SE Labs

INTELLIGENCE-LED TESTING

EMAIL SECURITY SERVICES PROTECTION

DECEMBER 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 Director Stefan Dumitrascu

TESTING TEAM
Thomas Bean
Dimitar Dobrev
Liam Fisher
Gia Gorbold
Pooja Jain
Ivan Merazchiev
Jon Thompson
Dave Togneri
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

SE Labs is BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

SE Labs is a member of the Microsoft Virus Information Alliance (VIA); the Anti-Malware Testing Standards Organization (AMTSO); and the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG).

CONTENTS

Document version 1.02 Updated 14th December 2018, correction to 4. Threat Detection Results; 1.01 Updated 13th December 2018, minor typographical errors; Written 5th December 2018.

INTRODUCTION

Email security test explores how and when services detect and stop threats

This new email protection test shows a wide variation in the abilities of the services that we have assessed. You might see the figures as being disappointing. Surely Microsoft Office 365 can't be that bad? An eight per cent accuracy rating seems incredible. Literally not credible. If it misses most threats then organisations relying on it for email security would be hacked to death (not literally).

But our results are subtler than just reflecting detection rates and it's worth understanding exactly what we're testing here to get the most value from the data. We're not testing these services with live streams of real emails, in which massive percentages of messages are legitimate or basic spam.

Depending on who you talk to, around 50 per cent of all email is spam. We don't test anti-spam at all, in fact, but just the small percentage of email that comprises targeted attacks.

In other words, these results show what can happen when attackers apply themselves to specific targets. They do not reflect a "day in the life" of an average user's email inbox.

We have also included some 'commodity' email threats, though – the kind of generic phishing and social engineering attacks that affect everyone. All services ought to stop every one of these. Similarly, we included some clean emails to ensure that the services were not too aggressively configured. All services ought to allow all these through to the inbox.

So when you see results that appear to be surprising, remember that we're testing some very specific types of attacks that happen in real life, but not in vast numbers comparable to spam or more general threats.

The way that services handle threats are varied and effective to greater or lesser degrees. To best reflect how useful their responses are, we have a rating system that accounts for their different approaches. Essentially, services that keep threats as far as possible from users will win more points than those that let the message appear in or near the inbox. Conversely, those that allow the most legitimate messages through to the inbox rate higher than those which block them without the possibility of recovery from a junk folder or quarantine.

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 20.

EXECUTIVE SUMMARY			
Tested	**Protection Accuracy Rating (%)**	**Legitimate Accuracy Rating (%)**	**Total Accuracy Rating (%)**
Symantec Email Security .cloud with ATP	97%	100%	98%
Proofpoint Essentials Advanced	98%	97%	98%
Fortinet FortiMail Cloud - Gateway Premium	92%	100%	93%
Microsoft Office 365 Advanced Threat Protection	20%	95%	35%
Microsoft Office 365	-15%	100%	8%

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 30 or more. Products shown in red scored less than 30 per cent.

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

Email hosted protection services are potentially 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 public threats from reaching the inbox.

Targeted attacks were a different matter completely. The best overall services were **Proofpoint Essentials Advanced** and **Symantec Email Security .cloud with ATP**. Both stopped all of the malware-based targeted threats and the vast majority of the social engineering and phishing attacks. Their scoring was so close that this is virtually a tie for first place.

Fortinet FortiMail Cloud - Gateway Premium took a strong second place as it was effective against most threats, stopping all of the phishing and commodity attacks. It let through very few targeted and social engineering attacks.

Microsoft's services, with and without the **Advanced Threat Protection (ATP)** add-on, were the least effective. The ATP addition brought a noticeable benefit by effectively neutralising the content of phishing and commodity attacks that would otherwise have ended up in the inbox when using the standard Microsoft service.

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.

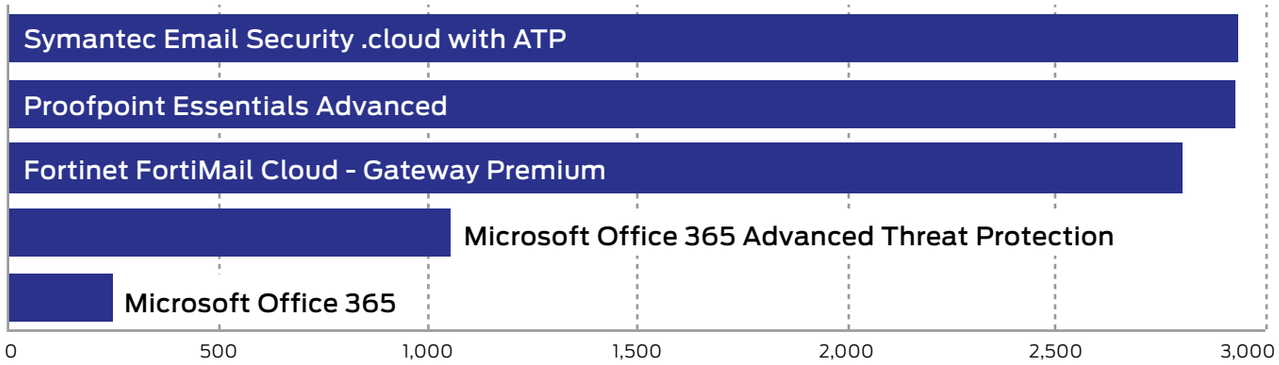
We take these different possible outcomes into account when attributing points that form final ratings.

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			
	Total Accuracy Rating	Total Accuracy (%)	Award
Symantec Email Security .cloud with ATP	2,932	98%	AAA
Proofpoint Essentials Advanced	2,926	98%	AAA
Fortinet FortiMail Cloud - Gateway Premium	2,804	93%	AAA
Microsoft Office 365 Advanced Threat Protection	1,050	35%	B
Microsoft Office 365	246	8%	



Total Accuracy Ratings combine protection and false positives.

Email Security Services Protection Awards

The following products win SE Labs awards:

- **Symantec** Email Security .cloud with ATP
- **Proofpoint** Essentials Advanced
- **Fortinet** FortiMail Cloud - Gateway Premium

- **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 (+10 for threats; -10 for legitimate)
If the service detects the threat and prevents any significant element of that threat from reaching the intended recipient we award it 10 points. If it miscategorises and blocks or otherwise significantly damages legitimate email then we impose a minus 10 point penalty.

Quarantined (Between +8 for threats; -8 for legitimate)
Services that intervene and move malicious messages into a quarantine system are awarded either six or eight points depending on whether or not the user or administrator can recover the message. However, there is a six to eight point deduction for each legitimate message that is incorrectly sent to quarantine.

Junk (+5 for threats; -5 for legitimate)
The message was delivered to the user's Junk box by **Microsoft Office 365** with and without **Advanced Threat Protection**.

Inbox (-10 for threats; +10 for legitimate)
Malicious messages that arrive in the user's inbox have evaded the security service. Each such case loses the service 10 points. All legitimate messages should appear in the inbox. For each one correctly routed there is an award of 10 points.

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

PROTECTION RATING COMPARISON		
Action	**Threat**	**Legitimate**
Inbox	-10	10
Junk Folder	5	-5
Quarantined (admin)	8	-8
Quarantined (user)	6	-6
Notified	10	-10
Stopped	10	-10
Rejected	10	-10
Blocked	10	-10
Edited (Allow)	-10	10
Edited (Deny)	10	-10
Junk (Deny)	10	-10
Junk (Allow)	-7	7

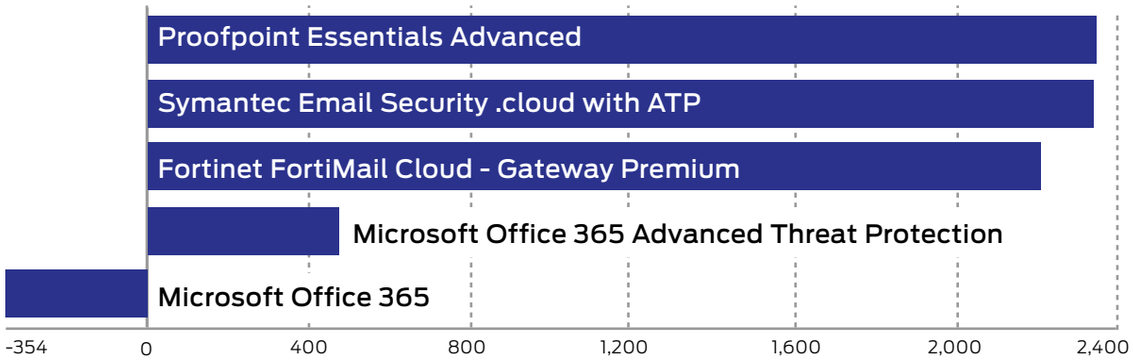
Protection rating =
(10x number of Stopped etc.) +
(6-8x number of Quarantined) +
(5x number of Junk) +
(-10x number of Inbox)
etc.

For legitimate results the formula is:
(10x number of Inbox) +
(-5x number of Junk) +
(-6 -8x number of Quarantined) +
(-10x number of Stopped etc.)
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 – 17) to roll your own set of personalised ratings.

PROTECTION RATINGS		
	Protection Rating	Protection Rating (%)
Proofpoint Essentials Advanced	2,344	98%
Symantec Email Security .cloud with ATP	2,332	97%
Fortinet FortiMail Cloud - Gateway Premium	2,204	92%
Microsoft Office 365 Advanced Threat Protection	480	20%
Microsoft Office 365	-354	-15%

Average: 58%



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

3. Targeted Attack Results

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 19.

These results illustrate how each service handled a range of attacks, categorised as Social Engineering, Phishing and Malware. 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.

Fortinet FortiMail Cloud - Gateway Premium									
	Stopped	Rejected	Edited (Deny)	Junk (Deny)	Quarantined (User)	Junk Folder	Inbox	Edited (Allow)	Junk (Allow)
Social	48	4	0	0	0	0	0	0	8
Phishing	58	2	0	0	0	0	0	0	0
Malware	57	0	0	0	0	0	3	0	0
Commodity	14	46	0	0	0	0	0	0	0
TOTAL	**177**	**52**	**0**	**0**	**0**	**0**	**3**	**0**	**8**

Microsoft Office 365									
	Stopped	Rejected	Edited (Deny)	Junk (Deny)	Quarantined (User)	Junk Folder	Inbox	Edited (Allow)	Junk (Allow)
Social	0	0	0	0	0	43	17	0	0
Phishing	0	0	0	0	0	29	31	0	0
Malware	0	0	0	0	0	1	59	0	0
Commodity	11	1	0	0	1	45	2	0	0
TOTAL	**11**	**1**	**0**	**0**	**1**	**118**	**109**	**0**	**0**

Microsoft Office 365 Advanced Threat Protection									
	Stopped	Rejected	Edited (Deny)	Junk (Deny)	Quarantined (User)	Junk Folder	Inbox	Edited (Allow)	Junk (Allow)
Social	0	0	0	0	0	50	10	0	0
Phishing	1	0	2	27	0	20	5	5	0
Malware	0	0	0	0	0	16	36	8	0
Commodity	11	1	0	9	0	38	1	0	0
TOTAL	**12**	**1**	**2**	**36**	**0**	**124**	**52**	**13**	**0**

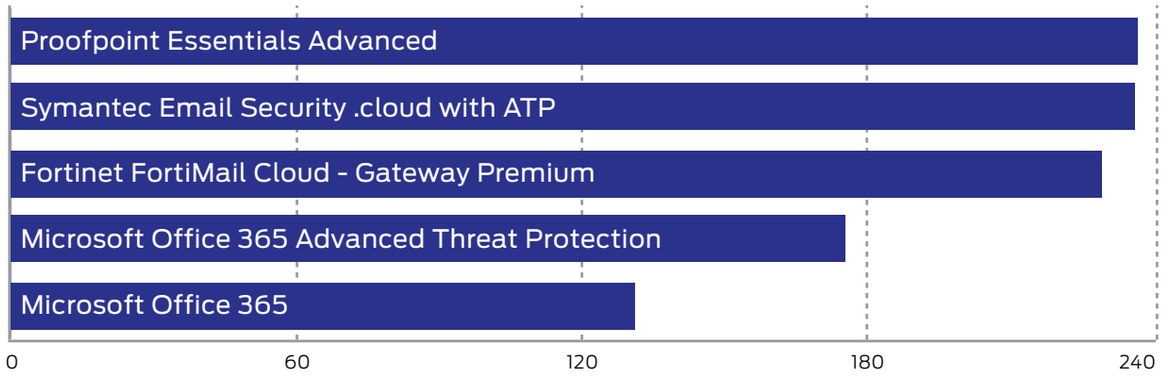
Proofpoint Essentials Advanced									
	Stopped	Rejected	Edited (Deny)	Junk (Deny)	Quarantined (User)	Junk Folder	Inbox	Edited (Allow)	Junk (Allow)
Social	60	0	0	0	0	0	0	0	0
Phishing	57	0	0	0	0	0	0	0	3
Malware	60	0	0	0	0	0	0	0	0
Commodity	11	49	0	0	0	0	0	0	0
TOTAL	**188**	**49**	**0**	**0**	**0**	**0**	**0**	**0**	**3**

Symantec Email Security .cloud with ATP									
	Stopped	Rejected	Edited (Deny)	Junk (Deny)	Quarantined (User)	Junk Folder	Inbox	Edited (Allow)	Junk (Allow)
Social	0	60	0	0	0	0	0	0	0
Phishing	0	60	0	0	0	0	0	0	0
Malware	0	60	0	0	0	0	0	0	0
Commodity	7	48	0	1	0	0	0	0	4
TOTAL	**7**	**228**	**0**	**1**	**0**	**0**	**0**	**0**	**4**

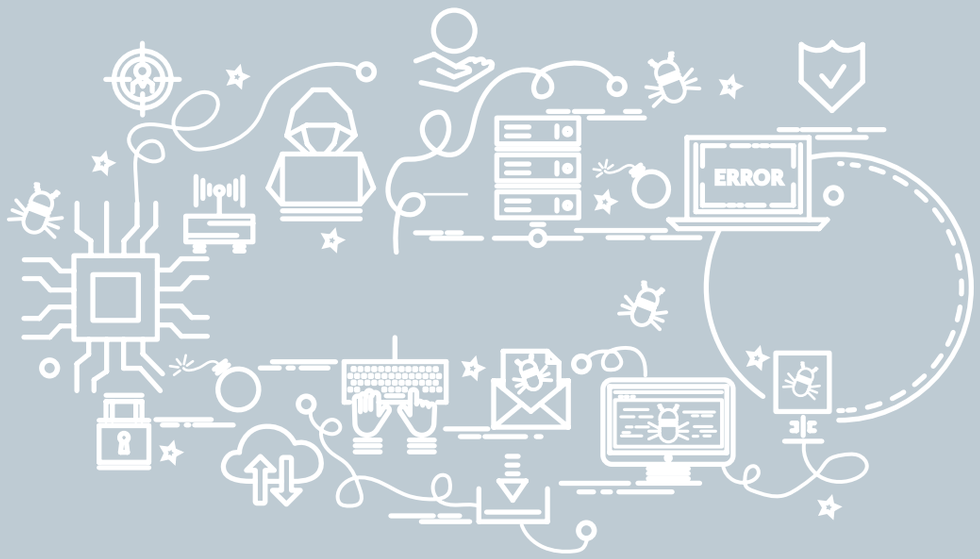
4. Threat Detection Results

While testing and scoring email security services is complex, it is possible to report straight-forward detection rates. The figures below summarise how each service handles threats in the most general, least detailed way. Threats that Microsoft moved to the Junk folder are counted as hits, while any messages that pass through a non-Microsoft service and end up in the Junk folder are misses for that service.

THREAT DETECTION RESULTS			
Detection Rates	**Misses**	**Detection Rate**	**Detection Rate (%)**
Proofpoint Essentials Advanced	3	237	99%
Symantec Email Security .cloud with ATP	4	236	98%
Fortinet FortiMail Cloud - Gateway Premium	11	229	95%
Microsoft Office 365 Advanced Threat Protection	65	175	73%
Microsoft Office 365	109	131	55%



Detection rates are a useful but unsubtle way to compare services



5. Commodity Attack Results

Fortinet FortiMail Cloud - Gateway Premium				
SOCIAL				
	Stopped	**Rejected**	**Inbox**	**Junk (Allow)**
Charity Donation	10	0	0	0
Sextortion	8	2	0	0
Money Mule	9	1	0	0
Inheritance	4	1	0	5
Pyramid Scheme	7	0	0	3
Fake love	10	0	0	0
SOCIAL TOTAL	**48**	**4**	**0**	**8**

PHISHING				
	Stopped	**Rejected**	**Inbox**	**Junk (Allow)**
Oakwood Bank	10	0	0	0
Netflix	9	1	0	0
Twitter	10	0	0	0
GoFundMe	10	0	0	0
Linkedin	9	1	0	0
PDF	10	0	0	0
PHISHING TOTAL	**58**	**2**	**0**	**0**

MALWARE				
	Stopped	**Rejected**	**Inbox**	**Junk (Allow)**
Framework generated payload	7	0	3	0
Payload zip password protected	10	0	0	0
Renamed zip password protected	10	0	0	0
Email link to payload	10	0	0	0
Download button	10	0	0	0
Excel spreadsheet with link to payload	10	0	0	0
MALWARE TOTAL	**57**	**0**	**3**	**0**
GRAND TOTAL	**163**	**6**	**3**	**8**

Microsoft Office 365		
SOCIAL		
	Junk Folder	**Inbox**
Charity Donation	3	7
Sextortion	4	6
Money Mule	8	2
Inheritance	10	0
Pyramid Scheme	10	0
Fake love	8	2
SOCIAL TOTAL	**43**	**17**

PHISHING		
	Junk Folder	**Inbox**
Oakwood Bank	3	7
Netflix	6	4
Twitter	7	3
GoFundMe	1	9
Linkedin	10	0
PDF	2	8
PHISHING TOTAL	**29**	**31**

MALWARE		
	Junk Folder	**Inbox**
Framework generated payload	0	10
Payload zip password protected	0	10
Renamed zip password protected	0	10
Email link to payload	1	9
Download button	0	10
Excel spreadsheet with link to payload	0	10
MALWARE TOTAL	**1**	**59**
GRAND TOTAL	**73**	**107**

Microsoft Office 365 Advanced Threat Protection						
SOCIAL						
	Stopped	**Edited (Deny)**	**Junk Deny**	**Junk Folder**	**Inbox**	**Edited (Allow)**
Charity Donation	0	0	0	3	7	0
Sextortion	0	0	0	7	3	0
Money Mule	0	0	0	10	0	0
Inheritance	0	0	0	10	0	0
Pyramid Scheme	0	0	0	10	0	0
Fake love	0	0	0	10	0	0
SOCIAL TOTAL	**0**	**0**	**0**	**50**	**10**	**0**

PHISHING						
	Stopped	**Edited (Deny)**	**Junk Deny**	**Junk Folder**	**Inbox**	**Edited (Allow)**
Oakwood Bank	1	0	0	9	0	0
Netflix	0	1	8	1	0	0
Twitter	0	1	9	0	0	0
GoFundMe	0	0	0	5	0	5
Linkedin	0	0	10	0	0	0
PDF	0	0	0	5	5	0
PHISHING TOTAL	**1**	**2**	**27**	**20**	**5**	**5**

MALWARE						
	Rejected	**Edited (Deny)**	**Junk Deny**	**Stopped**	**Inbox**	**Edited (Allow)**
Framework generated payload	0	0	0	2	8	0
Payload zip password protected	0	0	0	2	8	0
Renamed zip password protected	0	0	0	0	10	0
Email link to payload	0	0	0	6	0	4
Download button	0	0	0	6	0	4
Excel spreadsheet with link to payload	0	0	0	0	10	0
MALWARE TOTAL	**0**	**0**	**0**	**16**	**36**	**8**
GRAND TOTAL	**1**	**2**	**27**	**86**	**51**	**13**

Proofpoint Essentials Advanced		
SOCIAL		
	Stopped	**Junk (Allow)**
Charity Donation	10	0
Sextortion	10	0
Money Mule	10	0
Inheritance	10	0
Pyramid Scheme	10	0
Fake love	10	0
SOCIAL TOTAL	**60**	**0**

PHISHING		
	Stopped	**Junk (Allow)**
Oakwood Bank	10	0
Netflix	10	0
Twitter	10	0
GoFundMe	10	0
Linkedin	9	1
PDF	8	2
PHISHING TOTAL	**57**	**3**

TARGETED		
	Stopped	**Junk (Allow)**
Framework generated payload	10	0
Payload zip password protected	10	0
Renamed zip password protected	10	0
Email link to payload	10	0
Download button	10	0
Excel spreadsheet with link to payload	10	0
TARGETED TOTAL	**60**	**0**
GRAND TOTAL	**177**	**3**

Symantec Email Security .cloud with ATP	
SOCIAL	
	Rejected
Charity Donation	10
Sextortion	10
Money Mule	10
Inheritance	10
Pyramid Scheme	10
Fake love	10
SOCIAL TOTAL	**60**

PHISHING	
	Rejected
Oakwood Bank	10
Netflix	10
Twitter	10
GoFundMe	10
Linkedin	10
PDF	10
PHISHING TOTAL	**60**

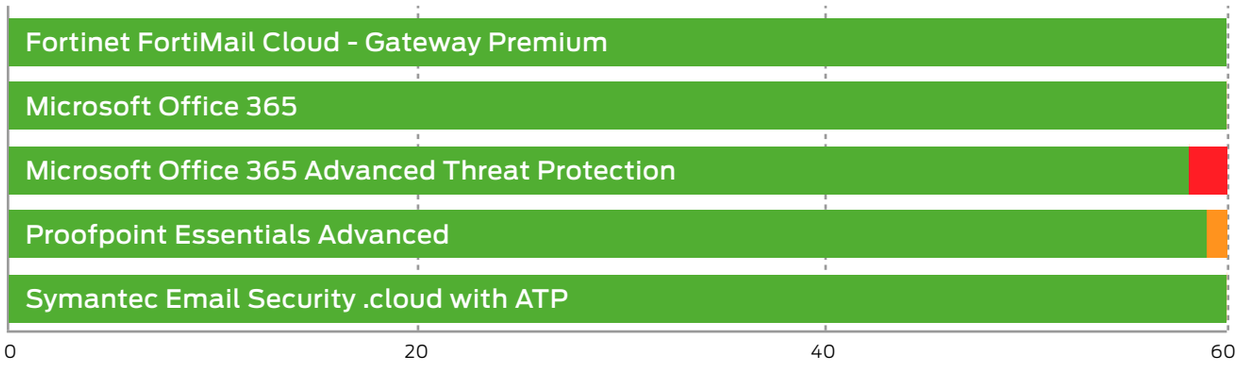
TARGETED	
	Rejected
Framework generated payload	10
Payload zip password protected	10
Renamed zip password protected	10
Email link to payload	10
Download button	10
Excel spreadsheet with link to payload	10
TARGETED TOTAL	**60**
GRAND TOTAL	**180**

6. Legitimate Message Management

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.

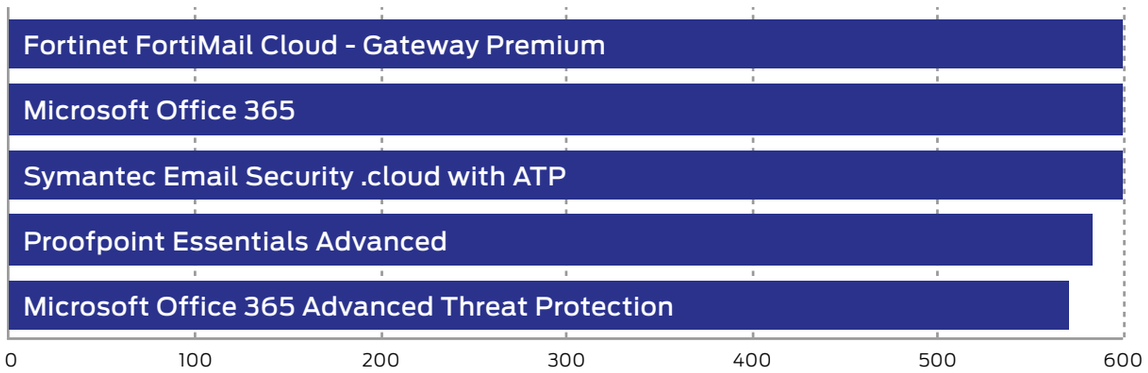
LEGITIMATE MESSAGE MANAGEMENT				
	Inbox	Quarantined (Admin)	Rejected	Junk Folder
Fortinet FortiMail Cloud - Gateway Premium	60	0	0	0
Microsoft Office 365	60	0	0	0
Microsoft Office 365 Advanced Threat Protection	58	0	0	2
Proofpoint Essentials Advanced	59	1	0	0
Symantec Email Security .cloud with ATP	60	0	0	0



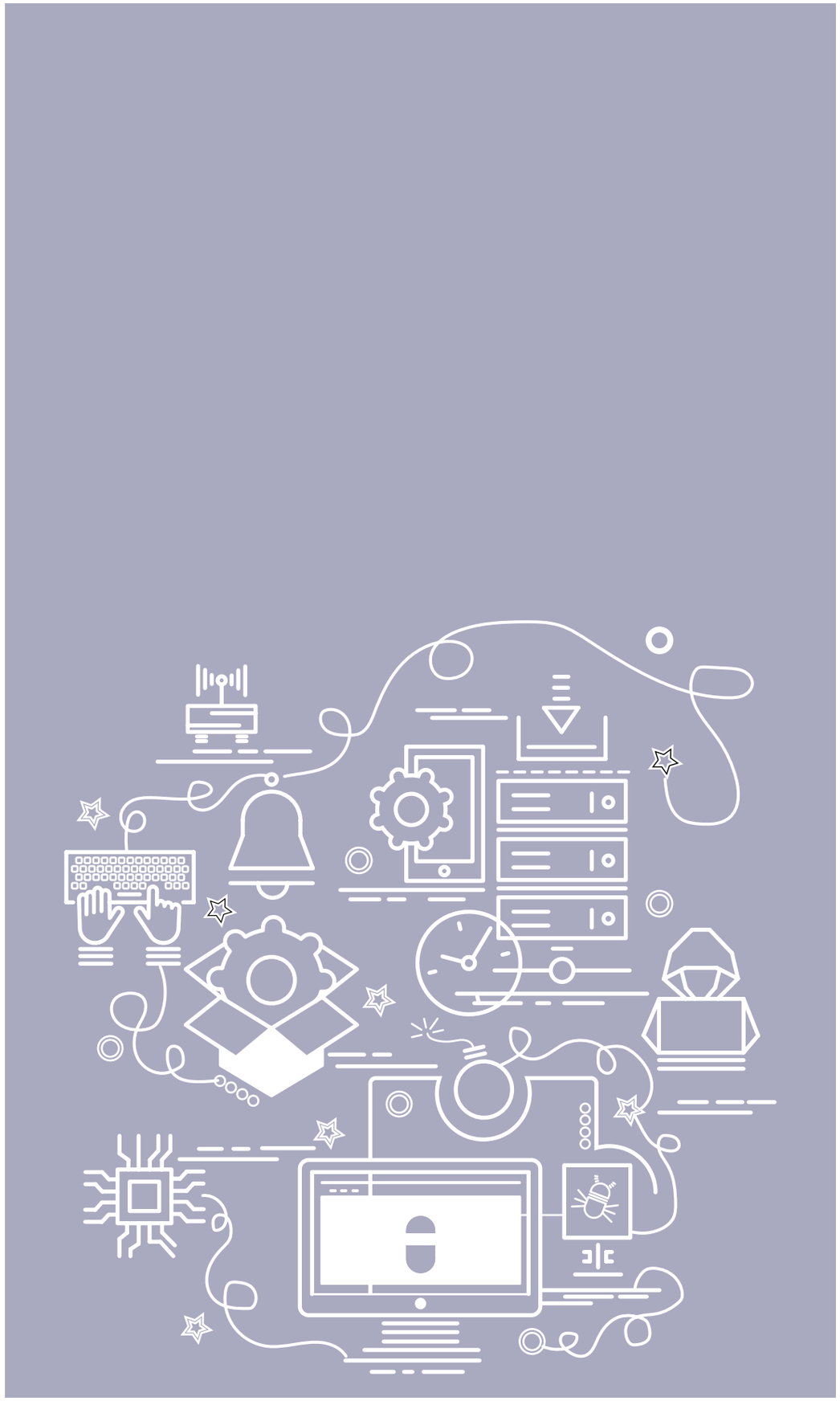
7. Legitimate Message Ratings

This graph shows how accurately the services handled legitimate email. The rating system is described in detail in ***2. Protection Ratings*** on page 8.

LEGITIMATE MESSAGE RATINGS		
	Legitimate Accuracy Rating	Legitimate Accuracy Rating (%)
Fortinet FortiMail Cloud - Gateway Premium	600	100%
Microsoft Office 365	600	100%
Symantec Email Security .cloud with ATP	600	100%
Proofpoint Essentials Advanced	582	97%
Microsoft Office 365 Advanced Threat Protection	570	95%



Legitimate Message Ratings give a weighted value to services based on how accurately they handle legitimate messages.



8. Conclusion

The results in this report show the combined protection levels of **Microsoft Office 365** and several 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 recommended an additional setting that renders quarantined emails non-recoverable, so users can see that they have been caught but cannot subsequently override the system and expose themselves to risk. In **Proofpoint's** own words, "**Proofpoint Essentials** offers customers the option to prevent Administrators from releasing quarantined messages. Although this is not a commonly recommended setting, as customers typically want Administrators to retain control over the release of quarantined messages, this setting was deployed for this test."

Symantec Email Security .cloud with ATP protected against all of the attacks with the exception of four commodity attacks, which were then caught by **Office 365** and placed into the Junk folder. All of the targeted threats, including social engineering, phishing and malware attacks were removed before users could encounter them. Its aggressive stance to attacks was not reflected in the way it handled legitimate emails, all of which made it through to the inbox.

Proofpoint's service was similarly effective with threat handling, although it achieved a slightly higher protection rating because it failed to stop only three attacks, while **Symantec** allowed four through. **Proofpoint Essentials Advanced** was more aggressive with legitimate email, though. It placed one message into quarantine which, as we've mentioned above, was not recoverable and so the penalty was greater than if a user or admin could have released the message to the inbox.

FortiMail stopped all but three of the targeted malware attacks, deleting all of the others well before the inbox stage. It also did extremely well with the public attacks, preventing all of them from coming without reach of the user. It was less effective against social engineering attacks than the other two leading services but only missed eight. It was completely accurate when handling legitimate messages.

Microsoft Office 365 in default mode, which is the least aggressive available, was completely accurate when handling legitimate email. It was also very effective at detecting the public threats, allowing only two 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 only deleted messages when they were well-known 'commodity' threats. All targeted attacks went either to the inbox or the Junk folder. With targeted malware all but one threats went to the inbox.

Microsoft Office 365 Advanced Threat Protection was more aggressive with legitimate messages, but only slightly. It condemned two of the 60 legitimate messages to the Junk folder but it didn't delete any of them. It prevented more targeted malware arriving in the user's hands (in either the inbox or Junk Folder) than **Office 365** without the **ATP** service. It also neutralised the malicious content of some messages sent to the Junk folder, making them completely safe. It was particularly strong in this area with the targeted phishing emails. It also managed to weed out seven extra social engineering threats that **Office 365** missed. The ATP add-on resulted in better protection and less threats being stored in the easily-accessible Junk folder.

Based on how effectively the services prevented public and targeted threats from reaching the user, the most effective were **Symantec Email Security .cloud with ATP** and **Proofpoint Essentials Advanced**. **Fortinet FortiMail Cloud - Gateway Premium** came close behind, also providing 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 between October and November 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**
Fortinet	FortiMail Cloud - Gateway Premium
Microsoft	Office 365
Microsoft	Office 365 Advanced Threat Protection
Proofpoint	Essentials Advanced
Symantec	Email Security .cloud with ATP

APPENDIX D: How we Tested

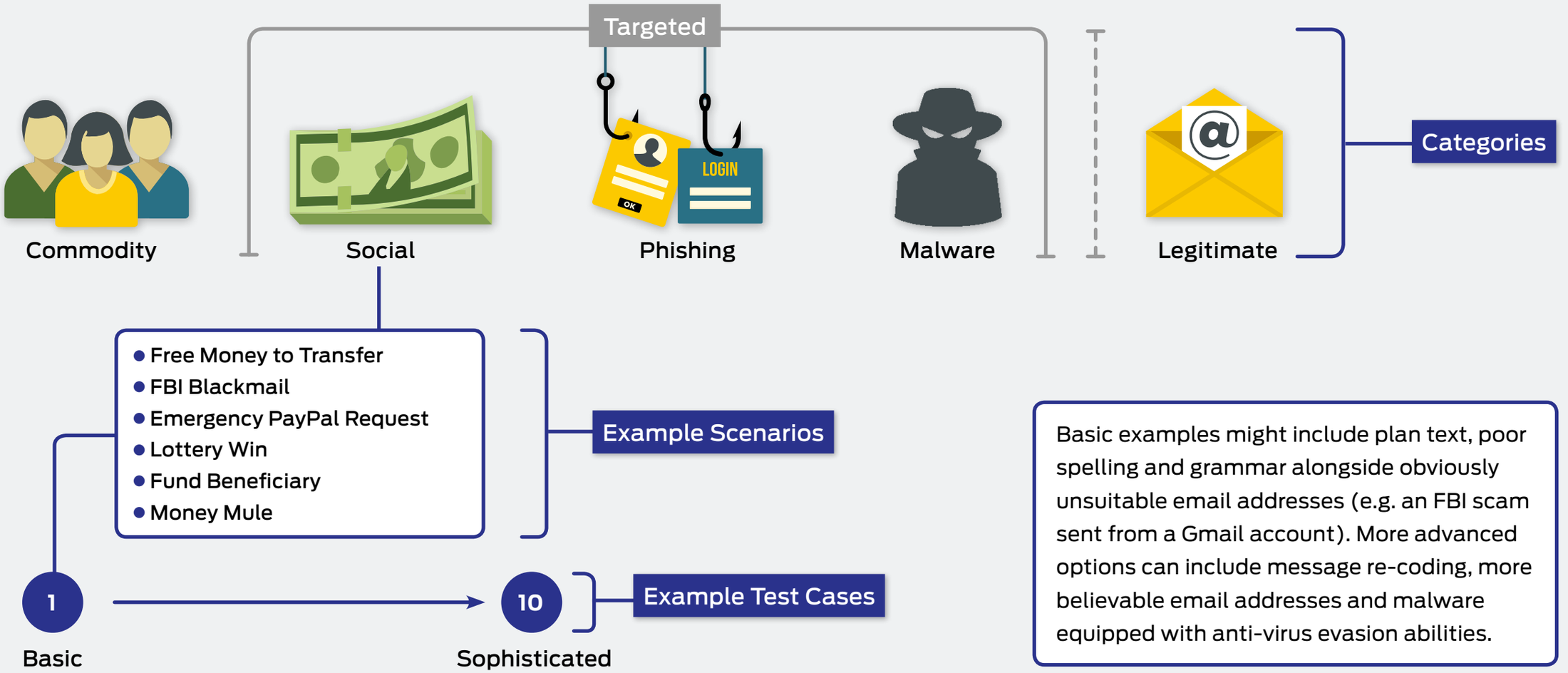
The common commodity threats were gathered from the wild and replayed through the email security services. Where possible data about the original attackers' IP addresses were provided to allow services that have reliable IP address reputation systems to use their threat intelligence during testing.

Legitimate messages were constructed in-house.

Targeted attacks comprise three distinct categories: Social Engineering; Phishing; and Malware. For each of these categories we created six main variations. In the example below you can see that the social engineering messages are formed into six groups (scenarios), including free money transfer, lottery win and law enforcement blackmail scams.

For each scenario we create 10 variants that range in sophistication from extremely basic to very advanced. The goal is to test how effective each email security service is when facing a range of different types of attacker, or at least a range of different attack approaches.

Test Case Structure



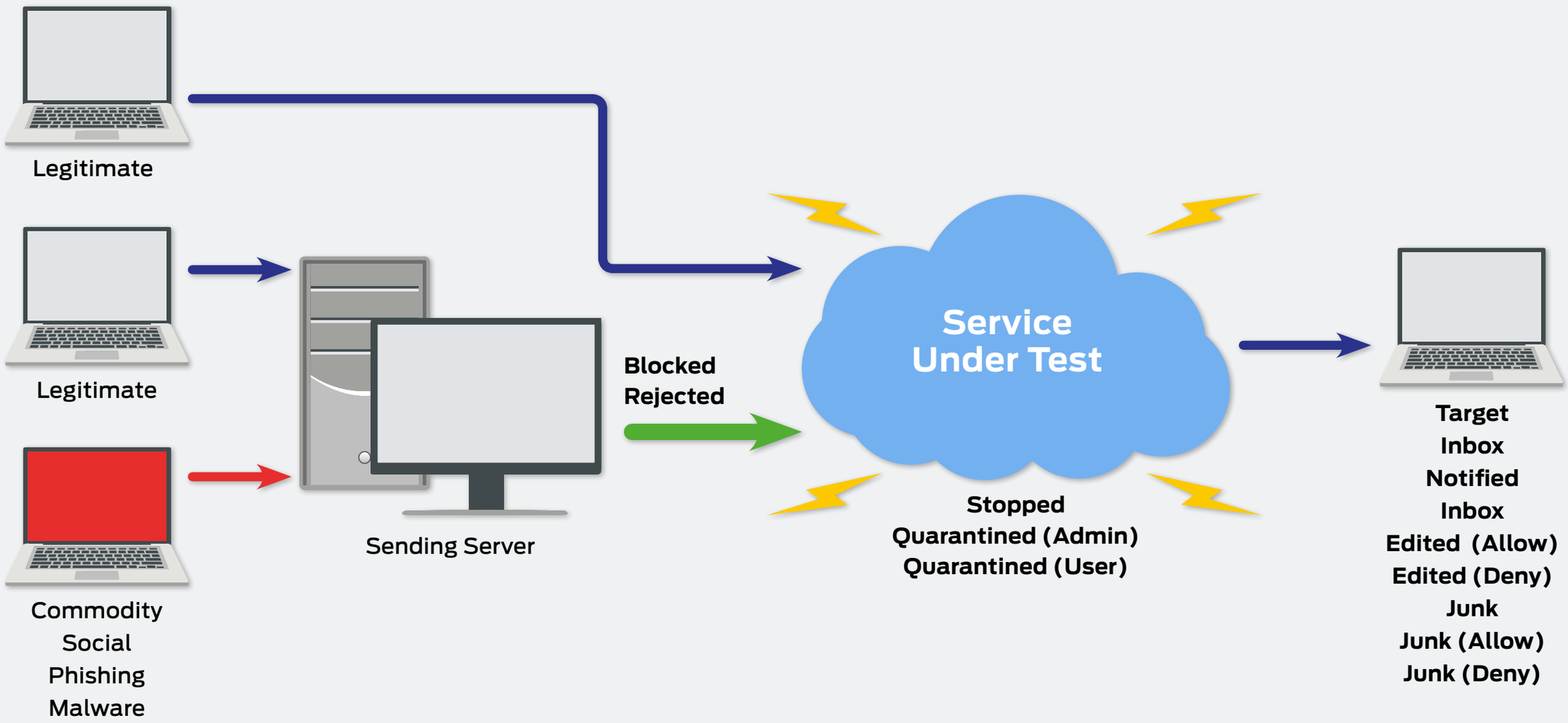
Basic examples might include plan text, poor spelling and grammar alongside obviously unsuitable email addresses (e.g. an FBI scam sent from a Gmail account). More advanced options can include message re-coding, more believable email addresses and malware equipped with anti-virus evasion abilities.

As the email messages, both good and bad, traverse the internet, the security services and the target's own infrastructure there are opportunities for detection and protection.

Bad messages might be prevented from entering the service under test, being blocked or otherwise rejected. Once within the service, the message might be detected and prevented from progressing further, or it might be placed into a quarantine from which either a user or administrator may release it.

Messages that have successfully run the gauntlet face possible detection by Office 365 or whichever email service is in use. Messages may end up in the inbox or quarantine, with or without changes such as removed or rewritten URLs, attachments and other elements.

Results and Scoring



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.