DATA SHEET

VMRAY

VMRAY EMAIL THREAT DEFENDER

Fast, accurate email threat detection for enterprises

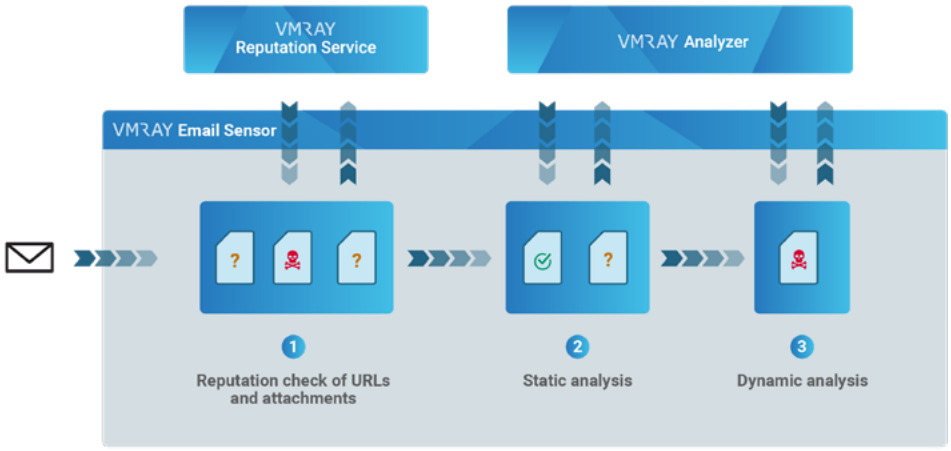
Given their heavy reliance on email communication, enterprises put a high premium on fast, accurate detection of email threats. Addressing this ubiquitous challenge, VMRay Email Threat Defender delivers an extra level of email defense for large, security-minded organizations.

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 known or 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



VMRay Email Threat Defender's automated work-flow for high-volume analysis and detection.

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.

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.

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.

THERE'S NO TIME LIKE THE PRESENT

Get an up-close look and a hands-on feel for how VMRay Email Threat Defender can help strengthen your organization's malware defenses. Sign up today for a 30-day free trial.

CONTACT US