SE Labs

INTELLIGENCE-LED TESTING

www.SELabs.uk info@SELabs.uk @SELabsUK www.facebook.com/selabsuk blog.selabs.uk

EMAIL-HOSTED PROTECTION

AUGUST 2017

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.

CONTENTS

Document version 1.1. Written 23rd October 2017
Corrected graph colour and product details for Mimecast.
Document version 1. 0. Written 30th August 2017.

SIMON EDWARDS
Director

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

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

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Gia Gorbold
Liam Fisher
Alexandru Statie
Jon Thompson
Jake Warren
Stephen Withey

IT SUPPORT
Danny King-Smith
Chris Short

PUBLICATION
Steve Haines
Colin Mackleworth

INTRODUCTION

Email provides a route right into the heart of our computers, phones and other devices. As such, it is frequently abused to perform a variety of attacks against potential victims of cybercrime. The sophistication of attacks vary but many rely on our almost unbreakable instinct to open, read and interact with messages sent to work and personal email accounts. Businesses rely on email security services to filter out large numbers of such attacks.

The range of attack types in the real world is wide, but in general we consider there to be two main categories: targeted attacks, in which the attacker attempts to target a specific individual; and public attacks, which spread wide and far in an attempt to compromise as many people as possible.

Many of the same techniques are used in public and targeted attacks. The least technically sophisticated include requests for a money transfer or banking login credentials. More credible attempts include professionally-formatted emails and links to fake websites designed to trick users into entering their valuable details.

Attackers with more resources may use malware to achieve their goals, either in the form of attached files or by linking to websites that exploit visiting computers.

SE Labs monitors email threats in real-time, analysing large numbers of messages and extracting samples that represent large groups of those threats. Human testers then manually verify that any malware included works properly before re-sending these threats to our own accounts through the tested services.

We also generate targeted attacks using the same tools and techniques used by advanced attackers. In gathering threats this way we achieve a realistic and relevant coverage of existing threats in a small set of test samples.

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

The services tested are listed in this report using the vendors' names.

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

PRODUCT	PROTECTION ACCURACY RATING	LEGITIMATE ACCURACY RATING	TOTAL ACCURACY RATING
Proofpoint Essentials	100%	100%	100%
Mimecast Secure Email Gateway	99%	100%	99%
Forcepoint Email Security Cloud	89%	100%	92%
Microsoft Office 365	78%	82%	79%
Microsoft Office 365 Advanced Threat Protection	84%	40%	69%

Products highlighted in green were the most accurate, scoring 85 per cent or more for Total Accuracy. Those in yellow scored less than 85 but 75 or more. Products shown in red scored less than 75 per cent. For exact percentages, see 1. Total Accuracy Ratings on page 6.

Email hosted protection services are capable of filtering out large numbers of threats before they hit 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 reaching the user.

Others equivocated somewhat and moved the messages to the 'Junk' folder, which is within easy reach of inquisitive users. These services also moved a significant proportion of legitimate messages to the 'Junk' folder.

Based on how effectively the services prevented public threats from reaching the user, the most effective services were those from **Mimecast**, **Proofpoint**, and **Forcepoint Email Security Cloud.** All of these services add significant protection compared to the basic **Microsoft Office 365** service.

The **Microsoft Office 365 Advanced Threat Protection** add-on adds some additional value and reduces this problem, but not to the same extent as the leading services listed here, which were all much better able to classify legitimate messages correctly.

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.

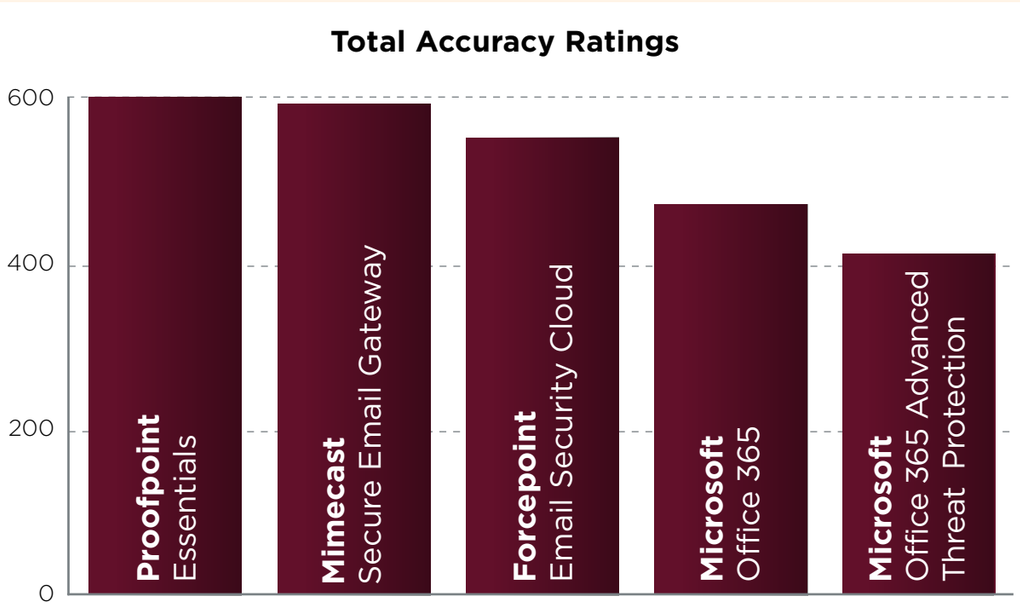
The graph below takes into account not only each service's ability to detect and protect against threats, but also its handling of non-malicious messages and components of those messages, such as attachments and links to websites.

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 Protection Ratings on page 8 for more details.



Total Accuracy Ratings combine protection and false positives.

AWARDS

The following products win SE Labs awards:

- Proofpoint Essentials
- Mimecast Secure Email Gateway
- Forcepoint Email Security Cloud

- Microsoft Office 365

TOTAL ACCURACY RATINGS			
Product	**Total Accuracy Rating**	**Total Accuracy%**	**Award**
Proofpoint Essentials	600	100%	AAA
Mimecast Secure Email Gateway	595	99%	AAA
Forcepoint Email Security Cloud	554	92%	AAA
Microsoft Office 365	475	79%	B
Microsoft Office 365 Advanced Threat Protection	415	69%	

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.

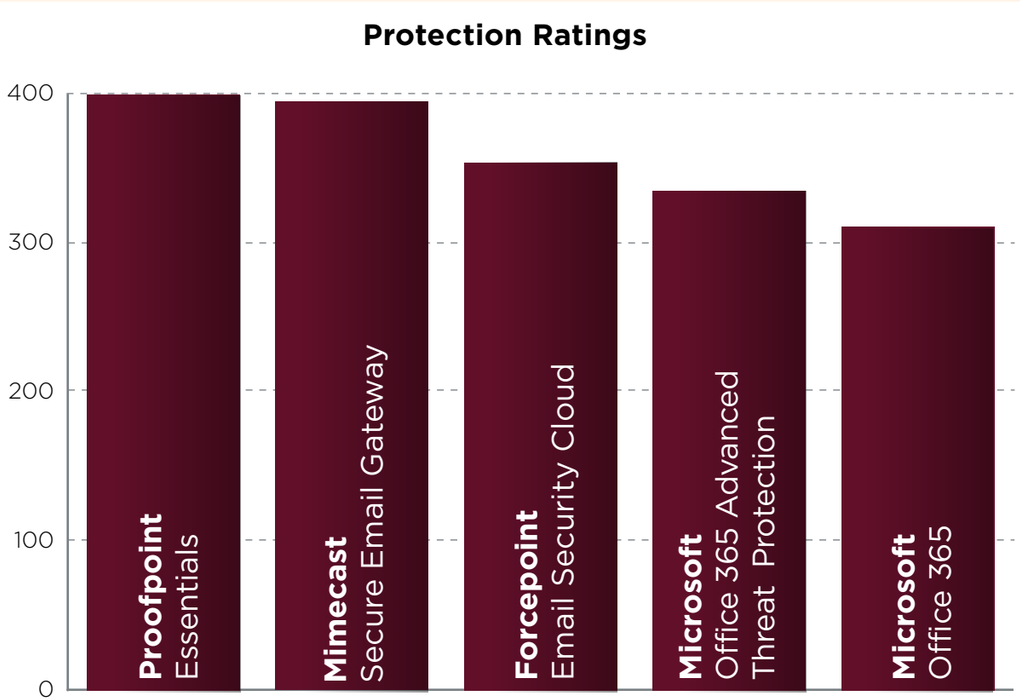
■ **Junk (+2 for threats; -4 for legitimate)**
Services that delivers malicious email into a client-side folder called 'Junk' or similar, which is easily accessible by the recipient, are awarded two points. The action of sending legitimate email to this folder brings with it a penalty of minus four points.

■ **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.

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

PROTECTION RATING COMPARISON

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

PROTECTION RATINGS

Product	Protection Rating	Protection Rating (%)
Proofpoint Essentials	400	100%
Mimecast Secure Email Gateway	395	99%
Forcepoint Email Security Cloud	354	89%
Microsoft Office 365 Advanced Threat Protection	335	84%
Microsoft Office 365	311	78%

Average: 90%

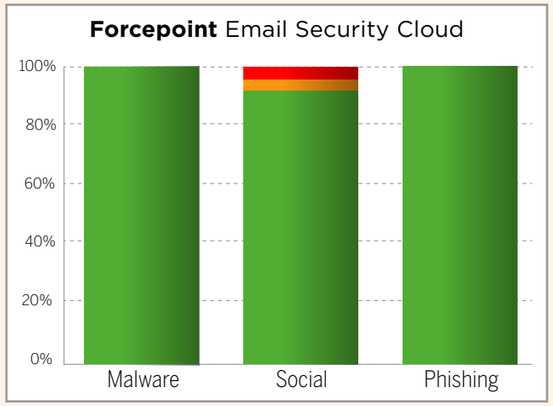
PUBLIC ATTACKS

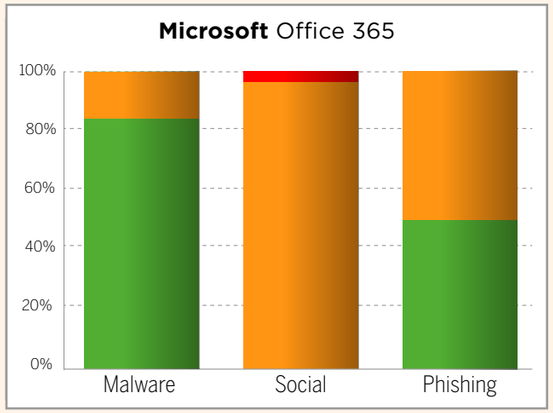
These results show how each service reacted when receiving a stream of messages such as ordinary internet users can expect to receive on a daily basis. They include PayPal phishing attacks, fake Apple account verification attempts and so-called advanced fee fraud messages, designed to trick victims into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

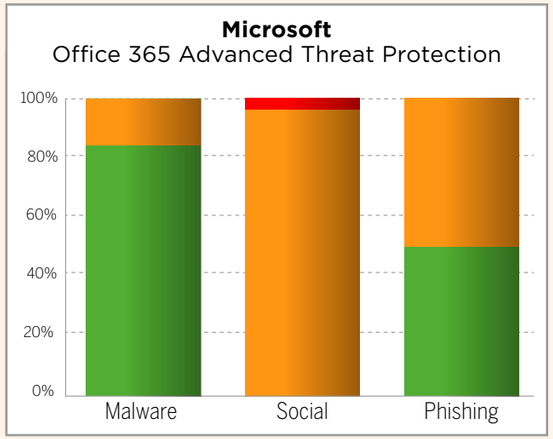
The results below use the following terms:

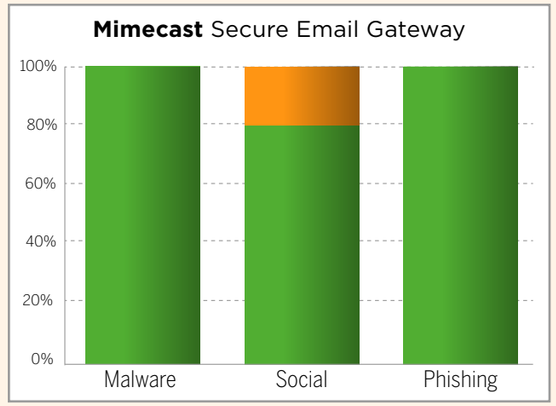
- **Stopped** The service silently prevented the threat from being delivered.
- **Rejected** The service prevented the threat from being delivered and sent a notification to the sender.
- **Notified** The service prevented the threat from being delivered and notified the user. There was no option for the user to recover the threat.
- **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** 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.
- **Inbox** The service failed to detect or protect against the threat.

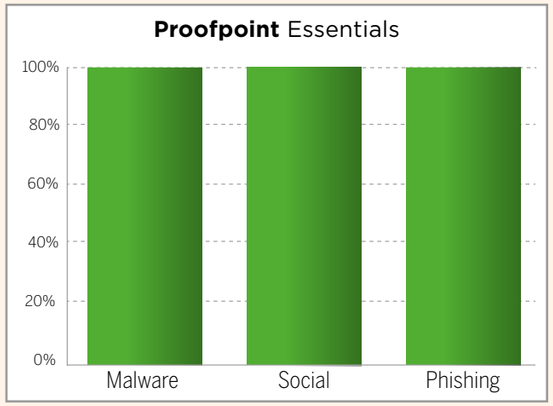
*For a more detailed explanation of these terms please see **Appendix A:** Terms Used on page 15.*











Forcepoint Email Security Cloud

	Stopped	Rejected	Notified	Quarantined	Edited	Junk	Inbox
Malware	22	2	1	0	0	0	0
Social	23	1	0	1	0	0	1
Phishing	24	0	0	0	0	0	0
TOTAL	**69**	**3**	**1**	**1**	**0**	**0**	**1**

Microsoft Office 365

	Stopped	Rejected	Notified	Quarantined	Edited	Junk	Inbox
Malware	21	0	0	0	0	4	0
Social	0	0	0	0	0	25	1
Phishing	12	0	0	0	1	11	0
TOTAL	**33**	**0**	**0**	**0**	**1**	**40**	**1**

Microsoft Office 365 Advanced Threat Protection

	Stopped	Rejected	Notified	Quarantined	Edited	Junk	Inbox
Malware	21	0	0	0	4	0	0
Social	0	0	0	0	4	21	1
Phishing	12	0	0	0	5	7	0
TOTAL	**33**	**0**	**0**	**0**	**13**	**28**	**1**

Mimecast Secure Email Gateway

	Stopped	Rejected	Notified	Quarantined	Edited	Junk	Inbox
Malware	0	25	0	0	0	0	0
Social	0	21	0	5	0	0	0
Phishing	0	24	0	0	0	0	0
TOTAL	**0**	**70**	**0**	**5**	**0**	**0**	**0**

Proofpoint Essentials

	Stopped	Rejected	Notified	Quarantined	Edited	Junk	Inbox
Malware	24	1	0	0	0	0	0
Social	26	0	0	0	0	0	0
Phishing	24	0	0	0	0	0	0
TOTAL	**74**	**1**	**0**	**0**	**0**	**0**	**0**

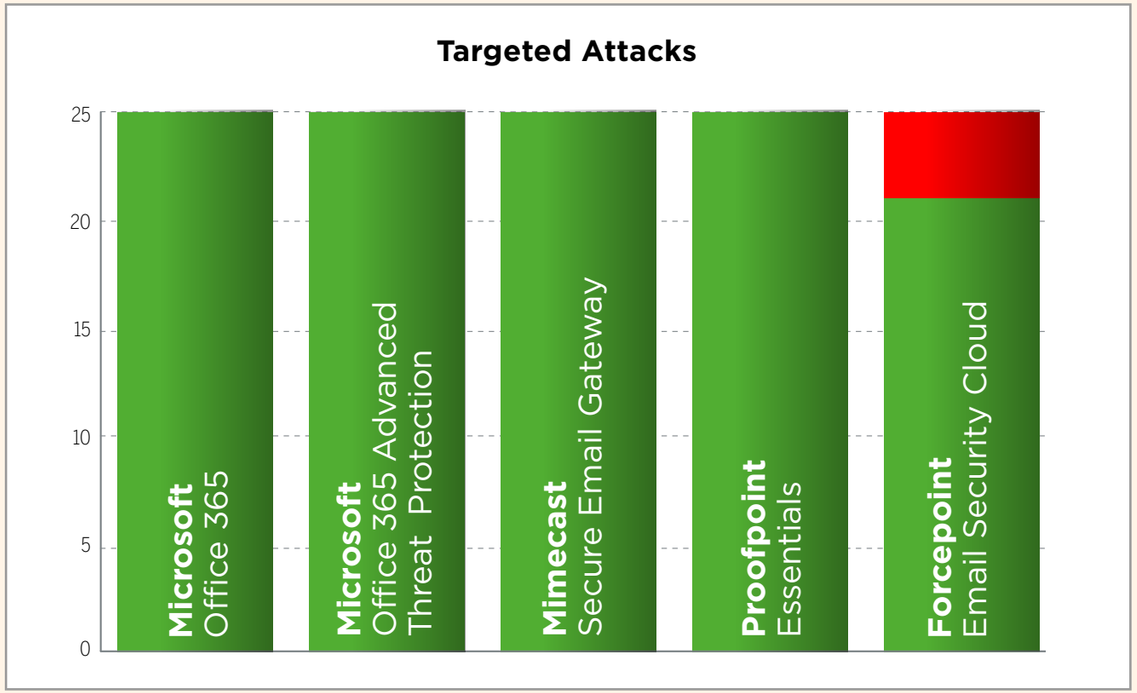
TARGETED ATTACKS

These results illustrate how each service handled the types of attacks that criminals use when attempting to compromise computers belonging to specific individuals. Tactics typically include sending email attachments containing customised malware and links to websites hosting exploits capable of automatically downloading threats onto visiting computers.

The same terms, such as 'Inbox', 'Junk' and 'Stopped' are used as with the public attacks results on page 06.

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

TARGETED ATTACKS			
Product	**Stopped**	**Notified**	**Inbox**
Microsoft Office 365	25	0	0
Microsoft Office 365 Advanced Threat Protection	25	0	0
Mimecast Secure Email Gateway	25	0	0
Proofpoint Essentials	25	0	0
Forcepoint Email Security Cloud	0	21	4

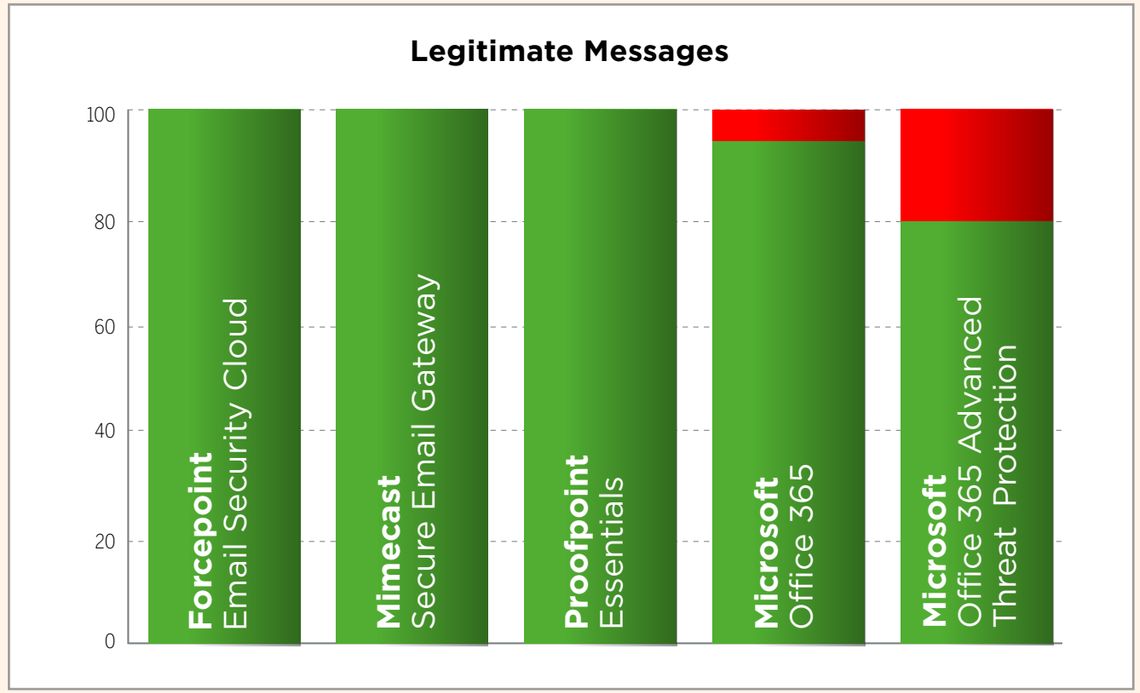


LEGITIMATE MESSAGES

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**	**Junk**
Forcepoint Email Security Cloud	100	0
Mimecast Secure Email Gateway	100	0
Proofpoint Essentials	100	0
Microsoft Office 365	94	6
Microsoft Office 365 Advanced Threat Protection	80	20



CONCLUSIONS

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 the email hosted protection services rarely work in isolation of other layers of protection. In addition to endpoint security solutions, other email hosted protection will almost certainly come into play. Specific 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.

Forcepoint did engage with this test but its **Forcepoint Email Security Cloud** service was tested just before the introduction of its new **Forcepoint Advanced Malware Detection** service.

Mimecast Secure Email Gateway protected against all of the malware attacks, none of which were made available to inquisitive users via a quarantine system. It quarantined five social engineering attacks and removed all of the phishing messages effectively. None of the targeted attacks were able to pass through the system but all legitimate messages passed through freely. Although Targeted Threat Protection was configured, it was not exercised in this test.

Proofpoint Essentials protected against all of the malware attacks and none were made available via the quarantine system. It blocked all of the social engineering and phishing attacks from reaching the user and also stopped all of the targeted attacks. The service allowed the delivery of all legitimate messages.

Forcepoint Email Security Cloud protected against all of the malware attacks, none of which were made available to inquisitive users via a quarantine system. It quarantined one social engineering attack and removed all of the phishing messages effectively. It allowed one social engineering attach through to the user's inbox. Four targeted attacks were also able to penetrate as far as the inbox. The service allowed the delivery of all legitimate messages.

Microsoft Office 365 in default mode, which is the least aggressive available, shielded the user from most of the malware, but allowed four infected messages to move as far as the Junk folder. All but one of the social engineering attacks ended up here as well, the exception making it as far as the inbox. Just over half of the phishing attacks were removed before the user could see them, but 11 also ended up within reach, in the Junk folder. It blocked all of the targeted attacks but sadly also sent six of the legitimate messages to the Junk folder.

Microsoft Office 365 Advanced Threat Protection was even more aggressive with legitimate messages, sending 20 of them to the Junk folder.It was completely effective against the targeted attacks and handled the public threats differently to the standard **Office 365** service. It made changes to many of the threats, re-writing URLs to protect users. As a result the Junk folder was less full and the user was completely shielded from more threats.

Based on how effectively the services prevented public threats from reaching the user, the most effective services were those from **Mimecast, Proofpoint** and **Forcepoint Email Security Cloud.** All of these services add significant protection compared to the basic **Microsoft Office 365** service.

In default mode **Microsoft Office 365** does pick up a lot of threats but puts these within easy reach of users, in the Junk folder. Its Advanced Threat Protection add-on adds some additional value and reduces this problem, but not to the same extent as the leading services listed here, which were all much better able to classify legitimate messages correctly.

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 July 2017.
- 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 hosted protection test using real email accounts running on popular commercial services.

Q I am a security vendor. How can I include my service in your test?

A Please contact us at **info@SELabs.uk**. We will be happy to arrange a phone call to discuss our methodology and the suitability of your service for inclusion

Q I am a security vendor. Does it cost money to have my service tested?

A We do not charge directly for testing products in public tests. We do charge for private tests.

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

A Partner organisations support our tests by paying for access to test data after each test has completed but before publication. Partners can dispute results and use our award logos for marketing purposes. We do not share data on one partner with other partners. We do not currently partner with organisations that do not engage in our testing.

Q So you don't share threat data with test participants before the test starts?

A No, this would bias the test and make the results unfair and unrealistic.

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 small subsets of data with non-partner participants at our discretion. A small administration fee is applicable.

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