

# iOA 零信任安全管理系统

## 产品简介



腾讯云

## 【 版权声明 】

©2013–2026 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

## 【 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 4009100100或 95716。

# 文档目录

## 产品简介

产品概述

产品组件

套餐与版本说明

产品优势

应用场景

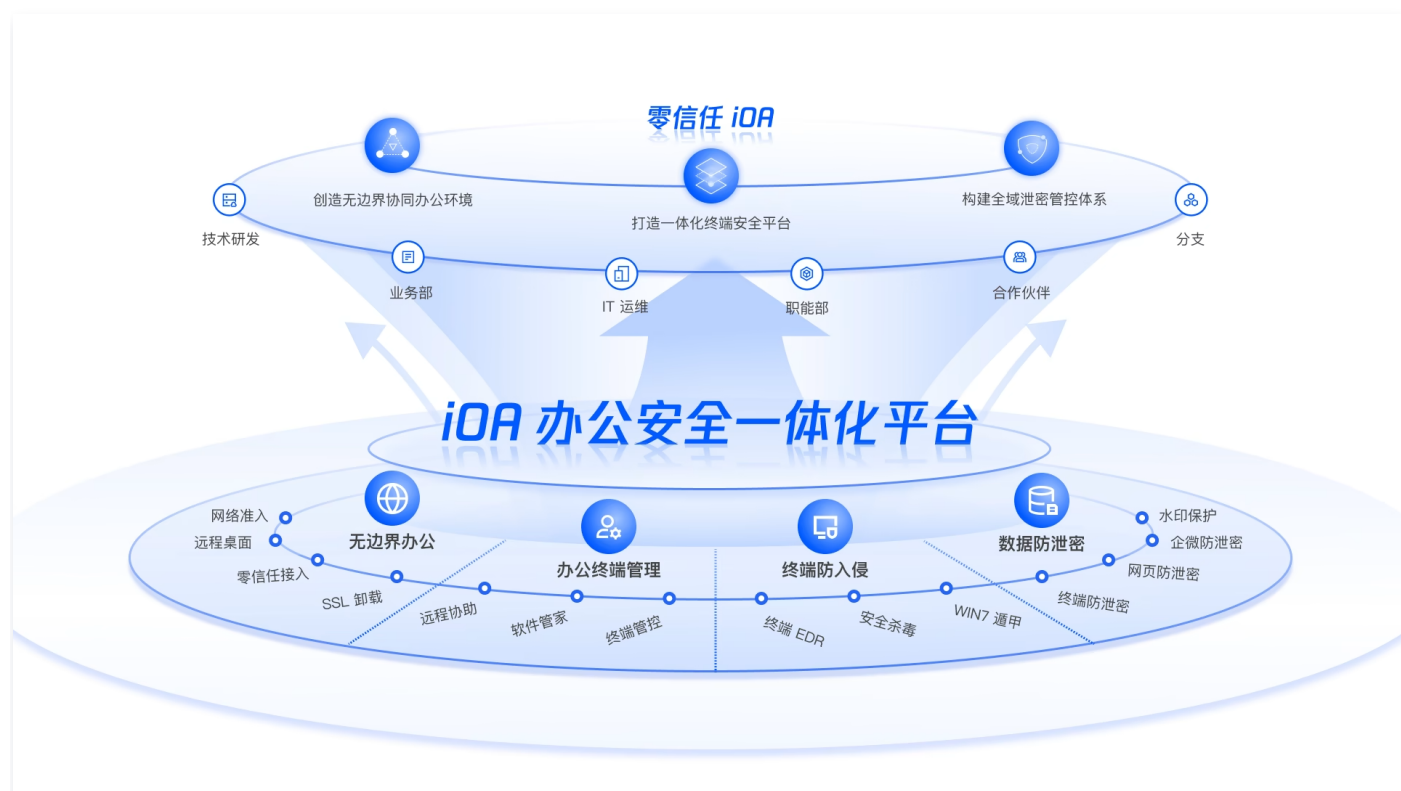
视频介绍

# 产品简介

## 产品概述

最近更新时间：2026-06-03 12:04:00

iOA 零信任安全管理系统，以下简称“腾讯 iOA”，是腾讯基于零信任安全理念和内部自用实践，自主设计和研发的一款办公安全产品，为客户提供一体化的终端安全能力，覆盖终端设备的各类办公使用场景，基于一个客户端构建零信任接入、终端管控、安全防护、数据防泄密等核心安全能力，帮助企业创造**安全、稳定、高效**的办公环境。



## 核心理念与架构设计

### 零信任原则

遵循“永不信任，持续验证”的安全理念，打破传统内网信任假设，无论访问者位于内网还是外网，对所有访问请求进行动态身份验证和最小权限控制。

### 一体化办公安全平台

腾讯 iOA 涵盖零信任接入、终端管理（UEM）、终端安全防护（EPP）、终端检测响应（EDR）、数据防泄密（DLP）、软件管理、远程协助等十余种安全能力，实现一体化的终端安全管控。

## 产品功能

### 零信任安全接入

腾讯 iOA 遵循零信任理念，构建以身份为核心的网络安全新边界，通过连接器反连、SPA 单包授权等技术收缩业务暴露面，无需暴露内网 IP，并对用户身份、终端环境、访问权限进行持续校验以及动态访问控制，保障用户访问企业应用过程中的安全性，帮助企业实现应用安全访问，并支持企业员工随时随地高效办公。

## 终端安全防护（EPP+EDR）

腾讯 iOA 支持终端杀毒 EPP 和终端检测与响应 EDR，快速发现及处置终端各类安全威胁。支持病毒查杀、漏洞修复、勒索防护、钓鱼防护等，并结合终端行为检测及时发现各类高级安全威胁，有效应对银狐等新型病毒攻击，帮助企业在复杂多变的网络攻防形势中，变被动为主动，快速发现威胁、及时响应处置和溯源。

## 统一终端管理（UEM）

腾讯 iOA 提供丰富灵活的终端管理手段和多样化的终端管控策略，帮助企业做好事前的终端管理，降低潜在的安全风险，支持终端软硬件信息采集、分组管理、运行监控、安全加固、软件管理、盗版软件检测、外设管控、文件管控、水印管控等，统一管理运维企业终端，让企业全网终端资产可视、可控、可管。

## 数据防泄密（DLP）

以数据为中心，通过数据资产识别、数据流转渠道识别、数据流转动态控制、泄密行为溯源等能力，覆盖终端、业务网关等多种泄密场景，实现端到端防护，有效防止企业敏感数据被未经授权的访问和泄露。

## 网络准入（NAC）

腾讯 iOA 提供网络准入控制能力，支持 802.1x 认证、MAC 认证、Portal 认证等多种接入方式，覆盖员工终端、访客终端、哑终端等多类型终端入网管理。支持网络基础配置、准入策略部署、接入审计与故障排查等全生命周期管理，实现终端入网身份可信、状态合规、行为可控，帮助企业构建安全有序的网络接入边界，保障内网资源仅对可信终端和可信用户开放访问。

## AI 安全中心

AI 安全中心通过 AI 资产清单管理、Skill 风险扫描与处置、Agent 运行时防护、安全沙箱隔离管控等能力，集中管理企业内 AI Agent 及 Skills，实时识别恶意 Skill、Prompt 注入和漏洞风险，并从命令、文件、网络多维度对 AI 应用进行边界管控与审计追溯，保障企业 AI 应用安全可控运行。

## 远程协助

支持一键发起远程协助，帮助管理员高效运维管理分散的终端，支持公有云加速、智能中继访问，在弱网环境/跨运营商下的访问速率大幅优化，支持扩展屏识别、远程文件传输、共享剪贴板、操作被控端 UAC 弹窗等，提高终端运维管理效率。支持控制台到终端、终端到终端远程，满足多种终端远程场景需求。

## 产品架构

腾讯 iOA 是腾讯基于零信任安全理念，自主研发设计的一款终端安全产品。在产品架构设计时，参考了零信任 SDP（Software-Defined Perimeter，软件定义边界）的设计理念，由零信任控制中心、零信任安全网关、零信任客户端等组件构成，并围绕可信接入、终端管理、入侵防护、数据保护等四个维度构建了多种安全能力，帮助客户解决不同场景下的终端安全问题。



## 部署方式

腾讯 iOA 支持私有化部署和 SaaS 化部署，客户可根据实际需求灵活选择：

iOA-SaaS	iOA-私有化
<ul style="list-style-type: none"> <li>基于腾讯云部署，开箱即用，灵活按需采购。</li> <li>无需复杂配置即可快速上线，满足企业不同层级需求，降低初期投入成本。</li> <li>支持自动更新和维护，确保系统始终处于最新状态，减少 IT 运维负担。</li> </ul>	<ul style="list-style-type: none"> <li>本地化部署，保障企业隐私，稳定可靠。</li> <li>确保数据安全和系统稳定，适合高合规要求行业、对数据隐私和安全性要求较高的企业。</li> <li>支持深度集成和个性化配置，满足企业特定需求，提供专属技术支持，确保系统高效运行。</li> </ul>

### 说明：

私有化和 SaaS 交付形式不同，但底层架构和用户呈现形态一致，均能灵活适应多种应用场景。

# 产品组件

最近更新时间：2025-08-12 10:53:02

## iOA-SaaS

### 零信任控制中心

零信任控制中心是整个零信任解决方案的控制管理平面，腾讯 iOA SaaS 版本的零信任控制中心部署在腾讯云的服务器上。管理员可以通过浏览器远程管理和查看，通过零信任控制中心可以实现用户认证和安全策略的配置与下发，主要包含用户管理、访问配置管理、终端管理、软件管理、终端杀毒 EPP、终端检测与响应 EDR、终端防泄密 DLP 等多个安全模块。同时零信任控制中心也具备良好的第三方对接能力，可以通过 Syslog、Kafka、API 接口等形式与第三方安全产品进行数据传输和功能调用。

### 零信任安全网关

零信任安全网关是零信任解决方案的数据转发平面，腾讯 iOA SaaS 版本的零信任安全网关部署在腾讯云的服务器上，负责执行零信任控制中心下发的各项授权策略，代理转发客户端的合法访问请求，拦截非法访问请求。通过代理转发的业务逻辑保护企业的核心资源和数据，确保未认证用户无法访问被保护的業務资源。

零信任安全网关支持多种常见访问协议代理：3 层 IP 代理、4 层 TCP 代理、7 层 Web 代理，基于腾讯内部自研高性能传输协议，可以适用于多种不同类型的应用代理访问，例如常见的 OA、Mail、ERP、H5 应用等，为用户提供稳定的加密访问通道。

### 零信任客户端

腾讯 iOA 客户端支持 PC 端和移动端部署，在零信任解决方案中，出于安全和业务稳定发布考虑，我们通常建议用户安装零信任客户端，但腾讯 iOA 也支持无端访问，在部分无法安装客户端的场景下，也可以帮助用户实现业务安全访问。

腾讯 iOA 客户端支持对终端安全环境进行实时监测，根据企业设置的策略及时上报终端信息给到零信任控制中心，并执行控制中心下发的各项安全策略。只有用户通过控制中心认证，才能实现业务安全访问。

腾讯 iOA 同时还具备强大的扩展能力，基于一个客户端，腾讯 iOA 可提供终端安全管理、终端杀毒 EPP、终端检测与响应 EDR、终端防泄密 DLP 等多项安全能力，在终端侧构建闭环的安全防护体系，帮助客户解决终端在办公场景下的多种安全问题，让安全融入业务。

### 连接器

为了便于客户通过腾讯云上的安全网关访问本地业务，在腾讯 iOA SaaS 交付时，需要在业务侧部署连接器，并反向连接到 iOA 零信任安全网关（部署在腾讯云），避免业务系统直接暴露于互联网上。连接器通常部署在 DMZ 区，打通业务资源到腾讯云网关，保障用户可使用客户端/浏览器安全地访问业务资源。

## iOA-私有化

### 零信任控制中心

零信任控制中心是整个零信任解决方案的控制管理平面，企业私有化部署在企业的服务器/云服务器上，管理员可以通过浏览器进行远程管理和查看，通过零信任控制中心可以实现用户认证和安全策略的配置与下发，主要包含用户管理、访问配置管理、终端管理、软件管理、终端杀毒 EPP、终端检测与响应 EDR、终端准入、终端防泄密 DLP 等多个安全模块。同时零信任控制中心也具备良好的第三方对接能力，可以通过 Syslog、Kafka、API 接口等形式与第三方安全产品进行数据传输和功能调用。

## 零信任安全网关

零信任安全网关是零信任解决方案的数据转发平面，一般部署在 DMZ 区域或其他内网可达区域，负责执行零信任控制中心下发的各项授权策略，代理转发客户端的合法访问请求，拦截非法访问请求。通过代理转发的业务逻辑保护企业的核心资源和数据，确保未认证用户无法访问被保护的業務资源。

零信任安全网关支持多种常见访问协议代理：3 层 IP 代理、4 层 TCP 代理、7 层 Web 代理，基于腾讯内部自研高性能传输协议，可以适用于多种不同类型的应用代理访问，例如常见的 OA、Mail、ERP、语音电话、视频会议、H5 应用等，为用户提供稳定的加密访问通道。

零信任安全网关支持高可用部署架构，并可以根据实际业务访问量及并发负载，进行水平扩展，保障访问企业后端业务系统的连续可用性。

## 零信任客户端

腾讯 iOA 客户端支持 PC 端和移动端部署，在零信任解决方案中，出于安全和业务稳定发布考虑，我们通常建议用户安装零信任客户端，但腾讯 iOA 也支持无端访问，在部分无法安装客户端的场景下，也可以帮助用户实现业务安全访问。

腾讯 iOA 客户端支持对终端安全环境进行实时监测，及时上报终端信息给到零信任控制中心，并执行控制中心下发的各项安全策略。只有用户通过控制中心认证，才能实现业务安全访问。

腾讯 iOA 同时还具备强大的扩展能力，基于一个客户端，腾讯 iOA 可提供终端安全管理、终端杀毒 EPP、终端检测与响应 EDR、终端准入、终端防泄密 DLP 等多项安全能力，在终端侧构建闭环的安全防护体系，帮助客户解决终端在办公场景下的多种安全问题，让安全融入业务。

# 套餐与版本说明

最近更新时间：2026-03-23 09:47:12

## iOA SaaS

腾讯 iOA-SaaS 零信任安全管理系统（以下简称 iOA-SaaS）采用订阅采购模式（按年/月），目前提供四种版本类型，包括基础版、终端安全专业版、远程接入专业版和高级版。具体版本所包含的能力如下，可单击 [立即选购](#) 进行购买。

模块	功能	基础版	终端安全专业版	远程接入专业版	高级版
敏捷运维	终端分组管理	√	√	√	√
	终端智能聚类	√	√	√	√
	导出终端信息	√	√	√	√
	终端运行状态监控	√	√	√	√
	软件安装统计	√	√	√	√
	软件/文件/壁纸/脚本分发	√	√	√	√
	软件盗版检测	√	√	√	√
	软件统一卸载	√	√	√	√
	软件运行管控	√	√	√	√
	远程协助	可升级极速版远程协助	可升级极速版远程协助	可升级极速版远程协助	可升级极速版远程协助
	办公终端合规检测	√	√	√	√
	安全加固	√	√	-	√
	定时关机/定时锁屏	√	√	-	√
	上网行为管控	√	√	-	√
	防火墙管控	-	√	-	√

	网络服务与端口管控	-	√	-	√
	进程注入白名单	-	√	-	√
	广告弹窗拦截	√	√	√	√
	客户端自保护	√	√	√	√
	客户端升级/卸载管理	√	√	√	√
	日志查看	√	√	√	√
终端防入侵	病毒查杀/定时查杀	√	√	-	√
	漏洞扫描与修复	√	√	-	√
	漏洞利用防御	√	√	-	√
	密码爆破防御	√	√	-	√
	文件实时防护	√	√	-	√
	访问信息采集	√	√	-	√
	钓鱼攻击防护	√	√	-	√
	远程登录防护(防勒索)	√	√	-	√
	文档备份(防勒索)	√	√	-	√
	终端勒索诱饵	√	√	-	√
	终端威胁告警	可选购	可选购	可选购	可选购
	全链路威胁事件调查	可选购	可选购	可选购	可选购
	威胁自动响应	可选购	可选购	可选购	可选购
威胁人工处置	可选购	可选购	可选购	可选购	
威胁狩猎溯源	可选购	可选购	可选购	可选购	

	检测规则运营	可选购	可选购	可选购	可选购
数据保护	敏感数据分级分类管理	可选购	可选购	可选购	可选购
	敏感数据分布统计	可选购	可选购	可选购	可选购
	文件外发行为审计	可选购	可选购	可选购	可选购
	文件外发告警拦截	可选购	可选购	可选购	可选购
	敏感资源访问控制	可选购	可选购	可选购	可选购
	加密 U 盘	-	√	-	√
	终端外设管控	√	√	√	√
	屏幕水印/打印水印	√	√	√	√
	文件操作管控	√	√	√	√
	文件操作审计	√	√	√	√
无边界办公	身份认证与账号安全	√	√	√	√
	业务资源访问	可选购	可选购	√	√
	动态访问控制	可选购	可选购	√	√
	用户行为风险分析	-	√	√	√
	办公提效工具	√	√	√	√

## iOA-私有化

腾讯 iOA-私有化零信任安全管理系统（以下简称 iOA-私有化）支持订阅采购和买断采购两种模式，由于私有化部署需要结合客户当前的终端规模、业务资源现状进行选型设计，若您需要进行私有化部署，请单击链接选择人工服务[在线支持](#)，我们的工作人员会及时与您沟通。

📢 说明：

如果您需要体验产品，可直接单击 [申请试用](#)，完成企业及联系人信息填写，我们的工作人员会尽快与您联系。

# 产品优势

最近更新时间：2025-08-20 19:10:42

腾讯 iOA 由腾讯电脑管家原生团队研发，基于腾讯集团内部零信任实践打磨，也是基于国内互联网背景研发的办公终端安全一体化产品，目前已服务上千家 B 端客户，是具有腾讯特色的终端安全产品。结合模块化的产品设计，让企业客户的采购和实施更加平滑，致力于持续提升用户的办公体验。

## 方案易落地

- 一体化终端交付：腾讯 iOA 集成了零信任接入、安全管控、终端杀毒 EPP、终端检测与响应 EDR、数据安全防护 DLP 等多个安全模块，具备完整的终端安全能力，可根据客户购买的版本进行一体化交付。
- 交付形态更多样：腾讯 iOA 支持多种交付形态，既可以私有化部署，也可以 SaaS 化部署，可基于客户的实际安全需求进行灵活部署，适用于不同行业、不同规模的客户需求。

## 安全效果好

- 终端安全更完整：腾讯 iOA 原生集成 EPP/EDR 模块，通过一个客户端实现终端安全闭环防护，基于腾讯安全多年来所积累的技术能力，在防钓鱼、防勒索、防横移等场景精雕细琢，构建了事前、事中、事后一体化防御能力，在多次攻防演练实战中取得了显著成果。
- 安全管控更强大：腾讯 iOA 深入挖掘企业 IT 管理痛点，提供了大量安全管控能力，包含违规外联检测、设备及端口管控、高危进程禁用、闲置终端管控、异常访问行为监测、弱密码监测等多个安全能力。
- 数据保护更完整：为帮助企业加强数据安全合规建设，腾讯 iOA 支持敏感文件识别管控、文件监控、文件水印等多种数据防泄密手段，降低企业核心资产数据泄露风险。
- 安全防护更全面：针对上下游供应链企业，腾讯 iOA SaaS 基础版可免费为其提供终端管控、病毒查杀、实时防护、勒索/钓鱼防护等一系列安全能力，帮助企业完善安全建设，提升企业安全防护效果。

## 用户体验佳

- 业务访问更稳定：基于腾讯内部需求打磨，iOA 团队自研新型安全接入协议，在 L3 层 VPN 基础上实现连接级访问控制，既解决传统 VPN 长连接不稳定的问题，同时也保障了安全防护效果。
- 终端部署更轻量：腾讯 iOA 原生打造多个安全模块，部署实施更轻量，同时兼顾了安全效果和兼容性，例如 EDR 终端 CPU 占用率 $\leq 1\%$ ，内存占用 $\leq 40\text{MB}$ ，大幅减少对终端性能的影响，降低 IT 管理员运维压力，与市面上主流杀毒软件均可以无打扰共存。
- 终端管理更便捷：支持多种电脑小工具，包含垃圾清理、净网、启动项管理，文档守护者等能力，通过一个终端帮助用户解决多种问题，基于内部实践，构建终端安全防护新体验。

# 应用场景

最近更新时间：2026-06-03 12:04:00

应用场景	现状	挑战	腾讯 iOA 解决方案	适用客户群
远程办公场景	远程办公成为常态，员工出差、分支接入等情况需要灵活地访问公司内部应用。	业务暴露面大，安全防护成本增加；VPN 漏洞频发，易被攻击利用，访问权限管理粗放等。	通过零信任安全架构，结合连接器反连或 SPA 单包授权技术隐藏企业应用暴露面，结合持续信任评估与动态访问控制，实现用户到应用的安全访问。	所有企业
多云业务访问	业务云化部署，除了自建 IDC，业务还分布在其他公有云，这些应用都需要能够安全且便捷地访问到。	传统零信任或 VPN 方案较重，无法灵活适应多云环境，需要购买多套或者分别部署网关，成本较高且管理复杂。	通过灵活部署轻量化的连接器，快速打通多个云环境中的业务系统，通过腾讯云零信任网关统一对外发布，实现业务快速上线，并通过零信任做持续风险评估及动态访问管控。	多云架构企业
IT 资产管理与加固	企业终端设备数量多且分散，资产信息混乱（如型号、配置、使用状态不明），并且终端没有统一管控措施，员工违规使用带来安全风险。	终端资产不可视，人工统计资产耗时且易出错，资产变更难实时跟踪，安全基线不统一，风险操作难管控。	腾讯 iOA 支持采集终端资产信息以实时更新资产状态，支持自定义分组管理及运行状态监控等；并可统一进行系统安全加固、外设管控、水印保护、上网行为管理等标准化管理控制。	所有企业
软件全生命周期管理	企业员工如果安装未授权软件（如盗版设计工具），可能占用终端资源并引发合规风险，部分软件还可能携带恶意插件。	人工排查效率低，难以覆盖多分支终端；伪装软件难识别，多终端软件版本难统一，盗版软件带来法律诉讼风险等。	腾讯 iOA 提供软件分发、安装统计、运行黑白名单管控、盗版软件检测、软件卸载等软件全生命周期管理与控制手段，帮助企业标准化管理内部软件的使用。	所有企业
远程 IT 运维	员工终端故障（如软件崩溃、系统异常）时，传统运维依赖现场支持，响应慢，影响工作进度。	现场运维成本高、效率低，IT 管理工作量大，传统远程工具卡顿、传输慢并可能存在安全风险。	通过极速远程协助，一键远程对应终端，支持文件传输、公有云加速、画质优化等，并且支持无人值守设备远程，提升远程体验与运维效率。	IT 团队较小、设备分散的企业
终端安全	企业内部终端面临各种病毒入侵、漏	内部防护工具碎片化、策略配置不统	腾讯 iOA 构建一体化安全防护平台，依托腾讯 TAV+云引	所有企业

防护	洞攻击、系统入侵等风险，亟需有效防护手段。	一、安全软件互相冲突等，导致安全防护无法形成合力，防护效果难保障。	擎，提供恶意样本查杀、热门威胁防御和漏洞修复等防御能力，并针对勒索/钓鱼进行专项防护，构建立体安全防御体系。	
高级威胁检测与响应	企业面临 APT 攻击（长期潜伏窃取数据）、勒索钓鱼、银狐攻击等威胁，防护手段不足，攻击响应依赖人工，处置效率低。	APT 攻击隐蔽性强，如加密通信、低频操作、白加黑劫持、驱动级对抗等，传统检测手段难发现，无法实现有效防护。	iOA-EDR 通过全面覆盖 ATT&CK 攻击链路，精准识别钓鱼、勒索攻击等高级安全威胁，利用全链路精确溯源系统，还原攻击事件，完成精准告警溯源与事件处理。	中大型企业
攻防演练安全防护	在攻防演练活动中，攻击方会使用多种攻击手法对防守方进行攻击，这对终端的安全防护提出了更大挑战。	攻击方更多会使用钓鱼、Oday 漏洞、无文件攻击等特定攻击手法进行定向攻击，传统杀毒等基础安全防护很难有效防护这些攻击手段。	iOA-EDR 实时采集终端安全信息，有效识别防护各类高级攻击手法，并对威胁进行实时对抗，保障客户在攻防演练活动中终端防护的有效性，降低因终端失陷丢分的情况。	参加重保/攻防演练的企业
数据防泄密	企业敏感数据（如客户信息、研发代码、财务数据）在协作、外发、存储时，易因未经授权员工的外发造成核心数据泄露。	数据缺少分级分类识别，只能一刀切管控；管控通道不全面，容易被绕过；泄露后无法追溯，操作日志缺失，难以满足监管审计。	腾讯 iOA 内置丰富的企业常见敏感数据识别规则库，支持自定义对敏感数据分级分类识别，并对数据外发通道进行全面审计或拦截，有效防止企业敏感数据泄漏。	科技型、研发型、互联网、制造业等企业
AI 安全中心	大模型与 AI Agent 加速覆盖研发、办公、客服等业务环节，员工自发使用客户端 Agent、编程类 Agent 等大量 AI 应用，并可随意从开源市场下载第三方 Skill 在本地终端运行。	AI 资产分散难盘点，Shadow AI 形成盲区；Skill 投毒、Prompt 注入等 AI 特有攻击传统安全防护方式无法识别；并且 Agent 拥有系统管理员权限缺少行为边界管控；针对 AI 行为无日志难审计。	腾讯 iOA AI 安全中心提供 AI 资产自动发现、Skill 多引擎检测、Agent 漏洞与暴露面治理、Agent 运行时三重防护（Prompt + Skill + 脚本）、独立安全沙箱（命令 + 文件 + 网络）及全量行为审计，构建一体化 AI 安全治理体系。	所有企业
网络准入	设备接入企业网络无任何检查，黑客的危险设备、外部访客的非授权设备入网后会造成企业	非法终端直接访问内网，横向移动风险高；访客和员工自带设备访问企业内网的行为不可审计。	腾讯 iOA 网络准入支持 802.1x、MAC、Portal 多种认证方式，实现员工终端可信接入、访客网络隔离与哑终端自动	所有企业

内网终端沦陷和数据泄密。

纳管，构建"身份+设备+行为"多维准入控制体系。

# 视频介绍

最近更新时间：2024-07-12 15:14:41

观看以下视频多方面了解腾讯 iOA 解决方案。

为什么企业需要零信任?  
01'00"

为什么企业需要零信任?

腾讯零信任安全实践篇  
03'24"

腾讯零信任安全实践篇

腾讯零信任解决方案  
03'53"

腾讯零信任解决方案