cymulate

Relieving the Stress from Email-Based Threats

Secure Email Gateway Validation

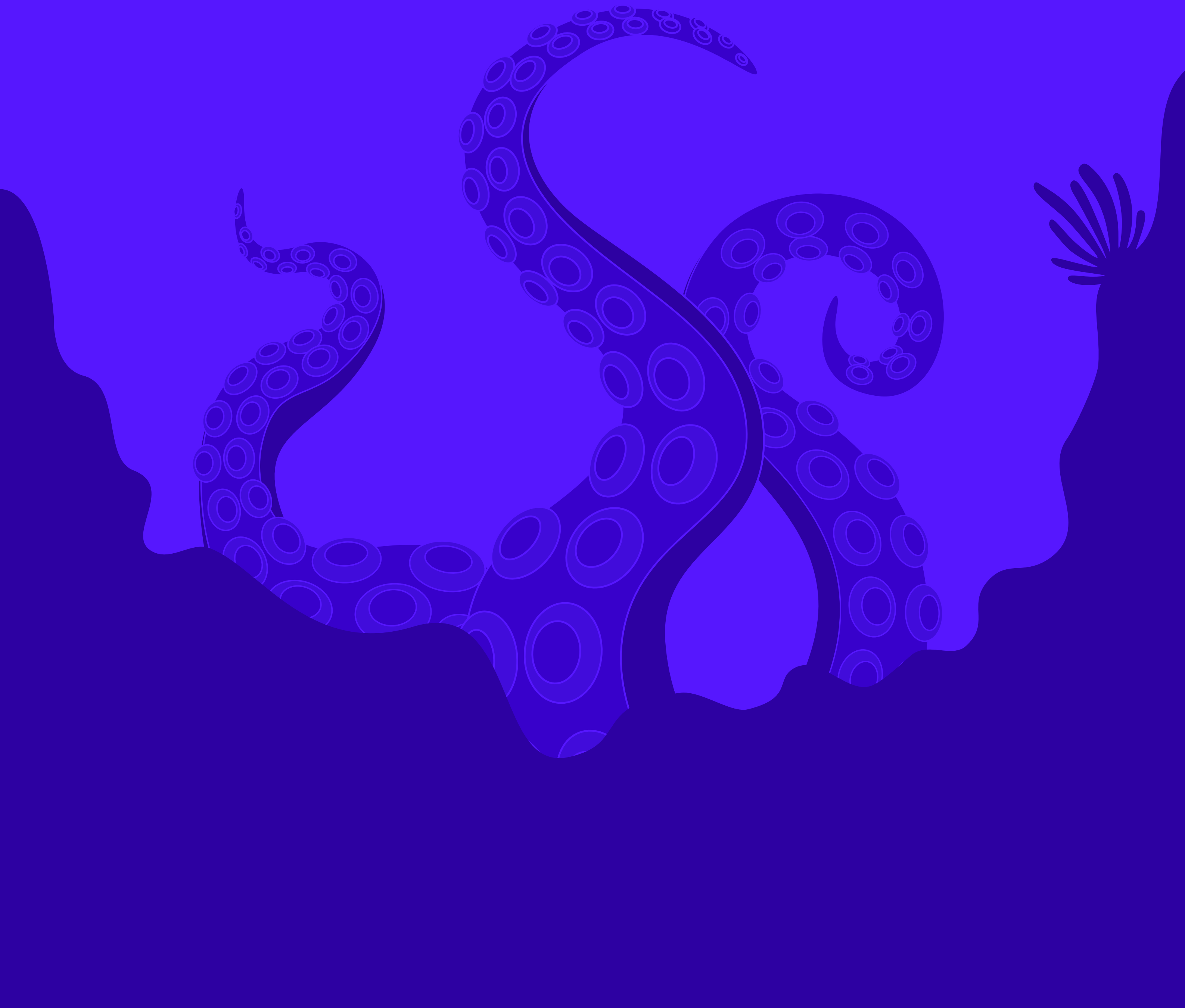


Table of Contents

01 Introduction

Email is the most prevalent form for the initiation of a cyber attack and the preferred method of many threat actors seeking to steal credentials or deploy malicious payloads that exploit security weaknesses. And it is the unsuspecting business user community (aka your people) who are the primary target of these phishing campaigns.

Sophisticated threat actors undertake recon activities to gain knowledge of a business, so they can cleverly devise spear-phishing emails and malicious content that can trap even the most discerning users. These emails are very personalized and targeted, using business information often gained from social media sites to make them look like legitimate business emails.

According to the 2024 Email Security Risk Report by egress, 94% of organizations fell victim to a phishing attack and 94% of organizations experienced email-based security incidents. With numbers like these, is it any wonder that cybersecurity leaders are stressed about email security.

Email remains the #1 attack vector for cyber criminals

Source: The State of Email & Collaboration Security Report 2024 by Mimecast

95% of cybersecurity leaders are stressed about email security

Source: 2024 Email Security Risk Report by egress

02

Notorious Email-Based Attacks of the Past Decade

Over the past decade we have seen some of the most notorious cyber attacks that began with phishing emails. These attacks serve as a constant reminder of the need to continuously optimize email security controls and stay vigilant as users when it comes to opening an email.

2023

T-Mobile

In January 2023, T-Mobile disclosed a data breach that was the result of a phishing attack. The attack allowed hackers to access personal data of 37 million customers, including names, addresses and birth dates. This breach highlighted the ongoing risks faced by telecom companies and the importance of securing customer data against phishing attacks.

2022

U.S. Department of Labor

A phishing campaign targeted the U.S. Department of Labor, with emails impersonating the agency and containing malicious links. These emails aimed to steal login credentials from employees. The attack was part of a broader campaign targeting various government entities, highlighting the persistent threat of phishing to critical infrastructure.

2021

Colonial Pipeline

Although the initial access vector is not confirmed to be phishing, it is suspected that phishing emails played a role in gaining initial access. The ransomware attack by the group DarkSide led to the shutdown of the largest fuel pipeline in the United States. The attack caused fuel shortages and disrupted supply chains along the East Coast. Colonial Pipeline paid a ransom of $4.4 million, although a portion was later recovered by the U.S. Department of Justice.

2020

SolarWinds Attack

This sophisticated supply chain attack involved a phishing campaign where attackers sent emails containing malicious links to SolarWinds customers. Once clicked, the link led to the download of a compromised version of SolarWinds' Orion software. The breach affected multiple U.S. government agencies and numerous private sector companies, exposing sensitive information and leading to a massive security overhaul.

2019

Wipro

Indian IT services giant Wipro experienced a major breach through a phishing campaign targeting its employees. The attackers used compromised credentials to access Wipro's systems and launch further attacks on Wipro's clients. The breach affected several of Wipro's clients, raising concerns about the security of IT service providers and their ability to protect client data.

2018

Marriott International

The breach began with a phishing attack targeting Starwood Hotels employees. Once hackers gained access, they maintained a presence in the network for several years, exfiltrating data. The personal information of up to 500 million guests was exposed, including names, addresses, phone numbers and passport numbers.

2017

Ukrainian Power Grid

In December 2017, a phishing attack targeted Ukraine's power grid, sending emails with malicious attachments to employees. The malware used in the attack was designed to disrupt the power supply. Although the attack did not cause a major blackout, it highlighted the vulnerability of critical infrastructure to phishing attacks and the potential for significant disruptions.

2016

Democratic National Committee (DNC) Hack

Russian hackers, allegedly from the group known as Fancy Bear (APT28), sent spear-phishing emails to members of the Democratic National Committee. These emails tricked recipients into providing their login credentials, leading to a significant breach of the DNC's email systems. Thousands of emails were stolen and subsequently leaked, causing major political repercussions and impacting the 2016 U.S. presidential election.

2015

Anthem Health Insurance

Anthem, a health insurance giant, suffered a breach after employees fell for phishing emails that stole their credentials. Hackers accessed a database containing sensitive information. The breach exposed the personal information of nearly 80 million individuals, making it one of the largest healthcare breaches in history.

2014

Sony Pictures Hack

The hacker group Guardians of Peace sent phishing emails to Sony Pictures employees. Once they gained access, they deployed malware that compromised Sony’s network and exfiltrated a large amount of data. The attack led to the release of confidential company emails, personal information of employees, and unreleased films. It caused severe damage to Sony’s reputation and led to substantial financial losses.

These attacks highlight the devastating impact that can occur by simply opening and acting on the wrong email.

Email security can be triangulated to your people, process and technology. The people side comes down to phishing awareness training and red team exercises to emphasize user vigilance to spot suspicious emails. Technology is also key with the use of a Secure Email Gateway (or SEG) solution to detect and block email-based threats. This whitepaper will explore the third side of the triangle (process) and the need for email gateway validation as a continuous process given the always evolving nature of email-based threats. By addressing all three sides of the triangle, you can better protect your users and fortify your defenses against email attacks.

03

Secure Email Gateway Control

A secure email gateway is one of the most effective security controls to block end users from ever receiving malicious emails. It is your first line of defense against email-based threats and stopping a key source of cyber attacks on your business.

The email gateway monitors and filters email communications to protect organizations from various email-borne threats and provide:

- Spam and Phishing Protection
- Malware Detection and Prevention
- Content Filtering
- Email Policy Enforcement
- Data Loss Prevention (DLP)
- Email Encryption
- Attachment and URL Sandboxing
- Advanced Threat Protection

Implementing a secure email gateway is the first step in protecting your email infrastructure and users from a wide range of threats, ensuring the safety and security of email communications.

However, an email gateway is not the only step required to stop email-based threats. You also need to continuously validate that your email gateway control is operating effectively against a constantly evolving group of advanced threat actors and the tactics and techniques they use to exploit email and your users.

04
Email Gateway Validation Best Practices

Threat actors constantly launch new malicious websites and content they can use in their latest phishing campaigns to entice users to click on a bad link or download a malicious payload as part of the attack chain. There is a growing list of known bad websites and URLs that should be blacklisted and blocked by your email gateway.

So how do you know if your email gateway is configured correctly and tuned to detect and block the latest email-borne threats?

The answer to that question lies in establishing a process of continuous email gateway validation that tests the gateway on a frequent basis (we recommend weekly validation) using a full range of the latest known bad links, malicious payloads, and other deceptive tactics. Email gateway validation should include test cases for the following attack types:

Malicious Links

Malicious links in the body of an email are a common tactic used by threat actors to deliver malware, steal credentials, or engage in other harmful activities. The email gateway should be tested for a full range of malicious links in the email body.

Malicious Attachments

Malicious attachments in emails are a common method used by threat actors to distribute ransomware, worms, trojans, and malware variants that perform malicious activities. These attachments can appear in various forms, including documents, spreadsheets, executables and compressed files, and they can have devastating effects if opened. The email gateway should be tested for emails containing different malware samples embedded as attachments to the email.

Executable Payloads (Attachments)

Executable payload attachments in emails are a significant threat, often used to deliver malware such as ransomware, trojans and worms. These attachments are designed to look benign, but once opened, they execute malicious code on the victim's system. Executable payloads typically include file types like executables (.exe), command files (.com), script files (.scr, .js, .vbs). Validation of the email gateway should test policy enforcement for handling emails with executable payloads like .exe, .com, .scr and other executable file extensions.

Dummy Code Execution

Simulate the possibility for real malicious code execution using dummy files with potential code execution capabilities. These files are not actually malicious, but they do show proof of concept for inserting executable code into an organization.

True File Type Detection

True file type detection is a crucial security measure to identify and block malicious files that masquerade as benign files. Threat actors often disguise malicious files by changing their extensions or manipulating file headers to bypass security systems. True file type detection involves inspecting the actual content of a file, rather than just relying on its extension, to determine its real type. Validation of the email gateway should test whether executable payloads with forged extensions are effectively blocked by the gateway.

File Attachment Policies

Creating and implementing robust email attachment policies is crucial for protecting your organization from the risks associated with the malicious attachments above. Validation of the email gateway should include the testing of policy enforcement for handling and blocking different file types.

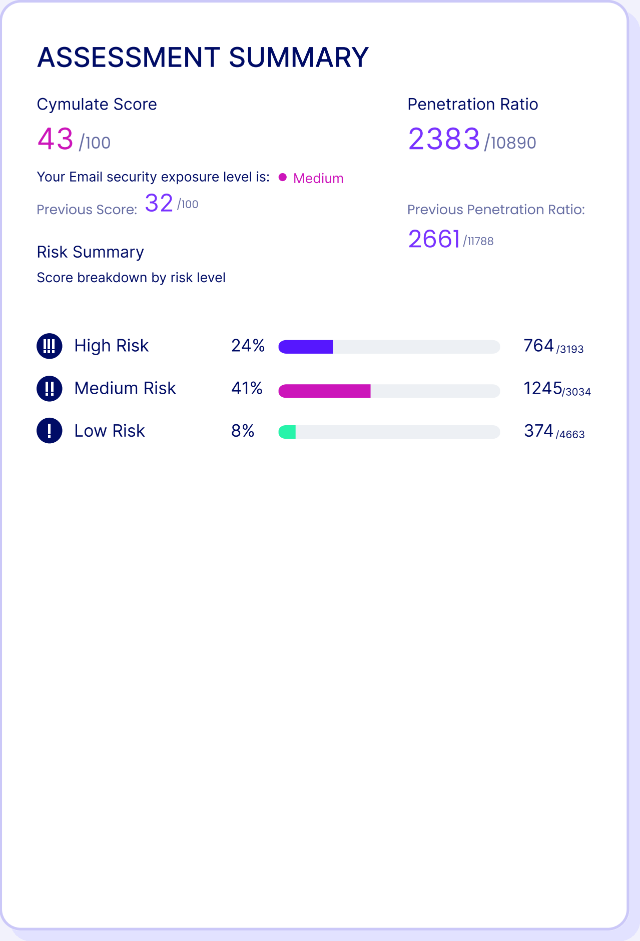
05

Breach and Attack Simulation for Email Gateways

The Cymulate platform delivers a production-safe assessment of your email gateway efficacy using a wide-range of malicious links and payload variants to provide insight into the effectiveness of your cybersecurity controls and policies. The assessment is a breach and attack simulation of the latest email-based threats against your secure email gateway to deliver the following outcomes:

- **Enable** continuous validation and improvement of your secure email gateway.
- **Identify** gaps and weaknesses in your email gateway controls and policies.
- **Optimize** protection based on mitigation guidance to filter and block the latest attack types.
- **Measure** the effectiveness of your email security controls over time.

The assessment summary report provides an overall Cymulate score out of 100 and an email security exposure level of minimum, low, medium or high for your secure email gateway performance. The assessment also shows the penetration ratio of how many emails get passed the gateway against the total number of emails sent. A score of 33 or better is considered an acceptable risk, however, each attack type should be further analyzed so that tuning and configuration of the email gateway can deliver continuous improvement over time as measured by your Cymulate score.



ASSESSMENT SUMMARY

Cymulate Score

43 /100

Your Email security exposure level is: ● Medium

Previous Score: 32 /100

Penetration Ratio

2383 /10890

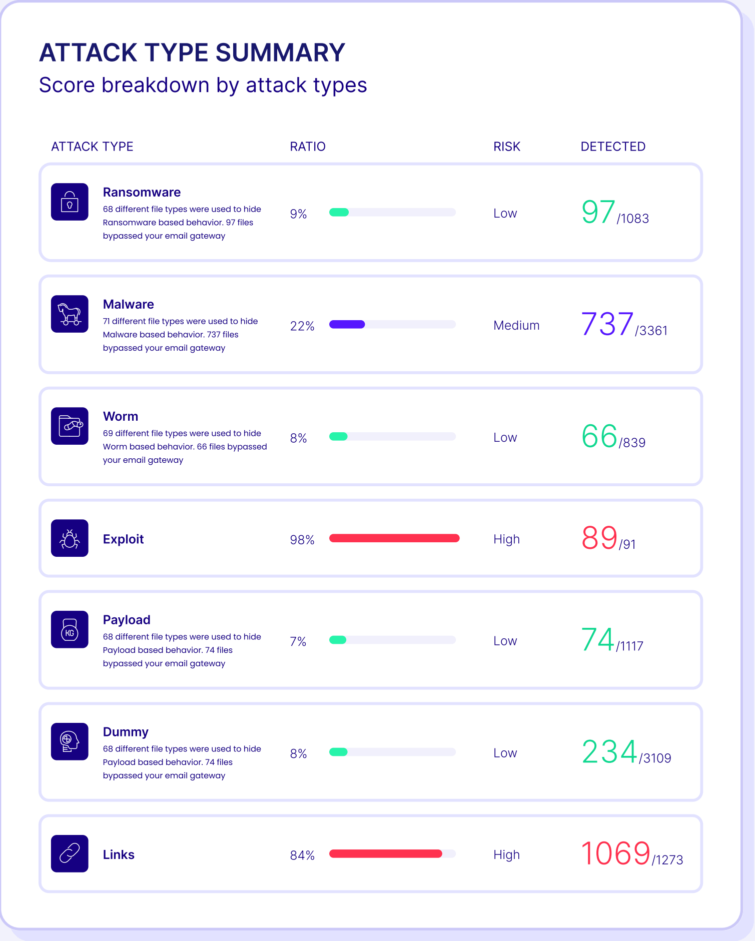
Previous Penetration Ratio:

2661 /11788

Risk Summary

Score breakdown by risk level

!!! High Risk	24%	764 /3193
!! Medium Risk	41%	1245/3034
! Low Risk	8%	374 /4663



ATTACK TYPE SUMMARY

Score breakdown by attack types

ATTACK TYPE	RATIO	RISK	DETECTED
Ransomware 68 different file types were used to hide Ransomware based behavior. 97 files bypassed your email gateway	9%	Low	97 /1083
Malware 71 different file types were used to hide Malware based behavior. 737 files bypassed your email gateway	22%	Medium	737 /3361
Worm 69 different file types were used to hide Worm based behavior. 66 files bypassed your email gateway	8%	Low	66 /839
Exploit	98%	High	89 /91
Payload 68 different file types were used to hide Payload based behavior. 74 files bypassed your email gateway	7%	Low	74 /1117
Dummy 68 different file types were used to hide Payload based behavior. 74 files bypassed your email gateway	8%	Low	234 /3109
Links	84%	High	1069 /1273

The Cymulate email gateway assessment sends over 10,000 production-safe emails to a dedicated Cymulate email box within your email domain. These email test cases are production-safe with no malicious payload or code execution that could impact your production environment. A full suite of test cases exists for each attack type and the report highlights which types represent the highest level of risk. Security operations teams can use this information to focus their attention on specific attack types which their email gateway is not blocking and use the mitigation guidance to enhance the effectiveness of their controls and policies. The assessment includes a comprehensive range of email-based threat samples, including:

Ransomware	1,000+ samples using 60+ different file types
Malware	3,000+ samples using 70+ different file types
Worms	800+ samples using 60+ different file types
Exploits	90+ samples
Payloads	100+ samples using 60+ different file types to hide payloads
Links	1,200+ malicious links
True File Types	800+ different file types
Email Policy	170+ email policy tests
Dummy Code	3,000+ samples with 200+ files used to hide malicious code

The test cases are continuously updated in the platform based on the latest known malicious links and payload variants. The automated assessment enables the full suite of test cases to be executed frequently. Based on the constantly evolving landscape of email-based threats, Cymulate recommends that these best practice assessments be executed on a weekly basis to test for the latest email-borne threats and to optimize the email gateway control.

06
Conclusion

With email being the number-one attack vector for cybercriminals, having the right email security strategy in place is critical. Security leaders can relieve the stress associated with email security by focusing on three key things:

- Vigilance
- Malware Detection and Prevention
- Control

By exercising **vigilance**, security leaders can conduct annual or semi-annual phishing awareness training so their end users can learn to detect suspicious emails and red team exercises using phishing campaigns to test the vigilance of those users after their training.

By maintaining **control** (secure email gateway control that is), security leaders can effectively block malicious emails by tuning the configuration and policies in their email gateway to the latest email-based threats.

And through frequent **validation**, security leaders can rest easier knowing that their email gateway controls have been tested against thousands of the latest malicious email links and payload variants.

Cymulate can help you with validation to test the effectiveness of your organization's email gateway and policies by simulating different types of email-based threats, including malware, worms, trojans and exploits delivered through attachments and malicious links.

About Cymulate

Cymulate, the leader in exposure management and security validation, provides the single source of truth for threat exposure and the actions required to close security gaps before attackers can exploit them. More than 500 customers worldwide rely on the Cymulate platform to baseline their security posture and strengthen cyber resilience with continuous discovery, validation, prioritization, and guided remediation of security weaknesses. Cymulate automates advanced offensive security testing to validate controls, threats, and attack paths. As an open platform, Cymulate integrates with existing security and IT infrastructure and drives the workflows of the exposure management process. For more information, visit www.cymulate.com.

Get a Demo