国内外云计算+安全动态报告

2019 年第 1 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 推出多项新产品及功能，正式发布 Amazon DocumentDB，推出全新 Amazon DynamoDB 密钥诊断库，同时多个产品提供新支持，AWS Database Migration Service 现在支持 Amazon DocumentDB，AWS Device Farm 现在支持 Appium Node.js 和 Appium Ruby，AWS Storage Gateway 集成 AWS Backup，AWS Glue 推出 Python Shell 作业以及 AWS IoT Core 将自定义身份验证支持扩展；VMware 将其 AWS 云服务扩展到伦敦；BigCommerce 迁移到 Google 云服务平台以提高 SaaS 速度；连锁超市艾伯森与微软签 Azure 云业务大单；阿里云正式开源实时计算平台；腾讯加速推进 IPv6 QQ、微信将完成 IPv6 技术升级。

开源云方面，启明星辰增资 EasyStack 实践云安全；九州云荣膺“iTech2018“两大奖项。

云安全厂商方面，启明星辰集团成为北京大数据行动计划首批合作单位、荣获“工业信息安全产业发展联盟优秀成员单位”、“国家网络与信息安全信息通报中心优秀技术支持单位“、”国家重大活动网络安全保卫技术支持单位”等称号，并推出视频数据防泄露解决方案；深信服获可信云•SD-WAN 解决方案产品型认证；山石网科提出智慧医院网络安全建设新思路；亚信安全移动虚拟化系统中标建设银行移动 APP 与数据安全防护项目；绿盟推出视频安全态势感知平台；安恒天池云安全管理平台入选为浙江省第二批行业云应用示范平台；360 企业安全与扬州市共建电子政务云安全服务示范基地；安天参研相关项目获国家科学技术进步二等奖；CheckPoint 发表第六代网络安全构想，提出纳米安全策略。

容器动态方面，CoreDNS 从 CNCF 正式毕业；OpenShift 推出 Kubernetes Federation V2 预览版，实现多集群负载均衡，避免单集群故障；造成巨大损失；通过可访问和使用多集群的混合云解决方案避免提供商锁定；RancherOS v1.5.0 发布，大幅提升启动性能，支持磁盘加密、wifi、4G、和 Hyper-V；Istio 1.1 将拥抱 NFV，支持多网络平面；Intel 推出开源版 Nauta，可定义和安排容器化深度学习实验。

安全新技术方面， 政府发力网络安全，越南网络安全新法生效责令互联网公司删除“有毒”内容，《网络空间安全工程技术人才培养体系指南（1.0 版）》现可下载，四部委联合开展“App 违法违规收集使用个人信息专项治理”；多家厂商推出新安全防御能力，微软推出全新的 Microsoft 365 安全性和合规性软件包，Adobe 修复了 Experience Manager 中可能导致信息泄露的漏洞；同时，NSA 宣布开源 GHIDRA 逆向工程工具，USB-C 接口将可加入认证协定，对抗恶意 USB 设备。

网络安全投融资方面，分别发生 1 起收购和 1 起融资事件。致力于研究 SAP 系统安全问题的安全厂商 Onapsis 完成对为 SAP 系统安全、合规和质量提供解决方案的供应商 Virtual Forge 的收购。云上认证和接入解决方案公司 OneLogin 获得 1000 万美元的 D 轮融资。

2019 年 1 月 30 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 云安全动态

1.1 Amazon DocumentDB 正式发布

1 月 9 日消息，Amazon DocumentDB（兼容 MongoDB）是快速、可扩展、高度可用且完全托管的文件数据库服务，支持 MongoDB 工作负载。开发人员可以使用相同的 MongoDB 应用程序代码、驱动程序和工具来运行、管理和扩展 Amazon DocumentDB 上的工作负载，并获得改进的性能、可扩展性和可用性，而无需费心管理底层基础设施。用户可以使用 AWS Database Migration Service (DMS) 轻松地将本地或 Amazon EC2 上的 MongoDB 数据库免费迁移到 Amazon DocumentDB（每个实例需要六个月），并且几乎不会出现停机。使用 Amazon DocumentDB 无需前期投资，而用户只需为使用的容量付费。

1.2 AWS Database Migration Service 现在支持 Amazon DocumentDB

1 月 9 日，AWS Database Migration Service (AWS DMS) 扩展了功能，增加了对 Amazon DocumentDB（兼容 MongoDB）目标的支持。现在，用户可以使用 DMS 实时从 MongoDB 副本集、分区集群或任何 AWS DMS 支持的源（包括 Amazon Aurora、PostgreSQL、MySQL、MariaDB、Oracle、SAP ASE 和 Microsoft SQL Server 数据库）迁移到 Amazon DocumentDB，并且停机时间最短。

1.3 AWS Device Farm 现在支持 Appium Node.js 和 Appium Ruby

1 月 10 日，用户现在可以针对 AWS Device Farm 上的本机、混合和基于浏览器的应用程序运行采用 Ruby 或 Node.js 编写的 Appium 测试。Device Farm 支持采用任何 JavaScript 和 Ruby 框架（如 Mocha 和 RSpec）编写的测试。用户还可以指定项目所需的依赖项，以及要在测试执行期间运行的确切命令，以确保测试的运行方式与在本地环境中的运行方式完全相同。

AWS Device Farm 是一种应用程序测试服务，可让用户在多个真实设备上运行自动测试并与 Android、iOS 和 Web 应用程序进行交互。Device Farm 支持运行采用大多数流行

测试框架（包括 Espresso、XCTest、Appium Python 和 Appium Java）编写的自动测试。从现在开始，用户可以使用 Device Farm 执行针对真实设备采用 Appium Node.js 和 Appium Ruby 编写的测试。 用户可以通过简单的配置文件使用这些框架自定义测试过程中的任何步骤。

1.4 AWS Storage Gateway 集成 AWS Backup

1 月 16 日，现在可以使用 AWS Backup 自动化和集中式备份服务来保护使用 AWS Storage Gateway 服务的块存储选项卷网关存储的卷。通过 AWS Backup，可以为卷网关卷配置备份，实现备份计划自动化，设置保留策略，监控备份并还原活动。

AWS Backup 可提供完全管理的基于策略的备份解决方案，从而消除了自定义解决方案或手动流程需求，保护网关卷，简化管理并帮助您满足业务和合规需求。通过 AWS Backup 管理的卷备份存储为 Amazon EBS 快照，易于还原到任何卷网关或 Amazon EBS 卷，用于 Amazon EC2。

1.5 AWS IoT Core 将自定义身份验证支持扩展

1 月 18 日，AWS IoT Core 将自定义身份验证功能支持扩展到适用于 iOS 的 AWS 移动软件开发工具包现在，用户可以重新使用已投入的现有身份验证机制，将 iOS 设备连接到 AWS IoT Core。用户可以利用不记名令牌身份验证策略（如 OAuth）连接到 AWS IoT Core，而不是依赖 X.509 证书作为连接 iOS 设备的唯一方法。

自定义身份验证适用于其他 AWS IoT 软件开发工具包，iOS 软件开发工具包的实施与现有用法一致。

1.6 推出全新 Amazon DynamoDB 密钥诊断库

1 月 21 日，AWS Cloud9 是一个基于云的集成开发环境 (IDE)，在该环境中，用户只需一个浏览器即可编写、运行和调试代码。现在，AWS Cloud9 已经与 AWS CloudTrail 进行了集成，让用户可以更轻松地跟踪对 Cloud9 所做的更改。CloudTrail 会捕获这些更改，并将日志文件传送到指定的 Amazon S3 存储桶，以便让用户了解 Cloud9 环境的创建和删除。

用户现在只需点击两下鼠标，即可在 AWS 管理控制台中打开 AWS CloudTrail

1.7 AWS Glue 推出 Python Shell 作业

1 月 22 日，现在可以在 AWS Glue 中使用 Python 脚本来运行中小型常规任务，这些任务通常是 ETL（提取、转换和加载）工作流的一部分。之前，AWS Glue 中只有在无服

务器 Apache Spark 环境中运行的作业。现在，用户可以使用 Python Shell 作业向 Amazon Redshift、Amazon Athena 或 Amazon EMR 等服务提交 SQL 查询，或者运行机器学习和科学分析。

AWS Glue 中的 Python Shell 作业不仅支持与 Python 2.7 兼容的脚本，还预装了 Boto3、NumPy、SciPy 和 Pandas 等库。用户可以使用 1 个 DPU（数据处理单元）或 0.0625 个 DPU（即 1/16 个 DPU）运行 Python Shell 作业。一个 DPU 提供的处理能力由 4 个 vCPU 和 16GB 内存组成。

2. VMWare 云安全动态

2.1 VMware 将其 AWS 云服务扩展到伦敦

1 月 14 日消息，AWS 上的 VMware Cloud 正在穿越池塘前往伦敦。首先，该软件供应商宣布，允许客户在亚马逊网络服务公共云中运行其软件的裸机云平台现已在欧洲上市。

这对于 VMware 的国际客户非常有用，他们可能希望将计算工作量放在离家更近的地方或美国以外的地方。这也预示着在将数据保存在特定辖区的情况下，公司服务进一步扩展到其他地区的时间越来越多。在世界各主要市场都很重要。

此举是在 VMware 宣布其在拉斯维加斯举行的 VMworld 大会上全面推出其云服务后不到六个月。

除了地理扩张，VMware 还宣布了其 AWS 云服务的合作伙伴计划。这意味着托管服务提供商等第三方公司可以开发围绕在 AWS 上部署 VMware Cloud 的技能，然后使用它来帮助企业迁移和运行其工作负载。这已经可以通过现有的 VMware 合作伙伴网络获得，其中

包括大量帮助销售现有 VMware 软件和服务的公司。

VMware 公司 AWS 产品的扩展是该公司今天发布的更多公告的一部分，因为它推出了几款新产品，包括日志智能服务，该服务适用于私有数据中心和 AWS 上的 VMware Cloud，可帮助管理员进行异常检测和分析。潜在的问题。

VMware 还更新了其 Cost Insight 服务，以便为客户提供有关他们在 AWS 上将其应用程序迁移到 VMware Cloud 所需支付的费用的详细信息。管理云迁移的价格标签对 CIO 和财务领导者来说非常重要，因此该计划可以为那些考虑采取暴跌的人增添信心。

3. GOOGLE 云动态

3.1 BigCommerce 迁移到 Google 云服务平台以提高 SaaS 速度

1 月 24 日消息，电子商务科技公司 BigCommerce 于近日宣布，它已将其基础设施迁移到谷歌云平台（GCP），标志着谷歌在云服务业务上的胜利。对于电子商务 SaaS 提供商 BigCommerce 来说，转向 GCP 是为加速和改善对国际客户的支持需要。

BigCommerce 的首席技术官 Brian Dhatt 表示，Google 的网络性能使其云服务优于其他托管服务提供商。Dhatt 说，“迁移到谷歌云是由我们和他们的客户所在地决定的。商家希望尽可能接近他们的消费者，谷歌是唯一一家拥有自己的国际光纤和海底电缆网络的托管服务提供商。因此，性能是竞争优势，因为 Google 背后的物理基础设施、网络更优越”。

Dhatt 表示，自去年 4 月启动该项目以来，BigCommerce 已将 90％的商家迁移到谷歌云平台 GCP，零停机时间。该公司表示，其商家的连接时间平均缩短了 81％，页面加载时间更短，转换率也有所提高。整个迁移预计将在下个月底完成。

4. 微软 Azure 云动态

4.1 连锁超市艾伯森与微软签 Azure 云业务大单

1 月 25 日消息，微软表示，与连锁超市艾伯森签署了一项为期 3 年的协议，将使用微软 Azure 作为公共云。除了部署在 Azure 上并与微软的员工签约之外，艾伯森还计划使用微软的人工智能技术，两家公司还可以在 cashierless 系统上合作。

5. 阿里云动态

5.1 阿里云正式开源实时计算平台

1 月 28 日，阿里云正式对外宣布，已开源实时计算平台 Blink，这一技术被认为是引领“下一代计算”的 “计算王牌”。

Blink 是阿里在 2015 年开始对 Flink 进行成功改造的结果。目前，阿里巴巴已经收购创办 Flink 的公司 Data Artisans。Flink 虽然代表了一种全新的计算方式，但早期只适用于小流量互联网场景的数据处理，并未被大范围看好。

阿里引入并进行改造后，将其计算能力推向了巅峰，可以作为企业应对大规模数据处理的解决方案。现在 Blink 已经将计算延迟降低到人类无法感知的毫秒级：浏览网页的时候，你只是眨了一下眼睛，处理的信息已经刷新 17 亿次。

据悉，在阿里集团内部，目前全部核心业务已经用上 Blink。

关于这次开源，Data Artisans 的 CTO Stephan Ewen 兴奋地表示：“阿里巴巴是 Flink 最大的贡献者之一，很高兴阿里能将内部优化的 Flink 版本开源给社区，让开发者享受到更先进的计算能力。”

阿里巴巴集团副总裁周靖人说：“我们一直密切关注并积极参与最前沿的计算技术。Flink 过去几年在计算领域获得了很大成功，阿里、Uber、Netflix 等都是 Flink 的受益者，我们希望通过这次开源进一步服务整个社会。”

2004 年，谷歌曾开启大数据离线计算的时代，但伴随着大数据、人工智能、物联网、边缘计算等新技术的兴起，有延迟的计算结果已经远远不能满足开发者尤其是企业的需要。

以 Flink 为代表的一系列实时计算技术得到了更多关注，在过去几年 Flink 的采用量增长了 125%。阿里巴巴、腾讯、美团、滴滴、Netflix、Uber 等大型公司都已经陆续采用 Flink 技术。

实时计算正处于上升期，除了 Flink 之外还有 Spark、Storm 等多个技术流派，谷歌、英特尔、IBM 等全球科技公司都在积极布局。

6. 腾讯云动态

6.1 腾讯加速推进 IPv6 QQ、微信将完成 IPv6 技术升级

1 月 7 日消息，在腾讯云 IPv6 智联升级产品今天的发布会上，腾讯全面展示了推进 IPv6 的最新进展和未来规划。据介绍，目前，腾讯网、腾讯游戏、腾讯视频、QQ 浏览器等腾讯旗下核心产品已全面支持 IPv6 上线，两大国民级应用 QQ 和微信也即将完成 IPv6 技术升级。2019 年，腾讯将成为全球拥有最多 IPv6 用户的企业之一。

基于在 IPv6 上的技术储备，腾讯云也将通过灵活过渡和智能双栈的 IPv6 智联升级解决方案，帮助企业用户分钟级平滑升级到 IPv6 网络。

工信部信息通信发展司副处长梅杰表示，推进 IPv6 规模部署是一项庞大、艰巨的系统工程。腾讯作为国内 IPv6 的实践先行者，率先完成了一批典型互联网应用的 IPv6 升级，期待腾讯云全生态 IPv6 解决方案，引导和支撑更多互联网应用和用户向 IPv6 迁移。

腾讯云副总裁陈平表示，IPv6 是产业互联网的核心要素，腾讯全生态体系都将积极拥抱 IPv6，并会持续开放 IPv6 技术积累给产业生态，推动 IPv6 和产业互联网的协同发展。

7. 华为云动态

暂无消息。

二、 开源云动态

1. Openstack 动态

暂无消息。

2. Easystack 动态

2.1 启明星辰增资 EasyStack 实践云安全

2019 年 1 月 18 日，启明星辰发布公告，为加强在信息安全方向布局的发展战略，决定由全资子公司向易捷思达(EasyStack)增资 5,000 万元，增资完成后，公司将合计持有易捷思达 5.858%的股权。

公司增资易捷思达，意在加强云安全，布局云计算。一方面，启明星辰将利用易捷思达在云方面的积累，结合公司自身安全的能力，大力实践云安全。另一方面，公司提出安全独立运营、安全技术的互联网+(针对云计算、物联网、大数据、移动互联等)、人工智能化的的战略，该战略与云计算密不可分；公司也将积极布局云计算行业。云计算将成为标配的基础设施已经成为共识，安全仅是其中一部分，公司将以安全为核心拓展 AI、云等基础领域。本次公司可以将其在信息安全技术及市场资源方面的优势与易捷思达在云计算及超融合领域的优势相互融合，达成强强联合、优势互补的目的。

3. 99CLOUD（九州云）动态

3.1 九州云荣膺“iTech2018“两大奖项

1 月 25 日消息，在国家信息化专家委员会的指导下，由《中国信息化》杂志社联合华信研究院信息化与信息安全研究所主办的“iTech2018”年度盛典榜单正式出炉，凭借自身对开源技术的敏锐洞察力和研发能力，以及对行业应用需求的精准把握力和实践能力，九州云荣获 iTech2018“年度创新企业”奖和“年度明星产品”奖。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰集团成为北京大数据行动计划首批合作单位

1 月 23 日，北京市经济和信息化局开展了北京大数据行动计划首批数据合作单位签约仪式，与启明星辰集团等 18 家社会机构（或其代表主体）在北京城市副中心签署数据合作框架协议，启明星辰信息技术集团股份有限公司总裁严立应邀出席并签署合作协议。

北京大数据行动计划于 2018 年正式启动，是北京市深入贯彻落实党中央、国务院关于推动大数据发展决策部署的重大举措，计划通过若干个三年计划的滚动实施，建成完备的大数据产业生态体系，使北京市大数据整体发展水平达到国际领先。

启明星辰信息技术集团股份有限公司总裁严立表示，集团成功入选首批 18 家北京大数据行动计划名单，是国家对集团数据安全保障服务与独立安全运营战略布局的认可和鼓励。数据安全需要连同网络安全、系统安全、业务安全等多重因素共同保障，集团将为用户完善数据的安全汇聚和共享，持续提供数据安全解决方案与保障服务，并通过独立安全运营中心以专业安全视角平衡用户方与建设方信息化和安全建设，助力北京市网络安全与信息化建设。作为专业的安全厂商，集团从第三方专业安全视角介入网络安全业务设计，可以更好的平衡信息化建设和风险的防控。从 2017 年 12 月成都安全运营中心建立，到 2018 年 11 月青海省

运营中心落成，不到一年的时间，启明星辰集团建成或筹划建设的运营中心近 20 个，安全运营业务完全得到了各地区用户的认可。

1.2 启明星辰集团获评工业信息安全产业发展联盟优秀成员单位

1 月 18 日，2018 年度工业信息安全产业发展联盟（以下简称“联盟”）年会在北京召开。启明星辰集团作为联盟成员，一直以来积极参与联盟建设工作，得到了联盟和成员单位的认可。在本次大会上，启明星辰集团荣获“2018 年度联盟优秀成员单位”和“第一届工业信息安全应急服务支撑单位”。

会上，工业和信息化部信息化和软件服务业司副司长董大健代表信息化和软件服务业司致辞，他指出在下一步的工作中，希望联盟继续发挥好桥梁纽带作用，加强协同联动，增进政企沟通与信息共享。同时，希望工控企业进一步落实企业主体责任，建立工控安全责任制；希望工控企业、安全厂商、科研机构加大对工业信息安全基础技术、关键共性技术和前沿技术的研发力度，重点发展一批高端产品，形成具有市场竞争力的产品体系。

作为信息安全产业领军企业，启明星辰集团凭借在网络安全基础研究和技术服务网络的优势，与行业用户携手深入工控业务场景，开展行业针对性安全研究，根据新的用户场景和需求研发新的技术和产品。同时，积极响应网络强国建设号召，参与国家和行业工控安全标准编制，开展产学研用协同联动推进国内用户在工控安全领域建设的稳步提升与创新。并且通过长期在工业领域耕耘，启明星辰已在石油石化、电力、煤炭、轨道交通、烟草、军队军工、先进制造等行业积累了大量实践经验，对行业应用的实际安全问题和需求有较为深刻的理解和实践，具备完整的工控安全产品体系和成熟的行业工控安全解决方案。未来，启明星

辰集团将继续支持联盟工作，与业界同仁一起携手构建开放、协作、共享、互联的工业互联网安全新业态，共同保障国家基础设施和国计民生生产领域中的工业互联网安全，实现信息化时代的国泰民安。

1.3 启明星辰荣获 2018 年度“优秀技术支持单位“、”国家重大活动网络安全保卫技术支持单位”称号

1 月 10 日，由公安部第十一局、国家网络与信息安全信息通报中心主办的“国家网络与信息安全信息通报机制和国家重大活动网络安全保卫技术支持单位 2018 年度工作总结及表彰会议”在北京召开。启明星辰荣获国家网络与信息安全信息通报中心“优秀技术支持单位”及“国家重大活动网络安全保卫技术支持单位”称号。

作为网络安全领军企业，启明星辰凭借自身优势及经验积累，在信息通报、重大会议安保等工作提供技术全力保障。自 2016 年通报平台开通以来，启明星辰作为技术支持单位一直为通报中心提供数据源，2018 年通报平台升级，在这一年中，启明星辰提供了系统漏洞、软件漏洞、手机应用漏洞等。除了通报平台以外，通过通报中心邮箱，及时提供了安全事件文章，包括预警、研判与分析各类型题材。

近年来，启明星辰通过不断的技术积累与自主创新，先后全面出色完成北京 2008 年奥运会、2010 年上海世博会、2010 年广州亚运会、2012 年亚欧博览会、2014 年 APEC 大会、2016 年 G20 杭州峰会、2017 年一带一路峰会、2018 年青岛上合峰会、2018 年上海进博会以及嫦娥号、天宫号、玉兔号等众多国家级重大安保项目，成为国家网络安全发展中不可或缺的主力军，为国家网络安全保驾护航。

1.4 启明星辰推出视频数据防泄露解决方案

近年来，随着平安城市、雪亮工程等项目的开展，随处可见的交通道路监控、繁华地段的电子眼监控，给非法份子带来有力震慑的同时，也因不断出现的公共视频图像信息泄露事件（个人酒店开房监控录像、交通违法监控照片泄露等），一次次的撞击着社会大众的敏感神经、为社会的稳定带来极大的安全隐患。

启明星辰基于对公共视频图像信息泄露事件的分析了解到， 视频监控管理终端，一直是公共安全视频监控网络安全建设管理过程中的薄弱环节，进而导致了手机拍屏、非法外联、外带终端非法接入等违规行为的发生。基于此，启明星辰提出了“接入终端要准入，入网终端管得住，安全管控要主动，泄露事件可追溯”的视频图像信息防泄露防护方针，从事前预防、事中管控、事后追溯全过程提供视频图像信息防泄露解决方案，保护大众隐私，守护视频数据安全。

视频数据防泄露方案 10 大安全防护维度：

1） 身份合法、终端合规人员才能入网，非法人员“进不来”；

2） 防止人员私接网络、U 盘、WIFI 设备，非法设备“用不了”；

3） 只有经过认证人员才能拷贝视频文件，视频文件“管得住”；

4） 使用点阵水印对视频内容进行保护，视频内容“窃不到”；

5） 在视频文件外送时添加水印标记，视频流向“有痕迹”；

6） 视频文件所有拷贝行为详细记录，视频泄露“赖不掉”；

7） 终端电脑所有使用行为均有记录，非法操作“可发现”

8） 控制终端应用程序使用和安装，非法软件“装不上”；

9） 通过终端可视化平台直观运维，安全状态“看得到”；

10）具备分级或者多级管理功能，安装防护“统一化”。

2. 深信服

2.1 深信服获可信云•SD-WAN 解决方案产品型认证

1 月 10 日，2019 云管和云网大会在北京举办。深信服安全 SD-WAN2.0 凭借其立体安全、易部署易运维、智能选路&加速特性，获得由中国信通院颁发的《可信云•SD-WAN 解决方案评估证书》，成为国内首家 SD-WAN 解决方案产品型认证厂商。

SD-WAN 四大核心客户价值在于：分支安全合规、提高访问体验、降低组网成本、简化运维。本次参与认证评估的深信服安全 SD-WAN 2.0（Software-Defined WAN v2.0）解决方案，通过其四大核心能力帮助企业提速降费：

□ 易部署上线

通过邮件开局方式，实现分钟级快速部署上线分支设备。多分支 VPN 端对端配置复杂，通过 AUTO VPN 秒级下发 VPN，快速互联互通。

□ 可视化运维

在网络运维阶段，通过集中管理平台构建了广域网运营中心，以地图和拓扑的形式，展现分支的在线离线、资源负载度、健康度等信息，可以批量编辑和下发管控策略到全网设备。同时实现了 SD-WAN 拓扑健康可视化，可以看到每个虚拟隧道的丢包、时延、繁忙度，实现真正全网可视可控。

□ 基于加速的智能选路

在体验保障方面，基于加速智能选路，提供广域网优化、智能应用选路策略（如指定线路、剩余带宽、包负载）保障核心应用的访问体验，提升 300%传输速度、80%线路利用率。

□ 立体安全防护

不仅可以通过 SD-WAN 分支端设备（UCPE）的虚拟探针和防火墙等安全模块收集安全线索，而且结合着外部威胁情报，通过安全大脑的大数据分析，可以真正地打造包含广域网互联在内的安全防护体系。

目前，深信服作为国内率先推出的安全 SD-WAN 2.0 方案的厂商，已经将该方案全球范围进行了一定规模商用，用户群体包括政企业、金融、政府、连锁零售、跨国企业等，根据用户不同广域网建设需求适配高性价比的解决方案。

3. 山石网科

3.1 山石网科智慧医院网络安全建设新思路

1 月 19 日，以"信息化推进医疗核心制度完善，建立现代化管理医院"为主题的汇溪湖 2019 医院信息化论坛成功召开。在"医院信息安全建设"分论坛上，山石网科发表了主题为"智慧医院网络安全建设的思考"的演讲。

在如火如荼的医院信息化发展的背后，安全形势日趋严峻：攻击类型增多、攻击方法传播更快、院内院外互联互通导致攻击面不断扩大、医疗业务云化颠覆传统安全理念、数据窃取事件层出不穷、监管要求升高带来的合规风险等等。山石网科创新的分布式网络侧微隔离产品山石云·格利用微隔离和可视化技术，实现云内主机间威胁检测与隔离、流量及应用可视化、攻击审计与溯源等。山石云·格集成了东西向网络安全防护所需的各种防护功能，在业务运行的过程中，对各类活动进行有效的监测，对异常的行为进行报警和记录，第一时间响应和处置，实现最小化故障影响的目的。

山石云·格可适配多种云环境，并已获得 VMware Ready 认证。作为 CSA 国际云安全联盟的成员，山石网科积极参与由 CSA 与公安三所联合组织的云计算信息安全产品认证标准制定工作。

4. 亚信

4.1 亚信安全移动虚拟化系统中标建设银行移动 APP 与数据安全防护项目

近日，中国建设银行移动 APP 及数据安全防护项目招标结果揭晓，亚信安全凭借长期服务金融行业的丰富经验和行业领先的移动安全技术能力获得中国建设银行认可，成功中标该项目。亚信安全移动虚拟化系统将为中国建设银行全行打造内部移动应用的统一管理平台，满足移动办公平台场景适应以及便捷管理的需求，实现“数据不落地”的移动安全进阶目标。

作为“科技＋金融场景应用”的重要成果，中国建设银行全力推广基于移动终端的办公应用体系，通过改善内部员工工作的移动性、便捷性，自主开发了多个 APP 应用。但是，移动应用突破了传统的网络安全防御边界，给数据安全的防御提出了极大挑战。为此，建信金融科技有限责任公司着手为全行部署新一代移动应用软件，并将安全特性作为项目招标的首位要求。

建信金融对市场上多款移动办公安全方案进行了严格测试和多方认证，最终亚信安全移动虚拟化系统脱颖而出，凭借其产品的高效应用体验、数据安全能力和合规优势，成功中标。亚信安全移动虚拟化系统，即移动应用在客户云计算中心的“云手机”上集中发布，基于虚拟移动基础架构（VMI），以创新的方式应对传统安全挑战，满足了数据不落地的要求，同时更解决了移动智能终端办公带来的安全风险高、运营成本高、开发成本高等问题，帮助客户站在更高的起点开始并加速移动化进程，有效地提升了运维能力和效率，是行业中领先的移动虚拟化平台。

5. 绿盟

5.1 绿盟推出视频安全态势感知平台

近年来，视频监控系统被广泛应用于政府、金融、交通、教育和医疗等行业。绿盟科技针对视频专网，推出安全态势感知平台解决方案。绿盟视频安全态势感知平台集全网设备自动发现、设备故障实时报警、漏洞自动探知、安全准入自动甄别、网络行为大数据分析、违规行为自动阻断等多种安全功能于一身。

绿盟视频安全态势感知平台，通过旁路部署分析引擎，分析网络中的数据流量，监控和分析网络中的异常行为。绿盟视频安全态势感知平台从资产管理、运行监测、安全控制三个维度出发，实现设备自动发现、漏洞自动探知、接入自动甄别、行为自动分析、违规自动阻断等多种安全功能。

资产管理

基于部门、安全域、设备资产等对象，从设备资产自动发现、类型型号自动识别、信息导入、版本识别、漏洞识别到安全域、部门管理，实现从点到面的全面资产管理功能。

运行监测

以流量分析为基础，强化网络行为自动分析和白名单自动识别，通过可视化方式全面展示，监测视频专网运行。

安全控制

通过非法和未知行为报警、核心数据访问审计、视频设备漏洞检测、非法接入阻断，从被动到主动两方面实现视频专网安全控制。

6. 安恒

6.1 安恒天池云安全管理平台入选为浙江省第二批行业云应用示范平台

近日，根据《浙江省深化推进“企业上云”三年行动计划（2018-2020 年）》(浙信发〔2018〕1 号)要求，浙江省经济和信息化厅对各市经信委推荐的第二批行业云应用平台进行了审核，并组织专家进行了评审，经社会公示后，确定了 10 家企业的平台为浙江省第二批行业云应用示范平台。安恒信息的“安恒天池云安全管理平台”名列其中。

此次评选的行业云应用平台，是指为特定行业提供云基础设施、云应用软件和解决方案、云应用开发和部署环境、通用模块和组件，以及运维和信息安全保障、技术支撑等产品和服务，有助于提升行业整体云化水平的专业性云服务平台。该类云应用平台应具备面向细分行业或块状经济领域、具备较强的行业覆盖能力和服务能力等特点。

安恒天池云安全管理平台为客户提供整个安全资源池的管理员视角，管理员可以实现对安全资源池的集中、统一、全面的监控与管理，同时该平台提供了丰富的拓扑、设备配置、故障告警、性能、安全、报表等网络安全管理功能，使安全管理过程标准化、流程化、规范化，极大地提高故障应急处理能力，降低人工操作和管理带来的风险，提升信息系统的管理效率和服务水平。云安全租户平台为用户提供租户管理员视角，实现了租户间的安全隔离，即租户与租户之间的安全数据完全隔离。租户可以通过管理平台管理自己所拥有的多个安全产品，实现安全产品统一认证，策略统一下发，业务安全数据统一监控。

7. 360

7.1 360 企业安全与扬州市共建电子政务云安全服务示范基地

2019 年 1 月 25 日上午，扬州市委市政府举办了云上扬州成果发布暨展示中心开馆仪式。扬州市副市长方桂林、扬州市副市长刘禹同、扬州市政府副秘书长张伟以及其他相关部门的领导、360 企业安全集团副总裁何新飞、360 企业安全集团副总裁吕韬、浪潮集团和中国电子科技集团公司第 28 研究所、国家信息中心中国智慧城市发展研究中心的相关领导出席。

在开馆仪式上，市经信委（云上办）介绍了云上扬州正式启动一年来的工作，国家信息中心现场发布了 2018 年云上扬州建设成效评价。云上扬州建设一年来，云上办统筹工作部署、强化制度落实、加快项目推进，工作成果已初显成效，建立形成了一套规范（一套项目全生命周期管理规范）、二级推进（市县两级协同推进项目落地机制）、三大创新（创新采用总集成机制，采用项目主办、项目联络员、项目秘书推进机制以及采用智慧城市建设评价机制）、四个突破（4 大基础性项目率先启动并建成）、五类提升（基础设施整合、网站整合、数据应用、民众好用政府好管、产业合作）。

会上，扬州市与 360 企业安全集团合作共建的“大数据协同安全技术国家工程实验室电子政务云安全服务示范基地”，与浪潮集团合作共建的“数字中国研究院政府数据研究中心创新实验室”等多个项目正式揭牌。在开馆仪式上，“我的扬州 App”正式上线，首期开放了与公众生活密切相关的交通出行、医保社保、公积金、生活缴费、电子卡包、旅游服务、

垃圾分类等查询和支付功能，让公众通过一部手机、一次认证即可便捷地享受各类生活服务。今后，“我的扬州 APP”将逐步接入更多服务，让公众更加充分地共享云上扬州建设带来的便利。

8. 安天

安天参研相关项目获国家科学技术进步二等奖

1 月 8 日，中共中央、国务院在北京人民大会堂隆重举行 2018 年度国家科学技术奖励大会，对为我国技术研究、技术开发、技术创新、推广应用先进科学技术成果、促进高新技术产业化，以及完成重大科学技术工程、计划等过程中做出创造性贡献的中国公民和组织授予奖励。

此次奖励大会上，由国防科技大学牵头，主要是由哈尔滨安天科技集团股份有限公司等四家单位参研的“大规模网络安全态势分析关键技术及系统 YHSAS”获国家科学技术进步奖二等奖。

编号	项目名称	主要完成人	主要完成单位
J-220-2-07	大规模网络安全态势分析关键技术及系统YHSAS	贾 焰，方滨兴，韩伟红，李爱平，周 斌，方 华，景晓军，江 荣，黄九鸣，李润恒	中国人民解放军国防科技大学，哈尔滨工业大学深圳研究生院，哈尔滨安天科技股份有限公司，任子行网络技术股份有限公司，哈尔滨工业大学

9. Fortinet

无。

10. Checkpoint

10.1 CheckPoint 发表第六代网络安全构想 提出纳米安全策略

CheckPoint 于全球年度盛会 CPX360 中，发表第六代网络安全的构想，提出纳米安全策略（NanoSecurity），可嵌入在所有装置、网络或云端服务，为未来的超级互联提供强大的保护。

CheckPoint 创办人兼执行长 GilShwed 表示，我们的任务是不断提升网络安全，确保可随时抵御所有类型的网络攻击。在第六代网路安全中，纳米级代理策略将被部署在所有装置

和云端平台上，支援与预测、侦测和预防攻击的智慧控制系统即时连接，提供从单一物联网装置到超大规模网络的全方位无缝保护，删除弱连接并保护我们的未来。

四、 容器技术及安全动态

1. CNCF 基金会宣布：CoreDNS 毕业

2019 年 1 月 24 日 - 支持 Kubernetes 和 Prometheus 等开源技术的 Cloud NativeComputingFoundation（CNCF）今天宣布，CoreDNS 成为 2019 年第一个毕业的项目，继去年 Kubernetes，Prometheus 和 Envoy 的第 4 个毕业项目。要从孵化的成熟水平升级到毕业，项目必须表现出蓬勃的采用，多样性，正式的治理过程，以及对社区可持续性和包容性的坚定承诺。

为了正式从孵化状态毕业，该项目采用了 CNCF 行为准则。 CoreDNS 团队在过去一年中还完成了 12 个版本，现在有 35 个内置插件和 15 个外部插件，其中几个为 Kubernetes 社区开发。

CoreDNS 是用 Go 编写的一种快速，灵活且现代的 DNS 服务器。它根据 Apache 许可证版本 2 获得许可，并且是完全开源的。可用于 Kubernetes 服务发现，权威 DNS 服务器，DNS 重型应用程序的本地缓存等等。每个插件链接在一起，启用其他功能，如 Prometheus 指标或开箱即用的查询重写。

除了从标准区域文件提供 DNS 之外，CoreDNS 还通过 Kubernetes 插件与 Kubernetes 集成，使用 etcd 插件直接通过 etcd，以及与许多其他后端数据提供程序集成。

由于它提供了与 Kubernetes 向后兼容、可扩展的集成，最新的 Kubernetes 版本（1.13）正式推荐 CoreDNS 作为所有部署的默认 DNS。该服务器还可用于 AWS 的混合云环境中的本机云集成，使用 AWS Route53 和 etcd - 计划尽快添加 Google Cloud DNS 支持。

该项目由 Miek Gieben 于 2016 年 3 月创建，他当时是 Google 的站点可靠性工程师。在构建 CoreDNS 时，社区考虑了其他 DNS 服务器的局限性，以创建可与多个后端通信的通用 DNS 服务器 - 如 etcd，Consul 和 Kubernetes。 CoreDNS 于 2017 年加入了 Cloud Native Sandbox，并于 2018 年 2 月成为了一个孵化项目。今天，该项目有 100 多个贡献者，16 个活跃的维护者，以及许多组织在 Kubernetes 内外使用它 - 包括 Bose，Hellofresh，Skyscanner，SoundCloud，Trainline 和 Zalando。

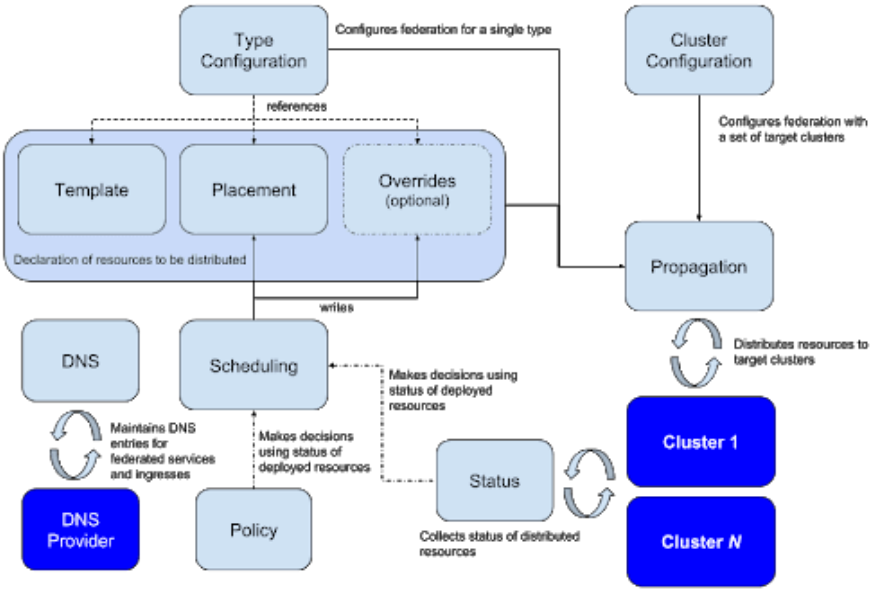
2. OpenShift 推出 Kubernetes Federation V2 预览版

随着数据中心遍布全球，用户越来越多地寻求跨区域或集群传播其应用或服务的方法。这种需求由多种用例驱动：实现多集群负载均衡，避免单集群故障造成巨大损失；通过可访问和使用多集群的混合云解决方案避免提供商锁定。

Red Hat 一直在研究 Kubernetes Multicluster Special Interest Group（SIG）和 Federation Working Group，近日发布在 OpenShift 3.11 上的 Kubernetes Federation V2 预览版本，旨在允许用户通过单一 API 将服务和工作负载部署到多个集群。

Red Hat 对多集群问题的探索出于用户需求推动，其用例包括：

- 将应用程序、服务和策略分发到多集群；
- 应用程序和服务迁移及其在集群之间的存储；
- 应用程序和服务的灾难恢复。
- 为了满足这些需求并尽可能获取广泛受众，Red Hat 在设计时考虑了模块化



3. RancherOS v1.5.0 发布

RancherOS 团队正式发布 RancherOS v1.5.0 版本。在此期间同为 Container Linux 阵营的 CoreOS 已经从红帽再入 IBM。

此次版本的重大特性更新包括：

- 启动性能提升

一直以来 RancherOS 的 initrd 一直采用 xz 格式压缩，随着 RancherOS 的体积不断增大，xz 压缩越来越影响系统启动速度。虽然 xz 格式能够带来比较小的 initrd 和 ISO， 但是我们也需要兼顾启动速度。v1.5.0 版本的 initrd 已经采用了 gzip 格式，文件体积有所增大，但是启动速度有了质的飞跃。 同时优化了 system-docker 的镜像加载和 cloud-init 的启动，对启动速度进行了深度优化。

- LUKS 磁盘加密支持

支持 LUKS，允许用户对跟磁盘分区进行加密，在一些特殊场景下增强了 RancherOS 的安全性。运行效果参考下图：

- WiFi 和 4G 支持

Intel 正在 micro PC 领域不断发力，RancherOS 被纳入其生态体系，支持了 WiFi 和 4G 网络，用户可以通过简单的 cloud-config 配置就可以开启， 带来了十分简洁的用户体验。

- Hyper-V 支持

很多社区用户一直希望能在 Hyper-V 使用 RancherOS，先前我们一直提供给用户一些 custom build 的方式来实现它，现在我们正式支持了它，并会持续维护。 无论是 docker-machine 方式还是 boot from ISO 方式均可以支持。下一个版本也会带来 RancherOS 的 Azure Cloud 支持。

- 多 docker engine 支持

这是一个很有趣的特性，目前 RancherOS 中默认拥有一个 user docker。在 v1.5.0 中，用户可以用过 ROS CLI 来创建多个 user docker engine， 并且每个 docker 拥有独立的 ROOTFS 和网络栈，并且可以在 console 很容易的切换使用任意一个 docker。

- 改善 VMware 的支持

RancherOS 的广大用户中 Vmware 是占有很大的用户群，之前版本中只针对 docker-machine 方式做了一些改善，但是很多用户还希望使用 boot from ISO 方式和 VMDK 方式， 相关的镜像也做了支持，用户可以直接下载使用它：

- ARM 的支持

由于 Rancher 和 ARM 已经开始了战略合作，。RancherOS 的 ARM 支持也是其中的一部分，原先只是对 RPi 做了支持， 现在提供 ARM 版本的 initrd 和 vmlinuz，用户可以用它们使用 iPXE 方式启动。RancherOS 依然只会对 ARM64 支持，且 v1.5.0 的 ARM 支持只是实验性质的，并不推荐应用在生产中，后续的版本将会是更稳定的。

- 更加友好的自定义

社区中越来越多的发烧友并不局限使用 RancherOS 的正式发布版本，他们会根据自己的需求修改 RancherOS，构建自己的 RancherOS。 我们提供了一些友好的编译选项，用户可以自定义自己的 RancherOS。

- 更改默认 docker engine

RancherOS 的每个版本都会有自己设定的默认 docker engine，而在用户的场景下，可能需要一个内部认可的 docker engine，且希望它是 RancherOS 默认的版本。 那么用户可以在构建时候指定 docker engine 版本，来构建自己的 RancherOS，以 docker 17.03.2 为例：

USER_DOCKER_VERSION=17.03.2 make release

- 更改默认 console

RancherOS 支持很多 console，比如 ubuntu、alpine、centos 等，由于 default console 基于 busybox，有些用户并不喜欢它，且不希望每次都去切换 console。 那么用户可以使用这种方式构建一个默认 console 是自己喜欢的版本，以 alpine console 为例：

$ OS_CONSOLE=alpine make release.

4. 拥抱 NFV，Istio 1.1 将支持多网络平面

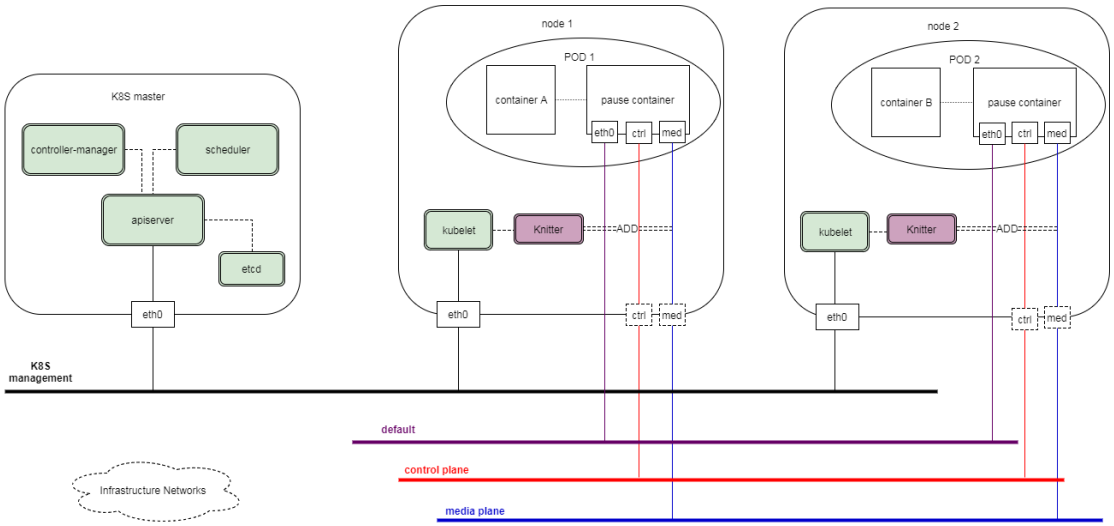
Istio 1.0 版本只支持在单个网络，即 Mesh 中的服务只能连接在一个网络上。虽然在架构设计上是开放的，但从目前的代码来看，Istio 的内部实现还是和 Kubernetes 高度集成的。由于 Kubernetes 集群中 Pod 缺省只支持一个网络接口，因此 Istio 也存在该限制并不让人意外。

随着 Kubernetes 在 NFV 领域中的逐渐应用，已经出现多个 Kubernetes 的多网络平面解决方案，Istio 也需要考虑支持多网络平面，以为 5G 的微服务化架构提供服务通讯和管控的基础设施。

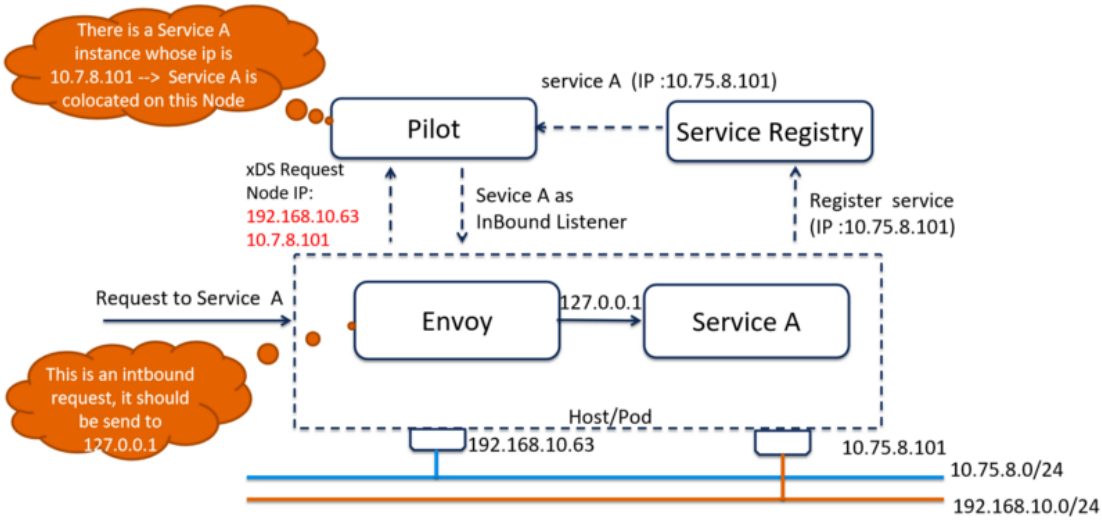
多网络平面是一个电信行业的常用术语，即将一个电信设备或者系统同时连接到多个网络上。简而言之，就是一个主机上有多个物理或者虚拟的网络接口，这些接口分别连接到不同的网络，这些网络之间一般是相互独立的。由于电信系统对可靠性的要求非常高，因此系统会通过配置多网络平面来避免不同网络流量的相互影响，提高系统的健壮性。

在电信的 NFV（网络功能虚拟化）领域中，已经有多个针对 Kubernetes 的多网络平面解决方案。其中一个 Kubernetes 推荐的方案是中兴通讯提供的 Knitter 开源实现。下图展示

了 Knitter 是如何实现 Kubernetes 的多网络平面支持的。



要支持多网络平面，Istio 需要修改 Pilot 生成 Outbound Listener 的代码实现



服务注册：

1) Envoy 所在节点存在两个网络接口，分别连接到 10.75.8.0/24 和 192.168.10.0/24 两个网络上。

2) Service A 被注册到 Service Registry 中，使用的是第二个网络接口的 IP，即 10.75.8.101。

Envoy 初始化（增加多网络平面处理逻辑）：

1) Envoy 通过 xDS 接口向 Pilot 获取配置信息。

2) Envoy 在 xDS 请求中携带所在节点上的所有网络接口的 IP，在本例中即 192.168.10.63 和 10.75.8.101。

3) Pilot 从 xDS 请求中解析出 Envoy 所在节点的所有 IP，在本例中即 192.168.10.63 和

10.75.8.101。

4) Pilot 用 Envoy 节点 IP 来和 Service Registry 中所有 Service Instance 的 IP 进行对比。

5) 由于 Service A 的注册 IP 10.75.8.101 和节点的两个 IP 之一相同，Pilot 判断该节点上存在 Service A 的 Instance，为 Service A 创建了一个 Inbound Listener。

服务请求：

1) 节点的网络接口 10.75.8.101 上收到一个来自 downstream 的请求，被重定向到 Envoy。

2) Envoy 在 15001 端口上收到该请求，要求访问 Service A。

3) Envoy 根据 Pilot 下发的配置将该请求交由在 Service A 端口的 Inbound Listener，该 Listener 将请求分发到 Service A 的 Inbound Cluster 上，对应 IP 地址为 127.0.0。1。

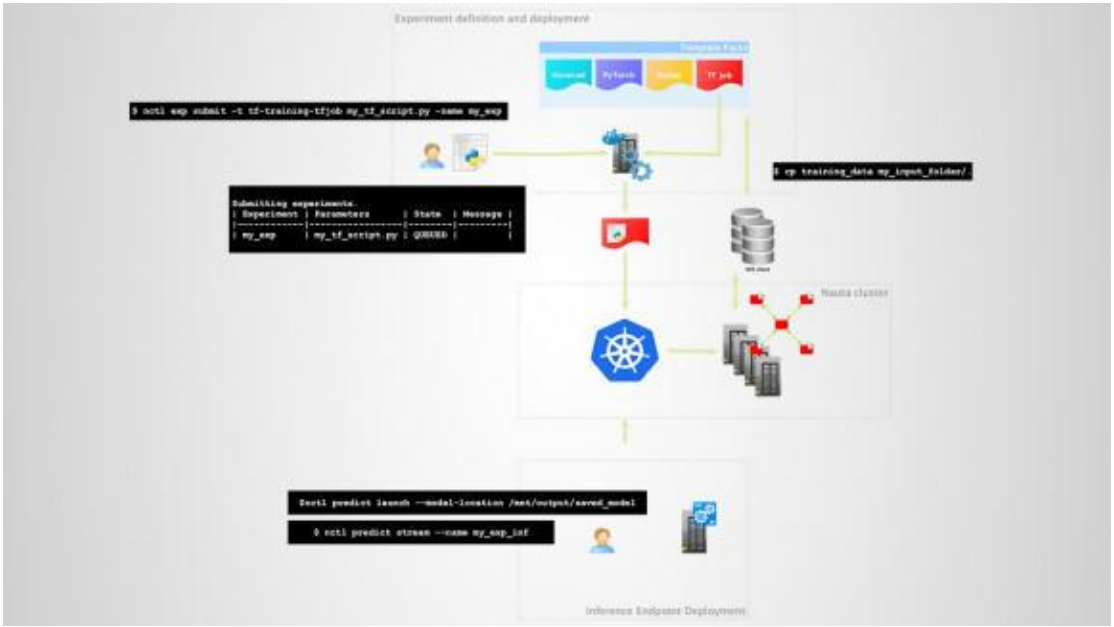
4) Envoy 将请求发送到 127.0.0.1 的 Service A 进程的服务端口上进行处理。

该修改方案已实现并提交 PR 合入到 Istio 代码中，在 1 月份发布的 Istio 1.1 Release 中将会正式支持。

5. Intel 推出开源版 Nauta，可定义和安排容器化深度学习实验

Intel 今天公布了 Nauta 的开源版本，这是一个使用 Kubernetes 或 Docker 分布在多个服务器上的深度学习平台。

该平台可以使用 MXNet、TensorFlow 和 PyTorch 等许多流行的机器学习框架，并使用可以与 Intel 的 Xeon CPU 集群协同工作的处理系统，深度学习实验的结果可以使用 TensorBoard、命令行代码或 Nauta Web 用户界面看到。



Nauta 是一个企业级的堆栈，用于需要运行深度学习工作负载来培训将部署到生产环境中的模型的团队。使用 Nauta，用户可以在单个或多个工作节点上使用 Kubernetes 定义和安排容器化深度学习实验，并检查这些实验的状态和结果，以进一步调整和运行其他实验，或准备训练模型进行部署。

Nauta 是最新发布的可以使用 Kubernetes 或 Docker 容器的工具，这种方法允许从业人员在通过内部服务器部署人工智能和在云中部署人工智能之间进行选择。

去年 11 月，谷歌引入了 Kubeflow 管道，这是一个 Kubernetes 工作流，而微软上个月在公共预览版中也引入了 Azure Kubernetes 服务。Linux 基金会的 LF 深度学习基金会去年秋天还推出了用于深度学习的 Acumos AI 工具，用于 Docker 或 Kubernetes。

五、 安全新产品及技术

1. 越南网络安全新法生效，责令互联网公司删除“有毒”内容

据法新社 1 月 1 日报道，越南网络安全新法于 1 月 1 日正式生效。该法规定，互联网公司必须删除被政府认定为“有毒”的网上内容，越南互联网用户也不得在互联网上散布反政府信息或歪曲历史。此外，脸书、谷歌等国际科技巨头要在越南开展业务必须在越南国内设立代表处，而且在越南政府要求下必须将用户数据提交给政府。

越南公安部两个月前发布法令草案，说明如何实施这项法律，且给予在越南提供网络服务的公司 12 个月的宽限期。

2. 微软推出全新的 Microsoft 365 安全性和合规性软件包

微软宣布从 2019 年 2 月 1 日开始增加两项新的合规和安全包，作为对欧盟通用数据保护法规（GDPR）等信息保护法规和当今日益增长的网络安全攻击威胁所增加的新要求的回应。新的安全性和合规性软件包旨在为尚未准备好使用 Microsoft 365 E5 软件包的企业客户提供相关支持。

Microsoft 365 是一个软件包，包括 Office 365、Windows 10 和 EMS（企业移动+安全的简称），旨在为客户提供一种轻松的方式来享受安全和管理平台，同时还能增强生产力和团队合作精神。此外，新的 Microsoft 365 身份和威胁防护软件包将多种高级威胁防护服务整合在一起，包括 Microsoft 威胁防护（Windows Defender ATP，Azure 高级威胁防护（ATP）

和 Office 365 ATP，包含威胁情报），以及 Microsoft Cloud App 安全性和 Azure Active Directory。

3. USB-C 接口将可加入认证协定，对抗恶意 USB 设备

USB 接口因为通用规格和易用的特性，成为了电子设备常见的连接端口，但也成了不法分子使坏的手段之一，以伪装成充电器和储存设备的外观来骇进电脑、手机等。USB 开发者论坛（USB-IF）就趁着 USB-C 仍然成长的阶段，为这新接口加入认证计划，希望能阻挡经物理连接的恶意攻击。

计划提议 USB-C 设备和充电器能有加密认证，让主机系统可以在连接上外接设备之时，马上通过这协定来确认「身份」，包括设备描述和其能力。这功能对于公用充电器尤其有用，这样使用者就能确保在外面充电时不会误坠陷阱，导致设备受损；公司或组织的 IT 部门也能限制电脑只可以连接经认证的 USB 设备。目前这计划只是建议，并非强制所有 USB-C 界面的设备都加入相关认证。不过 USB-IF 主席 Jeff Ravencraft 相信这将会是未来趋势，因为不光是 USB-C 界面愈变普及，大众也变得更加关注 USB 口的安全性，所以日后可能会变成标准配置啊。

4. NSA 宣布开源 GHIDRA 逆向工程工具

美国国家安全局（NSA）刚刚宣布，它将免费向公众开放其逆向工程工具 GHIDRA，源码将于今年 3 月登陆代码托管平台 GitHub 。NSA 指出，GHIDRA 框架的本质，是一款适用于 Windows、Mac 和 Linux 平台的反汇编程序。它能够将可执行文件分解为汇编代码，以进行分析。对于希望深入了解恶意软件，以查看其工作原理的安全研究人员来说，反汇编工具是相当实用的。

5.《网络空间安全工程技术人才培养体系指南（1.0 版）》现可下载

中国网络空间安全人才教育联盟作为一个全国性、行业性、非营利性的创新组织，响应党和国家号召，组织和动员全国网安领域高校、企业、事业单位和社会团体，针对人才教育、培训、认证以及就业等环节，探索科学可行的新模式。《网络空间安全工程技术人才培养体系指南（1.0 版）》就是一次研究探索和实践尝试。

“指南”首先提出了网安人才培养框架，并针对院校培养体系这一主要人才渠道，阐述了补充强化实践教学和实战能力培养环节；其次，梳理并提出了网安人才“标签化”知识技

能体系，突出以“人”为核心、以“知识技能”为业务内容，为工程技术人才培养和考核认证提供参考；最后，在分析国外发达国家网安人才认证体系建设的基础上，结合我国实情和人才渠道现实，提出我国网安人才认证体系建设思路。

6. 知名文件传输协议 SCP 被曝存在 35 年历史的安全漏洞

基于 SSH 的文件传输协议 SCP（Secure Copy Protocol）被曝存在安全漏洞。安全研究人员公布了 SCP 存在的多个漏洞，这些漏洞可以结合起来利用，分别为 CVE-2018-20685、CVE-2019-6111、CVE-2019-6109 与 CVE-2019-6110。

漏洞中最主要的地方是 SCP 客户端无法验证 SCP 服务器返回的对象是否与请求的东西一致，而该问题可以追溯到 SCP 的基础——RCP 协议（Remote file Copy Protocol），它允许服务器控制发送的文件，那么结合客户端无法验证请求与实际返回的对象是否一致这一弱点，攻击者就可以采用中间人或直接操纵 SCP 服务器的方法，覆写客户端用户的 .bash_aliases 文件，一旦用户启用 Shell，则执行文件中的恶意代码。

7. 四部委联合开展“App 违法违规收集使用个人信息专项治理”

中央网信办、工信部、公安部、市场监管总局等四部门召开新闻发布会，联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》。 《公告》指出，App 运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导 App 运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

8. Adobe 修复了 Experience Manager 中可能导致信息泄露的漏洞

近日，Adobe 发布安全更新，修复了 Experience Manager 和 Experience Manager Forms 中大量可能导致信息泄露的 XSS 漏洞。其中，影响到 Experience Manager 的主要是一个“严重”级别的存储式 XSS 漏洞和一个“中等”级别的反射型 XSS 漏洞。据报道，Adobe 暂未发现相关漏洞的在野利用实例，并在发布补丁的同时，提醒并催促管理员在 30 天内安装更

新。

六、 网络安全投融资、收购事件

1. 收购

1.1 Onapsis 完成对 Virtual Forge 的收购

1 月 16 日，Onapsis 完成对 Virtual Forge 的收购，收购价未公开。Onapsis 是一家致力于研究 SAP 系统安全问题的安全厂商。SAP 是很多大型企业的平台核心。通过采用预防和纠正方法保护 SAP 系统和应用程序的工具，来改变企业保护那些处理关键数据及程序应用的方式。Virtual Forge 则是一个为 SAP 系统和应用打造安全、合规和质量解决方案的供应商。

2. 投融资

2.1 OneLogin 获 1000 万美元 D 轮融资

1 月 10 日，OneLogin 从 CRV 和其他 3 位投资者处获得 1000 万美元的 D 轮融资。OneLogin 是一家云上认证和接入管理解决方案公司，保障用户终端 APP 安全。