Avira

威胁情报源

Avira 威胁情报源可以让您访问 Avira 反恶意软件解决方案的核心数据，从而提升您自身的威胁情报服务。

它们可让您“超视距”地看到新出现的威胁，并创造构建主动安全态势的机会。文件和 URL信誉源提供关键的威胁信息，并持续补充完善。前者包含在 Windows 和 Android 上发现的广泛情报。所有情报源均定期提供，使您能够构建强大有效的威胁检测系统

通过访问 Avira 的全球传感器网络和强大的恶意软件检测引擎收集和分析的数据，威胁情报源可为您自身的业务创造价值。Avira 的威胁情报源是独一无二的，因为它们可提供与安全供应商和服务提供商高度相关的全面、清晰且易于使用的情报。

实现

Avira 的威胁情报源可以提供从 Avira 保护云中提取的持续更新的威胁数据流。这些数据托管在 Amazon S3 云上，以易于访问的 JSON 格式传递，并且每 60 秒更新一次。

合作伙伴可以选择情报中的不同属性来做决策。情报信息不包含任何可识别个人身份的数据与源文件本身，仅传递由分析产生的元数据，从而确保数据隐私。

Avira 的威胁情报源作为解耦的非侵入式服务模式：它们无需部署特殊代码或结构 (SDK 或 API)，也无需 Avira 访问客户的基础架构来启用服务。

简单

以易于使用的 JSON 格式传递数据

解耦模式 - 无需 API 或 SDK

可在任意平台上实现

完整的文档和应用示例

轻松访问和授权

价值

URL 、域、 Windows 、Android 、二进制可执行文件、各类文档的关键属性

数据来源于 Avira 全球 5 亿多企业和个人用户

提供接近于实时的更新，涵盖零日威胁

安全可靠

数据存储于安全的 Amazon S3 云上

在高可用性平台上提供不间断的服务更新

非侵入式，无需 Avira 访问本地系统

优势

符合数据隐私法规；无需共享客户数据即可确保安全

当威胁在全球范围内出现时能及早预警

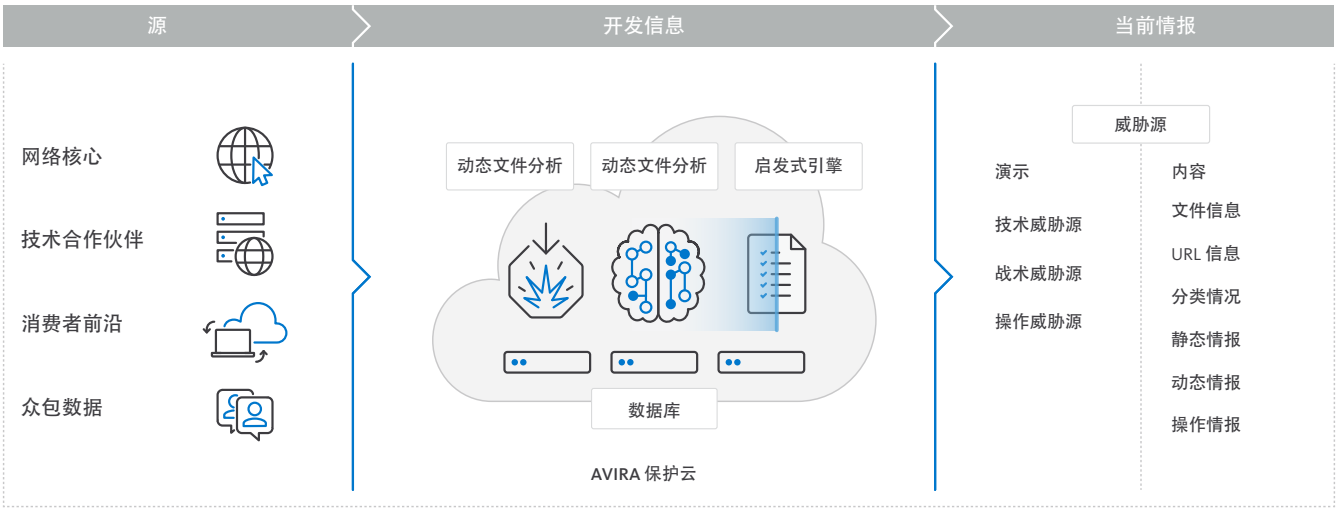
自动提供信息，最大限度降低集成工作量

由知名的市场领先企业提供数据集

以易于使用的方式强化应用 Avira 的检测技术

Avira

开发威胁情报



文件信誉源

包含用于标识干净文件和恶意软件文件的关键属性，包括：PE、二进制文件、Android 和文档的哈希、分类和时间信息等。

网站信誉源

Avira 的网站信誉源包含主要分类，可用于识别包含恶意或潜在恶意内容的域和 URL。提供的信息不包含任何可识别个人身份的数据。

文件情报源

Avira 的文件情报源提供在 Windows 和 Android 文件上开发的不断更新的威胁数据流。包括：

— 包含哈希、时间戳、大小和格式的基本数据的文件信息
— 识别恶意软件及其功能（恶意软件、网络钓鱼、PUA 和分类上下文）的分类情报。
— 包含相关证书的属性以及文件与特定漏洞的关联性的静态情报。
— 包含 Avira 传感器网络发现的相关地理位置信息的感染情报。

域分类

Avira 的域分类包含符合 IAB-1、第 1 层和第 2 层的相应的域安全分类和内容归类。在域或子域级别提供的 400 多个类别，对于需要家长控制、提升生产效率或一般域分类的解决方案特别有用。类别示例包括 IAB25-3 成人内容、IAB12-WS1 社交网络或 IAB17 体育。

了解更多

网站: oem.avira.com
电子邮件: oem@avira.com
博客: insights.oem.avira.com
社交媒体: @Avira

欧洲、中东、非洲

Avira
Kaplaneiweg 1
88069 Tettnang, Germany
Tel: +49 7542 5000

美洲和亚太地区

Avira, inc
c/o WeWork, 75 E Santa Clara Street
Suite 600, 6th floor San José
CA 95113 United States

日本

Avira GK
8F Shin-Kokusai Bldg
3-4-1, Marunouchi Chiyoda-ku
Tokyo 100-0005, Japan

中国

艾维华有限公司
中国北京市朝阳区东方东路19号
外交办公大楼D1座17层1727室
邮编：100016
电话：+86 10 8531 7336