SOPHOS
Security made simple.

Sophos Sandstorm

下一代高级威胁安全防护操作简便

Sophos 使用高效技术如实时 JavaScript仿真和行为分析引领高级恶意程式防御产业。传统反恶意程式防护作为安全防御第一项，企业需要其它工具抵御当前恶意程式。

Sophos Sandstorm是高级持续威胁（APT）和零日恶意程式防御方案，可弥补 Sophos 安全产品。功能强大、云、下一代技术可快速、准确探测、拦截、回应潜在威胁。

主要优势

- Sophos 安全解决方案无缝集成
- 几分钟内运行
- 抵御高级持续威胁、未知恶意程式和目标攻击
- 威胁情报
- 全面的平台覆盖
- 精细事故报告

抵御目标攻击高级防护

察觉未知数据盗窃恶意程式功能强大、云、下一代技术可快速、准确探测、拦截、回应高级持续威胁和零日威胁。

我们让一切变得简单

Sophos Sandstorm 集成至Sophos 安全解决方案。更新产品、应用Sandstorm 政策、抵御目标攻击。.您会在几分钟内启动并运行。

拦截潜在威胁

探测第一代应用程序未知威胁我们系统仿真方案可深入查看未知恶意程式，探知恶意攻击。

深入报告

数据泄露分析加速高级威胁回应提供优化高级持续威胁信息该方案降低干扰、节约时间

综合分析

探知终端用户设备和关键基础设施潜在威胁行为操作系统(Windows、Mac OS X和Android)；物理和虚拟主机；服务；用户；网络基础设施；网络、邮件、文件和移动应用程序探知Sandstorm云威胁，将数据中心和风险恶意程式隔离。

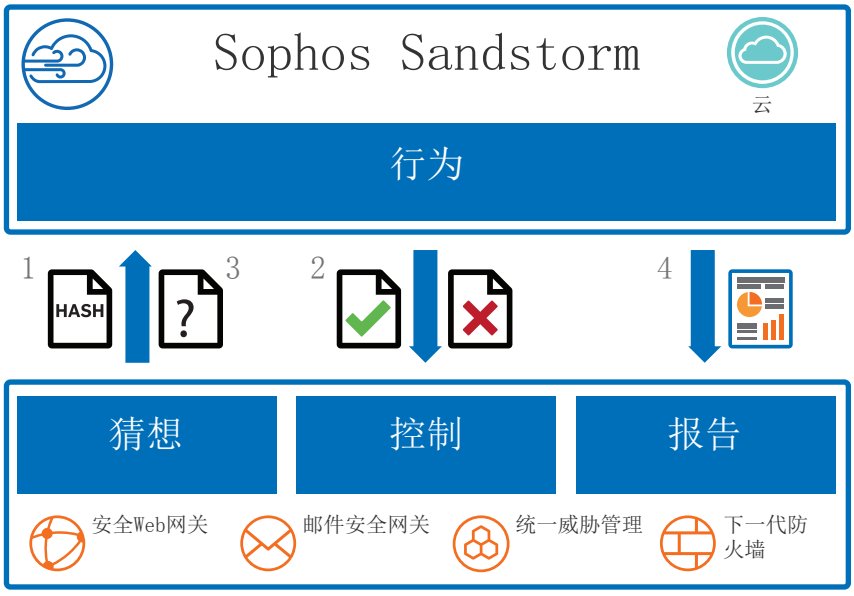
闪电般的性能

Sophos 安全解决方案可准确预先过滤流量，这样可疑文件可提交至 Sandstorm，最小化潜在威胁和终端用户影响。

Sophos Sandstorm 功能

- 真实环境动态恶意程式行为分析
- Sophos安全解决方案控制面板集成
- 40文件类型检查包括：
  - PE (32 or 64-比特可执行程序和 DLLs)
  - Microsoft Office 文件 (.doc、.docx、.xls、 .xlsx、 .ppt、.pptx、 .docm、 .xlsm、 .pptm、 .rtf)
  - PDF, HWP, XPF, CHM, JAR, APK Archives (ZIP, BZIP, GZIP, RAR, TAR, LHA / LZH, XZ)
- 深入恶意文件报告和控制面板文件
  - 平均分析时间小于120秒
  - 文件大小、类型、除外条款和分析操作灵活政策选项
  - 探知系统环境流量，了解已知 C&C 流量
  - 支持的综合环境包括Windows、 Mac和 Android
  - 支持一次性下载链接

工作原理



1. Sophos安全解决方案测试潜在威胁 (比如：反病毒签名、恶意 URLs等等).如果可疑文件未确定为威胁文件， Sophos 安全解决方案发送文件散列至 Sophos Sandstorm确定是否先前已经过分析。
2. 如果文件散列先前已分析，Sophos Sandstorm 将威胁信息发送至Sophos安全解决方案。根据 Sophos Sandstorm提供的信息，文件发送至用户设备或被拦截。
3. 如果散列先前未发送，可疑文件将发送至Sophos Sandstorm。一旦发现可疑文件，系统将监控该行为。一旦程序完成分析过程， Sophos Sandstorm 将威胁信息发送至Sophos 安全方案。根据 Sophos Sandstorm提供的信息，文件发送至用户设备或被拦截。
4. Sophos 安全方案采用 Sophos Sandstorm 提供的详细信息，深度剖析各个安全威胁事故。

立即免费试用

注册即可免费试用 30 天
sophos.com/zh-cn/sandstorm

英国和全球销售处
电话：+44 (0)8447 671131
电子邮件：sales@sophos.com

北美销售处
免费电话：1-866-866-2802
电子邮件：nasales@sophos.com

澳大利亚和新西兰销售处
电话：+61 2 9409 9100
电子邮件：sales@sophos.com.au

亚洲销售处
电话：+65 62244168
电子邮件：salesasia@sophos.com

英国牛津 | 美国波士顿

2015.11.13 DS-NA (GH)