users fall for these tricks.*

### Fooling cybersecurity

Bad actors also need to evade detection by cybersecurity companies. They learn the IP address ranges of these companies and block the connection attempt. Or they change a couple of pixels in a fingerprinted image so the tampering is not detected. Target website HTML code is often obfuscated and encrypted. These are but a few of the techniques used to avoid detection. There are many others.

# Time to Establish an IDR Layer in Corporate Email Security

By 2021, Gartner expects 70% of public and private companies to be using cloud email services. Also according to Gartner:

**1 in 5**

corporate employees now use Microsoft 365 cloud service.

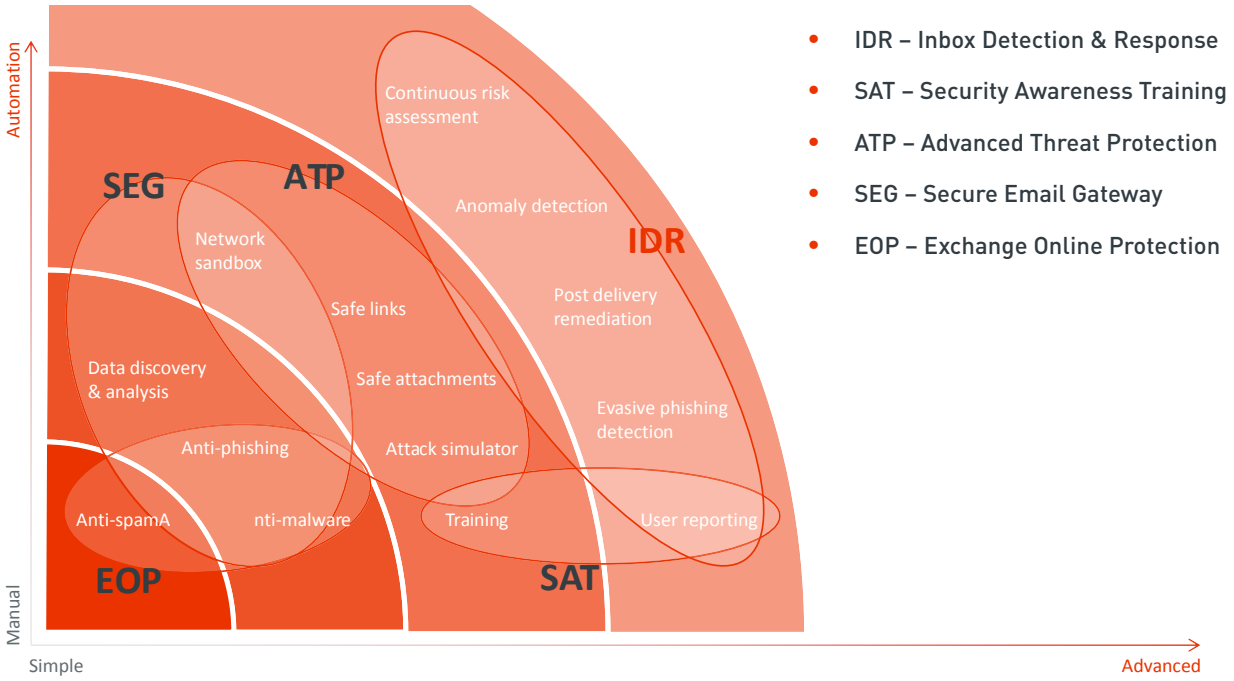
Microsoft 365

is the most widely used cloud service by user count.

Business applications hosted in the cloud have created the need for an inner layer of email security. While the SEG remains an important perimeter defense system, it lets sophisticated threats through. Inbox Detection and Response (IDR) allows enterprises to close this gap in email security by deploying an additional layer of intelligent and adaptive threat protection where it's needed most – in the Inbox.

The IDR layer of email security is easy to implement and scale in the cloud, and it focuses on the user Inbox rather than on the network paths to and from the Microsoft 365 server.

## Email Security – Maturity Model




- IDR – Inbox Detection & Response
- SAT – Security Awareness Training
- ATP – Advanced Threat Protection
- SEG – Secure Email Gateway
- EOP – Exchange Online Protection

Microsoft 365 is a mature application that requires a mature cybersecurity solution

## IDR – Advanced, Automated and Adaptive Corporate Email Security

Inbox Detection and Response (IDR) recognizes that the SEG should remain an essential first layer of preventative security control. It ensures a clean Internet pipe by removing spam, malware, and known threats as emails pass through it.

The IDR layer complements and strengthens cybersecurity posture, by filling the gaps left by the SEG and by native Microsoft 365 EOP and ATP add-ons.

By design, the IDR layer has continuous access to all emails in the Microsoft 365 mailbox. Therefore, it can provide continuous monitoring and detection rather than the one-pass detection provided by the SEG and its add-ons. Persistent rescanning of emails also facilitates more sophisticated detection and remediation controls that utilize machine learning and closed loop automation. For example, in the IDR layer, organizations can:

- Monitor user behaviors and interactions in the mailbox to identify anomalies.
- Collect and correlate multiple sources of data to determine whether an email is malicious and requires action.
- Enable automated remediation in the mailbox and across all mailboxes
- Allow users to interact with detection technologies and provide feedback
- Incorporate user feedback automatically
- Utilize feedback loops to reinforce machine-learning (ML) algorithms and predict what the next threat might look like.
- Push intelligence to SEGs and other security assets, strengthening the organization's overall security posture.

## IDR – Reducing Business Risk

The rise in evasive phishing puts your business at risk. First it overwhelms SOC and IT personnel who are responsible for analyzing and remediating these suspicious/malicious emails. Security teams don't have time or resources to process all the threats. Second, even if only one employee opens a tainted email and takes the phishing bait or falls for the fraud, the damage to your business assets, data and reputation can be severe.

While security training programs focus on awareness and behavior modification, they rarely result in the employee's ability to spot phishing. By putting a layer of protection right in the mailbox, IDR solutions make it easier for employees to keep email security top-of-mind, without expending a lot of time and impinging on productivity.

# Best Practices in IDR Implementation

Organizations ready for the benefits of an IDR solution should insist on four capabilities: frictionless onboarding, automation, adaptive threat protection, and effective user engagement.

## Easy Onboarding

Installing a layer of protection in the Microsoft 365 mailbox must be frictionless for IT admins and users alike. IDR solutions are best delivered as a cloud service that plugs directly into cloud mailboxes using native APIs provided by Microsoft 365. Plug and play solutions improve time-to-value and lower adoption costs.

Deployment should take minutes rather than days, and require no change at all to the organization's current email security infrastructure. This approach leaves the SEG undisturbed, preserving sunk costs. It also protects ongoing investment for organizations that have licensed the native SEG capabilities of Microsoft 365.

## Automated Response and Remediation

The continuous scanning, detection, analysis and remediation functions of the IDR layer should be fully automated. The IDR layer should be able to scan all emails when they arrive at the mailbox and then persistently rescan the mailbox when new threats are discovered or at regular intervals.

Zero touch automation is key to accelerating time to response and remediation. Automation increases the productivity of IT admins and security teams. Look for automated remediation actions that include:

- Tag and deliver suspicious emails, allowing users to close the loop
- Move detected threats to different folders and send alerts
- Remove detected threats from every mailbox across the entire organization – per security policy. This alone will save hours of manual remediation for the security team.

## Adaptive Threat Protection

To keep pace with evasive attacks, IDR solutions must offer truly adaptive threat protection. Look for solutions that utilize superior native detection capabilities complemented by machine-learning algorithms. The IDR layer must be able continuously learn and to adapt as attackers pivot and try different methods. Ideally, IDR solutions should perform multiple analyses, including:

Sender Behavior Analysis: detects imposter or spoofed emails based on header analysis, cousin or look-alike domain detection, as well as natural language processing to determine whether the language in the body of an email might be indicative of social engineering.

## Effective User Engagement

The best IDR solutions provide an email detection, analysis and remediation framework that enables productive employee participation in the company's security goals. Users should receive clear warning of threats, and be able to automatically scan, report and remediate suspect emails that appear in their Inbox. Likewise, as users close the remediation loop, their feedback should be incorporated into the system, making it more effective over time.

Ideally, IDR solutions should perform multiple analyses, including:

URL Behavior Analysis: protects users from credential theft by extracting URLs from emails and examining the destination web page for evidence that it might be a phishing site. Underlying technologies should be built specifically to detect evasive phishing tactics. For example, automatically access suspect sites from multiple source IP addresses and emulate different browsers to observe how the site renders in different environments.

Mailbox Behavior Analysis: profiles mailbox activity to create a baseline of trusted behaviors and relationships. Who sends emails to whom and at what time of day? What volumes? What do the contents look like? And many others. Mailboxes are then continuously monitored for anomalous behaviors and predictive analytics are used to detect threats. For example, if an executive never sends emails to a finance cloud, and then suddenly he does, late on a Friday evening, requesting a money transfer, this behavior will be an anomaly, indicating a possible BEC attack.

Incident Analysis: Enables rapid investigation, containment, response and remediation of threats. Incidents are created whenever an email contravenes a security policy or is reported by the user. Look for automation here too, including clear display of detailed forensic data per incident and automatic aggregation of similar incidents into a single case that can be remediated in one fell swoop. Automated incident analysis and workflows mean security teams need fewer skilled resources and can respond to threats much faster.

# Summary

The prevailing email security architecture in most organizations has not kept pace with the challenges introduced by Microsoft 365 and evasive attacks. Email-borne phishing, BEC and fraud threats continue to avoid detection and land in user mailboxes. Regardless of how well employees are trained, they still fall victim to these scams, increasing the risk of data breach.

Inbox Detection and Response provides an automated and adaptive layer of cybersecurity where it is needed most - right in the Microsoft 365 mailbox. Organizations are advised to choose an IDR solution that is not-invasive and deploys seamlessly for both IT admins and users.

Inbox Detection and Response solutions are successfully filling the gaps left by Security Email Gateways. Business risk and SOC overload is reduced dramatically through rapid containment of phishing threats using continuous monitoring and detection, automated response and remediation, and effective employee engagement.

CYREN

Cyren is a messaging security company that protects enterprise email users from today's evasive threats and supplies threat intelligence solutions to security software integrators, hardware OEMs, and large service providers. Cyren's GlobalViewTM threat intelligence network analyzes billions of email and web transactions daily and is trusted by companies like Microsoft, Google and Check Point, who utilize Cyren's APIs and SDKs to operationalize threat intelligence for their customers.

**HEADQUARTERS**

**US Virginia**
1430 Spring Hill Road Suite 330
McLean, Virginia 22102
Tel: 703-760-3320
Fax: 703-760-3321

**SALES & MARKETING**

**US Austin**
10801-1 North Mopac
Expressway Suite 250
Austin, Texas 78759

**UK Bracknell**
Maxis 1
43 Western Road
Bracknell Berkshire RG12 1RT

**US Silicon Valley**
1230 Midas Way Suite 110
Sunnyvale, CA 94085
Tel: 650-864-2000
Fax: 650-864-2002

**R&D LABS**

**Germany**
Hardenbergplatz 2
10623 Berlin
Tel: +49 (30) 52 00 56- 0
Fax: +49 (30) 52 00 56- 299

**Iceland**
Dalshraun 3
IS-220, Hafnarfjordur
Tel: +354-540-740

**Israel**
1 Sapir Rd. 5th Floor, Beit
Ampa P.O. Box 4014
Herzliya, 46140
Tel: +972-9-8636 888
Fax: +972-9-8948 214

Cyren.com
@CyrenInc
linkedin.com/company/cyren