EXECUTIVE SUMMARY

Responding To Inbox Threats: Where Do You Begin?

An increasingly dangerous threat ecosystem

More threats are landing in your inbox everyday. And they're growing too, not only in volume but in sophistication, evasiveness and variety. Nowadays your employees are liable to being extorted for money by ransomware, tricked into opening malicious file attachments, fooled by spoof sites and deceived by downloads from client-side attacks. Not to mention the number one cybersecurity threat facing businesses today - phishing.

But the problem isn't just that these attacks are breaching existing defences and landing in your inbox. It's that they're also taking time to detect and remediate. The larger that window is, the quicker these attacks spread throughout your organisation and the more damage they end up doing.

A different kind of email security

It's clear that there needs to be an enhanced level of inbox protection to deal with these threats. One that can detect and remove even the most advanced phishing attacks from every email account in your organisation quickly and easily.

So what are the key components needed for this new kind of email security to be effective? We've identified three vital elements.

Automation

It's important that any response to phishing incidents is automated. Because simply reporting phish with the click of a button won't get rid of it. All that happens is that they're transferred over to the response team who then have to deal with them. And when these incidents pile up, which they inevitably do, they result in delays. The influx of alerts, 40,000 on average per month, means they're not only struggling to keep with the responses, they're creating more time for the attack to circulate and cause damage. But by automating phishing incident responses, you're empowering the business to better manage the deluge of alerts, giving them visibility over the entire threat situation and helping them prioritise urgent cases.

It also means security teams no longer have to manually investigate each and every threat they're alerted to, which can be up to 615 in a week. And it eliminates the risk of serious threats being overlooked. Easily done when you're fatigued, but at a huge cost to the business. In fact, according to the Anti-Phishing Working Group, the cost of a successful business email compromise attack is exponentially increasing. So much so that the average wire transfer attempt between April and June 2020 was USD$80,183.

That's why security teams need better tools to combat the sheer volume and diversity of threats they're facing. Having a solution like Cyren Inbox Detection and Response automating the process of phishing incident response eases the burden on your staff and makes remediation quicker and easier. It sits right at the heart of your inbox and strengthens your security by continuously monitoring, detecting and automatically removing even the most advanced phishing attacks from every mailbox.

A multi-layered approach

As any cybersecurity professional will already know, there's no catch all for every threat. You need a layered, adaptive security architecture that can prevent, detect, respond to, and predict threats. Something that's noticeably absent in corporate email security today.

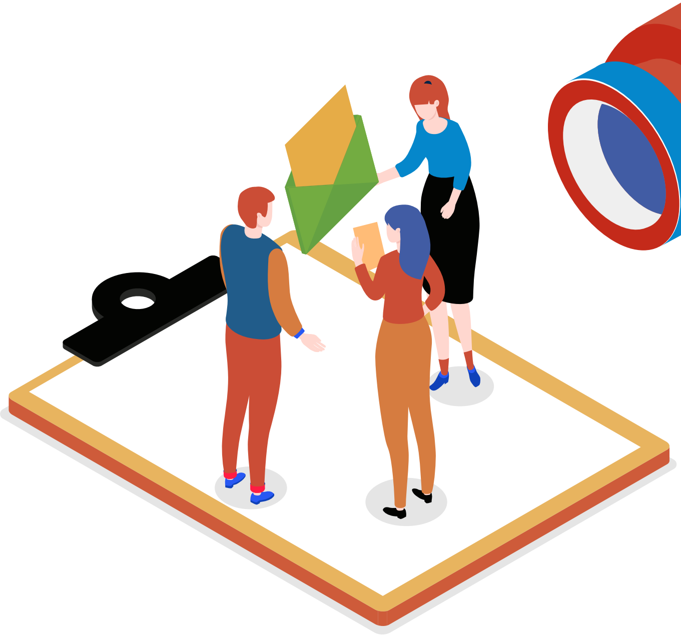
Right now, many businesses still rely only on the prevention delivered by the deployment of a secure email gateway (SEG) at the network perimeter. These are designed with just one purpose in mind: to prevent email-borne attacks from penetrating your network. But as phishing attacks grow in number and sophistication, many are getting through the SEG and reaching your inbox, despite improvements in filtering and performance technology.

The rise in successful email-borne phishing attacks is driven by 3 main factors:

1. **First**, the ubiquitous use of Office 365. This makes it a popular target for cybercriminals, mainly because it creates an attractive and convenient launch surface for attacking hosted email platforms in the cloud.

2. **Second**, The increasingly sophisticated evasion techniques being used by phishing attacks to avoid detection. This includes the use of social engineering to create a sense of urgency that induces people to cooperate.

3. **Third**, Cybersecurity skills are in short supply. Many IT teams are stretched to their limits and when depleted staff are continuously bombarded by security alerts, it's inevitable that some will slip under the radar.



Organizations need to act now to bolster their perimeter approach to email security, particularly in light of the increased vulnerability presented by the migration to cloud hosted services like Office 365. It's expected that by 2021, 70% of public and private companies will be using cloud email services. Already we're seeing 1 in 5 corporate employees use the OffIce 365 service. And yet with 78% of Office 365 administrators reporting security breaches with phishing as the leading cause, it's clear something needs to be done.

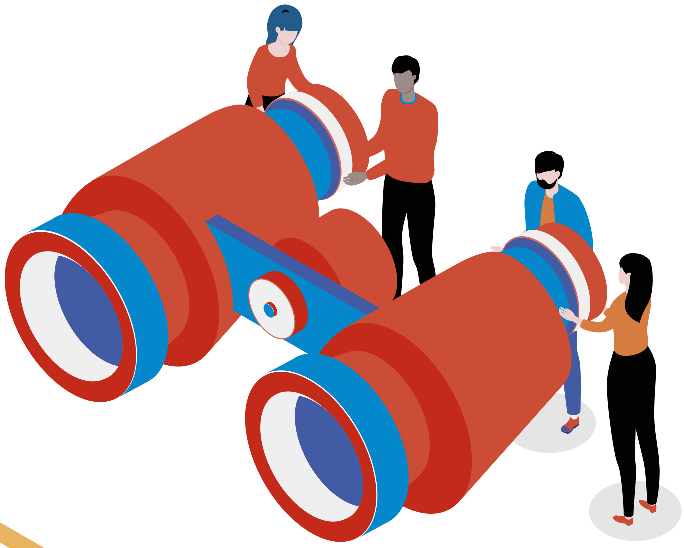
Cyren's Inbox Detection and Response catches all the phish that got away by providing an automated and adaptive layer of cybersecurity right in the mailbox. Through continuous monitoring, detection, automated response and remediation, it fills the gaps in detection and remediation left by the SEG, greatly reducing business risk and the burden shouldered by security teams.

Responding quickly

From ransomware, zero-day malware, account takeovers and brand hijacking to all the different types of phishing, security threats are not only increasing in volume but in diversity too.

With cybercriminals often acting at speed when carrying out phishing campaigns, the ability to respond quickly is essential to minimising the risk of serious damage.

Unfortunately security teams are stretched way beyond capacity. They deal with too many alerts, too many false positives and unfortunately, there's just simply not enough of them to do the work. That's why it came as no surprise when a study published in 2020 found that 76% of respondents reported a shortage of cybersecurity skills in their teams.



But with good visibility and intelligence, researchers, analysts and others can address threats with minimum processing and analysis. This results in a quicker, more efficient process and a more proactive security capability that can anticipate, detect and prevent attacks before they start causing damage.

The reality is most organizations have experienced some sort of security breach, whether it's the smallest bit of malware infecting a single computer or a full-blown ransomware attack. And the length of time that these threats spend in the system before being detected - known as the dwell time - vary widely. Often it's 24 hours or less, but some threats can take considerably longer. Trends Report states that the median dwell time in 2019 was 56 days, down from 78 days a year earlier. While that's a positive sign that things are improving, it's still not ideal having a security breach roaming around in your corporate networks for 8 weeks undetected. Because the longer that dwell time is, the longer these cybercriminals have to learn about the internal workings of your business. You're giving them the opportunity to craft a highly targeted and effective attack that is more sophisticated and harder to detect and remediate by conventional means.

But when you've got the right threat intelligence offering timely, detailed information on indicators of compromise (IOCs) and IP addresses of concern, you can thwart these attacks more quickly. And by harnessing this intelligence to gain insight into the tactics, techniques and procedures employed by cybercriminals, security teams are better prepared to anticipate future attacks too.

Cyren Inbox Detection and Response offers continuous monitoring that gives you far better visibility and understanding of the threat landscape. It creates the opportunity for you to react in real-time and often at the same speed with which the cybercriminals are carrying out their attack. And by slashing the dwell time of these threats, you're minimising business risk and protecting your inbox from future phishing attacks.

So what can you do now?

It's clear that traditional, gateway-focused email security isn't going to stop threats from reaching your inbox. For businesses to protect themselves from an ever more pervasive and diverse phishing industry, they need a different kind of security. Something that works in tandem with your SEG to catch all the phish already landing in your inbox. Something that provides you with enterprise-wide visibility over every threat and can act automatically to remove them for you.

Cyren's Inbox Detection & Response solution is an adaptive, automated layer of additional security that continuously scans your email inboxes looking for phishing attacks. It monitors behaviours and incorporates feedback from you to identify and automatically remediate even the most advanced threats. Giving you the visibility you need to protect your business and saving you valuable time and effort.

You'll be in safe hands too. More than 1.3 billion users around the world rely on Cyren's security solutions for protection against cyber attacks and data loss every day.

Click here to learn more about what Cyren IDR can do for you

LEARN MORE