SOPHOS
Security made simple.

Cloud Sandbox

Strengthen your antivirus defenses with dynamic malware analysis

Sophos' next-gen sandboxing platform provides a complete solution for quickly integrating advanced emulation-based malware analysis. Cloud-based, Sophos Sandbox provides a highly scalable and powerful environment to run in-depth, sophisticated analysis of unknown or suspicious programs and files. Sophos Sandbox can easily be integrated into any messaging or web security product via its published APIs, and includes Sophos Antivirus SDK as a pre-filter, thereby reducing the cost and complexity associated with implementing advanced threat detection systems.

Key Benefits

- Advanced detection of unknown malware and zero-day viruses
- Ease of integration for a wide range of use cases and business models
- Scalable to secure any size network
- Flexible and simple licensing allows for cost-effective integration
- Powerful pre-filtering and pre-built logic determines which files require advanced detection

Industry Insights

As cybercriminals develop new and more sophisticated malware to remain elusive, the cost and complexity of managing such infections is growing increasingly. Zero-day malware has become more prevalent than ever, often bypassing known techniques and existing security layers.

Developing advanced malware security solutions requires a tremendous level of research and development, customization, integration, and creation of complex decision processes about which files need to undergo sandbox analysis in order to balance advanced detection, user experience, and financial viability.

Sophos Sandbox allows security vendors to easily and quickly deploy a comprehensive solution. At its foundation lies a unique detection platform complemented by Sophos' award-winning anti-malware and closely integrated with SophosLabs threat intelligence.

Ease of Integration, Depth of Detection

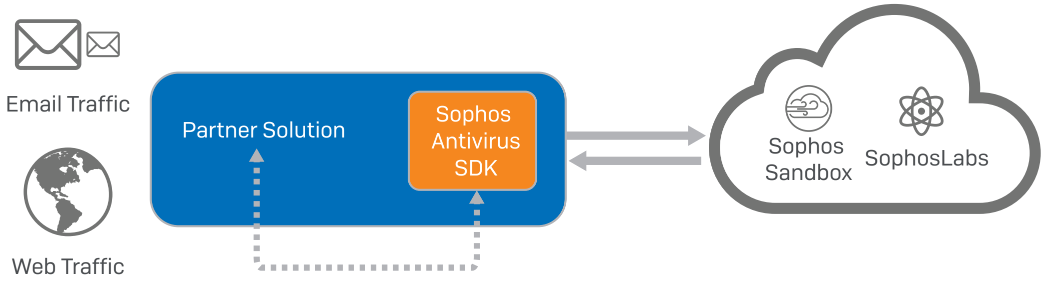
Sophos Sandbox, now in its fourth generation, is available as a cloud service. It combines the latest threat analysis with powerful emulation tools to ensure that files are inspected using real-time intelligence along with comprehensive detection techniques.

Integrated via comprehensive APIs and coupled with Sophos Antivirus SDK, it allows security vendors to deploy sandboxing capabilities for a wide range of use cases in the most efficient manner, saving significant time and resources, as well as eliminating the potential for human error.

Advanced Detection Analysis

Sophos Antivirus SDK complements its cloud Sandbox and functions as an efficient pre-filter, providing the first line of defense and helping to reduce the number of wrongly convicted files sent for advanced analysis. This results in optimal performance, enhanced user experience and faster analysis of suspicious files.

The Sophos Threat Intelligence lab further supports detection capabilities as it provides unique data available through Sophos Synchronized Security: dual analysis from both endpoints and network security appliances, providing a comprehensive layered security solution.



Improved detection and risk mitigation

Sophos Sandbox detects zero-day threats and sophisticated attacks, delivering risk ratings and attack details necessary for remediation. Security vendors can then utilize these detection findings to trigger preventive actions to ensure the safety of users until remediation is in place.

Lowest Total Cost of Ownership

Sophos Sandbox is purpose-built to deliver advanced detection capabilities while keeping your costs low:

- Powerful pre-filter detection and built-in logic allows for the majority of files to be classified immediately. As fewer files are sent to the cloud sandbox, bandwidth costs are kept to a minimum.
- Ease of integration and platform scalability allows security vendors to get to revenue faster.
- Subscription-based model with unlimited files per user allows for a predictable cost structure.

Key capabilities

Pattern-based detection	Helps uncover malicious files including polymorphic and other disguised threats designed for undetectable targeted attacks
Thwarts sandbox-aware malware	Sophos Sandbox can detect evasive behavior of VM-aware malware, and also protects against other generic memory exploits such as "heap sprays"
Automatic pattern updates	Ensures continuous protection and maximum performance against rapidly evolving advanced threats
Granular verdict	Provides conclusive evidence for suspicious websites, files, applications, and events by analyzing threats in a secure environment
Integrated with Sophos Global Threat intelligence	Leverages comprehensive crowdsourced threat intelligence by drawing on the experience of our global customer base

Evaluation

Evaluate Sophos Sandbox today by contacting us at oem.sales@sophos.com

For more information

Please visit Sophos.com/oem

OEM Contact
Email: oem.sales@sophos.com

Oxford, UK

SOPHOS