终端安全管理系统

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2018-12-06 18:34:11

什么是终端安全管理系统？

终端安全管理系统（下文中也叫御点）是腾讯出品的企业级安全服务。依托腾讯多年的安全经验积累，御点将百亿量级云查杀病毒库、引擎库以及腾讯 TAV 杀毒引擎、系统修复引擎应用到企业内部，可有效防御企业内网终端的病毒木马攻击。御点具备终端杀毒统一管控、修复漏洞统一管控以及策略管控等全方位的安全管理功能，可帮助企业管理者全面了解和管理企业内网的安全状况，保护企业安全。

应用场景

多级管理

网络环境日愈复杂，使得政府机关和大型企事业单位在管理网络安全时面临严峻的挑战。御点利用创新的理念和技术，以统筹管理的树状架构搭建“一个中心、多级管理”的企业安全管理模式，完美解决企业多维度的安全管理诉求。

多平台管理

针对企业多操作系统并存的场景，御点实现了单控制台集中管理，并支持在线、离线、邮件等多种终端部署方式。

策略管理

面对不同行业、不同网络环境、不同发展时期的企业安全诉求，御点可提供最匹配需求的安全管控策略，帮助企业轻松构建360度的立体防御体系。

产品功能

最近更新时间：2019-05-22 14:58:38

智能首页

智能挖掘全网高危和紧急安全事件，提供解决方案一键处置安全风险；可视化图表展现全网安全评级、部署情况、病毒与漏洞等信息，企业安全状况一目了然。

病毒查杀与实时防护

御点客户端具备多层防护能力，实时防护可即时拦截来自网络、驱动、硬件端口、软件、系统内核等安全威胁和黑客攻击；同时国际领先的病毒查杀能力，可深入挖掘潜伏于终端的高级持续威胁（APT）。管理员可通过控制中心，便捷地调用病毒查杀与实时防护能力，高效集中管理企业安全与威胁防御。

漏洞监测与修复

御点可智能扫描企业内网终端的安全漏洞，企业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。

外设管控

通过外设类型和硬件端口两种维度，御点能够帮助管理员快速禁用指定终端的外设使用，诸如禁用 USB 接口、蓝牙、U盘、无线网卡等。对于有特殊需求的终端，管理员可通过白名单，临时放行其指定外设的使用。

进程管控

支持进程名、数字签名、进程描述等多种维度的管控措施，灵活的自定义规则组合配合通配符的支持，极大提升进程管控的覆盖场景。

网络端口管控

管理员能够通过 IP 段、端口段、协议、数据流向等维度，灵活定义终端的网络端口行为。此外，预置数十种常用端口的管控策略和安全建议，极大地提高了管理效率并降低安全风险。

软件统计与分发

详尽掌握企业终端软件的安装和使用情况，软件分发极大方便企业构建终端标准化体系，同时提供卸载指定终端的指定软件的能力，使终端软件合规易如反掌。

策略中心

策略中心包含病毒查杀、漏洞修复、终端管控等众多功能模块的策略管理。通过策略中心，管理员能够针对不同分组和终端，制定最适合的安全和管控策略，真正做到灵活可靠地管理企业安全。

日志报表

图形化日志报表，帮助管理员快速汇总所需信息，以提供可靠的安全决策，见微知著。同时提供终端、事件、详情等多种维度汇总数据，信息量全，条理清晰。支持接入腾讯御见或第三方 SOC 平台，帮助企业统筹信息安全。

远程协助

管理员实时操作远程终端，降低维护成本提高管理效率。高效的图像算法和通信协议，保证画质同时提供极低延迟的操作体验。

管理员权限

普通管理员、审计管理员和帐号管理员三权分立，权限划分精确到分组和功能模块。帮助企业从管理制度消除安全风险，分工有序，权责明晰。

产品优势

最近更新时间：2019-05-22 14:59:05

独立研发的腾讯 TAV 反病毒引擎

TAV 是腾讯安全反病毒实验室独立研发的自主杀毒引擎，代表了中国新一代自主杀毒引擎技术水平。集成该引擎能力的产品曾在国际国内多项权威评测中均取得过多次优异成绩。

- TAV 引擎拥有5大技术特性：
  - 增强版特征识别技术，通杀效果好，识别能力高。
  - 复合类文件处理能力，隐匿再深的病毒木马也轻松处理。
  - 脱壳技术，粉碎一切加壳伪装，让病毒无所遁形。
  - 动态模拟检测技术，提前预判恶意行为，动态检测无误判。
  - 基于1000亿以上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。

基于多步行为判断的主动防御技术

御点可根据样本的系列行为特征来进行综合风险判定，其监控和判断能力由后台的大数据训练集群支持，比根据简单的单步行为规则来做监控的传统防技术安全系数更高，捕获风险能力更强。

超强宏病毒专杀能力

御点精准分析引擎，可准确地判断常见宏病毒文档样本，精准地打击新型宏病毒的攻击。

智能和灵活的漏洞修复策略

针对各种不同类型、不同版本的的操作系统，御点可智能识别终端安全漏洞。为避免集中打补丁导致内网流量暴增，御点还可根据企业内网流量支撑情况的不同限制最大下载带宽，并根据终端补丁修复量灵活地采取分时分段的修复策略。

全面便捷的终端管控能力

御点支持对终端的硬件外设、网络端口、软件进程、软件分发等多种维度的管控，全面杜绝企业敏感数据通过 U 盘、无线网卡、不合规的软件和网络使用等渠道泄露，同时极大降低外部黑客入侵的风险。御点提供便捷快速的管理方式，能够快速设定所需管控的项目，建立标准化的终端安全体系。

适应复杂的企业终端环境

御点是专为企业用户定制的安全解决方案，客户端支持 Windows、Windows Server、Linux、macOS 等主流操作系统，支持从普通 PC 到服务器端的安全管理能力，同时对非管理员权限和受限用户的终端具备很好地兼容性。