

Sandbox comparison

Intro

ReversingLabs combines our advanced static analysis with dynamic analysis techniques to provide security teams with a unified threat analysis platform that can detect the most sophisticated threats that are invisible to traditional tools.

Sandbox comparison	ReversingLabs	Sandbox Alone
Speed of Analysis	Milliseconds	5 to 30 Minutes
Possibility of Evasion	No	Yes
Configuration	No Configuration per Sample	Samples Require Custom Configuration
File Identification	4000+ File Types	140 File Types
Integration	API and Connectors	API
Scalability	License Cost	Hardware and License
Threat Reputation information	Yes	No
File Size Limits	2GB	200MB
Operating System Support	Windows, macOS, Linux, Android, IOS	Windows, macOS, Linux
Deployment Options	On Premise/ Cloud	On Premise
Network Analysis	Yes	Yes
MITRE ATT&CK Mapping	Yes	Yes
Throughput	Unlimited	Based on Hardware

Benefits

Having a unified threat analysis platform allows security teams to choose the level of inspection required for a file without the risk of missing malware due to obfuscation, or sophisticated packing techniques. This level of control speeds the detection of malware without negatively impacting the user with slow file transfer.