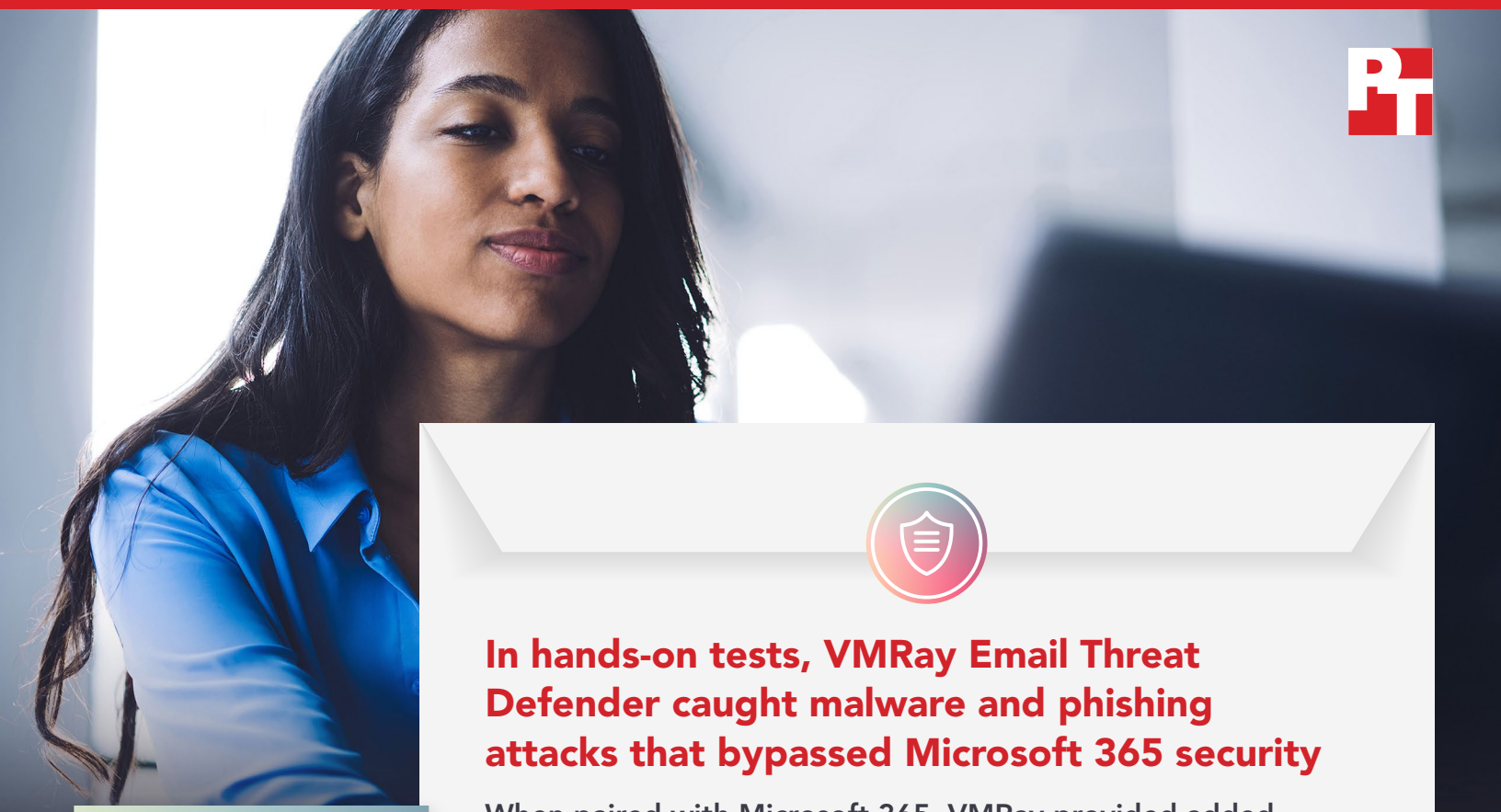


In hands-on tests, VMRay Email Threat Defender caught malware and phishing attacks that bypassed Microsoft 365 security

When paired with Microsoft 365, VMRay provided added protection against novel attacks, sophisticated malware, and phishing attempts

On a Microsoft 365 Enterprise E3 account:

13 additional types of malicious emails detected

On a Microsoft 365 Enterprise E5 account:

5 additional types of malicious emails detected

People are often the weakest links in an organization's security chain. Despite the powerful advancements in server, processor, and personal computer security that make it difficult for hackers to simply take data by brute force, just one high-value employee accidentally clicking on a malicious email URL is all it takes to render many of these defenses useless.

As email attacks aimed at employees grow ever more prevalent and sophisticated, security teams are looking for tools to help keep their sensitive data secure. Though Microsoft 365 offers its own email security features, sometimes threats can still slip through.

VMRay Email Threat Defender (ETD) is a supplemental tool for Microsoft 365 that can help enhance organizational security by adding an extra layer of security and reducing the opportunities for employees to be deceived. At Principled Technologies, we tested VMRay Email Threat Defender with two Microsoft 365 offerings that had the following configurations:

- Standard-preset Microsoft Exchange Online Protection (EOP) policies consistent with a Microsoft 365 E3 deployment
- Standard-preset Microsoft Defender for Office 365 and Standard-preset EOP policies consistent with a Microsoft 365 E5 deployment

In our tests, we found that supplementing the standard Microsoft 365 Defender and EOP policies with VMRay ETD increased protection against various types of threat, including malicious file types within email attachments, types of password-protected archives containing malware, malicious URLs in documents, and more.

Our results

Tables 1 and 2 give a breakdown of the type and quantity of threats that VMRay Email Threat Defender identified where Microsoft policies alone did not. Though Microsoft policies caught several types of malicious emails in each account, VMRay Email Threat Defender extended this protection to cover additional types of threats.

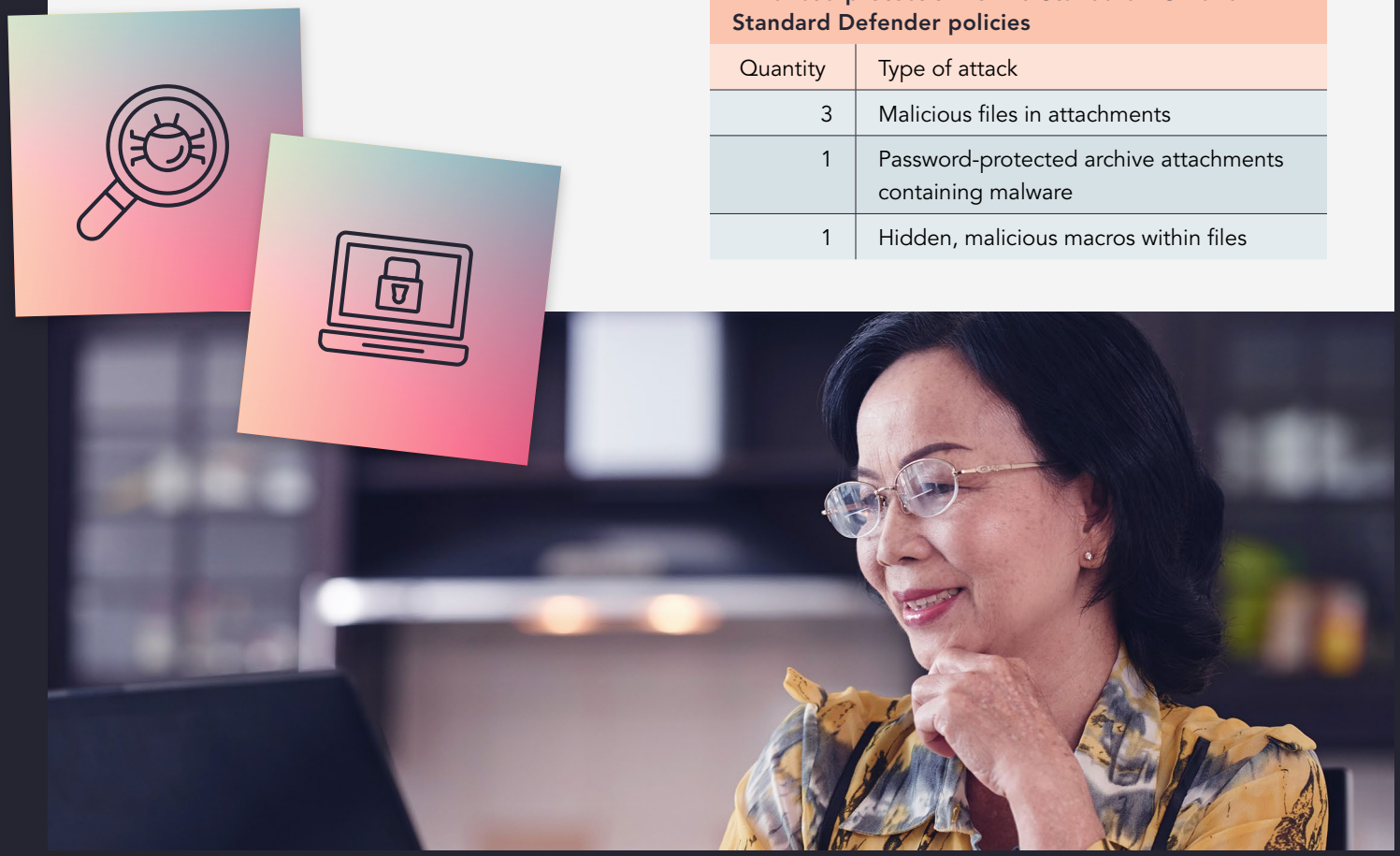
Microsoft 365 E3 with EOP offers basic protection, and Microsoft 365 E5 with EOP and Microsoft Defender offers the best recommended standard protections for a typical user without introducing a large number of false positives. Our testing shows that VMRay Email Threat Defender can supplement these robust sets of security policies for additional peace of mind.

Table 1: Types of attack that VMRay Email Threat Defender identified for the E3 account that Microsoft EOP alone did not. Source: Principled Technologies.

Enhanced protection for E3 Standard EOP policies	
Quantity	Type of attack
4	Malicious files in attachments
2	Password-protected archive attachments containing malware
2	Hidden, malicious macros within files
1	Malicious URL within a document
4	Obscured or shortened URLs within the email body

Table 2: Types of attack that VMRay Email Threat Defender identified for the E5 account that Microsoft EOP and Defender alone did not. Source: Principled Technologies.

Enhanced protection for E5 Standard EOP and Standard Defender policies	
Quantity	Type of attack
3	Malicious files in attachments
1	Password-protected archive attachments containing malware
1	Hidden, malicious macros within files



How we tested

We deployed two accounts within Microsoft 365 using security policies consistent with either an E3 EOP or E5 EOP and Microsoft Defender deployment. E3 and E5 are enterprise subscription plans for Microsoft 365, with E5 offering more advanced security settings than E3. The E5 plan uses the cloud-based Microsoft Defender for Office 365 in conjunction with Microsoft EOP policies. After configuring each account with VMRay Email Threat Defender, we began our tests.

We sent to each account a set of email messages, each of which contained a particular type of threat (such as malicious links and attachments) to see which threats were still able to reach each account's inbox. When an email did not arrive at the inbox, we checked the Microsoft and VMRay quarantines. We configured VMRay Email Threat Defender to process emails only after Microsoft 365 security features had a chance to respond. Therefore, any emails caught within the VMRay Email Threat Defender quarantine would not have been picked up by Microsoft 365 alone. Email Threat Defender can scan emails at earlier points, but we did not test those features.

We generated each attack type in one of two ways: either by obtaining (and altering, if necessary) threat samples from third-party websites that collect samples for security professionals, or by using recent threat samples that VMRay has obtained from its customers (after scrubbing all sensitive information). Because we used live threats, our samples were limited by the number of threats available around the time of testing.

Note that in this report, we have purposefully obfuscated or omitted sensitive details that could lead bad actors to identify and exploit vulnerabilities we found in our testing. For some additional details, see the science behind the report.

About VMRay Email Threat Defender

According to the VMRay website, Email Threat Defender fully automates inbound email scanning by analyzing attachments and links before an email can land in a user's inbox. Rather than fully replace an email app's existing security features, VMRay works to enhance native protection as a second layer of defense, integrating with Microsoft Defender APIs and connectors and sharing its analytics with other security tools.

To learn more about Email Threat Defender, visit https://www.vmray.com/products-email-threat-defender-etd/.

Conclusion

The best data center security in the world may be unable to stop a hacker if one gains access to a high-value account via a convincing phishing email. To reduce the likelihood of a successful attack, it can help to supplement your organization's existing email security tools for an added layer of protection.

In our tests, we found that VMRay Email Threat Defender enhanced the native security of Microsoft 365 E3 and E5 accounts by protecting against more types of malicious email attacks—13 types of attacks beyond E3 protection and 5 types of attacks beyond E5 protection. Adding VMRay Email Threat Defender to your Microsoft 365 deployment could help prevent successful phishing attempts and help keep your business safe. Just one malicious email reaching the right inbox is enough opportunity to compromise critical organizational assets as well as employee and customer data.

For more information, visit https://www.vmray.com/solutions/close-the-gaps-in-your-office-365-email-security/.

Read the science behind this report at https://facts.pt/iHN6LLy ►

Principled Technologies®

Facts matter.®

Principled Technologies is a registered trademark of Principled Technologies, Inc.
All other product names are the trademarks of their respective owners.
For additional information, review the science behind this report.

This project was commissioned by VMRay.