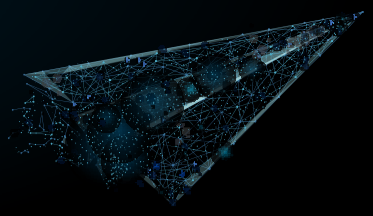
VMRAY ETD

EMAIL THREAT DEFENDER

Bring X-Ray Vision to your Email Defenses



Data Sheet

Fast, Accurate Enterprise Email Threat Detection

Given their heavy reliance on email communication, enterprises put a high premium on fast, accurate detection of email threats. Addressing this ubiquitous challenge, VMRay Email Threat Defender (ETD) delivers an extra level of email defense for large, security-minded organizations.

Based on VMRay's industry-leading sandboxing solution for malware analysis and detection, VMRay Email Threat Defender subjects email attachments and URLs to a multistage winnowing process. In milliseconds, the system identifies and dismisses benign elements while submitting suspected malware to increasing levels of scrutiny.

VMRay's solution detects even the most evasive malware threats. In turn, detection results can be used by diverse security systems to automate block/allow decisions and other protection measures.
While VMRay Email Threat Defender is not an anti-spam or anti-phishing solution, it complements those tools and fills the security gaps they leave. The solution can be deployed in the cloud or on-premises.

Analysis & Detection of Malicious Email at Scale

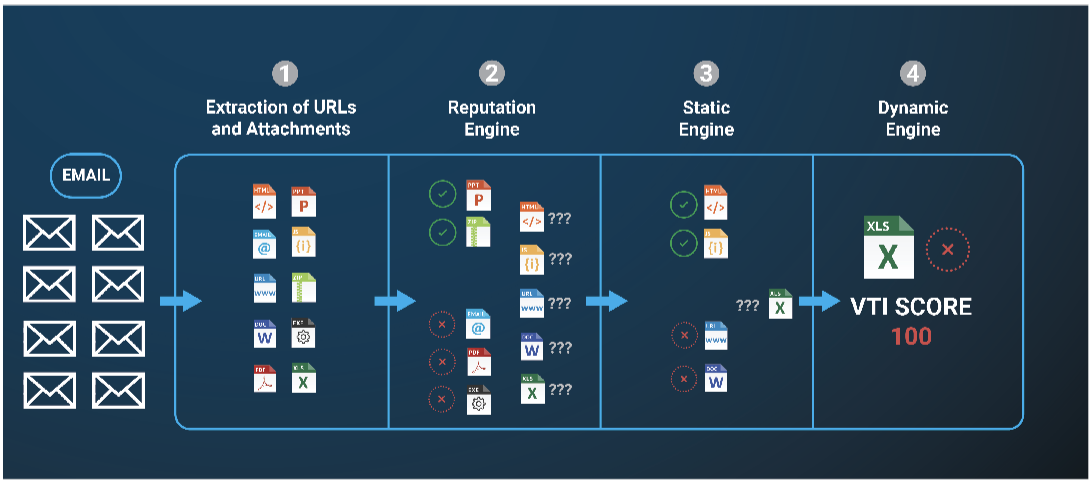


Figure 1. Email Analysis Workflow

Key Benefits

- Groundbreaking technology detects highly evasive malware that other platforms miss.
- Accurate detection, without human intervention, reduces false positives that divert SOC staff from more critical tasks.
- Solution scales to support increased email volumes without hurting performance or TCO.
- Complements anti-spam and anti-phishing solutions.
- Can be deployed in the cloud or on-premises.

Features

- **Scans incoming mail** and extracts potentially malicious attachments and URLs, which are subjected to an escalating detection process.
- **Email users are auto-notified** when an email has been compromised.
- **Detection** results can be used by other security tools to automate block/allow actions.

VMRAY

VMRAY Email Threat Defender

The Power of VMRay's Now, Near, Deep Architecture

VMRay Email Threat Defender is based on VMRay's groundbreaking sandboxing platform for malware analysis and detection and our Now, Near, Deep architecture, illustrated below. Because the sandbox is agentless and hypervisor-based, it is invisible to malware and detects even highly evasive strains other solutions miss.

The multistage detection process integrates three core components: rapid reputation lookup, static analysis, and dynamic analysis of malware behavior.

Now: Rapid Reputation Lookup

Email attachments and embedded URLs are submitted to the reputation engine. In milliseconds, benign samples are identified and dismissed, receiving no further attention. Unknown and suspicious URLs and files are handed off to static analysis for further examination.

Near: Static Analysis Reveals Active Elements

In seconds, static analysis looks at embedded scripts, macros and other active elements that could be part of a multistage threat. Safe files are dismissed, while those with higher severity scores are submitted for dynamic analysis.

Deep: Dynamic Analysis Enhances Accuracy

Isolated in VMRay's malware sandbox, suspected malware is allowed to execute without interruption. Based on the observed behavior, confirmed malware will be flagged as malicious by the VMRay Threat Identifier (VTI) severity score.

Auto alerts are sent to the affected email users. Machine-readable detection results can be shared with other security tools automate protective actions and inform incident response. The enhanced accuracy provided by dynamic analysis distinguishes VMRay's solution from other platforms.

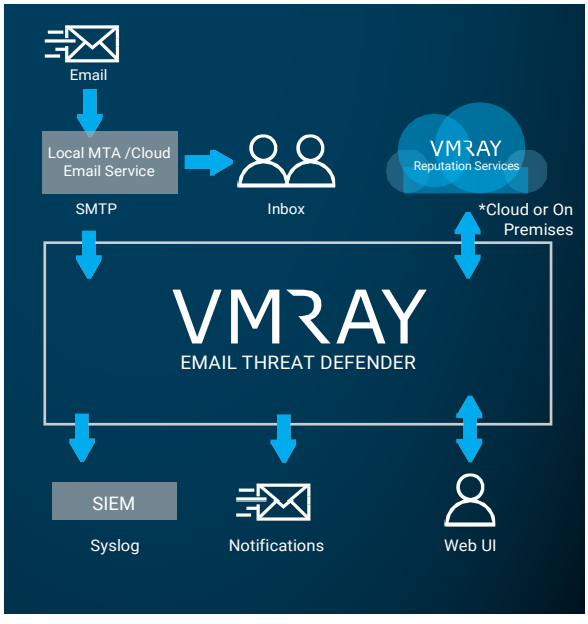


Figure 2: Deploying VMRay ETD

Key Facts

Platforms: Windows, macOS

Coverage: Full range of file types and URLs

Deployment: Cloud or on-premises

Integration: 25+ built-in connectors for web, email, SOAR, EPP/EDR and other tools

Compliance: GDPR-compliant, ISO-27001 certified

Support for industry standards: MITRE ATT&CK™ Framework, YARA rules, STIX™ and others

Tailored environments: Golden images and cloud localization for optimizing detection of targeted malware

Let's Talk

Contact us at sales@vmray.com or call +49 234 973 55 40 0

Contact Us