SNDBOX
malware research platform

COMBATING MALWARE INNOVATION WITH INNOVATION

The Next Generation SNDBOX of Malware Detection

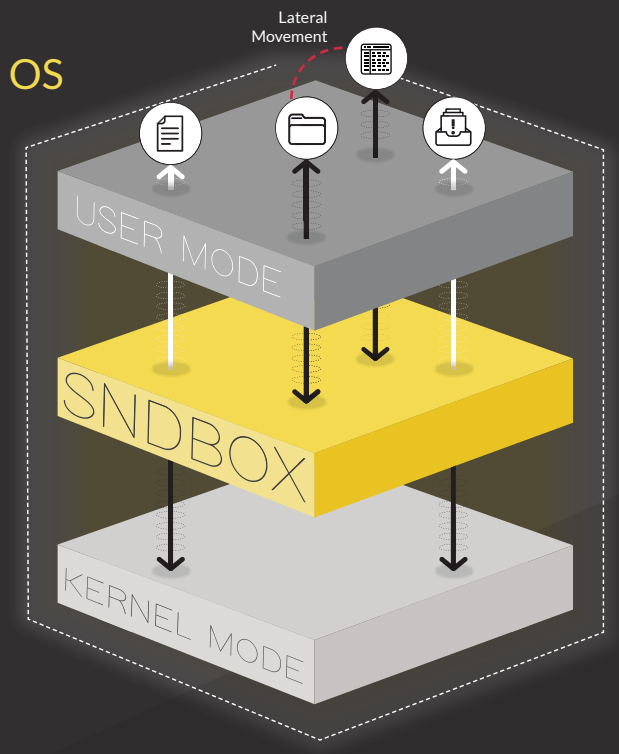
Due to the rapid rate of evasive malware innovation, it is becoming ever more challenging to classify new permutations as they appear and identify unknown malware samples before they strike.

SNDBOX applies an invisible kernel mode agent and AI to offer the next generation Sandbox, extending the individual capabilities and expertise of your security and research teams through AI, dynamic analysis and network mapping.

Undetectable Kernel Mode Agent

Reveal Malware's Full Malicious Nature

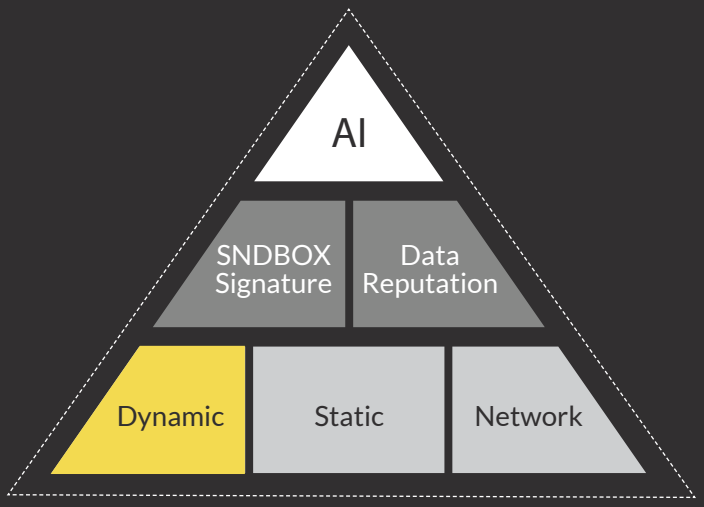
Located between the User mode and Kernel mode, SNDBOX's invisible agent deceives malware into executing its full range of intended functionality, revealing its true malicious nature, intent and capabilities.



1. All key operations run through the kernel
2. SNDBOX kernel driver generates a fictional environment to deceive malware into executing full range of functionality
3. Kernel driver aggressively monitors malware every step and modify the expected results.

SNDBOX
malware research platform

ARTIFICIAL INTELLIGENCE (AI) POWERED



SCALE WITH AI

SNDBOX's multi-vector AI detection aggregates static, dynamic and network inputs to provide insight evaluation and data-driven discovery.

GAIN DATA VISIBILITY

Easy-to-digest analysis results, all members of your team can access the information relevant to their work and area of expertise.

DO MORE FASTER

Seamless Integration Designed to streamline security processes, SNDBOX easily integrates with a wide variety of 3rd party security platforms.

WAYS TO USE SNDBOX

Security Platforms

Use SNDBOX as the world's first AI malware research platform

DFIR & Threat Hunting Teams

Leverage SNDBOX for incident and response.

Threat Intelligence Departments

Depend on SNDBOX to strengthen security products.

MSSPs and OEM

Integrate SNDBOX into their perimeter security services.

SNDBOX
malware research platform

ANALYSIS FLOW

1

PREPERATION

AI supplements traditional research limitations by leveraging the extracted labeled key attributes and raw inputs from automatic static and dynamic malware analysis, at scale.

2

TRAINING

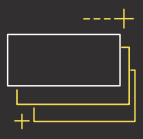
1. Across all vectors, preparation data is leveraged to create AI prediction models as domain experts.
2. A single answer is returned per vector.
3. Raw inputs are aggregated together with all domain expert decisions for a higher level AI learning model that returns a single summary answer.

4

ANALYSING

When an unknown sample is received, automatic malware analysis extracts attributes and raw data for prediction and similarity search queries.

3



INDEXING

SNDBOX converts static and dynamic behavioral inputs into searchable vectors.

5

PREDICITING

Multi-vector AI detection mechanisms and behavioral indicators work together to detect malicious activity and aggregate data to provide decisive conclusions about the nature of the file.

6

SIMILARITY

Our reputation engine works alongside AI search to reduce false positives. Highly similar results are returned and scored based on their relevance.

7

VISIBILITY

All research data, conclusions and corresponding expert explanations are available in our open research platform, supporting the community's ability to collectively scale efforts to combat evasive malware.