SE LABS ®

EMAIL
PROTECTION

Advanced Security Test Report

Mimecast
Email Security

ONLINE REPORT

OCTOBER 2026

SE LABS tested **Mimecast Email Security**, 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.

Contents

Introduction	**04**
Executive Summary	**05**
Advanced Security Test Awards	**05**
How We Tested	**06**
Case Structure	**06**
Results and Scoring	**07**
Attack Details	**08**
1. Threat Detection Result	**09**
2. Total Accuracy Rating	**10**
3. Protection and Legitimate Handling Accuracy	**11**
Protection Accuracy Rating	**12**
Legitimate Accuracy Rating	**12**
4. Conclusion	**13**
Appendices	**14**
Appendix A: Attack Details	**14**
Appendix B: Detailed Results	**15**
Appendix C: Legitimate Message Details	**16**
Appendix D: Terms Used	**17**
Appendix E: FAQs	**17**

Document version 1.0 Written 5th October 2026

SE LABS

Management
Chief Executive Officer Simon Edwards
Chief Operations Officer Marc Briggs
Chief Human Resources Officer Magdalena Jurenko
Technical Director Thomas Bean

Testing Team
Nikki Albesa
Daniel Botez
Solandra Brewster
Billy Coyne
Jarred Earlington
Gia Gorbold
Anila Johny
Cameron Love
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Enejda Torba

Marketing
Sara Claridge
Isobel Edwards
Tessa Welsh

Publication
Rahat Hussain
Colin Mackleworth

IT Support
Danny King-Smith
Chris Short

Website selabs.uk
Email info@selabs.uk
LinkedIn www.linkedin.com/company/se-labs/
Blog https://selabs.uk/blog/
Post SE Labs Ltd,
55A High Street,
Wimbledon,
SW19 5BA, UK

SE Labs is ISO/IEC 27001 : 2022 certified and BS EN ISO 9001 : 2015 certified for The Provision of IT Security Product Testing.

© 2026 SE Labs Ltd

Introduction



CEO
Simon Edwards

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us. SE Labs uses current threat intelligence to make our tests as realistic as possible. To learn more about how we test, how we define 'threat intelligence' and how we use it to improve our tests please visit our website and follow us on LinkedIn.

Test email security against business-focussed attackers

Ignore Business Email Compromise test cases at your peril

Good security testing is realistic, using the kinds of threats customers see in real life. This is why we put a lot of focus on Business Email Compromise (BEC) scenarios, rather than just more conventional threat types (like generic phishing and malware).

Many organisations focus on blocking spam and detecting malware, but BEC attacks present a different kind of threat. BEC targets the human element of email communication. Attackers craft convincing, fraudulent emails that appear to come from legitimate sources, tricking recipients into transferring money, sharing sensitive information or performing other actions that compromise the organisation.

BEC cases are not about malware detection or basic spam filtering. Instead, they exploit trust and authority. These attacks may bypass traditional security mechanisms because they often don't contain malicious links or attachments. Instead, they rely on social engineering, making them incredibly dangerous and quite hard to spot by either people or technology.

Testing email security without BEC scenarios is to ignore a highly effective and popular method that attackers use every day to infiltrate businesses. It's essential to ensure that email security solutions are able to recognise these nuanced threats and react accordingly.

Furthermore, adding security to a standard email platform shouldn't be an afterthought. Many businesses assume that the platforms they use, such as Microsoft 365 or Google Workspace, have robust, built-in defences. While these platforms offer a solid baseline, they are not infallible. Attackers continuously evolve their tactics, exploiting gaps in standard security settings.

Comprehensive email security requires layered defences that integrate seamlessly with these platforms, providing advanced detection capabilities, including AI-driven anomaly detection, BEC filtering, and more.

By enhancing the built-in security of these platforms, organisations can mitigate risks more effectively. Security should be adaptive and proactive, not reactive, ensuring that your organisation stays protected even as threats evolve. Including BEC scenarios in testing is an essential part of validating these systems' robustness.

Executive Summary

This test examined the effectiveness of **Mimecast Email Security** against a wide range of threats that target enterprise businesses through email.

SE Labs used advanced targeted attack techniques, as seen in devastating real-world attacks, to assess how well this service handles email cyber threats

Legitimate messages were also sent through the service to ensure that security settings were balanced with reasonable usability.

Mimecast Email Security is a commercial service designed to act as a gateway to email platforms such as Microsoft 365 and Google.

It achieved excellent protection and detection scores and was effective against all four categories of targeted attacks: phishing, malware, business email compromise and social engineering. Its threat detection score was only slightly higher than its protection accuracy rating.

The service was not overly strict, despite achieving such high detection and protection ratings. It correctly identified legitimate email, allowing end user access to almost all of them without any hindrance.

By achieving a Total Accuracy Rating of 96%, **Mimecast Email Security** was given an AAA Advanced Security Test Award for protection.

Executive Summary

Mimecast Email Security		
	Accuracy Score	**Rating (%)**
Protection Accuracy	4,620/4,860	95%
Threat Detection Rates	474/486	98%
Legitimate Accuracy	1,080/1,100	98%
Total Accuracy	5,700/5,960	96%

For exact percentages, see **2. Total Accuracy Ratings** on page 10.

Advanced Security Test Award

The following product wins the SE Labs award:



Mimecast
Email Security

How We Tested

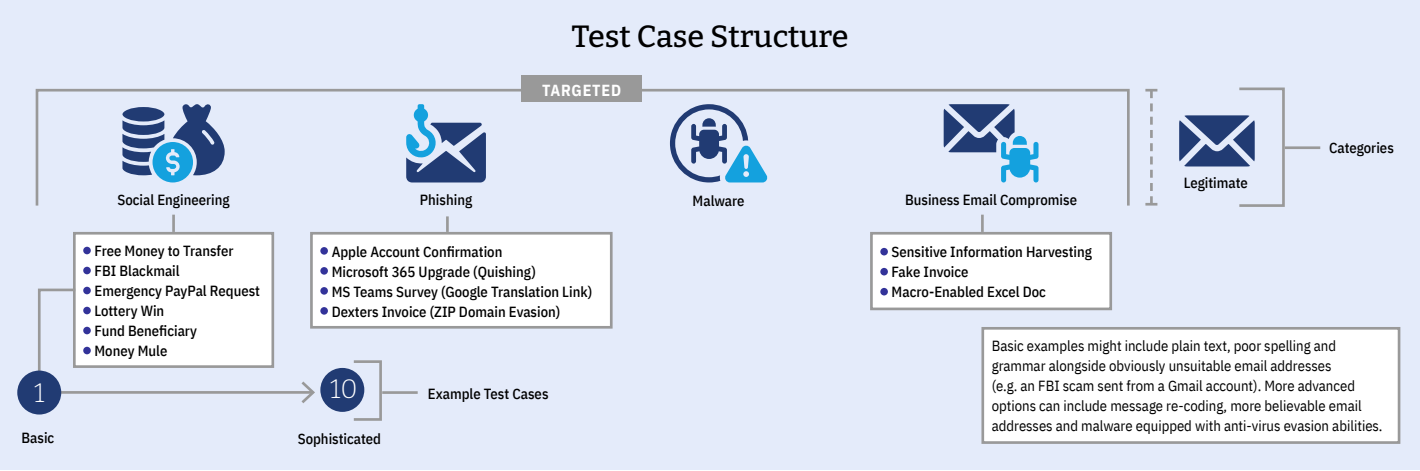
Targeted attacks comprise four categories: Social Engineering; Phishing; Malware; and Business Email Compromise. For each of these categories we created a number of main Test Case Structure variations.

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 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.

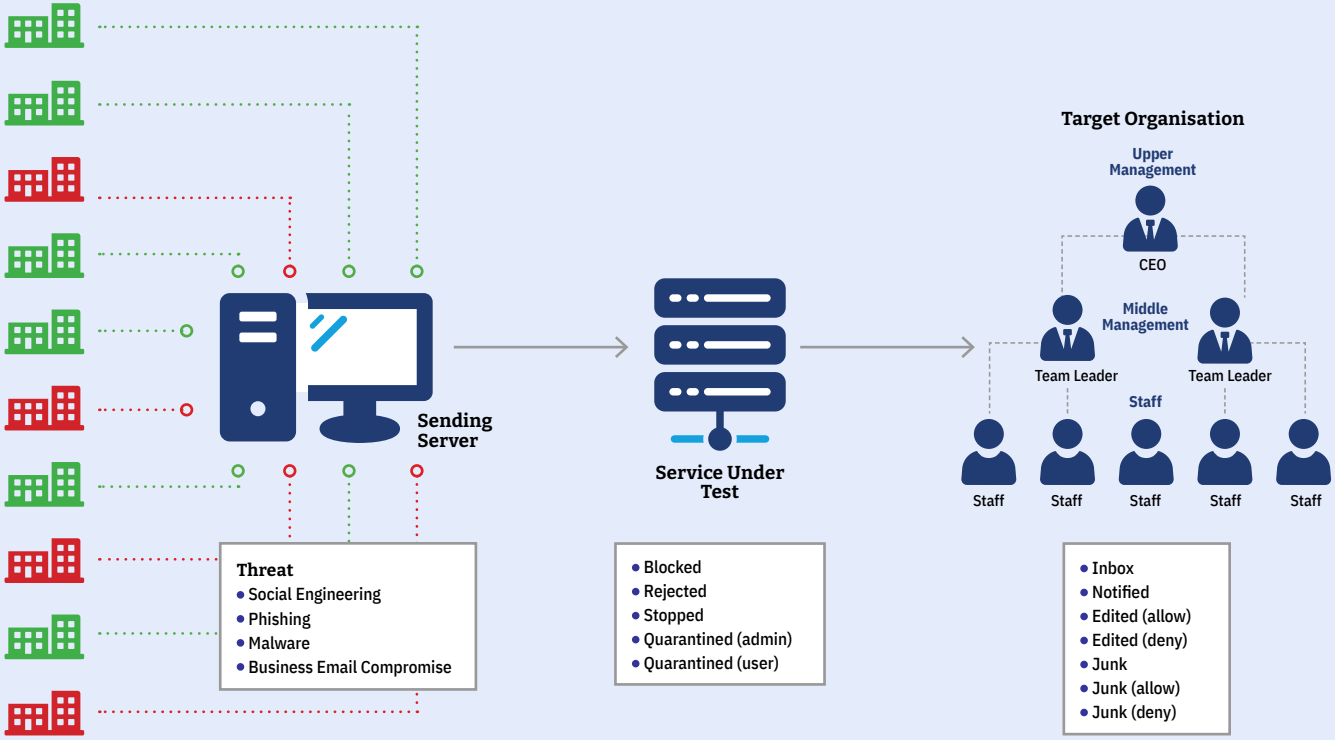
Legitimate messages were constructed in-house. Email messages travel over the internet to their recipients. Before they reach the Inbox, they negotiate their way through various security services before reaching the target's own infrastructure. There are opportunities for detection and protection at 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 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



Attack Details

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 14.

Attack Details

Attacker/ APT Group	Method	Target	Details
Andariel	Webpage to .exe file		Drive by Download to an .exe containing ransomware
Sandworm Team	Hidden link to .exe file		Malicious PowerPoint containing ransomware
APT29	Hidden link to .exe file		Malicious PDF Document containing ransomware
Lazarus Group	Zipped to .exe file		Malicious .exe that creates a backdoor to a C2 server
APT32	shellcode/exe		Zipped malicious .exe that creates a backdoor to a C2 server
Cobalt Group	Lnk .exe file		Malicious .exe that creates a backdoor to a C2 server

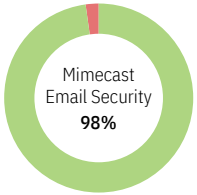
KEY					
	Electrical		Entertainment		Financial
	Government		Healthcare		Journalists
	Research Institutes		Technology		Telecommunications

1. Threat Detection Result

While testing and scoring email security services is complex, it is possible to report straightforward detection rates. The figures below summarise how each service and configuration handles threats in the most general, least detailed way.

Threat Detection Result

Products Tested	Detection Rate	Misses	Detection Rate (%)
Mimecast Email Security	474	12	98%



- **Detection rates are a useful but unsubtle way to compare services.**

2. Total Accuracy Rating

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.

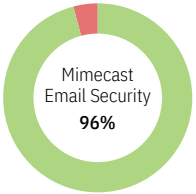
We take these different possible outcomes into account when attributing points that form final ratings.

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 "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.

Total Accuracy Rating

Products Tested	Total Accuracy Rating	Total Accuracy Rating (%)
Mimecast Email Security	5,700/5,960	96%



Total Accuracy Ratings combine protection and false positives.

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.

Rating Calculations

For threat results we calculate the protection ratings using the following formula:
Protection rating =
(10x number of Stopped etc.) +
(6-10x 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 -10x number of Quarantined) +
(-10x number of Stopped etc.)
etc.

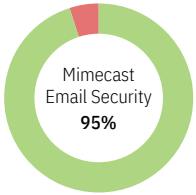
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in Quarantine, or for a malware threat to end up in the Inbox. You can use the raw data from this report (See **Appendix B: Detailed Results** on page 15) to roll your own set of personalised ratings.

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

Protection Accuracy Rating

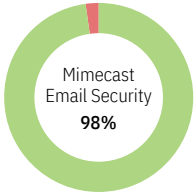
Products Tested	Protection Accuracy Rating	Protection Accuracy Rating (%)
Mimecast Email Security	4,620/4,860	95%



Legitimate Accuracy Rating

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 11.

Products Tested	Legitimate Accuracy Rating	Legitimate Accuracy Rating (%)
Mimecast Email Security	1,080/1,100	98%



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

4. Conclusion

This test exposed **Mimecast Email Security** to a wide range of threats. We used documented targeted attack methods as used by real-life attackers. These included focussed phishing, custom malware, Business Email Compromise (BEC) techniques and other types of social engineering.

We've listed the attacker groups that inspired our attacks on **page 14**. To make things even more realistic, we created a simulated target organisation with a staff hierarchy, 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.

SE Labs believes 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 the product being tested to help simplify things, while providing enough data to allow you to create your own scoring system should you wish.

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 integrate directly into the platform. Others, such as **Mimecast Email Security**, act as gateways, receiving and processing messages before either deleting them or forwarding them to the platform.

Test results show that **Mimecast Email Security** was effective at providing an additional layer of protection against the types of sophisticated email attacks typically deployed by state-sponsored groups. It detected 98% of the attacks and was able to protect against 95% of them.

The small difference between the detection and protection ratings may be attributed to how the service handles different types of email threats. The service scans every email, attachment and URL but does not block threats straightaway. Instead, it places those it deems suspicious in a quarantine that can only be accessed by an administrator.

This approach was most effective against phishing email and those with embedded malware. None of these escaped the administrator-managed quarantine. This is a good result since it kept end users well away from Office files that that have hidden links to ransomware, some of which were even drivebys.

However, one BEC sample (out of a total of 26) did manage to land in the end user's Inbox, as did 11 (out of 100) social engineering emails.

Mimecast Email Security was very effective at recognising legitimate email and achieved an excellent Legitimate Accuracy Rating of 98%. This, combined with the 98% Threat Detection Rating and the 95% Protection Accuracy Rating, contributed to the 96% Total Accuracy Rating, an excellent result which made deserving of its AAA award.

Appendices

Appendix A: Attack Details

Targeted Attack Types

Attack Group: **Andariel**
Method of Attack: **Webpage to .exe file**
Targets: **Government**

Andariel is a North Korean state-sponsored threat group active since 2009. It targets South Korean government, military and businesses, conducting destructive attacks and cyber-financial operations against ATMs, banks and cryptocurrency exchanges, including notable campaigns.

References https://attack.mitre.org/groups/G0138/

Attack Group: **Sandworm Team**
Method of Attack: **Hidden link to .exe file**
Targets: **Electrical**

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: **APT29**
Method of Attack: **Hidden link to .exe file**
Targets: **Research Institutes**

APT29, based in Russia and linked to the foreign intelligence service, includes groups like IRON RITUAL and NobleBaron. It targets research institutes and government networks using malicious PDFs with decoy documents to silently infect victims.

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

Attack Group: **Lazarus Group**
Method of Attack: **Zipped .exe file**
Targets: **Entertainment**

Lazarus Group is a North Korean state-sponsored cyber threat group linked to the Reconnaissance General Bureau. Active since 2009, it has conducted major cyberattacks, including the 2014 Sony Pictures attack, and is associated with campaigns such as DarkSeoul and Operation Troy.

References https://attack.mitre.org/groups/G0032/

Attack Group: **APT32**
Method of Attack: **Shellcode/exe**
Targets: **Journalists**

APT32, also known as SeaLotus and OceanLotus, is a suspected Vietnam-based threat group targeting private industries and neighbouring governments. It uses spear-phishing campaigns and malicious Microsoft Office documents to gain network access.

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

Attack Group: **Cobalt Group**
Method of Attack: **Lnk to malicious .exe file**
Targets: **Financial Institutions**

Cobalt Group is a financially motivated threat group targeting financial institutions since 2016. It steals money through ATM, card processing, payment and SWIFT systems, mainly targeting banks in Eastern Europe, Central Asia and Southeast Asia. The group remains active.

References https://attack.mitre.org/groups/G0080/

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**

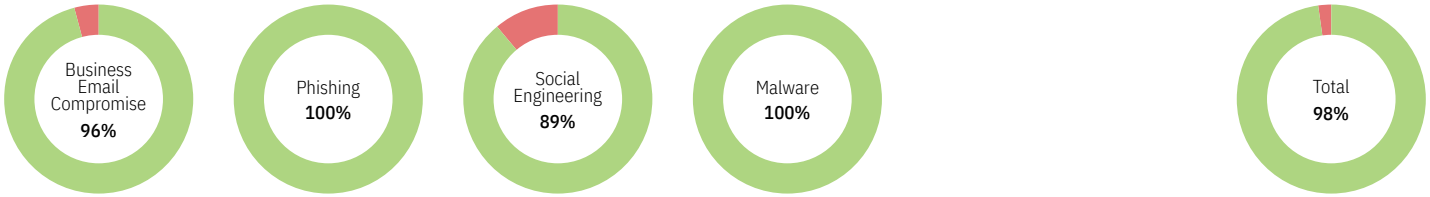
Each service has a number of options when handling such threats. The tables show how each service handled each category.

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	Stopped	Blocked	Quarantine (admin)	Rejected	Edited (deny)	Quarantine (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	25	0	0	0	0	0	0	0	1
Phishing	0	0	300	0	0	0	0	0	0	0	0
Social Engineering	0	0	89	0	0	0	0	0	0	0	11
Malware	0	0	44	0	16	0	0	0	0	0	0
Total	**0**	**0**	**458**	**0**	**16**	**0**	**0**	**0**	**0**	**0**	**12**



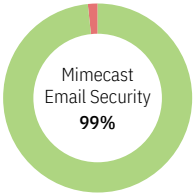
Appendix C: Legitimate Message Details

These results show how effectively the 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.

Product	Inbox	Edited (allow)	Junk Folder	Junk (allow)	Quarantine (admin)	Blocked
Mimecast Email Security	109	0	0	0	1	0



Appendix D: Terms Used

The results 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 E: FAQs

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.

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

- The test was conducted between 24th August and 9th September 2026.
- 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

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.