Cofense Validator™: The Only Objective Analysis of SEG Performance

Business Challenge

There are numerous choices when it comes to Secure Email Gateways (SEGs). They all promise to block bad emails. Customers have traditionally relied on SEG vendors to demonstrate how effective their products are against new threats. But who is keeping those vendors accountable? How can customers trust that their SEG is blocking what they say it's blocking? Cofense proves time and time again that SEGs provide a false sense of security.

The table below shows how SEGs stop most simple threats like malicious attachments. However, we routinely find malicious URL threats in environments protected by a variety of SEGs.

BEC, Cred Theft & Other Types of Phishing Attacks Evade Existing Email Security Tools at High Rates

Microsoft E3	Microsoft E5	Proofpoint	Cisco Ironport	Mimecast
Attacks Containing Malicious Attachments that Reach Inbox				
9%	2%	1%	3%	2%
Attacks Containing Malicious URLs that Reach Inbox				
94%	40%	49%	61%	82%

As seen in Cofense Customer Environments over 6 Months

Solution

Use Cofense Validator™ to test your SEG with real phish. Cofense is the only email security company that sees phish that have bypassed all the major SEG vendor products. The individual SEG vendors only see what is being stopped by their technology. Cofense sees what is being missed by all of the SEGs, and is the only company with that advanced level of phishing intelligence. This intelligence fuels Cofense Validator™ and provides unmatched insight for customers to understand the performance of their SEG. Real, in-the-wild phishing threats identified by Cofense are sent through the SEG to see how effective they are at stopping these *active threats*. Customers realize instant ROI through reports with immediately actionable information.

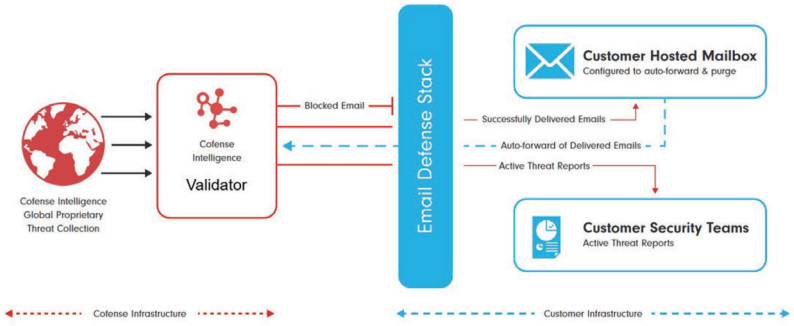
How It Works

1 Customers set up a mailbox in their mail environment exclusively for Cofense Validator™. The mailbox is configured with an auto-forward rule to send any emails it receives back to Cofense.

2 Cofense Validator™ sends real threats identified by Cofense Intel to the mailbox. The email is either allowed by the SEG or blocked.

3 Cofense Validator™ analyzes emails auto-forwarded from the customer's mailbox to determine if the SEG performed any actions (such as modifying the URL or attachment).

4 Customers review the test results and modify their SEG configuration to ensure a balance between efficiency and security.



We Know the Threats

> *Validator has allowed us to get meaningful valuations of how each of our environments stacks up in a way that reflects real-world attacks, helping us determine which controls we are lacking (or which controls are too tight). Validator has also provided us with an additional means of testing potential email security solutions against our current setup to make smarter purchasing decisions that have an actual impact on our organization's security."*

> *While there are many 'attack simulation/testing' services out there - 99% of them leverage custom built pseudo-malware, edited malware (**so it's not really malicious anymore**), old samples, open source/public, or consumer focused threat payloads (data from virus total, phishtank, etc.). **All of the emails Cofense uses are real malicious payloads seen by Cofense through the "Cofense Network"** that are targeting actual enterprises right now.*

> *Configuring SEGS is a complicated and hard task. IT teams experience non-stop anxiety about making a change that will increase false positives that generate end user complaint. No one wants to hear, "Why is my nana's email in my junk folder I love my nana" or equally important "They told me they sent the contract, but I don't see it anywhere in my inbox."*

Key point. Cofense Validator™ gives a security team peace of mind. How else would they know if a change made filtering worse?

About Cofense

Cofense® is the leading provider of phishing detection and response solutions. Designed for enterprise organizations, the Cofense Phishing Detection and Response (PDR) platform leverages a global network of close to 30 million people actively reporting suspected phish, combined with advanced automation to stop phishing attacks faster and stay ahead of breaches. When deploying the full suite of Cofense solutions, organizations can educate employees on how to identify and report phish, detect phish in their environment and respond quickly to remediate threats. With seamless integration into most major TIPs, SIEMs, and SOARs, Cofense solutions easily align with existing security ecosystems. Across a broad set of Global 1000 enterprise customers, including defense, energy, financial services, healthcare and manufacturing sectors, Cofense understands how to improve security, aid incident response and reduce the risk of compromise. For additional information, please visit www.cofense.com or connect with us on Twitter and LinkedIn.

COFENSE

W: cofense.com/contact **T:** 703.652.0717

A: 1602 Village Market Blvd, SE #400
Leesburg, VA 20175