EMAIL SENSOR
Automated Analysis and Detection of Malicious Email

Introduction

The VMRay Email Sensor enables organizations to protect their email infrastructure from malware and targeted attacks using VMRay's unique agentless threat detection. The sensor can be integrated into any email deployment with minimal configuration adjustments to email gateways.

VMRay Email Sensor scans the email for known malicious URLs that lead to malicious downloads. Furthermore, it extracts attached files and sends them to a VMRay Analyzer installation for further investigation.

Please note VMRay's email protection serves as the last link in the entire protection chain and is not a spam or phishing protection solution. To ensure best performance, we recommend first scanning emails using common anti-spam and anti-virus engines before submission to the email sensor.

Key Benefits

- Automated analysis and detection of potentially malicious attachments using VMRay's evasion resistant analyzer

- Scans inbound email for known malicious URLs that lead to malicious downloads

- Easy deployment with your existing email infrastructure
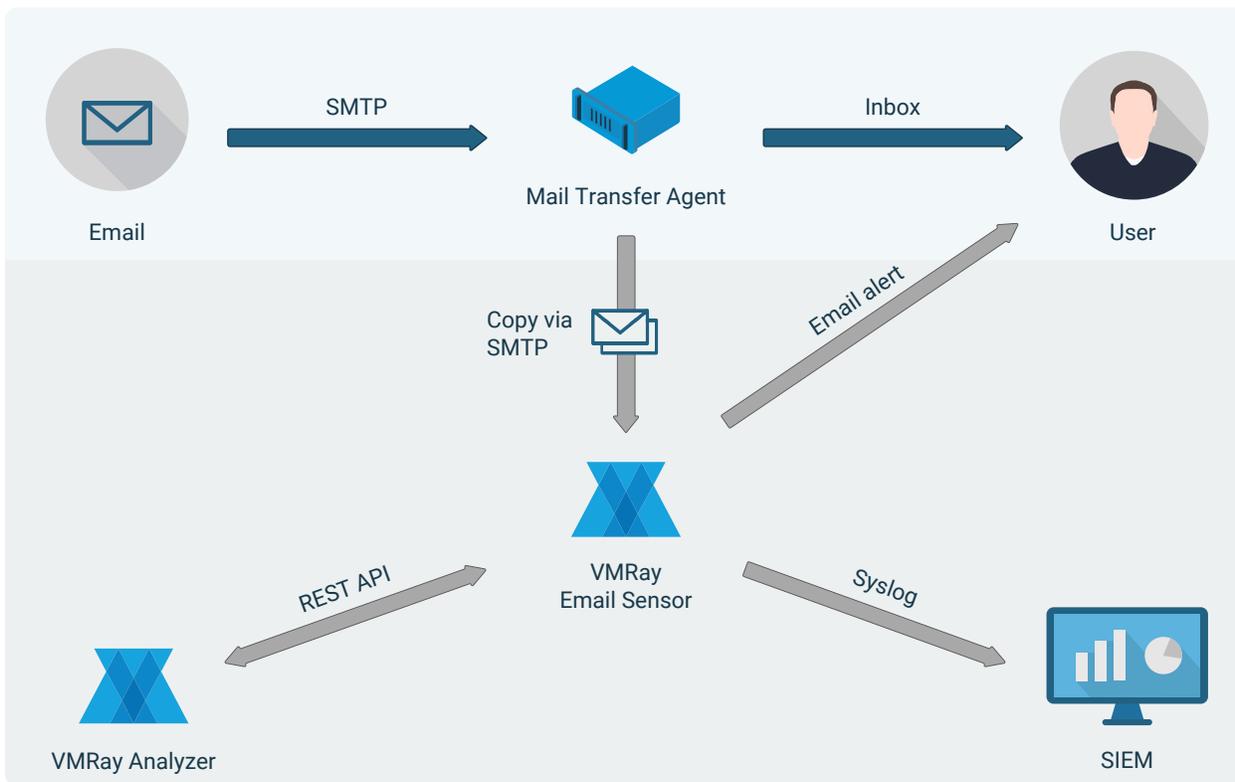
Deployment Details

The VMRay Email Sensor must receive emails from a mail transfer agent (MTA) using the SMTP protocol. It then detects advanced email threats by analyzing the URLs and attachments contained in the email. The maliciousness of URLs is determined by the VMRay Reputation Engine. Attachments are processed using file triage and dynamic analysis. The deployment is depicted in the following figure on page 2:

The mail transfer agent (MTA) must be configured so that a copy of every email that needs to be scanned is sent to VMRay Email Sensor using SMTP. In the simplest scenario, a copy of every email is sent to the VMRay Email Sensor.

When the analysis is completed, results can be sent to a Security Information and Event Management (SIEM) system using syslog in a JSON-based or custom format for further insights and advanced correlation. The format and kind of data that is transmitted is configurable.

VMRay Email Sensor Deployment

Alternatively, the system can also send an email alert directly to the user if a malicious attachment was identified. Please note that this is a non-blocking, out-of-bound deployment scenario. The email will be forwarded to the user in any case in parallel to the actual analysis.

To get started, you need to install the VMRay Email Sensor on an Ubuntu 16.04 machine and a running deployment of VMRay Analyzer (either Cloud or On-Premises). It is possible to run the VMRay Email Sensor and VMRay Analyzer on the same machine.

Protect Your Organization From
Malicious Email with VMRay Analyzer

START YOUR TRIAL