# SE LABS

# Email Security Services
## Enterprise and Small Business

ONLINE REPORT

SE LABS ® tested three email security services, one that is commercial, the other open-source. We also tested a commercial email platform.

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 and shortly after the attacks took place.

# Contents

Document version 1.0 Written 23th September 2024

# 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 three email security solutions. **Google Workspace Enterprise Plus** is a commercial email platform. **Trend Vision One Email and Collaboration Security** and **mailcow: dockerized** are 'add-on' services designed to provide additional security. **Trend Vision One Email and Collaboration Security** is a commercial service, while **mailcow: dockerized** is open-source.

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.

Clear winner **Trend Vision One Email and Collaboration Security** achieved an excellent Total

Accuracy rating of 97%, by virtue of detecting all the threats then providing protection against almost all of them. All legitimate messages reached the Inbox, so that it scored a 100% Legitimate Accuracy rating. **Trend Vision One Email and Collaboration Security** earned an AAA rating for its outstanding performance.

**Google Workspace Enterprise Plus** detected 63% of the threats and provided protection against 26% of them. It had misclassified some legitimate email as malicious, scoring an 80% Legitimacy Accuracy rating. It received a C rating for its Total Accuracy score of 36%.

**Mailcow** performed poorly, detecting only 30% of the malicious emails, then scoring a negative 40% Protection Accuracy rating. It did, however, allow all legitimate emails to go through. **Mailcow**, which had a Total Accuracy rating of -14%, was not rated.

## Email Security Services Protection Award

The following product wins the SE Labs award:

SE LABS
AAA
SEPTEMBER 2024
EMAIL SECURITY SERVICES

**Trend**
Vision One Email and Collaboration Security

## Executive Summary

| Products Tested | Protection Accuracy Rating (%) | Threat Detection Rates (%) | Legitimate Accuracy Rating (%) | Total Accuracy Rating (%) |
|---|---|---|---|---|
| Trend Vision One Email and Collaboration Security | 90% | 100% | 100% | 97% |
| Google Workspace Enterprise Plus | 26% | 63% | 80% | 36% |
| mailcow: dockerized | -40% | 30% | 100% | -14% |

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

# 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.
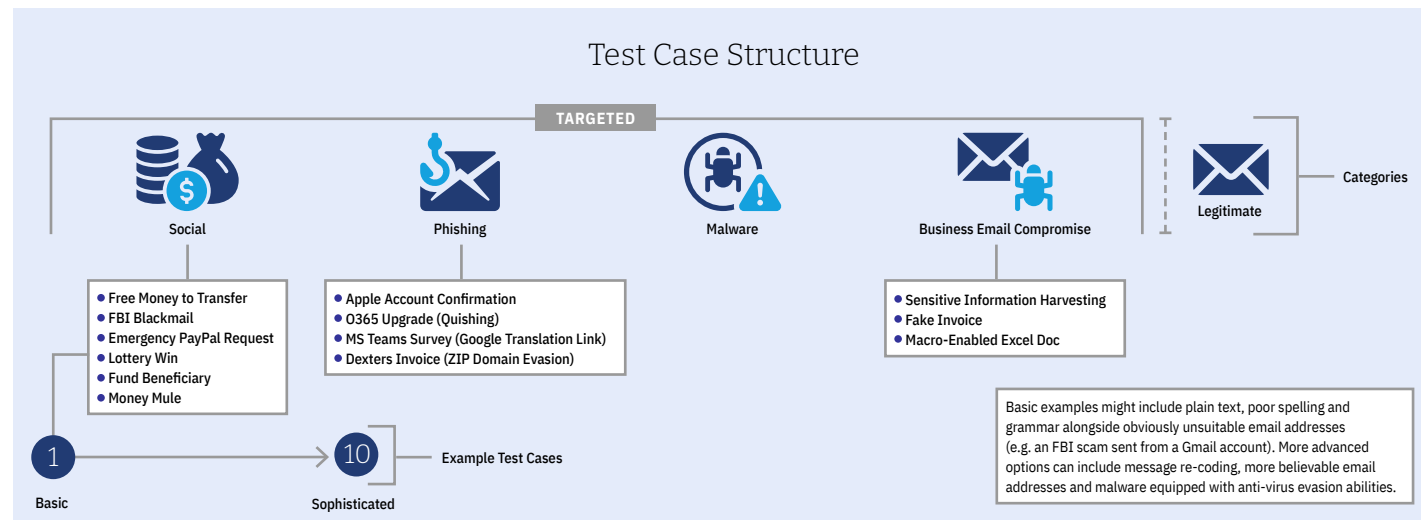
Legitimate messages were constructed in-house.

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

## Test Case Structure

TARGETED

Social — Phishing — Malware — Business Email Compromise — Legitimate — Categories

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

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

**Business Email Compromise**
- 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.
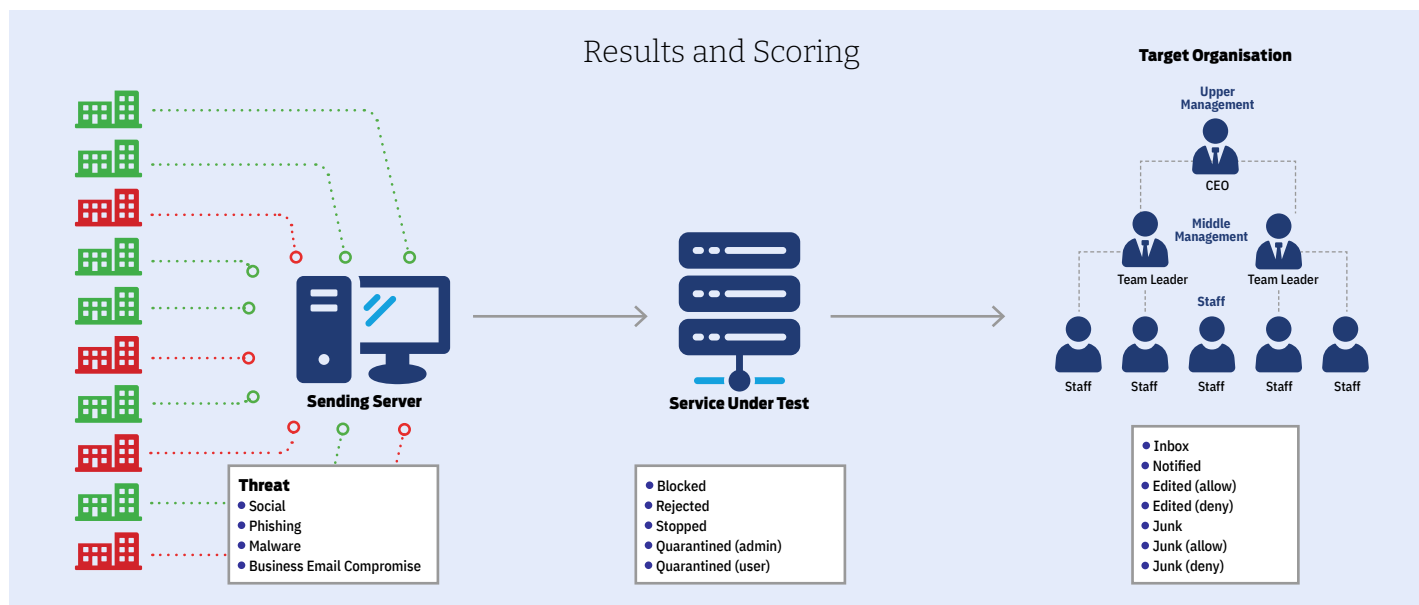
1 Basic → 10 Sophisticated — Example Test Cases

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



**Target Organisation**

Upper Management

CEO

Middle Management

Team Leader    Team Leader

Staff

Staff   Staff   Staff   Staff   Staff

**Sending Server**

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

**Service Under Test**

- 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 |
|---|---|---|---|
| Mustard Tempest | Webpage to .exe | | Drive by Download to an exe containing ransomware |
| APT39 | Hidden link to .exe | | Malicious PowerPoint containing ransomware |
| Mofang | Hidden link to .exe | | Malicious PDF Document containing ransomware |
| Higaisa | .exe | | Malicious Exe that creates a backdoor to a C2 server |
| Turla | shellcode/.exe | | Zipped Malicious Exe that creates a backdoor to a C2 |
| Inception | Link to .exe | | Malicious Exe that creates a backdoor to a C2 |

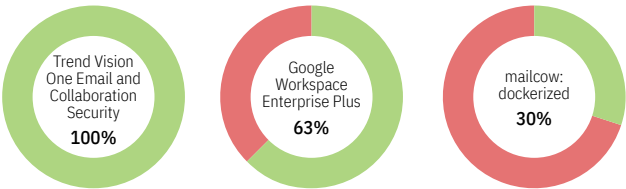| KEY | | | | | |
|---|---|---|---|---|---|
| | Financial Industries | | Government Espionage | | Private-sector Energy |
| | Research Institutes | | Trade Organisations | | Travel Industries |

# 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 Rates

| Products Tested | Detection Rate | Misses | Detection Rate (%) |
|---|---|---|---|
| Trend Vision One Email and Collaboration Security | 486 | 0 | 100% |
| Google Workspace Enterprise Plus | 305 | 181 | 63% |
| mailcow: dockerized | 147 | 339 | 30% |

Trend Vision One Email and Collaboration Security
**100%**

Google Workspace Enterprise Plus
**63%**

mailcow: dockerized
**30%**

● 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 Ratings

| Products Tested | Total Accuracy Rating | Total Accuracy Rating (%) |
|---|---|---|
| Trend Vision One Email and Collaboration Security | 5,773 | 97% |
| Google Workspace Enterprise Plus | 2,120 | 36% |
| mailcow: dockerized | -820 | -14% |



Trend Vision One Email and Collaboration Security **97%**

Google Workspace Enterprise Plus **36%**

mailcow: dockerized **-14%**
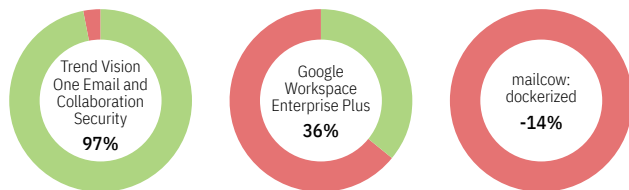
● **Total Accuracy Ratings combine protection and false positives.**

# 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.) +
(6-8x 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 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 Ratings

| Products Tested | Total Accuracy Rating | Total Accuracy Rating (%) |
|---|---|---|
| Trend Vision One Email and Collaboration Security | 4,673 | 96% |
| Google Workspace Enterprise Plus | 1,240 | 26% |
| mailcow: dockerized | -1,920 | -40% |

Trend Vision One Email and Collaboration Security **96%**

Google Workspace Enterprise Plus **26%**

mailcow: dockerized **-40%**
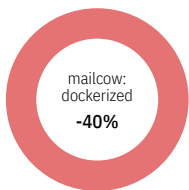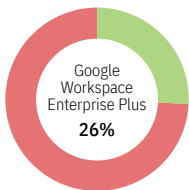
● The table above shows how accurately the services handled legitimate email. The rating system is described in detail in **3. Protection and Legitimate Handling Accuracy on page 11.**

## Legitimate Accuracy Ratings

| Products Tested | Legitimate Accuracy Rating | Legitimate Accuracy Rating (%) |
|---|---|---|
| Trend Vision One Email and Collaboration Security | 1,100 | 100% |
| Google Workspace Enterprise Plus | 880 | 80% |
| mailcow: dockerized | 1,100 | 100% |

Trend Vision One Email and Collaboration Security **100%**

Google Workspace Enterprise Plus **80%**

mailcow: dockerized **100%**
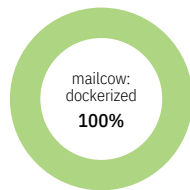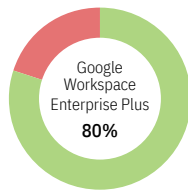
● Legitimate Accuracy Ratings give a weighted value to services based on how accurately they handle legitimate messages.

# 4. Conclusion

**This test exposed** a well-known email platform and two third-party security services to a range of threats. These included focussed phishing, custom malware, business email 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 each product to help simplify things, while providing enough data to allow you to create your own scoring system should you wish.

Each product tested belongs to a separate category of email security solutions. Their differences hinge on two variables: (**1**) whether the product is a platform or an 'add-on' service; and (**2**) whether the product is open-source or paid for. Think of it this way: if you're

paying for a suite of productivity applications and an email service is part of the package, would adding another layer of email security be worth it?

Google's **Google Workspace Enterprise Plus** email service differs from its free Gmail account in that the former is managed by an administrator. There's room for improvement in the way that **Google Workspace Enterprise Plus** distinguishes malicious from legitimate emails. It correctly identified 63% of the emails with threats and 80% of those that were legitimate. The malicious emails that it failed to detect immediately landed in the end-user's Inbox. Joining these were the emails that were correctly identified as malicious but could not be protected against.

Could adding an open-source email security service add value to an email platform such as **Google Workspace Enterprise Plus**? Perhaps not, if the candidate is **mailcow: dockerized** in its current configuration. **Mailcow** had shown enough improvement in last year's comparative test to earn a B rating. In this test, its Total Accuracy rating is -14%. That's all down to its poor detection of and protection against malicious emails since it correctly identified all of the legitimate email. Roughly twice as many malicious emails landed in a **mailcow: dockerized** Inbox as they did in one protected by **Google Workspace Enterprise Plus**.

If an administrator wants to increase the level of security for an email platform such as **Google Workspace Enterprise Plus**, then he might consider the AAA awardee **Trend Vision One Email and Collaboration Security**. Boasting a Total Accuracy rating of 97%, **Trend Vision One Email and Collaboration Security** winnows malicious from legitimate email at the detection stage, achieving a 100% rating for both.

**Trend Vision One Email and Collaboration Security** handles malicious email by stopping them outright, placing them in quarantine where only the administrator can access them, or placing them in a junk folder where they cannot be opened by the end-user. It differs from **Google Workspace Enterprise Plus** which did not stop or block malicious email, preferring instead to place them in quarantine for admin review.

From these results, we can see that **Trend Vision One Email and Collaboration Security** is definitely effective at adding a layer of protection against harmful email. All that's left to consider for any business, of whatever size, is its own cost-benefit analysis and that largely depends on how much it values data protection. In evaluating the upfront cost of **Trend Vision One Email and Collaboration Security**, it's also worth factoring in the administrative cost of reviewing malicious email that mostly end up in quarantine.

# Appendices

## Appendix A: Attack Details

### Targeted Attack Types

**Attack Group** Mustard Tempest
**Method of Attack** Webpage to .exe file
**Targets** Financial Industries

Operating from at least 2017, they are a cyber-criminal group known to operate with the SocGhoulish malware through fake browser updates. They also typically provide access to compromised system to other attackers.

**References** https://attack.mitre.org/groups/G1020/

**Attack Group** APT39
**Method of Attack** Hidden link to .exe file
**Targets** Travel Industries

APT39 refers to cyber espionage conducted by the Iranian Ministry of Intelligence and Security since 2014 against targets in the travel, hospitality, academic and telecommunications sectors.

**References** https://attack.mitre.org/groups/G0087/

**Attack Group** Mofang
**Method of Attack** Hidden link to .exe file
**Targets** Government Espionage

Suspected to be of Chinese origin and observed since 2012, Mofang are a cyber espionage group with a focus towards political & economic espionage, specifically against Myanmar, India and US governments.

**References** https://attack.mitre.org/groups/G0103/

**Attack Group** Higaisa
**Method of Attack** .exe
**Targets** Trade Organisations

First disclosed in 2019 yet operating from at least 2009, Higaisa are a South Korean threat group noted to conduct attacks primarily against North Korea, though China, Japan and Russia also fell victim.

**References** https://attack.mitre.org/groups/G0126/

**Attack Group** Turla
**Method of Attack** .exe
**Targets** Trade Organisations

This Russia-based threat group targets victims in different countries and across a wide range of industries. These include governmental organisations, notably including embassies and the military. Its main purpose is gathering intelligence.

**References** https://attack.mitre.org/groups/G0010/

**Attack Group** Inception
**Method of Attack** Link to .exe
**Targets** Private Sector Energy

Primarily targeting Russia, Inception are a cyber espionage group operating since around 2014. With a focus on multiple industries, they have conducted attacks against the US, the Middle East and throughout Europe.

**References** https://attack.mitre.org/groups/G0100/

# 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

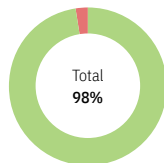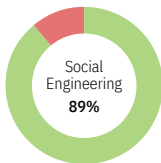Each service has a number of options when handling such threats. The tables show how each service handled each category.

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

### Trend Vision One Email and Collaboration Security

| Targeted Attack | Stopped | Blocked | Quarantine (admin) | Rejected | Edited (deny) | Quarantine (user) | Junk (deny) | Junk Folder | Junk (allow) | Edited (allow) | Inbox |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Business Email Compromise | 5 | 0 | 21 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Phishing | 95 | 0 | 72 | 0 | 1 | 0 | 132 | 0 | 0 | 0 | 0 |
| Social Engineering | 0 | 0 | 54 | 0 | 0 | 0 | 35 | 0 | 11 | 0 | 0 |
| Malware | 10 | 0 | 40 | 0 | 0 | 0 | 10 | 0 | 0 | 0 | 0 |
| **Total** | **110** | **0** | **187** | **0** | **1** | **0** | **177** | **0** | **11** | **0** | **0** |

Business Email Compromise **100%**

Phishing **100%**

Social Engineering **89%**
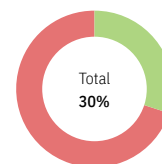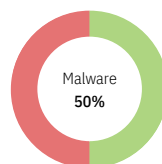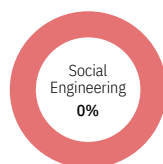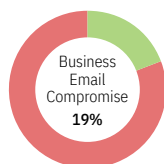
Malware **100%**

Total **98%**

## Google Workspace Enterprise Plus

| 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 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 22 |
| Phishing | 0 | 0 | 263 | 0 | 3 | 0 | 1 | 0 | 0 | 0 | 33 |
| Social Engineering | 0 | 0 | 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 96 |
| Malware | 0 | 0 | 20 | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 30 |
| Total | 0 | 0 | 291 | 0 | 13 | 0 | 1 | 0 | 0 | 0 | 181 |

Business Email Compromise **18%**    Phishing **89%**    Social Engineering **4%**    Malware **50%**    Total **63%**
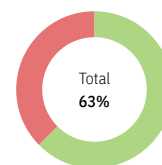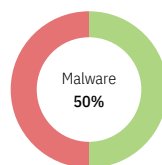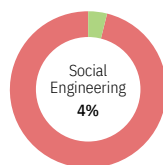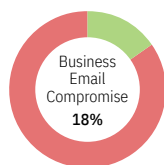
## mailcow: dockerized

| Targeted Attack | Stopped | Blocked | Quarantine (admin) | Rejected | Edited (deny) | Quarantine (user) | Junk (deny) | Junk Folder | Junk (allow) | Edited (allow) | Inbox |
|---|---|---|---|---|---|---|---|---|---|---|---|
| BEC | 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 21 |
| Phishing | 60 | 0 | 0 | 0 | 52 | 0 | 0 | 0 | 0 | 0 | 188 |
| Social Engineering | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 100 |
| Malware | 20 | 0 | 0 | 0 | 10 | 0 | 0 | 0 | 0 | 0 | 30 |
| Total | 85 | 0 | 0 | 0 | 62 | 0 | 0 | 0 | 0 | 0 | 339 |

Business Email Compromise **19%**    Phishing **37%**    Social Engineering **0%**    Malware **50%**    Total **30%**

## 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.

| Product | Inbox | Edited (allow) | Junk Folder | Quarantine (admin) | Blocked |
|---------|-------|----------------|-------------|--------------------|---------|
| Trend Vision One Email and Collaboration Security | 110 | 0 | 0 | 0 | 0 |
| Google Workspace Enterprise Plus | 99 | 0 | 0 | 11 | 0 |
| mailcow: dockerized | 110 | 0 | 0 | 0 | 0 |

## Appendix C: Product Version

The table below shows the service's name as it was being marketed at the time of the test.

| Vendor | Product | Build Version (start) | Build Version (end) |
|--------|---------|----------------------|---------------------|
| Google | Workspace Enterprise Plus | — | — |
| Open Source | mailcow: dockerized | 2024-08a | 2024-08a |
| Trend Micro | Trend Vision One Email and Collaboration Security | — | — |

# 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 8th July and 9th August 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.

# SE LABS