SE Labs

INTELLIGENCE-LED TESTING

ESS PROTECTION

Email Security Services

Microsoft Defender for Office 365

May 2024

SE LABS ® tested **Microsoft Defender for Office 365** against 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 service was at detecting and/or protecting against those threats in real time and shortly after the attacks took place.

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

Testing Team
Nikki Albesa
Thomas Bean
Solandra Brewster
Jarred Earlington
Gia Gorbold
Anila Johny
Erica Marotta
Luca Menegazzo
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Georgios Sakatzidis
Dimitrios Tsarouchas
Stephen Withey

Publication and Marketing
Colin Mackleworth
Sara Claridge
Janice Sheridan

IT Support
Danny King-Smith
Chris Short

Website selabs.uk
Email info@SELabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog blog.selabs.uk
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 Initiative (MVI);
the Anti-Malware Testing Standards Organization (AMTSO);
the Association of anti Virus Asia Researchers (AVAR);
and NetSecOPEN.

Contents

Document version 1.0 Written 6th May 2024.
1.01 Edited 12th September 2024 Text correction to the Introduction and Conclusion.

Introduction

Email Security Is Essential

Failure to use it is irresponsible

Email is one of the most common ways that threats will hit an organisation. It's the first stage in a series of unpleasant, expensive events that leads to data theft, data destruction and business cessation. Email is one of a very few standard ways that hackers start their attacks.

Classic examples of email threats include phishing emails, designed to steal important information that aid deeper attacks. Emails can contain links to dangerous websites that can trick users into handing over critical information or may even directly attack the user's computer. Attached documents may contain nasty surprises, such as backdoors that give attackers access to the business' network. Access means theft and destruction (e.g. ransomware).

If the email security service you use can stop most of that, it massively reduces the risk from hacking. Not using one is, frankly, irresponsible.

You cannot just plug in email security or rely on the security features provided by your email platform, though. Configuration is king. Given that most businesses in the UK and USA don't have a cyber security plan, it's likely that many Office 365 users have not changed their email security settings from the default.

In this report we used Microsoft's best practice configuration, rather than the default.

The threats in this test include ransomware and backdoors pushed through email, using a variety of advanced attack methods including exploits hosted on websites and within seemingly innocent documents such as PDFs. All of these attacks replicate the real-world behaviour of previously and currently active attack groups.

In this report, we emulate the behaviour of each of these attack groups to see how well-known email security solutions protect against these significant threats. For more details about the attack groups see **Attackers vs. Targets** on page 8 and **Appendix A: Attack Details** on page 13.

As with all of our reports, if you have any questions, please contact us via our **website** and **LinkedIn**. Our **newsletter** is an excellent source of updates, too.

Executive Summary

This test examined the effectiveness of **Microsoft Defender for Office 365** against a wide range of threats that target enterprise and small business through email.

SE Labs used advanced targeted attack techniques, as seen in devastating real-world attacks, to assess how well these services handle email cyber threats. Legitimate messages were also sent through the services to ensure that security settings were balanced with reasonable usability.

Microsoft Defender for Office 365 detected malicious email and prevented most of them from reaching the end-user's Inbox. Most of the malicious emails ended up in Quarantine where it could only be recovered by an administrator. The product was especially effective against phishing emails and malware attacks, achieving 100% protection against these types of threats.

It achieved a protection accuracy rating of 85% because it missed some email that employed social engineering and business compromise techniques.

In contrast, **Microsoft Defender for Office 365** allowed the end-user to access almost all legitimate email in his Inbox.

Microsoft Defender for Office 365 achieved 87% total accuracy and was therefore awarded with an AAA rating.

Executive Summary

Product Tested	Protection Accuracy Rating	Legitimate Accuracy Rating	Total Accuracy Rating	Total Accuracy Rating (%)
Microsoft Defender for Office 365	4,100	1,040	5,140	87%

Products highlighted in green were the most accurate, scoring 40 per cent or more for Total Accuracy. Those in orange scored less than 40 but 30 or more. Products shown in red scored less than 30 per cent.

For exact percentages, see **2. Total Accuracy Ratings** on page 9.

Email Security Services Protection Award

The following product wins the SE Labs award:

Microsoft Defender for Office 365

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.

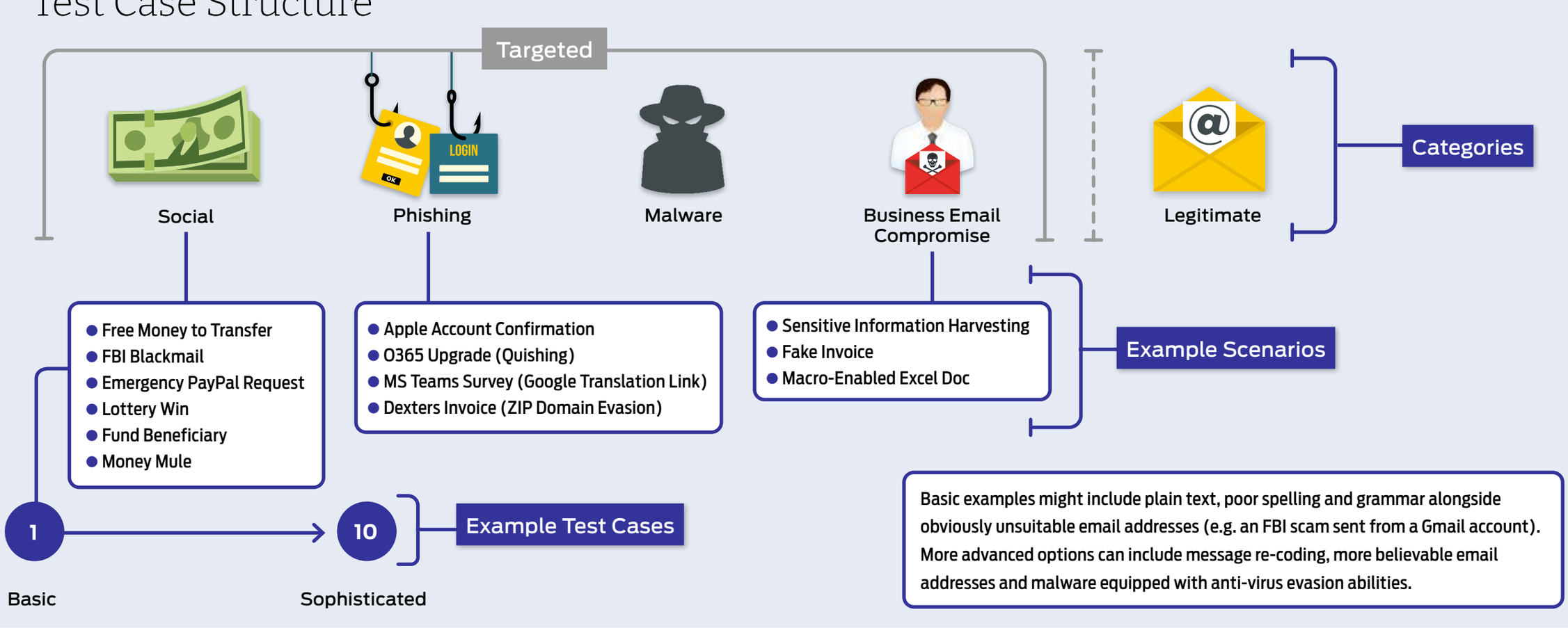
Targeted attacks comprise four distinct categories: Social Engineering; Phishing; Malware; and BEC. For each of these categories we created a number of main Test Case Structure variations.

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 the effectiveness of each email security service and configuration 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

Test Case Structure

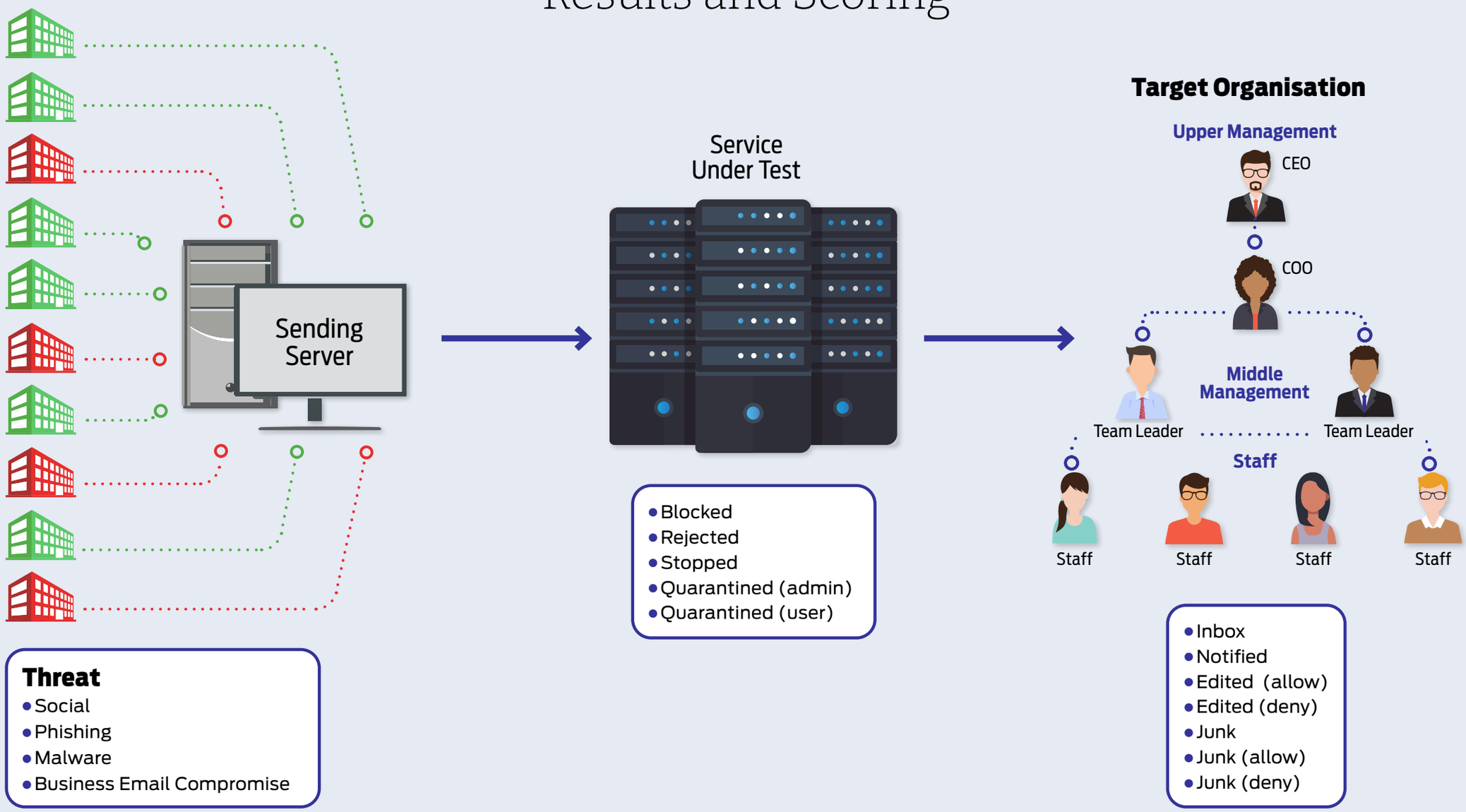


reaching the target's own infrastructure. There are opportunities for detection and protection at different stages in this journey.

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 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

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 13.

Attackers vs. Targets

Attacker/ APT Group	Method	Target	Details
Ajax Security Team			Ransomware via drive-by download of .exe file.
APT32			Ransomware inside PowerPoint document.
APT29			Ransomware inside PDF document.
Indrik Spider			Connection to command and control server created by .exe file inside Zip archive.
FIN13			Connection to command and control server created by .exe file.
FIN7			Connection to command and control server created by .exe file.

Key

Aviation
Banking and ATMs
Defence
Energy
Education
Entertainment
Financial
Gambling
Government Espionage
Healthcare
Information Technology
Law
Natural Resources
Private Sector Industries
Research Institutes
Telecommunication
Travel
US Retail, Restaurant and Hospitality

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 and configuration handles threats in the most general, least detailed way.

Threat Detection Results			
Product	**Detection Rate**	**Misses**	**Detection Rate (%)**
Microsoft Defender for Office 365	446	36	93%

■ 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.

Total Accuracy Ratings		
Product	**Total Accuracy Rating**	**Total Accuracy Rating (%)**
Microsoft Defender for Office 365	5,140	87%

■ Total Accuracy Ratings combine protection and false positives.

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 "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 +10 for threats; -10 for legitimate)
Services that intervene and move malicious messages into a Quarantine system are awarded either six or ten points depending on whether or not the user or administrator can recover the message. However, there is a six-to-ten 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 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.

Scoring Different Outcomes		
Action	**Threat**	**Legitimate**
Inbox	-10	10
Junk Folder	5	-5
Quarantined (admin)	10	-10
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

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 14) to roll your own set of personalised ratings.

Protection Accuracy Ratings		
Product	**Protection Accuracy Rating**	**Protection Accuracy Rating (%)**
Microsoft Defender for Office 365	4,100	85%

The table below shows how accurately the services handled legitimate email. The rating system is described in detail in **3. Protection and Legitimate Handling Accuracy** on page 10.

Legitimate Accuracy Ratings		
Product	**Legitimate Accuracy Rating**	**Legitimate Accuracy Rating (%)**
Microsoft Defender for Office 365	1,040	95%

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

4. Conclusion

This test exposed **Microsoft's** email security service to a range of threats. We used documented targeted attack methods as used by real-life attackers. These included focussed phishing, custom malware, business compromise techniques and other types of social engineering.

We've listed the attacker groups that inspired our attacks on **page 13**. To make things even more realistic, we created a simulated target organisation with regular suppliers and other partners. This enabled us to create look-alike adversaries. We used techniques such as using similar domain names to send malicious emails.

Following this test **Microsoft** updated its best practice script to fix a configuration issue, after which the service stopped the BEC attacks.

I've told them we'll have this fixed by Monday. The website is currently down, but at least we can get the PDF ready to upload in the meantime...

You can divide the email services that we test regularly into two main groups: platforms and third-party services. Platforms include Google, **Microsoft** and Yahoo. Third-party services handle email before or as it is delivered. Some act as gateways, receiving and processing messages before either deleting them or forwarding them to the platform. Other integrate more directly into the platform, which is an increasingly common approach.

At SE Labs, we believe that security products should keep threats as far away from end users as possible. Our scoring reflects that. With most security testing, and email in particular, there are so many variables and possible outcomes that the results can look a little overwhelming. We've tried to provide a neat 'Total Protection' score for each product to help simplify things, while providing enough data to allow you to create your own scoring system should you wish.

Microsoft Defender for Office 365 achieved an excellent detection score of 93% and a very good Protection Accuracy Rating of 85%. It was especially effective at preventing the execution of malware contained in targeted attacks. It stopped or blocked half of the targeted attacks, putting the rest in Quarantine where it could only be accessed by an administrator.

It also detected all of the phishing emails used in this test. Most of these also ended up in strict Quarantine that the end-user cannot access.

Two phishing threats were stopped outright, and one was edited but ultimately prevented from reaching the end-user's Inbox.

Microsoft Defender for Office 365 was slightly less effective against malicious business emails and social engineering scams, missing 26% and 30% respectively.

Microsoft's email platform was much better at recognising legitimate email and achieved an excellent Legitimate Accuracy Rating of 95%.

We awarded **Microsoft Defender for Office 365** a AAA rating for a combined 87% Total Accuracy Rating of its protection and legitimacy scores.

Appendices

Appendix A: Attack Details

Targeted Attack Types

Attack Group Ajax Security Team

Method of Attack Webpage to .exe file
Targets US Defence Industry

An Iran based group that has been active from at least 2010, this group mostly targets the US defence industry. It has leveraged various social engineering tactics to trick users into executing malicious files. This includes using a fake conference page as a lure to trick targets into installing a fake proxy application.

References:
https://attack.mitre.org/groups/G0130/

Attack Group APT32

Method of Attack Hidden link to .exe file
Targets Private Sector Industries

APT32 is a suspected Vietnam-based threat group, that also goes by the name of SeaLotus and OceanLotus. It has targeted multiple private sector industries as well as foreign governments in neighbouring countries such as Laos, Cambodia and the Phillippines. In spear phishing campaigns it utilises malicious Microsoft Office documents for initial access into various networks.

References:
https://attack.mitre.org/groups/G0050/

Attack Group APT29

Method of Attack Hidden link to .exe file
Targets Research Institutes

Based in Russia, APT29 has a large amount of associated groups, including IRON RITUAL, IRON HEMLOCK and NobleBaron. They have been attributed to Russia's foreign intelligence service, and mostly target research institutes and government networks. They have used malicious PDF files to silently infect recipients using decoy documents as distractions.

References:
https://attack.mitre.org/groups/G0016/

Attack Group Indrik Spider

Method of Attack .exe file
Targets Healthcare

This Russian cyber criminal group has been active since 2014 and mostly targets healthcare and public administration. It also goes by the name 'Evil Corp'. It has used the SocGholish framework hidden within a compressed Zip file to compromise victims.

References:
https://attack.mitre.org/groups/G0119/

Attack Group FIN13

Method of Attack shellcode/exe
Targets Hospitality Industries

FIN13 is a cyber threat group that has targeted financial, retail and hospitality industries in Mexico and Latin America. It has been known to steal intellectual property, financial data and mergers and acquisition information by means of data exfiltration.

References:
https://attack.mitre.org/groups/G1016/

Attack Group FIN7

Method of Attack Link to .exe file
Targets Financial Services

Also associated with GOLD NIAGARA, ITG14 and Carbon Spider, FIN7 is a financially-motivated threat group that has been active since 2013. It has a wide range of targets that includes financial services, retail and hospitality. It's initial compromises normally begins with spearphishing emails sent via a PHP mailer that includes a malicious link.

References:
https://attack.mitre.org/groups/G0046/

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:

- **Business Email Compromise**
- **Phishing**
- **Social Engineering**
- **Malware**

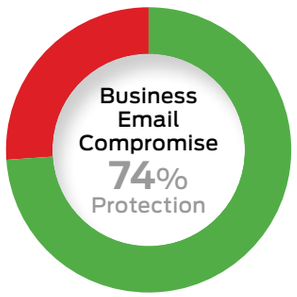
Each service has a number of options when handling such threats. The tables show how each service handled each category.

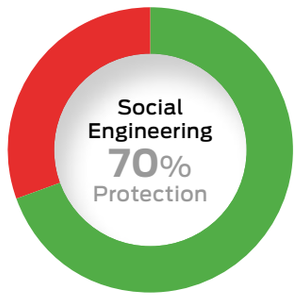
For example, you can see how many social engineering samples made it through to the Inbox; how many were sent to the Junk folder; and how many were prevented from coming anywhere near the user – the Junk folder and Quarantine (admin) are common options.

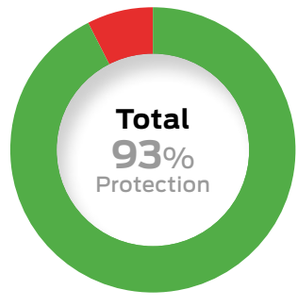
Not every possible option needs to be taken by a service under test, so the tables show only those outcomes that occurred.

Targeted Attack Details

Targeted Attack Details	Stopped	Blocked	Quarantined (admin)	Rejected	Edited (deny)	Quarantined (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	3	0	14	0	0	0	0	0	0	0	6
Phishing	2	0	297	0	1	0	0	0	0	0	0
Social Engineering	0	0	69	0	0	0	0	0	0	0	30
Malware	20	0	30	10	0	0	0	0	0	0	0
Total	**25**	**0**	**410**	**10**	**1**	**0**	**0**	**0**	**0**	**0**	**36**







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					
	Inbox	Edited (allow)	Junk Folder	Quarantined (admin)	Blocked
Microsoft Defender for Office 365	107	0	0	3	0

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** The service prevented the threat from being delivered and logged the event.

- **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 platform.

- **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 test was conducted between 8th December and 22nd December 2024.
- 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.

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.

SE Labs

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.