SOPHOS

Cybersecurity made simple.

Sophos Sandstorm

简化的下一代先进威胁防御

Sophos Sandstorm 使用下一代云沙箱技术，为您的企业提供针对勒索软件和针对性攻击的额外安全防护。

作为唯一采用深度学习分析实现更高效侦测的网络沙箱，与 Sophos Central 上的 Sophos XG Firewall、Sophos UTM、Sophos Web Appliance、Sophos Email Appliance 和 Sophos Email 集成 — 无需额外硬件。

绝对物有所值，您可以通过相宜的价格获取企业级安全防护功能。

产品亮点与您的 Sophos 安全解决方案无缝集成

- 几分钟内即可运行
- 防范勒索软件 APT、未知恶意软件、PUA 和针对性攻击
- 可供采用的威胁情报
- 深度学习分析
- 精细事故报告

抵御针对性攻击的高级防护

将勒索软件和未知数据窃取恶意软件隔离在网络以外。基于云的强大下一代沙箱技术和深度学习分析意味着可以快速准确侦测、阻止和响应 APT 及零日威胁。

我们让一切变得简单

Sophos Sandstorm 集成至Sophos 安全解决方案。只需更新产品、应用Sandstorm 政策、您即可抵御针对性攻击。几分钟即可内启动并运行。

拦截能逃过其他方案的潜在威胁

探测勒索软件和能逃过第一代沙盒程序的未知威胁我们全系统仿真方案可深入查看未知恶意程式的行为，探知能逃过其他方案的恶意攻击。

深入报告

以简易的事件为本的入侵分析加速对高级威胁的回应。我们提供优先的高级持续威胁信息，备有证据支持。该方案减少干扰、节约时间

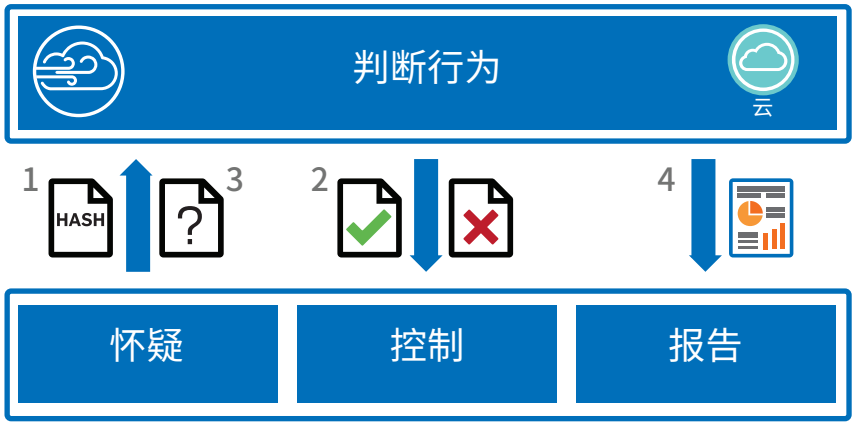
闪电般的性能

您的 Sophos 安全解决方案可准确预先过滤流量，仅向 Sandstorm 提交可疑文件，保持最低延迟和对最终用户的影响。

Sophos Sandstorm 功能

- 全面与Sophos安全解决方案控制面板集成
- 侦测可执行文档和包含可执行内容的文档
  - Windows 可执行文档 (包括 .exe, .com, and .dll)
  - Word 文档 (包括 .doc, .docx, docm and .rtf)
  - PDF文档
  - 含有以上列出的任意文件类型的档案 (ZIP、BZIP、GZIP、RAR、TAR、LHA/ LZH、7Z、Microsoft Cabinet)
  - 支持超过20种文件类型
- 动态恶意软件行为分析和深度学习在真实环境中运行文件
- 深入恶意档案报告和控制面板档案发放能力
  - 平均分析时间小于120秒
  - 在文件类型、异常情况和分析操作方面具灵活的用户、群组策略选项
  - 支持一次性下载链接

工作原理



1. Sophos安全解决方案对所有档案进行常规安全扫描 (比如：反恶意软件特征码、恶意 URLs等等).如果某档案可执行，包含可执行内容或从非安全网站下载的话，它将被视为可疑。Sophos 安全解决方案发送可疑档案散列至 Sophos Sandstorm确定是否先前已经过分析。
2. 如果档案散列先前已分析，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，档案将发送至用户设备或被拦截。
3. 如果散列先前未曾见过，可疑档案的备份将发送至Sophos Sandstorm。在這裡檔案將引發連串行動，其行為並受系统监控。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，档案将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 30 天免费评估版
www.sophos.cn/sandstorm

北京：
电话：4006506598
+86 13552376911
电子邮件：salescn@sophos.com

上海：
电话：+86 18521070801
+86 18901838899
电子邮件：salescn@sophos.com

华南：
电话：+86 13859998247 （深圳）
+86 18100273273 （广州）
电子邮件：salescn@sophos.com

2019-01-03 DSZHCN (PC)

SOPHOS