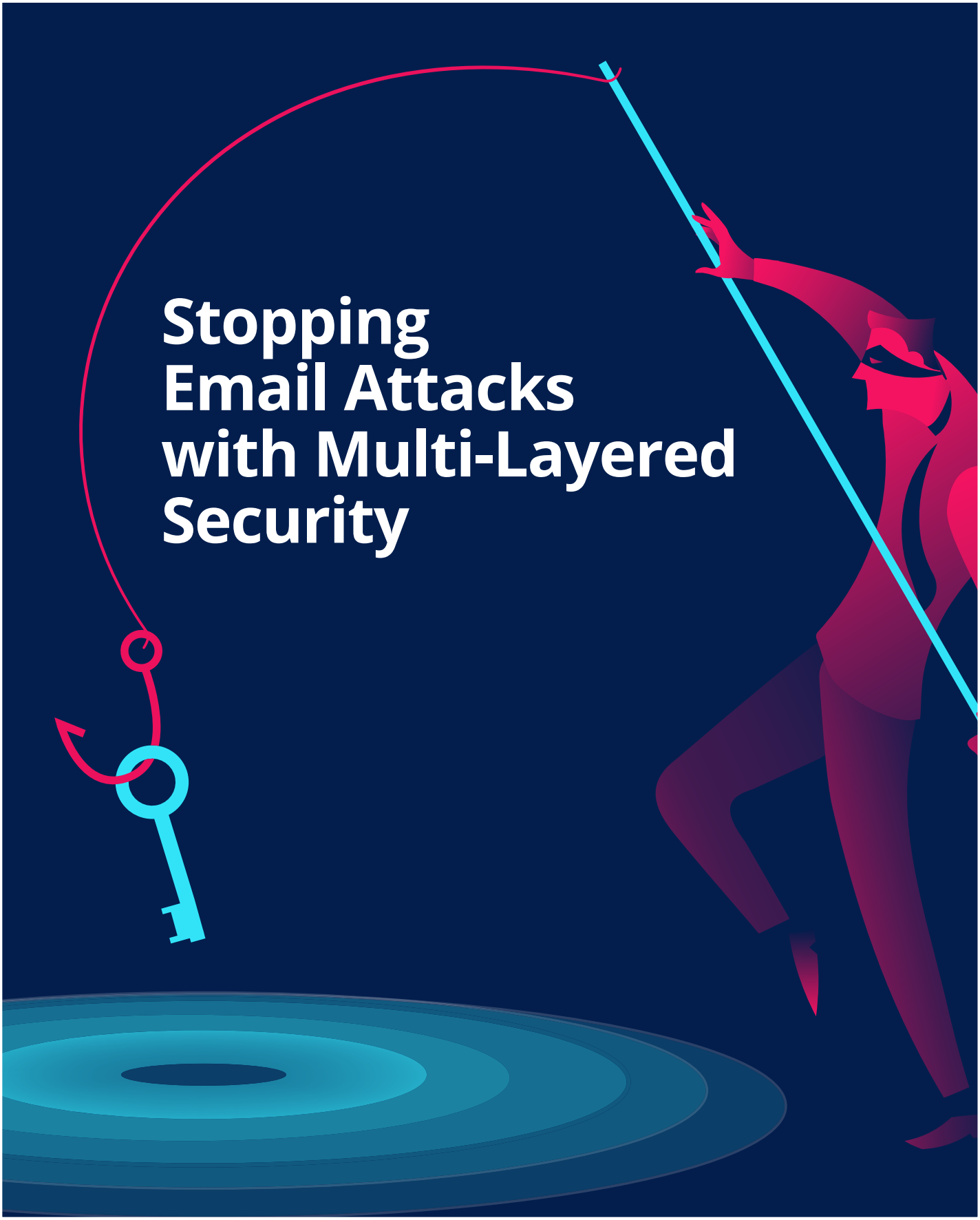
GoSecure

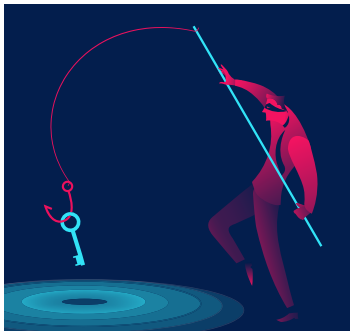
EMAIL
SECURITY
EBOOK

Stopping Email Attacks with Multi-Layered Security



Stopping Email Attacks with Multi-Layered Security

EMAIL SECURITY EBOOK



According to the latest FBI Internet crime report, Business Email Compromise (BEC) continues to be the most impactful cybercrime. The FBI estimates 2021 losses at nearly $2.4 billion in the US alone. As the gateway to many other cybercrimes including ransomware, phishing attacks like BEC are a key threat faced by companies of all sizes, and one of the main entry points threat actors use to infiltrate networks. Email security defenses are evolving but so are the tactics threat actors use to circumvent those defenses. While a vital part of a multi-layered defense strategy, traditional email security gateways alone are no longer enough.

This eBook examines the evolving threat landscape, how IT and business leaders have tried to thwart phishing and BEC attacks in the past, and best practices that can be applied to increase email security, reduce downtime, and help eliminate the threat of ransomware and other advanced attacks.

Setting the Stage: The Evolving Threat Landscape

Cyber threats are proliferating in number and frequency, with the FBI Internet Crime Complaint Center (IC3) averaging over 500,000 complaints in the past five years and reporting total losses exceeding $18 billion in the US alone. Since the beginning of the pandemic, cybercrime is up 600% with the average time to identify a breach climbing to 207 days (about 7 months)[1]. While ransomware gets the headlines, the number one crime in terms of impact was BEC, which itself can be a vector for phishing and ransomware.

Even though email malware attacks surged by over 150% between 2020 and 2021[2], many organizations continue to rely on older email security solutions with limited anti-malware capabilities. And even if the anti-malware technology has been updated, organizations are not taking advantage of the updates. In this type of

environment, it's not surprising that over half of all small to midsized businesses (SMBs) were victimized by cyberattacks last year, and 90 percent of those attacks began with a phishing email (Verizon DBIR 2021).

The Struggle is Real to Maintain Email Security

The cybersecurity skills shortage, combined with the proliferation of cyber-attacks, continues to challenge IT and security teams charged with keeping email safe. A recent International Information System Security Certification Consortium study[3] pegged the number of unfilled cybersecurity positions around the world at 4.07 million. A direct impact of this resource shortage is the inability to prioritize and respond to security alerts, with 70% of IT security decision-makers saying they are "emotionally overwhelmed" by security alert volume.[4]

These overwhelmed teams struggle to manage day-to-day tasks such as detecting and analyzing suspicious emails. More than 70 percent of organizations use only manual processes for reviewing user-reported phishing emails[5], making it far too labor-intensive. And the statistics can be alarming:

24%: The amount of 40-hour workweek security analysts spend investigating, detecting, or remediating phishing emails[6]

82 Seconds: The scant amount of time until the first link is clicked on during a typical phishing attack[7]

USD $8,900: The monthly cost of managing phishing attacks for an organization with 5000 users[8]

75%: The percentage of organizations that do not have the resources to act on phishing intelligence in real-time[9]

Clearly, the security skills shortage is having an impact on an organization's ability to deal with phishing properly and the strain

Stopping Email Attacks with Multi-Layered Security

on IT is palpable, and more importantly takes time away from other priorities.

The Impacts and Risks of Successful Attacks

Successful phishing and BEC attacks are just the tip of the iceberg. If successful, cybercriminals use their newfound access to:

- Exfiltrate data
- Encrypt enterprise disks to extort ransomware
- Maliciously cause downtime
- Hijack computing and network resources

When attacks are successful, those compromised experience a range of hard and soft costs including loss of customer goodwill, brand damage, revenue losses, and increased insurance premiums. Compromised businesses often must then face increased workforce costs to repair and remediate cybercrime, adding insult to injury.

How bad can it be? The 2021 IBM / Ponemon Data Breach Report found the average data breach cost roughly $4.24 million, and the Cyber Security Alliance reports that 60% of small businesses that suffer a breach or cyberattack are *out of business within six months of the attack*, due to lack of resources, lack of remediation expertise, lack of time, and the continued difficulty in finding and keeping cybersecurity talent.

Traditional Email Security Is Not Enough, Here's Why

Secure Email Gateways (SEGs) are highly effective at preventing spam and most malicious emails from reaching user inboxes. For example, GoSecure's Secure Email Gateway dynamically adjusts to emerging threats by combining Machine-Learning, behavioral scanning, exploit preventions, signature-based detection and structure heuristics to determine if an email poses a possible threat.

Unfortunately, traditional security layers such as SEGs and antivirus have a tough time catching and stopping evasive phishing. Evasive phishing is not new, but threat actors are constantly evolving, their tactics are becoming more sophisticated

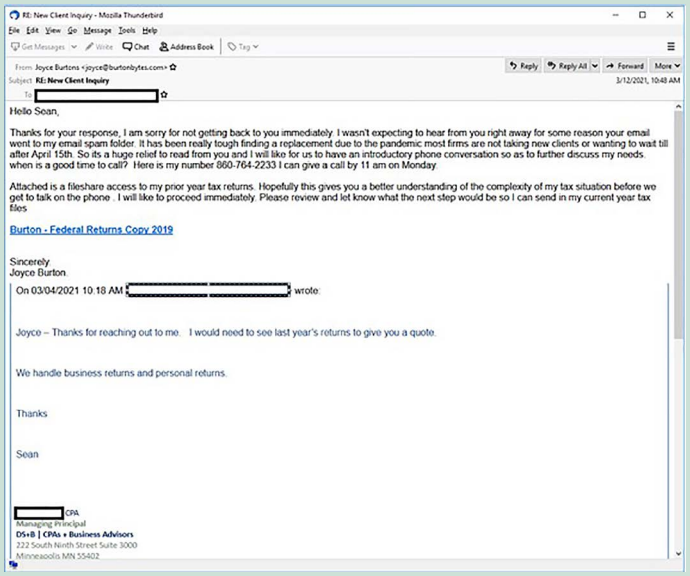
as they continue trying to evade detection with their increasingly targeted attacks. The existence of offerings like Phishing-as-a-Service indicates how advanced and profitable phishing campaigns have become, and why they work so hard to remain effective.

Protection Requires a Multi-Layered Approach

A multi-layered approach is required when dangerous emails make it through email security filters so that the end user can be part of the solution. Although no layer is 100% effective on its own, combining

The Bait Phish

Although SEGs are very effective, cyber criminals look for ways to evade them and ultimately some malicious emails end up in user inboxes. For example, an apparently innocuous email may be the first in a series designed to engender trust in the recipient and may not include a payload or request until a conversation is well established.



In this sample the threat actor uses a ploy to trick the recipient into asking for something from the threat actor. The threat actor is emailing a CPA looking for help in preparing business taxes. In this case the threat actor bought a new domain name called burtonbytes.com, which was only a couple of months old at the time; of course there was no web presence, but the domain existed and any check by a spam filter or an email gateway would come back clean. So, after the initial email to the CPA, the response is "Sure, we can help! Can you send me your taxes from last year?" The response from the threat actor has a link which leads to a file sharing host mega.nz, and having already established communication, it is almost a given that the potential victim will click on the link and download and run the MALDOC.

several layers together provides dramatic results. However, adding additional layers of security can also burden existing security teams, for example with the additional workload of analyzing suspicious emails. Ideally, organizations should build additional layers of security without impacting already overburdened security teams.

CASE STUDY: Protection Requires a Multi-Layered Approach

Law firms are a big target for threat actors. There are many examples of business email compromise, lawyer scams, credential theft, wire fraud and phishing – many of which could easily bypass any filter or AI driven solution. There is nothing of note to set off red flags as many of these emails are from legitimate sources and don't contain any or very few suspicious elements.

A large corporate law firm serving clients worldwide adopted GoSecure Inbox Detection and Response (IDR) as part of its email cybersecurity program for its 1100 email users. Over 3,000 emails were submitted to GoSecure IDR and malware or phishing attempts were found in nearly half – 46% of the suspicious emails submitted.

The breakdown of the threats detected in those emails included:

- **23% were credential stealing phishing attempts**
- **11% were BEC phishing attempts**
- **8% were Refund/Invoice Fraud**
- **7% were targeted law firm phishing fraud attempts**
- **3% were fraud or wire fraud attempts -non law firm specific**
- **2.5% were email harvesting phishing**
- **.08% were virus infection attempts**
- **Of the remaining 54% of emails submitted, 8% on average were marked "Caution", while 41% were marked "Spam".**

This is where IDR makes a difference – through knowledge, experience and research, IDR analysts can tell what is legitimate and what is an attempt at fraud. IDR provides that human element in identifying and stopping email threats from going any further.

Stopping Email Attacks with Multi-Layered Security

A post-delivery layer, like GoSecure's Inbox Detection and Response (IDR), can help support end-users by providing an easy way to submit any email they find suspicious for examination by skilled professionals. This helps support and reinforce programs like cybersecurity training, as well as combat the dangers of phishing attacks.

The GoSecure Difference

With over a decade of experience in email security, GoSecure understands the need for a multi-layered approach to address the limitations of traditional security tools. What makes GoSecure a leader in email security is the combination of SEG with IDR to provide comprehensive, in-depth

When looking to add a post-delivery layer of email security to address the phishing gap, organizations should consider:

- **Ease of use and deployment** – is it a simple integration with existing mail clients?
- **Impact to existing resources –** does it add or reduce workload to manage?
- **A positive reinforcement loop** that delivers responses or resolution in minutes not days
- **The ability to train users over time** via self-validation of submissions
- **An experienced team** that augments Artificial Intelligence and Machine Learning with trained humans who can evaluate questionable emails based on years of expertise
- **The ability to turn a perceived weakness (curious users) into an asset.** Users are on the front line when it comes to attacks, making their email submissions vital intelligence in preventing breaches.

All these benefits – and more – can be realized with GoSecure Inbox Detection and Response (IDR).

defense at both the pre-delivery and post-delivery stages.

GoSecure SEG provides:

- Industry leading inbound/outbound spam, malware, and antivirus filtering
- Mail reputation and custom filtering rule sets
- Defense from spam, viruses, spyware, phishing schemes, and identity theft
- Automated seamless directory integration
- All in a hosted SaaS solution that can be provisioned in minutes not days

How does GoSecure Titan® Inbox Detection & Response Work?

1. Employee notices suspicious email and clicks the GoSecure Titan IDR button to begin the submission process.
2. Email is automatically quarantined and routed through the GoSecure Active Response Center.
3. GoSecure automated machine learning engines investigates the suspicious email.
4. Human security experts conduct a further review on inconclusive messages through a multi-faceted analysis.
5. Within minutes a status message is returned, either the message is verified or removed.
6. Real-time reporting gives the in-house security team clear visibility into the incident and its resolution.

Next Steps:

- **Learn more by watching this video https://www.gosecure.net/inbox-detection-response/overview-video/**
- **Request a demo of GoSecure Inbox Detection and Response: https://www.gosecure.net/sales-contact/**

The GoSecure IDR post-delivery managed detection solution is a unique offering that

- Removes the guesswork and provides a simple automated process for employees to report suspicious emails with one click
- Utilizes the security experts in the GoSecure Active Response Center (ARC) to investigate emails with capabilities beyond those that automation only can deliver
- Supports the in-house security team and alleviates resource constraints by removing the burden of email review

When an employee submits a suspicious email, GoSecure IDR provides rapid and accurate investigation and incident response, which is critical since it can take days for internal teams to review and evaluate submissions. This accelerates the time from first detection to complete containment, and the shorter the lifecycle of a threat, the smaller the cost to the organization.

The positive feedback loop offered by GoSecure IDR helps activate employees as the front line of defense.

GoSecure IDR is easy to deploy with minimal impact to internal teams and does not require users to learn a new email client to successfully protect emails. And GoSecure IDR works with already installed email gateways so organizations can add another layer of defense without having to replace existing technology.

In addition, GoSecure has a breadth of security knowledge and is much more than an email security provider. This enables

GoSecure to take intelligence gleaned from other parts of their security suite and apply them to email security. This holistic 'cross-pollination' combined with research from GoSecure Titan® Labs provides more intelligence than many other email-only security providers.

The difference is in the numbers: GoSecure has analyzed hundreds of thousands of submitted emails, of which nearly 60% were found to be malicious – a testament to not only the GoSecure staff but the increasing accuracy of the users submitting emails for quarantine and analysis.

---

[1]PurpleSec
[2]https://www.techrepublic.com/article/how-midsize-companies-are-vulnerable-to-data-breaches-and-other-cyber-attacks/
[3]https://thecyberwire.com/stories/0e1b915f738448e181cc72ab3fa42f37/understanding-the-cybersecurity-skills-gap-and-how-education-can-solve-it
[4]https://venturebeat.com/2021/10/12/enterprises-struggle-with-security-monitoring-tool-sprawl/
[5]Osterman Research
[6]Ibid
[7]Verizon DBIR
[8]Osterman Research
[9]ibid

About GoSecure

GoSecure is a recognized cybersecurity leader, delivering innovative managed security solutions and expert advisory services. GoSecure Titan® managed security solutions deliver multi-vector protection to counter modern cyber threats through a complete suite of offerings that extend the capabilities of our customers' in-house teams. GoSecure Titan Managed Detection & Response (MDR) offers a best in class mean-time-to-respond, with comprehensive coverage across customers' networks, endpoints and inboxes. For over 10 years, GoSecure has been helping customers better understand their security gaps, improve organizational risk and enhance security posture through advisory services provided by one of the most trusted and skilled teams in the industry. To learn more, please visit: https://www.gosecure.net.

gosecure.net | 855-893-5428