SE Labs

INTELLIGENCE-LED TESTING

EMAIL SECURITY SERVICES PROTECTION

APRIL 2018

SE Labs tested a range of email hosted protection services from a range of well-known vendors in an effort to judge which were the most effective.

Each service was exposed to the same threats, which were a mixture of targeted attacks using well-established techniques and public attacks that were found to be live on the internet at the time of the test.

The results indicate how effectively the services were at detecting and/or protecting against those threats in real time.

MANAGEMENT
Director Simon Edwards
Operations Director Marc Briggs
Office Manager Magdalena Jurenko
Technical Lead Stefan Dumitrascu

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Liam Fisher
Gia Gorbold
Pooja Jain
Ivan Merazchiev
Jon Thompson
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Steve Haines
Colin Mackleworth

Website www.SELabs.uk
Twitter @SELabsUK
Email info@SELabs.uk
Facebook www.facebook.com/selabsuk
Blog blog.selabs.uk
Phone 0203 875 5000
Post ONE Croydon, London, CR0 0XT

CONTENTS

Document version 1.0 Written 26th April 2018;
v1.01 Updated 12th September with further details on which version of the Proofpoint Essentials service was tested.

INTRODUCTION

Wide range of targeted attacks makes for a tough test

Last summer we launched our first email cloud security test and, while it was very well received by our readers and the security industry as a whole, we felt that there was still work to do on the methodology. This report shows the results of six months of further development, and a much clearer variation in the capabilities of the services under test.

The most significant change to the way we conducted this test lies in the selection of threats we used to challenge the security services: we increased the number and broadened the sophistication. Whereas we might have used one fake FBI blackmail email previously, in this test we sent 10, each created using a different level of sophistication. Maybe a service will detect the easier versions but allow more convincing examples through to the inbox? We wanted to test the breaking point.

We also used a much larger number of targeted attacks. There was one group of public 'commodity' attacks, such as anyone on the internet might receive at random, but also three categories of crafted, targeted attacks including phishing, social engineering (e.g. fraud) and targeted malware (e.g. malicious PDFs).

Each individual attack was recreated 10 times in subtly different but important ways.

Attackers have a range of capabilities, from poor to extremely advanced. We used our "zero to Neo" approach to include basic, medium, advanced and very advanced threats to see what would be detected, stopped or allowed through. The result was an incredibly tough test.

We believe that a security product that misses a threat should face significant penalties, while blocking legitimate activity is even more serious. If you're paying for protection threats should be stopped and your computing experience shouldn't be hindered. As such, services that allowed threats through, and blocked legitimate messages, faced severe reductions to their accuracy ratings and, subsequently, their chances of winning an award.

SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our website and follow us on Twitter.

Executive Summary

Services
Some services tested may be listed in this report using just the vendors' names for clarity and brevity.

*For a list of full service names please see **Appendix C**: Services tested on page 17.*

EXECUTIVE SUMMARY			
Products tested	Protection Accuracy Rating (%)	Legitimate Accuracy Rating (%)	Total Accuracy Rating (%)
Mimecast Secure Email Gateway	76%	50%	73%
Forcepoint Email Security Cloud	45%	75%	48%
Symantec Email Security .cloud	41%	92%	47%
Proofpoint Essentials	42%	33%	41%
Microsoft Office 365 Advanced Threat Protection	22%	92%	30%
Microsoft Office 365	-4%	95%	7%

■ **Products highlighted in green were the most accurate, scoring 40 per cent or more for Total Accuracy. Those in yellow scored less than 40 but more than 20 per cent. Products shown in red scored less than 20 per cent.**

*For exact Total Accuracy Rating values, see **1. Total Accuracy Ratings** on page 6.*

Email hosted protection services are capable of filtering out large numbers of threats before they reach the user. In this test the products detected many of the threats used but handled them differently.

The best had the courage of their convictions and prevented the malicious messages from hitting the user's inbox.

Some, due to their design, moved the messages to the 'Junk' folder, which is within easy reach of inquisitive users. Others made changes to the messages to attempt to neutralise the malicious elements. This approach was generally effective but some threats were still able to bypass this protection layer.

All of the products were effective at stopping public threats from reaching the user, although **Microsoft Office 365** did allow a large percentage to reach as far as the Junk folder. All of the non-Microsoft services prevented all (or all-but-two) public threats from reaching the inbox.

Targeted attacks were a different matter completely. The best overall service was **Mimecast Secure Email Gateway**, which stopped all of the malware-based targeted threats and the majority of the social engineering and phishing attacks. **Forcepoint Email Security Cloud** took second place as it was less effective with the malware but managed to prevent all of the phishing attacks.

Symantec and **Proofpoint** received similar protection ratings while **Microsoft's** services, with and without the **Advanced Threat Protection (ATP)** add-on, were the least effective. The ATP addition had a noticeable effect on removing additional phishing and malware attacks.

1. Total Accuracy Ratings

Judging the effectiveness of an email hosted protection service is a subtle art and many factors need to be considered when assessing how well it performs. To make things easier we've combined all of the different results into one easy-to-understand graph.

The graph below takes into account not only each service's ability to detect and protect against threats, but also its handling of non-malicious messages and components of those messages, such as attachments and links to websites.

Not all protection measures, or detections for that matter, are equal. A service might completely delete an incoming malicious email and never allow the intended recipient to see (and subsequently 'play' with) it. Services may condemn suspicious messages to a 'quarantine' area if it lacks the utter conviction that the message is unwanted. This keeps threats away from recipients unless the recipient judges that the message is really safe. At the weaker end of the scale, the service might simply add a warning to the email's Subject line.

We take these different possible outcomes into account when attributing points that form final ratings.

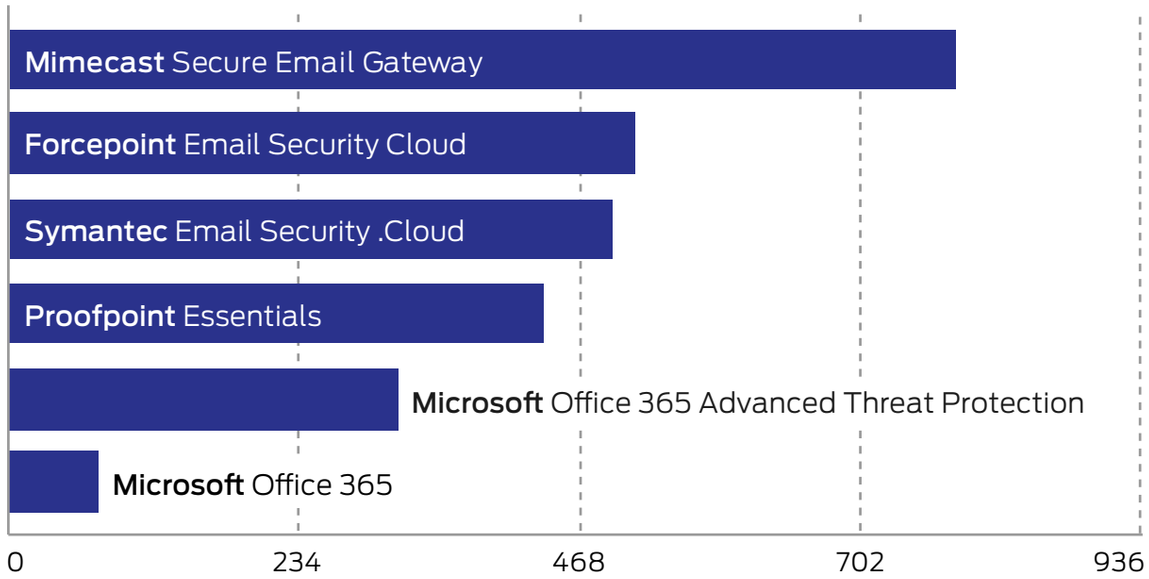
For example, a service that completely blocks a malicious message from falling into the hands of its intended recipient is rated more highly than one that prefixes the Subject line with "Malware: " or "Phishing attempt: ", or sends the message to a 'Junk' folder.

Categorising how a service handles legitimate messages is similar, but in reverse. Making a small change to the Subject line is much less serious a failing than deleting the message and failing to notify the recipient.

*See **2. Protection Ratings** on page 8 for more details.*

TOTAL ACCURACY RATINGS

Product	Total Accuracy Rating	Total Accuracy (%)	Award
Mimecast Secure Email Gateway	786	73%	AAA
Forcepoint Email Security Cloud	519	48%	A
Symantec Email Security .cloud	503	47%	A
Proofpoint Essentials	442	41%	A
Microsoft Office 365 Advanced Threat Protection	324	30%	B
Microsoft Office 365	71	7%	



Total Accuracy Ratings combine protection and false positives.

SE Labs

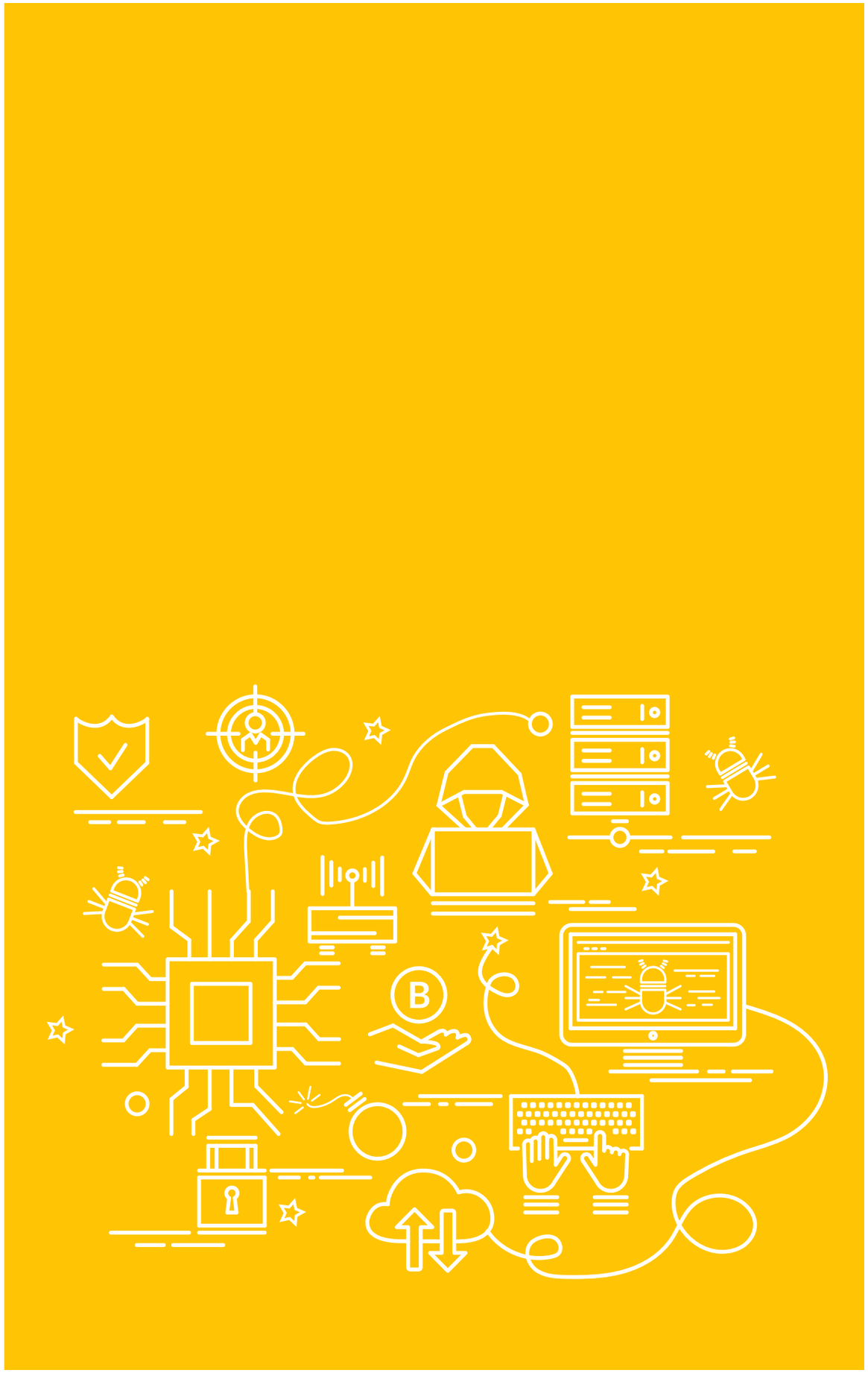
Email Security Services Protection Awards

The following products win SE Labs awards:

- **Mimecast** Secure Email Gateway

- **Forcepoint** Email Security Cloud
- **Symantec** Email Security .cloud
- **Proofpoint** Essentials Business Edition

- **Microsoft** Office 365 Advanced Threat Protection



2. Protection Ratings

The results below indicate how effectively the services dealt with threats and legitimate email. Points are earned for detecting threats and for blocking or otherwise neutralising it. Points are also earned for allowing legitimate email entry into the recipient's inbox without significant damage.

Stopped; Rejected; Notified; Edited effectively (+4 for threats; -8 for legitimate)
If the service detects the threat and prevents any significant element of that threat from reaching the intended recipient we award it four points. If it miscategorises and blocked or otherwise significantly damages legitimate email then we impose a minus eight point penalty.

Quarantined (+3 for threats; -6 for legitimate)
Services that intervene and move malicious messages into a quarantine system are awarded three points. However, there is a six point deduction for each legitimate messages that is incorrectly sent to quarantine.

Junk (+2 for threats; -4 for legitimate)
The message was delivered to the user's Junk box by **Microsoft Office 365** with and without **Advanced Threat Protection**.

Inbox (-5 for threats; +2 for legitimate)
Malicious messages that arrive in the user's inbox have evaded the security service. Each such case loses the service five points. All legitimate messages should appear in the inbox. For each one correctly routed there is an award of two points.

PROTECTION RATING COMPARISON		
Action	**Threat**	**Legitimate**
Stopped; Rejected; Notified; Edited effectively	+4	-8
Quarantined	+3	-6
Junk	+2	-4
Inbox	-5	+2

Rating calculations

For threat results we calculate the protection ratings using the following formula:

Protection rating =
(4x number of Stopped etc.) +
(3x number of Quarantined) +
(2x number of Junk) +
(-5x number of Inbox)

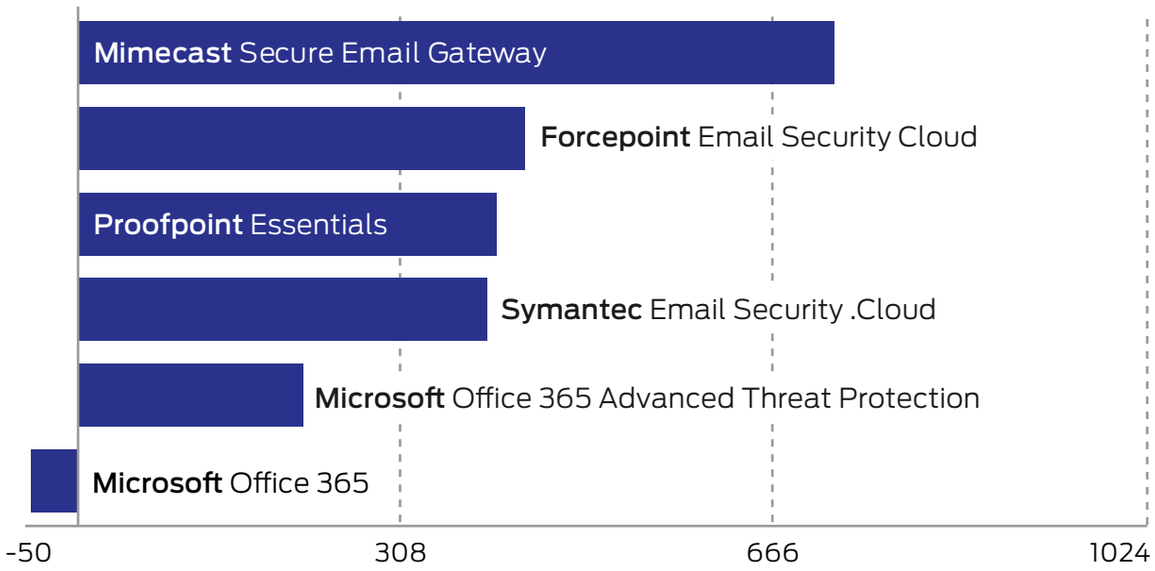
For legitimate results the formula is:
(2x number of Inbox) +
(-4x number of Junk) +
(-6x number of Quarantined) +
(-8x number of Stopped etc.)

These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in quarantine, or for a malware threat to end up in the inbox. You can use the raw data from this report (pages 10 – 13) to roll your own set of personalised ratings.

PROTECTION RATINGS

Product	Protection Rating	Protection Rating (%)
Mimecast Secure Email Gateway	726	76%
Forcepoint Email Security Cloud	429	45%
Proofpoint Essentials	402	42%
Symantec Email Security .cloud	393	41%
Microsoft Office 365 Advanced Threat Protection	214	22%
Microsoft Office 365	-43	-4%

Average: 37%



Protection Ratings are weighted to show that how products handle threats can be subtler than just 'win' or 'lose'.

3. Targeted Attacks

The results below use the following terms:

- **Notified** The service prevented the threat from being delivered and notified the user. There was no option for the user to recover the threat.
- **Stopped** The service silently prevented the threat from being delivered.
- **Rejected** The service prevented the threat from being delivered and sent a notification to the sender.
- **Quarantined** The service prevented the threat from being delivered and kept a copy of the threat, which could be recovered by the user or an administrator.
- **Edited** The service delivered the message but altered it to remove malicious content.
- **Junk** The message was delivered to the user's Junk box by **Microsoft Office 365** with and without **Advanced Threat Protection**.
- **Inbox** The service failed to detect or protect against the threat.
- **Missed (Junk)** A non-**Microsoft** service has allowed through ('missed') the threat and **Microsoft Office 365** has subsequently sent it to the Junk folder.

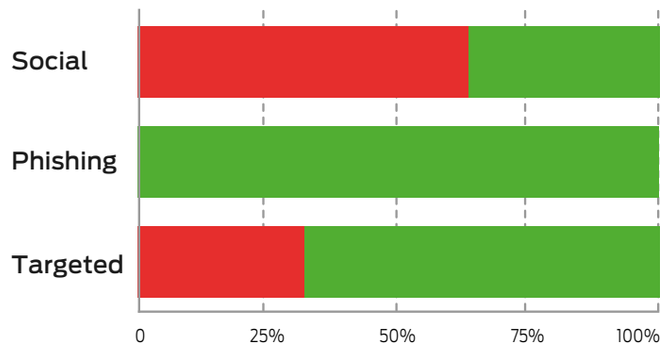
*For a more detailed explanation of these terms please see **Appendix A:** Terms Used on page 15.*

These results illustrate how each service handled a range of attacks, categorised as Social Engineering, Phishing and Targeted. These are typical, general methods that criminals use to gain unauthorised access to victims' computer systems, internet accounts or funds.

Tactics typically include sending customised malware as email attachments; links to websites hosting exploits capable of downloading threats onto computers; links to websites posing as legitimate services such as Gmail and Amazon; and requests for money, while impersonating a friend, relative or colleague.

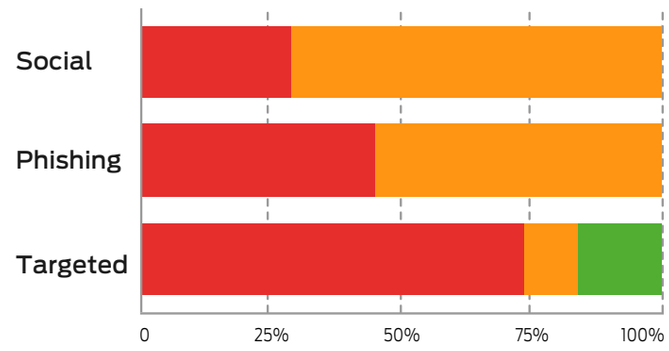
Forcepoint Email Security Cloud

	Inbox	Missed (Junk Folder)	Edited (Allow)	Junk Folder	Notified	Stopped	Rejected	Edited (Deny)
Social	20	18	0	0	0	22	0	0
Phishing	0	0	0	0	1	28	0	31
Targeted	16	3	0	0	30	1	0	10
TOTAL	**36**	**21**	**0**	**0**	**31**	**51**	**0**	**41**



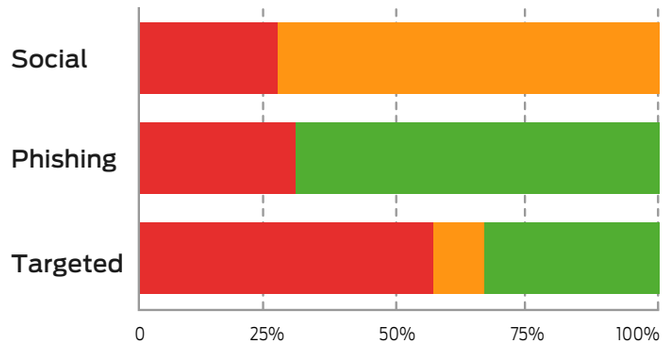
Microsoft Office 365

	Inbox	Missed (Junk Folder)	Edited (Allow)	Junk Folder	Notified	Stopped	Rejected	Edited (Deny)
Social	17	0	0	43	0	0	0	0
Phishing	27	0	0	33	0	0	0	0
Targeted	44	0	0	6	0	10	0	0
TOTAL	**88**	**0**	**0**	**82**	**0**	**10**	**0**	**0**



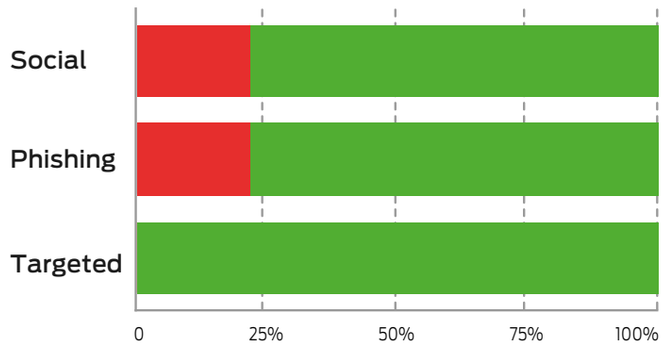
Microsoft Office 365 Advanced Threat Protection

	Inbox	Missed (Junk Folder)	Edited (Allow)	Junk Folder	Notified	Stopped	Rejected	Edited (Deny)
Social	16	0	0	44	0	0	0	0
Phishing	0	0	18	0	2	0	0	40
Targeted	34	0	0	6	0	11	0	9
TOTAL	**50**	**0**	**18**	**50**	**2**	**11**	**0**	**49**



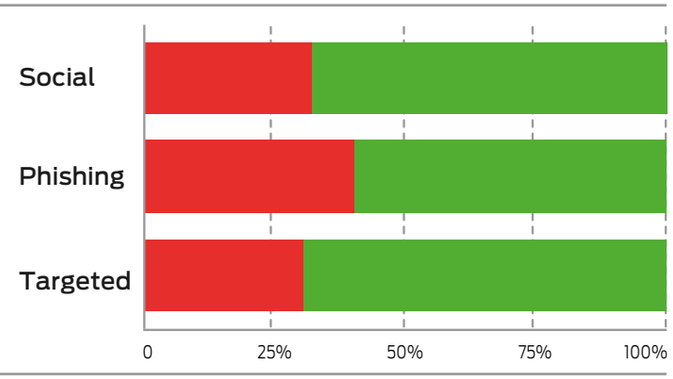
Mimecast Secure Email Gateway

	Inbox	Missed (Junk Folder)	Edited (Allow)	Junk Folder	Notified	Stopped	Rejected	Edited (Deny)
Social	7	6	0	0	0	0	47	0
Phishing	0	0	13	0	0	10	25	12
Targeted	0	0	0	0	0	33	27	0
TOTAL	**7**	**6**	**13**	**0**	**0**	**43**	**99**	**12**



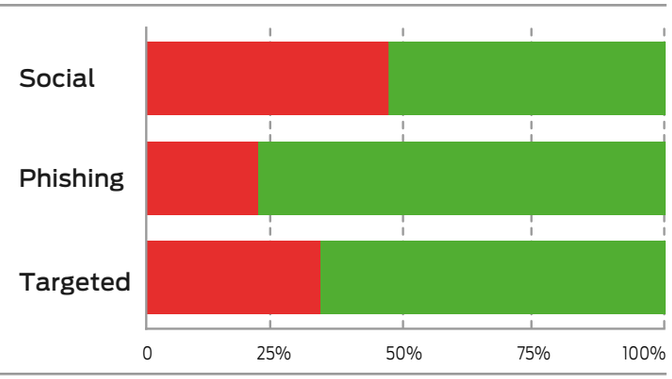
Proofpoint Essentials

	Inbox	Missed (Junk Folder)	Edited (Allow)	Junk Folder	Notified	Stopped	Rejected	Edited (Deny)
Social	10	9	0	0	0	41	0	0
Phishing	20	4	0	0	0	36	0	0
Targeted	18	0	0	0	0	42	0	0
TOTAL	**48**	**13**	**0**	**0**	**0**	**119**	**0**	**0**



Symantec Email Security .cloud

	Inbox	Missed (Junk Folder)	Edited (Allow)	Junk Folder	Notified	Stopped	Rejected	Edited (Deny)
Social	15	13	0	0	0	31	1	0
Phishing	0	1	12	0	0	32	0	15
Targeted	20	0	0	0	0	30	9	1
TOTAL	**35**	**14**	**12**	**0**	**0**	**93**	**10**	**16**

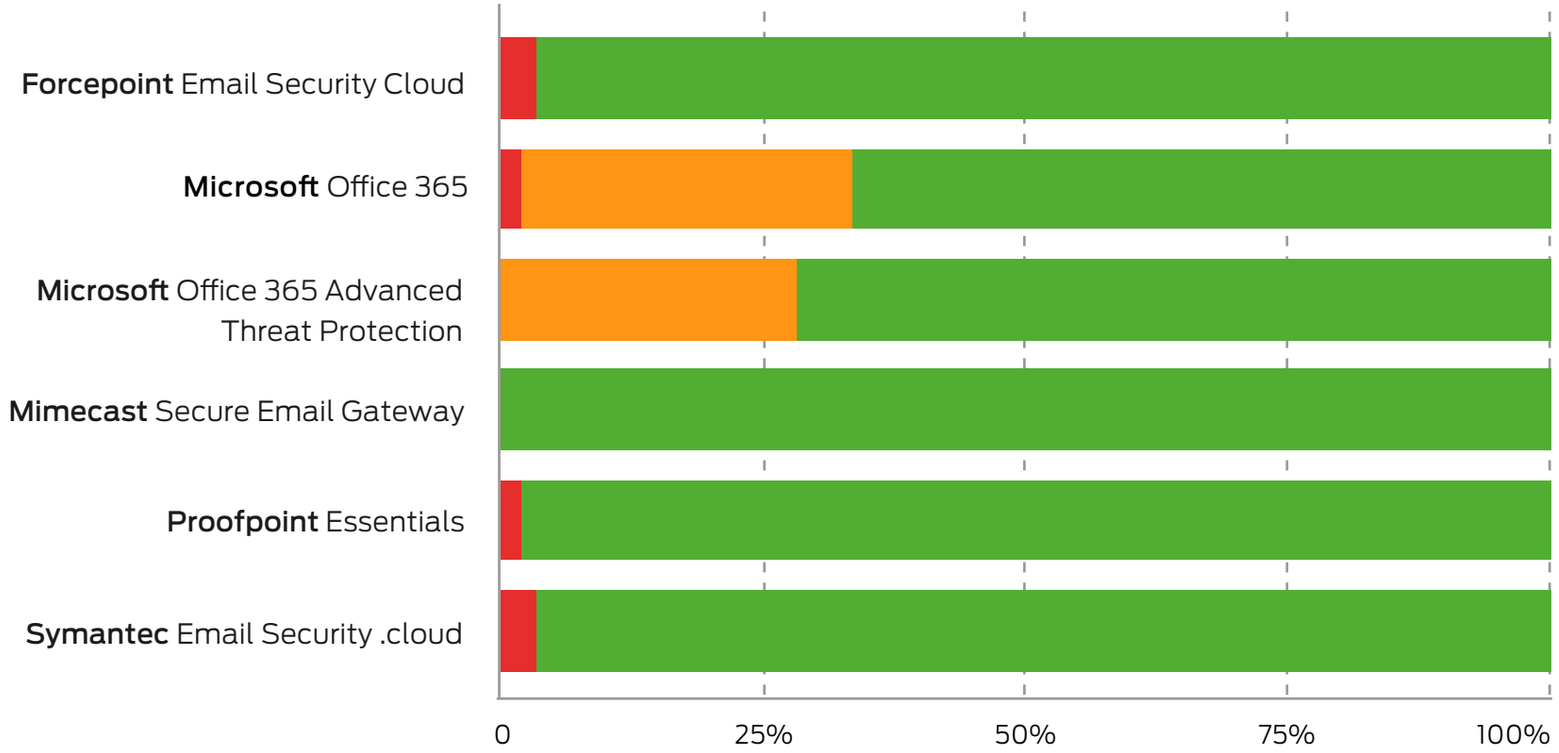


4. Public Attacks

These results show how each service reacted when receiving a stream of messages such as ordinary internet users can expect to receive on a daily basis. They include PayPal phishing attacks, fake Apple account verification attempts and so-called advanced fee fraud messages, designed to trick victims into sending the attacker money.

The same terms, such as ‘inbox’, ‘Junk’ and ‘Stopped’ are used as with the targeted attacks on page 10 and 11.

PUBLIC ATTACKS						
Product	Inbox	Missed (Junk Folder)	Junk Folder	Stopped	Rejected	Edited (Deny)
Forcepoint Email Security Cloud	1	1	0	56	0	2
Microsoft Office 365	1	0	19	40	0	0
Microsoft Office 365 Advanced Threat Protection	0	0	17	40	0	3
Mimecast Secure Email Gateway	0	0	0	0	60	0
Proofpoint Essentials	1	0	0	59	0	0
Symantec Email Security .cloud	0	2	0	5	53	0



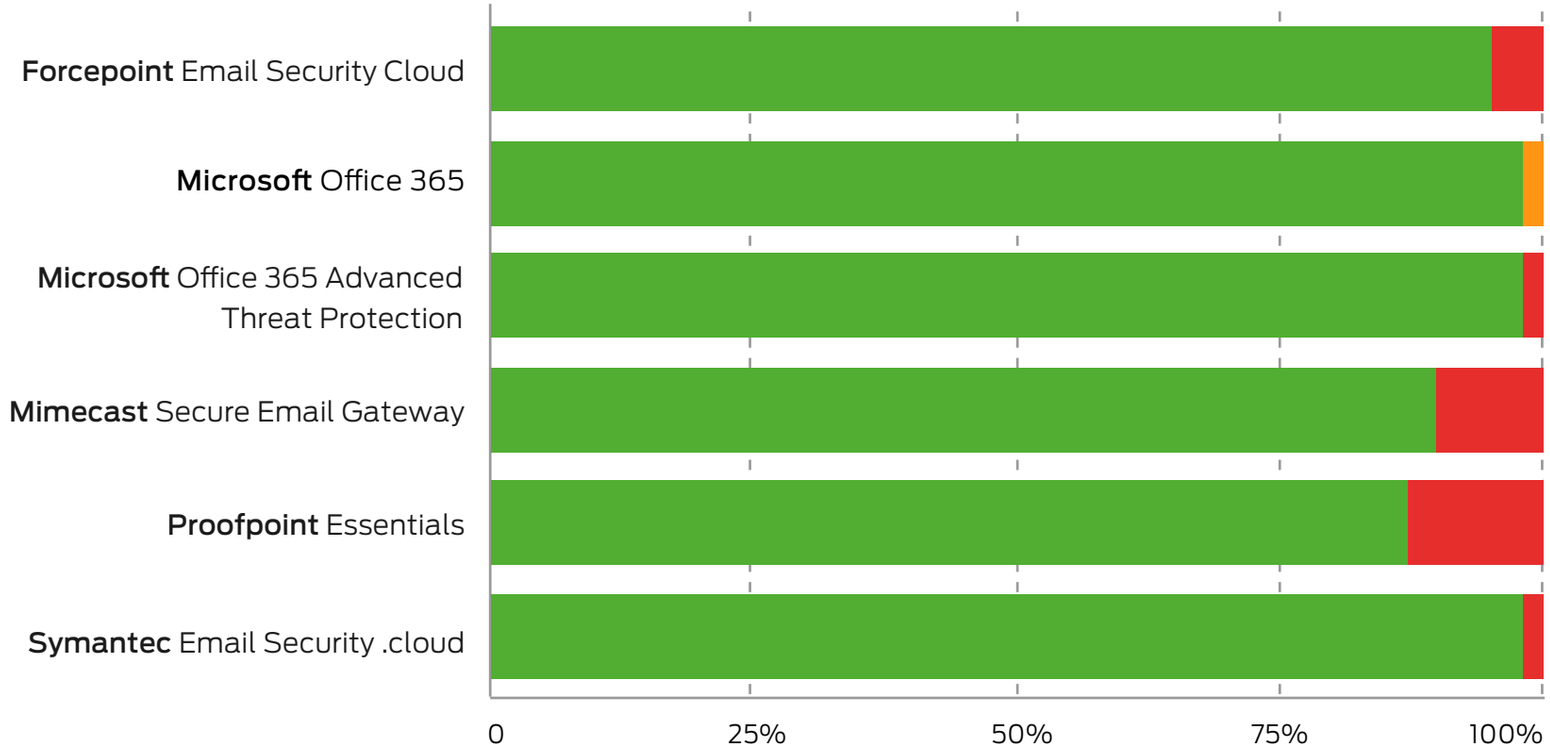
5. Legitimate Messages

These results show how effectively each service managed messages that posed no threat. In an ideal world all legitimate messages would arrive in the inbox. When they are categorised as being a threat then a 'false positive' result is recorded.

It is important to test for false positives because too many indicate a product that is too aggressive and will block useful email as well as threats. It would be easy to create a product that blocked all threats if it was also allowed to block all legitimate email. Finding the balance between allowing good and blocking bad is the key to almost every type of security system.

LEGITIMATE MESSAGES

Product	Inbox	Edited (Allow)	Junk Folder	Stopped	Rejected	Edited (Deny)
Forcepoint Email Security Cloud	57	0	0	1	0	2
Microsoft Office 365	59	0	1	0	0	0
Microsoft Office 365 Advanced Threat Protection	50	9	0	0	0	1
Mimecast Secure Email Gateway	49	5	0	2	4	0
Proofpoint Essentials	52	0	0	8	0	0
Symantec Email Security .cloud	49	10	0	1	0	0



6. Conclusion

The results in this report show the combined protection levels of **Microsoft Office 365** and a number of additional email security services when facing both common public threats and targeted attacks designed to compromise individual targets.

It is important to understand that email security services rarely work in isolation of other layers of protection. In addition to endpoint security solutions, other email protection products will almost certainly come into play. Specifics depend on which email services users choose. For example, **Google's** free and paid-for email services include anti-spam and anti-malware protection, as does **Microsoft Office 365**.

This test used **Office 365** as the standard email platform. It provides a default level of protection that can be increased by an account's administrator but not disabled. The lowest level of protection is the default setting. All of the additional products were configured according to the vendor's recommendations for standard use.

Proofpoint did not engage with this test and so its default settings were used.

Mimecast Secure Email Gateway protected against all of the public attacks and did extremely well against the targeted attacks. All of the targeted malware was removed before users could encounter it. Some social engineering and phishing attacks made it through, but far fewer than with competing services. Its aggressive stance to attacks was such that it also removed a lot of the legitimate messages in comparison to the other services. Only **Proofpoint** was more inaccurate when it came to handling non-malicious messages.

Forcepoint Email Security Cloud stopped all of the targeted phishing attacks, deleting half and neutralising the malicious content of the other half. It also did extremely well with the public attacks, preventing all but one from coming without reach of the user. It was less effective against social engineering attacks than the other services but better than most at handling targeted malware. It was relatively accurate at handling legitimate messages.

Symantec Email Security .cloud missed just two of the public threats and deleted far more of the other threats than it allowed. Notably, it allowed quite a few of the social engineering threats through, and one third of the targeted malware, but its handling of phishing emails was excellent and its high accuracy when handling legitimate email puts in a comfortable third place.

Proofpoint Essentials stopped all but one of the public threats but was similarly challenged by the targeted malware, allowing just under one third of the files through to the inbox. It struggled with the phishing threats too, allowing more through than any other non-Microsoft service. It was the most aggressive when handling legitimate email and only let one third through into the user's inbox.

Microsoft Office 365, was the most accurate when handling legitimate email. It was also very effective at blocking the public threats, allowing only one into the inbox. It relied heavily on sending messages to the Junk folder, rather than deleting messages before they reached the user, which lowered its protection rating. It also missed a lot of the targeted social engineering and phishing threats, while also allowing a very large proportion of the targeted malware through to the inbox.

Microsoft Office 365 Advanced Threat Protection was more aggressive with legitimate messages, but still more accurate than most of the services tested in this report. It prevented more targeted malware arriving in the user's hands and stopped all of the public threats. By editing messages it neutralised many more of the targeted phishing emails that plain **Office 365** had allowed through.

Based on how effectively the services prevented public and targeted threats from reaching the user, the most effective was **Mimecast Secure Email Gateway**. Services from F**orcepoint, Symantec** and **Proofpoint** also provided significant additional protection to users of **Microsoft Office 365**.

In default mode **Microsoft Office 365** does pick up a lot of threats but very often puts these within easy reach of users, in the Junk folder. Its Advanced Threat Protection add-on provides some additional value and reduces this problem, but not to the same extent as the leading services listed here.

Appendices

APPENDIX A: Terms Used

TERM	MEANING
Stopped	The service silently prevented the threat from being delivered. This may be a result of the service preventing the email from even entering its own system, or it may analyse it before deleting it.
Rejected	The service prevented the threat from being delivered and sent a notification to the sender. This is equivalent to a 'bounced' message such as you'd see when sending an email to an account that does not exist.
Notified	The service prevented the threat from being delivered and notified the user. There was no option for the user to recover the threat. In this way the user is aware that a message was sent and blocked, but inquisitive users cannot recover and investigate the message.
Quarantined	The service prevented the threat from being delivered and kept a copy of the threat, which could be recovered by the user or an administrator. In this way an organisation can investigate the nature of incoming threats, although users can also expose themselves to threats if they elect to recover malicious messages.
Edited	The service delivered the message but altered it to remove malicious content. There are many possible methods but common ones include deleting malware attachments, deleting malicious links and re-writing embedded links to redirect users to warning pages.
Junk	The message was delivered to the user's Junk box by **Microsoft Office 365** or **Office 365 Advanced Threat Protection**. When other services show 'Junk' results this means they missed the threat and the user was protected by **Office 365's** security layer. The Junk folder is within easy reach of users, who may be tempted to recover and examine malicious messages.
Inbox	The service failed to detect or protect against the threat. It arrived in the user's inbox and appears as a legitimate message, which the user is free to open and examine.
Targeted attack	A targeted attack is aimed at a specific person or organisation. It may be sent from email accounts and IP addresses that are not known to be the source of more widely-spread threats. Such attacks may use malware that is not widely recognisable by anti-malware scanners.

APPENDIX B: FAQs

A full methodology for this test is available from our website.

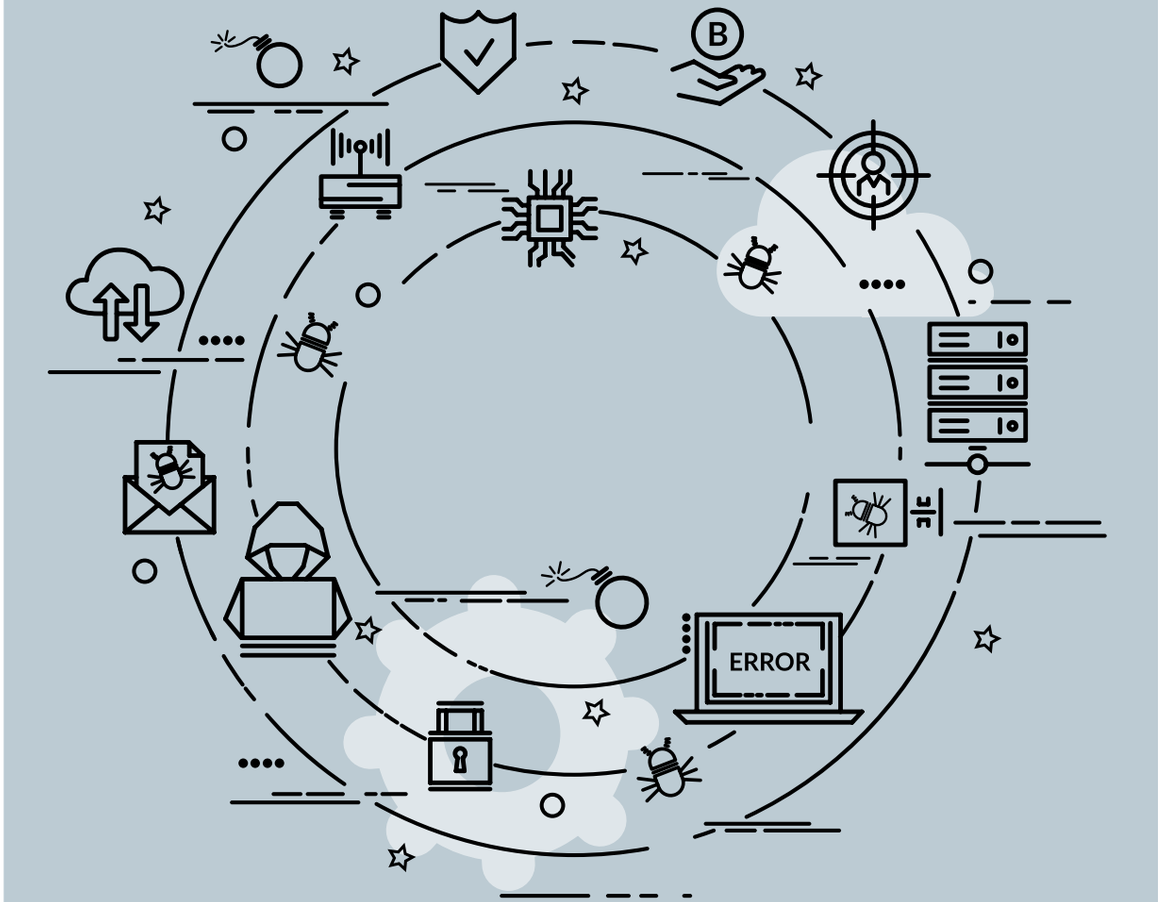
- The products chosen for this test were selected by SE Labs.
- The test was unsponsored.
- The test was conducted in February 2018.
- All products were configured according to each vendor's recommendations, when such recommendations were provided.
- Malicious emails, URLs, attachments and legitimate messages were independently located and verified by SE Labs.
- Targeted attacks were selected and verified by SE Labs.
- Malicious and legitimate data was provided to partner organisations once the test was complete.
- SE Labs conducted this email security services protection test using real email accounts running on popular commercial services.

Q What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

A Partner organisations benefit from our consultancy services after a test has been run. Partners may gain access to low-level data that can be useful in product improvement initiatives and have permission to use award logos, where appropriate, for marketing purposes. We do not share data on one partner with other partners. We do not partner with organisations that do not engage in our testing.

Q I am a security vendor and you tested my product without permission. May I access the threat data to verify that your results are accurate?

A We are willing to share a certain level of test data with non-partner participants for free. The intention is to provide sufficient data to demonstrate that the results are accurate. For more in-depth data suitable for product improvement purposes we recommend becoming a partner.



APPENDIX C: Services tested

The table below shows the service's name as it was being marketed at the time of the test.

SERVICES TESTED	
Vendor	**Service**
Forcepoint	Email Security Cloud
Microsoft	Office 365
Microsoft	Office 365 Advanced Threat Protection
Mimecast	Secure Email Gateway
Proofpoint	Essentials Business Edition
Symantec	Email Security .cloud

SE Labs Report Disclaimer

1. The information contained in this report is subject to change and revision by SE Labs without notice.
2. SE Labs is under no obligation to update this report at any time.
3. SE Labs believes that the information contained within this report is accurate and reliable at the time of its publication, which can be found at the bottom of the contents page, but SE Labs does not guarantee this in any way.
4. All use of and any reliance on this report, or any information contained within this report, is solely at your own risk. SE Labs shall not be liable or responsible for any loss of profit (whether incurred directly or indirectly), any loss of goodwill or business reputation, any loss of data suffered, pure economic loss, cost of procurement of substitute goods or services, or other intangible loss, or any indirect, incidental, special or consequential loss, costs, damages, charges or expenses or exemplary damages arising his report in any way whatsoever.
5. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.
6. The testing and subsequent results do not guarantee that there are no errors in the products, or that you will achieve the same or similar results. SE Labs does not guarantee in any way that the products will meet your expectations, requirements, specifications or needs.
7. Any trade marks, trade names, logos or images used in this report are the trade marks, trade names, logos or images of their respective owners.
8. The contents of this report are provided on an "AS IS" basis and accordingly SE Labs does not make any express or implied warranty or representation concerning its accuracy or completeness.