互联网安全领袖峰会
Cyber Security Summit

腾讯安全

# CSS视角下的2019年产业互联网安全十大议题

出品单位：腾讯安全

# 目录

# 前言

随着互联网发展进入下半场，消费互联网向产业互联网升级，AI、大数据、云计算等科技发展驱动传统产业加速数字化发展进程，产业互联网安全成为关系国计民生、基础设施发展建设的重要保障，也成为企业在数字经济时代构建核心生产力的重要基础。

**在产业政策方面**，产业互联网发展带动的安全产业红利正逐步释放，《国家网络安全产业发展规划》正式发布，我国网络安全相关法规、政策呈现出系统化、及时化、产业化三方面特点：一是网络安全保障体系逐步完善。截止 2018 年，我国政府制定网络安全相关法律共 24 个，制定法规：11 个、规范性文件 136 个，共有 22 个部委参与；二是政策出台紧随网络安全形势变化。通过法律法规、指导意见、管理条例、通知规定等各种方式保障网络安全管理的及时性；三是网络安全产业化特征逐步明显。在传统网络安全基础之上，持续加大对于产业安全的保障力度。业内预期在未来十年，网络安全产业有望成为万亿元规模的社会支柱产业。与此同时，合规和自主可控将成为产业互联网时代的安全主诉求。即将于 2019 年 12 月 1 日实施的网络安全等级保护制度 2.0 标准，将云计算、大数据、物联网、移动互联和工业控制信息系统等也纳入到等级保护对象。

**在技术应用方面，**随着数字经济发展，各领域企业、机构纷纷上云，进行数字化转型。云计算、大数据、人工智能等先进科技在带来效率提升的同时，也引发了新的网络安全问题，产业互联网时代安全形态也已发生改变，安全不仅是企业必须守护的底线，也已经成为制约企业发展的天花板，决定着企业发展的高度，每一家企业都需从战略视角重新规划安全。

**在业务场景方面，**伴随新技术在产业领域的应用落地，网络安全的基础保障作用和发展驱动效应日益突出，产业互联网安全愈发重要。金融、能源、交通、制造业、医疗等智慧产业领域新场景安全需求不断涌现，“数据资产安全、业务安全、身份权限管理”将成为产业互联网安全的三大核心痛点，企业需要扭转被动防御的传统安全思维，积极构建防御能力。

本报告将试图从产业政策、技术应用、业务场景等方面对产业互联网时代的安全变化和技术趋势进行盘点和解读，选取最具代表性的年度十大议题，诠释产业互联网安全的发展趋势，提升安全认知。

## 议题一：物联网及汽车产业数字化全新安全技术洞察

## 研究团队：腾讯安全科恩实验室

## 议题方向：物联网及车联安全

近年来，物联网发展迅猛。预计到 2020 年，活跃的物联网设备数量将增加到 100 亿，到 2025 年将增加到 220 亿。原本独立、隔离、安全的传统设备通过网络连接成为万物互联中的终端。而随着智能化、网络化程度越来越高，汽车也在这样的发展趋势下成为了智能终端设备之一。

设备本身拥有更多的入口和控制方式，这为用户带来操作便利性的同时，也形成了更多暴露面。2018 年英特尔 CPU 芯片漏洞、亚马逊物联网操作系统漏洞，以及汽车安全漏洞等事件的曝光，揭示着并没有绝对的安全。一方面，IoT 设备的严重碎片化现象以及开发人员安全意识薄弱，导致出厂的固件中存在着各种各样的漏洞；另一方面，由于 IoT 本身使用的操作系统数量多，使用的架构不统一，固件格式更是因厂商而异，给安全自动化检测带来了挑战。

如，智能汽车除了常规车辆的各种硬件设备外，还会根据需求，使用各种 ECU 硬件芯片，以及网关、车电网络、车电协议等软件系统，保障大量的无线通信和信息交换。其中任何一个环节出现问题，或漏洞被利用，都有可能造成用户隐私或商业数据泄密，甚至对人身财产造成直接威胁。

传统解决方案，不能快速适应新的产品形态和产品生命周期，也无法适应碎片化 IoT 产品生态，不能从底层洞悉安全问题产生的原因，无法解决因软件安全能力带来的问题，适配灵活性太低，产业链深入能力不足。

同时，IoT 厂商对于安全的投入和重视程度还没有达到一个较为理想的阶段，受制于一些交付压力和成本控制，诸多 IoT 设备相当于处在“裸奔”的状态中。产业链上下游应该尽快就交付消费者的终端产品安全问题进行产业协同合作，并且引入腾讯安全等顶尖安全行业解决方案提供商。腾讯愿意开放核心技术能力，护航 IoT 产业安全，并提供先进漏洞扫描

检测工具，安全专家服务以及 SOC、OS 加固等产品与解决方案。

## 解决方案：

近年来，腾讯安全科恩实验室扩展了新领域的研究能力，包括智能网联汽车、物联网产品、云计算和虚拟化以及人工智能等。同时，腾讯安全科恩实验室根据全球领先的技术积累和理解，开放核心能力，对各产业的数字化、信息化转型针对性的推出了相关行业解决方案，包括汽车信息安全、智能应用生态安全、IoT 信息安全等行业解决方案。

其中，面对安卓移动应用生态安全推出了 Apkpecker。ApkPecker 是科恩实验室研发的一款全自动 Android App 静态漏洞扫描工具，通过对 App 的攻击面和漏洞模式进行全面的建模，使用数据流，控制流以及静态污点分析的方法，跟踪从攻击入口点到漏洞触发点的完整代码路径，高效和准确的发现可利用的 App 漏洞，并在保证准确性的基础上，大大降低检测的误报率，提高检出结果对分析人员的帮助。

目前 ApkPecker 已在 Google、Amazon、Starbucks 和国内百度、阿里，小米，京东、滴滴和携程等厂商的 App 中发现了大量可利用的漏洞，并全部得到了厂商的确认和认可。

针对 IoT 产业，科恩研发了一款全自动 IoT 固件安全扫描系统 IoTSec。该系统通过对 IoT 设备的常见攻击面、漏洞与安全风险模式进行建模，使用数据流、控制流以及静态污点分析等方法，可以对设备固件以及固件配套的源代码进行安全扫描。平台通过静态分析以期在多个维度、最大化并尽量精准地识别设备中的安全风险问题。

## 典型事件：

**全面测试汽车安全问题，腾讯安全科恩实验室协助宝马提升车辆安全等级**

在 2017 年 1 月至 2018 年 2 月间，腾讯安全科恩实验室车联物联研究团队，对各款宝

马车型进行了测试。在长达 13 个月的研究后，科恩实验室团队共计发现了 14 个不同的安全问题。其中，9 个访问场景需要在车内通过物理连接或者在车辆旁边进行；5 个访问场景需要使用移动电话网络进行远程连接实现。研究团队在获得信息娱乐系统部件访问权限后，通过执行专门开发的软件安全利用代码，从而获得 CAN 总线的控制权限，可远程启动车辆诊断的功能。

该测试获得了宝马的支持并提供试验条件。宝马集团认为，此项研究是迄今为止由第三方机构对宝马集团车辆进行的最全面、最复杂的测试。随后，宝马集团在后台运行了升级程序，并通过无线连接上传到了远程信息处理控制单元。在两家公司的合作努力下，宝马集团研发的安全更新提升了宝马产品和服务的安全等级。

鉴于此项研究，腾讯安全科恩实验室在 2018 年 5 月，被宝马集团授予首个“宝马集团数字化及 IT 研发技术奖”。

## 议题二：软件和芯片重塑世界催生出新的威胁模型

## 研究团队：腾讯安全玄武实验室

## 议题方向：新型威胁攻击模型

万物互联让我们生活更加便利，释放更多生产力的同时，也因为联网终端的数量、种类、复杂性的增加，而催生了更多的安全威胁。早期的安全威胁成因大多比较简单，往往源自一行错误的代码、一个错误的配置。这样的问题，相对容易发现，也容易修复。

然而，软件和芯片对我们的世界渗透越来越深，我们周围的信息系统越来越多。这些大大小小的系统之间通过各种通信方式又形成了复杂的互动关系。这就催生出一些更复杂的安全威胁形态。问题不再只源自某个对象内部，也可以由多个对象相互或共同作用而导致。在这个背景下产生的新的多维威胁，已经不再是一个对象的问题。对这些对象自身而言，安全问题可能并不存在，但当多个对象在我们身边互动时，问题就出现了。而这些对象甚至可

能源自不同设备、不同厂商，甚至不同时代。

因此，不仅传统安全问题依然存在，新的安全问题也产生了。比如，我们使用的智能手机与智能手表，单独来看，这两种硬件设备都会有安全措施保障用户的使用安全以及隐私问题。但是，两者在通信时，或许因为兼容性，以对协议的实现不完全一致等问题，造成信息在传输过程中可能被人盗取。在以物联网为基础构建的智慧生活场景中，各类设备都需要不断采集使用者的各种生活甚至生理信息。这些信息一旦被人窃取、利用而实施诈骗、敲诈等，后果就会很严重。

对于这类威胁，可能看起来谁都没有犯错，似乎每个设备自身都是安全的，但当它们结合在一起之后，就会变成我们面临的新的安全问题。

如果抛开软件或者硬件的视角，以更抽象的视角来看，今天的信息安全和网络空间进化中遇到的安全问题，如同生物进化一样，已经进化成了一种非常复杂的形态，而这种形态的安全问题用传统的方法是难以进行发现、分析和防御的。因此，安全措施也必须随之进化。作为安全防御者，我们需要随着安全问题进化。

## 典型事件：

### 1、 发现“BadBarcode”漏洞，帮助国内扫码器行业整体提升了安全性

扫码器不仅被用于扫码支付，也广泛用于物流、零售、医疗、制造、安防等诸多行业。2015 年玄武实验室发现影响条码阅读器这一大类产品的“BadBarcode”漏洞。利用该漏洞可以通过扫描条码甚至发射激光来入侵条码阅读器所连接的上位机。该问题是条码阅读器的解码协议、传输协议、上位机操作系统三者共同作用导致的。

玄武实验室发现当前大多数条码阅读器以键盘仿真的模式进行数据传输，同时又会尽可能多地支持解码协议，就导致了可以通过条码模拟操作系统热键，从而对系统执行任意操作。

2016 年以来，玄武实验室通过和微信支付的合作，持续对国内主流扫码器厂商的

产品逐一进行检测。在检测中，除“BadBarcode”漏洞外，还发现了多种其它漏洞。对这些漏洞，玄武实验室均帮助厂商进行了修复，从而大大提升了我国扫码器行业的安全水平。

**2、 发现“残迹重用”漏洞，帮助国内手机行业解决屏下指纹识别技术致命缺陷**

指纹解锁已逐渐成为智能手机的标配功能。然而，这种相对安全、便捷的解锁方式，曾经存在致命缺陷。2018 年 10 月，在 GeekPwn 2018 会上，腾讯安全玄武实验室首次向外界公开了针对屏下指纹解锁型设备的“残迹重用”漏洞。利用这个漏洞，安全研究员在活动现场，通过一张普通的塑料片，就可以在几秒钟内破解安卓手机的屏下指纹识别。

究其原理，当时的屏下指纹解锁功能是利用一种新的光学结构捕捉用户的指纹影像，而玄武实验室发现，对这种新的光学结构，可以利用屏幕上残存的指纹痕迹，让屏下指纹传感器认为手机的主人正在使用指纹验证，从而达成破解指纹的目的。

而早在公开该漏洞前的 2018 年初，腾讯安全玄武实验室已将研究成果陆续提交给国内几家主流手机厂商，通过更新算法修复了已上市手机中的漏洞。同时，相关解决方案也提交给上游芯片厂商，推动了供应链层面的安全修复，从而确保了未来使用该技术的手机不再受该漏洞的威胁。

## 议题三：常态化网络攻防对抗成产业安全防御新标尺

## 研究团队：腾讯安全湛泸实验室

## 议题方向：网络攻防对抗

在产业互联网时代，企业面临的网络安全威胁更复杂，且危害更大。不仅传统的漏洞攻

击方式愈演愈烈，APT 攻击（高级可持续威胁攻击）等具有极强隐蔽性和针对性的攻击活动，也层出不穷。

从单个企业层面而言，由于安全事故发生频率较低，且在业务层面极少有直接感知。在尚未发生安全事故，或者说攻击未直接造成损失时，很可能让企业产生自身安全防护足够完善、业务数据足够安全的错觉，甚至导致防护手段逐渐落后，安全流程越发陈旧，人员意识日益懈怠。

事实上，自动化扫描做得再强大，也无法发现所有的漏洞，而且也不能对网络防御纵深能力做出评估。而一次攻防演练往往能让各方更加直观的感受到攻击现场，强化业务的安全意识。因此，在常态网络环境下，以红蓝对抗、用接近真实攻击的方式，进行网络攻防对抗演习，成为了检验企业安全防御的新标尺，以弥补企业现有防御体系的不足。

## 解决方案：

目前，不仅有国家层面的网络安全实战演练，国内的各大企业也在构建自身的红蓝军对抗，例如腾讯、阿里、美团等企业都在建立自己的红蓝军。

相较而言，网络攻防对抗演习，可以弥补真实入侵事件低频的不足，又因为红蓝对抗双方，既熟悉本公司的业务体系，能够以黑客视角持续渗透公司资产，更有可能早于黑客发现公司的各项安全隐患，暴露风险盲点，客观检验企业安全态势和防护水平。

此外，网络攻防对抗的攻击目标往往是企业的核心业务和数据，通过扮演了一个外部攻击者的角色，可以正面反映出安全投入的必要，证明安全工作的价值。

腾讯安全从事 APT 研究，并多次基于 APT 攻击的研究向行业发出警示；同时腾讯安全积极对外赋能，参与过多次国家级的较大型网络安全攻防演练。

## 典型事件：

**1、WannaCry 事件两年后，攻击余威依然存在**

2017 年 4 月，黑客组织 Shadow Brokers 公开了 NSA 的网络漏洞“军火库”。当年 5 月，利用“军火库”中的 SMB 漏洞，名为 WannaCry 的蠕虫勒索软件袭击全球网络，肆虐全球数百万台电脑，许多大型企业、政府机构都受攻击，造成的损失触目惊心。然而在两年后的今天，由于安全意识不足、未装漏洞补丁，以及 WannaCry 出现变种等原因，WannaCry 依然存在继续传播的可能性。

今年 5 月，为了有效控制 WannaCry 勒索病毒的传播感染，国家互联网应急中心开通了 WannaCry 病毒感染数据免费查询服务。

**2、"海莲花"等 APT 组织，攻击威胁向移动端扩散**

自 2015 年首次被曝光以来，海莲花（OceanLotus）APT 组织一直动作不断，是近年来针对中国大陆攻击最频繁的组织，甚至没有之一。

腾讯安全御见威胁情报中心近期公布的《全球高级持续性威胁（APT） 2019 年上半年研究报告》显示，海莲花的攻击目标众多且广泛，包括政府部门、大型国企、金融机构、科研机构以及部分重要的私营企业等。该组织攻击人员非常熟悉我国，对我国的时事、新闻热点、政府结构等都非常熟悉，如刚出个税改革时候，就立马使用个税改革方案做为攻击诱饵主题。此外钓鱼主题还包括绩效、薪酬、工作报告、总结报告等。

此外，随着移动互联网的普及，越来越多的机密载体转移到了移动设备中，2019 年，多个 APT 组织的移动端木马相继被发现和披露，包括海莲花、donot Team 都已经使用了 Android 的恶意程序等。高级持续威胁不再限于计算机，未来如智能路由等均可能成为 APT 攻击的目标和持久化的宿主。

## 议题四：云和万物互联时代的数据安全保护面临新挑战

## 研究团队：腾讯安全云鼎实验室

## 议题方向：密码及数据安全保护技术

产业互联网时代，万物通过“云”逐渐实现了互联互通。但在以数据的深度挖掘和融合应用为主要特征的智慧化阶段，也蕴藏着严重的安全隐患，容易出现海量敏感数据的泄露事件，给企业带来严重甚至致命性损失的同时，也让企业面临严厉的法律法规的处罚。

事实上，无论攻击技术趋势如何演变，攻击目标的主体均为关键数据。“数据保护”和“安全合规”是信息安全建设的核心要素。

然而，传统的企业安全防护是“以网络为中心”，将数据一层层保护在网络中心，一旦防火墙或应用系统被攻破或绕过，以及因为权限问题、固有的漏洞问题等因素，都有可能让恶意人员从系统层面将数据拿走，那么，此前的所有安全手段就会瞬间被瓦解。在 2017 年 11 月 15 日，Oracle 就发布了五个针对 Tuxedo 的补丁，修补了 5 个极高危的漏洞，攻击者可以利用这些漏洞从应用层面获得数据库的完全访问权限，而无需有效的用户名和密码即可获得数据库中的关键数据。

因此，随着防护边界越来越模糊、攻击复杂度越来越高，数据共享需求越来越频繁，“以网络为中心”防护思路渐渐失效。企业安全架构建设逐步从“以网络为中心”转向“以数据为中心”。

在安全防护向以数据为中心的转变过程中，密码技术应用是其中最主要的措施之一。但是传统的密码技术存在难做、难用、难管的三难局面。因此，在用户业务与密码层解耦中，可引入数据加密服务中台，以加密为核心，贯穿数据全生命周期的防护，并通过中台服务以安全合规的方式，更新完成加密措施或加密算法（国密）改造。

## 解决方案：

针对新形势，腾讯安全云鼎实验室通过专业的数据治理技术、加密服务中台设施、以及核心数据安全产品，从技术层、云产品层、安全服务层、解决方案层，共建云上数据安全应用生态，提供给云用户覆盖数据获取、事务处理及检索、数据分析与服务，数据访问与消费

的数据全生命周期的安全保护，帮助企业便捷快速地搭建起安全合规的数据安全策略及业务加密架构。例如，数据安全能力中台服务，从数据加密软硬件服务、数据加密和密钥服务、身份凭据与授权等方面，为企业提供一站式关键数据安全服务；“数据加密服务中台”可简化密码技术的使用，适配多元业务场景，构建基于云技术的极简密码服务。

## 典型事件：

**1、数据加密技术获政策持续加码，多项安全法律法规文件即将实施**

信息安全已上升至国家战略层面。而为了适应云计算、移动互联、物联网、工业控制和大数据等新技术、新应用情况下的安全需求，国家有关部门高度重视，出台了一系列的政策法规、文件要求，推动数据加密技术的应用。

2018 年 7 月，《关键信息基础设施安全保护条例（征求意见稿）》面向社会公开征求意见，其中第五十三条指出，关键信息基础设施中的密码使用和管理，还应当遵守密码法律、行政法规的规定。

2019 年 6 月，《中华人民共和国密码法（草案）》提请十三届全国人大常委会第十一次会议审议。《密码法》第十二条指出，关键信基础设施应当依照法律、法规的规定和密码相关国家标准的强制性要求使用密码进行保护，同步规划、同步建设、同步运行密码保障系统。

即将于 2019 年 12 月实施的网络安全等级保护制度 2.0 标准，则强调要保障数据完整性和数据保密性，应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

同时，该标准也指出，在密码管理方面，应使用国家密码管理主管部门认证核准的密码技术和产品。

**2、因黑客攻击导致数据泄露，英国航空公司面临 1.83 亿英镑巨额罚款**

今年 7 月，英国数据安全监管部门——英国信息专员办公室宣布，将对英国航空公司 2018 年客户数据遭泄露事件开出 1.83 亿英镑巨额罚单。这是自欧盟《通用数据保护法》（GDPR）生效以来的最高金额罚单。

2018 年 9 月，英国航空公司（ British Airways，以下简称英航）发布声明称因遭黑客攻击从而导致其乘客数据被盗。据了解，约有 38 万乘客数据在此次数据泄露事件中受到影响，这些被盗数据信息包括个人基本信息和付款记录，但不包括个人护照信息。

## 议题五：新形势下的数字城市建设亟需监管科技打破监管孤岛

## 研究团队：腾讯安全反诈骗实验室

## 议题方向：互联网+监管

随着移动互联网的飞速发展，大量新商业模式、新兴互联网经济体应运而生。但是，由于新的互联网经济的网络行为跨领域、跨区域、传播快、交叉性等多样特点，对政府监管部门提出了新的挑战。

2017 年 9 月，善心汇传销组织被依法取缔，600 多万人参与，涉案金额 1000 多亿，传销团伙非法获利 22 亿；2018 年 5 月，涉案金额达 3300 亿元的云联惠传销案被广州警方查处，全国加盟商 11294 家，受害人数高达 500 多万；而借天价保健鞋垫和负离子卫生巾起家的天津权健公司，在令人瞠目的 7000 多家加盟火疗店的掩护下，花了 14 年，在中国构建起一个年销售额接近 200 亿的保健帝国。

这些事件的发生，也暴露了新时代监管部门的一些不足。如，市场主体数量迅速增长，导致监管工作任务更加繁重，让监管任务增长与执法力量不足的矛盾突出；互联网经济等跨行业、跨领域、跨区域新业态蓬勃发展，对联合监管协同监管提出了新的挑战；新经济、新业务带来的挑战，让监管工作的预见性不高，提前发现风险问题的能力薄弱；而基于企业信

用分级、企业分类、企业风险的随机抽查监管，很难做到精准监管。

## 解决方案：

在产业互联网的时代，腾讯不断思考，腾讯的大数据、人工智能、安全能力等技术能力能否协助各监管部门对风险“打早打小”，响应国家号召，创新监管方式，实现精准监管；同时，借用腾讯在消费互联网积累的优势经验和对用户的触达优势，让监管信息更加的“触手可达”。

因此，基于 20 年积累的大数据优势、技术优势、安全优势、人才优势，腾讯推出了“灵鲲大数据监管科技平台”，协助监管部门提升整体监管能力，实现智慧监管。

目前，灵鲲大数据监管科技平台已经广泛的应用在各个监管领域，包含国家电子政务办、国家发改委、原国家食品药品监督管理局、原工商行政管理局、各地方金融监督管理局、公安经侦、市场监督管理局等部门，已为北京、广东、广州、深圳、河北、山西、西安等多个省市提供智慧监管服务。

## 典型事件：

**1、金融科技监管“新武器”，累计识别风险平台破万家**

2018 年 7 月，深圳市金融办与腾讯公司双方共建的灵鲲大数据监管科技平台正式上线运行。双方共建的金融安全监管科技实验室也同步揭牌成立，共同为打赢防范化解金融风险攻坚战研发监管科技“新武器”。

灵鲲大数据监管科技平台在试运行期间，已先后扫描深圳 25 万多家从事金融业务的企业，对其中的 5 万余家做了重点分析，识别风险企业 1400 余家，已全部移交公安等部门核

查。同时，结合深圳市金融办整合的深圳市 40 余个行政管理单位的政务数据，运用多源数据融合技术，能够对 P2P 、投资理财、外汇交易等十多个金融类别的识别与风险指数计算，对发现的高风险平台及时向政府相关部门进行预警，做到对金融平台的识别全、预警快，实现针对非法金融活动的“打早”和“打小”。

截至 2019 年 3 月底，灵鲲大数据监管科技平台已累计监测出非法集资金融风险平台 1.1 万家，上报超过 7 万条非法集资平台网站、APP 线索，日拦截传销等非法集资网站逾 1000 万人次，输出案件线索报告 500 余份。

**2、协助监管部门整治市场乱象，打造智慧监管**

在数字化进程、IT 资源调用能力和人机交互模式等三大信息技术变量的共同推动下，互联网发展已进入产业互联网时代。各行各业的营商环境因此发生了巨大变化，也对市场监管的流程、模式、风险甄别防范和预警等能力提出了更高要求。

依托 20 年黑灰产对抗经验和安全技术能力优势，腾讯积极地参与到产业互联网时代的监管体系优化实践中，在行业和政府部门的监管机制完善、平台升级建设、风险防御体系搭建等方面都提供了助力，全力推动“智慧监管”的创新建设。

目前，腾讯已在“互联网+监管”平台建设、市场监管等领域为行业和监管部门提供了有效助益和产品支持。通过腾讯安全反诈骗实验室设计研发的灵鲲大数据监管科技平台，已能做到对制假售假、网络传销、虚假广告、舆情监测、网络侵权等的全网监测与联合惩戒，不仅为市场监管部门提供全流程的数据服务，解决了现有市场监管领域“数据、算法、计算力”不足的问题，也为构建更为清朗的市场环境和秩序提供技术支持。

2018 年 12 月 25 日，广州天河警方在腾讯安全灵鲲大数据监管科技平台的线索支持下，捣毁一个涉嫌虚假销售男性壮阳药的诈骗团伙，抓获涉案人员 77 人，查货涉案伪劣保健品 26 种 702 箱，涉案金额过千万元。

自腾讯灵鲲上线以来，已陆续与全国各地 10 多个市场监管部门展开合作，用“AI+大数据”技术为监管部门提供实时监测和预警，累计帮助国家市场监督管理局、国家食药总局以及地方版权局、网安、经侦、烟草专卖、环食药、市场监管、金融监管部门等政府部门监

测非法平台数十万个。

## 议题六：信息技术自主可控趋势下的产业安全生态新挑战

## 研究团队：腾讯安全反病毒实验室

## 议题方向：信息安全自主可控

随着 5G 的到来，云计算、AI、IoT 等前沿技术的不断突破，万物互联的世界正展现在我们面前。在全球信息领域，创新链、产业链、价值链整合能力越来越成为决定成败的关键，而关键中的关键则在于核心技术。互联网核心技术是一个企业乃至国家发展的“命门”，在当前复杂多变的国际环境下，核心技术受制于人是小到个人、大到国家发展最大的隐患。

因此，在关键技术、关键领域必须实现自主可控，走独立自主的国产化之路势在必行。目前，国产化信息安全建设呈现出三大趋势：首先，自主可控国产化将全面覆盖国防、党政及事业单位，以及特殊行业（重点行业及关键领域）等各大行业，并将全面替代核心元器件、安全可信应用、核心关键技术、终端等产品或服务，释放出千亿市场空间；其次，安全行业逐步过渡到万亿市场空间，而半导体和操作系统是“安全可靠工程”最核心的部分。最后，安全生态的构建将成为行业需要长期协力完成的命题，因为信息产业国产化生态能否建成是一个关系国家、产业、企业以及个人是否安全的全维度问题。

从国家层面来说，芯片、操作系统等是否国产涉及的是全局性安全问题，杀毒软件作为其中的重要一环，需要补齐国家关键领域技术等自有产权的能力，需要广大厂商共同努力；而在产业发展过程中，安全生态建设的不同环节也可能爆发潜在威胁。

当下，网络安全面临突发性、复杂性、破坏性等新变量。加之产业互联网的提速发展，国产化信息安全建设也需要进入一个新的阶段。只有确保研发、生产、组装、流通、服务全周期的全产业链环节的全流程安全，才能最终实现降本增效、产业进化。

## 解决方案：

要推动我国国产化信息安全建设，仅靠几家企业的单打独斗努力是远远不够的，通过生态协同的力量，强强联合的同时也优势互补，打造从源头核心技术到前端应用的全流程的国产、自主、可控，切实保障信息资产的安全。同时，还需要站在核心技术研发的最前线，借助已有的优势，在推动核心技术成果转化的同时，构建国产化信息安全建设，保障互联网产业安全和国家安全。

目前，腾讯御点终端安全管理系统已率先完成适配中标麒麟、银河麒麟、深度等众多国产操作系统，并可完美运行于龙芯、飞腾、兆芯等国产 CPU 平台之上，完善了信息技术国产化之路上安全问题的重大课题。而御点搭载的 TAV 杀毒引擎系腾讯安全反病毒实验室独立研发的自主杀毒引擎，代表了中国新一代反病毒技术水平。集成该引擎能力的产品曾在国际国内多项权威评测中取得过多次优异成绩。

腾讯御点愿做信息技术国产化道路上坚强的盾牌，为保卫全行业产业互联网业务顺利蓬勃发展提供坚强的支撑。

## 典型事件：

**1、支持集成电路与软件产业发展，财政部发布减税政策**

今年 5 月，为支持集成电路设计和软件产业发展，财政部发布了集成电路设计和软件产业企业所得税政策的公告，在 2018 年 12 月 31 日前自获利年度起计算优惠期，第一年至第二年免征企业所得税，第三年至第五年按照 25%的法定税率减半征收企业所得税，并享受至期满为止。这次所得税优惠政策是对 2012 年优惠政策的延续，也是鼓励科技型企业创新发展、鼓励产业产能升级换代的重要举措之一。

**2、腾讯御点推出国产专版，与国产软硬件厂商达成 9 项认证**

今年年初，腾讯公司推出腾讯御点终端安全管理系统-国产专版，并与中标麒麟、银河麒麟、湖南麒麟、深度等国产操作系统，龙芯、飞腾、兆芯等国产 CPU 平台互认证共完成 9 项认证并全面支持以上系统及 CPU。

据了解，腾讯御点国产专版针对性的优化了国产相关平台的兼容性、稳定性，实现了全方位覆盖，助力国产平台构建安全可靠环境，完善了信息技术国产化之路上安全问题的重大课题，为国产信息产业生态保驾护航。

## 议题七：移动安全新趋势，构建垂直行业的可信生态体系

## 研究团队：腾讯安全移动安全实验室

## 议题方向：可信技术

伴随着移动终端的多样性发展和智能化演进，移动终端面临的安全威胁也变得更加多样化。网络犯罪分子针对这些变化，不断翻新攻击手段，给行业、用户带来潜在威胁或重大安全隐患。

频发的信息泄露事件、电信网络诈骗事件显示出手机等移动端的安全形势依旧严峻；而通过对 APP 进行破解或漏洞利用、伪造通信协议等手段，甚至可以控制智能电视、智能音箱等智能家居设备，扩大家庭使用的 IoT 设备的安全风险。

因此，从硬件、操作系统、通信技术、云端服务器、数据库等各个模块之间做好统一的安全体系建设，以可信技术构建移动安全生态，让安全紧跟产业发展步伐，是持续对抗“黑产”，保障移动智能终端安全性的有效手段。

从广义上而言，移动终端可信生态包括了可信设备、可信环境、可信应用、可信数据与可信交互在内的立体化的安全生态，并且可以针对不同应用场景，选用最适合的安全策略。

其中，可信设备，是指 APP 在运行时对终端设备进行检测，判断终端设备是否是真实的终端设备；可信环境，是指 APP 在运行时对运行环境进行感知，包括各种作弊环境、病

毒环境等，确保 APP 是在一个安全的环境下运行；可信应用，是指 APP 运行时进行可信校验计算，确保 APP 是没有被二次打包或恶意篡改的正版应用；可信数据，是指 APP 在运行时获取的数据没有经过篡改，可以作为分析、打击恶意行为的重要证据；可信交互，是指 APP 在运行时用户通过安全键盘输入的内容不会被窃取，并且通过防截屏、防劫持等功能来达到 APP 内部页面信息的保护。

## 解决方案：

目前，腾讯安全移动安全实验室面对垂直行业提供了系列解决方案，有助于帮助企业应对各类移动安全威胁，为企业打造一个安全可靠的移动生态环境。

**金融行业：**提供集成漏洞扫描、APP 加固、安全键盘、防截屏、防界面劫持、白盒加密、威胁环境清场等能力于一体的高强度流程化终端防护系统。

**社交行业：**提供终端安全 SDK、通信协议加密、APP 加固能力，确保应用不会被恶意篡改，保证用户隐私，同时提供一定的终端反外挂能力。

**AI 行业：**通过源码混淆能力，保护 AI 核心算法逻辑，集成调用者识别功能，避免算法库被恶意窃取或被恶意调用。

**游戏行业：**通过专用游戏加固保护游戏引擎，包括 Unity3d、cocos2d、UE4，保护游戏脚本与游戏音视频资源。

## 典型事件：

**1、腾讯移动安全环境清场技术服务，为移动安全保驾护航**

各行业移动化不断推进，如今移动安全成为了金融行业最关注的领域。随着等保 2.0 与人行 146 号文的影响深化，除了应用安全，环境安全同样是国家政策关注的安全需求。

基于多年实践积累的安全检测能力，以及众多强大乃至独有的安全检测能力，腾讯安全

移动安全实验室提供的移动安全解决方案，全方位为各政企单位移动安全保驾护航。

以腾讯安全移动安全实验室为银行客户提供的“移动安全环境清场技术服务”为例，该移动安全解决方案，提供的服务包括，WiFi 安全检测、病毒查杀、网址检测、伪基站检测、防界面劫持、防截屏录屏等。

其中，WiFi 安全检测为腾讯特色能力，基于腾讯手机管家、腾讯 WiFi 管家等产品矩阵的安全检测触点，每日感知数以亿计的 WiFi 连接，实时防御 ARP 攻击、DNS 欺骗、SSLStrip 攻击等风险。同时，根据海量 WiFi 风险检测数据，借助大数据学习和 AI 算法，实时判断虚假钓鱼 WiFi，构建业内最大的 WiFi 威胁情报库，保护用户 WiFi 网络安全。

伪基站检测为腾讯特色能力，可检测用户是否在伪基站覆盖范围内，减少诈骗行为发生。

**2、应用加固防篡改，保障移动出行安全**

自滴滴等移动出行平台诞生之日起，此类移动应用自身的安全问题就受到广泛关注。近期，在广州正式推出市场的明星出行产品——如祺出行，在产品开发之初就对应用安全给予足够重视，采用腾讯安全移动安全实验室多年能力积累的应用加固产品——乐固。

作为乘客与平台、司机直接沟通的中介，“如祺出行”APP 的安全是重中之重。腾讯移动安全乐固为“如祺出行”APP 提供安全防护，防御黑产逆向分析及恶意攻击，护航平台安全。出行类 APP 的安全重要性与其他 APP 不可同日而语，一旦被不法分子恶意逆向篡改，危害的甚至是乘客人身安全。

腾讯移动安全的乐固应用加固产品可以在不改变应用源代码的情况下，将针对应用各种安全缺陷的加固保护技术集成到应用各层，从而提升应用的整体安全水平。应用加固主要功能包括：VMP 虚拟化技术，文件水印，内存水印，控制流完整性，DEX 反编译保护、控制流混淆，二进制信息隐藏等功能。

伴随着产业互联网的推进，车企和出行领域转型升级将迎来更多元的选择，腾讯安全移动安全实验室将通过自身安全能力的释放及安全专家服务，携手越来越多的车企共同构建安全、美好的智慧出行生态。

## 议题八：联动与整合，“智”时代的云安全

## 研究团队：腾讯安全云安全团队

## 议题方向：云安全发展趋势

作为数字时代的重要基础设施和产业互联网的核心产业之一，云计算已成为数字化和产业互联网的重要推力。然而，随着业务云端化的变革，联网设备的激增，在释放生产潜能的同时，也因为安全边界模糊、数据管理混杂、业务风险难防、防御技术失衡，以及安全投入产出比的压力，让企业传统的单点防御措施，在面对各类新型攻击手段和威胁态势时应接不暇。事实上，日益繁荣的网络黑产已将云服务和其他相关技术变成攻击武器；而万物互联的趋势，更是给了攻击者更多的攻击渠道和安全漏洞。

得益于大数据、人工智能和云计算的整合，云上安全智能化成为必然趋势。海量数据归档能力的提升、云端计算资源的丰富、AI 智能分析算法的成熟都让安全实时分析和智能决策成为现实。云时代的大步迈进，让安全防护更加智能和强大。

在新形势下，不同于以往的单点防御，未来的企业安全将更强化业务纵深闭环和数据流全生命周期防控，以此构建云、管、端协同的智慧安全体系。

这样的安全体系，需要从以下 4 点实现业务保障：一是通过将多点威胁聚合，实现全路径风险感知；第二，通过以数据为中心的云端防护措施，通过定位和分析敏感数据、实现对数据的全生命周期管控；第三，关注企业生产业务流转，及时定位业务层面的安全问题；第四，通过云计算的智能学习+专家策略，实现对未知威胁的感知和防护；最后，可提供按需、按量、实时的产品和服务，帮助企业实现更加有效的 ROI 管理。此外，在复合网络生态空间下，仅仅聚焦于点和线的防御是不够的，而基于“云、管、端”协同的全链路智慧安全，对实现主动防御意义重大。

## 解决方案：

复杂的世界形势给全球广泛的领域带来了空前的安全挑战，谋求独立强大与合作共赢是众所周知的共识。因此，在数字经济时代，构建一个云安全生态依然需要集共同之力来完成。网络安全非常复杂，防御和攻击难度严重失衡，没有任何厂商可以独立应对。过去的经验也表明，全行业的生态合作与联合在现在和未来都不可或缺。

从安全的视角和经验来说，云安全生态构建的是一个可复制的、高效的立体防御体系，联动孤立的产品，从数据等方面进行联通，围绕 AI，实施有逻辑、有目的、有框架的整合。这个防御系统，需要结合多方力量来共同构建。

目前，腾讯云与腾讯安全联合实验室形成紧密的安全技术研究模式，并联手 100 多家在各自领域有着出色表现的安全厂商和安全服务机构，形成了多个领域、多个维度的生态合作，为企业数字化转型提供技术和服务能力。

腾讯希望依靠云管端协同的智慧生态，为用户持续提供安全的、可信的、智慧的云，助力更多企业高效迎接数字化浪潮，助力企业安全发展，为企业提供省时、省心、无感知的稳定安全管理平台，解决从安全设计到应急响应的全量安全需求，并且可一键式的启动全栈式安全防护能力（如 DDoS 防护、WAF、主机安全、数据安全等）。

## 典型事件：

**腾讯数盾，提供基于数据流的全周期安全防护**

数字化时代，企业数据一旦生产出来后就会进入传输、存储、处理、分析、访问与服务应用等各环节，且周而复始如同流淌的血液，而这些环节涉及到研发运维人员、最终用户、生态伙伴、服务器、办公终端、内外网络、大数据分析平台、云平台等，任意一个环节都面临着数据安全挑战，造成企业数据失血。所以企业试图在关键节点构筑防御堡垒，意义并不大。

导致泄漏事件持续发生的根本原因，主要是传统信息安全防护体系在云时代下，难以全

面支撑企业数据的安全防御。如果企业数据安全的防护还停留在基于静态资产的二维网络空间来思考和布局，就意味着将被时代列车抛在后面。物联网和云的出现，以及 5G 时代的到来，让传统网络边界变得更加模糊，进一步加大企业的数据安全防护难度。

面对日益复杂的网络空间和数据流动性加剧带来的挑战，企业在思考数据安全时，必须首先认识到数据的流动性，并从整体来看待数据安全的问题。

基于对数据流全流程的深刻理解，腾讯安全推出了数盾企业数据安全综合治理中心，以数据安全治理为核心，重点强化对数据资产感知、数据安全治理和联防联控的能力，并借助 AI 实现各孤立安全防护节点的联动与整合，从广度和深度两个方面对用户、行为、数据流实现全面防护。

数盾不是一套产品，数盾也不是一套解决方案，数盾是由人、解决方案和产品构成的企业数据安全综合治理中心，是企业数据安全的指挥官。

除此之外，数盾还结合腾讯安全的生态能力，以及围绕抗量子加密算法、AI 引擎数据库审计、K 匿名脱敏算法、新一代的智能数据安全网关——DASB 等全新技术探索带来的优势，同时整合服务能力、业务能力，为企业提供安全管理咨询、安全技术咨询以及安全专家服务。最终，数盾将实现助力企业构建服务、指挥、防护一体化的数据安全综合治理体系。

通过数据流串起企业的数据安全问题，以数据安全治理中心为核心，加上数据防护安全产品联动形成服务、指挥、防护一体的解决方案，为数据提供全生命周期的保护。

## 议题九：5G 到来，物联终端的终端安全与认证方案迫在眉睫

## 研究团队：腾讯安全无线安全团队

## 议题方向：终端安全与认证

第四次技术革命正在引领人类社会迈向万物互联、万物智能的全新时代，以智能手机、笔记本电脑为代表，涵盖智能家居、智能穿戴设备、智能 POS 机等智能终端有效的提高了

社会效率、降低了营运成本。而即将到来的 5G，更是凭借高带宽、低延时等特性，让联网设备的接入数量、数据传输数量等呈现一个爆发式的增长。

与此同时，从安全方面来看，万物互联打破了传统的网络安全边界，对安全管理提出了更大的挑战。首先，联网终端的数据在层层传输过程中极容易被攻击者劫持、窃听甚至篡改。同时，由于物联终端接入认证不完善，容易被仿冒、伪造接入。此外，受限于成本、技术等因素，物联终端难免出现安全防护水平参差不齐的情况，一旦被攻破，物联终端就会成为攻击物联云中心的跳板。

因此，有效的物联终端身份认证机制，以及各类接入权限控制措施，是解决物联终端安全必不可少的构成部分。

## 解决方案：

要解决物联终端的安全问题，仅依靠企业自身是不够的。还要从以下三个方面发力：监管层面，加快相关监管政策和安全标准体系建立，提高行业准入门槛，约束发展乱象；产业层面，推动构建多网互联下的全生命周期立体防御体系，将安全防护作为物联网每个环节必要的配套手段，推动整个产业对安全需求从被动转为主动，让安全紧跟产业发展步伐；技术方面，需探索更多新技术在物联终端安全领域的应用，加快对去中心化认证、边缘计算、终端安全轻量化防护技术等新技术新应用的研究，满足物联终端未来发展的安全保护需求。

而腾讯无线安全产品团队基于多年实践沉淀的业务移动化安全管理经验，推出了统一端点管理系统（Unified Endpoint Management）的行业解决方案。通过建立企业“身份流”、“数据流”、“业务流”三流安全体系，企业可根据自身的需求集中管理和保护终端设备、应用程序及移动数据，大幅提高企业 IT 管理效率，保障企业移动环境的安全。

系统主要拥有以下四项核心能力：

**设备全周期管理，移动风险轻松解**

提供设备从注册到注销的生命周期管理，如移动设备丢失/被盗/违规可远程擦除受保护

的数据和应用程序。

**数据公私能分离，个人隐私可兼顾**

业内领先的虚拟安全域能力，工作区内高强度数据加密及防泄露策略，工作区外最小化信息采集。

**应用加固再分发，统一管理全掌控**

提供企业私有应用商店，覆盖应用从分发到卸载的周期管理，支持自有应用安全增强及外部应用安全管控。

**移动威胁全监控，安全风险及时防**

依托十年的移动安全能力及 PB 级安全大数据，实时感知并防御病毒木马、网络攻击等风险。

目前，基于多年实践输出的业务移动化安全管理经验，腾讯安全推出了统一端点管理系统（Unified Endpoint Management）的行业解决方案。该系统通过建立企业的“身份流”、“数据流”、“业务流”三流安全体系，帮助企业企业根据自身的需求，集中管理、配置和保护终端设备、应用程序及移动数据，大幅提高企业 IT 管理效率，保障企业移动环境的安全。

## 典型事件：

**1、因物联设备遭攻击，美国多城市互联网曾遭遇大面积瘫痪事故**

2016 年，美国发生了一起规模极大的互联网瘫痪事故，多个城市的主要网站被攻击，人们发现连经常登录的推特、亚马逊、Paypal 等在内的大量网站也连续数小时无法正常访问。而造成这起事故的，是一种名为“Mirai”的恶意程序，通过扫描智能摄像头，尝试默认通用密码进行登录操作，一旦成功即将这台物联网设备作为“肉鸡”纳入到僵尸网络里，进而操控其攻击其他网络设备，当控制的设备达到一定数量级后，进行 DDoS 攻击。

而仅仅一年以后，相似的病毒“Rowdy”对中国 2 亿多台电视机顶盒发起了攻击。如

果攻击成功，将影响 2.23 亿户用户，后果将不堪设想。因此，物联设备的安全引起了各国政府和厂商的重视，陆续推出关于物联设备的管理意见。

**2、腾讯联合东华软件和华体科技中标成都市“智慧绿道”项目**

“智慧绿道”通过前端高度集成的 5G 智慧灯杆，搭载智能路灯、多媒体发布、无线 AP、一键报警、5G 微基站及多种功能，将信息传输到统一的大数据中心平台进行控制、管理和联动。数据的采集和管控是 5G 智慧灯杆的核心，也成为万物互联的关键节点。这对每一个灯杆的设备准入、设备安全、数据安全、通道安全提出了更高的挑战。

## 议题十：政企数字化转型中面临的安全管理挑战

## 研究团队：腾讯安全桌面安全团队

## 议题方向：智能安全管理

伴随着互联网的下半场向产业互联网转移，云计算、大数据、人工智能等领域涌现出产业、行业改造新机遇。同时，企业所面临的网络安全环境也愈加复杂，已不是传统的安全运营所能应对的。威胁攻击复杂多变，传统安全防护体系亟待升级；基础设施全面云化，安全运营更加复杂，如云内资产发现与管理，云内流量检测与分析、云安全运营责任共担以及云安全通报与处置闭环等。同时，随着网络安全等级保护制度 2.0 标准将于 2019 年 12 月实施，国家对企业的安全准入门槛和发展要求也越来越高。安全已经成为了制约企业发展的天花板。

如何应对新威胁、新技术、新要求带来的挑战，不仅关系到组织的发展，也是最根本的生存问题。对于企业而言，被动、静态、单点、粗放和孤立的安全管理模式和理念已经过时，需要的是更为主动、动态、整体、精准和开放的安全运维、运营和管理。

## 解决方案：

基于“开放共治”的安全管理新模式，腾讯安全今年 5 月份，推出了全新的企业级安全管理平台——腾讯御见安全中心，从打破安全信息孤岛、行业协同共治、及时全面的威胁情报，以及智能化的安全运营等角度，打造开放共治的安全管理模式。

以企业内网常见的横向渗透为例，腾讯御见安全中心会对一连串入侵过程进行溯源分析，在发现内部风险与匹配的外部情报后，会对平台所有资产进行扫描，显示出受影响的主机数量和机房分布，并提供完整防御方案、操作手册及专家服务，协助受威胁伙伴对漏洞进行处置和修复。

腾讯御见安全中心是腾讯基于 20 年服务 10 亿级用户、海量业务安全运营经验，行业内最全的安全大数据库和领先的大数据能力，以及全球最顶尖的安全专家团队等三大核心优势，打造的大数据+智能化安全管理平台，有效打通安全管理中的检测、分析、响应和预测各个环节，实现企业级安全威胁的全方位检测、智能化分析、高效率处置。

同时，腾讯御见安全中心也很好地发挥“人”在安全运营管理中的价值，通过这一中心性枢纽，腾讯安全对外开放自身的安全专家服务和管理流程经验，实现安全管理中人、技术和流程的有机整合。

目前，腾讯御见安全中心平台已经接入了数家第三方合作伙伴的能力技术和解决方案，合作链条、覆盖面不断拓展。同时随着腾讯组织架构变革，腾讯安全进一步与腾讯云深度融合，构建全球领先“云、管、端”产业互联网安全防护体系，并结合腾讯全球最大、覆盖最全的安全大数据库，构建全景化、分类化的威胁情报知识图谱。除此之外，腾讯安全还整合旗下七大实验室安全专家的经验技术，对外输出全球最顶尖的安全专家服务，为企业客户量身定制安全解决方案。

## 典型事件：

**1、窃密团伙瞄准企业机密信息，备用病毒超 60 个**

数据正在成为信息时代最有价值的资产，在网络黑市，大量个人及企业数据被肆意买卖交换，窃取、出售数据是网络黑产牟利的主要方式之一。国家对保护个人及企业信息安全，有严格的法律法规要求，即将颁布《网络安全等级保护技术 2.0》做为全国各个行业改进信息安全的指导性文件。

2019 年 5 月，腾讯御见威胁情报中心截获一个恶意利用高危漏洞攻击的 Office 文档，该窃密团伙通过多种方式分发病毒模块，包括：利用漏洞构造 Office 攻击文档、伪装为 explorer 或诱饵压缩包的快捷方式执行远程控制木马等，在该窃密病毒团伙的木马下载站点，主要恶意病毒类型为远程控制类及窃密类木马，总计有 34 个分类目录，病毒数量总计超过 60 个。

**2、化被动为主动，御见安全帮助客户“防患于未然”**

近年来频繁爆发的数据泄露事件、各类型 APT 攻击等，在造成大量损失的同时，也促使企业更加重视对安全问题的研究。在产业互联网时代，安全保障的主体将从人演变为以产业为中心；面对安全问题时，也需调整思维，从被动防御转变为主动规划。

作为一款安全大数据分析及可视化平台，腾讯御见安全中心平台以安全检测为核心、以事件关联分析、腾讯威胁情报为重点、以 3D 可视化为特色、以可靠服务为保障，针对企业面临的外部攻击和内部潜在风险进行深度检测，为企业提供及时的安全告警。通过对海量数据进行多维度分析、及时预警，并且对威胁及时做出智能处置，实现企业全网安全态势可知、可见、可控的闭环。

在为上汽集团提供安全服务时，腾讯御见安全中心平台协助实现了云内主机威胁检测、数据中心内部高级威胁检测，实现了安全运营与处置闭环。例如，通过多源信息汇聚关联，面对突发的 ECShop 漏洞攻击，不仅提前发出预警通报，还针对性给出了解决方案，化解了危机；而御见态势大屏，兼顾了汇报故事性与运营使用性，方便安全运营人员了解安全运营工作的开展情况。

# 总结

当下，产业互联网构建新型的、产业级的数字生态，正在加速打通各产业间、内外部连接，以新兴产业的技术提高传统产业效率、以传统产业的市场带动新兴产业规模，达到1+1>2 的效果。

但是，随着各行各业的数字化程度不断加深，联网终端的多样性、使用环境的复杂性，正在让产业环境下的人、信息、物之间的交叉连接日益复杂，随着防护边界越来越模糊、攻击复杂度越来越高，催生了更多的安全威胁，传统的安全问题并没有消失。

在这种复杂多变的环境下，腾讯安全科恩实验室、玄武实验室、湛泸实验室、云鼎实验室、反诈骗实验室、反病毒实验室、移动安全实验室、云安全团队、无线安全团队、桌面安全团队等十大国内最顶尖的安全实验室联合发布了首份产业互联网时代的十大安全议题。

通过实验室的联合解读，我们可以发现，当前产业安全面临的问题或趋势主要有以下几方面：受制于一些交付压力和成本控制，诸多 IoT 设备相当于处在“裸奔”的状态中；安全问题的隐蔽性和传染性更强；安全措施必须随着安全问题不断进化；企业面临的网络安全威胁更复杂，且危害更大；防护边界越来越模糊、攻击复杂度越来越高，数据共享需求越来越频繁；产业互联网时代需要的是更为主动、动态、整体、精准和开放的安全运维、运营和管理。

根据产业安全面临的不同问题，十大实验室也给出了针对性的解决方案，比如， 针对物联网及车联安全，科恩研发了一款全自动 IoT 固件安全扫描系统 IoTSec；针对企业安全架构建设逐步从“以网络为中心”转向“以数据为中心”的趋势，腾讯安全云鼎实验室通过专业的数据治理技术、加密服务中台设施，以及核心数据安全产品，从技术层、云产品层、安全服务层、解决方案层，共建云上数据安全应用生态，提供给云用户覆盖数据获取、事务处理及检索、数据分析与服务，数据访问与消费的数据全生命周期的安全保护，帮助企业便捷快速地搭建起安全合规的数据安全策略及业务加密架构。


CSS
互联网安全领袖峰会
Cyber Security Summit
腾讯安全
出品单位：腾讯安全