国内外云计算+安全动态报告

2019 年第 3 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 增加多项支持，包括 AWS Elemental MediaPackage 支持资源标记，Elemental MediaLive 新增了对加密的 HLS 和 VPC 输入的支持，License Manager 支持根据实例数量和优化 CPU 设置跟踪许可证，同时推出多项功能，包括 Amazon ECS 引入了增强型容器依赖项管理，Elemental MediaConvert 推出详细作业状态和服务器端 S3 加密功能，Amazon EKS 推出了 Kubernetes API 服务器终端节点访问控制，并且 AWS Direct Connect 增加了 500 Mbps 以上的托管连接容量；VMware 打造首个原生的超融合系统；谷歌推出 Stadia 云游戏服务，Google 云端硬盘现在支持自然语言搜索；微软推出 Azure Bot 服务将更多机器人和 AI 带入云端，并发布 Data Box Edge 等 5 款新品；阿里云发布 SaaS 加速器计划；腾讯云推动教育行业数字化升级；华为云数据库新品发布，并发布多数据上云系列解决方案。

开源云方面，中兴通讯技术专家在 6 个 OpenStack 正式项目中当选 PTL；EasyStack 工程师当选 OpenStack 基金会技术委员会成员。

云安全厂商方面，全国政协委员、启明星辰集团首席执行官严望佳在两会上提交三个网络安全提案、2019 年度启明星辰（上海）合作伙伴大会圆满召开、启明星辰集团又斩获四枚创新大奖；深信服发布“卫信云”；山石网科 2019 获 CDM 3 大前瞻奖项；亚信安全解读 RSA2019；绿盟科技发布 EDR 新品；安恒 AiLPHA 大数据智能安全平台获“2019 年度 SIEM 突破奖”；360 企业安全与 Gartner 联合发布基于“零信任”的数字化工作空间白皮书；超两成有效移动杀毒软件采用安天反病毒引擎。

容器动态方面，Kubernetes1.14 版本发布，对 windows 节点达到生产级支持，持久化本地卷达到通用级别，kubectl 定制化更新等 31 项增强功能组成；Istio1.1 版本发布，大幅提升数据平面与控制平面的执行效率，完成了命名空间隔离等关键功能；CNCF 宣布在继 Kubernetes、Prometheus、Envoy 以及 CoreDNS 之后，宣布 containerd 已经成为其第五个毕业项目。

安全新技术方面，App 安全受到重视，9 款违规 App 曝光，涉及恶意扣费、隐私窃取、赌博；安全风险持续爆出，Facebook 数亿用户密码被发现在内部数据库明文保存，UC 浏览器存在中间人攻击(MITM)漏洞，可能影响十多亿设备；新安全标准和工具发布，W3C 批准 WebAuthn 成为无密码登录的 Web 标准，ISACA 发布针对区块链、CASB 和 GDPR 的全新审计程序，谷歌开源内部沙箱安全策略 Sandboxed API；Axonius 获得创新沙盒冠军。

网络安全投融资方面，分别发生 1 起收购和 4 起融资事件。全美第二大移动运营商 Verizon 完成对威胁检测公司 ProtectWise 的收购。融资方面，保护网络内核心资产的公司 eSentire 以 4700 万美元的私募股本融资拔得头筹，运营网络安全公司 CyberX 和基于日志和网络数据记录用户会话视频公司 LogRocket 分别以 1800 万美元和 1100 万美元融资位列二三。

2019 年 3 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 Elemental MediaPackage 支持资源标记

3 月 4 日，用户可以为 AWS Elemental MediaPackage 资源添加标签。MediaPackage 标签允许用户以不同的方式（例如按成本中心或拥有者）对资源进行分类，这简化了直播频道和终端节点的成本分配。

借助 MediaPackage，用户可以降低工作流的复杂性、提高源弹性，并更好地保护多屏幕内容，没有基础设施不足或过度预置的风险。

MediaPackage 可独立运行，也可作为 AWS Elemental Media Services 的一部分运行，后者是一系列服务，构成了基于云的视频工作流的基础，并为您提供创建、打包和交付视频所需的各种功能。

1.2 Elemental MediaLive 新增了对加密的 HLS 和 VPC 输入的支持

3 月 5 日，可以使用加密的 HLS 输入配置 AWS Elemental MediaLive 频道。MediaLive 将支持 #EXT-X-KEY 代码规范。这使用户可以加密直播频道的输入源，并让 MediaLive 解密，然后将其编码到频道输出中。

用户还可以从自己的 Amazon Virtual Private Cloud (Amazon VPC) 配置 MediaLive 频道的输入，以支持 VPC 输入。在用户配置 VPC 输入时，系统将使用 VPC 中的 IP 地址创建 RTP 或 RTMP 推送交付的终端节点。

AWS Elemental MediaLive 是一种广播级直播视频处理服务。借助此服务，用户可以创建高品质的广播视频，并流式传输到连接互联网的设备。

该服务可独立运行，也可作为 AWS Elemental Media Services 的一部分运行，AWS Elemental Media Services 是一系列服务，构成了基于云的工作流的基础，可为用户提供传输、创建、打包和交付视频所需的各种功能。

1.3 Amazon ECS 引入了增强型容器依赖项管理

3 月 7 日，Amazon Elastic Container Service (Amazon ECS) 引入了其他任务定义参数，使用户能够定义容器启动和关闭的依赖项，以及每个容器的启动和停止超时值。

之前，没有办法确保容器按照任何特定的顺序启动或关闭。现在，AWS 启用了许多常见的应用程序使用案例。例如，遥测 Sidecar 容器必须在任务中的其他容器之前启动且在其之后关闭，或者初始化容器必须完成其工作之后任务中的其他容器才能启动。此外，容器的启动和关闭超时先前是通过 ECS 代理中的环境变量设置的。现在，任务定义中的容器都可以拥有自己的启动和关闭超时。这将启用新功能，例如容器的延迟停止超时，它必须执行复杂的清理操作然后关闭，而不要求同一实例上的所有容器具有相同的关闭超时。

1.4 License Manager 支持根据实例数量和优化 CPU 设置跟踪许可证

3 月 8 日，AWS 通过添加对两个新方案的支持，增强了 AWS License Manager 中可用的许可证计数方法。首先，License Manager 现在可以跟踪基于实例数量的许可证。这对于跟踪负载均衡器和防火墙等软件的许可证非常有用。其次，License Manager 现在集成了优化 CPU 功能，可以跟踪一个实例上正在使用的 vCPU 的自定义数量。这使客户能够持续节省基于 vCPU 的许可成本，同时受益于 License Manager 提供的集中式许可跟踪。

1.5 Elemental MediaConvert 推出详细作业状态和服务器端 S3 加密功能

3 月 13 日，可以访问 AWS Elemental MediaConvert 的这两个新功能。首先，用户可以使用 Amazon CloudWatch 访问更详细、更频繁的转码作业进度状态更新。其次，用户可以使用 Amazon S3 的服务器端加密来保护使用 MediaConvert 静态生成的内容。

使用新的作业进度状态功能，用户可以配置在 Amazon CloudWatch 中获取更新的频率，范围从每 10 秒到每 10 分钟。这些事件现在显示作业的当前阶段以及作业完成百分比。

现在，用户可以保护 MediaConvert 输出的媒体文件，并在将它们写入 Amazon S3 时对其进行加密。这包括视频和音频文件、缩略图、字幕文件等。服务器端加密由 Amazon S3 处理，因为它将内容写入磁盘，当您访问文件时，文件将自动解密。有两个选项可用：Amazon S3 托管密钥和 AWS Key Management Service (KMS) 密钥。

借助 AWS Elemental MediaConvert，具有任何规模内容库的视频提供商都能够轻松可靠地对点播内容进行转码，用于广播和多屏播放。MediaConvert 可以独立运行，也可以作为 AWS Elemental Media Services 的一部分运行。AWS Elemental Media Services 是一系列服务，构成了基于云的工作流的基础，可以提供视频传输、转码、打包和交付所需的各种功能。

1.6 AWS Direct Connect 增加了 500 Mbps 以上的托管连接容量

3 月 19 日，通过支持 AWS Direct Connect（AWS Direct Connect 合作伙伴）的 AWS 合作伙伴网络技术和咨询合作伙伴，AWS Direct Connect 现在能够支持 500 Mbps 以上的托管连接容量。经批准的 AWS Direct Connect 合作伙伴能够预置 1、2、5 和 10 Gbps 的容量。

AWS Direct Connect 服务可轻松建立一个连接本地设施和 AWS 的专用私有网络。AWS Direct Connect 合作伙伴将帮助用户在 AWS Direct Connect 位置与用户的数据中心、办公室或主机托管环境之间建立 AWS Direct Connect 服务。托管连接使 AWS Direct Connect 合作伙伴能够通过预先配置的网络电路按需预置连接。

直到今天，托管连接仅支持从 50 Mbps 到 500 Mbps 的容量。1、2、5 和 10 Gbps 的托管连接将为客户提供以前只能通过专用连接提供的更高容量。AWS 还将与合作伙伴合作，进一步监控 AWS Direct Connect 合作伙伴与 AWS 之间的网络链接，用于识别和解决问题。

1.7 Amazon EKS 推出了 Kubernetes API 服务器终端节点访问控制

3 月 19 日，现在可以控制对 Kubernetes API 服务器终端节点（由 Amazon Elastic Container Service for Kubernetes (EKS) 托管）的访问，以便 Kubernetes 工作线程节点、Kubectl 命令行工具和 EKS 托管的 Kubernetes API 服务器之间的流量保留在用户的 Amazon Virtual Private Cloud (VPC) 中。这允许用户隔离 VPC 中的 Kubernetes 控制平面和工作线程节点，从而提供一层额外的保护来加强集群免受恶意攻击和意外暴露。

以前，可以从 VPC 外部访问 Kubernetes API 终端节点。工作线程节点需要在您的 VPC 外部调用，以获取正确的 IP 地址，才可以连接到 API 服务器，并且使用安全组限制对 API 服务器的访问。

现在，用户可以管理对终端节点的访问，以便所有流向 API 服务器的流量保留在用户的 VPC 中。这将使用户获得一层额外的安全性，并对 EKS 管理的 Kubernetes 集群进行控制。

2. VMWare 云动态

2.1 VMware 打造首个原生的超融合系统

3 月 21 日消息，为了展现对自身混合云和多云战略将赢得企业客户青睐的信心，VMware 今天进一步扩大了其服务的功能和地区覆盖范围。其中，VMware 推出了一个可以原生运行在超融合硬件平台上的 Cloud Foundation 迁移产品。

VMware 与 AWS 达成具有标志性的合作伙伴关系，是朝这一方向迈出的重要一步，两家厂商此后通过一系列增强型服务和围绕 Amazon 首款内部部署产品的合作，进一步强化了彼此之间的关系。VMware 高管表示，目前有超过 1000 家客户正在运行 VMware 提供的 AWS 服务，并明确表示计划未来将运行在任何公有云以及主要的本地云平台上。

“关于平台的争论早已不复存在，”VMware 产品开发和云服务高级副总裁 Ajay Patel 这样说到。“只要客户需要，在任何地方都可以部署。”

新推出的 VMware Cloud Foundation 版本是在 Dell EMC VxRail 超融合平台上本地运行的，其重要意义在于，它是第一款从一开始就针对 VMware 混合云基础设施堆栈设计的超融合系统。

VMware 高管表示，由于采用了一系列双方共同设计的功能例如生命周期管理和自动化，因此该集成平台要比安装在相同硬件上的标准软件速度高出 60%。IDC 数据中心和云研究副总裁 Rick Villars 表示，这款将于 4 月上市的平台，将为客户提供向 VMware 混合云服务的快速迁移。

CloudHealth by VMware 是 VMware 在去年夏天收购 CloudHealth Technologies 获得的一款统一监控平台，目前这款平台也将进行重大的升级改进，新功能包括增强的多云报告、多维报告、容量管理、与 VMware 云分析和监控平台 Wavefront 的集成等。

CloudHealth 创始人 Joe Kinsella 表示，这些增强功能是为了应对企业内部采用云技术越来越去中心化的趋势。他说：“如今企业拥有大量公有云和私有云已经不稀罕了，但这大大增加了复杂性。”

根据该公司发布的数据显示，收购 CloudHealth 显然是符合 VMware 目标的。CloudHealth 目前为客户管理着超过 80 亿美元的年度云支出，每月要接收近 40 亿个 API 调用。

Cloud Foundation 3.7 的新功能中，还包含了对 VMware Horizon 7 虚拟桌面基础设施的自动部署功能，包括应用程序卷的安装、用户环境管理器和统一访问网关。目前 VMware 已经在 AWS 的加拿大中部、巴黎、新加坡等地区提供 Cloud Foundation，使得全球可用地区增加到 13 个。VMware 拥有 4200 家云合作伙伴，这“对我们来说是一个重要优势”，Patel 说。

VMware 还宣布推出了新版本的 vCloud Director——一款面向云平台的自动配置、管理和数据保护套件。这次推出的 9.7 版本通过统一监视和管理，跨私有云和多租户 VMware 云中提供集中的全局云管理、可扩展性、增强的可扩展性框架。

此外，VMware 推出了统一迁移和灾难恢复服务 vCloud Availability 的 3.0 版本，它与 vCloud Director 进行本地集成，提供了一个充满活力的用户界面。

3. GOOGLE 云动态

3.1 谷歌推出 Stadia 云游戏服务

3 月 20 日，谷歌 CEO Sundar Pichai 在游戏开发者大会（GDC）上公开了云游戏平台 Stadia，为玩家提供不受硬件性能限制的跨平台云游戏服务，并将于年内在美国、加拿大、英国以及大部分欧洲地区推出，具体时间和售价待定。

前索尼和微软高管 Phil Harrison 补充说，谷歌将联合 YouTube 强化这一服务。在 YouTube 上，用户在观看游戏视频的过程中可以随时点击“立即游戏”按钮，无需安装即时开始游戏。“我们的愿景是将这两个世界融合起来，在观看游戏的时候也可以动手玩游戏。”无论是手机、平板还是电脑等设备均可通过 Chrome 浏览器进行游戏，游戏存档也会通过云端同步。

谷歌云游戏的操控通过 Stadia 手柄来实现。手柄通过 Wi-Fi 连接到云，赋能玩家使用“分享”按钮在 YouTube 上上传游戏片段，点按 Google Assistant 按钮访问界面。

不延迟是有效传输游戏的关键，对服务器有较高的要求。谷歌希望通过互联网连接以大约 25Mbps 的带宽支持高达 4K 的 60 fps,计划在未来支持 8K、120 帧游戏。此外，谷歌与 AMD 合作构建 GPU，其浮点运算能力高达 10.7Terraflops，比 Xbox One X 和 PS4 Pro 的性能更强劲。

近几个月来，谷歌将此服务作为 Project Stream 进行测试，允许 Chrome 用户在浏览器中流式传输游戏。《刺客信条：奥德赛》（Assassin’s Creed Odyssey）是唯一一款进行公开测试的游戏，该测试在 1 月份完成。《毁灭战士：永恒》（Doom Eternal）将成为首个登陆谷歌云游戏平台 Stadia 的项目，支持 4K 分辨率、每秒 60 帧的游戏画面输出、HDR 以及环绕立体声。

微软、索尼和任天堂目前都各自推出了云游戏服务。在云游戏领域，谷歌不仅需要解决自身和行业的问题，还面临着激烈的竞争。

3.2 Google 云端硬盘现在支持自然语言搜索

3 月 23 日消息，谷歌今天宣布发布其谷歌云端硬盘云文件同步和共享服务的新功能。现在，当用户在搜索框中输入内容时，该工具将为拼写错误的单词提供建议。此外，用户可以继续输入与用户在尝试查找特定文档时说话时使用的相同单词。

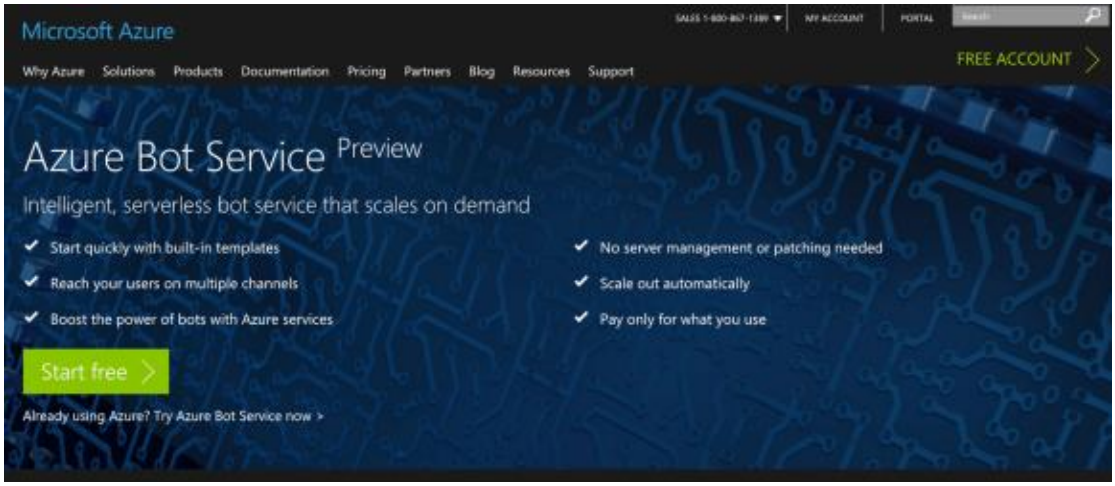
添加此功能(称为自然语言搜索)意味着用户不再需要仅键入文件名中的单词。用户可以说“从 2015 年开始显示电子表格”，然后出现一些搜索结果，以及可能的“您是不是意味着”建议来优化用户的查询。谷歌使用自然语言处理(NLP)进行网络搜索，现在它可以更广泛地使用。

此版本中的其他功能包括在列中排列 Google 文档文件的新方法，以及在云端硬盘中打开或编辑非 Google 文件后将其保存到 Google 云端硬盘的选项。

4. 微软 Azure 云动态

4.1 微软推出 Azure Bot 服务将更多机器人和 AI 带入云端

3 月 16 日消息，微软推出 Azure Bot 服务，让机器人创造者可以选择将机器人移植到云端，让微软处理服务器和存储问题。



微软 FUSE 实验室总经理 Lili Cheng 今天在一篇博客文章中写道，该服务已经创建，“随着您的机器人越来越受欢迎，您只需支付使用的费用即可为您提供运营和处理规模的运营灵活性。此外，您也不必担心配置或管理运行机器人的服务器。为您处理补丁和基础架构维护 - 您专注于编写代码。“

Microsoft Bot Framework 可以制作可在超过六个平台上运行的机器人，包括 Skype，Microsoft Teams，Facebook Messenger 和 Kik。

Azure Bot 服务每月可免费提供一百万个服务器请求，并提供类似于帮助填写表单的机器人模板或利用语言理解智能服务(LUIS)的模板，LUIS 是 Microsoft Cognitive Services 提供的主要自然语言处理器。

4.2 微软发布 Data Box Edge 等 5 款新品

3 月 27 日消息，微软官方重磅推出几款边缘计算的新品，并宣布全面商用。这意味着，这家全球第二的云厂商已经在边缘计算大战中重兵布阵了。

微软 Azure 的边缘计算网络示意图（含 5 款新品）

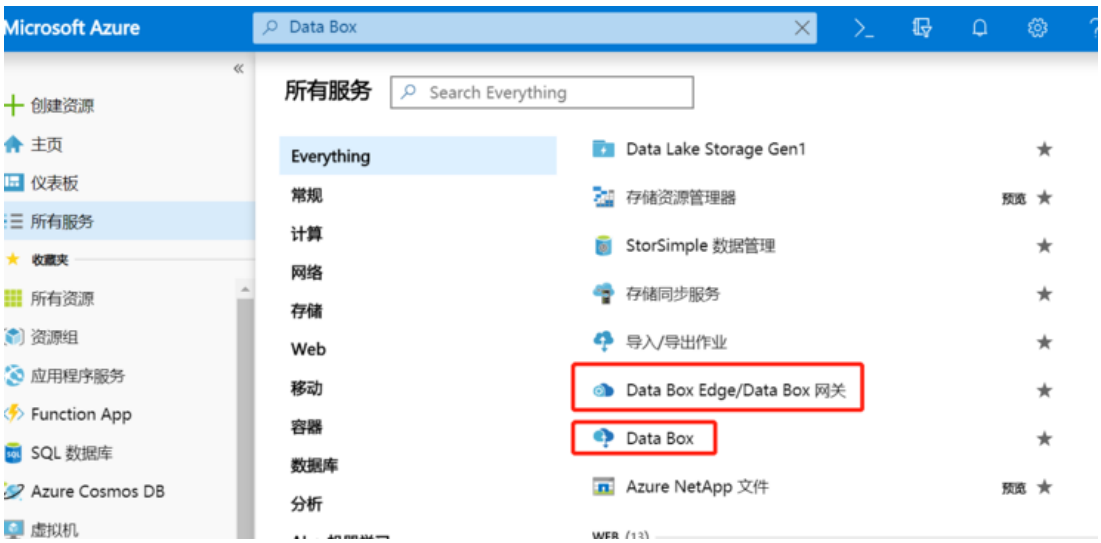
5 款 Data Box 新品，矩阵式打法

具体而言，依照联网在线和脱机离线两种场景，微软都配备了不同的产品矩阵。其中：

联网在线场景下，推出的是 **Data Box Edge 和 Azure Data Box Gateway2 款**；

脱机离线场景下，推出的是 **Data Box、Data Box Disk 和 Data Box Heavy Preview3 款**。

当微软 Azure Data Box 总经理 Dean Paron 宣布这些消息时，她还指出，用户可以在 Azure 门户中获取这些产品。雷锋网尝试了下，确实 Azure 门户已经开放申请。



Data Box Edge 如何承载微软的边缘计算野心？

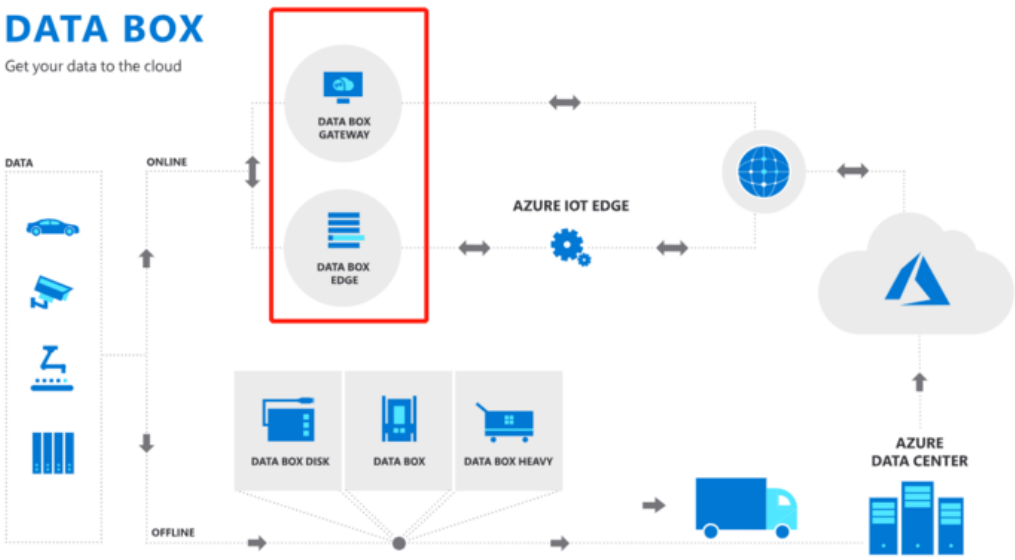
Data Box Edge 能充当存储网关，在用户站点和 Azure 存储之间创建链接。这使得将数据移入和移出 Azure 存储与使用本地网络共享一样简单。Data Box Edge 提供本地缓存并优化进出云的网络流量（雷锋网注：移入移出数据是联网时才有，而脱机之下只能做数据移入而无法移出）。

此外，Data Box Edge 还通过 IoT Edge 提供计算平台，使用户可以将 Azure 服务和自定义代码、应用程序部署到边缘。

Data Box Edge

总而言之，Data Box Edge 是一款让微软布局边缘计算更彻底的设备。

在使用方式上，Data Box Edge 可以与现有的企业硬件一起存放，也可以存在于从工厂车间到零售通道的非传统环境中。使用 Data Box Edge，无需购买其他硬件，用户只需要像任何其他 Azure 服务一样注册并按需付费就行了。



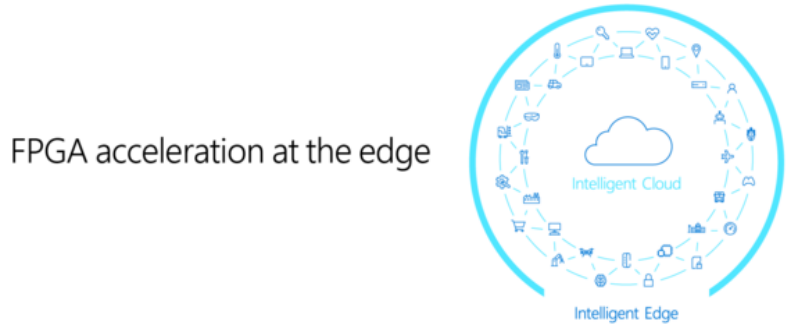
这款机架式设备 Data Box Edge 具有哪些特点？

本地计算。Data Box Edge 可以与本地化系统进行交互使用，在数据上传至云端之前就完成存储与计算。

网络存储网关。在本地设备和 Azure 存储帐户之间自动传输数据。Data Box Edge 在本地缓存最热门的数据，并将文件和对象协议与本地应用程序对话。

使用英特尔 Arria 10 FPGA 的 Azure 机器学习。使用 FPGA 加速数据的推理，然后将其传输到云上以重新训练和改进模型。

云管理。使用 Azure 门户轻松订购设备并为用户的机群管理这些功能。



从这些特点来看， Data Box Edge 能和 Azure 形成很好的配合，优化对用户数据的存储和计算，并迅速进行决策反馈。

Data Box Gateway 是微软“新的考虑”

Data Box Gateway 的产品思路相对简单：独立的虚拟网关设备，可以部署在基础架构中的任何位置。

微软澄清说，Data Box Gateway 实际上是内置在 Data Box Edge 这个硬件设备中的“虚拟设备组件”（软件），一旦用户并不想购买 Data Box Edge 来部署边缘计算，而只需要一些数据流通共享能力，则只需要购买独立的虚拟设备组件 Data Box Gateway 就行了。

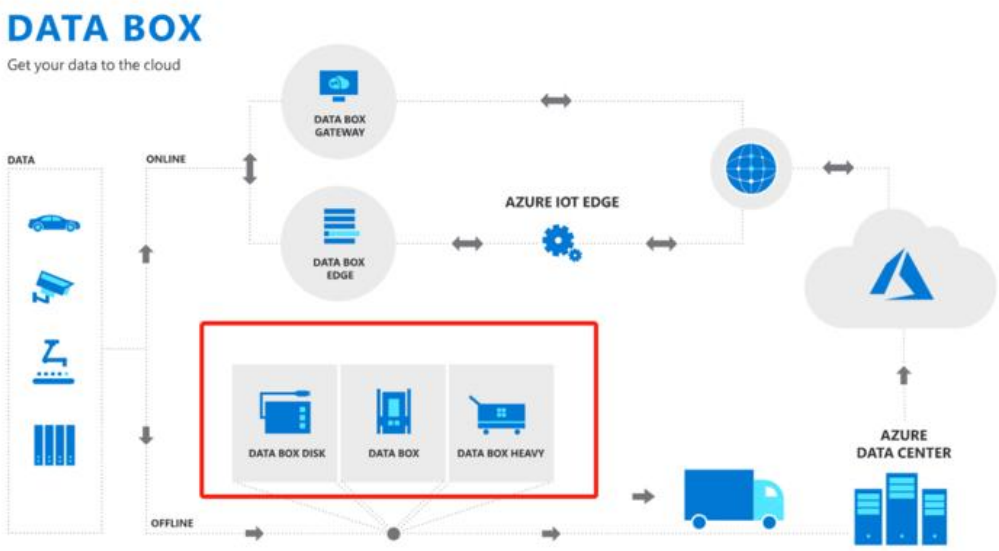
这相当于留了一手，对灵活部署的企业而言，这种方式更便宜也更便捷。

在使用方式上，用户可以使用 Hyper-V（微软的一款虚拟化产品）或 VMware 在管理程序中配置它，并通过 Azure 门户进行管理。Data Box Gateway 将在本地网络上设置服务器消息块（SMB）或网络文件系统（NFS）共享，而共享后的数据将自动上载到 Azure 存储帐户，支持块 blob（存储设备）、页 blob（存储设备）或 Azure 文件。

不过，微软强调了，无论是使用 Data Box Edge 内部的存储网关还是部署 Data Box Gateway 虚拟设备，存储网关功能都是相同的（对客户而言就是二选一的问题）。

离线场景下 Data Box 的“组合拳”方案

除公布了 Data Box Edge 和 Data Box Gateway 两个核心产品外，微软官方还提供三种尺寸的 Data Box 样式，以便在离线时使用：



Data Box：坚固耐用的 100 TB 运输设备。

Data Box Disk（数据盒磁盘 ）：更小更灵活的传输选项，每个订单具有单独的 8 TB 磁盘和高达 40 TB 容量。

Data Box Heavy Preview：更大版本的数据盒，可扩展至 1 PB。

自此，微软的 Data Box 和 IoT EDGE 等产品一结合起来，就形成了用户在线离线双重梳理数据的方式。这在未来一段时期，也必将成为边缘计算革命的一个重要的研究方向。

5. 阿里云动态

5.1 阿里云发布 SaaS 加速器计划

3 月 21 日消息，2019 阿里云峰会·北京在北京国家会议中心召开，此次峰会以“十年再出发”为主题，全面解读阿里云智能的全新品牌形象、技术实力和发展战略，并发布了 SaaS 生态加速器计划。

定位：阿里云自己不做 SaaS 让大家来做更好的 SaaS

对于未来，阿里云第一次表态“被集成”：阿里云自己不做 SaaS，而是让合作伙伴来做更好的 SaaS，希望把阿里云的技术和理念变成客户和合作伙伴解决方案的一部分。

方向：阿里云发布 SaaS 加速器，与合作伙伴共建 SaaS 生态，为客户创造新价值

核心：商业、能力和技术的合力输出全面加速生态合作伙伴发展

商业中心：围绕企业商业软件从产品研发到部署交付的生命周期，为合作伙伴提供商业化助力，和阿里云共赢。

能力中心：开放阿里沉淀的业务能力汇聚生态业务场景，共建业务互联互通

技术中心：助力伙伴业务能力，开放阿里技术红利，提供 SaaS 应用快速开发和上云能力，助力伙伴提效降本，共创云时代企业应用最佳实践。

6. 腾讯云动态

6.1 腾讯云推动教育行业数字化升级

3 月 21 日，腾讯云在深圳举行首次教育合作伙伴生态大会。会上，腾讯云介绍了其在新工科、智慧校园、在线教育等领域的解决方案，以及如何实现在课堂教学、家校互动、校园管理等多个场景下的落地应用，并表示将同合作伙伴一同打造教育行业的云端生态。

会上，腾讯云副总裁谢岳峰说道：“腾讯云作为腾讯能力对外输出的桥梁，依托云服务、大数据、AI 等底层能力，会做好教育产业智慧化升级的数字化助手，发挥连接器和工具箱的作用，未来，腾讯云将投入更多资源和精力，携手更多合作伙伴，加速与校园、教育管理部门之间合作的推动，进一步完善全教育周期的智慧教育体系，推进智慧校园在更多地区落地，打造智慧教育云端生态。”

此外，腾讯云的合作伙伴们也表示，未来将通过借助腾讯云的云服务能力、智慧教育体

系和产品支持，持续落地智慧校园、创新教育等场景，助力教育行业数字化升级。

依托腾讯云在教育行业的生态优势和云计算、大数据、人工智能等技术能力，腾讯云与合作伙伴打造了具有教育数据交换、治理、可视化平台的完备的大教育体系，涵盖从学前教育到成人教育以及线上教育的全流程技术、服务和内容支持。

从腾讯教育云、教研云，再到智慧教育数据中心、线上教育合作，腾讯云已在教育领域推动多个项目落地及多方面布局。

在智慧校园建设方面，腾讯云与其合作伙伴已与诸多教育局、学校达成合作。并为其提供覆盖智慧安防、智慧办公、智慧家校、智慧数据等多个领域的场景式服务。从而改变传统教学方式。通过腾讯云智慧校园云平台，学生可以实现在家学习，老师实时检查学习进度，实现“停课不停学”。目前，腾讯云智慧校园在全国服务超 14000 所学校，触达 1900 余万师生和家长，并与河南省电教馆、江西省上饶市、福建省福州市等超 300 个教育主管部门进行了全面合作。

在高校教育方面，腾讯云已与天津大学、青岛大学等十几所高校达成战略合作协议。并通过参与到教育部“新工科”项目，构建认证考试体系、竞赛赛事、互联网产业人才生态库等，助力高校培养符合“新技术、新业态、新产业、新模式”要求的新一代工程科技人才。

7. 华为云动态

7.1 华为云数据库新品发布

2019 华为中国生态伙伴大会上，华为云发布了两款具有划时代意义的云数据库产品：最新一代企业级高扩展海量存储分布式数据库 Taurus，和全球化的 NoSQL 分布式多模数据库 Gemini。二者均为华为云厚积薄发的自研产品，针对用户普遍需求，结合当下云数据库领域最新技术，在功能和性能方面都有大幅提升。

新一代企业级高扩展海量存储数据库 Taurus

极致可靠

华为云 Taurus 采用存储与计算分离的新型架构，提供跨 3 个城市的数据副本，将备份数据保存至 OBS(对象存储服务)，数据可靠性高达 11 个 9(99.99999999%)，绝无数据丢失的担忧。此外通过数据分片技术，Taurus 能实现秒级恢复存储故障，软件故障恢复则可保障业务不中断和数据 0 丢失。小到软/硬件故障，大到自然灾害，都有自动化快速恢复方案。

极致性价比

华为云 Taurus 的单节点性能最大可达原生 MySQL 的 7 倍;同时通过只读扩展，读性能可以成倍线性提升，业界同类产品无与争锋。在同等规模下，Taurus 成本只有商业数据库的 1/10，且提供整套数据库运维服务，可大大减少企业人力投入。

多维扩展

Taurus 集群规模高达 1 写 15 读，其中只读节点企业可以根据业务需要在线动态扩展/收缩，无论是 CPU、内存、还是数据库节点，都能够简便地一键扩展，方便快捷。Taurus 还会根据用户存储容量自动扩容，存储空间最大可达 128TB，且扩容期间不会对业务造成任何影响，消除了运维人员通宵部署硬件之苦。

完全可信

Taurus 通过与 DBSS(数据库安全服务)的透明化集成，不用修改应用，只需在界面配置即可享受智能化的安全保障，可以防御各种互联网攻击，防护数据泄露。 当前，华为云数据库已通过可信云认证，提供国际级的隐私和数据保护。

值得一提的是，Taurus 完全兼容 MySQL 8.0 版本，用户可以将原有的 MySQL 线下业务无缝迁移上云，不用担心额外业务改造成本。后续，华为云将在持续优化 Taurus 性能和功能的基础上，同步社区更新，使用户在技术上同时享受商业级的技术服务，和开源软件的

生态红利。

全球化的分布式多模数据库 Gemini

Gemini 是一款华为自研的旗舰级、Cloud Native 架构、Serverless 按需弹性伸缩、跨 Region 容灾、自驱动的、多模 NoSQL 云数据库服务产品。其兼容支持多种主流 NoSQL 生态/接口模型，包括 MongoDB、Cassandra 和 DynamoDB 等。

三倍性价

Gemini 在社区版的相同配置情况下，能达到 3 倍性能提升。Gemini 具备业界领先的 Serverless 特性，即根据吞吐量需求自动的弹性伸缩，为客户节省大量成本。

企业级可靠性

Gemini 具备企业级的数据可靠性，能够容忍 N-1 个节点故障，并且在节点故障时对客户的应用无感知，不影响数据的读写。通过多节点并行的快照备份，做到 10 倍以上的备份恢复性能提升，20 分钟内能够完成任意时间点的恢复。

灵活全托管

Gemini 基于业界领先的计算存储分离架构模式，灵活性能够达到同类产品百倍。此外它在内核层面做到实时监控实例的数据存储量以及吞吐量，一旦达到扩容阈值，在 2 分钟内能够自动扩展完成，让用户可以放心托管数据库。

完善的数据库生态

Gemini 具备完善的数据库生态体系，有 DAS 作为图形化的数据编辑工具，有 DRS 支持数据的在线迁移、同步和跨版本的复制，有云 DBA 作为自动化的数据库诊断工具，并且能够与大数据组件无缝对接。

Gemini 的特性使其非常适用于游戏、工业制造、互联网等行业。游戏具有快速迭代、开服吞吐量高峰、快速开服、全球同服、降成本、附近玩家、回档等行业关键需求，在 Gemini

下都能够很好地支持。工业制造、互联网行业需要存储海量数据，Gemini 能很好的支持 7*24 小时实时高并发数据写入，作业高峰期弹性扩展。

华为云 Gemini 将在全球布局规划，让每个 Region 间数据实时进行超低时延的同步，帮客户业务实现全球容灾和就近读写。

轻松上云：华为云 DRS 实现多场景数据迁移

作为核心业务运行的主要承载体，数据库上云一直是客户最关心的问题之一。如何保障迁移时核心业务不中断?如何确保数据不丢失?数据库迁移实施难度大、没有专家团队怎么办?华为云数据复制服务 DRS 正是为了解决这些问题而推出。

华为云 DRS 是一种易用、稳定、高效，用于数据库在线迁移和数据库实时同步的云服务，业内首家提供数据预估功能、参数迁移、用户迁移，并通过多项核心技术，让 RPO&RTO 双控在秒级，数据库异地灾备的业界最高水平，完美解决跨云灾备、本地到云灾备、混合云灾备、跨区云灾备等场景下的能力空白。

DRS 的引导式操作、近百项检查、详细的指导让没有迁移经验的用户也能做好迁移。此外通过在线迁移技术和数据实时同步，能确保数据库迁移上云业务中断时间最小化。DRS 的断点续传、故障重试、迁移后对象、数据对比等多项特性组合，实现迁移任务高效、无死角，数据 0 丢失的完成。

当前，DRS 支持多来源、多网络、多引擎迁移。无论用户是从本地机房、其他云、华为云内部，采用公网网络、华为 VPN 网络、专线网络、华为 VPC 网络，均可对 MySQL、SQL Server、MongoDB、PostgreSQL 任意一款数据库进行迁移。

7.2 华为云发布数据上云系列解决方案

3 月 27 日消息，在华为中国生态合作伙伴大会分论坛上，华为云推出了基于其领先的 OBS 对象存储服务构建的数据上云系列解决方案，帮助合作伙伴和企业解决海量数据管理和数据增值面临的挑战。

大数据和 AI 方案行业领先

华为云认为，企业大数据和 AI 应用中会遇到几个主要困难，包括：性能不足导致的分析周期长;资源无法灵活配比，存在浪费;IT 投资和维护成本高;数据多次拷贝导致的容量和效率浪费等等。为解决这一系列的问题，华为云推出了“大数据和 AI 解决方案”，其基于公有云服务的“存储与计算分离”方式，能为企业客户带来更高性能和更优的成本。

在发布现场，华为云展示了该方案与行业内同类方案的对比测试结果。结果显示，依靠华为云强大的 BMS 集群和性能领先的 OBS 服务，其在 Spark Terasort 测试场景下的整体效率和综合成本大幅领先。据华为云专家介绍，该方案可以应用在互联网数据分析、自动驾驶、金融风控、国土气象、机器学习和 AI 训练等多个行业和场景。

医疗和视频数据云上管理更便捷

随后，华为云还向嘉宾介绍了更多成熟应用的解决方案，如在医疗行业推出的“医疗云 PACS”方案，让医院无需自建数据中心，就可以满足医疗数据长期存储和容灾的需求，结合 AI 辅助诊疗，让医师工作效率更高。

在当前热门的长短视频领域，华为云也推出了其集视频编转码、AI 分析、存储和 CDN 加速云服务的“视频点播、直播、短视频解决方案”。该方案可以让 H.265 高清格式视频码率

降低 30%，并且支持 AI 画质重生，让人印象深刻。

华为云表示，基于其领先的智能云基础设施服务和持续的技术投入，将源源不断为合作伙伴和客户带来更多业务创新引擎，加速企业智能进化。

二、 开源云动态

1. Openstack 动态

1.1 OpenStack Train 版本项目领导人选举

3 月 26 日消息，从 OpenStack 基金会获悉，在刚刚结束的 OpenStack Train 版本的项目领导人（Project Team Leader, PTL）选举中，中兴通讯技术专家在 6 个 OpenStack 正式项目中当选 PTL。中兴通讯当选正式项目 PTL 的项目数量在全社区排名第二（电信设备商第一），充分展示了在开源领域强大的技术实力。

OpenStack 是由各功能项目整合形成的一个系统。每个项目的治理方式是由核心贡献者（Core）组成核心团队，具有评审代码控制合入的权限。该团队也控制着项目的技术发展方向。PTL 作为项目的总负责人，从核心团队中选出。每个 OpenStack 版本周期开始前，由各项目中有代码贡献的开发者投票，选出本项目此版本的 PTL。

中兴通讯新当选的 PTL 均是在 OpenStack 社区中长期投入，对项目贡献名列前茅的贡献者。其中朱荣连任 Murano 和 Solum 两个项目的 PTL，耿常才连任 Freezer 项目 PTL，刘雪峰再次当选 Senlin 项目 PTL，冯圣琴再次当选 Zun 项目 PTL，李灿伟新当选 Watcher 项目 PTL。

中兴通讯自 2016 年起投入了大量的资源和人力到开源社区中，在 OpenStack 社区中的贡献不断攀升。特别是新功能贡献在近三个版本（P/Q/R）中，中兴通讯均名列前五，最高位列第三。中兴通讯目前已经拥有包括上述几位 PTL 在内的 13 位核心贡献者，覆盖了 11 个 OpenStack 正式项目。本次 PTL 的选举，也进一步提高了中兴通讯在社区内的技术影响力。

2. Easystack 动态

2.1 EasyStack 工程师当选 OpenStack 基金会技术委员会成员

3 月 14 日消息，OpenStack 基金会技术委员会（TC）最新选举结果揭晓，易捷行云 EasyStack 开源社区工程师林冠宇当选 OpenStack 基金会技术委员会成员。

作为 OpenStack 社区的最高技术领导力，OpenStack 技术委员会负责监督社区技术问题和上游开源项目，其成员直接由上游项目的贡献者选举产生。OpenStack 技术委员会保证 OpenStack 理念的贯彻落实（如保持其开放性，透明度，通用性，注重技术集成和质量），决定跨社区合作和交叉合作问题，为技术路线和一般监督提供最终决策。

EasyStack 开源社区工程师林冠宇持续多年深度参与 OpenStack 社区的代码贡献和社区建设，曾连续两年担任 Heat 项目 PTL，在 2018 年 OpenStack 柏林峰会上，林冠宇还被授予 OpenStack 社区贡献者奖。此次林冠宇当选基金会技术委员会成员，代表着更多的中国声音和力量将加入到国际开源社区的规划和决策中来。

3. 99CLOUD（九州云）动态

暂无消息。

三、 云安全厂商动态

1. 启明星辰

1.1 全国政协委员、启明星辰集团 CEO 严望佳在两会上提交三个网络安全提案

2019 年两会正在进行中，全国政协委员、启明星辰董事长严望佳在两会上提交了三份提案，内容涉及网络安全制衡能力、人工智能安全和数据法治建设等方面。

（一）《关于增强大数据时代中网络安全制衡能力的提案》

提案指出，当今数据已成为国家基础性战略资源，应利用网络安全技术 “对信息化建设加以适当的安全制衡和引导”，才能实现习总书记提出的 “网络安全和信息化是一体之两翼、驱动之双轮” 的要求，保证国家社会的健康良好发展。提案建议在处理网络安全和信息化关系时，“要将网络安全放在一个平等的、独立第三方的位置，而不是处于信息化的附属地位”，“保障和制衡数据时代的可持续性发展”。具体建议如下：

1）制定政策配套细则，提高网络安全制衡能力

出台政策配套细则文件，强调网络安全在信息化规划、建设和运营时的重要性，并有效指导基层单位进行落实。包括在关键信息基础设施建设中制定网络安全管理办法、设立网络安全的“一票否决权”、设定项目网络安全预算最低比例要求（如 8%-12%）、规范网络安全独立审计制度等。

2）强调网络安全独立性，落实网络安全保障职责

信息化部分和网络安全部分须由不同责任主体承担，并严格落实 “网络安全和信息化三同步原则” 。同时，在涉及国家安全、国计民生和公共利益的信息化项目中，鼓励建设独立于信息系统运营的网络安全运营中心，强化网络安全事件独立处理能力和网络安全保障效果。

3）实施国家网络安全重大工程，强化网络安全可控水平

围绕国家重大战略需求和重要信息化系统，布局实施一批重大安全工程，如建设统一的威胁情报、态势感知和数据安全预警系统等。通过实施国家层面的网络安全重大工程，不仅可以加快构建关键信息基础设施安全防御体系，提高对智慧城市和关键信息基础设施的安全管控能力，还可以显著带动各单位提高对网络安全的重视程度，形成网络安全与信息化发展并重的局面，并切实维护国家网络空间主权和发展利益。

（二）《关于规范人工智能安全健康发展的提案》

提案认为，由于人工智能的快速发展，如果缺乏有效地安全控制和管理，则会“留下难以估量的安全隐患”。为了达成习总书记提出的：要加强人工智能发展的潜在风险研判和防范，维护人民利益和国家安全，确保人工智能安全、可靠、可控的要求，提案建议如下：

1）加快开展人工智能安全应用法规和伦理道德的研究

具体的安全规范机制包括研究出台相关法律法规，界定人工智能应用的法律主体及相应的权利和义务；开展人工智能伦理道德的探讨，约束人工智能研究与实际应用的范围界限。

2）建立关键领域内的人工智能应用安全审查机制

加强人工智能算法及应用的安全性、可控性和透明性的审查。

3）展开人工智能安全评估技术研究，健全完善测评机制

一方面引导加快研究人工智能产品和应用的安全评估评测技术，逐步积累安全检测样例库、测试样本库等知识资源和研发测试工具集，提高人工智能产品和应用的安全评估评测能力；另一方面推动人工智能安全相关的国家标准和行业标准的制定工作，明确相关安全评估指标、方法和要求，建立安全测评流程和管理规范，健全人工智能产品和应用安全测评机制。

（三）《关于加快完善数字经济时代数据法治建设的提案》

提案指出，在数字经济快速发展的社会实践中，出现了大量个人信息被窃取或泄露、非法收集和买卖等现象，也造成电信诈骗、金融诈骗等事件屡屡发生，个人人身和财产安全乃至国家安全都受到严重威胁，迫切需要加快出台数据保护法和个人信息保护法，当前如何建设数字经济法治体系以保护数据产权，如何以法治方式规范数据收集使用以鼓励市场主体创新，如何借助大数据资源提升司法治理能力，成为我们在推进法治中国建设和数字中国建设

进程中面临的重要议题。提案建议：

1）建议加快数字经济时代的数据保护立法工作

落实习近平总书记 “要制定数据资源确权、开放、流通、交易相关制度，完善数据产权保护制度”的要求，更好的满足我国高速发展的数字经济保驾护航需求和提高社会数据治理水平，针对在 2018 年我国人大已纳入立法计划之中的《数据安全法》，建议加快其研究与立法工作。

2) 建议加快推进我国个人数据保护立法工作

我国至今还未制定个人信息保护法等专门法律，个人数据保护亦面临严重危机。个人数据经常可能在云服务--管道--终端的每一个环节未经数据主体授权就被不当收集、储存、利用，甚至用来非法交易。 因此，针对在 2018 年我国人大已纳入立法计划之中的《个人信息法》，建议加快推进我国个人数据保护--《个人信息法》立法与研究工作。

3) 建议及时完善数字经济数据要素相关法律法规

数字经济快速发展对我国现有法律法规体系提出了新的挑战，数字经济发展需要法治来保障，建议加强研究并做好以数据为核心生产要素的数字经济法律法规治理体系的顶层设计，根据数字经济发展形势和需要，及时调整完善现行相关法律法规，明确数据市场监管主体、负面清单、参与主体权责以及相关法律责任，为我国数字经济持续健康发展和国际竞争力的提升营造良好法治环境

1.2 2019 年度启明星辰（上海）合作伙伴大会圆满召开

3 月 21 日，以“星辰为友 众行致远”为主题的 2019 年度启明星辰（上海）合作伙伴大会在上海拉开帷幕，200 多家启明星辰的合作伙伴汇聚一堂，探讨网络安全市场的新动态，一起分享网络安全前沿解决方案。会上，启明星辰发布了全新的合作伙伴计划及推出了适合中小企业的超惠产品，邀请权威机关为参会者解读了网络安全的新政策。

本次会议特别邀请了上海市信息安全测评认证中心对网络安全政策进行了权威解读。同时，启明星辰向合作伙伴介绍了网络安全市场的新蓝海，推出了全新的公共安全智能监控网络视频安全解决方案，并在会议上正式宣布：启明星辰成为中国首家推出下一代防火墙与软件定义广域网融合网关产品，SDWAN 与 NGFW 的全面融合，会有效提升用户 IT 系统的安全性、可靠性及业务体验，必将成为渠道市场的核心产品。这一市场新蓝海引起了合作伙伴的极高热情，为合作伙伴提供了新的市场增长方向，坚定了合作伙伴共赢未来的信心。

本次会议启明星辰重磅发布了全面进军中小微企业市场的渠道战略，隆重推出下一代防火墙、负载均衡和堡垒机三个系列的多款超惠产品，充分让利合作伙伴，设立多种渠道业务模式，与合作伙伴一起聚势合赢。

1.3 启明星辰集团斩获四枚创新大奖

（一）年度创新产品奖——物联网安全接入防护系统（IoT-VBox）

物联网安全接入防护系统（IoT-VBox）定义企业“泛在物联网”新安全，以物联网可视化管控技术路线，布局物联网+下的企业网络安全防护。过去的 2018 年在智慧城市、交通、安防和电力等行业均得到成功的应用，得到了行业客户的认可。

可视化：IoT-VBox 以无代理技术为核心，全面洞察企业网络中的泛在物联网终端，并智能分类。全生命周期的立体化识别能力，从资产发现，包括设备、操作系统；到流量发现、连接关系、访问请求；到行为学习、业务属性。为后续的管控形成决策基础。

管控：IoT-VBox 的可视化和管控形成闭环，可实现设备仿冒检测，秒级的检测引擎保障安全；实现按需通断，保证合法访问，减少攻击平面；实现行为管控，基于人工智能的算法攻克碎片化安全难题。

编排：IoT-VBox 安全节点，具备数百种 API 接口，将采集的安全信息和城市安全运营平台进行快速对接；IoT-VBox 具备强大的编排能力，可以和交换机、FW、VPN 和 WIFI 节点进行联动，对物联网进行防护；IoT-VBox 从诞生之初就对接了广泛的市场需求，形成多行业的防护价值。

（二）年度创新产品奖——网络用户实体行为智能安全分析系统(V-UEBA)

网络安全是人与人的对抗，来自网络的威胁也是和网络技术发展并行的。对应于安全威

胁变化，也要有相应的安全防护方式。启明星辰自主研发的网络用户实体行为智能安全分析系统（简称：“V-UEBA”）是通过对用户和实体(网络、端点、数据存储)进行细粒度异常行为检测和分析，为用户打造的安全智能分析产品。在为用户解决上述问题的同时提供：

多元异构海量安全数据处理

用户画像，找出正常行为模式

高效智能异常发现能力，准确提供第一线索

高级安全分析能力

更快速的安全事件研判，提供证据

（三）启明星辰荣获年度影响力产品奖

启明星辰集团基于工控终端安全、边界防护（工控防火墙和工控网闸）、工控异常检测、工控漏扫和工控 SOC 等产品打造了面向工业互联网的安全管控平台。在经过多年对工业的深入理解和产品迭代，已经形成了成熟的安全体系，并在先进制造、石油石化、电力、军工、轨道交通和烟草等国家基础设施行业都取得独特价值和重大的突破。同时针对主流行业的安全需求差异，实现了针对性的方案。基于通用的工控安全技术积累和行业化差异的产品特性，奠定了启明星辰在工控安全的领导地位。随着国家工业互联网战略的推进，启明星辰会持续创新，来防护生产网与云端互联的安全场景。

（四）新兴产业创新典范企业奖

启明星辰多年前已积极战略布局网络安全新技术，带动和提升了智慧城市、人工智能、工业互联网、关键信息基础设施保护、物联网等业务的安全发展，并创新性提出“第三方独立安全运营”新模式。借助技术实力过硬的安全分析队伍，提供覆盖全行业全技术的安全能力，实现网络安全的可观、可管、可控。目前，集团已在成都建立了国内规模最大、最具专业实力的企业级运营中心，在青海建立了首个省级安全运营中心，此外，在济南、郑州、杭州、天津、昆明、广州、青岛等近 20 个城市均已开展了安全运营中心业务，帮助城市全面提升安全能力。

2. 深信服

2.1 深信服发布“卫信云”

3 月 23 日，由卫宁健康主办的 Winning World 2019 会议在广州顺利举办。本次会议以“新互联 • 新医态”为主题，汇聚了全国超过 1200 位医疗信息化行业专家，共同探讨“互联网+”新政下，移动互联技术为医疗信息化建设带来的全新改变。

深信服+卫宁健康=卫信云。深信服自 2018 年与卫宁健康缔结战略合作关系以来，在产品、方案整合、客户拓展方面展开了深入合作。 “卫信云”凝聚了深信服在安全、云计算、基础架构领域以及卫宁健康在医疗软件领域多年的研发经验，通过在代码层面的深度融合来实现深信服硬件和卫宁软件优良基因的完美契合，将两者的优势最大化。

“卫信云”具备如下特点：

1）实现业务标准化交付：对 HIS、集成平台等软件进行深度优化和功能适配，保障业务稳定性。

2）安全可靠：结合软件业务流及应用服务特性，融合了深信服的安全基因，系统具备原生的安全保护能力，确保业务安全。

3）稳定高效：系统采用全冗余设计、支持拉伸集群，组件故障对业务连续性无影响；一体化交付实现平台的统一管理，单人即可维护。

4）更高性价比：标准超融合配置可承载年门诊量约 100 万人次，其它模块可按需配置，比传统架构方案 TCO 降低 30%。

同时，深信服还于现场重点展示了桌面云／超融合解决方案、医院智慧安全大脑方案（态势感知安全平台／等级保护平台演示），并通过部署卫宁 HIS、PACS、全民信息健康平台等软件，向业界同行们直观地展现深信服硬件系统如何与卫宁软件深度融合，为医疗机构业务的应用打造极致稳定、安全、高效的场景解决方案。

3. 山石网科

3.1 山石网科 2019 获 CDM 3 大前瞻奖项

美国时间 3 月 6 日，美国知名网络安全杂志 Cyber Defense Magazine 为山石网科，颁发了包括：数据中心安全、网络安全分析、云安全等三个极具前瞻性和创新的重要奖项。山石网科全面的数据中心防护能力再次受到国际认可。

（一）最具创新数据中心安全产品（The Most Innovative Data Center Security for 2019）：山石网科数据中心安全防护平台 X10800

山石网科数据中心安全防护平台 X10800，是应用在数据中心边界，应对大流量、高可靠场景的数据中心级安全防护产品，具备电信级高可靠性的保障、强大的网络适应性、创新的分布式架构、领先的虚拟化防护技术以及面向未来的平台化设计。X10800 整机吞吐性能目前最大 1Tbps，新建连接速率 1000 万，并发连接数 4.8 亿，支持高达 400Gbps 的 IPS 防护性能，同时全面支持 IPv6。

（二）突破性安全分析解决方案（Breakout Cybersecurity Analytics for 2019）：山石网科 T 系列智能下一代防火墙

山石网科智能下一代防火墙，采用了全新的威胁检测技术，基于行为分析，准确发现变种恶意软件、内网异常行为等网络风险，从而弥补了传统检测技术的弊端。同时，智能下一代防火墙在威胁检测的基础上，提供了风险与网络攻击的可视化、策略联动实时风险减缓等功能，从而使安全防护成为闭环，为用户带来全新的安全体验。

（三）下一代云安全方案（The Next Gen Cloud Protection for 2019）：山石云·格

山石云·格是创新的分布式网络侧微分域产品，通过专利引流技术、虚机微分域及可视化技术，能够为用 户提供全方位的云安全服务，包括流量及应用可视化，虚机之间威胁检测与隔离，网络攻击、网络应用审计与溯源等，帮助政府、金融、运营商、企业等搭建安全、合规的“绿色”云平台。

4. 亚信

亚信安全解读 RSA2019

RSA 大会于美国当地时间 3 月 4 日在旧金山拉开帷幕，本次峰会共吸引全球 700 多家机构参展，其中近 42%为云安全和网络安全相关企业，在所有演讲主题中，云安全超过网络安全和数据安全，成为热门关键词第一。

亚信作为本次参展商之一，对本届会议的热点和安全趋势做了解读：

（一）数字世界中的信任问题

随着数字化的演进，如何确认对方在数字虚拟世界的身份、保证身份安全变得尤为重要，这对传统以威胁防御为主的安全厂商是一个不小的挑战。

（二）终端安全与机器学习相结合

与以往强调防护技术相比，机器学习作为安全防护技术的补充，在终端安全上运用相当普遍。EDR 技术在去年大热过后，今年也作为终端安全的标配，为应急响应提供了基础数据。我们还需要关注的是，由于传统的终端安全产品架构无法满足大量数据的收集与关联分析需求，我们这次在 RSA 大会上看到几乎 100%的 EDR 方案都是基于云的，其在国内如何落地是厂商和客户都要考虑的问题。

（三）基于云架构的安全产品和服务越来越普遍

MSSP(安全托管服务提供商)提供的服务随之更具备竞争力，其不仅能提供更高的安全价值，还帮助客户降低了运维成本，这一点在 RSAC 的展台上也得到证明，提供安全服务、安全运维的公司也随处可见。这是由于目前安全产品已经从威胁防护、未知威胁发现，逐渐过度到应急响应和溯源，一般企业的安全运维人员几乎没有能力完全满足这样的技术要求，所以企业对专业的安全运维人员需求将更加迫切。MSSP 作为企业的安全服务合作伙伴，无疑能很好的满足这个需求。

5. 绿盟

5.1 绿盟科技发布 EDR 新品

对于勒索病毒和挖矿木马来说，每天的变种数量呈指数级增长，而杀毒软件的病毒库更新的滞后性以及对未知威胁的“不敏感”使得传统杀毒软件无法应对这种场景。对于 APT 攻击来说，其非常重要的一个特征就是隐蔽性强、攻击特征难以提取，这就给基于已知特征进行检测的杀毒软件带来很大挑战。

面对终端安全的新态势，绿盟科技推出了新一代终端安全防护产品，绿盟终端检测与响应系统（NSFOCUS Endpoint Detection and Response 简称 NSFOCUS EDR），系统采用主动防御和横向对比模式，对非正常行为实时拦截和对可疑文件删除隔离，摆脱传统防病毒软件静态特征库对比的弊端。同时，系统能够帮助用户识别终端风险，并可对安全事件进行溯源分析。绿盟终端检测与响应系统(EDR)使企业的防御模式从静态、被动、基于规则的防御，逐渐转变为主动、动态、自适应的弹性防御，全面提升企业的安全防御能力。

Gartner 预测，到 2020 年有 80%的大型企业，25%的中型企业，以及 10%的小型企业将投资部署 EDR。国内 EDR 市场也已经进入高速发展期。

6. 安恒

6.1 安恒 AiLPHA 大数据智能安全平台获“2019 年度 SIEM 突破奖”

安恒信息 AiLPHA 大数据智能安全平台斩获 Cyber Defense Magazine（网络防御杂志，以下简称 CDM 杂志）所颁发的“Breakout Security Information Event Management (SIEM) InfoSec Award for 2019”奖项（2019 年度 SIEM 突破奖）。

当前安全形势错综复杂，未知威胁、高级的持续性不断的增加并成为主流，企业通常疲于应对甚至无能为力。AiLPHA 大数据智能安全平台采用大数据技术和智能学习算法，将客户海量的安全数据以多副本的方式，分布在多个计算节点上，充分发挥多台服务器的计算能力，同时规避单台计算机的不可靠性，面对海量数据的挖掘、分析和建模能力，对安全能力提供支撑和保障。真正从用户的资产出发，打破传统的信息数据孤岛式分布，最终为用户安全提供：实时预警、亿级存查、异常检测、智能学习、深度关联、追踪溯源等服务内容。为企业用户提供全局安全态势感知能力和业务不间断稳定运行的安全保障，提高整个安全管理体系的安全态势感知预警能力，为用户信息系统安全提供全方位支撑。

目前，AiLPHA 大数据智能安全平台已被广泛应用于政府、金融、运营商、媒体、教育、高校、公安等单位或企业的内网、外网、专网等复杂网络环境，为用户提供全局安全态势感知能力，为业务提供不间断稳定运行安全保障，为信息系统安全决策提供数据支撑。

7. 360

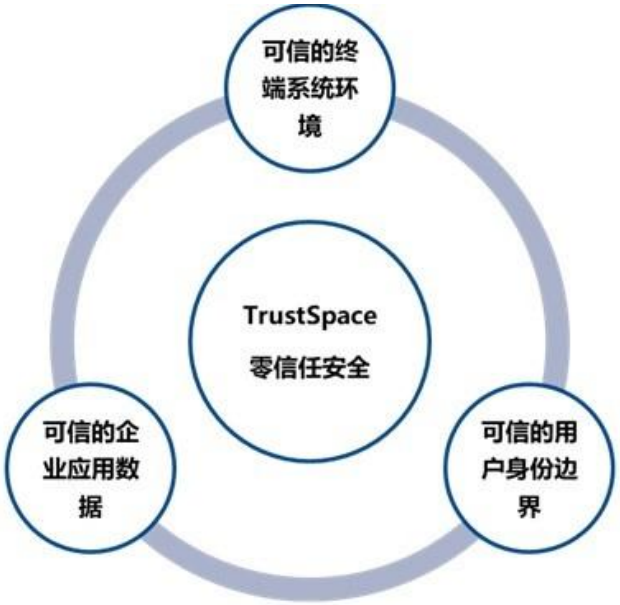
7.1 360 企业安全发布基于“零信任”的数字化工作空间白皮书

近期，360 企业安全集团与 Gartner 经过数月的市场调研和需求分析，联合发布了《TrustSpace，基于“零信任”的数字化安全工作空间》白皮书。360 企业安全和 Gartner 认为，当前移动化面临的安全困境迫切需要一种全新的安全架构和解决方案，而“零信任”架构以及基于零信任架构的数字化工作空间解决方案从终端可信、消除边界、动态授权等角度出发，能够完美解决移动办公场景下带来的诸多安全问题。

《TrustSpace，基于“零信任”的数字化安全工作空间》白皮书提出了未来企业移动安全的几个重要趋势：趋势一，设备管理不再是企业关注的重点，企业更多关注的是如何安全高效的交付移动应用程序以及如何保护企业数据。趋势二，BYOD 以及高合规性的行业场景（如政府、金融等）对于移动威胁防御的需求越来越强烈。趋势三，多因素身份认证、动态的身份授权以及统一的身份管理正在成为企业移动安全考虑的重点。趋势四，员工个人隐私的保护以及移动办公用户体验，逐渐受到企业 IT 高层关注。

基于此，360 企业安全和 Gartner 为企业提出了以下重要战略建议：建议一，将原来的以设备为核心的移动管理战略升级为以用户为核心的工作空间战略。建议二，构建一个全新的移动安全模型来应对工作空间战略下的安全以及合规性挑战。建议三，充分考虑 BYOD 和 COPE 两种设备场景在安全管理和用户隐私方面的差异，并制定差异化的安全策略。

360TrustSpace 安全工作空间是在 360 企业安全发布的基于零信任架构的移动安全解决方案，其基本理念是在移动化场景下，从 IT 管理者和最终用户的双重视角出发，以设备、人、应用三个维度，构建基于 TrustSpace 的系统环境、身份边界、应用数据三级信任体系，让移动办公对于 IT 管理者来说变得安全可信；通过设备零管理、隐私零收集、使用零成本三种方法，消除移动用户的隐私担心，激发最终用户的移动办公活力，从而实现全面激活 BYOD。



8. 安天

8.1 超两成有效移动杀毒软件采用安天反病毒引擎

2019 年 3 月 12 日，世界知名测评机构 AV-Comparatives 发布了其对谷歌官方应用商店（Google Play）上架的全球 250 款杀毒软件防护能力的测评报告。报告指出，大约三分之二的安卓杀毒软件都不能实现广告宣传中的杀毒功能，其病毒检出率竟低于 30%，根本无法为用户提供有效防护。在此次测试中安天（Antiy）和另一家国内厂商腾讯，与卡巴斯基、赛门铁克等国际厂商均取得了检出率 100%的满分成绩。值得一提的是，在检出率超过 85%的有效杀毒软件中，有超过两成采用了安天反病毒引擎。充分证明了安天在反恶意代码和移动安全领域的重要的基础地位。

Test Results

Vendor	%	Vendor	%	Vendor	%
AhnLab	100%	eScan	99.80%	Alibaba	92.90%
Antiy		Ikarus		Tapi	92.40%
Avast		Quick Heal		IntelliAV	91.80%
AVG		REVE		Panda	91.60%
AVIRA		Securion		Dr. Web	90.80%
Bitdefender		VIPRE		Privacy Lab	89.90%
BullGuard		Lookout	99.60%	Zoner	88.90%
Chili Security		Supermobilesafe		APUS	87.80%
Emsisoft		BSafe	99.50%	CAP Lab	
ESET		MyMobile		Clean Boost+	
ESTSoft		Malwarebytes	99.40%	Fotoable	
F-Secure		CheckPoint	99.10%	Hyper Speed	
G Data		K7		IOBit	
Kaspersky Lab		Qihoo	99.00%	ONE App	
McAfee		Hi Security	98.60%	Phone Clean	
PSafe		NSHC	98.40%	Power Tools	
Sophos		AegisLab	98.30%	Smooth Apps	
STOPzilla		Samsung	97.70%	Super Cleaner	
Symantec		Webroot	97.40%	Super Security	
Tencent		Zemana	97.30%	We Make It Appen	
Total Defense		Hawk App	97.10%		
Trend Micro		TrustGo	96.00%		
Trustwave		DU Apps	94.70%		

2006 年起，安天先后将反病毒引擎技术授权给美国等其他发达国家安全厂商使用，成为中国早期实现核心技术授权出口欧美的安全厂商。安天 AVL SDK 反病毒引擎先后获得了科技部创新基金、863 计划和发改委信息安全专项支持。

9. Fortinet

暂无消息。

10. Checkpoint

暂无消息。

四、 容器技术及安全动态

1. Kubernetes 1.14 发布

新版本由 31 项增强功能组成，具体包括：10 项稳定版功能，12 项 beta 测试功能，以及 7 项全新功能。此次版本的核心主题在于可扩展性，以及在 Kubernetes 上支持更多工作负载。本轮共有三项主要功能迎来通用版本，另有一项重要安全功能步入 beta 测试阶段。

对 Windows 节点的生产级支持

在此之前，Kubernetes 当中的 Windows 节点一直处于 beta 测试阶段，旨在允许众多用户以实验性方式体验 Kubernetes for Windows 容器的实际价值。如今，Kubernetes 开始正式支持将 Windows 节点添加为工作节点并部署 Windows 容器，从而确保庞大的 Windows 应用程序生态系统得以利用我们平台提供的强大功能。

本次 Kubernetes 为 Windows 容器带来的核心功能特性包括：

- 支持将 Windows Server 2019 引入工作节点与容器
- 支持采用 Azure-CNI、 OVN- Kubernetes 以及 Flannel 的树外网络
- 改进了对 Pod、服务类型、工作负载控制器以及指标/配额的支持能力，以便与 Linux 容器的自有功能实现更为紧密的匹配。

Kubectl 更新

Kubectl 的说明文档完全重写，其重点在于利用声明性 Resource Config 实现资源管理。文档目前以独立站点的形式发布，采用电子书格式，并在 k8s.io 文档中提供对应链接（具体请访问 https://kubectl.docs.kubernetes.io）。

Kustomize 的声明性 Resource Config 创作功能现在可以通过-k 标记（适用于 apply 及 get 等命令）以及 Kustomize 子命令在 kubectl 中获取。Kustomize 旨在帮助用户创作及复用包含 Kubernetes 各原生概念的 Resource Config。用户现在能够利用 kubectl apply -k dir/将拥有 kustomization.yaml 的目录适用于集群。此外，用户也可以将定制化 Resource Config 发送至 stdout，而无需通过 kubectl kustomize dir/加以应用。这些新的功能被记录在新的说明文档当中，具体请参阅：https://kubect.docs.kubernetes.io。

通过 Kubernetes 的 kustomize repo 对 Kustomize 子命令进行开发。最新的 Kustomize 功能将以独立的 Kustomize 二进制文件（发布至 kustomize repo）的形式更为频率地发布，且在每一轮 Kubernetes 发布之前在 kubectl 中得以更新。

kubectl 插件机制逐步趋于稳定:kubectl 插件机制允许开发人员将自己的定制化 kubectl 子命令以独立二进制文件的形式发布出来。这些成果将可帮助 kubectl 与附加 porcelain（例如添加 set-ns 命令）实现更多新的高级功能。

持久本地卷迎来通用版本

这项功能正逐渐稳定，允许用户将本地连接存储作为持久卷来源。考虑到实际性能与成本要求，分布式文件系统与数据库往往成为持久性本地存储的主要用例。与云服务供应商相比较，本地 SSD 一般可提供超越远程磁盘的性能水平。而与裸机方案相比，除了性能之外，本地存储通常成本更低，亦是配置分布式文件系统的一项必要条件。

PID 限制正转向 beta 测试阶段

在目前的 beta 功能中，管理员可以对每个 Pod 中的 PID 数量进行预定义，从而实现 Pod 与 Pod 间的 PID 隔离。此外，管理员还可以通过 node allocatable 为用户 Pod 保留大量可供分配的 PID，即以 alpha 测试功能的方式实现类似的 Pod 与 Pod 间 PID 隔离。

更多其它值得关注的功能

Pod 优先级与抢占机制使得 Kubernetes 调度程序能够首先调度更为重要的 Pod，从而在集群资源不足时删除不太重要的 Pod，最终为意义更重大的 Pod 保留运行空间。具体重要性由优先级机制负责指定。

Pod Readiness Gates 能够为 Pod 的就绪情况提供外部反馈扩展点。

强化默认的 RBAC 的 clusterrolebingdings 发现能力，其移除了原本默认可通过未授权访问的 API 集发现功能，旨在提升 CRD 隐私性以及默认集群的总体安全水平。

2. Istio 1.1 正式发布

新版本注重在企业生产环境的就绪能力，关注的主要方向之一正是性能与可扩展性，以提升数据平面与控制平面的执行效率。测试结果：https://istio.io/docs/concepts/performance-and-scalability/

新版本也完成了命名空间隔离的工作。这使您可以使用 Kubernetes 命名空间来强制控制边界，并确保您的团队不会相互干扰。

在改进了多集群功能和可用性。我们听取了社区的意见，并改进了交通管制和政策的默认设置。我们引入了一个名为 Galley 的新组件。Galley 负责验证 YAML 以降低发生配置错误的可能性。另外，Galley 还能够在多集群设置当中发挥作用，从各个 Kubernetes 集群当中

收集服务发现信息。再有，我们还支持其它多集群拓扑结构，包括在无需扁平网络的前提下实现单一控制平面与多个同步控制平面。

3. 云原生计算基金会宣布 containerd 项目正式毕业

时至今日，containerd 已经成为阿里云、AWS、Cloud Foundry、Docker、谷歌、IBM、Rancher Labs 以及更多生态系统支持方们采用范围最广的容器运行时选项。

云原生计算基金会日前宣布，继 Kubernetes、Prometheus、Envoy 以及 CoreDNS 之后，containerd 已经成为其第五个毕业项目。事实上，要从孵化阶段一步步发展成熟至毕业水平，这些项目必须表现出活跃的采用度、良好的多样性、规范的治理过程，以及对社区可持续性与包容性的坚定承诺。

诞生于 2014 年的 containerd 最初由 Docker 所打造，旨在为 Docker 引擎提供低层运行时管理器。而在 2017 年 3 月被纳入云原生计算基金会之后，containerd 已经逐步发展成一款行业标准性质的容器运行时方案。此项目始终强调简单性、健壮性与可移植性，目前被广泛用作 Docker 引擎与 OCI runc 执行器之间的对接层。

为了正式由孵化阶段走向毕业，containerd 项目遵循云原生计算基金会提出的基本原则，接受独立的外部安全审计，并确定了自身治理结构[2]以保障社区发展。此外，containerd 还获得并保有核心基础设施倡议最佳实践徽章[3]（简称 CII 徽章）。这项成就于 2018 年 9 月 1 日正式达成，CII 徽章[4]代表着整个社区对于代码质量与安全最佳实践做出的不懈承诺。

containerd 项目背景信息：

- containerd 是一套行业标准化容器运行时，强调简单性、健壮性与可移植性。Containerd 可作为 Linux 与 Windows 系统中的守护程序。
- containerd 管理其所在主机系统上的整个容器生命周期——从镜像传输到存储、到容器执行与监督，再到底层存储乃至网络附件等等。
- containerd 项目： https://github.com/containerd/containerd。

五、 安全新产品及技术

1. W3C 批准 WebAuthn 成为无密码登录的 Web 标准

万维网联盟（W3C）近期宣布，Web 身份验证 API（WebAuthn）现在已成为官方 Web

标准。 WebAuthn 于 2015 年 11 月由 W3C 和 Fido 联盟宣布，现已成为网上无密码登录的开放标准。它由 W3C 贡献者支持，包括 Airbnb、阿里巴巴、苹果、谷歌、IBM、英特尔、微软、Mozilla、PayPal、软银、腾讯和 Yubico。

该规范允许用户使用生物特征、移动设备和/或 FIDO 安全密钥登录在线帐户。Android 和 Windows10 已经支持 WebAuthn。在浏览器方面，谷歌 Chrome、Mozilla Firefox 和微软 Edge 浏览器去年都开始支持 WebAuthn。自去年 12 月以来，苹果就在 Safari 的预览版中支持 WebAuthn。

2. Axonius 获得创新沙盒冠军

美国当地时间 3 月 4 日（北京时间 3 月 5 日凌晨左右），RSA 2019 大会在旧金山正式开幕。备受关注的创新沙盒竞赛也在当天举行。据最新消息显示，主打网络资产管理的 Axonius 公司在十个入围项目中表现突出，获得了创新沙盒的冠军。

Axonius 的主打产品是网络安全资产管理平台，该平台主要帮助用户梳理工作网络中存在哪些资产和设备，确认是否符合该单位的安全保护要求。这个平台可以为用户和资产提供可操作、可视化的方案，并协助策略执行，能提供 100 多种管理和安全解决方案。连纽约时报这样的大公司都在使用 Axonius 来确保资产安全。

3. App 收集使用个人信息必须有法律依据

人民日报刊文称，App 收集使用个人信息，需要遵循合法、正当、必要的原则。报道称，中国消费者协会发布的《100 款 App 个人信息收集与隐私政策测评报告》表明，被测评的 App 普遍存在涉嫌过度收集或使用个人信息的情况，且其中用户协议的隐私条款存在瑕疵。

对此，中央网信办等四部门决定自 2019 年 1 月至 12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理。报道指出，App 收集使用个人信息，需要遵循合法、正当、必要的原则。

4. 9 款违规 App 曝光：涉及恶意扣费、隐私窃取、赌博

据网信广东消息，国家计算机病毒应急处理中心近期在净网行动中通过互联网监测发现，9 款违法有害移动应用存在于移动应用发布平台中，其主要危害涉及恶意扣费、隐私窃取、赌博三类。

这些违法有害移动应用具体如下：

1、《PhotoLoop》（版本 20.4）、《快对答案》（版本 7.9.0）这两款应用存在扣费恶意代码，通过隐蔽等手段，导致用户经济损失。

2、《蓝贷》（版本 1.0）、《吃鸡神助攻》（版本 2.2.0）这两款应用存在危险行为代码，警惕该应用私自下载安装软件，窃取用户隐私信息，造成用户隐私泄露、资费消耗。

3、《Remember Everything-数字记忆》（版本 1.1.0）、《大菠萝-线上平台》（版本 1.0）、《炸金花-全民真人炸金花欢乐版》（版本 1.0）、《Cuncaoxin Education》（版本 1.0.6）、《银河娱乐》（版本 1.1）这五款移动应用涉及赌博，通过押点数、斗牌、博彩等形式进行含有赌资往来的赌博活动，涉及违法并存在财产风险。

5. ISACA 发布针对区块链、CASB 和 GDPR 的全新审计程序

审计人员面临着将新技术、新系统和新法规纳入评估程序的挑战。国际信息系统审计协会（ISACA）推出全新的审计程序，为审计人员提供了额外的工具包框架，以便为区块链、云访问安全经纪人（CASB）和欧盟 GDPR 提供审计支持。

该计划涵盖区块链的所有方面，从实施前、治理、开发、安全、交易和共识，指导审计人员确定和制定关键政策，程序和控制，旨在在区块链实施之前降低风险和简化流程，并包括区块链技术审计准备计划工作表。为了帮助 IT 审计人员评估 CASB 解决方案的有效性，ISACA 发布了云安全访问经纪人（CASB）审计计划。企业通常使用 CASB 来管理风险，例如与各种部署模型、身份管理以及数据合规相关的风险。ISACA 为中小企业审计提供了一个审计框架，用于评估 GDPR 的管理，监控和管理的有效性。

6. 谷歌开源内部沙箱安全策略 Sandboxed API

谷歌宣布称将开源 Sandboxed API 以促使软件开发人员更容易地创建安全的产品。应用程序受内存损坏或其它类型漏洞影响从而导致远程代码执行或其它后果的情况并不少见。使用沙箱能够确保负责处理用户输入的代码智能访问需要访问的资源，从而通过将利用代码限制到受限环境中并阻止它和其它软件组件交互的方法缓解缺陷的影响。

虽然沙箱能够发挥重大作用，但谷歌表示通常实现起来并不容易。这也是谷歌决定开源其 Sandboxed API 的原因，它应当能够更容易地对 C 和 C++ 库进行沙箱操作。谷歌还开源了其核心沙箱项目 Sandbox2，它可用于确保 Linux 处理器的安全。谷歌 ISE 沙箱团队

成员解释称，“Sandboxed API 使得为单个软件库创建安全策略成为可能。这种理念能够创建存在于流行软件库中的可复用且安全的功能实现，而且也具有足够的颗粒度保护余下所使用软件基础设施的安全。”

7. Facebook 数亿用户密码被发现在内部数据库明文保存

KrebsOnSecurity 援引匿名消息来源披露，Facebook 有数亿用户的密码被发现明文保存，允许公司雇员搜索和访问。社交巨人随后发表声明证实确有此事。Facebook 称今年一月它在例行安全检查中发现部分用户密码以可读模式保存在内部的存储系统。它已经修复了问题并将会通知受影响的用户。Facebook 声称这些明文保存的密码对外部人员是不可见的，它没有发现有证据显示公司内部人士滥用或不恰当的访问了这些密码。受到影响的用户包括了数亿 Facebook Lite 用户，数千万 Facebook 用户，数万 Instagram 用户。Facebook Lite 是为网络连接状况不佳的地区用户提供的 Facebook 版本。

8. UC 浏览器存在中间人攻击(MITM)漏洞，可能影响十多亿设备

研究人员发现 UC 浏览器中存在易受攻击的功能模块，可被攻击者利用执行中间人攻击。由于 UC 浏览器采用 HTTP 协议与服务器通信，传输的信息没有经过加密，所以会被攻击者 hook 来自应用程序的请求，并将命令和链接替换为恶意地址，导致从 UC 浏览器下载模块时，会下载来自恶意服务器的内容。而 UC 浏览器本身使用未签名的插件，因此没有任何验证就可能启动恶意模块。攻击者可以利用这种机制，使用 UC 浏览器分发、执行不同的恶意插件，甚至利用木马访问受保护的浏览器文件并窃取存储在程序目录中的密码。UC 浏览器有十几亿下载量，相关设备都可能暴露在风险之中。

六、 网络安全投融资、收购事件

1. 收购

1.1 Verizon Communications 完成对 ProtectWise 的收购

3 月 1 日，Verizon Communications 完成对 ProtectWise 的收购，收购价未公开。Verizon(VZ)是全美第二大移动运营商，仅次于 AT&T。主要业务是：语音通话、固定宽带和无线通信。

ProtectWise 是一家信息安全初创企业，开发了一种平台，使得安全人员能够获得自身网络的整体概况，即使在没有注意到入侵早期征兆的情况下。该平台由 ProtectWise 公司开发，这是美国丹佛市的一家新兴安全企业，目前有三十名员工。自从 2013 年 4 月创立以来，该公司一直没有发声，直到最近才开始披露其技术信息。ProtectWise 的发展方向是整合大量的企业级威胁探测产品，它开发了一套名 ProtectWise Cloud Network DVR 的系统，该系统由一系列轻量级探测装置组成，使用时这些探测器将被部署在网络的各个角落，记录网络数据，将其加密并传到亚马逊云上，ProtectWise 在云端进行多种分析，以检测是否存在威胁。

2. 投融资

2.1 eSentire 获 4700 万美元私募股本融资

3 月 4 日， eSentire 从 Edison Partners 和其他 2 位投资者处处获得 4700 万美元的私募股本融资。eSentire 提供信息安全解决方案，保护企业免受高级网络威胁。通过基于行为的解决方案，eSentire 专注于保护网络内的核心资产，重新创造了企业网络安全。

2.2 LogRocket 获 1100 万美元 A 轮融资

3 月 21 日，LogRocket 从 Battery Ventures 和 Matrix Partners 处获得 1100 万美元的 A 轮融资。LogRocket 用日志和网络数据记录用户会话的视频，识别用户体验问题并揭示每个 bug 的根源。

2.3 Attivo Networks 获未知数额的 C 轮融资

3 月 21 日，Attivo Networks 从 Bain Capital 和其他 3 位投资者处获得未知数额的 C 轮融资。Attivo Networks 是一家网络安全公司，其采用诱骗技术来检测、调查和帮助缓解已存在网络中的攻击，帮助用户网络、数据中心、云端、SCADA、物联网和销售终端组织恶性攻击，消除网络隐患。

2.4 CyberX 获 1800 万美元的公司轮融资

3 月 25 日，CyberX 从 Flint Capital 和其他 5 位投资者处获得 1800 万美元的公司轮融资。CyberX 是一家网络安全技术公司，通过对运营网络的完全可视化，实时检测网络和运营事故。