SOPHOS
Partner Program

Sophos Sandstorm Deskaid

What is Sophos Sandstorm?

Sandstorm is a powerful, cloud-based, next-generation sandbox that detects, blocks and reports on zero-day, evasive, threats.

What is a sandbox?

A sandbox is an isolated environment used to execute suspicious programs attached to emails and downloaded from websites to determine if they contain malware.

What does Sandstorm analyze?

- Executable content not detected as malicious by Sophos antimalware technology.
- More than 20 file types containing executable content.
- Windows executables (including .exe, .com, and .dll).
- Word documents (including .doc, .docx, docm and .rtf).
- PDF documents – Archives containing file types listed above (ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet).

What can I sell Sandstorm with?

Product	Sandstorm SKU
Sophos Web Appliance	WPA-SAND
Sophos Email Appliance	EPA-SAND
Sophos UTM	SG-(model)-SAND or UTM-(model)-SAND
Sophos XG Firewall	Coming Soon
Sophos Cloud Web Gateway	Coming Soon

Why buy Sandstorm?

Sandstorm is Simple

- Easy to try – sign up in minutes from within the product interface.
- Easy to deploy – simply activate the policy.
- Easy to manage – seamless integration with your three clicks to anywhere interface.

Sandstorm is Effective

- Blocks evasive threats – detects threats designed to evade sandboxes that other solutions miss.
- Threat intelligence you can act on – reduces noise and saves you time.
- Visible protection – granular incident based reports.
- Comprehensive platform coverage – Windows, Mac, and Android.

Sandstorm is Cloud-based

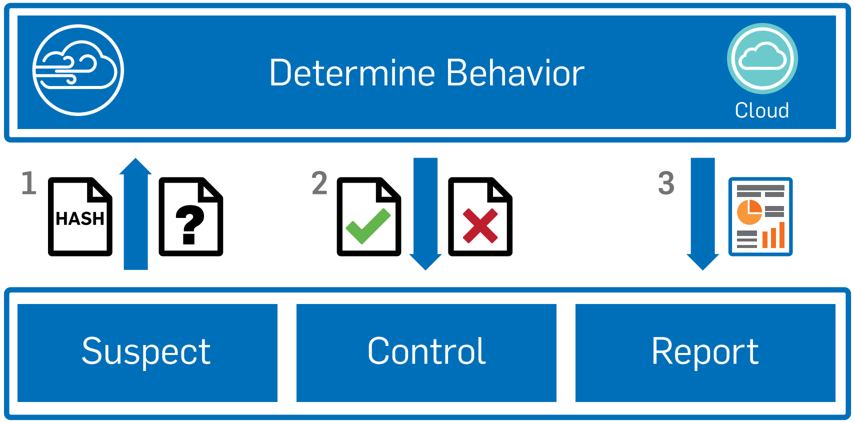
- Rapid deployment – instant protection with no hardware to deploy or appliance upgrade needed.
- Minimal impact on performance – all processing done in cloud.
- Collective intelligence – benefit from all customer threat analysis.

How do I start a conversation?

- What do you think about new security technologies such as Sandboxing?
- There's been a lot in the media about targeted threats and advanced persistent threats (APTs), and seeing the likes of Talk Talk and Target Stores compromised shows us that no one is safe.
- How do you currently combat these threats?
- These attacks are specifically designed to bypass traditional security. Many organizations believe these systems protect them, but unfortunately that is not the case.
- They protect users by filtering out known threats at the gateway. Attackers are using unknown threats to evade detection.
- There is a way to mitigate this risk – quickly and cost effectively – by seamlessly extending the capability of your Sophos security with Sophos Sandstorm.

How does Sophos Sandstorm work?

1. If the file has known malware it's blocked immediately. If it's otherwise suspicious, and hasn't been seen before, it will be sent to the sandbox for further analysis. When web browsing, users see a patience message while they wait.
2. The file is detonated in the safe confines of the sandbox and monitored for malicious behaviour. A decision to allow or block the file will be sent to the security solution once the analysis is complete.
3. A detailed report is provided for each file analyzed.



Determine Behavior

Cloud

1 HASH ?

2

3

Suspect

Control

Report

How do I overcome objections?

Why don't my current products protect me against APTs and zero-day threats?

- APTs are specifically designed to evade traditional anti-malware defenses.
- Sophos Sandstorm augments Sophos' existing strong anti-malware technology with additional advanced threat detection capabilities to detect and block APTs.

No one is attacking me. I'd know about it wouldn't I?

- How? Targeted threats are designed to evade traditional gateway security.
- They use unknown malware that your anti-virus may not detect.
- They move your data outside by hiding it in normal web traffic.
- You may be losing valuable data now and not realize.

Who would attack me, we aren't important? Or I'm just an SMB?

- You're more important than you think.
- You have large organizations as customers or clients.
- Attackers could use you as the entry point to attack your key customer.
- You are seen as an easy target without large enterprise resources.
- Q. How would that affect you relationship with that customer? Or all your customers?

How do I beat the competition?

	Sophos Sandstorm	FireEye	Palo Alto Wildfire
Easy-to-use	✓	–	–
Affordable	✓	–	–
Integrated	✓	–	✓

Oxford, UK | Boston, USA

Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK

2016.2.18 DA-NA (RG)