ipsip VN

Advanced Security Test Report

FlexSecure360

Email and Cloud Security

MAY 2025 | EMAIL PROTECTION

Introduction

Test Overview

IPSIP Vietnam tested FlexSecure360 Email and Cloud 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.

Objective

To provide an honest, objective and well-informed view of the email security platform's capabilities against business-focused attackers.

Advanced Security Test Report | Email Protection | FlexSecure360 Email and Cloud Security | May 2025

Introduction to IPSIP Vietnam

"This certification demonstrates our company's commitment to professional standards, security best practices, and continuous improvement."

It reflects our dedication to delivering reliable, high-quality solutions and maintaining trust with our clients and partners.

If you spot a detail in this report that you don't understand, or would like to discuss, please contact us. **IPSIP Vietnam** uses current threat intelligence to make our tests as realistic as possible.

Test email security against business-focussed attackers: Ignore Business Email Compromise test cases at your peril. Good security testing is realistic, using threats seen in real life.

Comprehensive defences: Comprehensive email security requires layered defences that integrate seamlessly with platforms like Google Workspace or Microsoft 365, providing advanced detection capabilities.

Proactive Approach: Security should be adaptive and proactive, ensuring that your organisation stays protected even as threats evolve.

Executive Summary

This test examined the effectiveness of Coro Email and Cloud Security against a wide range of threats that target enterprise and small business through email. **IPSIP Vietnam** used advanced targeted attack techniques to assess how well this service handles email cyber threats.

Coro Email and Cloud Security	Accuracy Score	Rating (%)
Protection Accuracy	4,545/4,860	94%
Threat Detection Rates	479/486	99%
Legitimate Accuracy	1,070/1,100	97%
Total Accuracy	**5,615/5,960**	**94%**

Advanced Security Test Award

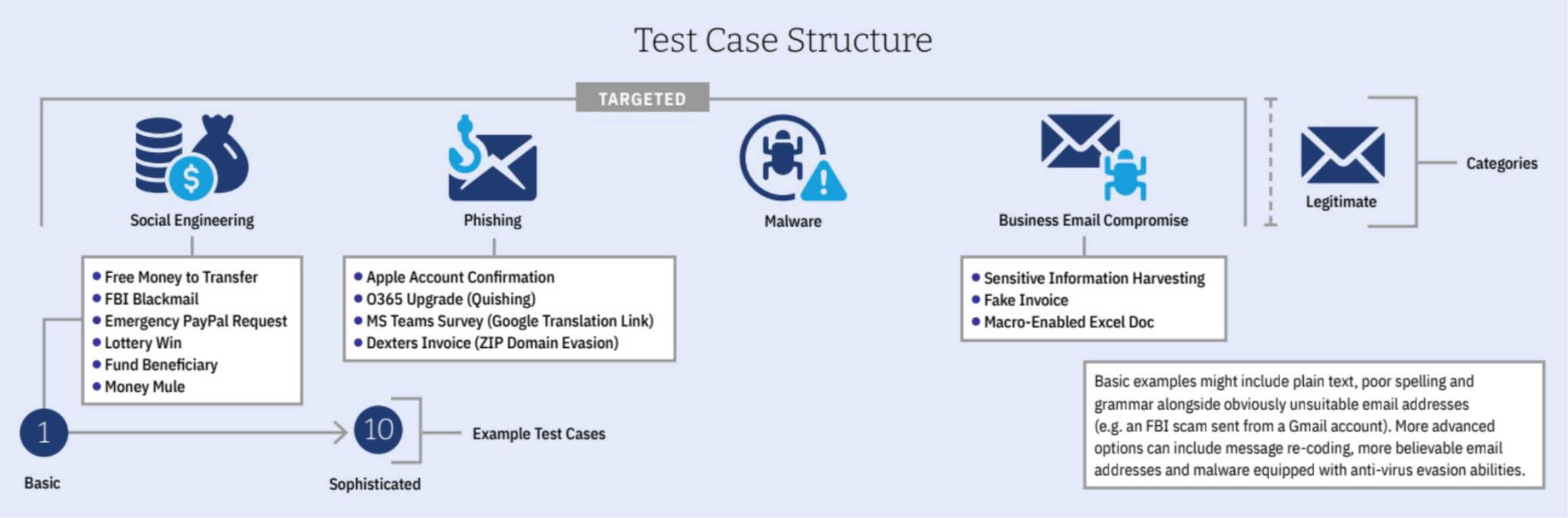
Outstanding Performance

Coro Email and Cloud Security achieved an overall Protection Accuracy Rating of 94%, missing only a few emails that employed social engineering and business compromise techniques.

These excellent scores contributed to Coro Email and Cloud Security's 94% Total Accuracy Rating and its AAA award.

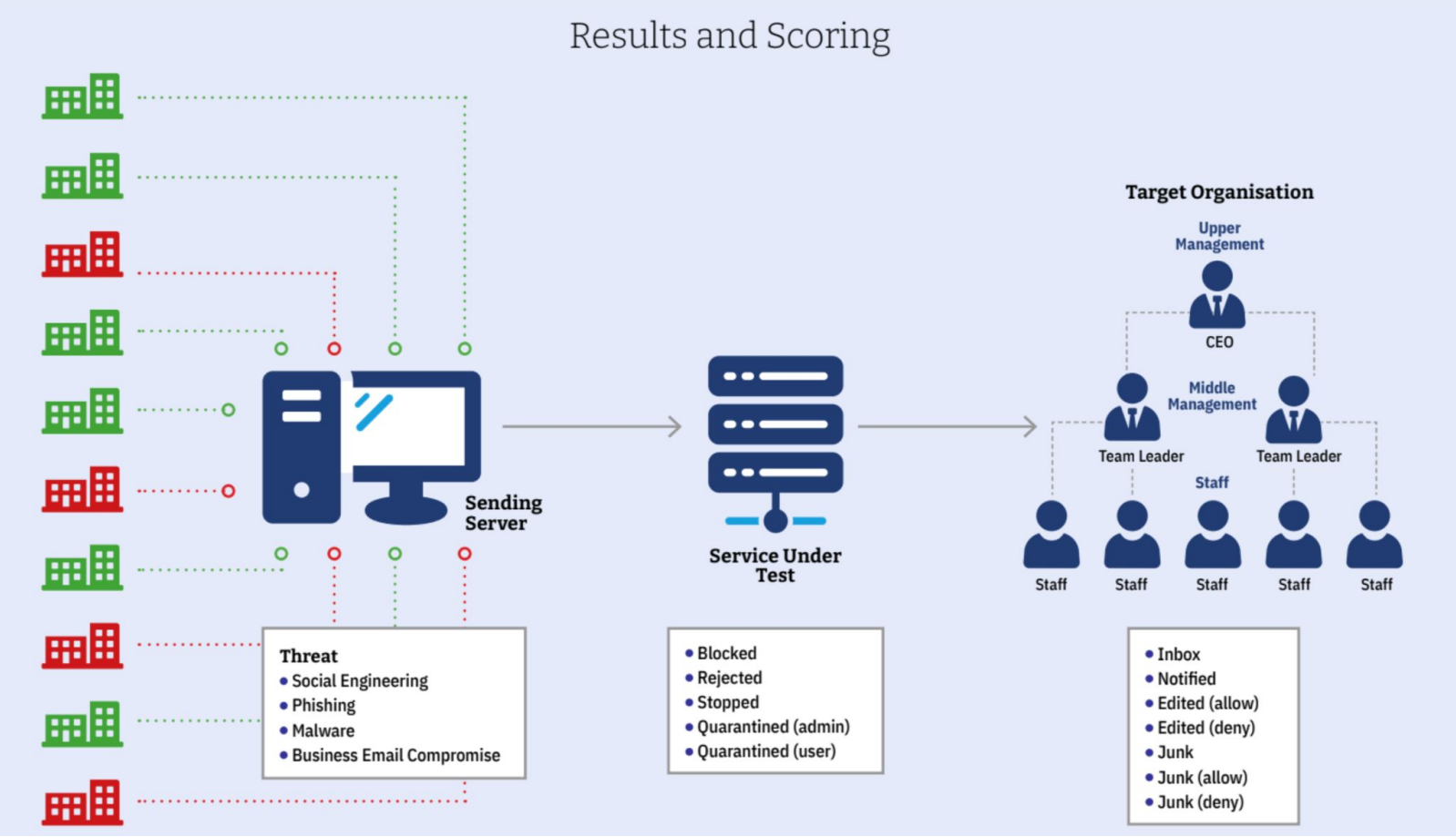
How We Tested

Targeted attacks comprise four categories: Social Engineering; Phishing; Malware; and Business Email Compromise. The goal is to test the effectiveness of each email security service and configuration when facing a range of different types of attacker.



Results and Scoring Architecture

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.



Attack Details

When testing services against targeted attacks, it is important to ensure that the attacks used are relevant. **IPSIP Vietnam** uses current threat intelligence to look at what the bad guys have been doing over the last few years and copied them closely.

Attacker/ APT Group	Method	Details
OilRig	Webpage to .exe	Driveby-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

Target Sectors & Attack Methods

KEY					
	Critical Infrastructure		Defense		Energy
	Financial Industries		Government Espionage		Research Institutes

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

1. Threat Detection Result

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.

Products Tested	Detection Rate	Misses	Detection Rate (%)
Coro Email and Cloud Security	479	7	**99%**

IPSIP Vietnam PRESENTS THE-C2

The-C2 is an exclusive, invite-only threat intelligence event that connects multinational business executives with the cutting edge of the cyber security industry.

Hosted by **IPSIP Vietnam**, it provides a route to understanding both the developing threat landscape and the evolving security measures for defending against attackers.

2. Total Accuracy Ratings

Judging the effectiveness of an email hosted protection service is a subtle art and many factors need to be considered. The rating takes into account not only each service's ability to detect and protect against threats, but also its handling of non-malicious messages.

Products Tested	Total Accuracy Rating	Total Accuracy Rating (%)
Coro Email and Cloud Security	**5,615/5,960**	**94%**

** Total Accuracy Ratings combine protection and false positives.*

3. Protection & Legitimate Handling

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.

Quarantined (Between +6 to +10 for threats; -6 to -10 for legitimate): Services that intervene and move malicious messages into Quarantine are awarded points depending on whether the user or admin can recover it.

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 security. Each such case loses 10 points. All legitimate messages routing correctly earn 10 points.

Scoring Different Outcomes

Action	Threat	Legitimate
Inbox	-10	10
Junk Folder	5	-5
Quarantined (admin)	10	-10
Quarantined (user)	6	-6
Notified	10	-10
Stopped	10	-10
Rejected	10	-10
Blocked	10	-10
Edited (Allow)	-10	10
Edited (Deny)	10	-10
Junk (Deny)	10	-10
Junk (Allow)	-7	7

Rating Calculations

Protection Rating Formula

```
Protection rating =
(10 x number of Stopped etc.) +
(6-10 x number of Quarantined) +
(5 x number of Junk) +
(-10 x number of Inbox)
etc.
```

Legitimate Rating Formula

```
Legitimate rating =
(10 x number of Inbox) +
(-5 x number of Junk) +
(-6-10 x number of Quarantined) +
(-10 x number of Stopped etc.)
etc.
```

These ratings are based on our opinion of how important these different outcomes are. You can use the raw data from this report to roll your own set of personalised ratings.

Accuracy Ratings Breakdown

Protection Accuracy Rating

Products Tested	Protection Accuracy Rating	Protection Accuracy Rating (%)
Coro Email and Cloud Security	4,545/4,860	**94%**

Legitimate Accuracy Rating

Products Tested	Legitimate Accuracy Rating	Legitimate Accuracy Rating (%)
Coro Email and Cloud Security	1,070/1,100	**97%**

4. Conclusion

This test exposed Coro Email and Cloud 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 compromise techniques and other types of social engineering.

Test results show that Coro Email and Cloud 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 99% of the attacks and was able to protect against 94% of them.

The product was very effective at recognising legitimate email and achieved an excellent Legitimate Accuracy Rating of 97%. This, combined with the 99% Detection Accuracy Rating and the 94% Protection Accuracy Rating, contributed to the 94% Total Accuracy Rating, an outstanding result which made Coro Email and Cloud Security deserving of its **IPSIP Vietnam AAA award**.

Appendix A: Attack Details (1/2)

OilRig (Energy)

Method: Webpage to .exe file

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.

Saint Bear (Government)

Method: Hidden link to .exe file

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.

MuddyWater (Defense)

Method: Hidden link to .exe file

A cyber espionage group linked to Iran's MOIS, active since 2017. It targets government and private sectors including defense, telecoms, and energy across multiple continents.

Appendix A: Attack Details (2/2)

APT38 (Financial)

Method: Zipped .exe

A North Korea-based threat group targeting banks, financial institutions, and cryptocurrency exchanges in over 30 countries. Notable attacks include the Bank of Bangladesh.

APT29 (Research)

Method: shellcode/exe

Based in Russia and linked to the foreign intelligence service. It targets government networks and research institutes using malicious PDFs with decoy documents.

Windshift (Critical Infra)

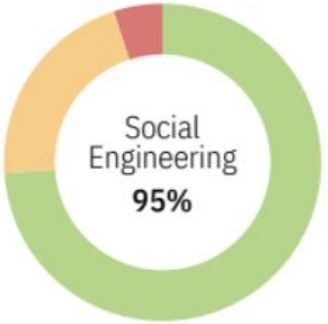
Method: Link to .exe

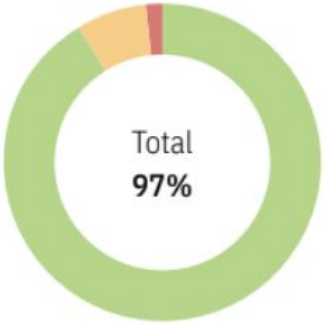
A threat group active since at least 2017, targeting specific individuals for surveillance in government departments and critical infrastructure across the Middle East.

Appendix B: Targeted Attack Visuals

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	7	0	1	0	2	14	0	0	2
Phishing	34	0	265	0	0	0	1	0	0	0	0
Social Engineering	1	0	73	0	0	0	0	21	0	0	5
Malware	0	0	40	0	20	0	0	0	0	0	0
Total	**35**	**0**	**385**	**0**	**21**	**0**	**3**	**35**	**0**	**0**	**7**





Targeted Attack Details Table

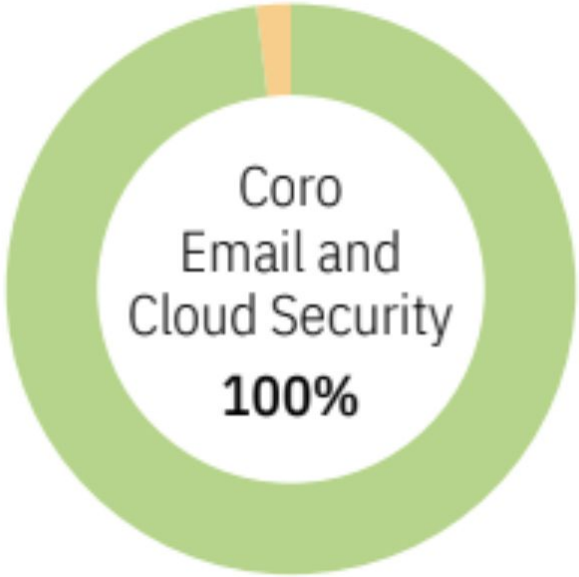
The table below summarises how they handled different categories of commodity threats. Not every possible option needs to be taken by a service under test, so the tables show only those outcomes that occurred.

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	7	0	1	0	2	14	0	0	2
Phishing	34	0	265	0	0	0	1	0	0	0	0
Social Engineering	1	0	73	0	0	0	0	21	0	0	5
Malware	0	0	40	0	20	0	0	0	0	0	0
Total	35	0	385	0	21	0	3	35	0	0	7

Legitimate Message Details

These results show how effectively the service managed messages that posed no threat. 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
Coro Email and Cloud Security	108	0	2	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)
Coro	Email and Cloud Security	2.5.65.1 (3.2)	2.5.75.1 (3.4.2)

Appendix D: Terms Used (1/2)

Notified: The service prevented the threat from being delivered and notified the user. There was no option 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.

Appendix D: Terms Used (2/2)

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

What is a partner organisation? Can I become one to gain access to the threat data used in your tests?

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.

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?

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.

IPSIP Vietnam Report Disclaimer

1. The information contained in this report is subject to change and revision by IPSIP Vietnam without notice.

2. IPSIP Vietnam is under no obligation to update this report at any time.

3. IPSIP Vietnam believes that the information contained within this report is accurate and reliable at the time of its publication, but does not guarantee this in any way.

4. The contents of this report does not constitute a recommendation, guarantee, endorsement or otherwise of any of the products listed, mentioned or tested.

5. 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.

6. 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.

ipsip

Contact us

We're here to help!

ipsip.vn

+84 91 885 30 68

sales-vn@ipsip.eu