网络资产风险监测系统

产品简介

产品文档

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系95716。

文档目录

产品简介
产品概述

最近更新时间：2019-08-15 16:52:38

什么是网络资产风险监测系统

网络资产风险监测系统（Network Assets Risk Monitor System，NARMS）是一款自动探测企业网络资产并识别其风险的产品。依托腾讯20年累积的安全能力，网络资产风险监测系统能够对企业的网络设备及应用服务的可用性、安全性与合规性等，进行定期的安全扫描、持续性的风险预警和漏洞检测，并且为企业提供专业的修复建议，降低企业安全风险。

产品功能

资产自动发现

对设备操作系统、端口、服务、组件等企业资产进行高效识别，有效帮助企业发现未知资产、管控现有资产。

漏洞深度扫描

- Web 漏洞检测
  支持 SQL 注入、命令注入、代码注入、文件包含、XSS 攻击、CSRF 等数十种常见的漏洞类型检测，为网站安全保驾护航。
- 0day/1day/Nday 漏洞检测
  系统内置了数千条经过腾讯安全工程师严格测试和专业审计的无伤 Poc（Proof of concept），Poc 的类型包括 Web 应用漏洞、Web 中间件漏洞、数据库漏洞、操作系统漏洞、软件服务漏洞、IOT 设备漏洞、路由器漏洞、摄像头漏洞、工控设备漏洞等。

违规敏感内容检测

基于腾讯全体系内容鉴定平台与资深专业的审核团队，网络资产风险监测系统使用丰富的训练数据资源与先进的算法模型，快速准确发现网站涉黄、涉恐、赌博、涉政等敏感图片及文字等信息，防止品牌形象受损，提高网站内容安全性，保障网站符合政策要求。

篡改挂马挖矿检测

基于腾讯的用户 URL 检测体系以及实时监测系统，利用多种模型融合技术从多维度对网站进行实时监控，及时发现页面异常篡改和挂马以及挖矿行为，并第一时间进行告警和应急处理。

弱口令检测

对资产组件进行弱口令扫描，扫描对象包括 FTP、SSH、RDP、MySQL、ORACLE、IMAP、MEMCACHE、Redis 等数十项内容。

风险评估报表

针对扫描结果形成全面多维的风险扫描报告。风险扫描报告涵盖漏洞检测与内容风险两方面内容，并可提供专业修复建议。

产品优势

最近更新时间：2019-08-15 16:52:15

全面资产风险监测

网络资产风险监测系统依靠腾讯安全20年与黑产对抗累积的经验和海量威胁情报打造而成，全方位监控企业网站风险，包含弱口令检测、Web 漏洞扫描、违规敏感内容检测、网站篡改检测、挂马挖矿检测等多类资产风险。

深度风险检测

- 网络资产风险监测系统采用 Web2.0 的威胁检测引擎，通过20年与黑产对抗而学习到的黑客攻击经验，编排攻击策略，模拟真实黑客攻击，从黑客视角深入直观地获取 Web 站点的脆弱性情况。
- 基于腾讯安全专家严格测试和专业审计的数千条无伤 Poc，网络资产风险监测系统能有效检测出操作系统、数据库、Web 中间件、CMS 应用等资产组件的 1day 漏洞和 Nday 漏洞，同时依托腾讯七大安全实验室强大的 0day 深度挖掘与感知能力，深入保护用户资产安全。
- 基于在社交平台信息安全审核领域多年发展，所研制的智能内容安全检测引擎，并结合大数据和 AI 技术，网络资产风险监测系统能快速精准的检测出网站篡改、敏感词、钓鱼、木马、暗链、涉黄、涉恐等风险。

精准资产探测

- 网络资产风险监测系统不仅支持 Linux、Windows 主机的资产，还支持常见 IOT 设备，例如摄像头、路由器、工控设备。
- 网络资产风险监测系统内置了强大的协议库与指纹信息，能够快速、准确地识别资产操作系统、开放端口、服务组件等信息。

监防一体化协同

网络资产风险监测系统一旦发现安全风险，可以与云上的主机安全（云镜）和 Web 应用防火墙（网站管家）联动，实现从风险监测到风险处置的闭环。

专业化安全团队

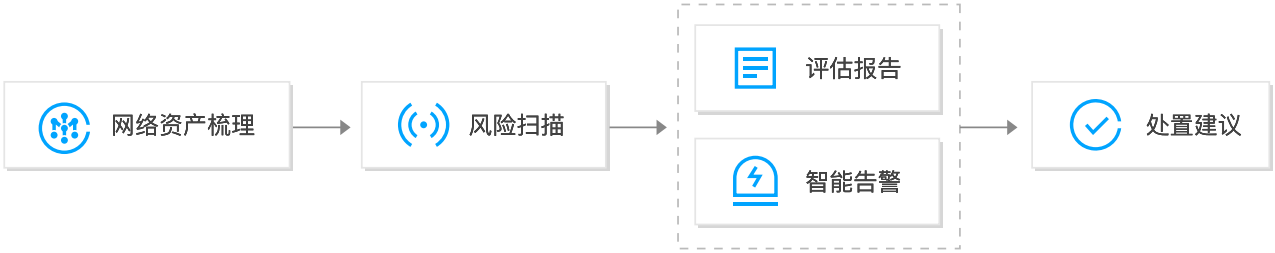
- 腾讯安全专家团队可以针对发现的安全风险，提供专业的修复建议，并对已知威胁定期检测，确保威胁已解除。
- 腾讯安全专家包括曾获得 “Master of Pwn（世界破解大师）”、“Pwn2Own 世界总冠军”称号，并多次收到微软、Adobe 等公司致谢的科恩、玄武、湛卢团队，以及连续多次在国内外网络安全挑战赛中获得冠军的 eee 团队。

应用场景

最近更新时间：2020-01-09 16:09:55

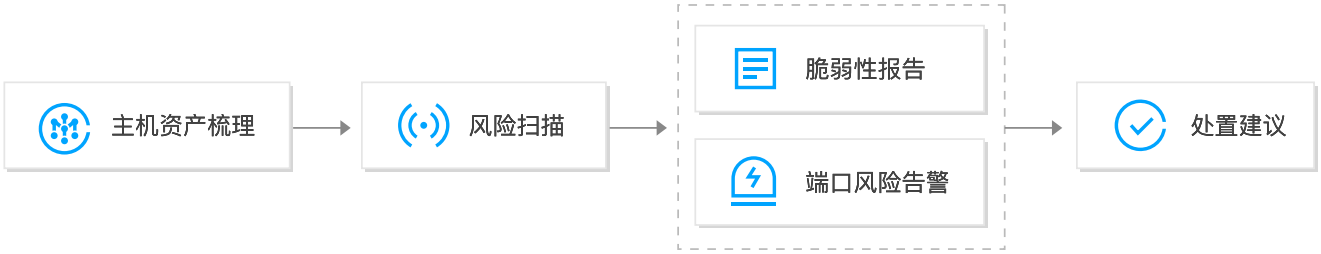
网站风险扫描

全方位检测客户网站风险，支持对 Web 漏洞、0Day/1day/Nday 漏洞、可用性、弱口令、内容安全风险、挂马篡改等威胁进行扫描，为网站安全保驾护航。



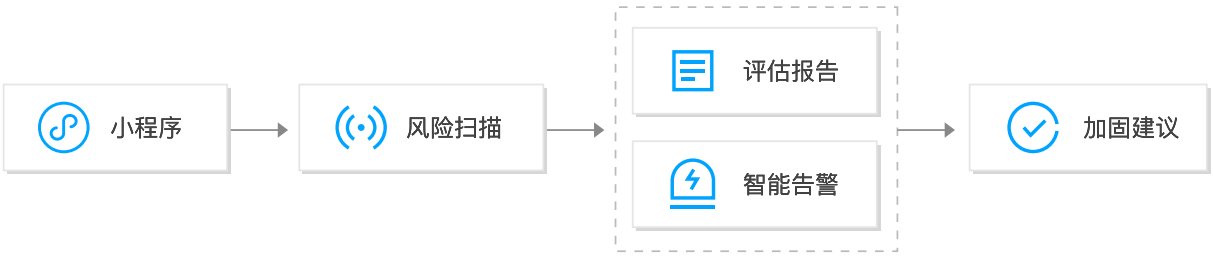
主机风险扫描

支持云上云下主机资产梳理，并对主机进行脆弱性扫描，包括漏洞风险、主机服务可用性、端口风险等，帮助企业发现影子资产、影子端口，为客户输出全面的资产分析报告和脆弱性报告，并提供专业的修复建议。



小程序安全

针对微信小程序安全提供自动化风险检测与防护，包括通用 Web 服务风险检测、API 安全检测、内容安全监测和 JS 源码虚拟机加固混淆服务，有效防止核心业务逻辑被破解、滥用，降低小程序安全风险。

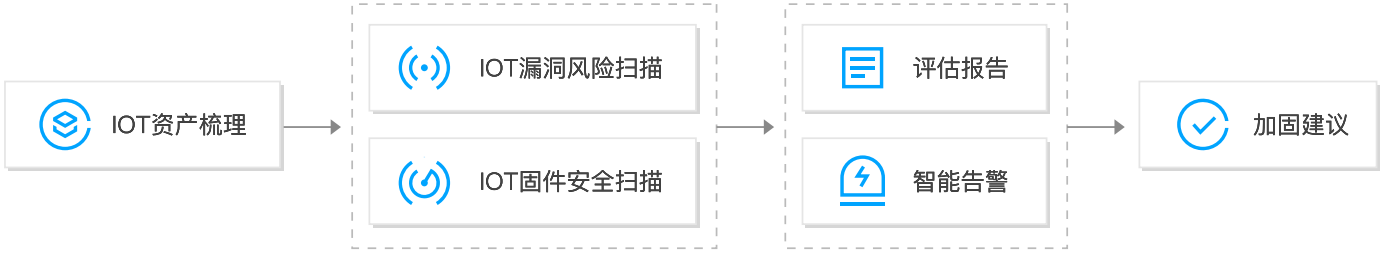


API 安全

对 API 进行 Web 层漏洞、配置合规、数据泄漏、功能可用性等方面检测，帮助客户构建基于 OpenAPI 等行业规范的积极安全模型与 API 的统一安全解决方案。

物联网安全

具有多种类型物联网（IOT）设备指纹、漏洞检测 PoC，具有 IOT 设备发现、漏洞检测以及 IOT 固件安全扫描能力，同时提供基于 ARM 等多种平台的代码混淆和指令级二进制混淆方案。



等保合规

支持为各行业网络资产提供全方位的防护解决方案，满足《信息安全技术网络安全等级保护基本要求》中漏洞和风险管理的要求，帮助用户定期对系统进行漏洞扫描，及时准确的发现系统安全隐患，第一时间进行告警通知和应急处理，并提供处置建议及应对方案，满足监管机构的合规性要求。