SE LABS ®

EMAIL
PROTECTION

Advanced Security Test Report

Cisco
Secure Email Threat Defense

ONLINE REPORT

JUNE 2025

SE LABS tested **Cisco Secure Email Threat Defense**, 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

How We Tested 06

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

Legitimate Message Details 16

Appendix D: Terms Used 17

Appendix E: FAQs 17

Document version 1.0 Written 9th June 2025

SE LABS

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

Testing Team
Nikki Albesa
Thomas Bean
Solandra Brewster
Billy Coyne
Jarred Earlington
Gia Gorbold
Anila Johny
Cameron Love
Erica Marotta
Jeremiah Morgan
Julian Owusu-Abrokwa
Joseph Pike
Enejda Torba
Dimitrios Tsarouchas

Marketing
Sara Claridge
Ben Tudor

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 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.

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 Cisco Secure Email Threat Defense 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 this service handles email cyber threats. Legitimate messages were also sent through the service ensure that security settings were balanced with reasonable usability.

Cisco Secure Email Threat Defense is a commercial service designed to provide additional security to cloud-based email platforms such as Microsoft 365. It scored excellent protection as well as detection ratings and was particularly effective against email that carry malware. It also protected against phishing and other types of social engineering email.

The service was not overly strict despite achieving such high detection and protection ratings. It correctly identified legitimate email, allowing end-user access to all of them without any hindrance. **Cisco Secure Email Threat Defense** was awarded an AAA rating for award for its Total Accuracy Rating of 94%.

Executive Summary

Cisco Secure Email Threat Defense		
	Accuracy Score	Rating (%)
Protection Accuracy	4,485/4,860	92%
Threat Detection Rates	468/486	96%
Legitimate Accuracy	1,100/1,100	100%
Total Accuracy	5,585/5,960	94%

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

Advanced Security Test Award

The following product wins the SE Labs award:

SE LABS
AAA
JUNE 2025
Advanced Security
Email Protection

Cisco
Secure Email
Threat Defense

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.

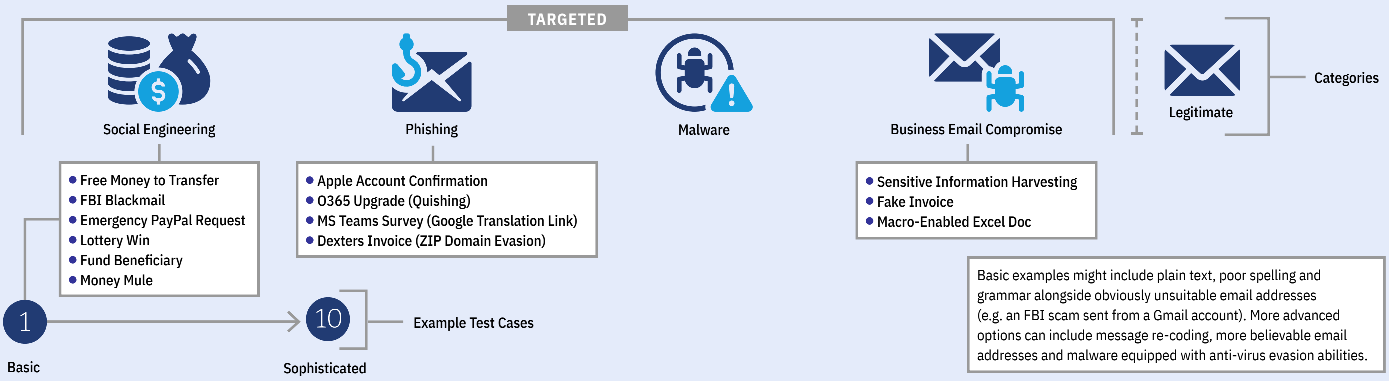
In the example below you can see that the social engineering messages are formed into six groups (scenarios), including free money transfer, lottery win and law enforcement blackmail scams. For each scenario we create variants that range in sophistication from extremely basic to very advanced. The goal 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.

Test Case Structure



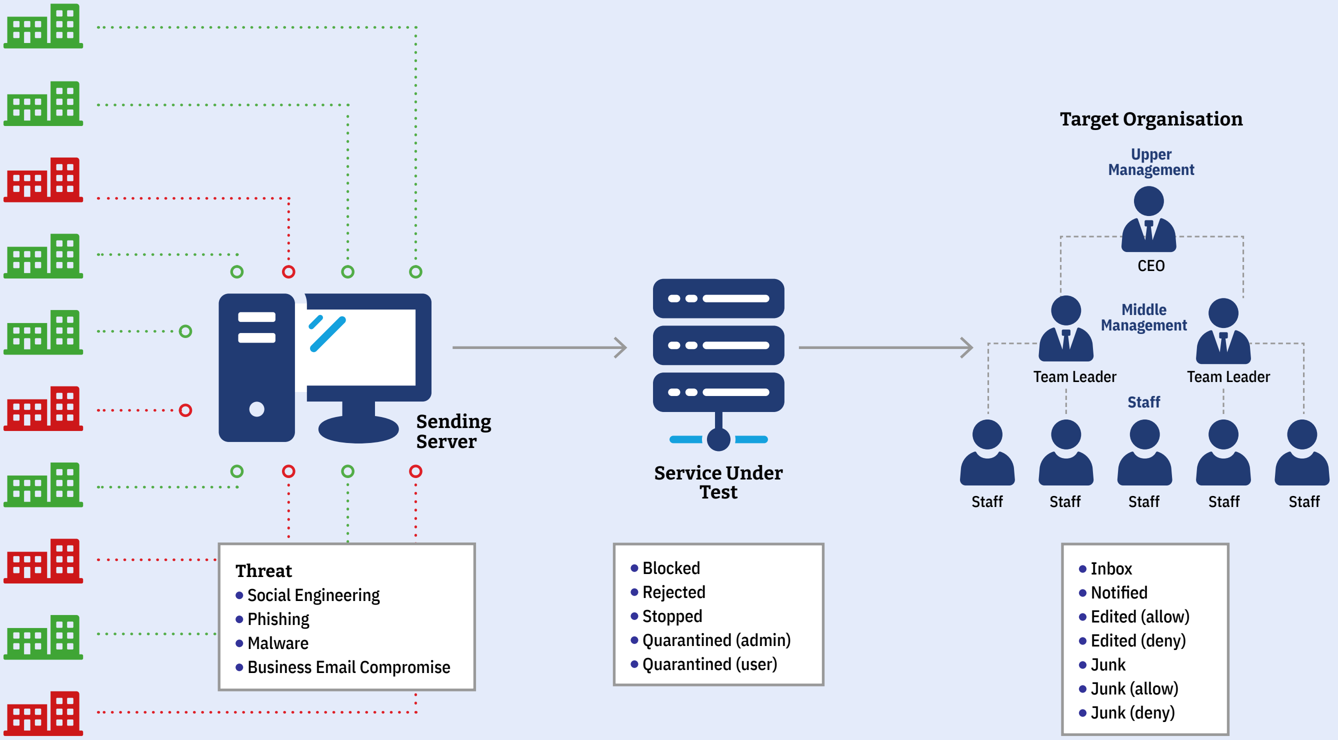
- Free Money to Transfer
- FBI Blackmail
- Emergency PayPal Request
- Lottery Win
- Fund Beneficiary
- Money Mule

- Apple Account Confirmation
- O365 Upgrade (Quishing)
- MS Teams Survey (Google Translation Link)
- Dexters Invoice (ZIP Domain Evasion)

- Sensitive Information Harvesting
- Fake Invoice
- Macro-Enabled Excel Doc

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

Results and Scoring



Threat

- Social Engineering
- Phishing
- Malware
- Business Email Compromise

- Blocked
- Rejected
- Stopped
- Quarantined (admin)
- Quarantined (user)

- Inbox
- Notified
- Edited (allow)
- Edited (deny)
- Junk
- Junk (allow)
- Junk (deny)

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
OilRig	Webpage to .exe	🏭	Drive-by download to an .exe file containing ransomware
Saint Bear	Hidden link to .exe	🏛	Malicious PowerPoint containing ransomware
MuddyWater	Hidden link to .exe	🛡	Malicious PDF document containing ransomware
APT38	Zipped exe	💰	Malicious .exe file that creates a backdoor to a C2 server
APT29	shellcode/exe	🔍	Zipped malicious .exe file that creates a backdoor to a C2 server
Windshift	Link to .exe	🌉	Malicious .exe that creates a backdoor to a C2 server

KEY

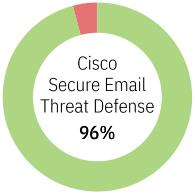
🌉	Critical Infrastructure	🛡	Defense	🏭	Energy
💰	Financial Industries	🏛	Government Espionage	🔍	Research Institutes

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 Result

Products Tested	Detection Rate	Misses	Detection Rate (%)
Cisco Secure Email Threat Defense	468	18	96%



● 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.

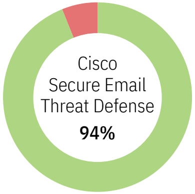
We take these different possible outcomes into account when attributing points that form final ratings.

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 "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 (%)
Cisco Secure Email Threat Defense	5,585/5,960	94%



● **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.

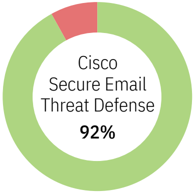
These ratings are based on our opinion of how important these different outcomes are. You may have a different view on how serious it is for a legitimate email to end up in Quarantine, or for a malware threat to end up in the Inbox. You can use the raw data from this report (See **Appendix B: Detailed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

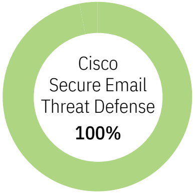
Products Tested	Protection Accuracy Rating	Protection Accuracy Rating (%)
Cisco Secure Email Threat Defense	4,485/4,860	92%



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 (%)
Cisco Secure Email Threat Defense	1,100/1,100	100%



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

4. Conclusion

This test exposed **Cisco Secure Email Threat Defense** 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 compromise 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 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.

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 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. Platform 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. Others, like **Cisco Secure Email Threat Defense**, integrate more directly into the platform, which is an increasingly common approach.

The service is designed to be an 'always-on' security layer for Microsoft's cloud-based email platform. Two numbers from the test demonstrate its ability to continuously analyse emails sent to the Microsoft 365 mailbox: a 100% Legitimate Accuracy Rating and a 96% Threat Detection Rating. Taken in tandem, these results show that **Cisco Secure Email Threat Defense** allows end-users quick access to messages they are meant to receive while keeping them away from email that carry dangerous threats. This degree of timeliness is a critical advantage for any business of whatever size.

Cisco Secure Email Threat Defense achieved a Protection Accuracy Rating of 92%, slightly lower than its Threat Detection Rating. The **Detailed Results** on page 15 show that the service did not stop nor block any of the threats upon delivery of the malicious emails. Instead, it placed the bulk of them in Quarantine which can only be accessed by an administrator. This seems in line with Cisco's maximalist approach to administrator management and visibility.

This worked very well for emails that had malware as all of them were contained in the administrator-controlled Quarantine. It was slightly less effective for phishing and social engineering email, three each of which ended up in the Inbox.

BEC threats were the most problematic as almost half of them could be accessed by the end-user. It's interesting to note that, when some phishing email were consigned to the Junk Folder, the service removed the malicious content. A few points were docked for the three BEC threats that were sent to the Junk Folder because they were not modified in the same way.

Overall, however, **Cisco Secure Email Threat Defense's** achieved a Total Accuracy Rating of 94%, an excellent performance that merited an AAA award for Advanced Security Email Protection.

Appendix A: Attack Details

Targeted Attack Types

Attack Group: OilRig

Method of Attack: Webpage to .exe file

Targets: Energy

OilRig is a suspected Iranian state-backed threat group active since 2014, targeting sectors such as finance, government, and energy through supply chain attacks, using Iranian infrastructure in alignment with Iran's national interests.

References https://attack.mitre.org/groups/G0049/

Attack Group: Saint Bear

Method of Attack: Hidden link to .exe file

Targets: Government

Saint Bear is a Russian-linked threat actor active since 2021, targeting Ukraine and Georgia. It uses tools like Saint Bot and OutSteel, relying on phishing and spoofed documents, and is distinct from Ember Bear in tactics and tools.

References https://attack.mitre.org/groups/G1031/

Attack Group MuddyWater

Method of Attack: Hidden link to .exe file

Targets: Defense

MuddyWater is a cyber espionage group linked to Iran's MOIS, active since 2017. It targets government and private sectors including defense, telecoms, and energy across the Middle East, Asia, Africa, Europe, and North America.

References https://attack.mitre.org/groups/G0069/

Attack Group APT38

Method of Attack: Zipped .exe

Targets: Financial Organisations

APT38, a North Korea-based threat group, targets banks, financial institutions, and cryptocurrency exchanges in over 30 countries. Notable attacks include the Bank of Bangladesh, Bancomext, and Banco de Chile, stealing billions in cryptocurrency.

References https://attack.mitre.org/groups/G0082/

Attack Group APT29

Method of Attack: shellcode/exe

Targets: Research Institutes

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

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

Attack Group Windshift

Method of Attack: Link to .exe

Targets: Critical Infrastructure

Windshift is a threat group that has been active since at least 2017, targeting specific individuals for surveillance in government departments and critical infrastructure across the Middle East.

References https://attack.mitre.org/groups/G0112/

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.

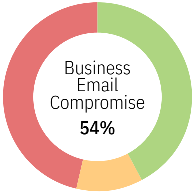
For example, you can see how many social engineering samples made it through to the Inbox; how many were sent to the Junk folder; and how many were prevented from coming anywhere near the user – the Junk folder and Quarantine (admin) are common options.

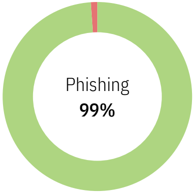
Not every possible option needs to be taken by a service under test, so the tables show only those outcomes that occurred.

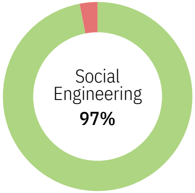
Targeted Attack Details

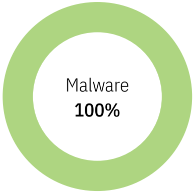
Targeted Attack	Stopped	Blocked	Quarantine (admin)	Rejected	Edited (deny)	Quarantine (user)	Junk (deny)	Junk Folder	Junk (allow)	Edited (allow)	Inbox
Business Email Compromise	0	0	9	0	2	0	0	3	0	0	12
Phishing	0	0	288	2	0	0	7	0	0	0	3
Social Engineering	0	0	97	0	0	0	0	0	0	0	3
Malware	0	0	60	0	0	0	0	0	0	0	0

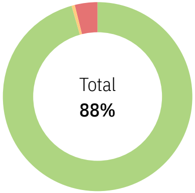
Total	0	0	454	2	2	0	7	3	0	0	18











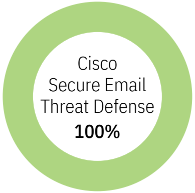
Legitimate Message Details

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
Cisco Secure Email Threat Defense	110	0	0	0	0	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 3rd March and 11th April 2025.
- 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.