

## Ayehu and VMRay

# Automated Malware Detection and Blocking



Ayehu, the IT automation and security orchestration platform, integrates with VMRay Analyzer, the hypervisor-based threat analysis and detection solution, to help organizations block malware and malicious software across their datacenters and applications in an automated way.

### Benefits

- Easily automate security incident response
- Reduce arduous manual investigation tasks
- Enhance incident detection and remediation
- Quickly disable a risky user or terminate a process
- Notify the person on-call and escalate if needed

---

### Features

- Cross-platform Incident detection
- Device quarantine
- Policy automation
- Intelligent decision-support

### The Challenge

Today's datacenter—from on-premises to cloud—is inundated with a continuous flow of data such as files, links, and emails rapidly moving in and out, unchecked. From emails including links, attachments such as PDFs to binary files, the sheer volume of data exchange is leaving the organization vulnerable to security breaches through malware or exfiltration of sensitive data via third-party applications.

In an effort to prevent potentially risky files from entering the datacenter and potentially compromise the entire infrastructure, organizations are challenged with arduous forensics and mitigation processes that involve a series of manual, repetitive checks to the system, increasing the potential for human errors that produce catastrophic results.

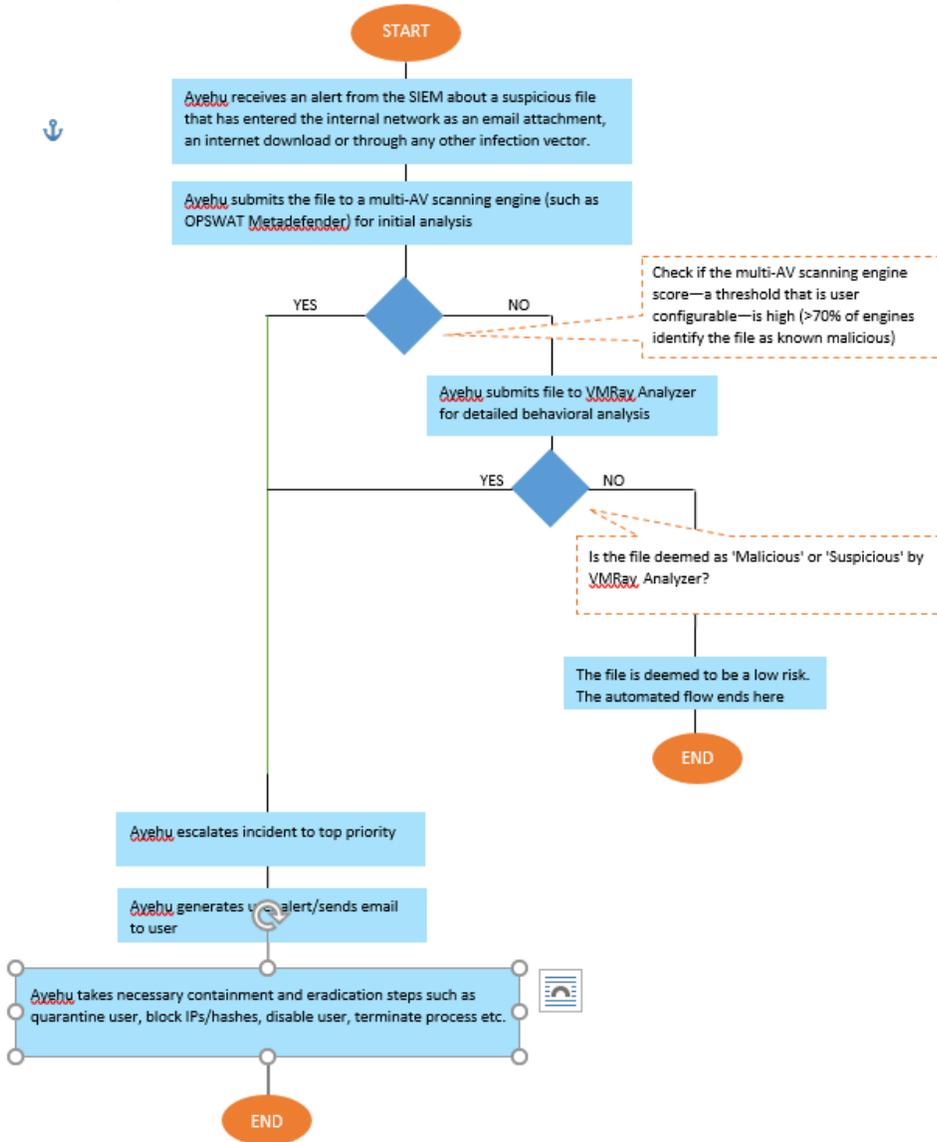
### Integration Overview

For security teams that require speed and accuracy of incident resolution, the Ayehu integration with VMRay Analyzer works in tandem to detect, isolate and block malware from the datacenter. Leveraging Ayehu's intelligent decision-support embedded within the platform, you can quickly set up automated security playbooks between Ayehu and VMRay, including the ability to:

- Effectively pinpoint and isolate malware before it spreads
- Significantly increase incident detection, while effectively filtering out noise
- Mitigate risk from a compromised device through automatic quarantine

# Intelligence-Driven Security Orchestration

The Ayehu and VMRay integration liberates the security team by removing time-consuming and error-prone incident detection and investigation, freeing up their time to focus on truly critical security issues. Simple, powerful automated playbooks can be implemented and working in a matter of minutes, such as detecting a potentially suspicious file:



## About Ayehu

Recently named by Gartner as a 2016 Cool Vendor, Ayehu helps IT and Security professionals to identify and resolve critical incidents, simplify complex workflows and maintain greater control over IT infrastructure through automation. Ayehu automation & orchestration solutions have been deployed by major enterprises worldwide and currently support thousands of IT processes across the globe.

## About VMRay

VMRay Analyzer combines rapid reputation scoring of files with a unique agentless hypervisor-based monitoring approach for deep analysis. With this combination VMRay Analyzer delivers rapid threat detection at scale coupled with the most comprehensive dynamic threat analysis in the industry.