腾讯御点技术白皮书

目录

腾讯御点技术白皮书 1

1 产品定位 3

2 设计理念 3

3 产品市场分析 4

4 产品架构 4

4.1 部署架构 4

4.2 产品架构 5

5 产品主要功能 7

5.1 产品功能列表 7

5.2 产品主要功能描述 11

6 产品主要技术特性 15

6.1 腾讯 TAV 反病毒引擎 15

6.2 基于多步行为判断的主动防御技术 16

6.3 压缩包查杀技术 17

6.4 宏病毒专杀能力 17

6.5 主动防御 17

6.6 实时监控 17

6.7 U 盘管控 17

6.8 隔离恢复 17

6.9 文件信任区 17

6.10 样本运营体系 18

6.11 升级服务 18

7 勒索病毒专项防护 18

8 评测升级与奖项 19

9 公司资质 20

10 产品资质 21

1 产品定位

腾讯御点终端安全管理系统（以下简称“腾讯御点”）是腾讯公司提供的一款国际领先的企业级产品，其依托腾讯 20 年的安全实践和经验积累，采用了百亿量级云查杀病毒库、引擎库以及腾讯 TAV 杀毒引擎、系统修复引擎，可有效防御针对企业内网终端的病毒木马和漏洞攻击，为企业级用户提供终端病毒查杀、漏洞修复和统一管控等全方位的终端安全管理方案，可帮助企业管理者更好地了解内网终端安全状况，保护内网终端安全。

腾讯御点以更轻、更快、更准、更易用为首要研究方向，在降低用户终端资源消耗同时，能使病毒查杀更精准，有效防御病毒木马的入侵，帮助用户快速修复终端漏洞，并提供统一便捷的终端集中管控功能。

2 设计理念

- 统一管控，智能预警

腾讯御点可以实时收集终端上的各种安全状态信息，包括但不限于：补丁修复情况、内网风险情况、病毒库/终端版本分布信息、终端安全配置以及终端各种软硬件信息等，可以根据安全信息智能分析全网存在的安全风险并通过短信、邮件、微信等告警方式推送给安全管理员。

- 多重防护，安全轻便

腾讯御点会针对恶意文件和病毒木马在传播、运行、高风险操作等多个环节因地制宜的设立不同的检测机制，层层过滤确保不会遗漏可疑文件，并尽可能不影响机器运行的性能。

- ✓ 漏洞修复：根据内网终端情况，智能识别、分发和修复漏洞，提高维护效率。
- ✓ 边界防护：从文件落点进行监控，支持监控通过聊天工具比如 QQ，邮件，浏览器，下载工具等多种文件传输工具接收或者下载文件， 精准拦截危险文件落地，将风险隔绝在系统之外。
- ✓ 进程防护：监控系统所有进程启动，发现病毒威胁时运行时，会根据用户的设置来处理威胁。
- ✓ 云端鉴定：由腾讯 TAV 云查杀引擎提供能力，鉴定客户端无法处理的灰类样本。
- ✓ 定时查杀：定期对终端进行病毒查杀，避免用户的随意性导致终端感染病毒。

- ✓ 主动防御：对潜在的威胁动作进行主动的识别，智能判定风险等级并拦截。
- ✓ 终端管控：全面管控终端的软件进程、外设、网络端口等使用，全方位杜绝外部入侵和数据泄露隐患。

3 产品市场分析

本世纪以来，各类网络威胁、黑客攻击等犯罪行为程爆发式增长，并呈现出攻击工具专业化、目的商业化、行为组织化的特点。随着获利逐渐成为信息安全犯罪产业链的核心，许多漏洞和攻击工具被不法分子商业化，以此来牟取暴利，从而使信息安全威胁的范围加速扩散。在“棱镜门”事件爆发后，我国的网络安全建设被提升到了国家战略高度，“没有网络安全就没有国家安全”成为共识。

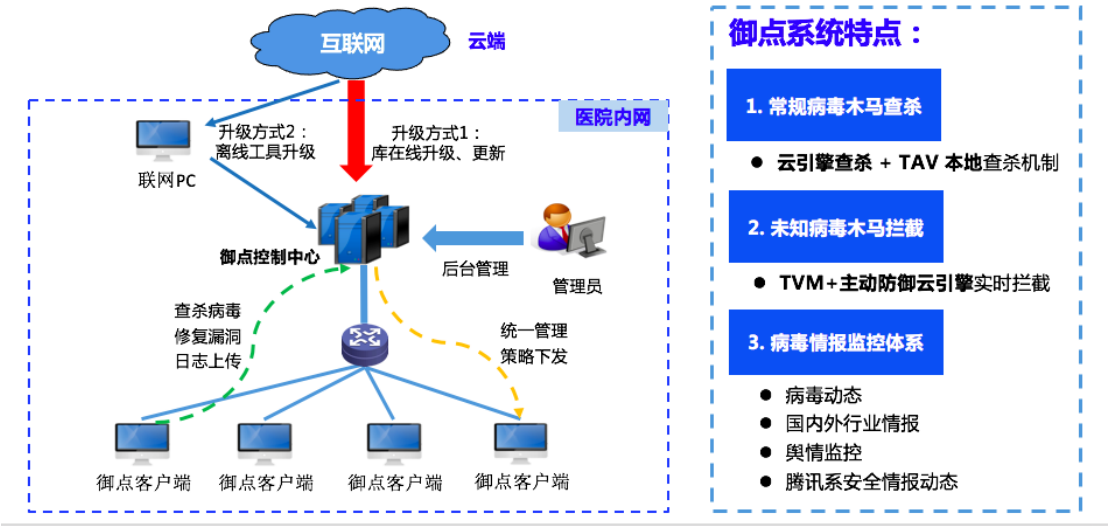
随着国家信息安全意识增强，政府、央企采购已明确将国外杀毒软件排除在外，目的就是要实现杀毒软件真正的自主可控。尖端技术生来便具备国家属性，腾讯御点无论资产还是技术都属于中国。腾讯 TAV 引擎作为国产反病毒引擎和御点的核心引擎之一，必将打破国内市场的垄断现象，为我国的杀毒软件注入了一针强心剂，这无疑将推进国产信息安全领域进入下一时代。

4 产品架构

4.1 部署架构

腾讯御点是 C/S & B/S 构架的系统，包括控制中心，客户端，云端 三个主体组成部分，服务器端和客户端均部署在企业内网。

系统构架如下图所示。



控制中心：控制中心部署在企业的内部私有服务器上，通过基于 B/S 模式的管理平台，管理员可以通过浏览器进行远程管理和查看，主要功能包括：全网终端资产管理，安全策略管控，全网安全状态自动分析/告警，以及云查杀引擎等。

控制中心主要提供以下功能：

1. 统一管理所有终端
2. 灵活配置和下发策略
3. 报表可视化展现

客户端：客户端部署在需要被保护的终端或服务器上，并与安全控制中心通信，响应控制中心设置的病毒防护，补丁修复，系统管理的策略以及任务，同时每个客户端在内网都具备一个探针的能力，实时收集内网的风险信息，实时上报给控制中心。

客户端主要提供以下功能：

1. 执行病毒查杀，漏洞修复，进程、外设、网络管控等操作，分自主执行和被动执行后台控制中心下发的策略两种方式
2. 将客户端的安全日志和行为日志上传至后台控制中心

4.2 产品架构

腾讯御点的产品架构从平台承载、功能模块、数据汇集和安全能力四个维度进行考虑。以下是产品架构图：

- 平台承载

腾讯御点后台控制中心部署环境支持 windows server 操作系统服务器和 Linux 操作系统服务器，windows server 操作系统包括 Windows Server 2003_SP2/Windows Server 2008/Windows Server 2012，Linux 操作系统包括 Linux 内核 V3.1 以上版本，支持 SuSE, Redhat, CentOS, Ubuntu 和 Debian 等；

腾讯御点客户端支持 windows server 客户端和 windows 系列操作系统的客户端，windows 系列操作系统包括 Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10。

- 功能模块

腾讯御点全面包含终端病毒查杀、漏洞修复、统一终端管理和策略管控等功能，其主要功能模块简介如下：

1) 终端管理：展示全网终端的软硬件信息和安全防护状态，分组、自定义或指执行统一的病毒查杀和补丁修复操作，终端统一升级管理
2) 病毒查杀：针对常规病毒木马，采用 **双云+TAV** 查杀机制，内存占用低、识别率高、兼容性强，支持隔离网样和宏病毒查杀；针对未知病毒木马，采用 TVM 人工智能启发式引擎+主动防御云引擎相结合实时拦截用户的可疑行为；
3) 漏洞修复：支持补丁类型分类，过滤掉无效补丁；支持补丁错峰下发，保障企业网络带宽资源的正常使用；提供漏洞排名、终端漏洞情况统计及数据画表的导出
4) 策略管控：提供安全策略和管控策略；安全策略包含系统基本安全设置、病毒查杀、实时防护、漏洞修复等策略配置；管控策略提供进程管控、外设管控、网络端口管控等策略配置；

5) 软件管理：覆盖 1 万多款 19 大类常用软件；同时支持软件禁用、软件分发等功能。
6) 多账户管理： 可分配三种管理员权限，普通管理员、账号管理员、审计管理员，适应企业不同人员权限的划分设置，以保证灵活与安全
7) 分组管理：支持多种自动分组规则，如：IP 分组，LDAP 同步等
8) 安全工具箱：现已集成文档保护、网络净化和垃圾清理等工具；文档保护提供文档自动备份和实时监控、文档找回及文档解密 3 种功能；网络净化支持软件弹窗拦截和捆绑安装拦截能力；垃圾清理除针对系统、上网、聊天、软件、游戏、影音等垃圾提供一键扫描清除外，还可对终端使用痕迹、、插件和文件进行指定清理。

- 产品联动

腾讯御点支持与御见、御界等其他腾讯企业安全产品联动，可采集终端的网络访问信息，病毒信息，漏洞信息、终端异常行为数据、DDos 信息和 DNS 信息等，结合腾讯威胁情报大数据，对全网终端的安全状态进行多维度的威胁态势分析、溯源、呈现和处置。

5 产品主要功能

5.1 产品功能列表

功能项		**描述**
环境要求	控制中心的安装环境要求	操作系统：64 位 Windows Server 2008 R2 及以上
		CPU：至少 4 核以上
		内存：不低于 16GB
		硬盘：不低于 1TB（需要存放补丁文件、日志等）
		其他要求： 1. 设定服务器一个固定 IP 地址 2. 至少有四个固定可用端口（安装时管理员自行设定） 3. 控制台页面浏览器推荐使用 QQ 浏览器或 chrome 最新版
	客户端的安装环境要求	操作系统：Windows XP_SP3 及以上/Windows Vista/Windows 7/Windows 8/Windows 10
部署终端	网页部署	管理员可以通知终端用户到指定网页下载腾讯安全企业版终端安装包进行安装，适用于终端能连通控制中心的情况
	离线包获取	管理员可自行下载为离线安装包，再拷贝到终端上进行安装，适用于终端无法连通控制中心的情况

首页	安全事件提醒		当内网出现重要安全事件时，在首页进行提醒，管理员可以一键处理、忽略或者进行预警条件的编辑
	安全概况		展示全网安全分数、已部署终端数、待处理威胁数、待处理高危漏洞数，支持一键部署终端、处理威胁和漏洞，同时展示服务器状态，包括 CPU 使用率、磁盘空间、流量情况
	病毒查杀概况图		展示全网一段时间内发生的病毒查杀相关事件的趋势图以及各类事件占比，其中包括未处理、清除成功、清除失败、已信任
	漏洞修复概况图		展示全网一段时间内发生的漏洞修复相关事件的趋势图以及各类事件占比，其中包括未修复、已忽略、修复成功、修复失败
	操作系统分布		展示全网终端的操作系统分布情况及占比
	终端版本分布		展示全网终端的产品版本分布情况及占比
	任务管理		管理员所有任务的管理，支持查看当前最新任务的类型、状态、下发时间、进度，可取消发起的任务，支持查看历史任务类型、下发时间、进度，可删除历史任务
	威胁终端 top10		展示了控制中心下属终端受到威胁最多的前十名
	实时事件展示		滚动展示终端近期发生的病毒漏洞等发现、修复事件
终端管理	终端概况		可查看全网或特定分组内终端的情况，包括计算机名、IP 地址、所在分组、操作系统、实时防护状态、未处理风险数、未修复漏洞数、终端版本等 此外，可选择某终端发起远程协助，直接操控终端进行维护
	病毒查杀		展示全网终端杀毒相关的状态信息，包括计算机名、IP 地址、病毒数、安全防护中心、文件防护、杀毒引擎等信息，并且可以针对选定终端进行快速扫描、全盘扫描等操作
	漏洞管理		按终端显示，可选定终端对漏洞进行扫描、修复操作 按漏洞显示，展示全网存在漏洞的终端，可修复、忽略、取消忽略指定或全部漏洞
	升级管理		展示全网或分组终端的计算机名、IP 地址、主程序版本、病毒库日期，可以对指定或全部终端进行病毒库、主程序版本升级操作
软件管理	软件统计	按软件查看	按软件名称展示全网软件安装情况，包括软件名称、版本、已安装终端、安装率，支持对已安装终端进行提醒卸载操作
		按终端查看	按终端展示全网软件安装情况，包括计算机名、IP 地址、已安装软件数量，支持对终端已安装的软件进行提醒卸载操作
	软件分发		支持用户自定义上传文件、软件、脚本，并分发到指定终端，支持失败重试，弹窗提醒等功能
设备管理	U 盘注册管理	注册 U 盘	注册后的须经管理员授权使用，同时启用加密存储保证数据安全，并支持设置内外网使用权限
		管理注册 U 盘	管理已注册的 U 盘，可修改权限或取消注册

资产管理	硬件资产管理	终端硬件信息	查看终端的主要硬件信息，包括 CPU、内存、硬盘、显示器，并记录硬件变更数，详细信息可进入单点维护查看
		硬件变更日志	查看终端的硬件变更情况，记录并展示变更项、原配置、新配置
策略中心	安全策略	基本设置	提供终端密码保护、升级设置、开机启动项设置、自保护设置等参数配置
		实时防护	安全防护中心：提供 4 层应用入口安全防护、5 层系统底层防护的相关配置，包括：桌面图标防护、摄像头防护、U 盘防护、文件下载防护，文件系统防护、注册表防护、进程防护、驱动防护、黑客入侵防护
		病毒查杀	病毒扫描设置：提供终端在执行扫描任务时的参数配置，包括病毒扫描设置、定时杀毒等设置，支持管理员按路径、扩展名和 MD5 管理信任区和隔离区
		漏洞管理	对终端进行漏洞修复和管理时的参数配置，包括漏洞修复时机、补丁排除列表、其他设置等
		信息采集	对终端进行 Ddos 入侵检测、DNS 入侵检测、杀毒与实时防护、修复漏洞等信息采集
		专家策略	可以查已有专家策略的名称、创建和更新时间、拉取率、执行率、上报率和当前状态，且支持进行相应失效操作等
	管控策略	外设管控	支持按设备类型和硬件端口两种维度管控，对存储类设备支持禁用、只读、读写管控，对其他设备支持禁用、启用，此外支持自定义添加黑名单、白名单，满足复杂管控场景
		进程管控	对常用 IM 进行进程管控，包括 QQ、TIM、微信 PC 版等
单点维护	终端概况	基本信息	显示终端基本信息，包括计算机名、登录用户、IP 地址、MAC 地址、登录域、状态、分组信息、终端版本、病毒库版本、漏洞特征库版本
		远程协助	可对终端发起远程协助，直接操控终端进行维护
		硬件信息	显示终端计算机型号、CPU、主板、内存、主硬盘、显卡、网卡、显示器、声卡信息
		硬件变更	展示终端的硬件变更记录，支持导出
		系统信息	显示终端系统名称、系统类型、系统版本、系统语言、安装日期
	管控策略	外设管控	对单终端的设备和端口进行管控，管控维度与策略中心中相同
日志报表	终端日志	病毒查杀日志	病毒查杀日志总览：展示累计发现病毒的类型分布及趋势图、处理结果分布及趋势图、病毒发现数最多的终端及分组排名、发现最多的病毒排名等
			查杀统计（按终端查看）：支持展示计算机名、分组、IP 地址、检出量，并支持查看各终端感染病毒的详情

			查杀统计（按病毒查看）：支持展示病毒名、类型、全网检出量、各处理结果的数量，可展开查看更详细的病毒信息，并支持查看每种处理结果的终端详情
			病毒查杀日志详情：支持展示检出时间、计算机名、分组、IP 地址、病毒名、类型、处理结果
		系统修复日志	系统修复总览：展示全网系统异常处理结果分布占比及趋势图、系统异常发现数最多的终端及分组排名等
			修复统计（按终端查看）：支持展示计算机名、分组、IP 地址、检出量，并支持查看各终端检出异常的详情
			修复统计（按异常查看）：支持展示异常名、全网检出量、各处理结果的数量，可展开查看更详细的异常信息，并支持查看各处理结果的终端详情
			系统修复日志详情：支持展示检出时间、计算机名、分组、IP 地址、异常名、处理结果
		实时防护日志	实时防护总览：展示全网风险行为处理结果分布占比及趋势图、风险行为发现数最多的终端及分组排名等
			防护统计（按终端查看）：支持展示计算机名、分组、IP 地址、检出量，并支持查看各终端检出的风险详情
			防护统计（按风险查看）：支持展示风险名、全网检出量、各处理结果的数量，并支持查看各风险影响终端的详情
			实时防护日志详情：支持展示检出时间、计算机名、分组、IP 地址、风险名、处理结果
		漏洞修复日志	漏洞修复总览：展示全网漏洞的处理结果比例及趋势图、累计发现漏洞类型的比例及趋势图、高危漏洞未修复数最多的终端及分组排名、发现最多的漏洞排名等
			漏洞统计（按终端查看）：支持展示计算机名、分组、IP 地址、最近扫描时间、检出量，并支持查看各终端检出漏洞的详情
			漏洞统计（按补丁查看）：支持展示补丁 ID、类型、全网检出量、各处理结果的数量，可展开查看更详细的楼栋信息，并支持查看各漏洞影响终端的详情
			漏洞修复日志详情：支持展示检出事件、计算机名、分组、IP 地址、补丁 ID、类型、处理结果
	终端行为日志	安装卸载日志	记录和查看终端机器的客户端安装卸载情况
		升级日志	记录和查看客户端升级情况
		开关机日志	记录和查看终端的开关机情况
系统管理	系统设置	基础设置	包含服务器的基础设置，包括网络通信、级联部署、P2SP 加速、信息登记、级联部署设置等
		升级设置	包含服务器的版本、客户端版本、病毒库、补丁库等升级设置
		安全设置	配置服务器云查杀库、补丁智能预下载等功能
		预警设置	管理控制中心首页安全预警的规则和提醒方式

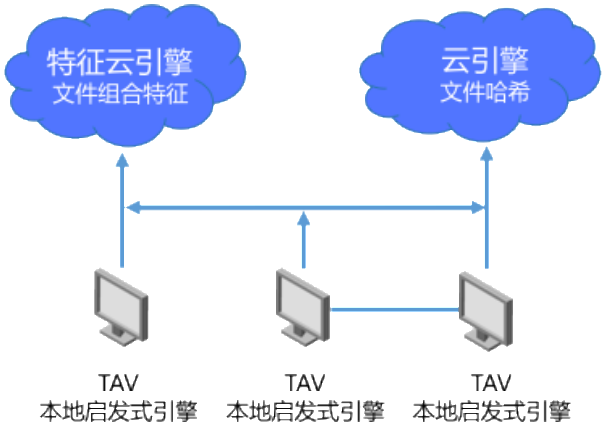
	账号管理	用于配置控制中心账号，超级管理员可新建管理员账号，分为分组管理员、账号管理员、审计管理员，可填入管理员名字，联系方式，管理员类型；可对管理员进行密码重置、信息修改、权限管理、停用、删除等操作
	操作日志	展示管理员操作日志，包括管理员名称、时间、IP、操作、URL、路径、操作内容等
扩展工具	数据备份与迁移	支持在控制中心备份、恢复数据，并支持进行控制中心迁移
	其他工具	右键管理、垃圾清理、文件粉碎、弹窗拦截、启动项管理、网络流量

5.2 产品主要功能描述

- 智能首页
  - 御点首页智能发现全网高危和紧急安全事件，支持一键处置，忽略提醒，自定义预警规则等；
  - 可视化展现全网安全评级、部署情况、病毒漏洞信息及终端版本分布状况等
- 统一的终端管理
  - 全网终端概况
    - 整体安全概况：御点可对内网受控终端安全做宏观展现，通过对当前内网终端感染威胁和漏洞数量进行阶梯形数据分析，便于管理员即时了解当前终端病毒与漏洞的数量比例，以便于及时避免大面积威胁情况的发生。还可提供病毒/漏洞威胁趋势，病毒/漏洞威胁报警，内网终端设备的即时感染状态展示等实用功能。管理员通过控制台可快速查看内网的安全状况，对存在安全威胁的终端迅速处理；
    - 终端概况：管理员通过控制台可查看内网终端的设备信息（如操作系统、CPU、主板等）和终端的基本状况（如在线状态、终端版本、未处理的病毒、未修复的漏洞等）。
  - 全网终端管理
    - 支持收集终端 ip，操作系统版本，登陆用户名，首次在线时间，上次在线时间硬件信息等信息，提供筛选，排序等功能。
    - 支持分组管理：用户对终端进行分组管理，支持手动分组，按照 ip 段分组，以及导入 ladp 组织架构的方式来分组。
    - 支持在终端自定义标签。

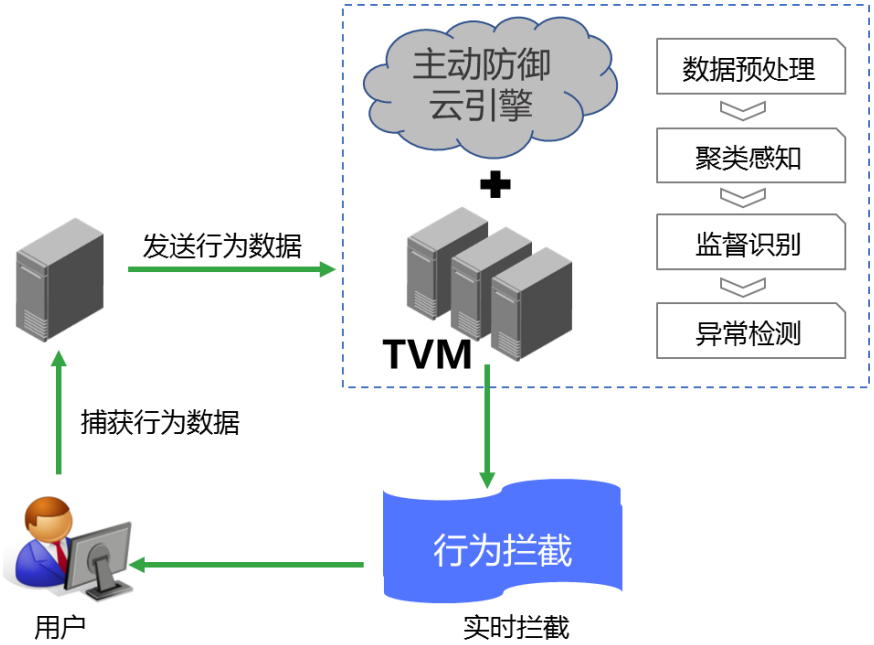
✧ 病毒查杀页面以终端维度，展示病毒数量、防护状态、引擎状态等信息。漏洞修复可以终端或漏洞两种维度，展示内网计算机的漏洞数量、漏洞描述、发布日期、危害程度等信息。

- 病毒查杀
  - 针对已知病毒木马，御点采用双云+TAV 查杀机制，支持企业隔离网的样本更新和宏病毒查杀；采用 TAV 具有速度快、内存占用低、识别率高、全平台支持等特点；适合各种性能配置的电脑终端设备，不卡不慢更安全。

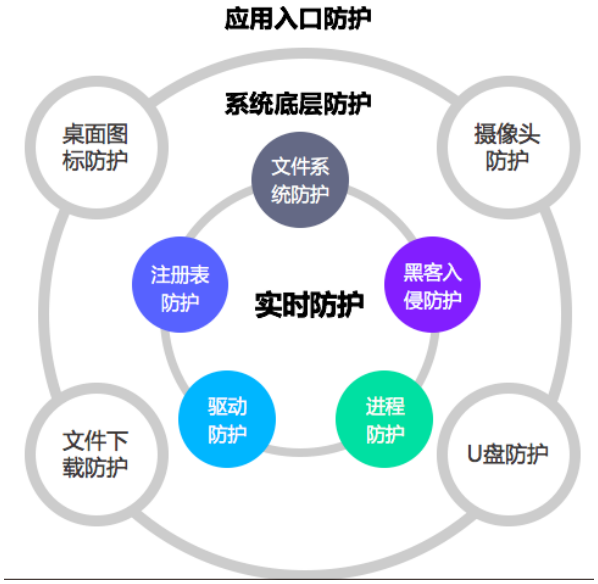


TAV特点：速度快、内存占用低、识别率高、全平台支持、AI启发

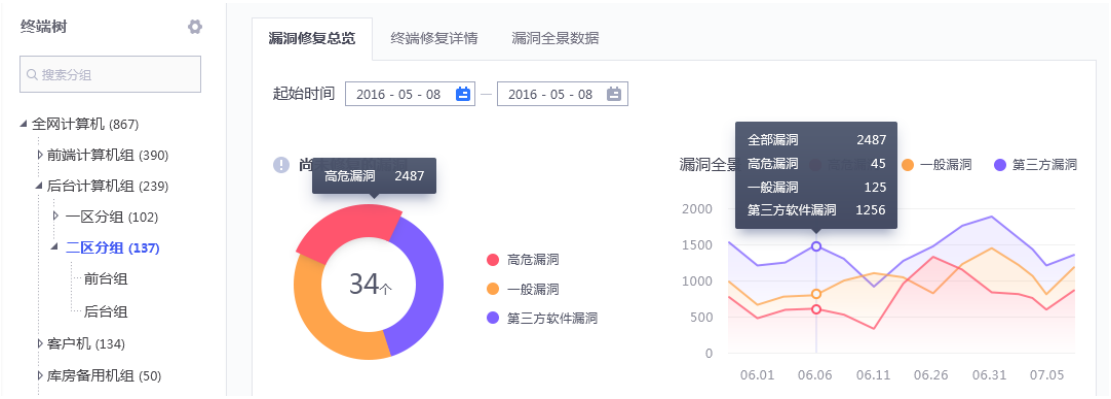
  - 针对未知病毒木马，御点充分利用腾讯安全在用户行为特征和沙箱技术方面的沉淀和优势，及时捕获终端行为数据进行聚类关联分析，识别异常风险，并主动实时拦截。



- 具有多层防护能力，可实时拦截来自系统级、应用入口级的安全威胁，同时可对全网终端设置定期杀毒策略实现全面扫描。



- 漏洞修复
  - 御点可智能扫描内网终端的安全漏洞，管理员通过控制台可查看全网的漏洞情况，并可设置合适的策略对终端漏洞进行修复，在紧急情况下也可通过漏洞修复的即时任务完成修复
  - 支持补丁类型分类，可为医院过滤掉无效补丁
  - 支持补丁错峰下发，保障业务网络带宽使用
  - 提供漏洞排名及终端漏洞情况统计



- 安全和管控策略
  - 可针对不同用户分组设置安全策略和管控策略。安全策略包括病毒查杀、漏洞修复、实时防护等功能配置；管控策略包括进程、外设、网络端口等使用的管控。管理员可以分组或单台终端为维度，制定不同的安全策略和管控策略。

- 软件管理

  该功能融合了腾讯海量软件库和企业上传私有软件库，保证企业内部网软件的正常分发和统计。从两种不同的管理视角（按软件展示和按终端展示）帮助管理员及时了解全网终端软件安装状态，并且可以快速下发相应分发软件及文件脚本等任务。目前覆盖 1 万多款 19 大类常用软件，可帮助用户监控、管理终端软件，具体包括软件统计、软件分发、软件升级、提醒卸载等主要功能。

  1、软件统计：
  - ✧ 按软件查看：软件名称、版本、已安装终端、安装率（已安装御点的终端中）
  - ✧ 操作：搜索、导出、提醒卸载
  - ✧ 按终端查看：终端名称、IP地址、所在分组、软件数量
  - ✧ 操作：搜索、导出、提醒卸载

  2、软件分发：
  - ✧ 支持对文件、脚本、软件进行上传、分发、下载、删除等操作；
  - ✧ 管理员可在上传时配置脚本执行参数，以及在外网搜索软件库中资源，并配置安装成功校验规则；
  - ✧ 分发：支持选择分发时间、分发位置、执行成功是否重试、是否静默安装、失败终端快速选择重试等；

  3、软件行为日志：

- 包含名称、类型、备注、大小、上传时间、成功终端、失败终端、查看详情（分发的详细配置）

- 日志报表

腾讯御点提供多维度，多粒度的日志汇总报表与分析报表，管理员通过控制台的日志报表可详细查看企业内网终端的病毒拦截、补丁修复等情况。御点的日志报表分终端日志和终端行为日志。

- 终端日志

通过控制中心的日志页面，可以看到所有终端的安全行为日志，详细展现终端状态，安全事件类型，处理状态，时间戳，终端名等信息，并能筛选管理员需要的信息。终端日志又分为病毒查杀日志、系统修复日志、主动防御日志和漏洞修复日志。

- 终端行为日志

御点支持对终端行为操作的日志审计，用户在终端行为日志页面，可以查看终端机器的客户端安装卸载情况、客户端升级情况和终端的开关机情况等日志内容。

6 产品主要技术特性

6.1 腾讯 TAV 反病毒引擎

- **引擎介绍**

伴随着我国互联网的迅猛发展，互联网安全问题也日益突出，其中病毒的肆意传播给光大网民带来了诸多困扰。从席卷全球的“WannaCry”勒索病毒，到卷土重来的“暗云Ⅲ”病毒，再到升级传播手段的“Petya”勒索病毒；从徐玉玉案引发大众对于电信网络诈骗的关注，到大学教授被骗上千万等等，2017 年上半年国内各类网络安全事件频发，互联网安全形势日益严峻。

腾讯反病毒实验室基于当前的严峻形式，独立研发推出了 TAV 杀毒引擎，该套引擎集成了腾讯本地反病毒引擎（TAV），腾讯反病毒云（TAV 云）两大功能模块，开放了多个功能性接口 SDK，支持 windows，linux，android 等平台，有完善的海量样本运营体系，更有专业的安全团队支撑，有近 10 年的反病毒技术以及数据积累。其中集成了 TAV 杀毒引擎的腾讯电脑管家和腾讯手机管家分别在 AVC、AVT、VB100、赛可达等国际国内权威评测中取得优异成绩。截止 2017 年 12 月，连续 26 次以 100%的检出率，0 误报通过 VB100 安全评测；以 100%的检出率，0 误报通过 AVC 移动安全测试，排名世界第一；

连续 11 次测试满分通过 AV-TEST 移动安全测试；在赛可达评测中荣获全球第一。

腾讯本地反病毒引擎（TAV）是腾讯反病毒实验室独立研发的运行于终端的判毒程序，无需联网，适合于断网或者隔离网环境下的终端产品集成，例如反病毒客户端、安全盒子、云服务器等应用场景。腾讯御点客户端集成了腾讯本地反病毒引擎（TAV），从而可在隔离网和断网环境为用户提供高效的病毒查杀能力。

- **TAV 杀毒引擎技术特性**

TAV 杀毒引擎代表了中国新一代自主杀毒引擎技术水平，其主要拥有五大技术特性：

1) 增强版特征识别技术，通杀效果好，识别能力高；
2) 复合类文件处理能力，隐匿再深的病毒木马也轻松处理；
3) 脱壳技术，粉碎一切加壳伪装，让病毒无所遁形；
4) 动态模拟检测技术，提前预判恶意行为，动态检测无误判；
5) 基于海量样本的全体系支撑，后台云计算平台提供病毒 DNA 解析大数据处理，支持 TAV 智能打击恶意病毒。

- **主要优势**

采用 TAV 引擎查杀病毒，主要有以下几个优势：

1) 速度快，单文件扫描平均 1ms
2) 内存占用小，内存占用均值在 15M
3) 识别率高，先后获得 AVC、AVT、VB100、赛可达等国内外多家机构的认证
4) 易于集成和扩展，集成代码在 50 行以内
5) 全平台支持，当前支持 windows、linux 以及 android 等全平台
6) AI 启发，除了传统的查杀方式以外支持 AI 查杀，使用 svm，深度学习等方式提升对未知病毒的启发报毒

6.2 基于多步行为判断的主动防御技术

腾讯御点根据样本一系列的行为特征来进行综合的风险判定，其监控和判断能力由后台的大数据训练集群支持。比传统的根据简单的单步行为规则来做监控的主防技术安全系数更高，捕获风险能力更强。

6.3 压缩包查杀技术

支持主流压缩格式，涵盖压缩包、安装包、文档格式解析能力。

6.4 宏病毒专杀能力

腾讯御点提供了精准的分析引擎，可以准确地判断常见宏病毒文档样本，对新型宏病毒攻击给予精确打击。

6.5 主动防御

主动防御通过启发式行为分析，对潜在的威胁动作进行主动的识别，智能判定风险等级并进行拦截，对网页访问、程序下载、文件拷贝等敏感系统边界入口主动发起检测，精准拦截危险文件的落地，将风险隔绝在系统之外。

6.6 实时监控

实时监控功能可以实时监测电脑运行过程中的所有进程。腾讯御点会对设备进行实时监测，出现病毒威胁时，会根据设置，自动删除病毒文件，或者锁定病毒文件禁止其运行，等待处理。

6.7 U 盘管控

腾讯御点 U 盘防护功能对于 U 盘中存储的风险文件进行自动扫描，并告知存在的风险，降低个人电脑遭到破坏的可能性。

6.8 隔离恢复

主动查杀、实时防护、U 盘防护中发现并清除的风险文件，将会被隔离在异常文件恢复区，可以在该恢复区手动恢复您信任的文件以及彻底删除被隔离的文件。

6.9 文件信任区

文件信任区即白名单，腾讯御点在查杀过程中，认为加入信任区的文件是安全的，跳过信任文件库中的文件，加快查杀速度。文件加入白名单需谨慎，若将病毒文件误入白名单，则会造成病毒爆发的严重后果。

6.10 样本运营体系

依赖腾讯 TAV 反病毒引擎准确的样本动态行为捕获技术，和对样本多维度的静态特征分析技术，结合机器学习算法，实现对样本的多方位判别，确保样本准确性。

6.11 升级服务

- **互联网自动升级**

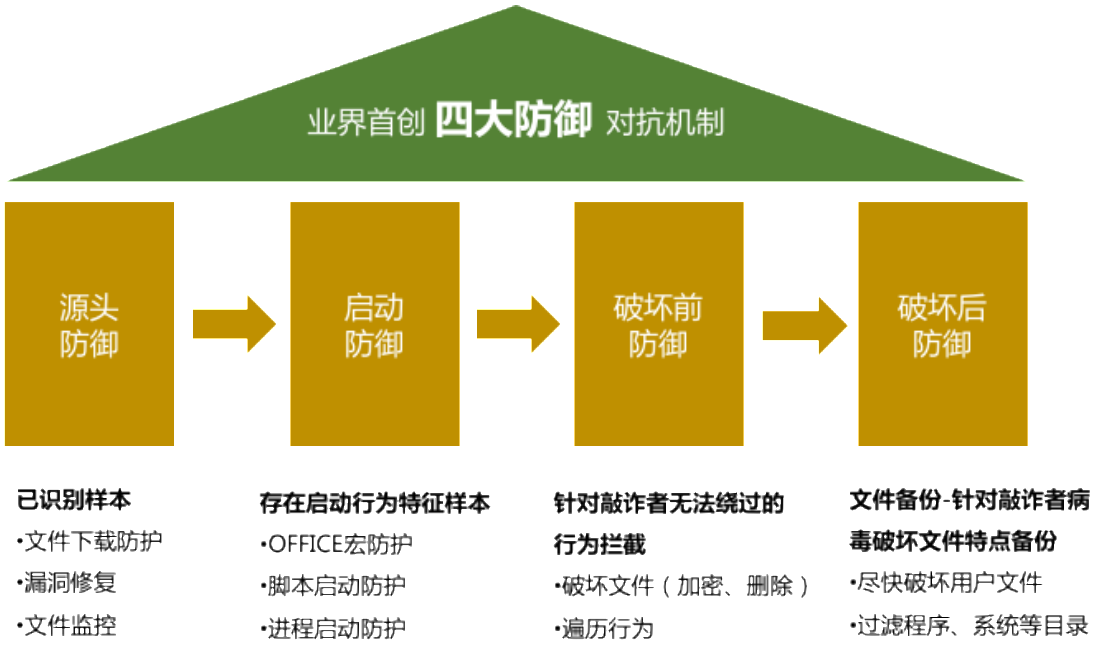
用户环境中，中控平台可以连接互联网，则中控平台定期向互联网病毒升级服务器发送一次请求，若发现更新的病毒库版本，则可自动升级到当前互联网最新病毒库。

- **离线工具手工升级**

若在用户环境中，中控平台不可以连接互联网，且必须通过外部存储器导入数据，则可通过使用离线升级程序来升级中控病毒库。可以使用隔离网离线升级工具，在一台能上网的机器上下载好升级数据，然后导入到中控中心去更新，中控中心下面子控制中心和所有终端客户也能及时进行病毒库、补丁库和终端软件的升级。

7 勒索病毒专项防护

针对时下热门的勒索病毒攻击事件，腾讯御点首创了四大防御对抗机制，从病毒源头、病毒启动、病毒破坏前、病毒后破坏后四个维度进行检测和防御，保证用户终端达到病毒不落地、病毒启动和破坏监控拦截、破坏文件有备份可恢复的防护效果，可为用户量身定制一套针对勒索病毒攻击的专项防护解决方案。



具体在针对勒索病毒的防护功能上，御点会有以下几个方面防护的价值：

1) 网络防护：通过拦截下载器自动下载木马程序、拦截恶意推广程序、拦截黑客远程控制本机、拦截盗号木马，从而降低用户在网络层面与病毒的接触面。
2) 聊天安全防护：御点能检测 QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，并检测 QQ 中对方发来网址的安全性，防止勒索病毒的扩散感染。
3) 移动设备防护：御点提供了 U 盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马。
4) 局域网共享查杀：御点能够对局域网共享文件传输进行检测和查杀，避免勒索病毒通过局域网传播扩散。
5) 漏洞利用防御：御点支持漏洞利用防御，尤其对通过文件漏洞（尤其是 0day 漏洞）的攻击行为进行有效检测与防御。
6) 压缩包杀毒：御点支持文件解压缩病毒查杀，支持对 zip、rar、7z 等多种格式的压缩文件查杀，降低勒索病毒通过伪装成压缩文件传输的可能。
7) 漏洞修复：御点支持修复 Windows 客户端的系统高危漏洞，同时提供功能性更新补丁，防止勒索病毒利用系统高危漏洞攻击。

8 评测升级与奖项

2017 重大评测	亮点

AVC	2017 年在真实世界测试、恶意软件防护测试、性能测试中共获得 3 项 A+； **同卡巴斯基，红伞，Bitdefender，成为上半年全 A+仅有的四个厂商之一**
VB100	连续第 26 次 100%通过
ICSA	继续保持检出、清除测试均通过的好成绩。
赛可达	全球杀软横评排名第一 **第二、第三依次为 360 杀毒、McAfee**
手管 AV-T	腾讯手机管家（WeSecure）获得 13 分满分，检出率 100%，0 误报。继续保持满分通过。 **国际厂商，与卡巴，BD 并列第一；国内厂商，排名稳居第一**
手管 AV-C	检出率 100%， **国际上与 BD、Mcafee、Trend 并列第一；国内安全厂商第一**

9 公司资质

签约方	资质说明
腾讯哈勃分析系统 及腾讯科技（北京）	★公司具备向国家信息安全漏洞库（CNNVD） 提交漏洞的能力
腾讯科技深圳	★公司具备国家计算机病毒应急处理中心 技术支持单位
深圳计算机系统	★公司具备国家网络与信息安全信息通报中心 技术支持单位
腾讯哈勃分析系统 及腾讯科技（北京）	★中国国家信息安全漏洞库支撑单位
玄武实验室 （深圳市腾讯计算机系统）	★国家信息安全漏洞共享平台技术组成员
Tencent PC Manager （腾讯科技深圳）	微软 MAPP 伙伴
腾讯云	CSA 联盟会员
腾讯科技深圳	★互联网安全工作组理事

10　产品资质

产品资质	销售许可证
	软件著作权