REVERSINGLABS

File Inspection Engine

Enterprise Scale File Inspection

Problem

Security vendors need file inspection to enable functionality for analyzing files for malicious content or other security threats. However, this is a complex and time-consuming task for many vendors.

Solution

Integrating the ReversingLabs File Inspection Engine (FIE) into your existing platform can swiftly address this issue with minimal customization or effort. Our engineering team will ensure the FIE remains up-to-date and delivers the latest commercial analysis.

The ReversingLabs FIE addresses the limitations of current file scanning solutions by leveraging Spectra Analyze and localized Spectra Intelligence Threat Data to provide accurate verdicts on scanned files.

Utilizing ReversingLabs Spectra Analyze technology, the FIE employs machine learning-powered static analysis and reputation lookups at scale to effectively analyze a wide range of file types.

Deployment

The FIE is a container-based image designed for file scanning. It is intended for deployment in Docker or Kubernetes environments and is exclusively accessible via API. The FIE operates independently, without additional containerized services like databases or queuing engines. It is commonly integrated with Security Orchestration, Automation, and Response (SOAR) systems or Threat Intelligence Platforms (TIP).

Reversinglabs has many existing integrations for commercial platforms and a complete Python Software Development Kit (SDK) https://pypi.org/project/reversinglabs-sdk-py3/ to enable users to develop customer integrations with the FIE.

Key FIE Features

- Simple Verdict: Ok / Suspicious / Malicious
- Small Containerized Footprint
- Default Port 9000
- Over 4000 file types supported
- Support for files up to 5GB
- Comprehensive Depth of scan
- Support for Concurrent execution

Users can upload a file and obtain a verdict in the same HTTP session. The FIE is not meant to be exposed to public networks but used in private environments to scan files. Some level of integration is required.

The FIE is based on ReversingLabs Spectra Core technology and has the same feature set: best-in-class static analysis combined with up-to-date best-in-class Threat Intelligence.

System Requirements

Supported Operating System – Docker or Kubernetes x86 Linux-based operating systems

Sample - Container Resource Requirements for up to 5GB processing

- CPU Cores: 16
- RAM: 64GB
- Disk: 500GB

Conclusion

The ReversingLabs File Inspection Engine (FIE) offers a robust solution to the challenges faced by internal security teams with their current file scanning tools. Its containerized design ensures seamless integration within Docker or Kubernetes environments, requiring minimal additional infrastructure. With support for over 4000 file types and files up to 5GB, the FIE stands out for its comprehensive scanning capabilities and concurrent execution support.

This makes the FIE an ideal choice for organizations looking to enhance their security posture without compromising performance or budget constraints. In summary, the FIE is a powerful, adaptable, and efficient tool that empowers security teams to achieve greater accuracy and efficiency in their file-scanning processes.

Partnering with ReversingLabs unlocks the full potential of your security solutions. Visit partners.reversinglabs.com to explore how our advanced file inspection and threat intelligence can enhance your offerings. Contact us today to start a conversation about collaboration opportunities!

Get started!

Experience the ReversingLabs Difference

REQUEST A DEMO

reversinglabs.com

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

DS-Rev-10.09.24

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com