国内外云计算+安全动态报告

2019 年第 4 期

启明星辰云计算安全事业部

目录

本期云安全动态内容摘要

云厂商方面，AWS 添加多项增强，包括 Amazon CloudFront 增强了将备用域名添加到分配的安全性、Amazon RDS 增强型监控添加了新的存储和主机指标以及 Amazon QuickSight 现在支持本地化、百分位数计算等，同时 AWS Amplify 控制台现在支持一键部署全栈式无服务器应用程序，AWS Server Migration Service 中支持 Azure 到 AWS 的迁移;英特尔和谷歌云宣布达成战略合作伙伴关系；阿里云通用电子标签系统正式上线、中国联通牵手阿里云聚焦 5G 时代的超高清视频发展、2018 年阿里云亚太市场份额领先；腾讯云携手四家合作伙伴签约落地，助力贵阳数字化建设，腾讯云与无锡广电战略合作；华为云发布四大金融行业解决方案。

开源云方面，OpenStack Stein 正式发布；EasyStack 入选创业黑马“中国科创企业 TOP100”；2018 年度中国 SDN、NFV 优秀案例奖公布，九州云中国人寿案例获奖。

云安全厂商方面，启明星辰参加信息技术应用创新研讨会积极推进网络安全可靠工作、入选工信部网络安全技术应用试点示范项目、助阵 CCBN2019 县级融媒体发展论坛、构建“安全中台” 迎接产业互联网安全升级；深信服“边云协同”方案亮相 IPF2019；山石网科推出满足 NFV 标准的安全网元解决方案“山石云•集”；亚信安全提出 5G 安全解决方案； 绿盟科技发布《绿盟数据安全解决方案》；奇安信上网行为管理产品持续多年领跑市场；安天两项目入选工信部网络安全技术应用试点示范项目。

容器动态方面，Linkerd 2.3 正式发布，为 Kubernetes 提供零接触、零信任网络； CNCF 宣布在继 Kubernetes、Prometheus、Envoy 以及 CoreDNS、containerd

之后，Fluentd 成为其第六个毕业项目；Google 在器 Google Cloud Next 2019 大会上发布了 Cloud Run 和 Traffic Director 两个项目；开源项目 Kubecost 让 k8s 花费一目了然；kubernetes 近期漏洞分析及解决。

安全新技术方面，网信办实施多项措施，包括启动小众即时通信工具专项整治和结合 4 部门联合启动启动剑网 2019 专项整治；国家发改委将虚拟货币”挖矿”列为淘汰类产业；高通近 40 款芯片被曝出泄密漏洞，可窃取机密信息；iLnkP2P 弱点暴露数百万物联网设备；研究人员开发新方法来检测隐藏在硬件组件中的恶意软件。

网络安全投融资方面，分别发生 1 起收购和 3 起融资事件。全球领导安全厂商 Palo Alto 公司所属投资机构收购安全风险管理(SRM)软件和解决方案公司 RedSeal，收购价未公开。融资方面，CASB 厂商 Bitglass 以 7000 万美元的 D 轮融资拔得头筹，容器安全公司 Aqua Security 以 6200 万美元的 C 轮融资位列第二，物联网安全公司 VDOO 则以 3200 万美元的 B 轮融资排名第三。

2019 年 4 月 29 日

云计算安全事业部

国内外云+安全动态报告

一、 云厂商动态

1. AWS 云动态

1.1 AWS Amplify 控制台现在支持一键部署全栈式无服务器应用程序

4 月 5 日消息，AWS Amplify 控制台现在有一个“部署到 Amplify 控制台”按钮，允许 GitHub 用户一键自动部署全栈式无服务器 Web 应用程序。

全栈式无服务器应用程序包含 GraphQL API 和 Lambda 函数等后端资源，以及使用 React、Angular 或 Gatsby 等框架构建的前端。单击“部署到 Amplify 控制台”按钮后，Amplify 控制台首先将存储库分叉到您的 GitHub 帐户，然后在单一工作流中部署后端和前端。“部署到 Amplify”按钮允许您公开或在团队内共享 Web 项目，以便所有贡献者可以一键将应用程序部署到各个 AWS 账户。

1.2 Amazon CloudFront 增强了将备用域名添加到分配的安全性

4 月 8 日，Amazon CloudFront 已能提高将备用域名添加到分配这个过程的安全性。现在，当用户将备用域名（如 www.example.com）添加到分配时，还必须将 SSL/TLS 证书附加到涵盖该备用域名的分配。只有经过授权可以访问域证书的人，才能将域名作为备用域名添加到 CloudFront 分配。

通过向 CloudFront 添加备用域名，用户可以使用 DNS 记录（例如 www.example.com）中的自定义 CNAME 代替 CloudFront 分配的默认域（如 d111111abcdef8.cloudfront.net）来提供内容。通过此更改，当用户使用 AWS 管理控制台或 CloudFront API 添加备用域名时，需要将证书附加到分配以确认用户有权使用该备用域名。证书必须有效，并且来自公众信任的证书颁发机构，例如 AWS Certificate Manager，它免费提供公共 SSL/TLS 证书。在此更改生效之前，已添加到 CloudFront 分配的所有备用域名将继续像以前一样工作。

1.3 Amazon QuickSight 现在支持本地化、百分位数计算等

4 月 10 日，Amazon QuickSight 已经实现 10 种主要语言的本地化。Amazon QuickSight 整体产品支持这些语言，任何人都能比以往更轻松地从数据中获取更深入的洞察。支持的语

言包括英语、德语、西班牙语、法语、意大利语、葡萄牙语、日语、韩语、简体中文和繁体中文。

此外，QuickSight 现在还支持百分位数计算，帮助用户生成任何度量的第 50、90、95 或 n 个百分位数，从而轻松地将数据分布可视化。现在，用户还可以格式化用户视觉效果，在显示“其他”类别之前，显示自定义数量的数据点或组。此功能可用于条形图、组合图表、线形图、饼状图、热图和树形图。

1.4 Amazon RDS 增强型监控添加了新的存储和主机指标

4 月 12 日，Amazon Relational Database Service (RDS) 增强型监控提供对 Amazon RDS 实例运行状况的可见性，现在可以报告物理存储设备指标和二级实例主机指标。

当 Amazon RDS 存储使用多个底层物理设备时，增强型监控会收集每个设备的数据。此外，当数据库实例在多可用区配置中运行时，将收集二级主机上每个设备的数据以及二级主机指标。

物理设备和多可用区二级主机指标均可在 RDS for Oracle、RDS for PostgreSQL 和 RDS for MySQL 上使用。通过在每个物理设备上报告数据，用户可以查看有多少物理设备组成其卷、I/O 在物理设备之间是否均衡，以及物理设备之间的延迟是否一致。

1.5 AWS Server Migration Service 中支持 Azure 到 AWS 的迁移

4 月 18 日消息，AWS Server Migration Service (SMS) 现在支持将 Microsoft Azure 中运行的虚拟机 (VM) 迁移到 AWS 云。新功能使用户可以更轻松地将 Microsoft Azure 中运行的现有应用程序迁移到 AWS 云，从而获得更大的可靠性、更快的性能、更安全的功能和更低的成本。

AWS Server Migration Service 是一种无代理服务，让用户能够更方便快捷地将现有工作负载迁移到 AWS。它可让用户自动执行实时服务器卷的增量复制、为其制定计划以及进行跟踪，从而能够更轻松地协调大规模服务器迁移。到目前为止，客户可以迁移在 VMware vSphere 和 Microsoft Hyper-V 环境中运行的 VM。从今天开始，客户还可以使用 Server Migration Service 轻松简单地迁移在 Microsoft Azure 中运行的 VM。用户可以发现 Azure VM，将它们分组到应用程序中，并将应用程序组作为单个单元迁移，而不必费力协调单个服务器的复制或分离应用程序依赖关系。Server Migration Service 显著缩短了应用程序的迁移时间，并且降低了迁移过程出错的风险。

2. VMWare 云动态

暂无消息。

3. GOOGLE 云动态

3.1 英特尔和谷歌云宣布达成战略合作伙伴关系

4 月 2 日消息，英特尔和谷歌云（Google Cloud）宣布建立战略合作伙伴关系，旨在帮助企业客户在企业本地和公有云环境之间实现无缝的应用部署。两家公司将合作开发一款基于第二代英特尔可扩展处理器的全新服务平台参考设计 Anthos。该参考设计是一套优化的 Kubernetes 软件堆栈，能够为希望利用混合云环境的客户提供更强的工作负载可移植性。英特尔会将这套服务平台生产环境的设计作为英特尔精选解决方案，同时会面向开发者提供相关方案平台。

尽管很多企业正在采用多云解决方案来推动业务发展，但仍有很多公司难以找到合适的混合云解决方案来实现工作负载在各云之间的无缝迁移。全新的 Anthos 参考设计将通过对工作负载可移植性进行优化的堆栈来应对这一挑战，支持跨企业本地数据中心和多个公有云提供商服务之间的应用部署。

此次合作是两家公司之间技术联盟的延伸。该联盟已经促成了多项基础架构优化、人工智能等高速发展领域的工作负载方面的合作，以及第二代英特尔至强可扩展处理器和英特尔持久内存等新技术在谷歌云平台上的集成。

4. 微软 Azure 云动态

暂无消息。

5. 阿里云动态

5.1 阿里云通用电子标签系统正式上线

4 月 23 日，阿里云通用电子标签系统正式上线，该产品为阿里云完全自主研发，包含 PaaS 平台和 LoRa 电子标签硬件产品。其中 LoRa 电子标签硬件产品待机时长超过 5 年，信息传输距离可超过 1000 米，可广泛应用在企业工位管理系统、智能会议系统、智能仓储系统、巡检系统、新零售门店价签系统和医疗系统中。

据了解，相比现有商超传统的电子价签，阿里云 LoRa 电子标签的信息传输距离超过 10~50 倍，同时具备功耗低，覆盖广，易部署等特点。另外在 PaaS 平台层面，提供了电子标签通用服务，可以接入多种通信协议电子标签类产品。该解决方案目前已经与钉钉打通，助力智慧办公应用场景，为中小企业客户提供一站式服务。

阿里云相关负责人介绍，目前在阿里巴巴园区，该方案目前已经广泛应用。首先是电子工位牌，每个员工拥有一个电子工位牌，上面除了显示员工的姓名、工号；同时实时显示员工每天的行程信息，每天一早无需查看手机，直接在工位牌就可以了解当天的重要事项，其次是电子会议桌签，只需要将信息输入手机端便可以直接在电子会议桌签上显示来访成员信息，同时也可以用手机更改会议议程，统计会议数据统计。最后是能效管理，可以帮助行政实时显示电费消耗情况、线路电量异常报警、力调电费情况，自动给出每月的电力需量、优化方案。

5.2 中国联通牵手阿里云聚焦 5G 时代的超高清视频发展

4 月 24 日消息，在中国联通合作伙伴大会上，阿里云与中国联通签署合作协议，未来双方将基于各自优势，聚焦 5G 时代下的超高清视频发展。

随着 5G 时代到来，视频不再被网速制约，超短延时、计算节点下沉等特性将更高清、更极速、更创新丰富的媒体形式更快地带到大众视野中，长视频、短视频和直播都将再次迎来爆发性发展，如超高清的 4K 视频体验、沉浸式的 VR/AR 体验、强交互的云游戏体验等。

中国联通与阿里云将发挥各自在 5G 技术、视频技术上优势，重点针对 5G 环境下 4K、8K 超高清节目的多路传输等进行全面测试和应用研究，积极开展 5G 环境下的视频制作和产品创新，致力于为用户带来全新的视听体验。

阿里云副总裁金戈表示，在视频制作领域，5G 使得传统视频生产更容易云化。传统需要卫星、微波、专线进行的体育赛事转播、新闻报道、远程视频制作，利用 5G 带来的大带宽以及网络切片技术，可以在云端进行制作，大大节省现场设备的布置，使得基于“云”的媒体生产线、转播间真正成为可能。

新应用场景的创新，也将对视频云服务的并发处理、内容传输、存储带来更大的挑战。

作为领先的视频云服务厂商，阿里云拥有强大的基础设施、多年积累的音视频编解码技术、人工智能技术与覆盖全球的媒体处理与分发网络，有能力构建 5G+4K 新媒体平台与 5G+8K 直播服务，赋能新媒体生态伙伴。

早在去年，阿里云就发布了全球首个 8K 视频云解决方案，宣告互联网 8K 时代的来临，

并联合中国联通、京东方、松下电器等多家企业成立 8K 产业联盟，推进超高清产业商用，这足以表明阿里云在 5G 时代的“野心”与布局。除此之外，阿里云 4K 新媒体平台可以将 4K 超高清、高帧率的视频实时处理，整体画质得到了大幅提升。

5.3 2018 年阿里云亚太市场份额领先

4 月 25 日消息，研究机构 Gartner 发布最新市场调研数据，在云计算基础设施领域，2018 年阿里云在亚太区域市场份额为 19.6%，同期亚马逊为 11%、微软为 8%。同比 2017 年，阿里云市场份额增长 4.7 个百分点。同时，在全球范围内，阿里云持续保持全球前三的领先地位。

公开资料显示，2018 自然年阿里云营收达到 213.4 亿元，四年间增长 20 倍。高速增长的同时，阿里巴巴还在不断加码对云业务的战略投入，将全集团的技术与云全面结合并对外输出，目标是构建数字经济时代的云智能基础设施。

同时，阿里巴巴自身也将在未来 1-2 年内 All in Cloud，为数字经济发展提供新技术和新理念。

6. 腾讯云动态

6.1 腾讯云携手四家合作伙伴签约落地，助力贵阳数字化建设

4 月 19 日消息，为加速推进与贵阳市政府深化合作协议的落地、积极参与贵阳市大数据的建设与发展，共同营造良好的营商环境，4 月 18 日，由腾讯云与贵阳市大数据发展管理局、贵阳国家高新技术产业开发区管委会联合主办，贵州优特云科技有限公司承办的贵阳市腾讯云生态企业沟通会在贵阳金阳大酒店举行，会上腾讯云与诸多合作伙伴共同探讨产业互联网生态体系打造，以及在贵阳市的合作商机。

贵阳市副市长唐兴伦、腾讯云和智慧产业西南总经理潘华与会并致辞，分别对贵阳市的“中国数谷”建设的总体战略目标以及推动云计算、大数据、区块链、人工智能等数字化工具在贵阳经济社会各领域的发展应用和融合创新进行了分享。

6.2 腾讯云与无锡广电战略合作

4 月 25 日消息，腾讯云与无锡广播电视集团(台)签订战略合作框架协议,携手打造全国融合云计算、人工智能以及大数据能力的城市级融媒体服务平台。无锡广播电视集团(台)党委书记、总裁、台长郭王、腾讯副总裁、腾讯云总裁邱跃鹏、腾讯云副总裁道峰以及腾讯云

智慧业务总经理蔡毅等人出席了本次签约仪式。

作为全国城市广电集团、首届中国广电“融媒体中心”改革大会的首倡者组织者,无锡广电近年来倾力于传统媒体的转型升级,积极运用新技术、新机制、新模式,推动媒体融合向纵深发展,做大做强主流舆论。突出移动优先战略,在引导舆论、服务群众中,把控主导权占领制高点。此次合作,双方意在共同建设集应急动员、资讯共享、舆情监控、AI 采编、社群服务等为一体的融媒体综合服务平台,为行业树立示范样板。

腾讯云依托自身在云计算、大数据、人工智能及基础技术服务等领域的经验与积累,将内容生产、生活服务、社会治理、商业变现四个维度相结合,为无锡广播电视集团(台)构建高覆盖度的互联网融合媒体平台。这个平台能自动获取互联网热点新闻,并对热点话题进行聚合、分析、评估,并且能够有效地对舆情进行监测并处理。聚焦社区公共服务,提供党群联系、意见上传、政务快达等一系列便民惠民服务,快捷满足社区居民即时需求,随时随地分忧解难,提升群众获得感幸福感。籍此次合作中累积的经验,腾讯云将打造更加全面的智慧媒体解决方案,助力其他媒体加快融合发展步伐。

7. 华为云动态

7.1 华为云发布四大金融行业解决方案

4 月 26 日消息，在 2019 华为全球金融峰会之“云上金融，智见未来”分论坛，华为云发布包含 5G 智慧银行、虚拟银行、商品交易所动产质押和区块链联合征信在内的四大金融行业解决方案，为构建智能金融提供“可靠选择”。

数字时代客户的行为模式不断变化，推动金融行业的商业模式和价值链不断改变，数据洞察驱动金融产品和服务不断创新，运营效率提升和成本优化带来了更优的客户体验，而 ICT 基础设施的发展推动高性能和高可靠的信息处理，整个金融行业正面临数字化转型的挑战和机遇。

华为云中国区副总裁胡维琦以“+智能 见未来 选择华为云更可靠”为主题发表演讲，她全方位介绍了华为云在金融行业的能力和价值：华为云全栈全场景解决方案为金融行业智能化升级提供强大动力，华为智能计算通过强大算力为金融机构提供最优性能，华为云 ModelArts 助力金融 AI 极简开发，5G 技术拓展金融物联的应用场景，而 HCS online 是最满足金融需求的混合云解决方案。华为云致力于携手伙伴帮助国内的银行、保险、证券、互联网金融企业快速实现业务云化部署，满足业务快速发展的需求，推进金融科技创新。

华为云金融行业总经理杨剑平发布了四大金融行业解决方案，将云计算、人工智能、5G、IoT 等技术整合应用到金融行业，端、边、云协同为客户提供安全可靠的行业解决方案，使能行业智能化升级。

华为云四大金融行业解决方案包括：

5G 智慧银行营业厅解决方案：基于 IoT、VR、8K、AI 等新技术，依托华为 5G 高速通道和边云协同技术，为用户提供沉浸式体验和个性化服务，打造创新的智慧营业厅，全面助力银行服务和用户体验智能化升级。

虚拟银行解决方案：通过提供 100%独享的基础设施、灵活组合的资源和服务、全栈安全防护体系、规范可靠的运维体系，提供一站式、安全合规的金融行业数字化信息底座，助力业务快速上线与创新。该方案保持开放架构、开放生态，防止客户被单一厂商锁定，实现与客户的全面协同，并赋予客户足够的自主选择权，为客户提供的定制服务。

商品交易所动产质押解决方案：针对传统的交易所动产质押、仓单的权利质押面临人工监管不可靠、资产状态难感知、一物多抵高风险、多方互信难解决等众多金融质押挑战，该方案依托 IoT、边缘计算、AI 等新兴技术，实现了对动产存货的识别、定位、跟踪、监控，以及智能化的管理，使客户、监管方、金融机构等各方参与者均可以从时间、空间等多维度全面感知动产存续的状态和变化，有效解决了动产融资过程中实时性差和信息不对称问题，帮助客户降低抵押业务风险。

区块链联合征信解决方案：针对金融行业征信业务面临信用信息不对称、数据采集渠道受限、数据隐私保护等挑战，该方案提供低于 150ms 的电信级系统时延，实现信用数据多源的毫秒级交叉验证与共享，征信信息加密存储和传输，确保信息主体隐私权，提高征信数据的可信度、降低征信成本，实现信用资源的共享共通、共建共用。

此外，德勤金融首席行业分析师张志钢、公安三所安全专家宋好好、上海大智慧股份有限公司 CTO 于青峰、上海前隆信息科技有限公司 CTO 周强、合胜科技业务总监鲍捷等行业专家、客户和合作伙伴先后发表重要演讲。众嘉宾还参与了以“多云架构、5G 技术和人工智能在金融科技中的应用”为主题的圆桌讨论，共同探索金融科技的发展方向。

二、 开源云动态

1. Openstack 动态

1.1 OpenStack Stein 正式发布

4 月 12 日消息，OpenStack 社区正式发布了广泛部署的开源云基础设施软件的第 19 个版本 Stein。目前，该软件为超过 75 个公有云数据中心和数千个私有云提供支持，其规模超过 1000 万个计算核心。OpenStack 是一个非常适合部署裸机、虚拟机（VMs）、图形处理单元（GPUs）和容器等架构的基础设施平台。

在 Stein 版本的几十项新增功能特性中，有三个主要亮点：

- 容器功能的强化
- 用于支持 5G、边缘计算和网络功能虚拟化（NFV）用例的网络升级功能
- 资源管理和追踪性能的增强

OpenStack Stein 为 Kubernetes 用户提供核心功能

2018 OpenStack 用户调查结果显示，Kubernetes 是在 OpenStack 上运行容器编排架构的首要选择，在所有部署 OpenStack 的用户中，有 61%的用户表示他们在集成这两个平台。

在 Stein 版本中，OpenStack 继续提供核心基础设施管理功能，以及运行容器所需的裸机和网络功能：

- OpenStack Magnum，经过认证的 Kubernetes 安装程序，显著提升了 Kubernetes 集群的启动时间—无论节点数量多少，每个节点从 10-12 分钟降至 5 分钟。
- 通过 OpenStack 云供应商，您现在可以在 Manila、Cinder 和 Keystone 服务的支持下启动完全集成的 Kubernetes 集群，从而充分利用其底层的 OpenStack 云平台。
- Neutron，OpenStack 网络服务，针对在组中创建端口的容器用例，更快速的创建批量端口。
- Ironic，裸机配置服务，持续改进部署模板，以便于独立用户请求分配裸机节点并提交配置数据，而不需要预先配置驱动器。

为 5G、边缘计算和 NFV 用例提供网络强化功能：

- Neutron，网段范围管理，云管理员可通过新的扩展 API 动态管理网段范围，而不是采用之前编辑配置文件的方法。StarlingX 和边缘用例将得益于此，更易于管理。
- 对于网络密集型应用程序，拥有最小可用网络带宽至关重要。在 Rocky 周期中开

始工作，提供基于最小带宽需求的调度，该功能已在 Stein 中交付。作为强化功能的一部分，Neutron 将带宽视为一种资源，并与 OpenStack Nova 计算服务协作，将实例调度到满足其带宽需求的主机上。

- 对 API 的改进增加了 OpenStack 体系结构和部署的灵活性，增加了对服务质量（QoS）策略规则 aliases 的支持，使调用者能够更高效地执行删除、显示和更新 QoS 规则等请求。

增强资源管理和追踪性能：

- Blazar，资源预留服务，引进了新的资源分配 API，运营商可查询其云计算资源的保留状态。
- Placement 是引入 Stein 版本的一个新项目，是从 Nova 项目中分离出来的。可定位候选资源供应商，简化了为工作负载迁移指定主机的任务。对于常见的调度操作，API 性能提升了 50%。Train 版本中将删除 Nova 中的 Placement 服务，其后安装 Nova 需要使用单独的 Placement 服务。
- Sahara，一个轻松配置 Hadoop 集群的项目，已经重构为核心+插件架构，以便于更好的利用其功能。

Jonathan Bryce, OpenStack 基金会执行董事表示：“OpenStack 已是在私有云和多云部署中管理 Kubernetes 集群的强大平台，运营商通过 Stein 可获得一系列新的功能，如裸机和网络管理，采用 GPUs 运行高性能工作负载，进行 NFV 部署，以及部署各种企业应用实例等。Stein 的发布是社区在提供开放基础设施服务方面辛勤工作的成果，这些服务为运营商和用户解决了真正亟需解决的问题。”

其他亮点：

- Keystone，OpenStack 身份识别服务，在 Stein 版本中引入了多重身份验证凭证，有助于实现更加自然有序的认证流程。
- Kolla，提供开箱即用的容器服务，且在部署工具中已添加了对执行 MariaDB 数据库的完整备份和增量备份的支持。
- Senlin，在暴雪娱乐团队的领导下，Senlin 集群服务中的 API 现在可在集群/节点锁定，冷却生效或操作冲突的情况下发出同步故障。运维人员还可使用 Senlin-manage 工具中的 action-purge 子命令删除已完成的操作。这对于在数据库中积累了大量操作指令且已长时间运行的集群非常有用。总之，在 Stein 版本中对 Senlin 的升级将操作性能提高了几个数量级。

2. Easystack 动态

2.1 EasyStack 入选创业黑马“中国科创企业 TOP100”

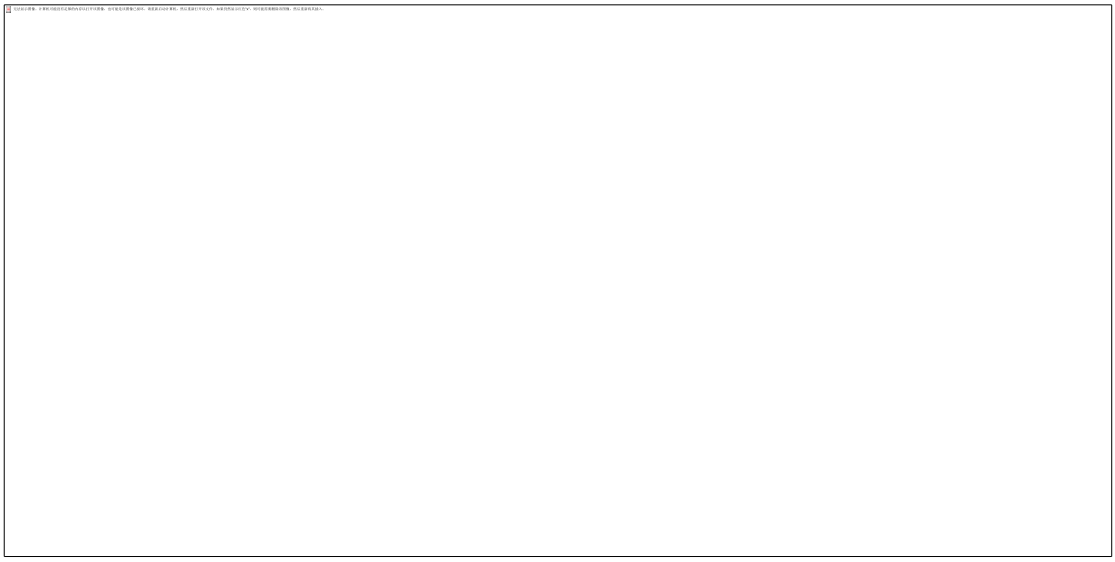
4 月 4 日消息，由创业黑马联合证券日报、上海证券报、新浪财经等多家机构共同发起“中国科创企业 TOP100”评选最终揭晓。在数百家参选企业中，评审团从科技实力、投资价值、成长价值、领先价值等四大维度进行全方位打分，最终得出涵盖云计算、人工智能、大数据、物联网、医疗行业等十大领域共 100 家入选企业。易捷行云 EasyStack 作为中国开源云计算领先的提供商，凭借强大的技术实力，先进的产品以及良好的市场影响力，最终入选“中国科创企业 TOP100”榜单。

3. 99CLOUD（九州云）动态

3.1 2018 年度中国 SDN、NFV 优秀案例奖公布，九州云中国人寿案例获奖

4 月 17 日，由 SDN/NFV/AI 标准与产业推进委员会指导，IT168 和 C114 联合主办的“2018 年度中国 SDN、NFV 优秀案例”评选结果正式出炉。中国人寿携手九州云共同推荐的“基于 SDN 的生产云联合实践”从 46 个候选案例中脱颖而出，经专家组评定，被授予优秀案例

奖，并在昨天举办的“2019 中国 SDN/NFV/AI 大会”上获得正式颁奖。



三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰参加信息技术应用创新研讨会积极推进网络安全可靠工作

启明星辰集团参加信息技术应用创新研讨会，积极推进安全可靠工作，并发布启明星辰入侵检测系统 V7.0、网御高性能飞腾防火墙、网御高性能飞腾安全网关 3 款安全可靠新产品，得到与会专家高度评价和认可。

本次信息技术应用创新研讨会在江苏省南京市召开，会议由中国电子工业标准化技术协

会安全可靠工作委员会和江苏省工业和信息化厅共同主办。工业和信息化部、国家工业信息安全发展研究中心、中国电子技术标准化研究院等 111 家党政金融等用户单位、7 家地方工信主管部门、203 家安全可靠工作委员会会员单位，共 640 余人参加会议。

启明星辰入侵检测系统 V7.0 产品亮点

1）安全可靠：硬件上 CPU 等关键零部件采用国产芯片，软件实现自主研发。

2）精准检测：采用多项技术及算法，有效地降低了误报率和漏报率，实现全面精细的检测库。

3）威胁可视化：全面呈现威胁事件对病毒、入侵、异常、流量等行为全面分析，提升用户了解网络状况的直观感受。

网御星云发布了两款新产品：网御高性能飞腾防火墙使用成熟稳定的飞腾处理器、专用网络处理器、安全可靠内存组成的硬件平台，产品的核心技术、关键零部件、各类软件实现自主研发、生产、升级及维护，基本摆脱对外部环境的依赖。

网御高性能飞腾安全网关是网御星云推出的综合安全防护与应用管控产品，提供应用识别与管控、web 安全防护、病毒防护、入侵防护、DDOS 攻击等综合防护能力的产品，规格覆盖百兆、千兆、万兆，除标准上架式 1U、2U 整机产品外，为了实现飞腾架构的全面技术优势，还将开发电信机架式 ATCA 架构整机产品。产品类型支持广泛，能够适应各类应用场景。

1.2 启明星辰入选工信部网络安全技术应用试点示范项目

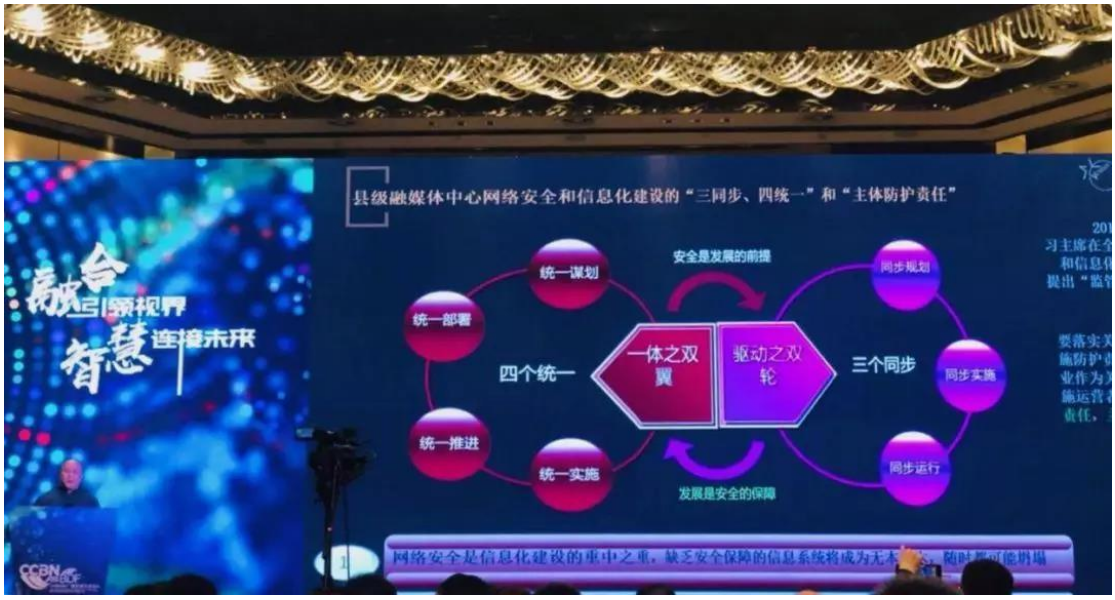
4 月 18 日，工信部网络安全管理局发布了网络安全技术应用试点示范项目公示名单，对经过专家评审的 101 个重点网络安全技术应用试点示范项目进行了公示。

启明星辰项目上榜：

与北京联通联合申报的《基于软件定义高级融合安全的面向互联网应用虚拟资源池平台》（第 14 项）

1.3 启明星辰泰合品牌“绝不能让用户的信息安全流浪”

近日，由国家广播电视总局举办的第二十七届中国国际广播影视发展论坛（CCBN-BDF）在北京举办。CCBN2019 聚焦媒体深度融合发展和智慧广电创新发展，全面展示和交流新一代信息技术与广播电视的深度融合应用。启明星辰作为“县级融媒体发展论坛”上唯一应邀参会的网络安全企业发表了《县级融媒体中心网络安全体系化建设》的主题演讲。



县级融媒体中心建设成为本届大会的一个新热点，启明星辰助理总裁毕亲波在《县级融媒体中心网络安全体系化建设》的主题演讲中，结合由启明星辰参与编写的即将发布的“县级融媒体中心网络安全规范”，探讨和分析县级融媒体中心的建设和业务模式，结合网络安全和信息化建设相关的“一法两战略”、“三同步、四统一”和“主体防护责任”等方面重点介绍了县级融媒体中心网络安全建设的必要性、重要性、紧迫性和实操性。

同时，基于网络攻击杀伤链和业界网络安全建设的最佳实践，结合媒体融合的业务特点，有针对性地从“云（网）管端”提出新型的网络安全保障能力建设框架，以便融媒体中心更好地应对新风险和新问题，更好地保障融媒体中心的安全，发挥融媒体中心的传播效能。

1.4 启明星辰构建“安全中台” 迎接产业互联网安全升级

随着云计算、大数据、物联网等新技术的迅猛发展，当前 “烟囱式”的、相对独立的安全保障模式遇到很大的挑战，“安全中台”服务架构的应运而生。“中台”早期是由美军的作战体系演化而来的，技术上“中台”主要是指学习这种高效、灵活和强大的指挥作战体系。当前数据中台、业务中台纷纷兴起，成为数据与业务的强大支撑。

安全中台的核心目标是提升安全效能、数据化运营服务、更好地保障客户业务持续、规模化地创新发展。利用安全中台一方面可以有效的整合已建设的各种安全能力，另一方面也可以真正做到自身安全能力与业务需求的持续对接，更好地服务于产业互联网。

安全中台包括了安全数据中台及安全业务中台。安全数据中台利用数据技术，对海量的各种安全日志、安全事件、流量数据等安全数据进行采集、计算、存储、加工，同时统一标准和口径。安全数据中台把安全数据统一，形成标准安全数据，再进行存储，形成安全大数

据资产层，进而为客户提供高效安全服务。它是位于基础安全保障要素和安全业务应用之间的服务，其安全模型和安全能力与安全业务系统具有强关联性。安全业务中台是适应用户需求变化，满足快速推出新业务的需要，适应产业互联网和业务对安全能力和服务的各种需求。

安全中台的建立与运行需要强大的安全运营能力，启明星辰几年来持续布局的独立安全运营中心业务接入了云计算、大数据、物联网等这些与企业实际业务结合紧密的新技术，为企业级用户提供了具有集中安全监测、安全应急、态势感知、安全防护、安全事件处置能力。

2. 深信服

2.1 深信服“边云协同”方案亮相 IPF2019，加速 AI 产业智慧落地

在浪潮 IPF2019 年度盛会上，深信服为众多生态合作伙伴及媒体带来了 “边云协同，加速 AI 落地”的主题分享。

AI 的落地需要依赖边缘侧的接入感知能力，如智能终端监控、智能家电、无人汽车，在边缘侧皆需解决单个部署、多个服务、远程分布式存储、统一运管等问题。随着边缘侧的应用不断增多，如果没有合理的建设模式，将会导致大量的服务器、工控设备、网关设备堆叠在边缘侧，大大影响 AI 的计算运行速度。 深信服云计算认为，超融合架构是最适合边缘计算的基础架构形态。超融合架构基于软件定义数据中心思想，将计算、存储、网络、安全等以软件的方式部署，比传统软硬一体的模式灵活性更高，非常适合边缘计算节点需要大规模远距离部署管理的需求。

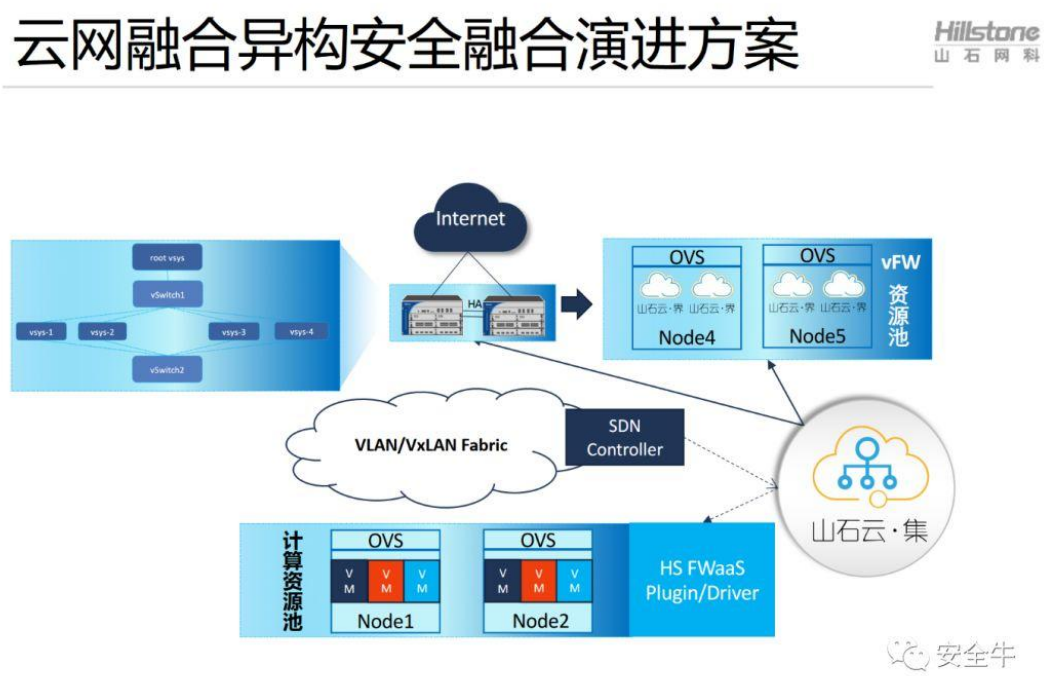
此次亮相的深信服边云协同解决方案，是基于领先的软件定义广域网、超融合、大数据等技术，提供边缘与中心协同的分布式混合云平台，实现边缘设备统一部署、统一管理、统

一策略和业务分发功能。同时，云平台集成 GPU 虚拟化、大数据平台等技术，满足中心侧数据汇聚后的大数据分析、人工智能的基础设施需求。深信服边云协同解决方案涵盖了 IaaS、PaaS、SaaS 各层面的全面协同。边缘侧 IaaS 与云端 IaaS 可实现资源协同、镜像协同、组网协同、安全协同和物联协同；边缘侧 PaaS 与云端 PaaS 可实现数据协同、智能协同、部署协同、服务协同；边缘侧 SaaS 与云端 SaaS 可实现应用层次的协同。

3. 山石网科

3.1 山石云·集 | 山石网科推出满足 NFV 标准的安全网元解决方案

在 4 月 18 日举办的 “2019 年 中国 SDN/NFV/AI 大会” 上，山石网科发布了自己的新产品 “山石云·集” ——面向 NFV 标准的安全网元解决方案。



“山石云·集” 可以理解为一个安全中间件，以软件+服务的方式将安全能力虚拟化以后，再在云以及 SDN 环境中进行相对应的部署应用。通过在云平台部署轻量级插件，运维人员可以快速通过 “山石云·集” 将软硬件的安全能力虚拟化后，与云平台进行对接。

4. 亚信

4.1 亚信安全:面向未来安全，共建 5G 之美

根据规划，2019 年下半年 5G 设备开始在国内尝试商用，将有更多的关键驱动因素进入

大众视野，而它们无疑都与网络安全息息相关。

新的信任模型

5G 网络的设计不仅提供了网络和通信服务的新模型，更实现了行业的广泛连接(如工业互联，智能交通，智能电网和远程医疗)。例如，5G 强大的网络能力将增强车辆的感知系统，使人从汽车驾驶中解放出来，道路上的所有参与者，车与车、人、交通灯、路况、云端等都会通过 5G 汇聚在一起产生新的场景。但与此同时，这些通过 5G 网络广泛连接的物联网设备不可能做到完全可信，而现有的信任模型(默认安全，不具备攻击性)显然没有能力捕捉到 5G 的这种业务演变。

新服务交付模型

涉及 5G 生态系统中的新参与者，将广泛采用云和虚拟化技术，以及 XaaS(一切即服务)的模式来降低成本，更快地部署和优化服务。但是，软件硬件分离的特点以及虚拟化网络的开放性给 NFV 带来了新的潜在安全问题。企业需要建立虚拟化和云端的安全管控平台，为资源和虚拟网络设备提供多元化的系统级防护，防止各类非法的攻击和入侵。

不断扩展的数据泄露问题

在 5G 时代，随着新的服务模式、交付模式的出现，网络和终端之中的各种漏洞将无处不在，这会产生更多的隐私泄露渠道。更重要的是，5G 系统承载的数据资产(硬件、软件、信息和收入流)由于具备更高的价值，对于不同类型的网络犯罪和网络恐怖分子攻击将更具吸引力。要保护 5G 时代的数据隐私，不仅需要逐步淘汰可疑的隔离方式、身份验证方法(例如用户名/密码)，还需要构建一个通用的认证机制和可信的运营网络。

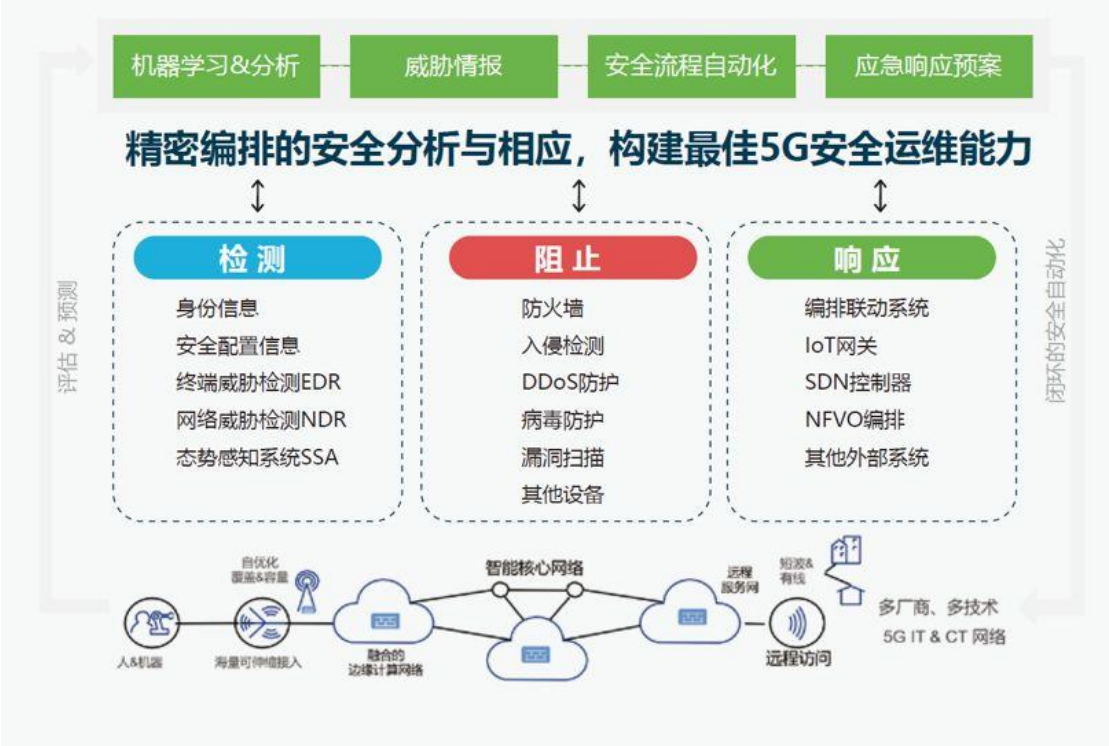
实现端到端的 5G 安全

与以往的移动通信系统相比，5G 需要满足更加多样化场景下的需求，抵御端到端的安全风险。通过整理和简化，亚信安全从设备威胁、空口威胁、无线接入威胁、后向传输威胁、5G 核心网和运维威胁、外部移动应用威胁这 6 个方面可以进行展现。

亚信安全以“安全指挥中心+态势感知平台+安全产品+安全服务”的融合，形成了业内

首个 5G 安全整体解决方案。在技术层面大量采用了机器学习、AI、大数据分析、威胁情报，以及自动化的安全流程和应急响应预案，通过精密编排的安全分析与应急响应，构建出具备“检测、阻止、响应”能力的 5G 安全运营中心。

同时，亚信安全在检测、阻止、响应层面这三个层面上，提供了完整产品链，为支持 5G 所需要的业务信任模式和业务交付模型，提供了符合软件定义安全和安全功能虚拟化需求的完整解决方案，实现抗 DDoS、IPS/IDS、IP/Domain/URL 过滤、病毒拦截等安全能力，保证切片及接入网络环境的内生性安全。在基础架构安全防护方面，亚信安全提供了统一管控本地物理、虚拟化服务器和 Docker 服务器的 DeepSecurity 产品，支持多种 SDN/NFV 方案、Docker 架构等技术为基础构建的电信云平台。另外，在 SDN 防护、网元安全防护和切片流量清洗方面，亚信安全提供了支持 ETSI 标准的 VNFSecurity 产品，可以融入 MANO 管理，形成 SDN/NFV 网络安全防护的内建能力，确保 5G 业务的安全推进。



5. 绿盟

5.1 绿盟科技发布《绿盟数据安全解决方案》

针对市场上不断出现的数据威胁乱象，绿盟科技推出全新的《数据安全解决方案》， 方案为数据安全设计了全面可信的防御体系，有效保护数据在全生命周期过程中的安全，达到合法采集、合理利用、静态可知、动态可控的防护目标。

结合客户的需求，以及对实际环境的调研了解，总结出了一套数据安全治理方法，及“知”、“识”、“控”、“察”，利用咨询服务发现数据风险，通过产品落地实现对数据的可视化监控、风险点排除，及时预警、及时阻止对数据的非法使用行为，最后对数据进行持续运营服务，让数据始终处于被监控的安全状态，当有新的业务上线时，可根据此数据治理方法快速的实现新数据的安全监控。

绿盟科技针对数据安全提出了完整的解决方案，包括数据梳理、风险分析、运维数据监管、业务数据监管、办公数据监管，以及数据的可视化分析展现，全面对数据在各种场景中的全生命周期安全进行了阐述。

客户价值：

1)满足合规要求：通过本方案的实施，可以对法规中提到的鉴别信息数据、重要个人信息、重要业务数据做到针对性的监控与保护，使企业在发现数据风险前及时做出响应，避免因数据丢失造成的危害与损失。

2)权限划定清晰：通过本方案的实施，将数据合理的进行级别划分，结合管理与业务的需要对数据的访问、使用，进行清晰的权限管控，做到权责分离，事后还可以通过审计结果明确事故责任方，避免了责任不清。

3)数据生命周期全面掌控：利用本方案对数据的生命周期中各个环节做监控，掌握数据的动态，了解数据的流向，提前对可能发生的数据泄露风险进行预警，保障数据在安全的可控范围内流转、使用与存储。

4)降低数据泄露风险：通过对数据的扫描与跟踪，利用内容识别、UEBA、机器学习等技术，及时发现数据所承载的系统、业务、网络、终端中的安全威胁，提前做好防范措施，让泄密风险看得见、使数据泄漏防得住。

5)提高数据使用者的安全意识：绿盟数据安全解决方案的应用，让数据使用者了解数据

的重要程度，规范数据使用者的操作行为，从潜意识里指导与帮助人们正确使用资源，合理利用资源，保护数据的安全。

绿盟数据安全解决方案为客户提供了全面可信的数据风险识别与防护体系，将个人隐私数据、企业敏感数据、鉴别类信息进行有效的分拣区分，从数据治理到合规监管，从及时预警到风险态势，对不同场景提供有效的数据安全保障服务。

6. 安恒

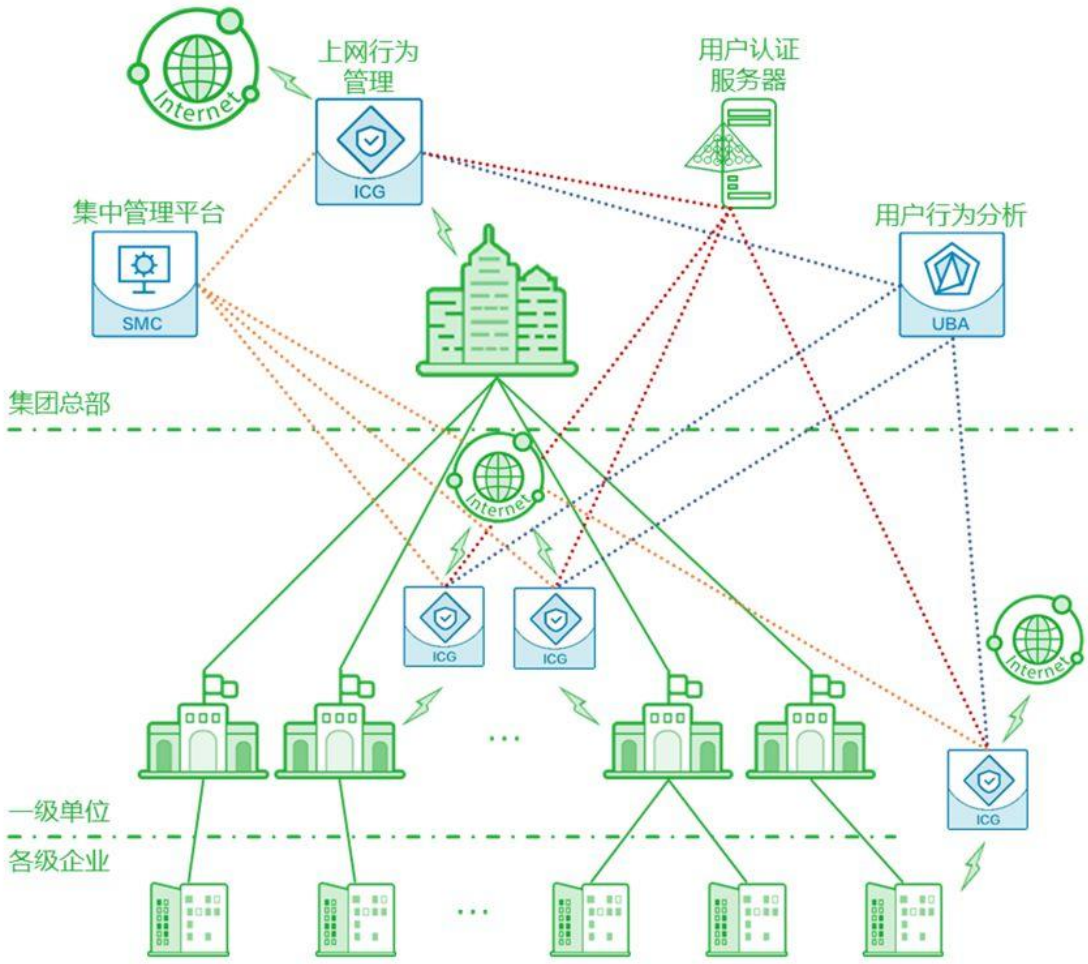
暂无消息。

7. 奇安信

7.1 奇安信上网行为管理产品持续多年领跑市场

近日，全球领先的数据分析和咨询机构 IDC 发布了 2018 年中国区“安全内容管理”市场排名。奇安信集团上网行为管理产品继续保持稳固增长，并以 13.4%的市场份额排名第二，持续多年领跑该子市场。据悉，上网行为管理产品的前身为“网康互联网控制网关（ICG）”，而网康科技作为国内“安全内容管理”领域的“老兵”，早在 2004 年就推出了国内首款上网行为管理产品。十余年来，该产品赢得了包括国家部委、大型央企、运营商、重点高校、金融机构、互联网电商、连锁机构等广大用户的信赖与好评。

奇安信协助国内某能源行业超大型企业顺利完成“全国互联网统一出口管控”项目建设。在该项目中，用户为解决其互联网出口众多导致的管控困难、边界防护薄弱问题，将其全国范围内近 200 个互联网出口收缩至十余个，利用奇安信提供的“多分支上网行为统一管控”解决方案，对集中后的十余个互联网出口实现了统筹化的上网行为管理。出口集中后，单一出口的上网人数和管控策略复杂度大幅度提升，这都是传统上网行为管理设备需要面临的巨大挑战。为此，奇安信采用基于 ATCA 分布式运算硬件架构的高性能上网行为管理设备，搭载专属优化设计的行为管理软件系统，轻松实现了 30 余万在线用户的“实名制”上网、200 余分支“策略漫游”及全网全局的“上网行为态势感知”，开创了上网行为管理产品在多分支超大型企业场景中集约化运用的先河。



另据了解，奇安信近年来积极探索上网行为大数据分析技术，其已发布的“行为感知分析系统（BAAS）”就是一款利用大数据分析技术等手段，对海量上网行为数据进行关联分析，进而实现行为建模、用户画像，最终帮助企业、高校等用户实现包括员工离职风险分析、校园网贷风险分析、违规外联分析等各类关乎用户业务安全的风险行为预警。

2019 年，上网行为管理团队将在已有基础之上，进一步扩大与奇安信集团其他优势产品的创新融合，包括与天擎、NGSOC、零信任等产品的联动。把‘数据驱动安全’理念下，各产品协同联动的价值最大化，为客户提供功能更全、性能更好、体验更佳的安全内容管理产品。”

8. 安天

8.1 安天两项目入选工信部网络安全技术应用试点示范项目

4 月 18 日，工信部网络安全管理局发布了网络安全技术应用试点示范项目公示名单，对经过专家评审的 101 个重点网络安全技术应用试点示范项目进行了公示。

安天两项目上榜，分别为：

1）安天申报的黑龙江省网信办态势感知与监测预警平台项目（第 53 项 《网络安全态势感知和应急处置平台》）。

2）与中国民航大学共同申报的《民航网络与信息安全管理平台》项目（第 73 项）。

9. Fortinet

暂无消息。

10. Checkpoint

暂无消息。

四、 容器技术及安全动态

1. Linkerd 2.3 正式发布

Linkerd 2.3 正式发布，为 Kubernetes 提供零接触、零信任网络，标志着 mTLS 已经由实验环境正式成长为一项全面支持功能，同时带来一系列重要的安全基元。最重要的是，Linkerd 2.3 在默认设置下即可在网格服务之间提供经过身份验证的保密通信能力。

保护各 Kubernetes 服务之间的通信内容，是实现零信任网络体系的重要一步。在零信任方法当中，Linkd 不再对数据中心安全边界做出种种不切实际的假设，而是将与身份验证、授权以及机密性相关的要求“落地”至各个单元。在 Kubernetes 术语当中，这意味着上述要求将运行在各集群内以验证、授权并加密对应通信内容。

实现流程描述：

1) 控制平面中附带证书颁发机制（简称为「身份」）。

2) 数据平面各代理从身份服务处接收 TLS 证书，该证书与代理所归属的 Kubernetes 服务账户绑定，且每 24 小时进行一次轮换。

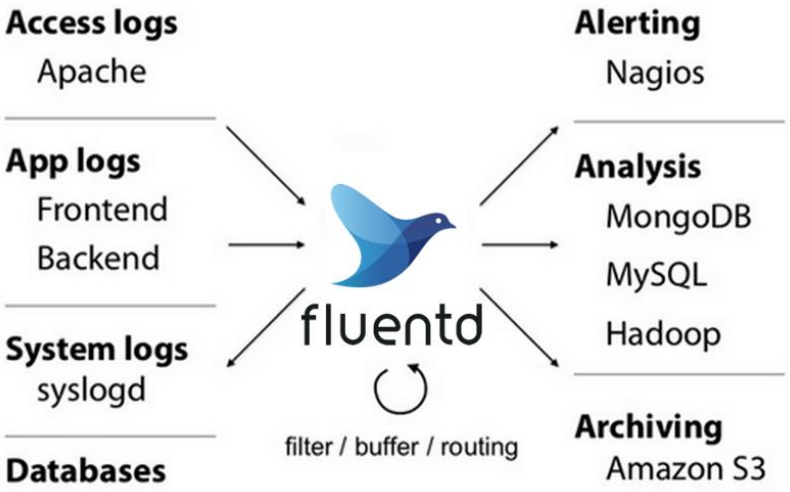
3) 数据平面各代理会自动对网格服务间的通信进行升级，从而利用证书实现 TLS 连接的验证与加密。

由于控制平面同样运行在数据平面之上，因此控制平面各组件之间的通信也将以同样的方式得到保护。

以上提到的一切都将默认启用，不需要额外配置。换言之，从 2.3 版本开始，Linkerd 将为全部网格服务之间提供经过加密以及身份验证的通信通道。虽然单凭这一次升级还无法实现 Kubernetes 中建立零信任网络的全部要求，但这仍然是一次重要的开端与尝试。

2. Fluentd 从 CNCF 毕业

CNCF（云原生计算基金会）在美国时间 2019 年 4 月 11 日宣布 Fluentd 正式毕业了。这是从 CNCF 毕业的第 6 个项目，之前已经毕业的项目为 Kubernetes、Prometheus、Envoy 、CoreDNS 和 containerd。



Fluentd 自 2011 年由 Treasure Data 公司的联合创始人 Sadayuki “Sada” Furuhashi 创建，作为构建统一记录层的开源数据收集器，统一记录层，统一收集采集和消费，以便更好的使用和理解数据。在 2016 年 11 月，Fluentd 也是第 6 个成为 CNCF 托管项目的。

Fluentd 可以从多种数据源采集事件，并将它写入文件，RDBMS，NoSQL，IaaS，SaaS，Hadoop 等等各类的目标地址。

3. Google 发布 Cloud Run 和 Traffic Director

在上周于旧金山举办的 Google Cloud Next 2019 大会上，Google Cloud 正式发布了 Cloud Run 和 Traffic Director。

Cloud Run 是业界第一个基于 Knative + Kubernetes + gVisor 体系的 Serverless 服务。允许开发者在完全受管理的无服务器执行环境中，运行无状态 HTTP 驱动的容器。它负责所有基础架构，涵盖配置、扩展和服务器管理，其能够在‘几秒钟内’自动向上或向下扩展、甚至将资源占用降低为零，因此用户只需为实际使用的资源而付费。Cloud Run 同时提供全托管和 GKE 两种部署模式，在全托管模式中基于 knative 在 Google 的内部实现和 gVisor 安全容器运行，GKE 模式中则完全基于开源 knative 来实现。两个 knative 实现在 API 层一致。

此外，Cloud Run 的计费模型也颇具创新性：它不是完全按照任务数和资源收费，而是将所有并发的请求算在一个计费单位内，这有望大大减低用户需要支付的成本。

Traffic Director 是一个与 AWS App Mesh 对标的 Service Mesh 产品。Traffic Director 通过 xDS 协议与数据平面的 Envoy 进行通讯，可分别与 Google Cloud 的 MIG 和 NEG 两款产品结合去提供 Service Mesh 的能力。Traffic Director 的功能与开源 Istio 项目中的 Pilot-discovery 相似，也复用了 Istio 的不少技术实现（比如，通过 iptables 完成流量透明拦截）。Traffic Director 支持全球负载均衡、集中式的集群健康检查、流量驱动的自动扩缩容等功能，帮助客户在全球部署与管理高弹性的无状态应用。

4. 开源项目 Kubecost

大多数 Kubernetes 管理工具都侧重于易用性，监控，对 pod 行为的洞察等。但是如何监控与运行 Kubernetes 相关的成本?

Kubecost 能够按照 Kubernetes 的原生 API,比如 Pod，Deployment，Service，Namespace 等概念逐层监控并详细的计算和展现出每一层上你的真实花费。更重要的是，无论你下层用的是 AWS 还是 GCP，Kubecost 内置的成本模型都可以应对自如。

如使用实时 Kubernetes 指标以及从主要云提供商上运行的集群派生的实际成本信息，以提供每个集群部署的每月成本的仪表板视图。内存，CPU，GPU 和存储的成本都由 Kubernetes 组件(容器，容器，服务，部署等)分解。

Kubecost 还可以跟踪“群集外”资源(例如 S3 存储桶)的成本，尽管目前仅限于 AWS。成本数据甚至可以共享回 Prometheus，因此可以使用数据以编程方式更改群集行为。

5. kubernetes 近期漏洞

CVE-2019-1002101 kubectl cp 漏洞

近期 kubernetes 的 kubectl cp 命令发现安全问题(CVE-2019-1002101)，该问题严重程度比较高，建议将 kubectl 升级到 Kubernetes 1.11.9,1.12.7,1.13.5 或 1.14.0 版本以解决此问题。

kubectl cp 命令允许用户在容器和主机之间复制文件，其基本原理是：

1) 在源地址将文件打包。

2) 打包输出内容作为 stream 流通过网络传递给目标地址。

3) 传递路径包括：apiserver、kubelet、runtime

4) stream 流在目的地址作为 tar 的输入，解压。

具体执行过程可以参考 kubernetes/pkg/kubectl/cmd/cp.go 文件中的 copyToPod 和 copyFromPod 两个函数。

在这个过程中，如果容器中的 tar 二进制文件是恶意的，它可以运行任何代码并输出意外的恶意结果。当调用 kubectl cp 时，攻击者可以使用它将文件写入用户计算机上的任何路径，仅受本地用户的系统权限限制。

Kube-proxy IPVS 添加 flag ipvs-strict-arp

kube-proxy 的 ipvs 模式会将 clusterIP/externalIP 等绑定到节点上名为 kube-ipvs0 的 dummy 设备，以确保节点上的 ipvs 规则可以对访问这些地址的流量作转发。

在 1.13 版本中，引入一个操作

echo 1 >/proc/sys/net/ipv4/conf/all/arp_ignore

echo 2 > /proc/sys/net/ipv4/conf/all/arp_announce

以禁止 IPVS 模式下对 kube-ipvs0 dummy 设备上绑定的 ip 的 ARP 回复，具体可参考 pr #70530，该改动是为了修复 ipvs 模式下 load banlancer 类型 service 不能正常使用的问题 (issue:#59976)。

而本次的 buf fix 则是跟前面的改动有关，因为前面的改动虽然解决了 loadbalancer 的问题，但是又引入了其他问题：有些 CNI 插件在主机和容器间的连接会用到 ARP 协议。因此我们看到有些用户升级到 1.13 后反馈下面的问题：

issue#72779：kube-proxy v1.13.0 and 1.13.1 brokes services with externalIPs

issue#71555：kube-proxy/IPVS: arpignore and arpannounce break some CNI plugins

而本 bug fix 也很简单，就是为 kube-proxy 加了一个启动参数 ipvs-strict-arp，默认为 0，即不改变节点上的 ARP 配置，如果需要改变，则设置该参数值为 1。

CVE-2019-3874

这个安全漏洞最早由红帽的工程师 Matteo Croce，Natale Vinto 和 Andrea Spagnolo 发现。当 Kubernetes 中的 Pod 以 Root 用户运行时，它可以绕过 cgroup 内存隔离，通过 SCTP 网络传输，创建一个潜在的 DoS 攻击，此问题本身与 Kubernetes 无关，但是涉及到 Kubernetes 调用的内核模块。问题的严重性被定义为中等，社区建议将 SCTP 内核模块列入黑名单来规避此问题。用户可以通过执行如下命令来测试是否会到此类攻击。

modprobe sctp; lsmod | grep sctp

用户可以通过执行如下命令来把 SCTP 列入内核模块的黑名单。

echo "install sctp /bin/true" > /etc/modprobe.d/sctp.conf

五、 安全新产品及技术

1. 国家发改委将虚拟货币”挖矿”列为淘汰类产业

4 月 8 日，国家发改委发布《产业结构调整指导目录（2019 年本，征求意见稿）》，涉及鼓励类、限制类、淘汰类三个类别的产业活动，，虚拟货币“挖矿”活动（比特币等虚拟货币的生产过程）赫然出现在淘汰类之中。

该指导目录还显示，未标淘汰期限或淘汰计划的条目为国家产业政策已明令淘汰或立即淘汰。而虚拟货币“挖矿”活动这一条没有标上“淘汰期限或淘汰计划”，侧面反应出国家产业政策鲜明态度。

摩根士丹利曾在 2018 年初给出数据，挖比特币成本大约三分之一来自电费，2018 年比特币乃至其他数字货币的挖矿用电需求将达到 120-140 万亿瓦时 （terawatt-hours），而全球电动车的能源消耗到 2025 年预计才不过 125 万亿瓦时。根据国际能源署 2015 年的数据，阿根廷全国一年的用电量也才不过 125 万亿瓦时。2018 年 10 月发表在期刊 Nature Climate Change 上的一篇论文显示，仅挖比特币一项就将导致 2033 年全球气温上升 2℃。

对于下一步的工作安排，互金整治办提出两点要求：一是积极引导辖内企业有序退出“挖

矿”业务，并请积极协调辖内有关部门，多措并举，综合采取电价、土地、税收和环保等措施，引导相关企业有序退出；并要求各地整治办于 1 月 10 日前上报目前辖内“挖矿”企业基础情况及引导退出情况。二是为及时掌握各地工作进展，要求各地整治办每月 10 日前填报辖内“挖矿”企业有关情况

2. 国家网信办启动小众即时通信工具专项整治

国家网信办发表新闻稿，宣布启动小众即时通信工具专项整治。新闻稿称：

针对即时通信工具传播违法违规信息、匿名注册、欺诈诱骗、为线下违法违规活动提供平台服务等行业乱象，国家网信办近日启动即时通信工具专项整治工作，从应用展现、服务导向、商业模式、注册机制、信息内容、群组管理等方面，对各类即时通信工具进行深入巡查和测试。首批清理关停 “比邻”“聊聊”“密语” 等 9 款传播淫秽色情信息，或为招嫖卖淫、售卖淫秽色情音视频等提供推广和平台服务的即时通信工具。关负责人表示，即时通信工具使用门槛低、用户多、传播快、隐蔽性强、管理难度大，有的即时通信工具使用者利用 “匿名注册”“阅后即焚”“私密群组” 服务开展网络诈骗、卖淫嫖娼等违法犯罪活动，有的即时通信工具运营者受利益驱使搭建私有服务器，使即时通信工具成为违法犯罪活动的组织平台，严重威胁公共安全，损害网民合法权益，社会危害大，必须依法从严处置，全方位清理。

3. 高通近 40 款芯片被曝出泄密漏洞，可窃取机密信息

英国安全业者 NCC Group 公布了藏匿在逾 40 款高通芯片的旁路漏洞，可用来窃取芯片内所储存的机密资讯，并波及采用相关芯片的 Android 装置，高通已于本月初修补了此一在去年就得知的漏洞。此一编号为 CVE-2018-11976 的漏洞，涉及高通芯片安全执行环境（Qualcomm Secure Execution Environment，QSEE）的椭圆曲线数码签章算法（Elliptic Curve Digital Signature Algorithm，ECDSA），将允许黑客推测出存放在 QSEE 中、以 ECDSA 加密的 224 位与 256 位的金钥。

NCC Group 早在去年就发现了此一漏洞，并于去年 3 月知会高通，高通则一直到今年 4 月才正式修补。根据高通所张贴的安全公告，CVE-2018-11976 属于 ECDSA 签章代码的加密问题，将会让存放在安全世界的私钥外泄至一般世界。它被高通列为重大漏洞，而且影响超过 40 款的高通芯片，可能波及多达数十亿台的 Android 手机及设备。

4. iLnkP2P 弱点暴露数百万物联网设备

一家深圳公司（该公司网站基本不更新）开发的软件 iLnkP2P 被发现存在严重安全漏洞，全世界有数百万物联网设备受到影响。

iLnkP2P 被广泛用于安全摄像头和网络摄像头、婴儿监视器、智能门铃和数字录像机，它允许用户从任何地方简单快捷的访问设备。用户只需要下载移动应用，扫描设备上的二维码或六位数 ID。

安全研究员 Paul Marrapese 发现， iLnkP2P 设备没有提供任何验证或加密，很容易被枚举破解，允许攻击者与这些联网设备建立直接连接，绕过防火墙的限制。

全世界有 200 多万物联网设备存在该漏洞，其中 39%位于中国，19%位于欧洲，还有 7%在美国。几乎半数存在漏洞的设备是海芯威视生产的，它的设备 ID 使用了前缀 FFFF、GGGG、HHHH、IIII、MMMM 和 ZZZZ。

5. 网信办等启动剑网 2019 专项整治

国家版权局、国家互联网信息办公室、工业和信息化部、公安部四部门今天宣布联合启动打击网络侵权盗版“剑网 2019”专项行动。专项行动将开展媒体融合发展版权、院线电影网络版权、流媒体软硬件版权、图片市场版权、网络重点领域版权等五方面专项整治。

此次专项行动自 4 月底开始到 10 月底结束，将开展 5 项重点整治。

一是深化媒体融合发展版权专题保护，严厉打击未经授权转载主流媒体新闻作品的侵权行为，严肃查处自媒体通过 “标题党”“洗稿” 方式剽窃、篡改、删减主流媒体新闻作品的行为，依法取缔、关闭一批非法新闻网站（网站频道）及微博账号、微信公众号、头条号、百家号等互联网用户公众账号。

第二方面内容为严格院线电影网络版权专项整治。严厉打击影院偷拍盗录及通过网盘分享、微博微信、淘宝等渠道传播盗版影视作品的行为，规范点播影院、点播院线在放映、发行活动中的版权秩序，大力整治通过将服务器设在境外传播盗版影视作品的非法活动。

第三方面内容为加强流媒体软硬件版权重点监管。严厉打击 IPTV、OTT 及各类智能终端等流媒体硬件和各种流媒体软件、聚合类软件非法传播他人作品的行为，严厉打击通过电商平台销售各种破解版、越狱版 OTT 产品的行为。

第四方面内容为规范图片市场版权保护运营秩序。严厉查处图片公司通过假冒授权、虚

假授权等方式非法传播他人作品的侵权行为，着力整治图片公司在版权经营活动中存在的权属不清、滥用权利、不正当维权等违法违规行为，推动相关企业合理合法维权，构建健康有序的图片市场版权秩序。

第五方面内容为巩固网络重点领域版权治理成果。对短视频、有声读物、知识分享、网络直播等平台继续强化版权治理，巩固网络影视、音乐、文学、动漫、应用商店、网盘等领域取得的治理成果。

6. 研究人员开发新方法来检测隐藏在硬件组件中的恶意软件

北卡罗来纳州立大学和德克萨斯大学奥斯汀分校的研究人员已经开发出一种可靠的识别潜入硬件固件中的恶意代码的方法。通过测量系统及其中每个组件的功耗，可以确定存在恶意软件的类型。研究由洛克希德马丁公司和国家科学基金会赞助。

微架构攻击的本质使它们很难被发现，但研究人员找到了一种方法来检测它们。物联网设备和工业嵌入式系统是重要的用例，这多这种设备没有操作系统，并且仅执行存储在非易失性存储器的一小部分机器代码。在部署到现实世界的大多数嵌入式系统中，防病毒软件甚至都不实用。

监控电源使用本身并不是一个新概念，但是能够与各种系统一起工作的即插即用解决方案的想法很有趣。唯一需要注意的是，写得非常仔细的恶意软件可以尝试表现出正常的功耗。在这些情况下，有时研究人员的工具无法检测到恶意软件的存在。然而，恶意软件窃取数据的速度会减慢 86%至 97%，这对善于掩盖其踪迹的黑客来说是一个重大损失。

六、 网络安全投融资、收购事件

1. 收购

1.1 Symphony Technology Group 完成对 RedSeal 的收购

4 月 10 日，Symphony Technology Group 完成对 RedSeal 的收购，收购价未公开。STG 隶属于 Palo Alto，Palo Alto 是全球网络安全行业的领导厂商。RedSeal 旨在开发安全风险管理(SRM)软件和解决方案，帮助企业消除网络威胁。

2. 投融资

2.1 Aqua Security 获 6200 万美元 C 轮融资

4 月 3 日，Aqua Security 从 Insight Partner 和其他 4 位投资者处获得 6200 万美元的 C 轮融资。Aqua Security 是一家专注于容器安全的虚拟化安全厂商。

2.2 Bitglass 获 7000 万美元 D 轮融资

4 月 8 日，Bitglass 从 Future Fund 和其他 4 位投资者处获得 7000 万美元的 D 轮融资。Bitglass 是一家专注于 CASB 的云安全厂商，帮助企业解决业务上云和移动部署中安全问题。

2.3 VDOO 获 3200 万美元 B 轮融资

4 月 24 日，VDOO 从 83North 和其他 7 位投资者处获得 3200 万美元的 B 轮融资。VDOO 是一家使命驱动的公司，旨在改变当前物联网安全局面。