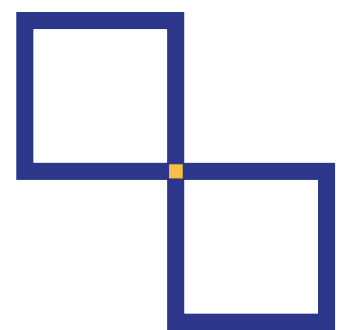




SE Labs

INTELLIGENCE-LED TESTING

EMAIL SECURITY SERVICES PROTECTION

JAN - MAR 2020



www.SELabs.uk



info@SELabs.uk



[@SELabsUK](https://twitter.com/SELabsUK)



www.facebook.com/selabsuk



blog.selabs.uk



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

Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Chief Technical Officer Stefan Dumitrascu

TESTING TEAM

Thomas Bean
 Solandra Brewster
 Dimitar Dobrev
 Liam Fisher
 Gia Gorbald
 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 SE Labs Ltd,
 55A High Street, Wimbledon, SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2013 certified and 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).

AMTSO Standard reference:
<https://tinyurl.com/essp2020>

© 2020 SE Labs Ltd

CONTENTS

Introduction	04
Email Security Services Protection Awards	05
Executive Summary	06
How we Tested	07
1. Threat Detection Results	10
2. Total Accuracy Ratings	11
3. Protection and Legitimate Handling Accuracy	12
4. Conclusion	15
Appendix A: Attack Details	16
Appendix B: Detailed Results	18
Appendix C: Terms Used	25
Appendix D: FAQs	26
Appendix E: Services Tested	26

Document version 1.0 Written: 16th March 2020



INTRODUCTION

Email security: Is it any good against hackers?

World's first in-depth, public test of security services vs. targeted attacks

This email security test report is the product of two years of advanced threat research. We have worked with the security companies themselves and with their customers. We have monitored what the bad guys have been doing and identified and replicated real-world email threats that affect everyone generally, and also specific types of businesses. There is no report like this anywhere in the public domain. We are extremely proud to present the results here.

As you scan the headlines, awards and data tables you may wonder why so many of the major players in the email security industry are absent. Over the last 24 months we've worked with most of them privately, but this is a new test and, frankly, they are worried about their results. It is to the massive credit of companies like Fortinet, Mimecast and Perception Point that they have enough confidence in their products to enter such a challenging test. And to be the first.

We will always welcome the participation of any vendor in the email security space but, as we move on with testing security products, please check in to see which companies are involved. Ask yourself

why certain companies continue to refuse to be tested. Do they have something to hide, or is the test just no good? To be fair, email security is in its infancy when compared to other computer security services. We expect services to improve over time as they face good independent testing. But these services are for sale now and you deserve to know which are the strongest.

We believe that this test is the best there's ever been in this space, but we don't expect you to just take us at our word. To add further credibility to our claims in this report we have submitted it to the Anti-Malware Testing Standards Organization, which assesses security tests for transparency. We won't know until after the test is published if it complies with the AMTSO testing Standard, but we have enough confidence in the integrity of ourselves and the testing methods that we're opening ourselves up to judgment. To verify its compliance please check the AMTSO reference link at the bottom of page three of this report or [here](#).

As with all of our reports, if you have any questions please contact us via our [website](#), [Twitter](#) or [Facebook](#).

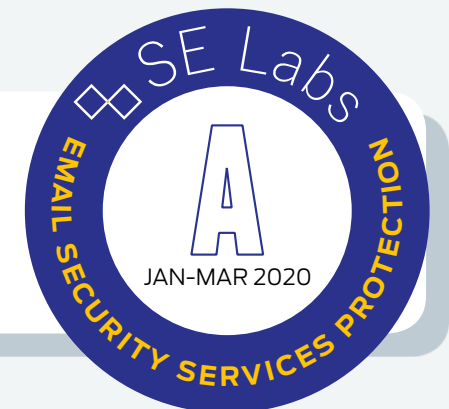
Email Security Services Protection Awards

The following products win SE Labs awards:

- **Perception-Point**
- **Fortinet FortiMail**
- **Mimecast**
Secure Email Gateway



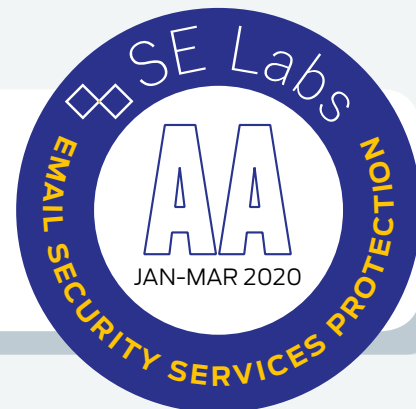
- **Google G Suite Enterprise**



- **Google G Suite Business**



- **Kaspersky Cloud**



- **Microsoft Office 365**
- **Microsoft Office 365**
Advanced Threat Protection



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 E: Services Tested** on page 26

EXECUTIVE SUMMARY				
Product	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)
Perception-Point	2,603	700	3,303	94%
Fortinet FortiMail	2,525	640	3,165	90%
Mimecast Secure Email Gateway	2,412	700	3,112	89%
Kaspersky Cloud	1,681	550	2,231	64%
Google G Suite Enterprise	956	505	1,461	42%
Google G Suite Business	825	535	1,360	39%
Microsoft Office 365	463	550	1,013	29%
Microsoft Office 365 Advanced Threat Protection	426	550	976	28%

Products highlighted in green were the most accurate, scoring 40 per cent or more for Total Accuracy. Those in orange scored between 20 to 40 per cent. Any products shown in red scored less than 20 per cent.

This test pitted a number of email security services against live targeted attacks that used the same or similar tactics to well-known groups operating over the last few years. Advanced malware and social engineering tactics were used to replicate nation-state-level attackers, as well as cyber criminals targeting individuals and the general public.

The services tested were standalone email security gateways and platforms, which are integrated email services that include security features.

Common 'commodity' threats were mostly detected. No product was able to detect and prevent all targeted threats.

- The highest overall detection rate was 96%.
- The lowest overall detection rate was 73%.
- False positives were surprisingly common, particularly with the email platforms.
- Legitimate message handling was generally successful, ranging from 72% to 100% accuracy.
- The Total Accuracy Ratings (see left) show how well each service handled threats and legitimate messages in a combined, weighted rating.

How We Tested

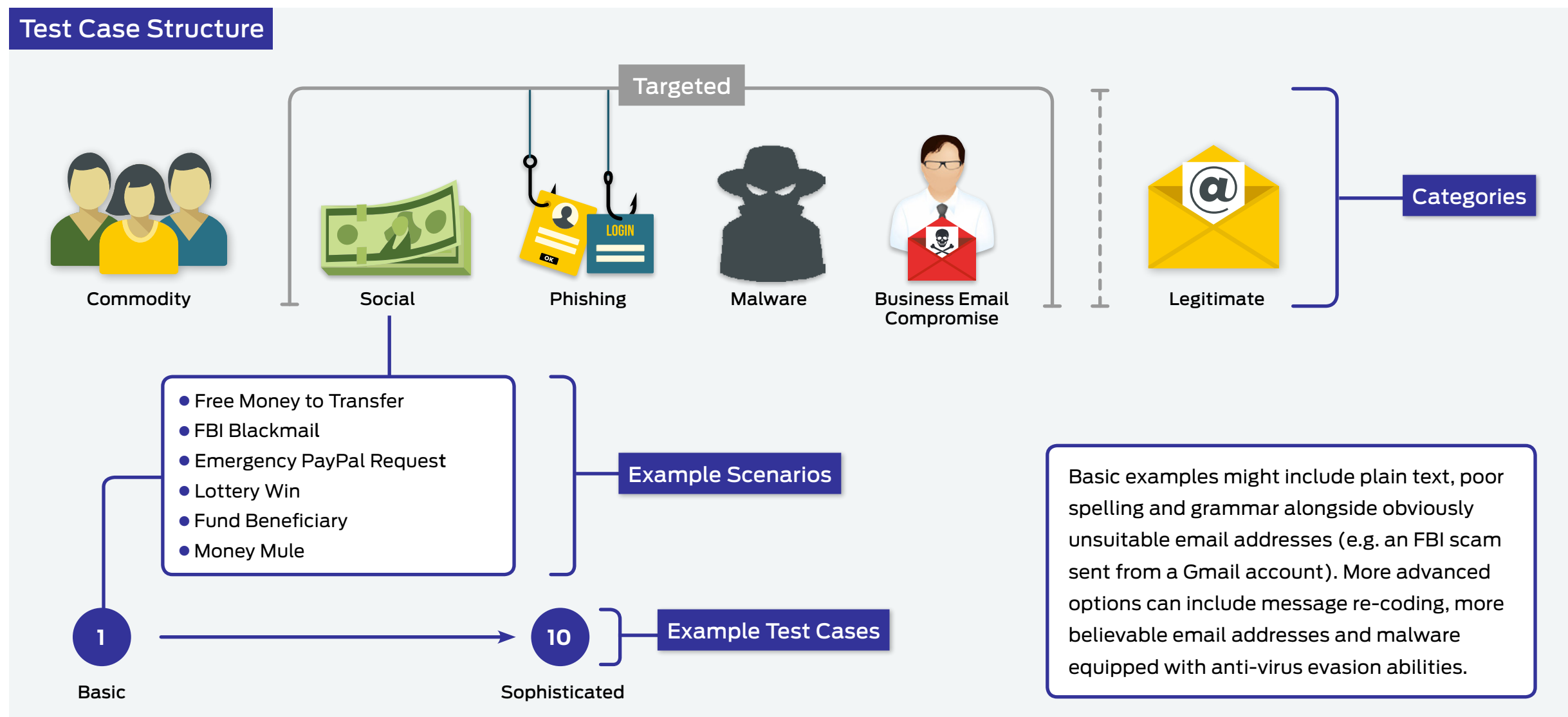
The common commodity threats were gathered from the wild and replayed through the email security services. Where possible, data about the original attackers' IP addresses were provided to allow services that have reliable IP address reputation systems to use their threat intelligence during testing.

Legitimate messages were constructed in-house.

Targeted attacks comprise four distinct categories: Social Engineering; Phishing; Malware and Business Email Compromise. For each of these

categories we created a number of main Test Case Structure 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 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.



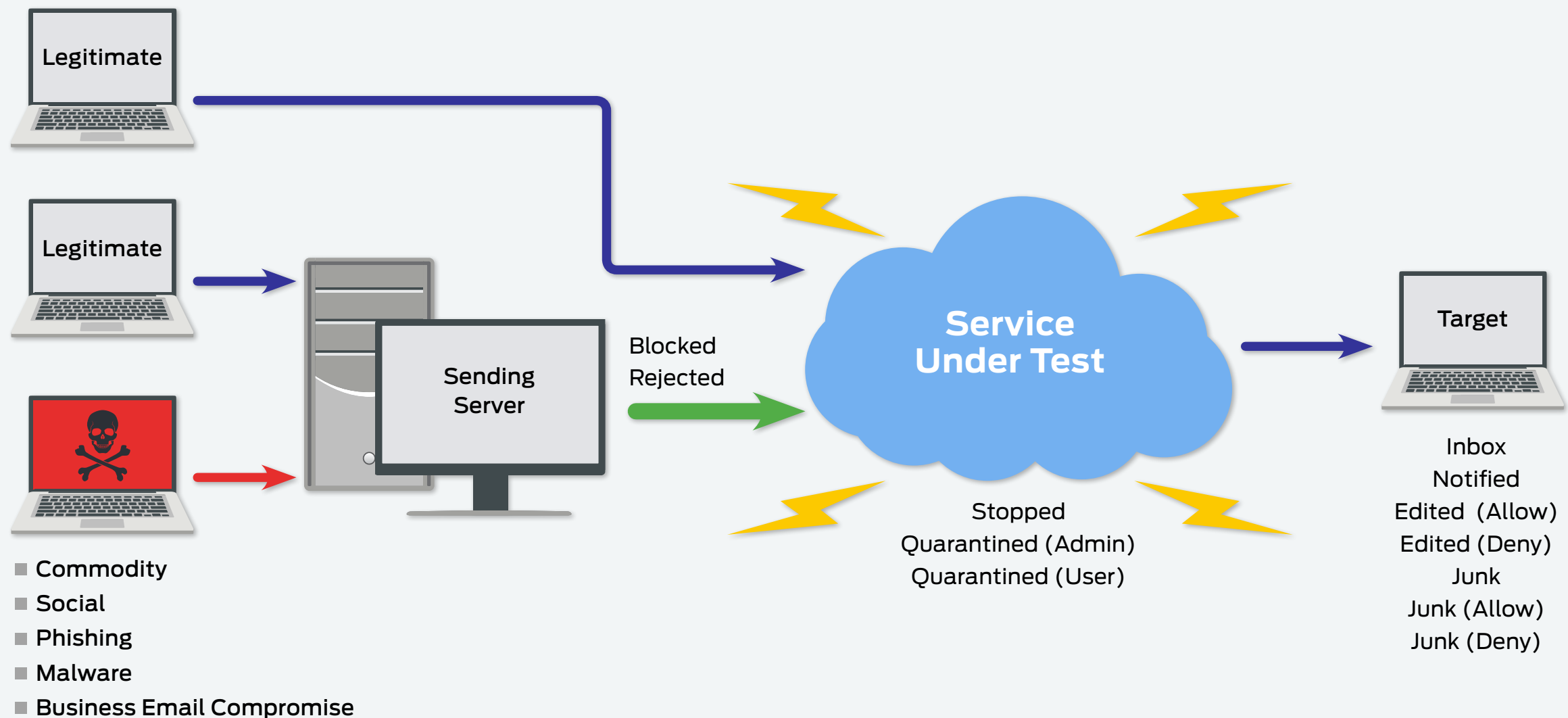
Email messages travel over the internet to their recipients. Before they reach the inbox they negotiate their way through various security services before reaching the target's own infrastructure. There are opportunities for detection and protection at different stages in this journey.

Bad messages might be prevented from entering the service under test, being blocked or otherwise rejected. Once within the service, the message might be

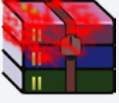
detected and prevented from progressing further, or it might be placed into a quarantine from which either a user or administrator may release it.

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.

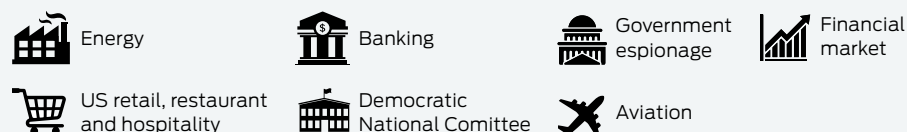
Results and Scoring



Attackers vs. Targets

Attacker/ APT Group	Method	Target	Details
Sandworm			Windows vulnerabilities via Office documents
FIN7			Documents containing hidden links to scripts
APT19			Documents containing hidden links to scripts
APT28			Microsoft Office macros
Dridex			Windows vulnerabilities via Office documents
APT33 (2019)			WinRAR exploit
APT33 (2017)			HTML application files
FIN4			Man-in-the-middle spear phishing

Key



When testing services against targeted attacks it is important to ensure that the attacks used are relevant. Anyone can run an attack randomly against someone else. It is the security vendor's challenge to identify common attack types and to protect against them. As testers, we need to generate threats that in some way relate to the real world.

All of the attacks used in this test are valid ways to compromise an organisation. Without any security in place, all would succeed in attacking the target. Outcomes would include systems infected with ransomware, remote access to networks and data theft.

But we didn't just sit down and brainstorm how we would attack different companies. Instead we used current threat intelligence to look at what the bad guys have been doing over the last few years and copied them quite closely. This way we can test the services' abilities to handle similar threats to those faced by global governments, financial institutions and national infrastructure.

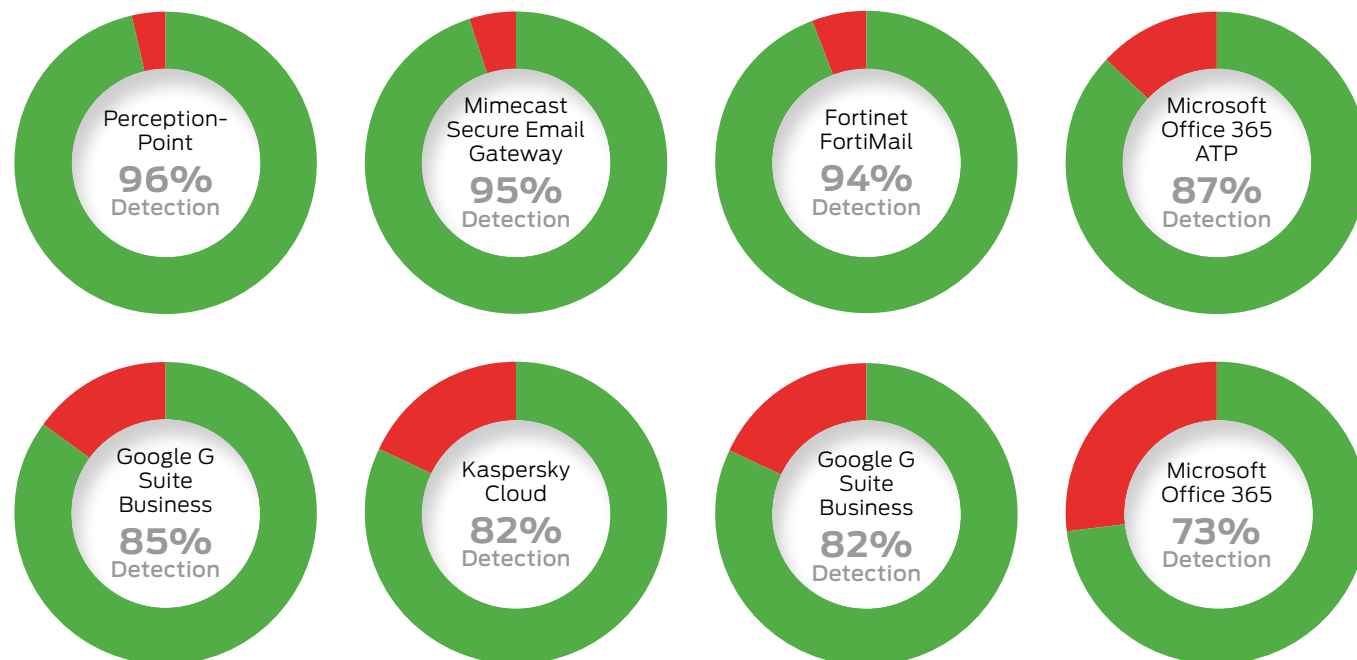
The graphic on this page shows a summary of the attack groups that inspired the targeted attacks used in this test. If a service was able to detect and protect against these then there's a good chance they are on track to blocking similar attacks in the real world. If they fail, then you might take their bold marketing claims about defeating hackers with a pinch of salt.

For more details about each APT group see [Appendix A: Attack Details](#) on page 16.

1. 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 for Microsoft, 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			
PRODUCT	Detection Rate	Misses	Detection Rate (%)
Perception-Point	270	10	96%
Mimecast Secure Email Gateway	266	14	95%
Fortinet FortiMail	264	16	94%
Microsoft Office 365 Advanced Threat Protection	244	36	87%
Google G Suite Enterprise	238	42	85%
Kaspersky Cloud	230	50	82%
Google G Suite Business	230	50	82%
Microsoft Office 365	205	75	73%



Detection rates are a useful but unsubtle way to compare services

2. 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 table.

The graphic 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.

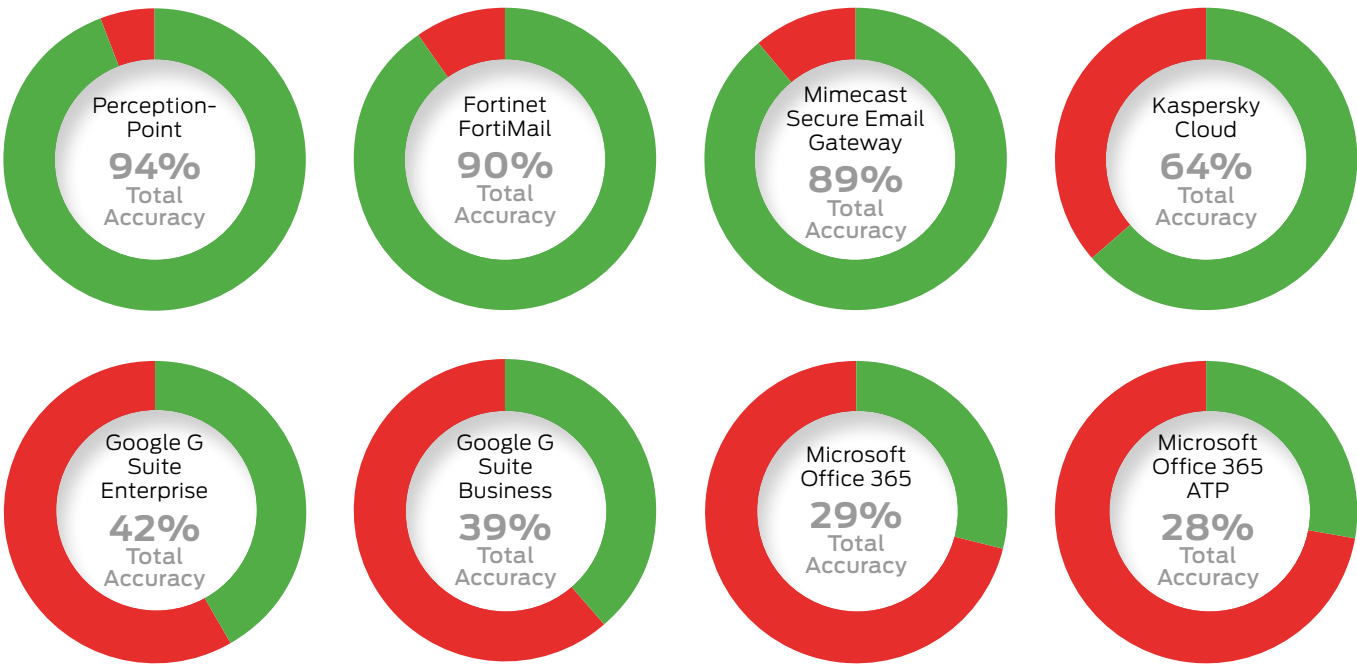
Not all protection measures, or detections for that matter, are equal. A service might completely delete an incoming malicious email and never allow the intended recipient to see (and subsequently interact with) it. Services may condemn suspicious messages to a 'quarantine' area if it lacks the utter 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

TOTAL ACCURACY RATINGS		
PRODUCT	Total Accuracy Rating	Total Accuracy Rating (%)
Perception-Point	3,303	94%
Fortinet FortiMail	3,165	90%
Mimecast Secure Email Gateway	3,112	89%
Kaspersky Cloud	2,231	64%
Google G Suite Enterprise	1,461	42%
Google G Suite Business	1,360	39%
Microsoft Office 365	1,013	29%
Microsoft Office 365 Advanced Threat Protection	976	28%

Total Accuracy Ratings combine protection and false positives.



"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.

3. Protection and Legitimate Handling Accuracy

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 them. 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 folder.

Inbox (-10 for threats; +10 for legitimate)

Malicious messages that arrive in the user's inbox

SCORING DIFFERENT OUTCOMES		
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

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 =

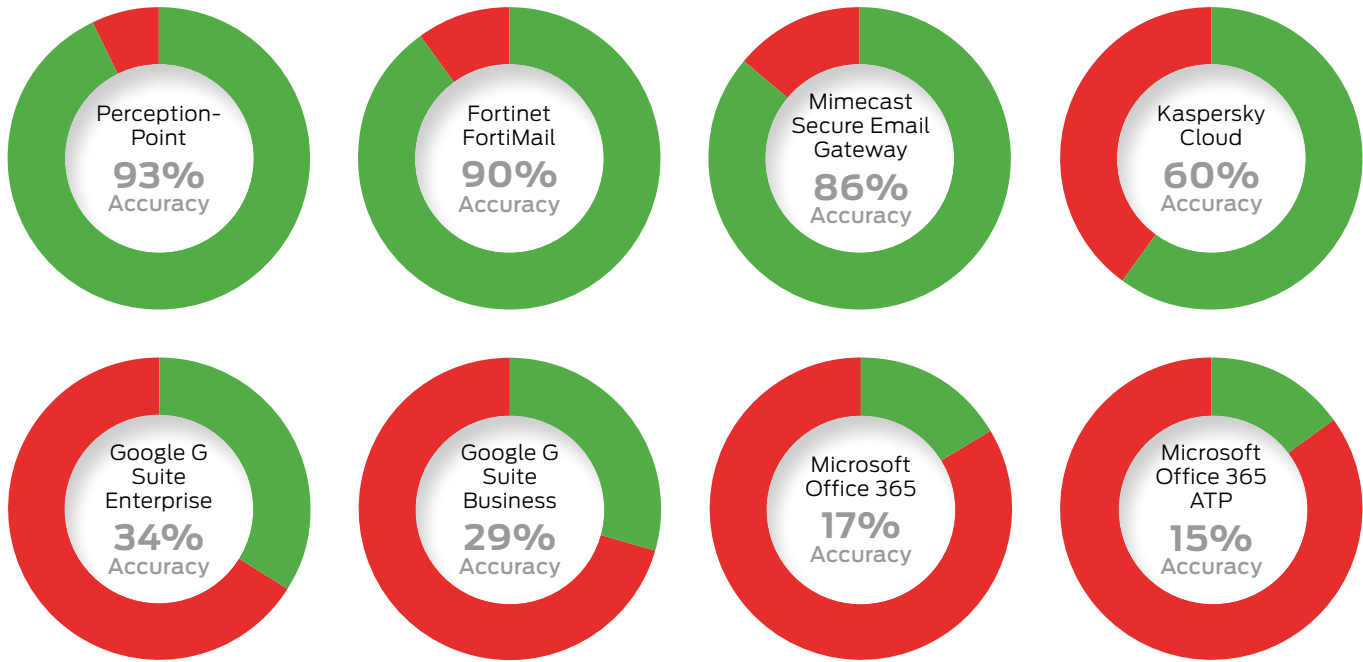
(10x number of Stopped etc.) +
 (6-8x number of Quarantined) +
 (5x number of Junk) +
 (-10x number of Inbox)
 etc.

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.

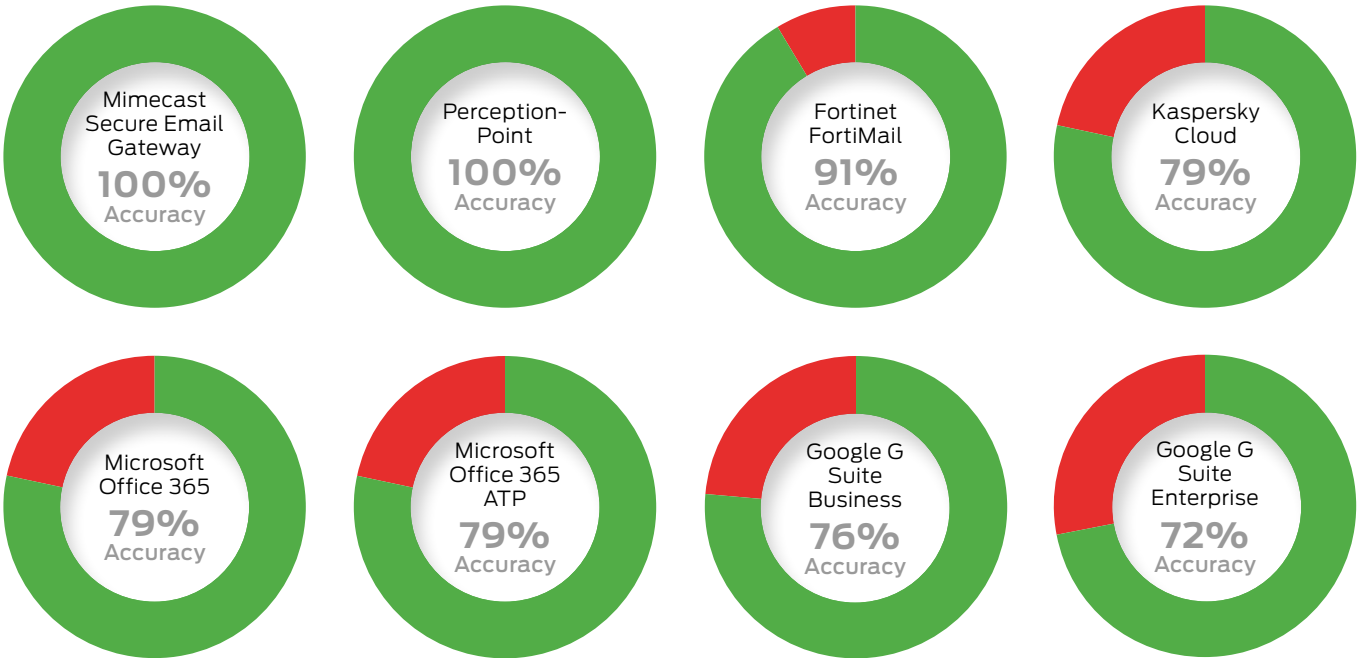
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in quarantine, or for a malware threat to end up in the inbox. You can use the raw data from this report (See **Appendix B: Detailed Results on page 18**) to roll your own set of personalised ratings.

PROTECTION ACCURACY RATINGS		
PRODUCT	Protection Accuracy Rating	Protection Accuracy Rating (%)
Perception-Point	2,603	93%
Fortinet FortiMail	2,525	90%
Mimecast Secure Email Gateway	2,412	86%
Kaspersky Cloud	1,681	60%
Google G Suite Enterprise	956	34%
Google G Suite Business	825	29%
Microsoft Office 365	463	17%
Microsoft Office 365 Advanced Threat Protection	426	15%



This table shows how accurately the services handled legitimate email. The rating system is described in detail in 3. Protection and Legitimate Handling Accuracy on page 12.

LEGITIMACY ACCURACY RATING		
PRODUCT	Legitimate Accuracy Rating	Legitimate Accuracy Rating (%)
Mimecast Secure Email Gateway	700	100%
Perception-Point	700	100%
Fortinet FortiMail	640	91%
Kaspersky Cloud	550	79%
Microsoft Office 365	550	79%
Microsoft Office 365 Advanced Threat Protection	550	79%
Google G Suite Business	535	76%
Google G Suite Enterprise	505	72%



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

4. Conclusion

This test pitted a number of email security services against live targeted attacks that used the same or similar tactics to well-known groups operating over the last few years. While malware was often involved, there was far more to the attacks used than just sending a ransomware file as an attachment. Advanced malware and social engineering tactics were used to replicate nation-state-level attackers, as well as cyber criminals targeting individuals and the general public.

In other words, we didn't just create a list of brand-new ways to attack targets over email. We were inspired by attack groups whose behaviour has been monitored, analysed and published.

The services that we tested can be roughly organised into two groups: email security gateways, such as Mimecast Secure Email Gateway and Fortinet FortiMail Cloud – Gateway Premium; and email platforms that include email security features, such as Microsoft Office 365 and Google G Suite. All services claim to protect their users from threats and our goal was to test that claim.

Before we get to the juicy stuff it's worth remembering that email security products are supposed to let real email through, while filtering out the dangerous messages. To ensure that the products weren't configured to block every

incoming email, we also tested with legitimate messages. We expected every service to allow all of these into the inbox. Additionally, we tested with some very well-known threats that affect the general public on an ongoing and non-discriminatory basis. In other words, all of the companies behind these services should be aware of them and detect them.

This report contains results for all of these test cases: targeted attacks; commodity threats; and legitimate messages. We have a weighted scoring system that generates one easy-to-understand Total Accuracy Rating, which takes all of the results into account. A service that blocks every message will score well in terms of protection but face strong penalties for blocking the useful emails. Similarly, a service that lets every message through will be penalised for allowing threats through.

The strongest services overall were from Perception Point, Fortinet and Mimecast. All three achieved high enough ratings to win AAA awards. They managed this by correctly detecting and handling threats, while allowing the vast majority of the legitimate messages into the inboxes. If you want more precise details about how they handled targeted social engineering, phishing and malware attacks please see **Appendix B: Detailed Results** on page 18.



APPENDICES

Appendix A: Attack Details

Targeted Attack Types

Attack Group: FIN4

Method of Attack: Man-in-the-middle spear phishing

Targets: Financial markets

This group stole clean Office documents from the target and edited them, embedding malicious macros. By using correctly formatted documents containing real information, stolen from compromised accounts, the attackers increased the likelihood that recipients would be tricked into opening the documents and allowing their own systems to be compromised.

References:

<https://attack.mitre.org/groups/G0085/>

Attack Group: FIN7

Method of Attack: Documents containing hidden links to scripts

Targets: Retail and hospitality industries

FIN7 used spear phishing attacks targeted at retail, restaurant and hospitality businesses. What appeared to be customer complaints, CVs (resumes) and food orders sent in Word and RTF formatted documents, were actually attacks that hid malicious (VBS) code behind hidden links.

References:

<https://attack.mitre.org/groups/G0046/>

Attack Group: Dridex malware campaign

Method of Attack: Windows vulnerabilities via Office documents

Targets: Banking

This attack campaign involved sending invoice requests to finance departments. The messages contained malicious documents that prompted the recipient to update the document with data from other linked files. However, user interaction was not required, and the attack would initiate regardless.

References:

<https://attack.mitre.org/software/S0384/>

<https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day>

Attack Group: Sandworm

Method of Attack: Windows vulnerabilities via Office documents

Targets: Energy industries

In late 2015 a group known as the Sandworm Team made use of a zero-day vulnerability to cause a widespread power outage in Ukraine. This threat actor is also known as Voodoo Bear and BlackEnergy APT Group.

References:

<https://attack.mitre.org/groups/G0034/>

Attack Group: APT28

Method of Attack: Microsoft Office macros

Targets: Government

Macro-based attacks are a popular choice as a starting point of a target attack. There is a low barrier to entry and a wide distribution of vulnerable targets. Infamous campaigns conducted by APT28, and associated groups Fancy Bear and Sednit, usually start with spear-phishing email messages designed to convince users to open specially crafted, attached Microsoft Office documents that lead to further compromise of their systems.

References:

<https://attack.mitre.org/groups/G0007/>

Attack Group: APT19

Method of Attack: Documents containing hidden links to scripts

Targets: Defence; financial markets; education; and legal services

Using similar techniques to those outlined in the description for FIN7 (above), the APT19 attack group sent spear phishing emails with hidden links to malicious code. While technically similar, the group focussed on different types of target.

References:

<https://attack.mitre.org/groups/G0073/>

Attack Group: APT33 (2017)

Method of Attack: HTML application files

Targets: Aviation

In 2017 this group sent spear phishing emails to employees in the aviation industry. The email messages were supposedly related to recruitment but contained links to malicious HTML application (.hta) files. These .hta files contained job descriptions and links to real recruitment advertisements, as well as links to malware.

References:

<https://attack.mitre.org/groups/G0064/>

Attack Group: APT33 (2019)

Method of Attack: WinRAR exploit

Targets: Government

Attacks in February 2019 involved sending spear phishing emails with malicious WinRAR file attachments. The group focused on Saudi Arabia and the United States, aiming to attack supply chains involved in government and related industries including research, chemical, engineering and manufacturing.

References:

<https://attack.mitre.org/groups/G0064/>

Commodity Attack Types

The main categories of the commodity attacks used represent very common types of approach to engaging with a target over email. These are by sending malware; trying to socially engineer a victim through persuasion to do something (like send money); and phishing, which is an attempt to trick the user into sending important information like account details or passwords.

In this test we attached all of the malware samples to the emails. For social engineering test cases we tried to trick the target into sending money for services that will never be delivered, such as fake lottery wins (Advanced Fee), as well as blackmail attempts (Sextortion), promises of sexual relationships (Fake Love) and enticement to cyber criminal enterprises (Money Mule).

Phishing attacks included links to fake websites purporting to be well-known banks, social media sites etc. (Links), and similar log-in forms embedded in the emails (Attachment).

Category	Sub-category	Totals
Malware	Attachment	15
Social	Advanced Fee	43
	Fake Love	2
	Sextortion	3
	Money Mule	2
Phishing	Links	4
	Attachment	1



Appendix B: Detailed Results

The following tables show how each service handled different types of targeted attack. The table at the end of the series also summarises how they handled different categories of commodity threats.

There are four main categories of targeted attack used in this test:

- Social Engineering
- Phishing
- Malware
- Business Email Compromise

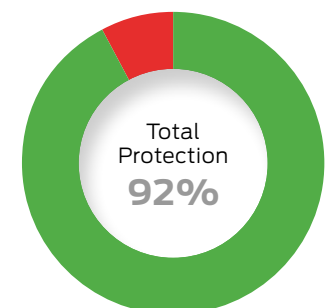
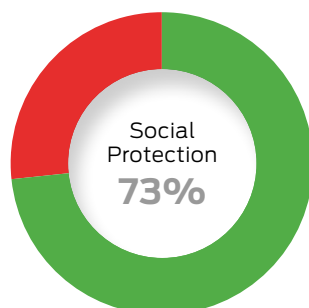
Each service has a number of options when handling such threats. The tables show how each service handled each category.

For example, you can see how many social engineering samples made it through to the inbox; how many were sent to the Junk folder; and how many were prevented from coming anywhere near the user - Stopped, rejected or Edited (deny) are common options.

Not every possible option needs to be taken by a service under test, so the tables show only those outcomes that occurred.

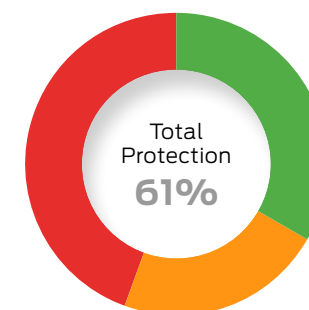
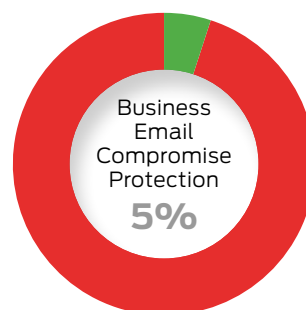
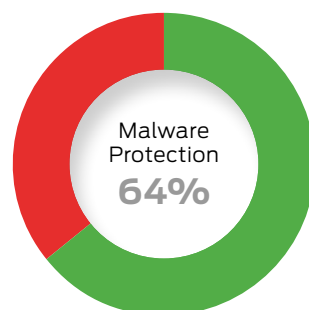
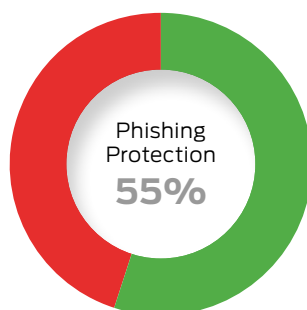
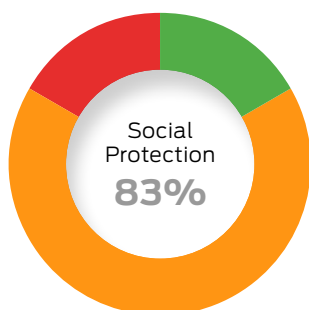
Targeted Attack Details

Fortinet FortiMail								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	43	1	0	0	0	1	0	15
Phishing	43	5	3	9	0	0	0	0
Malware	65	0	5	0	0	0	0	0
Business Email Compromise	20	0	0	0	0	0	0	0
TOTAL	171	6	8	9	0	1	0	15

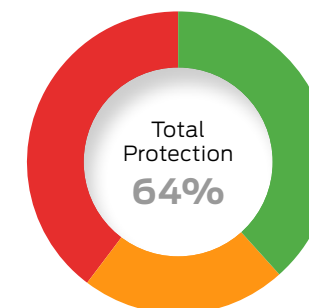
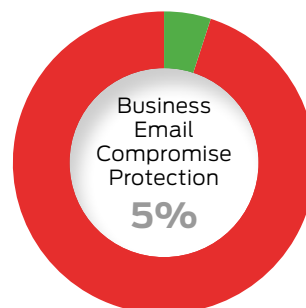
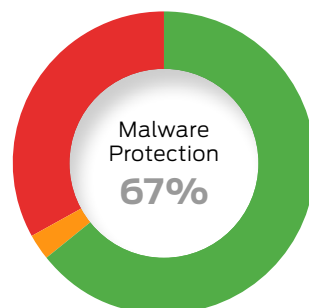
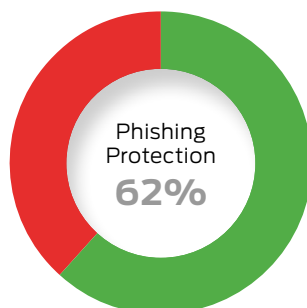
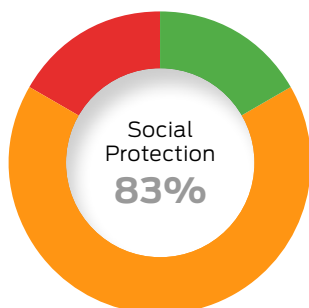


Google G Suite Business

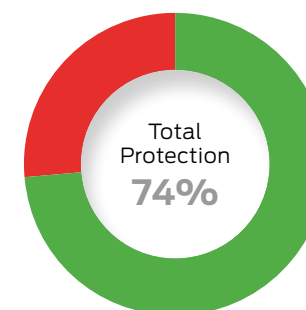
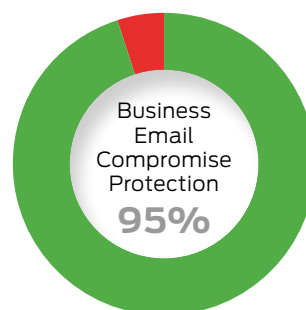
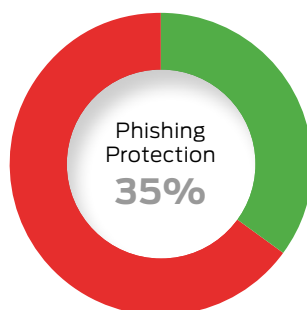
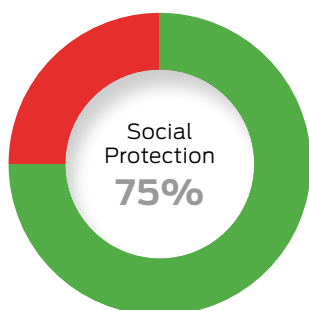
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	10	0	0	0	40	10	0	0
Phishing	9	0	0	24	0	6	0	21
Malware	0	45	0	0	0	15	0	10
Business Email Compromise	1	0	0	0	0	19	0	0
TOTAL	20	45	0	24	40	50	0	31

**Google G Suite Enterprise**

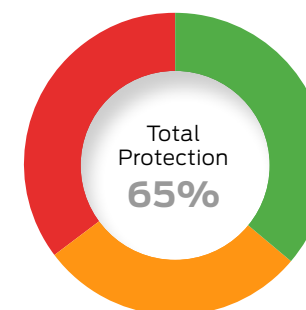
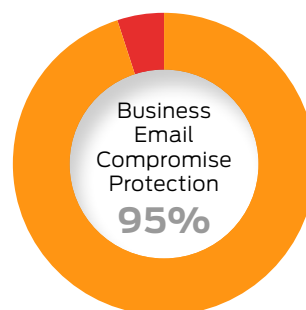
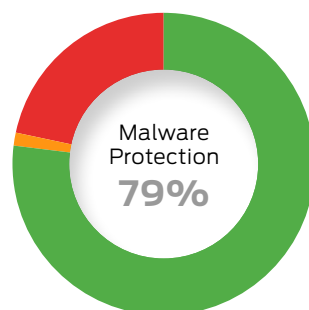
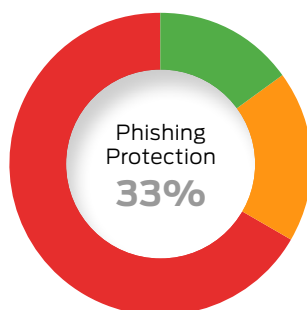
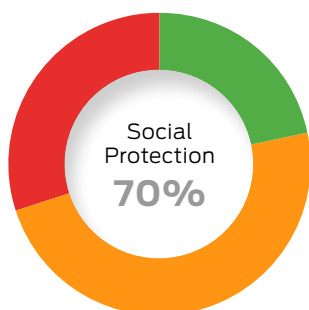
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	10	0	0	0	40	10	0	0
Phishing	9	0	0	28	0	0	0	23
Malware	0	45	0	0	2	13	0	10
Business Email Compromise	1	0	0	0	0	19	0	0
TOTAL	20	45	0	28	42	42	0	33



Kaspersky Cloud								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	12	0	1	32	0	14	0	1
Phishing	9	0	0	12	0	35	0	4
Malware	70	0	0	0	0	0	0	0
Business Email Compromise	0	0	0	19	0	0	0	1
TOTAL	91	0	1	63	0	49	0	6

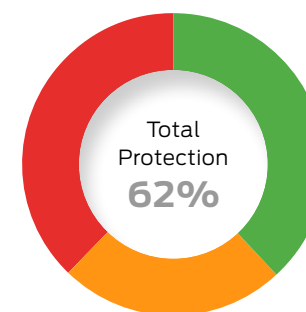
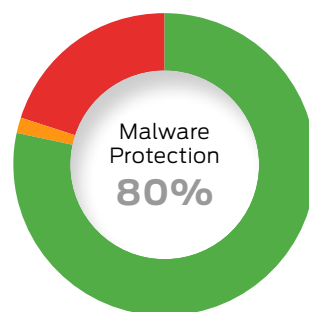
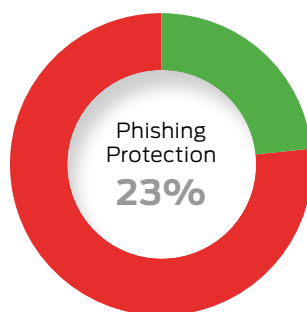
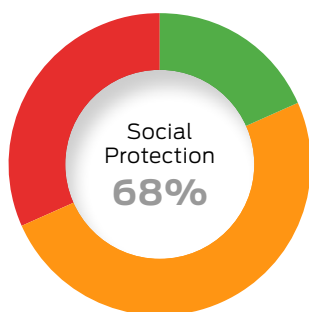


Microsoft Office 365								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	13	0	0	0	29	18	0	0
Phishing	9	0	0	0	11	39	0	1
Malware	54	0	0	0	1	15	0	0
Business Email Compromise	0	0	0	0	19	1	0	0
TOTAL	76	0	0	0	60	73	0	1



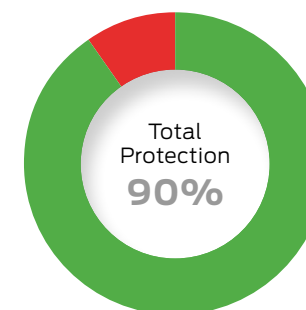
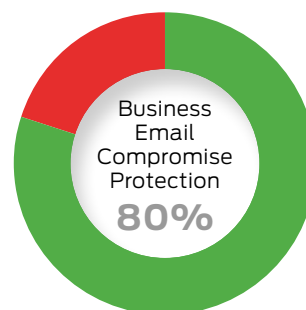
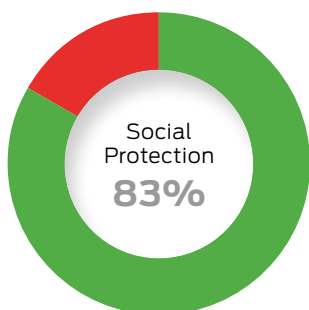
Microsoft Office 365 Advanced Threat Protection

	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	11	0	0	0	30	19	0	0
Phishing	10	0	3	1	0	1	34	11
Malware	47	1	7	0	1	14	0	0
Business Email Compromise	0	0	0	0	20	0	0	0
TOTAL	68	1	10	1	51	34	34	11

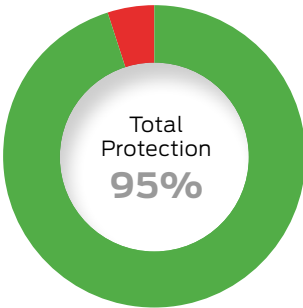
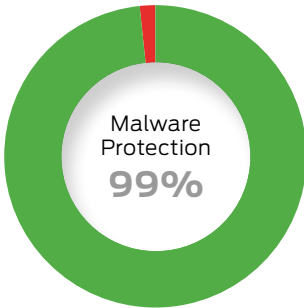
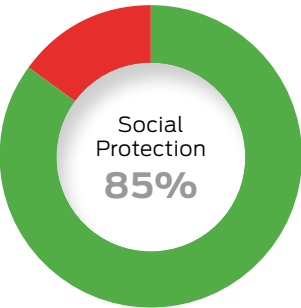


Mimecast Secure Email Gateway

	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	11	39	0	0	0	8	0	2
Phishing	9	36	6	3	0	0	6	0
Malware	3	58	9	0	0	0	0	0
Business Email Compromise	0	16	0	0	0	2	0	2
TOTAL	23	149	15	3	0	10	6	4

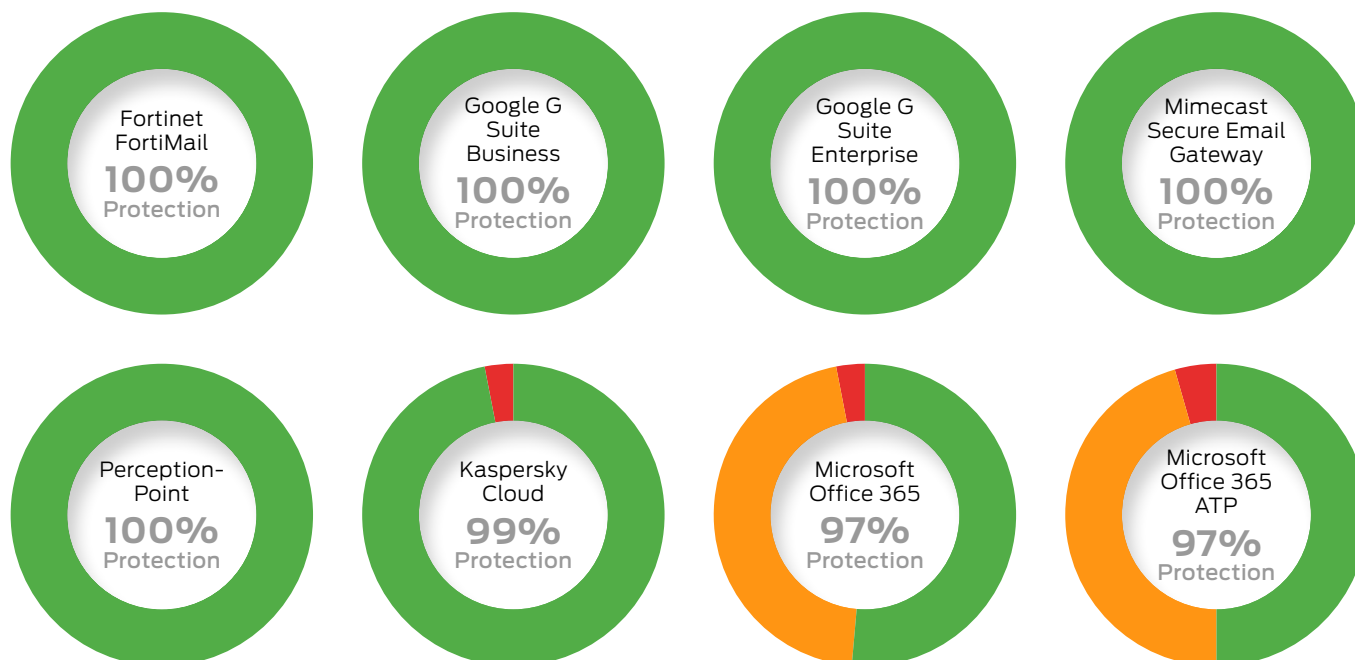


Perception-Point								
	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Social	51	0	0	0	0	9	0	0
Phishing	60	0	0	0	0	0	0	0
Malware	69	0	0	0	0	0	0	1
Business Email Compromise	20	0	0	0	0	0	0	0
TOTAL	200	0	0	0	0	9	0	1



Commodity Attack Details

Commodity Attack Details								
PRODUCT	Stopped	Rejected	Edited (deny)	Junk (deny)	Junk Folder	Inbox	Edited (allow)	Junk (allow)
Fortinet FortiMail	40	30	0	0	0	0	0	0
Google G Suite Business	10	60	0	0	0	0	0	0
Google G Suite Enterprise	10	60	0	0	0	0	0	0
Mimecast Secure Email Gateway	3	67	0	0	0	0	0	0
Perception-Point	70	0	0	0	0	0	0	0
Kaspersky Cloud	35	0	0	33	0	1	0	1
Microsoft Office 365	36	0	0	0	32	2	0	0
Microsoft Office 365 Advanced Threat Protection	35	0	0	0	32	2	0	1



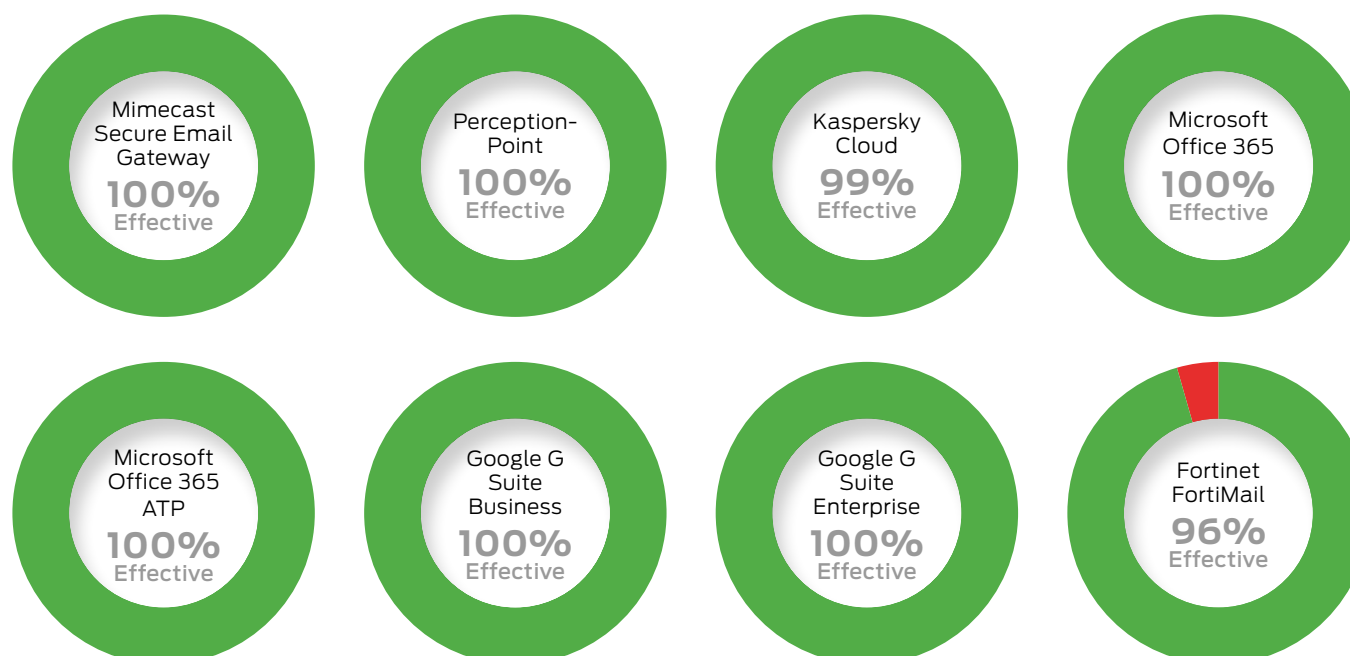
Legitimate Message Details

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 DETAILS			
Product	Inbox	Junk Folder	Stopped
Mimecast Secure Email Gateway	70	0	0
Perception-Point	70	0	0
Kaspersky Cloud	60	10	0
Microsoft Office 365	60	10	0
Microsoft Office 365 Advanced Threat Protection	60	10	0
Google G Suite Business	59	11	0
Google G Suite Enterprise	57	13	0
Fortinet FortiMail	67	0	3



Appendix C: Terms Used

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.

■ **Edited (deny)** The service delivered the message but altered it to remove malicious content.

■ **Junk (deny)** The service modified the message, which was sent to the target Junk folder. The malicious content was removed.

■ **Blocked** For some reason, other than the involvement of the tested service, the message was prevented from arriving.

■ **Quarantined (admin)** The service prevented the threat from being delivered and kept a copy of it, which could be recovered by the administrator only.

■ **Quarantine (user)** The service prevented the threat from being delivered and kept a copy of it, which could be recovered by the user.

■ **Junk Folder** The message was delivered to the user's Junk folder by the email service provider (e.g. Microsoft Office 365; Google G Suite Business) or by another integrated service.

■ **Junk (allow)** The service modified the message, which was sent to the target Junk folder, but didn't remove the malicious content.

■ **Inbox** The service failed to detect or protect against the threat.

■ **Edited (allow)** The service modified the message, which was sent to the target inbox, but didn't remove the malicious content.



Appendix D: 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 3rd and 17th of February 2020.
- 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 E: 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
Google	G Suite Business
Google	G Suite Enterprise
Kaspersky	Cloud
Microsoft	Office 365
Microsoft	Office 365 with Advanced Threat Protection
Mimecast	Secure Email Gateway
Perception-Point	Perception-Point

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.

