Datasheet

VMRAY Email Threat Defender

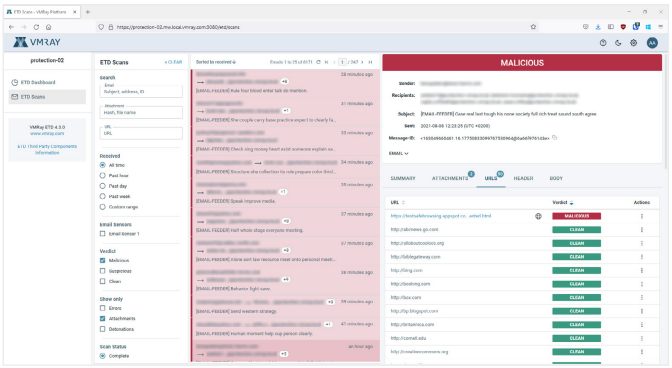
Closing The Gaps In Your Email Security

Challenge

One of email security's most persistent challenges is the inability to stay ahead of cybercriminals who continue developing new ways to evade the security controls in secure email gateways and cloud email services like Microsoft Office 365. While the volume, sophistication, and diversity of email-borne threats continue growing, so does alert fatigue among the security team.

From monitoring suspicious activity and analyzing security alerts to managing false positives and interacting with users, your security team is overloaded with vast amounts of incident data, often from various data sources. Your security team doesn't always know whether it is "noise" or valuable forensics when hunting down incidents. Yet when an email attack hits the organization, it is expected to be detected and contained with no delay.

Solution



VMRay Email Threat Defender closes the gaps your email security leaves exposed with a laser-focused solution for providing the industry's most robust threat detection and the lowest number of false positives. This solution achieves unmatched detection efficacy by using VMRay's unique agent-less sandboxing technology for threat analysis at scale without shortcuts that compromise effectiveness. Because the VMRay sandbox does not provide a surface cybercriminals could detect, exploit, or circumvent, it is resistant to highly evasive malware.

Unlike other solutions that rewrite URLs and only analyze links at the time of click, Email Threat Defender provides URL protection at the time of delivery, complementing the trade-offs of time-of-click approaches. The advantage of automatic URL analysis at email delivery is that it wins precious time, sufficient for a complete comprehensive multi-stage scanning workflow including user behavior emulation, computer vision, and other advanced techniques. In most cases, it detects a malicious link long before the user can click on it.

Evasive malware, spear-phishing, and zero-day threats missed by your first line of defense stand no chance.

And because Email Threat Defender seamlessly augments existing security controls, you maximize your security investments and avoid a complex, costly, and often disruptive replacement, resulting in a higher return on investment faster.

Key benefits

- Protect your mailboxes from evasive malware, spear-phishing, and zero-day threats that other security products miss
- Automatically detect malicious files and URLs before your users can interact with them
- Eliminate alert fatigue in the security team with noise-free analysis, clear verdicts, and response automation
- Seamlessly strengthen email security efficacy without a complex, costly, disruptive replacement
- Secure your Office 365 mailboxes within minutes via an easy-to-use API

Why is it unique?

- Evasion-resistant technology that provides the industry's most robust threat detection and the lowest number of false positives
- Automatic file and URL scanning at time of email delivery to complement the limitations of URL rewrites and Safe Links at the time of click
- Analyses of URLs in documents, password-protected attachments, nested files, URL rewrites, Safe Links
- Retrospective scans to identify rearmed malicious URLs

VMRAY

VMRAY Email Threat Defender

How it works

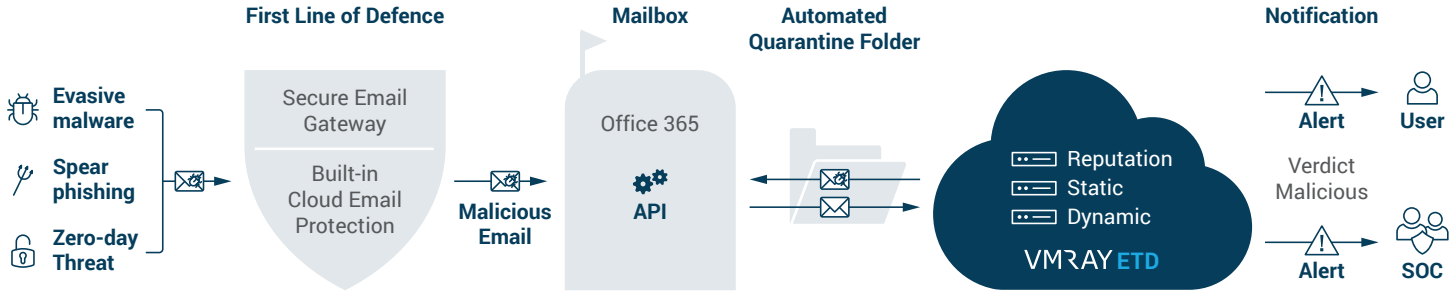
The VMRay Email Threat Defender sits behind your secure email gateway or the protection that comes with, for example, Microsoft Office 365, scanning every email at the time of delivery for threats that slip through the net.

It automatically extracts and analyzes all files and URLs – including links in documents, password-protected attachments, nested files, and URL rewrites or Safe Links—through a fast and accurate multi-stage analysis workflow that combines reputation lookup and static scans with VMRay's unique evasion-resistant sandboxing technology.

Once an email is identified as malicious, the security team and recipient immediately receive a warning. The system automatically moves the email to a quarantine folder, preventing it from infiltrating your network and compromising or disabling your computers.

Reporting is varied and comprehensive, from high-level dashboard views and clear verdicts to detailed noise-free reports of specific incidents, allowing your team and others to prioritize and contain incidents confidently and quickly.

Deployed in the cloud, Email Threat Defender integrates with your Microsoft Office 365 email service through the built-in API within minutes, with no changes to your MX records. Other email systems – whether cloud-delivered, on-premises, or hybrid—are supported via BCC forwarding.



Key Values

The VMRay Email Threat Defender seamlessly supplements the security controls in your Microsoft Office 365 email service and other email systems to ensure no malicious email slips through. With Email Threat Defender, you empower your organization to:

- **Gain unparalleled detection efficacy** – see all evasive malware, spear phishing, and zero-day threats that others miss.
- **Eliminate alert fatigue** – detailed noise-free reports and clear verdicts enable everyone to contain email-borne threats confidently and quickly.
- **Automate mailbox protection** – automatically move a malicious email to a quarantine folder, preventing the recipient from opening it and spreading any malicious contents.

Don't delay – try VMRay Email Threat Defender for free!

See the malicious emails that slip through Microsoft Office 365 and free your organization from the burden of email security.

Get your free trial

ABOUT VMRAY – MALWARE ANALYSIS INNOVATION IS IN OUR DNA.

At VMRay, we are focused on a single mission: to help organizations of all sizes protect themselves against the growing global malware threat. Our automated malware analysis and detection solutions help enterprises around the world minimize business risk, protect their valuable data and safeguard their brands.