CYREN

Cloud Sandbox Array

Advanced Threat Detection

Detect first and get full forensics on evasive zero-day threats with Cyren's sandbox array in the cloud

CYREN Threat Intelligence

Cyren's Cloud Sandbox Array service allows service providers and Cyren solution partners to easily deploy the next generation of sandboxing analysis, integrating a powerful security layer via Cyren's ThreatLookup API for enhanced web protection, email protection, endpoint protection or breach response.

Innovative Cloud Sandbox Array fully analyzes objects — and fast

Today's threats are altering their behavior along numerous dimensions in order to avoid detection by traditional technologies, requiring a new level of sophisticated analysis—and accompanying processing power—in order to fully identify malicious behavior at speed. Cyren's patent-pending cloud sandbox array technology uses a sophisticated natural language processing decision engine to ensure that objects are completely understood and all intelligence is captured and reported, including risk factors, indicators of compromise, and the details of artifacts like dropped files. Integrated cloud sandbox array capabilities include:

- Iterative multi-sandbox analysis which exposes files to not only different environments, but also varied sandbox engines
- Hybrid static and dynamic analysis running on both virtual and physical machines
- HTTPS inspection for analyzing encrypted network traffic
- Intrusion detection for detecting suspicious network traffic
- Internet simulation for unreachable domains
- Automated human interaction simulation (e.g., key strokes, mouse movements)
- Consolidated multi-sandbox analysis reports (JSON format)

Easily deployed for scalable protection

As a cloud-delivered service, it can be quickly deployed, requiring minimal set-up and configuration of the API calls, and scales easily and automatically utilizing Cyren's highly elastic global cloud infrastructure. The only prerequisites for using the service are connectivity to threatlookup.com via HTTPS and possession of a token API Key.

The Cloud Sandbox Array Difference

Cyren's patent-pending sandbox array technology is a fundamental step forward in the battle against hyper-evasive malware, providing:

Superior Detection

- **Cyren has automated the complex process of file analysis usually done manually by malware researchers, producing better analysis and deeper zero-day threat intelligence.**

Unlimited Scalability

- **As Cyren's sandbox array is purpose-built for cloud computing across Cyren's global infrastructure, it allows us to scale easily, utilizing highly elastic computing power to identify malicious behavior with both greater depth and speed.**

Faster Analysis

- **In many cases, a file's risk profile can be determined even before the actual dynamic analysis on the sandbox starts.**

Google Microsoft Check Point SOFTWARE TECHNOLOGIES LTD. DELL Deutsche Telekom

25B
Security Transactions Daily

1.3B
Users Protected

300M
Threats Blocked Daily

CYREN

CYREN SANDBOX ARRAY

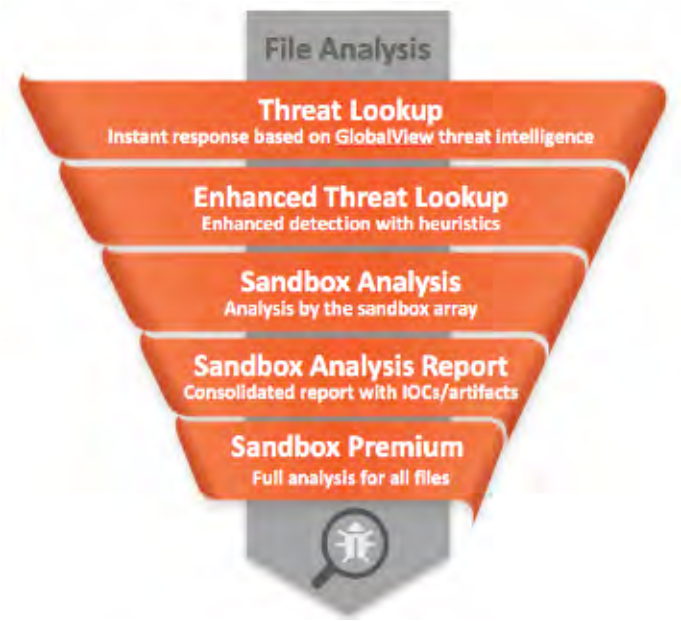
Advanced Threat Detection

Full Integration with Cyren Threat Intelligence Cloud

Cyren's sandboxing array is an integral component of our GlobalView™ Threat Intelligence Cloud. This allows layered treatment of objects uploaded for analysis, giving service providers, ISV's and appliance manufacturers several options in selecting the depth of analysis which best meets their objectives, thus guaranteeing efficiency in the return of results.

Solution partners can choose from five levels of service packages, ranging from instant evaluation via Threat Lookup to Sandbox Premium, which delivers a complete level of analysis and reporting for every file submitted. Each service package includes the features of the previous level.

CYREN Threat Intelligence



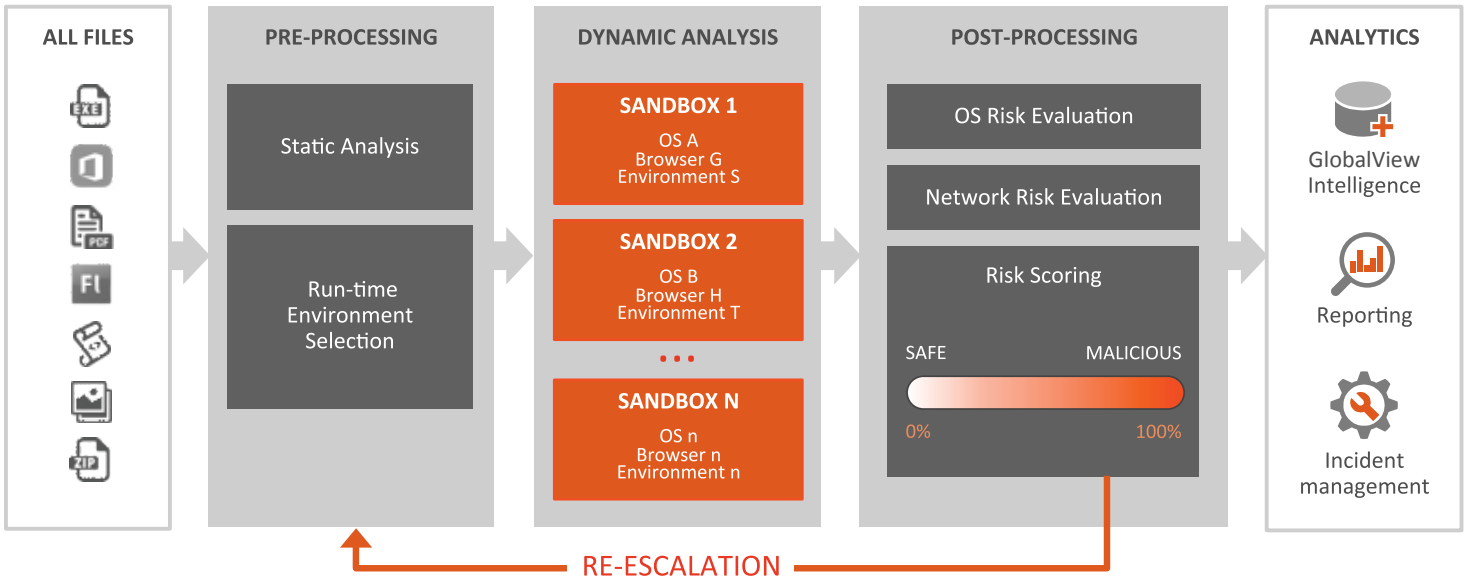
How the Cloud Sandbox Array works

Process steps for sandboxing analysis are:

1. Sophisticated pre-processing combines static and dynamic analysis; then the expected behavior of the file is predicted and an appropriate sandbox is selected.
2. The file is detonated in the selected sandbox and monitored for malicious activity, as well as complete expression of all expected behavior.
3. If the full set of expected behavior is not seen, then the file is recursively submitted to different types of sandboxes—which may vary by operating system, browser type, or virtual or physical environment—until full behavior is observed, and an aggregate threat score is calculated.
4. Once malicious files and URLs are fingerprinted, the information is available across the Cyren global intelligence cloud within seconds.

Supported OS's: Microsoft Windows 10/8/7/XP (32b/64b)

Supported File Types: Windows executable files, Mac files (Threat Lookup), Microsoft Office, PDFs, Flash files, Scripts, Archive files



©2018. Cyren Ltd. All Rights Reserved. This document and the contents therein are the sole property of CYREN and may not be transmitted or reproduced without CYREN's express written permission. All other trademarks, product names, and company names and logos appearing in this document are the property of their respective owners. [20180404]