cymulate

SOLUTION BRIEF

Email Gateway Validation

Email is the Preferred Method for Threat Actors to Initiate a Cyber Attack

Email is the most frequently used delivery method of attack for exploiting security weaknesses, making your secure email gateway a critical front-line component of your organization's cyber defense.

With more than 94% of organizations having suffered an email security incident and 79% of attacks originating from a malicious phishing email, cybersecurity leaders have reasons to stress about email security.

(Source: Egress 2024 Email Security Report)

Secure Email Gateways Require Continuous Validation Against the Latest Email-Based Threats

As a cybersecurity leader, you need to test and optimize the efficacy of your secure email gateway controls and policies to detect and prevent the delivery of malicious email content and protect your end users from inadvertently succumbing to an email-based attack.

Cymulate enables your security team to conduct comprehensive assessments of your email gateway that test and validate against thousands of known malicious links and payloads in a production-safe mode.

The best practice assessment simulates different types of email-based threats with the latest ransomware, malware, worms, trojans and exploits delivered through email attachments and malicious links. The simulated attack types include:

- **Malicious Links**
- **Malicious Attachments**
- **Executable Payloads**
- **Dummy Code Execution**
- **True File Type Detection**
- **Email Attachment Policies**

The results of these assessments highlight the gaps and weaknesses in your email security controls that could be used to exploit your users and lead to a cyber breach.

> **During initial testing of our email gateway, we found that some extensions were not being blocked and that sandboxing was not enabled. Once we blocked them and enabled the sandbox, our Cymulate score went from 54 (medium risk) to 6 (minimal risk) within 2 weeks. Quick win!**
> – Security Leader, Major Media Company

Solution Benefits

Automated validation

Automate continuous testing of secure email gateway controls and policies against the latest email-borne threats.

Identify gaps

Find the gaps and weaknesses in your email gateway controls and policies that could expose your users to malicious content.

Optimize controls

Configure and tune your email gateway controls with mitigation guidance to detect and block emails containing malicious links and payloads.

Reduce exposure

Continuously measure and improve your email gateway security controls to reduce the risk of phishing attacks and other email-based threats.

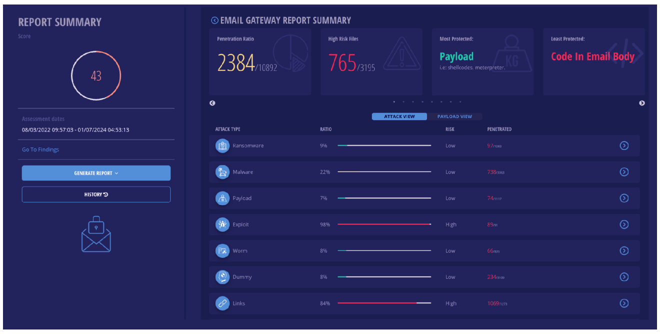
Automated Security Validation for your Secure Email Gateway

The Cymulate platform includes breach and attack simulation to automate production-safe security testing of your email gateway using a wide range of malicious links and payload variants that simulate the latest email-based attacks. The solution lets you identify the gaps and weaknesses in your email security controls that could enable a malicious email to reach your users and potentially initiate a cyber attack on your environment. The assessment enables you to optimize the investment you have made in your secure email gateway by configuring and tuning your email defenses with precise mitigation guidance from Cymulate.

Detailed Report and Findings

Gain deep insight into the effectiveness of your email gateway controls and policies with detailed reports and findings that include:

- **Risk Score** to measure the overall performance of your secure email gateway
- **Exposure Level** to measure your security posture
- **Penetration Ratio** highlighting the number of malicious emails not blocked by the email gateway
- **Ratio by Attack Type** to focus efforts on least protected areas of the email gateway controls
- **High Risk Files** to prioritize risk and focus mitigation efforts
- **Mitigation Guidance** to help optimize controls and enhance policies



REPORT SUMMARY

Score

43

Assessment dates

08/03/2022 09:57:03 - 01/07/2024 04:53:13

EMAIL GATEWAY REPORT SUMMARY

Penetration Ratio 2384/10892

High Risk Files 765/3195

Most Protected: Payload i.e: shellcodes, meterpreter.

Least Protected: Code In Email Body

ATTACK TYPE	RATIO	RISK	PENETRATED
Ransomware	9%	Low	97/1083
Malware	22%	Low	738/3363
Payload	7%	Low	74/1117
Exploit	98%	High	89/91
Worm	8%	Low	66/855
Dummy	8%	Low	234/3109
Links	84%	High	1069/1273

Email Gateway Report Summary

Why choose Cymulate?

Depth of attack simulations

The assessment contains a comprehensive suite of over 10,000 test cases to fully validate your email gateway against the latest malicious links and files.

Production safe

The full suite of test cases is completely production-safe with no malicious payload or code execution that could impact your production environment.

Automated validation

The assessment is fully automated enabling continuous validation and performance optimization of your email gateway control effectiveness every week.

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