顶 象
DINGXIANG

智能互联·万物安全

公司简介

顶象技术在互联网、物联网应用，云计算和大数据等领域构建了端到端、全环节、全链路和全维度的全景式业务安全风控体系，能够为航空、银行、保险、互联网金融、智能硬件、游戏、社交等行业提供智能风险感知和经济实效的安全防护，让企业免受薅羊毛、账号盗用、刷榜炒信、欺诈交易等威胁，保护物联网智能设备应用安全。赋予企业坚实、有限的防御能力。

顶象技术在全资收购北京花甲技术公司后，在物联网设备端安全防护领域进一步拥有了业内领先的安全防护技术。可以为企业客户提供国际领先、技术成熟的产品解决方案和服务。顶象技术目前可以为企业客户提供跨平台使用的安全防护方案。智能设备端安全防控，支持各种移动平台操作系统，支持芯片级的运行环境，为客户的业务发展保驾护航。

顶象技术致力于打造零风险的数字世界，是中国领先的业务安全产品与解决方案提供商，红杉资本中国基金成员企业。总部位于北京，在杭州设有分公司、广州、南京等城市均建立研发中心校，其创始团队主要来自阿里巴巴、腾讯、花甲科技、趋势科技、华为、百度等公司。

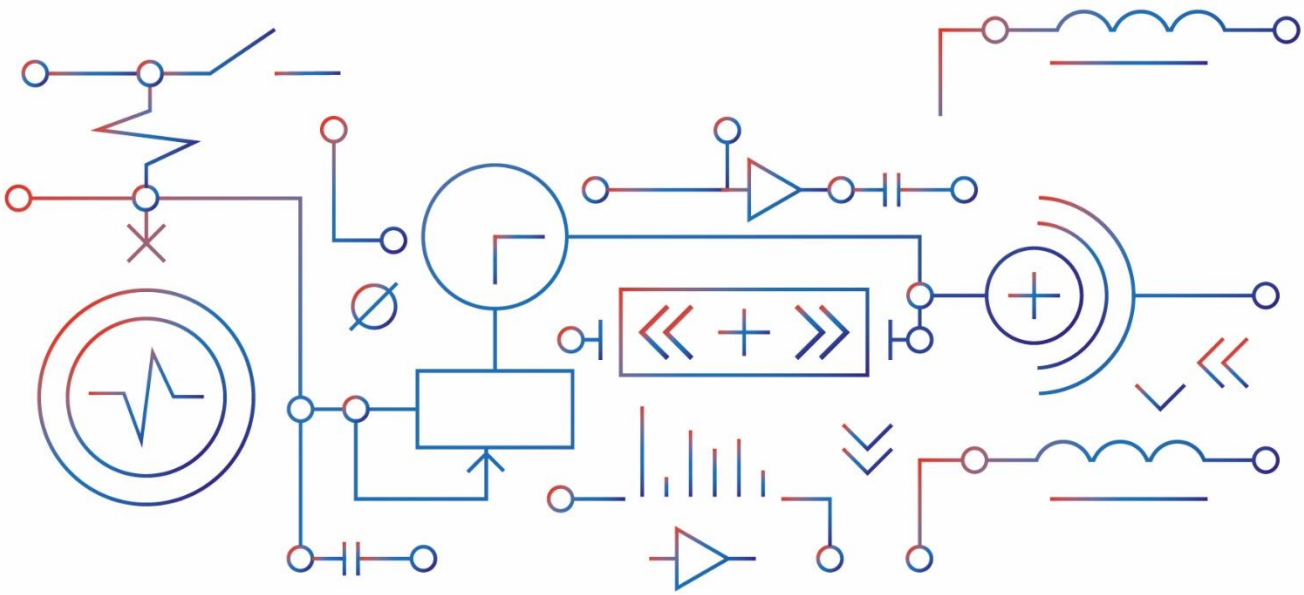
物联网安全防护需求日益凸显

2016年10月，Mirai僵尸网络爆发，导致半个北美州的网站服务断线，其中就包括了Twitter、Reddit和Netflix三大网络。黑客发动攻击的“僵尸网络”是大部分防护薄弱且已经被黑客控制的网络摄像头。无独有偶，今年上半年，北京、浙江多地爆出家用摄像头风险，除了公开出售IP，甚至还有破解软件在QQ群中传播叫卖。

随着越来越多的物联网设备开始接入互联网，由于防护困难或者对安全性的忽视，使得物联网设备里的应用程序体异常脆弱，很容易被攻击者发现漏洞并利用。

Mirai僵尸网络的出现可谓影响深远。事件发生26天后，美国国土安全部DHS就发布了《保障物联网安全战略原则》。其中提出，物联网制造商必须在产品设计阶段构建安全，否则可能会被起诉。工信部也在今年1月份发布的《物联网发展规划（2016—2020年）》提出了物联网产业未来五年发展的主要任务，在物联网关键技术标准制定、关键核心技术创新、行业标准研制、物联网与行业领域的深度融合等方面给出了详细的指导意见。

物联网的设备是基于智能感知、识别技术与计算通信技术，实现物物之间的互联互通，所以IoT设备的安全，除了其本身工业制造品质之外，还涉及移动设备安全、通讯协议传输安全、隐私信息数据等等安全问题。



来自黑灰产的严峻挑战

2017年末，中国数字经济总量超过27万亿，占GDP总量33%，与此同时，网络犯罪已经形成产业化黑灰产从业者已超过百万，黑灰产每年造成直接损失达千亿，导致社会成本增加5千亿。黑灰产从业人员专业度超过多数技术人员，攻防能力不对称将长期存在。网络犯罪不断被重新定义，国家安全经济发展受到严峻挑战，国家立法，安全产业化、产品化和知识经验共享是必由之路。

数据

数据窃取 数据伪造

用户

垃圾账号 虚假身份
网络钓鱼 隐私窃取

内容

违禁内容 涉黄图片

业务

黄牛刷单 活动作弊
账号盗用

应用

逻辑逆向 破解外挂
应用漏洞

传输

信息截取 消息伪造
流量劫持

系统

系统漏洞 病毒木马

硬件

硬件漏洞 协议漏洞

IoT行业解决方案

业内率先利用虚机保护技术，对工控级芯片的核心算法进行高强度保护，内存占用小于30K，且性能无损失。

顶象多平台全流程端安全产品 DX-ESS

DX-ESS（Endpoint Security Solution）针对各类终端面临的逻辑破解、数据篡改、业务欺诈、数据窃取等种类风险，为客户提供多平台、全流程的解决方案，用户可一站式组合应用，也可独立选用。

Android & iOS 平台APP防护

针对Android/iOS移动端App，顶象利用专利的虚机源码保护技术，将App的核心代码置于安全的虚机环境中隔离运行，强力对抗各种逆向分析工具和手段。不仅如此，顶象还为每款App生成完全不同的虚机，从而为App实现了一机一密的安全性。

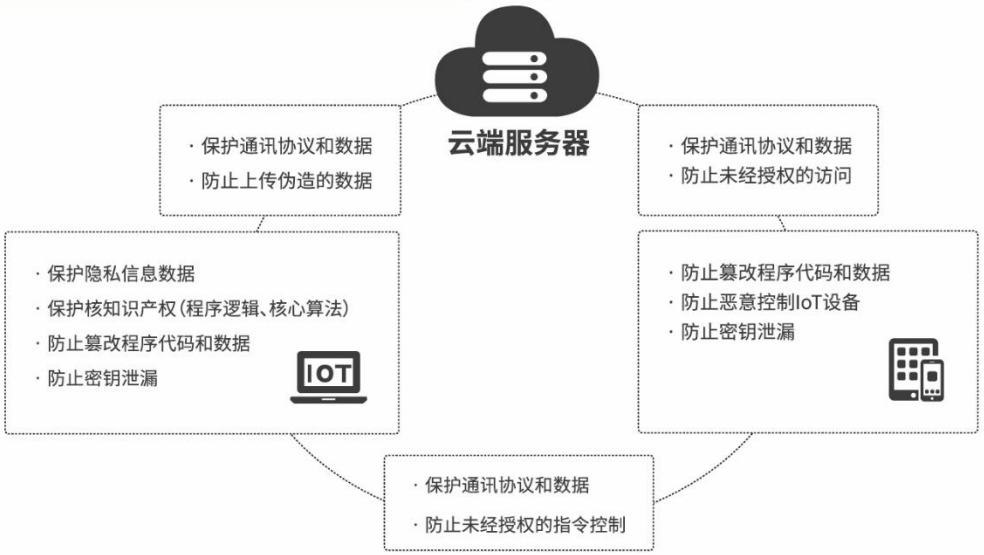
终端数据保护 与通讯链路保护

安全的核心是数据。顶象通过对终端保存的数据和通讯链路中传输的数据进行深度加密保护，使得数据从生产到传输到使用的整个生命周期均处于安全状态。

IoT设备固件防护

随着各种IoT（物联网）设备的不断出现，针对这些智能设备的攻击也随之而来。而由于IoT设备功能的特殊性，这些攻击带来的后果更为多样和严重。例如智能摄像头被攻破可能带来家庭或工作隐私视频的泄露，智能手表被攻击可能带来行动轨迹的泄露，智能汽车被入侵更是可能直接带来生命安全的威胁。

顶象技术针对IoT固件的防护，从源头入手通过对IoT设备上运行的程序进行深入保护，使得攻击者无法破解其内部工作逻辑，从而保证了这些IoT设备在复杂、不安全的环境中，仍能按照预设的功能正常、安全的运行。



· DX-ESS | 核心能力一 · Android & iOS 虚机源码保护

针对Android/iOS移动端App，顶象利用专利的虚机源码保护技术，将App的核心代码置于安全的虚机环境中隔离运行，强力对抗各种逆向分析工具和手段。不仅如此，顶象还为每款App生成完全不同的虚机，从而为App实现了一机一密的安全性。

特点与优势

◎ **一机一密：** 虚机加密指令动态可变，即使某一用户被攻破，其他用户不受影响

◎ **指令虚拟化：** 自动在源码中加入虚机，将源码转化为加密指令，运行于被保护的虚机中

◎ **控制流平坦化：** 在保证不改变源代码功能的前提下，将源代码中的条件（IF）、循环（WHILE/FOR/DO）等控制语句转化为调度器统一调用，隐藏原始执行流程

◎ **虚假控制流：** 在原始代码块中随机插入垃圾指令（花指令）、在原始代码块前后随机插入新的代码块，制造虚假的程序控制流

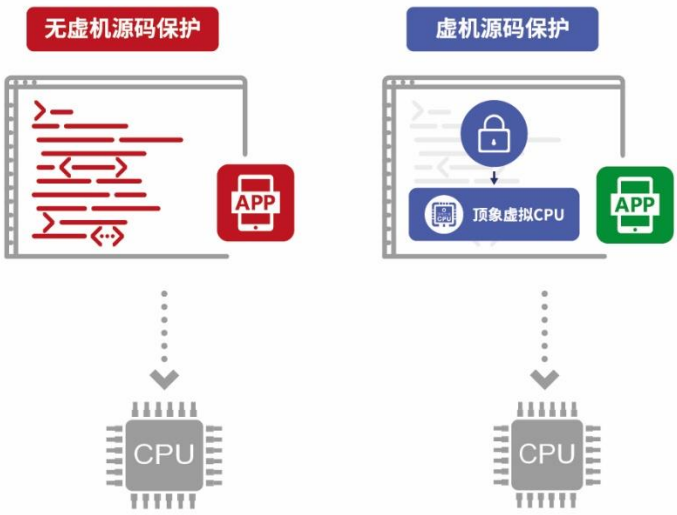
◎ **等价指令替换：** 自动挑选代码中的部分运算指令，用等价的随机代码块替换，增加逆向难度但不改变运算结果

◎ **代码切块化：** 针对大块的顺序执行代码块，将其切碎成若干独立代码片断并打散重组，增加逆向分析复杂度

◎ **字符串混淆：** 对源代码中的字符串常量进行混淆，防止攻击者通过字符串猜测代码逻辑

◎ **多全平台支持：** 不仅Aandroid、iOS双平台支持，还支持各种定制化操作系统甚至无操作系统的IoT设备。支持包括Java，Kotlin，C/C++，Objective-C，Swift等在内的多种语言

◎ **兼容性优：** 源码级别保护不使用任何操作系统未公开的API，不使用任何系统版本升级可能引起的不稳定机制，受保护的代码仍经正常编译打包流程生成App，避免兼容性问题



应对风险

◎ App中被植入恶意代码　◎ App核心知识产权被破解　◎ 隐私数据泄露　◎ 资产损失

应用场景

金融、电商、游戏、智能设备控制端等各类App

· DX-ESS | 核心能力二 · 安全SDK

研发团队开发任务重、开发周期短，普遍存在重功能而轻安全的现象；同时安全涉及面广、问题复杂，研发难度高、对持续攻防要求更高。为此顶象技术基于多年安全攻防经验、虚机源码保护等核心技术能力，为广大开发者提供两款安全SDK。

特点与优势

◎ **白盒加密：** 用复杂数学算法和庞大的Lookup Table取代密钥，解决密钥泄风险

◎ **网络数据防伪造：** 自动对客户端发出的数据加签，保证服务端接收到的数据真实性

◎ **设备绑定：** 加密数据设备绑定，能够提供一机一密的安全性

◎ **重打包防护：** 绑定签名和包名，防止盗版、广告插入、恶意代码注入等重打包行为

◎ **静态分析防护：** 对抗apktool、dex2jar等常用逆向分析工具

◎ **动态攻击防护：** 多维度实时监测进程调试、代码注入、代码hook、内存篡改等攻击手段

◎ **运行环境风险监测：** 多角度实时监测App多开、模拟器、root设备等风险运行环境

应对风险

◎ 抗逆向工具　◎ 调试器检测　◎ 防重打包　◎ 模拟器监测　◎ 内存保护

◎ App多开监测　◎ 代码注入监测　◎ 设备root监测　◎ 代码hook监测　◎网络代理监测

应用场景

◎ App有数据加解密功能；

◎ App与服务器端有安全通信的需求，需做到高安全性的相互身份认证

◎ IoT设备与服务器端、控制端之间传输协议的保护

· DX-ESS | 核心能力三 · IoT安全编译器

顶象技术的安全编译器，从开发编译阶段入手，直接生成受保护的固件，使得攻击者无法通过对设备软件的逆向，破解其内部工作逻辑。

特点与优势

◎ 专利技术的超轻量级虚机源码保护方案，适用于各种低运算能力设备

◎ 灵活的保护方案，保护颗粒度细至函数级

◎ 针对源码的保护方式，兼容各种处理器和操作系统

◎ 支持ARM/ARM64/X86/X86_64处理器架构

◎ 无缝集成GCC/CLANG/KEIL/IAR等主流IoT开发平台，不改变任何现有开发流程，无任何学习成本，开发者使用过程无感

◎ 包含BCF/FLA/XSE等代码防护手段

◎ 强力对抗逆向分析工具，包括IDA Pro的F5插件

使用前后控制流对比

使用前　　使用后

应对风险

◎ 对各类IoT设备的入侵，恶意控制，固件逆向破解，设备仿冒等

应用场景

◎ 智能家电、智能穿戴设备、智能汽车、智能充电桩等各类物联网设备