SOPHOS

Security made simple.

Sophos Sandstorm

Next-generation advanced threat defense made simple

Sophos leads the security industry in fighting advanced malware using highly effective technologies such as real-time JavaScript emulation and behavioral analysis. While conventional anti-malware protection is still important as a first line of defense, organizations need additional tools to combat today's targeted malware.

Sophos Sandstorm is an advanced persistent threat (APT) and zero-day malware defense solution that complements Sophos security products. It quickly and accurately detects, blocks, and responds to evasive threats that other solutions miss, by using powerful, cloud-based, next-generation sandbox technology.

Highlights

- Seamless integration with your Sophos security solution
- Up and running in minutes
- Protects against APTs, unknown malware, and targeted attacks
- Threat intelligence you can act on
- Comprehensive platform coverage
- Granular, incident-centric reports

Advanced protection from targeted attacks

Keep unknown data-stealing malware off your network. Powerful, cloud-based, next-generation sandbox technology means you quickly and accurately detect, block, and respond to APTs and zero-day threats.

We keep it simple

Sophos Sandstorm is fully integrated into your Sophos security solution. Simply update your subscription, apply the Sandstorm policy and you're protected instantly against targeted attacks. You'll be up and running in minutes.

Block evasive threats that others don't see

Detect unknown threats specifically designed to evade first-generation sandbox appliances. Our full-system emulation approach provides the deepest level of visibility into the behavior of unknown malware and the detection of malicious attacks that others simply miss.

Deep forensic reporting

Accelerate response to advanced threats with simple incident-centric breach analysis. We provide you with prioritized APT intelligence by correlating the evidence. This approach both reduces noise and saves you time.

Comprehensive analysis

Determine potential threat behavior across all your end user devices and critical infrastructure. This includes your operating systems (Windows, Mac OS X, and Android); physical and virtual hosts; services; users; network infrastructure; and web, email, file, and mobile applications. Safely detonate threats in the Sandstorm cloud, isolating your datacenters from dangerous malware.

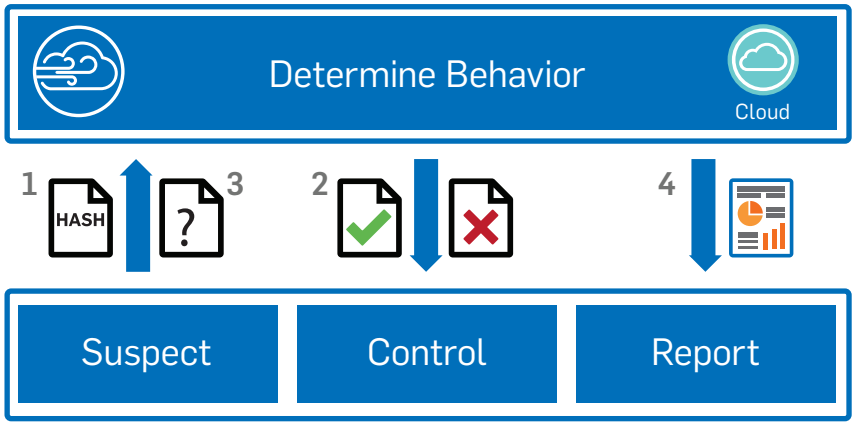
Lightning performance

Your Sophos security solution accurately pre-filters traffic, so only suspicious files are submitted to Sandstorm, ensuring minimal latency and end user impact.

Sophos Sandstorm Features

- Full integration into your Sophos security solution dashboard
- Inspects executables and documents containing executable content
  - Windows executables (including .exe, .com, and .dll)
  - Word documents (including .doc, .docx, docm and .rtf)
  - PDF documents
  - Archives containing any of the file types listed above (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
  - Supports more than 20 file types
- Dynamic malware behavior analysis runs files in real environments
- In-depth malicious file reports and dashboard file release capability
  - Average analysis time less than 120 seconds
  - Flexible user and group policy options on file type, exclusions, and actions on analysis
  - Comprehensive environment coverage including Windows, Mac, and Android
  - Supports one-time download links

How it Works



1. The Sophos security solution scans files against all conventional security checks (e.g., anti-malware signatures, bad URLs, etc.). If the file is executable or has executable content and is not downloaded from a safe website, the file is treated as suspicious. The Sophos security solution sends the suspicious file hash to Sophos Sandstorm to determine if it has been previously analyzed.
2. If the file hash has been previously analyzed, Sophos Sandstorm passes the threat intelligence to the Sophos security solution. Here, the file is delivered to the user's device or blocked, depending on the information provided by Sophos Sandstorm.
3. If the hash has not been seen before, a copy of the suspicious file is sent to Sophos Sandstorm. Here, the file is detonated and its behavior is monitored. Once fully analyzed, Sophos Sandstorm passes the threat intelligence to the Sophos security solution. Again, the file is delivered to the user's device or blocked, depending on the information provided by Sophos Sandstorm.
4. The Sophos security solution uses the detailed intelligence supplied by Sophos Sandstorm to create deep forensic reports on each threat incident.

Try it now for free

Register for a free 30-day evaluation at Sophos.com/Sandstorm

Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

Oxford, UK | Boston, USA

SOPHOS

2015.12.9 DS-NA (SM)