CYMULATE

HOW A BAS PLATFORM CAN ASSIST WITH EVALUATING SECURE EMAIL GATEWAY SOLUTIONS

February 2018

"EVERYTHING OF VALUE IS VULNERABLE"

CYMULATE

TABLE OF CONTENT

GLOSSARY

BAS platform	Breach & Attack Simulation platform
BEC	Business E-mail Compromise
DLP	Data Loss Prevention
ICO	Initial Coin Offering

TABLE OF FIGURES

1 / INTRODUCTION

Email is a core business tool for internal and external correspondence for organizations of all sizes. They contain valuable business information, both in the message itself as well as in attachments. When an organization has its own email domain, emails are sent and received by port 25 (SMTP). Needless to say, this makes port 25 a particular interest to cybercriminals.

HIGH PROFILE EMAIL ATTACKS			
Date	Target	Attack	Result
Jan 2018	Cryptocurrency startup BeeToken	The attackers targeted its ICO with phishing attacks	Investors lost over $1 million worth of Ethereum
Sep 2017	Deloitte	Attackers used an administrative password and account to access Deloitte's Azure storage	Hackers got access to usernames, passwords and personal details of Deloitte's 350 blue-chip clients
Aug 2017	The Lukitus WW campaign	Hackers sent out more than 23 million messages containing Locky ransomware in just 24 hours	The email comes with a ZIP attachment hiding the malware payload. The ransom is 0.5 Bitcoin (~$2,300) for a "Locky decryptor" to get their files back
Nov 2016	Boeing	An employee sent an email containing a spreadsheet with personal information to his spouse (a non-Boeing employee) for helping with a formatting issue	Personal information of approximately 36,000 Boeing employees was leaked
2016	US Democratic National Committee (DNC)	Hackers sent phishing emails to the DNC. One was opened by an aide, giving the hackers access	19,252 emails and 8,034 attachments were stolen and leaked to the public

Figure 1 - High Profile Email Attacks

To keep their email traffic safe, organizations use Secure Email Gateway (SEG) amongst other solutions such as sandbox, Content Disarm and Reconstruction (CDR) etc. When looking for such security solutions, organizations need to compare the pros and cons of each solution. The only foolproof way to know how effective an SEG solution really is, consists of testing how well it stands up against all kind of cyberattacks exploiting email such as phishing and ransomware. In this white paper, we will discuss how a Breach & Attack (BAS) platform offers a highly accurate and risk-free way to help evaluating SEG solutions.

We will also describe a recent secure email gateway assessment performed using Cymulate's platform. The results of this assessment provides a clear and comparative analysis of the tested gateways. It illustrates the importance of using a BAS platform like Cymulate to any organization already using or planning to start using SEG solutions.

2 / A SHORT HISTORY OF EMAIL SECURITY

Email as a business tool is 40 years old. At that time, it was not designed to be a secure, controlled protocol. Routing and labeling protocols were (and still are) used to define which computer can receive, send or forward emails and at what time.

To make email traffic safer, organizations started using public-key cryptography, in which users can each publish a public key that others can use to encrypt messages to them, while keeping a private key they can use to decrypt or encrypt messages. Although an improvement, it was not completely bulletproof and cumbersome for the users.

Enter the Secure Email Gateway (SEG) that provides basic security functions such as running antivirus, anti-malware, anti-phishing and anti-spam scans.

In 2017, people sent about 120 billion business emails per day, sharing their confidential data such as intellectual property, financial statements, and legal documents. According to LinkedIn's 2017 Cybersecurity Trends Report, 63% of employees share sensitive data over email.

Currently, there are an estimated 4.9 billion email addresses worldwide. For the last two years, there have been 6,789 email data breaches globally, with 886.5 million records being compromised.

In May 2018, GDPR will come into force, dictating new rules for data security and data breach disclosures. Failing to comply will result in stiff penalties. Having a top-notch SEG solution in place will prevent phishing, ransomware, malware payloads, spear phishing and similar attacks using email.

3 / EMAIL ATTACK VECTOR

The latest studies and reports present grim statistics, showing that around 75% of attacks are carried out by email. Furthermore, more than 90% of such email attacks involve a malicious attachment or URL link. To bypass the cybersecurity defenses of organizations, attackers use a number of techniques, including:

PHISHING

According to an APWG report, 1,220,523 attacks were carried out in 2016 which is an increase of 65% compared to 2015.

SPEAR PHISHING

Deceptive and personalized email messages and social engineering are tailored made to the intended target.

WHALING

Targets high-profile end users, such as C-level corporate executives, to disclose corporate information.

SPAM

The amount of unsolicited, undesired, or illegal email messages is estimated to have increased by 400% in 2016.

SPOOFING

Hackers impersonate another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls.

BUSINESS EMAIL COMPROMISE (BEC)

The FBI defines BECs as "sophisticated scams targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payment". They accounted for over $3 billion in losses during 2016 [link]).

RANSOMWARE

Hackers deliver malicious payloads by email to lock the users out, followed by demanding a ransom for unlocking the infected device.

4 / SECURE EMAIL GATEWAY (SEG)

A Secure Email Gateway (SEG) inspects inbound and outbound email for threats, spam, and phishing attacks. They can also be used to enforce corporate security policies, e.g., DLP and encryption. SEG products can be installed as on-premise appliances and as cloud-based services. SEGs are typically considered as preventive controls since they are put in place to block malicious messages before those can impact the organization. SEGs come in several forms to meet each organization's requirements, including:

- Public cloud-based;
- Hybrid - A combination of public and private clouds;
- Hardware appliance on-premise;
- Virtual appliance on-premise;
- Email server-based.

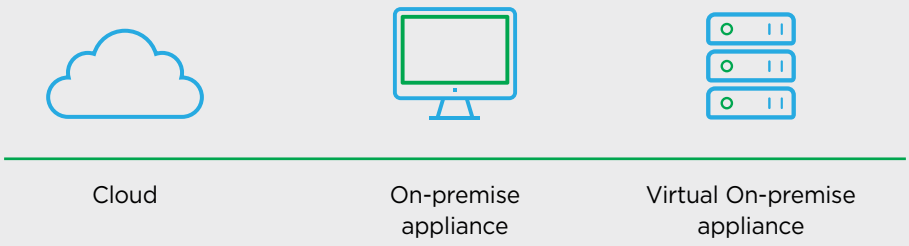


Figure 2 - SEG Deployments

SEG solutions perform a number of functions such as:

- Anti-spam and signature-based anti-malware.
- Marketing and graymail classification, and personalized controls for management of these types of messages.
- Network sandboxing and/or content disarm and reconstruction (CDR) for advanced, attachment-based threat defense.
- Rewriting and time-of-click analysis for advanced, URL-based threat defense.
- Context inspection, display name spoof, cousin domain and anomaly detection for advanced, impostor-based threat defense.

According to Gartner, the SEG market is mature, the market growth rate has leveled off to low-single digits, and there are no significant market entrants or acquisitions — all classic signs of a mature market. Despite the market maturity, companies can't do without SEG solutions (link). On the one hand, this makes selecting a SEG solution easier, since SEG solutions have been around for quite some time and have a proven track record. Still, comparing various options is complicated as we will see below.

When looking for a SEG solution, an organization has to look at various criteria to choose the optimal SEG that fits is size and needs.

1. The first criterion is how advanced the basic security functions of each solution are. Not all gateways are equally effective when it comes to detecting and stopping threats. To test these capabilities, sandboxing and threat intelligence are used. Although these methods have their merit, a BAS platform is a better way to evaluate since it is more accurate, easy to use and not a one-off.

2. The second criterion is evaluating the additional security features that each SEG solution offers, such as DLP or email encryption. Each DLP or email encryption feature should be checked, since some solutions offer robust implementations, while others provide only limited implementations. A BAS platform is able to test these features using simulated email attacks.

3. The third criterion is testing the usable and customizable of the management features. Small and medium-sized organizations tend to favor usability over customization, while large organizations often prefer customization to optimize the solution for detecting and stopping threats. In both scenarios, an organization can use a BAS platform to test its cybersecurity posture.

4. The fourth criterion is determining the detection ratio of each SEG solution. In other words, the typical false positive and negative rates for each detection technique. This is hard to determine since vendors do not share such data, but a BAS solution can assist during an assessment.

5 / USING A BAS PLATFORM TO EVALUATE SEG SOLUTIONS

Determining the best email security gateway product is hard since SEG vendors tend to provide relatively few details about the characteristics of their products, such as details regarding DLP robustness or false positives/negatives. This makes comparing the various SEG solutions difficult, since they are not truly comparable. The selected solution should be able to monitor and block incoming emails for spam, phishing, malicious files as well as other unwanted content. In short, it should lower their exposure level to a more secure posture.

A Breach & Attack Simulation platform is an excellent tool for testing the efficiency of various Secure Email Gateways. Assuming that the SEG's built-in security functionalities should be able to handle malicious email messages, the assessment simulates an actual attack through the use of emails. In order to test a wide range of possibilities, a large number of crafted malicious attachments are being sent to a designated target's email account. This way, it can be tested if these malicious emails are stopped by the SEGs under review, or if those malicious emails would slip through and be delivered to 'end users', possibly infecting them with viruses, Trojans and other malware.

An example of how Cymulate's BAS platform can assist, can be found in Appendix I.

▲ Back to Content

ABOUT CYMULATE

Cymulate helps companies to stay one step ahead of cyber attackers with a unique breach and attack simulation platform that empowers organizations with complex security solutions to safeguard their business-critical assets. By mimicking the myriad strategies hackers deploy, the system allows businesses to assess their true preparedness to handle cyber security threats effectively. An on-demand SaaS-based platform lets users run simulations 24/7 from anywhere, shortening the usual testing cycle, and speeding up time to remediation. Cymulate was established in 2016 by former IDF intelligence officers and leading cyber researchers with extensive experience in offensive cyber solutions. The company serves a broad range of industries, including finance, health care and telecommunication.

Cymulate's BAS platform is a plug & play cloud-based cyber security solution that is easy to deploy into any corporate network. It identifies security loopholes in the organization's infrastructure and provides insights for remediation. Attacks are run from the internet without causing physical interruption in the organization's local networks. For testing SEGs, the Cymulate's Secure E-mail module is used. This module enables organizations to test the resilience of their SEG solutions.

www.cymulate.com

Figure 3 - How Does it Work?

APPENDIX I – USE CASE
HOW CYMULATE'S BAS PLATFORM WAS USED FOR EVALUATING SEG SOLUTIONS

Three SEGs were evaluated by testing each one in a controlled environment with the Cymulate agent as the "target". The assessment simulated an actual attack through the use of emails. The question that needed to be answered was:

"Would these malicious emails be stopped by the SEGs or would they be allowed to be delivered to 'end users', possibly infecting them with viruses, Trojans and other malware?

The customer built the working environment and ran Cymulate's Email security module assessment for each of the tested SEGs. The assessment simulated an attacker that did not have any prior knowledge of the customer's security framework and architecture. A typical real-world scenario was used consisting of sending thousands of emails containing different types of malicious attachments, both previously-published and custom payloads, crafted by Cymulate.

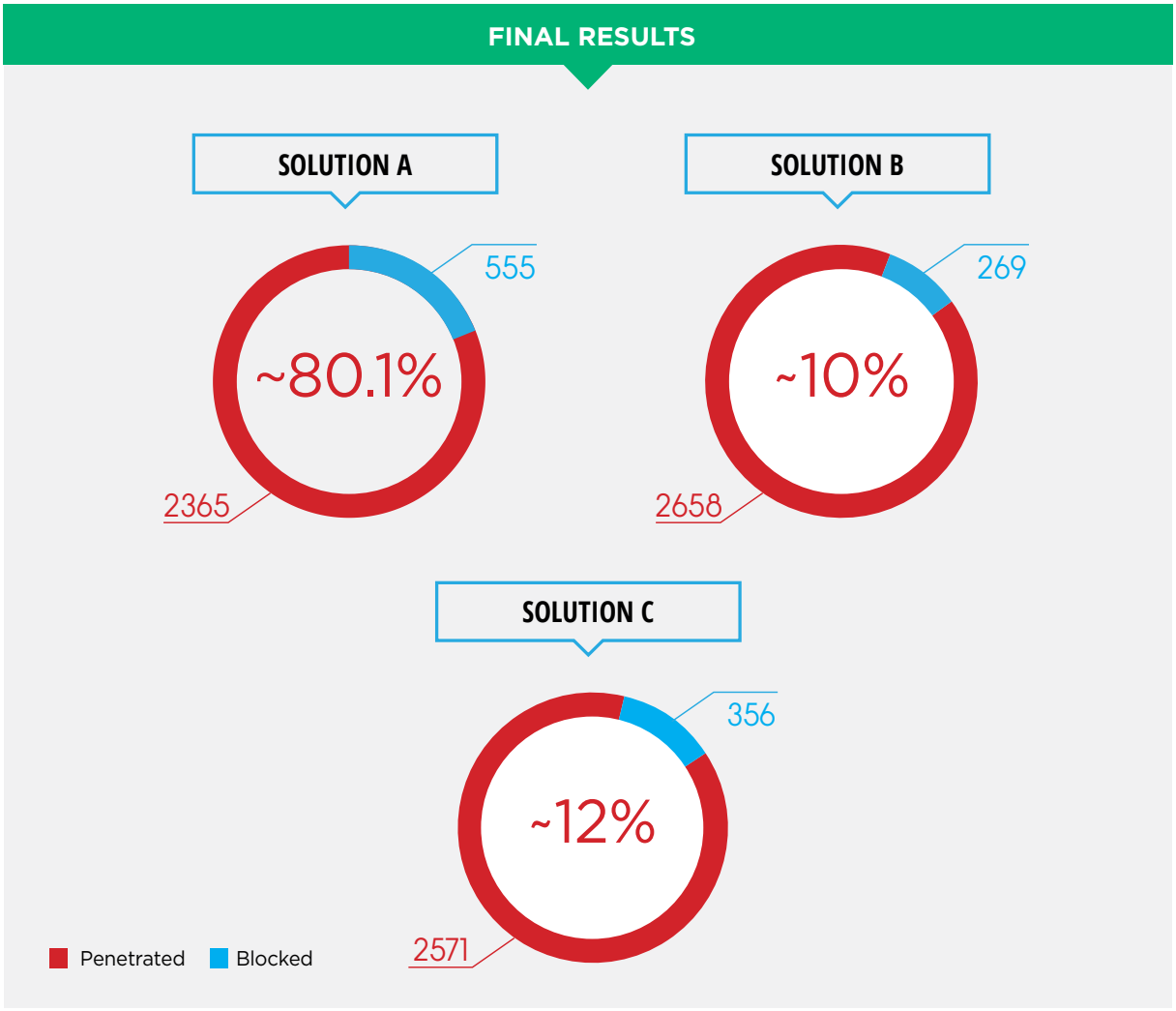
Each malicious file was concealed through variations of extensions, which enabled Cymulate to mimic an experienced hacker's attack. The files' extensions were deliberately changed to simulate the way an experienced attacker would act. The malicious files were disguised as work-related and presented to the user as common 'innocent' files such as PDFs, Excel spreadsheets, PowerPoint presentations, Word documents such as CVs, meeting invitations, etc. All messages were precision-monitored on a byte-by-byte level by comparing encrypted digital signatures of the sent and received items. This ensured that there could be no 'false alarms'.

Two of the tested SEGs performed reasonably well with a significant percentage of infected emails being blocked. The third SEG did not perform as well as the others and many of the malicious emails arrived at their destination without being disarmed.

Based on the results, it was decided to select the two SEGs that performed well, and combine them into one best-of breed solution. After the customer created a test scenario combining these two best performing SEGs, the combined solution was assessed again by Cymulate. It showed excellent results blocking almost every single "malicious email" sent during the assessment, presenting an interesting picture that emphasizes the difference between SEG vendors.

As shown below, an important differentiator between the tested products was their ability (or lack thereof) of dealing with malware embedded in files of various types: Word, PDF, Excel, PowerPoint, Zip, JavaScript, etc. The combination of Solution B and Solution C defenses resulted in outstanding, >99% malicious content block rate. In other words, the two better performing products were able to complement each other and form a "best-of-breed" SEG solution.

FINAL RESULTS

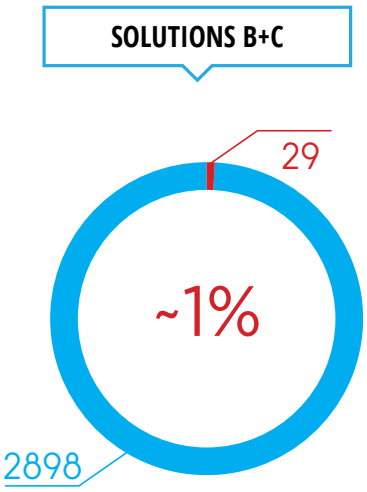


Amount and Percentage of Penetrated Emails

DETAILS BY CATEGORY

SEG	Solution A			Solution B			Solution C		
Attack	Blocked	Penetrated	Exposure	Blocked	Penetrated	Exposure	Blocked	Penetrated	Exposure
Dummy (480)	96	383 *Out of 479	~80%	425	55	~11.5%	423	57	~12%
Malware (1185)	212	973	~82%	1089	96	~8%	1046	139	~12%
Ransomware (405)	86	319	~79%	364	39	~10%	347	56	~12%
Worm (409)	77	332	~81%	375	34	~8%	356	53	~13%
Payload (413)	76	337	~81.5%	370	43	~10%	364	49	~12%
Exploit (37)	8	21 *Out of 29	~72%	35	2	~5%	35	2	~5%

The image below presents the number of malicious emails that were blocked and the amount that landed in the targeted email's inbox while using a combination of Solution B and Solution C.



Performance of the Combined B+C Solutions

Secure Email Gateway	Solution B + Solution C		
Attack	Blocked	Penetrated	Exposure
Dummy (480)	478	2	~0.5%
Malware (1185)	1181	4	~0.33%
Ransomware (403)	392	11	~3%
Worm (409)	401	8	~2%
Payload (413)	410	3	~1%
Exploit (37)	36	1	~3%

Breakdown of Penetrated/Blocked Malicious Email Messages by Type

The assessment's results clearly indicate that not all solutions 'are created equal'. Solution B and Solution C performed well and managed to block over 85% of attacks, while Solution A did not perform well, managing to block just ~20% of attacks. None of the tested solutions have shown perfect performance, since carefully concealed malware was able to bypass the defenses and lend up in the target's inbox.

The success of a SEG solution also relies on additional capabilities, configuration management, improvements on the vendor side and employee awareness training.

RANSOMWARE

Software encrypting user files and denies access until ransom is payed.

MALWARE

Malware, is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.

WORM

Software using common techniques inorder to spread itself inside a Windows based network.

DUMMY

Dummy category are code execution proof of concept without actual damage to the system.

EXPLOIT

Known and signed exploits of commonly used software that leads to code execution because of vulnerabilities discovered.

PAYLOAD

Common attacks delivered to clients like: Data extraction attacks or Stagers downloading the real malware.