CYREN

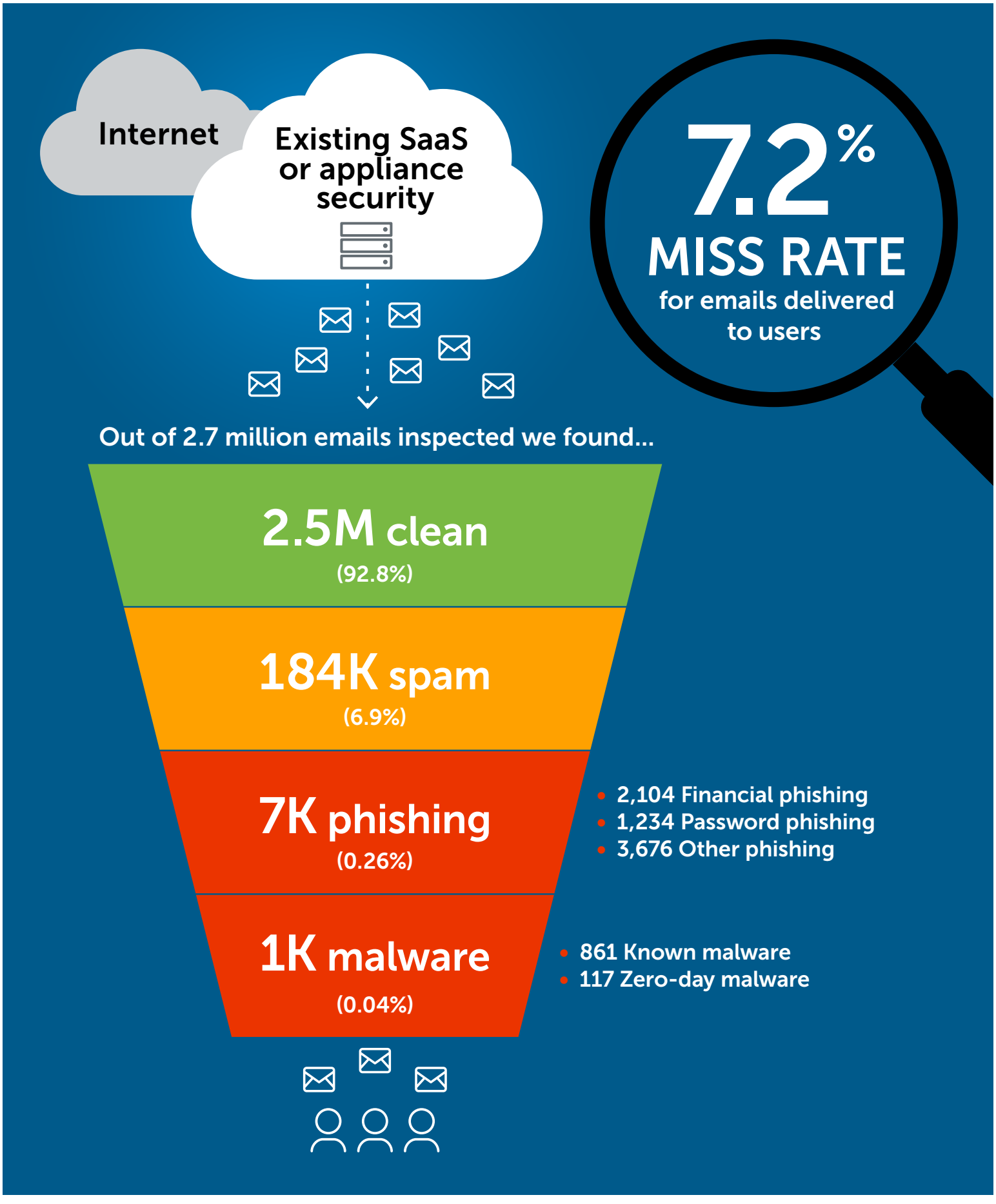
Email Security Gap Analysis: Aggregated Results

Average rates at which enterprise email security systems miss spam, phishing and malware attachments

October 2018

Email Security Gap Analysis

Aggregated results of live email infrastructure assessments



Email Security Gap Analysis

Summary of findings

Gap Analysis Overview

- Email volume analyzed: 2.7 million
- Average miss rate: 7.2%

Since early 2017, Cyren has engaged with a diverse set of organizations through its Email Security Gap Analysis program to assess the effectiveness of their current, live email security infrastructures. This report summarizes the results from a cross-section of 15 such engagements conducted in 2018, in which Cyren examined 2.7 million emails that were classified as clean by their existing email security systems and delivered to user mailboxes. Every email was also copied to Cyren for analysis.

Companies included in the tests were from a variety of industries and used several different types of email security, ranging from on-premises appliance gateway solutions to hosted email, such as Office 365 or G-Suite. The percentages discussed in this report are therefore averages which serve as a reference. As discussed further below, Gap Analysis results can vary significantly, even between companies using the same security solution.

Of the 2.7 million emails analyzed by Cyren, 2.48 million (92.8%) were found to be correctly classified as "clean" or legitimate. For the purposes of the assessments, emails classified as graymail, such as newsletters, were considered clean, since their categorization is subjective.

Of this total, 191,819 (7.2%) were found to be spam or malicious messages that were missed by the deployed solutions, also called "false negatives," and should not have been delivered to user mailboxes. This 7.2% "miss rate" breaks down into the following categories:

1. Spam emails found – 183,827

Users received 183,827 spam emails, 6.9% of the total email traffic. Spam is unsolicited bulk email, usually identified by content scanning techniques or by sophisticated pattern detection applied to elements of the email itself and email distribution patterns. As noted above, the spam category does not include legitimate newsletter emails.

2. Phishing emails found – 7,014

Of the email delivered to users, 7,014 emails, or 0.26%, were found to be phishing emails. From this total, Cyren identified 2,104 financial phishing emails, 1,234 password phishing emails, and 3,676 general phishing emails, which did not meet the criteria for either other category.

Financial phishing email senders typically pose as a well-known financial organization and encourage the recipient to validate their account, or warn of an unauthorized transaction. If a user clicks the link they are taken to a fraudulent copy of the organization's website, where the attacker attempts to steal their login credentials to gain direct access to their account.

Password phishing email senders typically pose as business applications, social websites or online merchants. The email will contain a link that directs a user to a fraudulent copy of a sign-in page designed to steal login information. The end-goal is to obtain sensitive information, company secrets and often to take over accounts such as Office 365. This enables the cyber-criminal to monitor company communications, understand internal company dynamics and business being conducted, and send further targeted emails from the genuine user account, such as requesting a finance team member transfer money to the criminal's bank account.

To learn more about the phishing threat landscape download Cyren's special threat report on phishing.

3. Malware found – 978

There were 978 emails delivered to users found to have either malware attachments or links to malware which is downloaded when the recipient clicks on the link. While this represents a small percentage of the total email delivered (0.04%), the high level of risk associated with malware obviously makes this of great concern.

Of these 978 messages, 861 (88%) included attachments with recognized malware signatures or known links to malware. These previously known threats could include, but are not limited to, ransomware, key loggers, rootkits, trojans, viruses, and worms.

Among the malware emails delivered to users by the various systems, 117 were "zero-day" malware attachments, i.e., new malware with no previously known malware signatures. Despite the lack of existing signatures, Cyren's security cloud identified these emails as malicious by utilizing proprietary techniques for detection.

Results Vary Even With the Same Email Security

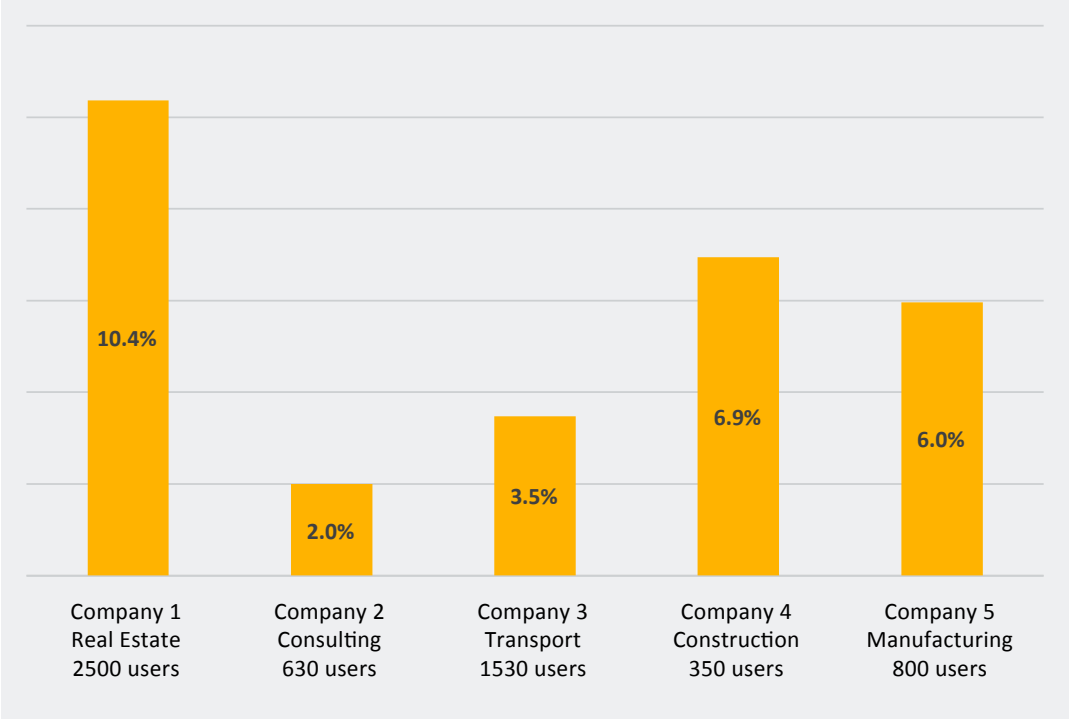
The results presented above are averaged across the fifteen companies and different deployed security systems. But it is important to note that even when the email security system is the same, results can vary widely, influenced by an organization's type of activity and user profile, and by security configuration choices made. The five case studies presented below compare the results for different organizations that had deployed security from the same vendor, with each identified by their industry. The total "miss rate," or percentage of spam and malicious emails (phishing + malware) making it through to users, varied significantly across these organizations.

All the percentages referenced are those of total emails received by the organization.

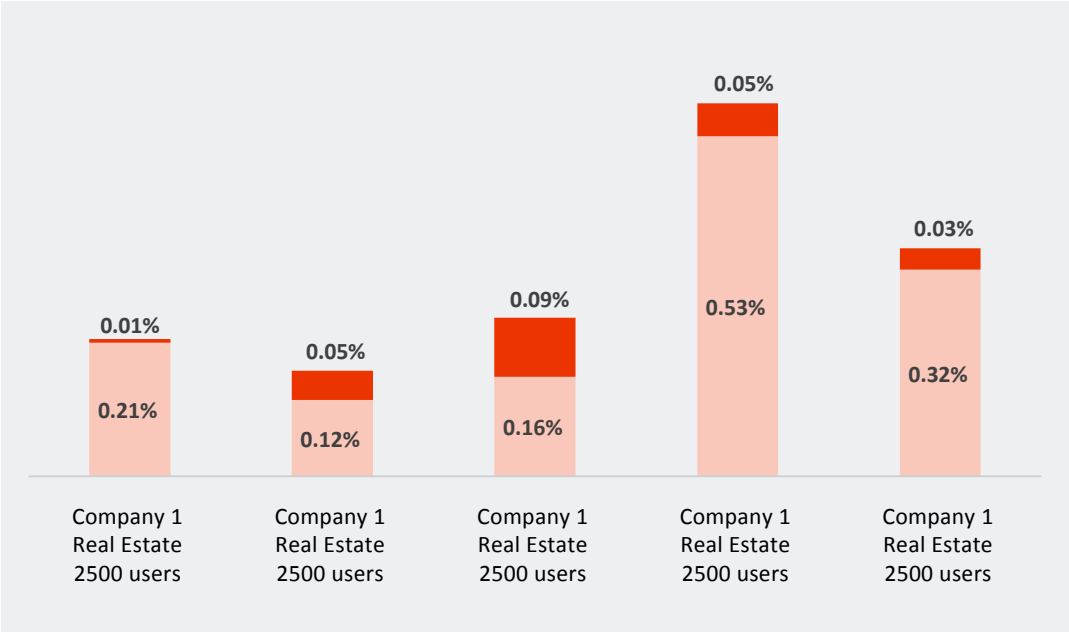
	CASE STUDY 1	CASE STUDY 2	CASE STUDY 3	CASE STUDY 4	CASE STUDY 5
Industry	**Real Estate**	**Consulting**	**Transport**	**Construction**	**Manufacturing**
No. of email users	2500	630	1350	350	800
Spam emails not blocked	119,247	2,122	13,529	4,451	16,317
% spam	10.4%	2.0%	3.5%	6.9%	6.0%
Malicious emails not blocked	2476	176	966	374	976
% malicious	0.22%	0.17%	0.25%	0.58%	0.36%
Total miss rate	**10.6%**	**2.2%**	**3.7%**	**7.5%**	**6.3%**

The varied results for each organization, despite using the same email security system, are shown graphically below. The real estate company receives by far the highest percentage of spam, but the lowest percentage of malware. The construction company has by far the highest rate of malicious email getting through, including more than twice the number of phishing as most of the others.

Spam: percentage missed by current email security infrastructure

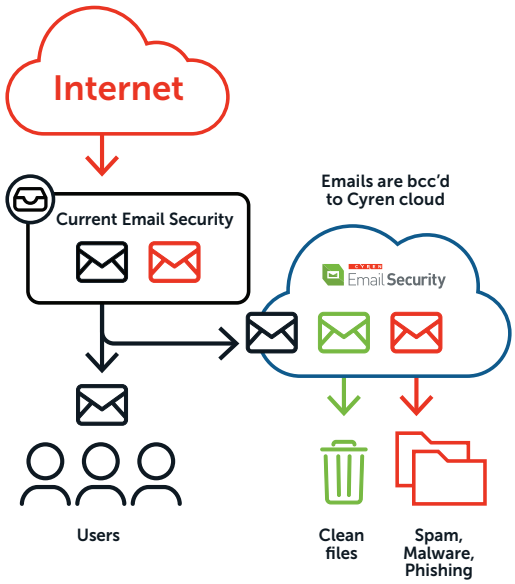


Malware and phishing: percentage missed by current email security infrastructure



Deeper analysis of these results and many others, not included in this report, demonstrates notable diversity across organizations in the same industry, with similar numbers of users and, most importantly, the same email security system. Clearly, security effectiveness appears to be influenced by other factors than purely the vendor solution chosen, such as the degree to which an organization might be being targeted or specifics of their deployment. This underscores the value of running one's own assessment to determine one's effective, real-world detection rates.

How Cyren Gap Analysis Works



Cyren Email Security Gap Analysis was developed as a tool to evaluate the email security performance of various email security appliances and services. This performance is compared to threat detection by the Cyren security cloud, which has the benefit of real-time intelligence from processing over 25 billion web and email transactions daily, and blocks over 300 million transactions every day. Given the increasingly dangerous nature of today's threat environment, Cyren works with companies to identify whether their existing security infrastructure or hosted email service is potentially delivering unwanted or dangerous emails to users, calculating a "Miss Rate" to quantify the results. The gap analysis requires no MX record change It relies on Cyren's cloud infrastructure to examine the existing email security system, with all messages delivered normally to users' mailboxes also "blind carbon copied" to Cyren's system for automated analysis. Emails classified as "clean" are automatically and immediately deleted, and those that are identified as spam or containing a threat are sorted and placed into folders in an administrative mailbox for company review, and to aid any needed remediation. A full report is provided on all threats discovered.

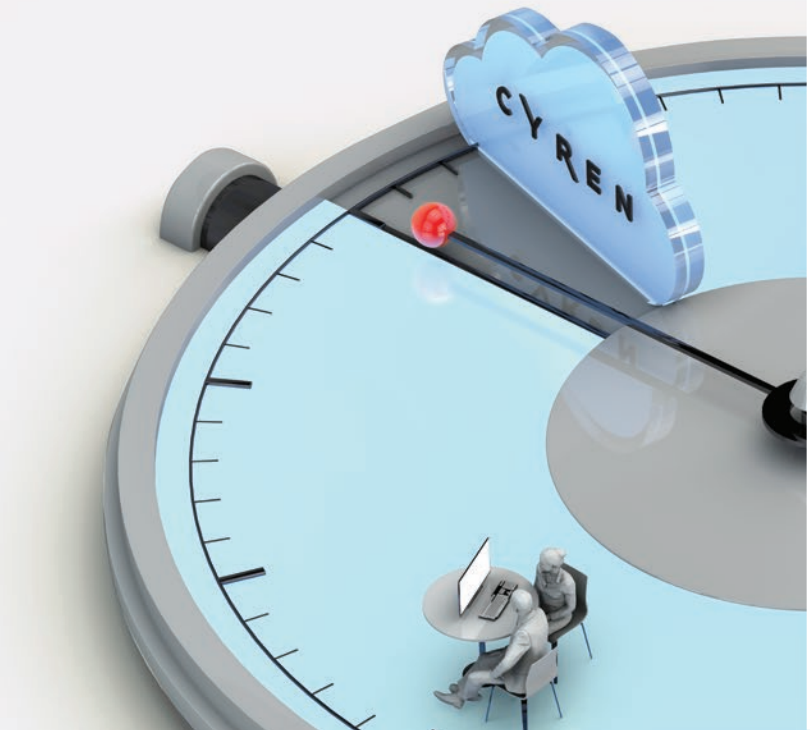
Opportunities for Testing Your Email Security

Businesses interested in similarly evaluating the effectiveness of their email security can review the program and apply for their own gap analysis on our website.

Opportunities for Testing Your Web Security

Businesses interested in testing the effectiveness of their web security can use Cyren's publicly available Web Security Diagnostic which returns results in less than 30 seconds on one's ability to block several types of virus, botnet, and phishing threats. Free trials for Cyren Web Security can be initiated on a self-service basis in a matter of minutes. For a description of the Cyren Web Security service, visit here.

Cyren–The Fastest Time to Protection



The Appliance Window of Exposure

About Cyren

Cyren is leading the SaaS revolution by moving internet security to the cloud. Traditional security appliances are too slow, leaving businesses vulnerable to cyber threats for hours, days, or even weeks.

Cyren's security cloud detects web and email-based threats as they emerge on the internet, and blocks them globally within seconds— before they reach users. We can do this because we analyze billions of transactions from around the world every day for customers like Google, McAfee, and Check Point. In the race to beat cyber attacks, Cyren's suite of services offers businesses the world's fastest, most accurate security.