国内外云计算+安全动态报告

2018 年第 8 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 在安全能力上进行了加强，可以使用 AWS Key Management Service (KMS) 来管理 AWS Storage Gateway 存储在云中的数据的加密，AWS Shield Advanced 支持新警报类型，推出 AWS IoT Device Defender，同时新增了多项支持，如在 AWS 中国（宁夏）区域提供 Aurora 支持，Amazon ECS 支持 Docker 卷和卷插件，Amazon EKS 现支持启用了 GPU 的 EC2 实例，AWS Config 新增了为配置项指定数据保留策略的功能，AWS Key Management Service 增加每秒 API 请求限额；VMware 公布第二财季报告，收入达 21.7 亿美元，同比增长 13%；谷歌云服务正与腾讯、浪潮商谈合作计划打入国内市场，增加新的图形加速器可支持 AI 和虚拟桌面工作负载，并且谷歌将在云平台上集成 AI 服务，首批曝光联络中心 AI、云人才解决方案、推荐解决方案三个项目；微软在 Azure 上推出以太坊授权验证算法；中国联通与阿里成立云粒智慧科技，关注金融生态等领域，阿里云新发布九款云产品与 AWS 等展开竞争，并且阿里云服务拿下数字重庆，还要布局区块链服务；腾讯云、腾讯 WeTest 和英特尔合作布局云游戏，长亮科技携手腾讯云发布“银户通” 助银行提升用户连接力，腾讯云企业客户数据丢失，赔偿意见存千万元分歧；华为发布云管理网络 2.0，即日起免费试用。

开源云方面，SUSE OpenStack Cloud 助力 TCS 企业云平台；京东云战略投资 EasyStack；牛商网携手九州云,构建新型互联网业务平台。

云安全厂商方面，启明星辰受邀参加中国网络安全年会，多项新技术研究成焦点，且携手守护者计划抵制网络诈骗；东软 RealSight APM 云应用性能监控提

案纳入 TOSCA 标准；山石网科、瑞星、VMware 共推云计算安全整体解决方案；亚信安全与新华三合作；安恒信息在区块链领域布局。

容器动态方面，华为云全球首发 GPU 共享型 AI 容器，已在华为云的 CCE 容器服务中开展公测。提供统一化的微服务连接、安全保障、管理与监控方式的 Istio 1.0 正式版发布，可用于生产环境。IBM 发布专为安全性设计的容器-Nabla。Prometheus 项目于 CNCF“毕业”，是继 Kubernetes 之后的第二个 CNCF 毕业项目。谷歌推出 K8S 二进制授权，确保只有授信的 workload 部署到 k8s 集群。

安全新技术方面，顺丰上线下单“隐址件”，收寄双方均看不到对方信息；新漏洞层出不穷，8 月安卓安全补丁发布共计修复 43 处漏洞，微软 Cortana 出现漏洞，即使系统锁定也能使用浏览功能，英特尔处理器曝出新漏洞；新型钓鱼攻击 PhishPoin 出现，可以绕过 Microsoft Office 365 保护。

网络安全公司投融资方面，共发生 1 起收购和 5 起投融资事件。老牌网络厂商 Cisco 以 23.5 亿美元的价格收购企业级移动认证安全服务商 Duo Security。投融资方面相较上半年热情下滑，其中针对虚拟容器提供安全技术的初创企业 Twistlock 以 3300 万美元的 A 轮融资拔得头筹，第三方软件风险评估厂商 RiskRecon 以 2500 万美元的 B 轮融资位列第二，其他 3 起投资事件均未超过千万美元。

2018 年 8 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 AWS Storage Gateway 提高加密功能

8 月 1 日，现在可以使用 AWS Key Management Service (KMS) 来管理 AWS Storage Gateway 存储在云中的数据的加密。AWS KMS 是一项托管服务，可轻松创建和控制用于加密您的数据的加密密钥。Storage Gateway 现在支持使用 AWS KMS 加密所有网关类型存储在 AWS 中的数据。这包括由磁带网关管理的虚拟磁带、由卷网关创建的云内卷和 EBS 快照，以及由文件网关将其作为对象存储在 Amazon Simple Storage Service (S3) 中的文件。

如果用户未使用 AWS KMS，Storage Gateway 服务存储在 AWS 中的所有数据均默认使用 Amazon S3 托管的加密密钥 (SSE-S3) 进行加密。除了静态加密之外，在任何类型的 Storage Gateway 和 AWS 之间传输的所有数据都使用 SSL 加密。

1.2 AWS IoT Device Defender 现已全面推出

8 月 2 日，在 AWS re:Invent 2017 上，AWS 发布了 AWS IoT Device Defender，这是一项完全托管的服务，可帮助保护 IoT 设备队列。今天，AWS 宣布全面推出 AWS IoT Device Defender。可以使用 AWS IoT Device Defender 来遵循推荐的安全最佳实践、持续监控设备行为并接收提醒，以便了解何时调查和解决安全问题。

AWS IoT Device Defender 会审计设备相关的 IoT 资源的配置，以确保不会背离安全最佳实践，用户能够轻松维护和实施安全的 IoT 配置，例如建立独特的设备身份、使用有效的证书进行识别，以及防止权限过度宽松的访问。AWS IoT Device Defender 还允许监控设备是否存在意外行为和异常，这可能预示着设备受损。AWS IoT Device Defender 会发出提醒，以便采取相应措施来解决任何潜在的问题。

1.3 Amazon Aurora 由西云数据运营的 AWS 中国（宁夏）区域提供

8 月 6 日，Amazon Aurora 现已面向由西云数据运营的 AWS 中国（宁夏）区域中的客户提供。Aurora 是为云构建的一种兼容 MySQL 和 PostgreSQL 的关系数据库，它既具有

高端商用数据库的性能和可用性，又具有开源数据库的简单性和成本效益。

Aurora 可提供高出典型 MySQL 数据库多达五倍的性能表现，以及高出典型 PostgreSQL 数据库多达三倍的性能，同时提高了可扩展性、耐用性和安全性。有关更多信息，请访问 Amazon Aurora 产品页面，并参阅文档。请参阅 AWS 区域表，了解完整的区域可用性信息。

1.4 AWS Config 新增了为配置项指定数据保留策略的功能

8 月 7 日，AWS Config 现在允许通过为配置项指定保留期的方式删除数据。如果指定了保留期，AWS Config 会将用户的配置项保留该指定期限。可以选择的期限最短是 30 天，最长是 7 年（2557 天）。AWS Config 会自动删除超过指定保留期的配置项。如果没有指定保留期，AWS Config 会继续将配置项保留 7 年（默认期限，即 2557 天）。

此功能已在所有提供 AWS Config 的 AWS 商业区域以及 AWS GovCloud（美国）区域推出。要查看支持的区域的完整列表，请参阅 AWS 一般参考中的 AWS 区域和终端节点。

1.5 Amazon ECS 现在支持 Docker 卷和卷插件

8 月 9 日，现在可以使用 Docker 卷驱动程序和卷插件（如 Rex-Ray 和 Portworx）轻松配置容器化应用程序，使其访问由本地实例存储支持的存储卷、Amazon Elastic Block Storage (EBS) 或 Amazon Elastic File System (EFS) 卷。

以前，如果想部署需要访问存储卷的容器化应用程序，必须通过使用自定义工具（如 Bash 脚本）、Lambda 函数以及手动配置 Docker 卷来手动管理存储卷。

现在，得力于对 Docker 卷的支持，可以在 Amazon ECS 上部署有状态的存储密集型应用程序。可以灵活配置 Docker 卷的生命周期，并指定它是一个特定于对任务进行单一实例化的暂存空间卷，还是一个在任务的独特实例化生命周期结束后继续存在的持久卷。还可以使用您在启动任务之前创建的预配置 Docker 卷。

1.6 AWS Shield Advanced 支持新警报类型

8 月 16 日，使用 AWS Shield Advanced 可以在升级的入门向导中轻松创建基于速率的规则 (RBR)。另外，还可以在向导中通过服务发布的分布式拒绝服务 (DDoS) 指标快速设置 Amazon CloudWatch 警报，从而更好地监控受保护资源。

AWS Shield Advanced 在入门向导中增加了两种新功能，该向导是帮助设置 DDoS 防护的分步工具。如果选择保护 Application Load Balancer 或 Amazon CloudFront 分发，该向导将帮助设置简单的 Layer 7 防护。首先，需要通过选择一个现有的 Web ACL 或创建一个新的，以指定一个 AWS WAF Web 访问控制列表 (ACL)。然后，可以通过选择现有规则或通过控制台创建一个新规则，以便将基于速率的规则添加到 Web ACL。

此外，向导还可以使用 Amazon CloudWatch 警报帮助监控受保护的资源。如需创建一个警报，可以为正在受保护的资源指定一个 Amazon Simple Notification Service (SNS) 主题。可以选择一个现有的主题或使用向导创建一个新的。设置完成后，只要服务发出 DDoSDetected Amazon CloudWatch 指标，就会收到通知。

1.7 AWS Key Management Service 增加每秒 API 请求限额

8 月 21 日，AWS Key Management Service (KMS) 增加了一组核心 KMS API 操作的请求速率限额，这些操作包括 Decrypt 、 Encrypt 、 GenerateDataKey 、 GenerateDataKeyWithoutPlaintext、GenerateRandom 和 ReEncrypt。在美国东部（弗吉尼亚北部）、美国西部（俄勒冈）和欧洲（爱尔兰）地区，请求速率限额从每秒 1,200 个请求增加到了每秒 10,000 个请求。在所有其他提供 KMS 的区域，限额增加到每秒 5,500 个请求。这些限额提升可以更轻松地扩展 KMS 操作。

1.8 Amazon EKS 现支持启用了 GPU 的 EC2 实例

8 月 23 日，Amazon Elastic Container Service for Kubernetes (EKS) 现在支持在启用了 GPU 的 EC2 实例上运行容器。

采用 NVIDIA GPU 的 Amazon EC2 P3 和 P2 实例可以为计算型工作负载提供支持，包括机器学习 (ML)、高性能计算 (HPC)、财务分析和视频转码。以前，使用 Kubernetes 在 P2 和 P3 EC2 实例上运行容器化工作负载需要自定义 EKS 优化型 Amazon 系统映像 (AMI)，以包含相应的 GPU 驱动程序。

现在，新的 Amazon EKS 优化型 AMI 包括为启用了 GPU 的 P2 和 P3 EC2 实例配置的 NVIDIA 驱动程序。这样一来，使用 Amazon EKS 运行需要启用了 GPU 支持的高级工作负载就非常容易。

2. VMWare 云安全动态

2.1 VMware 公布第二财季报告

8 月 24 日，VMware 公布了第二财季报告，收入和每股收益均超出预期，有力地回击了此前关于 VMware 核心计算虚拟化产品走向衰落的预测。不仅如此，VMware 也提高了第三财季和全年业绩指引，主要是客户对于 VMware 与 AWS 以及 IBM 达成合作伙伴关系做出了积极的响应，并且也在采用 VMware 新推出的混合云产品。

VMware 在第二财季收入同比增长 13%，达到 21.7 亿美元，超过分析师此前预测的 21.5 亿美元。许可收入增长了 15%，达到 9 亿美元。该季度 VMware 的净收入为 6.38 亿美元，或每股摊薄收益 1.54 美元，较去年同期增长 14%，超出分析师的预期以及 VMware 自己每股 1.49 美元的指引。VMware 密切关注的经营利润率以及现金流量也在增长。VMware 表示，所有主要产品类别的产品许可预订均实现了两位数的同比增长，甚至虚拟化收入也以高个位数增长。VMware 预计会继续保持收入的低两位数的增长。VMware 将当前季度的收入预测上调至 22 亿美元，比去年同期增长 11%，2019 财年总收入预期为 82.8 亿美元，增长 12%。“我们对今年剩余这几个月的许可收入和总收入感到满意，”VMware 首席财务官 Zane Rowe 这样表示。

用于内部部署的 vSphere 许可销售继续保持强劲增长，同时 NSX 网络虚拟化平台等新战略领域也在快速增长。VMware 首席执行官 Pat Gelsinger 表示，该季度 NSX 许可销售额增长了 40%，该平台已被 82 家财富 100 强企业采用。“他们很快就会看到 NSX 将成为软件定义网络的标准。”

此外，VMware 还推出了一项新的 VMware 云提供商计划，包括一套 VMware 云产品和第三方产品。Gelsinger 表示，该季度 VCCP 收入增长了 30%，其中大部分销售都包含 vSphere。他补充说，与 AWS 有着近两年的合作伙伴关系是非常有吸引力的。“我们在这个平台上有数百个付费客户，并且第二季度结束时发展势头有所回升。”与 IBM 的合作也吸引了近 1700 家客户。

新业务的另一个动力是客户的态度正在明显从云端转移到数据中心。IDC 最近报告称，有 80%的云采用者已经或者计划将一个或多个工作负载从公有云环境迁移到本地，出于安全性、性能和数据所有权等考虑因素。

3. GOOGLE 云动态

3.1 谷歌云服务计划打入国内市场，正与腾讯、浪潮商谈合作

8 月 3 日，根据彭博社报道，谷歌正在与腾讯、浪潮等国内几家科技巨头展开合作，打算在中国布局自己的云服务。

据知情人士透露，谷歌正积极与腾讯、浪潮等国内公司展开商谈，目的是通过国内的数据中心和中国企业的服务器来运行谷歌的互联网服务，例如谷歌云盘（Drive）和谷歌文档（Docs），这和其它美国云公司进入中国市场的方式很相似。在中国以外的其它大部分区域，谷歌云在互联网上提供计算资源和存储，并出售一套在其数据中心运行的办公应用——G Suite。但中国要求服务商将数字信息保存在国内，而谷歌在大陆并没有数据中心，因此它需要和本地企业合作。这场商谈始于 2018 年初。今年 3 月下旬，谷歌将候选合作伙伴缩小为三家企业。但鉴于中美之间紧张的贸易局势，该计划是否会进行下去尚不得而知。

谷歌云总裁 Diane Greene 在上周说道，她希望将谷歌云打造成「全球云」，但拒绝透露关于中国业务的具体细节。为拓展云业务，该公司正在招聘上海业务发展经理。相关招聘信息中把「中国市场的丰富经验和知识」列为优先条件。一位谷歌云发言人拒绝对此作出评论。浪潮和腾讯发言人也没有立即回应彭博社的置评请求。

谷歌在中国的云合作伙伴关系将有助于该公司与亚马逊和微软展开更多竞争。与腾讯、浪潮等中国大型科技公司的合作会给谷歌带来强大的盟友，但同时也将面临和本地企业的竞争，包括阿里巴巴，后者的云业务在中国市场占有很大份额。

在此之前，谷歌与腾讯已经展开了云服务相关的合作。腾讯官网显示，该公司运营着自己的云服务，而且正在搭建一个包括思科、英伟达、德勤在内的合作伙伴生态系统。其目前提供的云服务名为「Tencent Kubernetes」引擎，该服务基于一项流行的谷歌同名技术。

如果这次合作得以实现，谷歌可以在腾讯数据中心运行 Gmail、Drive 和 Docs，腾讯可能建议现有的云用户尝试谷歌的产品。此外，谷歌推出的人工智能应用编码库 Tensorflow 在国内的研究者、软件开发者中越来越受欢迎。虽然该编码库与其他云服务兼容，但它与谷歌的云计算进行协作效率最高。

3.2 谷歌云增加新的图形加速器 可支持 AI 和虚拟桌面工作负载

8 月 7 日消息，谷歌开始在自己的公有云上提供了一个新的图形加速器，以更好的支持人工智能和虚拟桌面工作负载。

据悉，谷歌采用的芯片是 Nvidia 的 P4，这让谷歌云平台支持的 Nvidia GPU 数量增加到 4 个，而且所有这些都是从 2017 年 2 月以来添加的。Nvidia 扩展其 GPU 产品线的步伐反映了企业采用人工智能的速度越来越快。

P4 的起价为每小时 60 美分，是 4 款 GPU 中价格第二低的。在处理最多 4 个字节的单精度值时，该芯片可提供 5.5 teraflops 的性能。

Nvidia 还为 P4 配备了 8GB GDDR5 内存，专门设计用于 GPU。片上芯片内存要比普通内存更快，因为让数据更接近 GPU 核心，从而减少延迟。

在人工智能部署方面，谷歌认为基于云的 P4 主要用于机器学习推理，也就是数据处理神经网络在经过适当训练之后可以在生产环境中做的事情，这是一种完全不同的任务，有时候利用更强大的 GPU 可以实现更好的性能。

P4 也适用于虚拟桌面环境。它采用了 Grid，这个 Nvidia 软件可以在多个虚拟机之间分配 GPU 硬件资源。此外，谷歌还支持合作伙伴 Teradici 的工具，该工具可以将运行在虚拟机中应用流式传输到员工的本地设备上。

谷歌瞄准的第三种场景是视频流。根据 Nvidia 的说法，该芯片有 3 个视频处理引擎，可以实时转码多达 35 个高清流。

另外，GPU 在谷歌的技术战略中扮演着越来越重要的作用，因此 Nvidia 也成为谷歌的一个重要合作伙伴。话虽如此，但谷歌并不完全依赖于这家 AI 处理器的芯片制造商。谷歌还支持 Tensor Processing Units，这款内部设计的芯片可定制用于运行神经网络，每个神经网络可提供 180 teraflops 的巨大计算能力。

3.3 谷歌将在云平台上集成 AI 服务 首批三个项目曝光

8 月 20 日消息，据可靠消息报道，云计算巨头们将推出预包装 AI 服务，旨在解决多个企业和行业所面临的 AI 问题。谷歌正计划使用其云平台来整合 AI 服务，这一服务与多个行业息息相关。

日前，该公司对创建预包装 AI 服务这一计划进行了详细介绍。在 7 月 24 日的谷歌云 Next2018 会议上，该公司表示，将在其云平台上集成 AI 服务，以满足商业需求。

谷歌的做法值得关注，因为 AWS 和微软 Azure 等云计算巨头可能也会采取类似的方法。事实上，AI 目前一直用于一些特定的行业，比如石油和天然气、零售和制造业等行业。但是，AI 的用途不止于此，它还有着一系列广泛的功能，每个企业和行业都与这一技术密不可分。

谷歌的预包装 AI 服务将主要通过合作伙伴提供，并附带参考架构和行业最佳实践。

首批预包装的 AI 服务包括以下设施：

- 联络中心 AI。

该服务推出仅一个月，谷歌云平台就新增 800 多名注册用户，其目的是利用 AI，提高机器人客服与消费者之间的交互会话，更快速高效地解决客户的需求。联络中心将使用会话来显示关键数据，这大大提高了客服的工作效率。此外，它还可以记录发展趋势，并对问题出现的频率进行分析。

- 云人才解决方案。

该 AI 包是为招聘人才和缩短招聘时间而设计的。该服务过去被称为“云工作发现”，现在仍被广泛使用。

- 推荐解决方案。

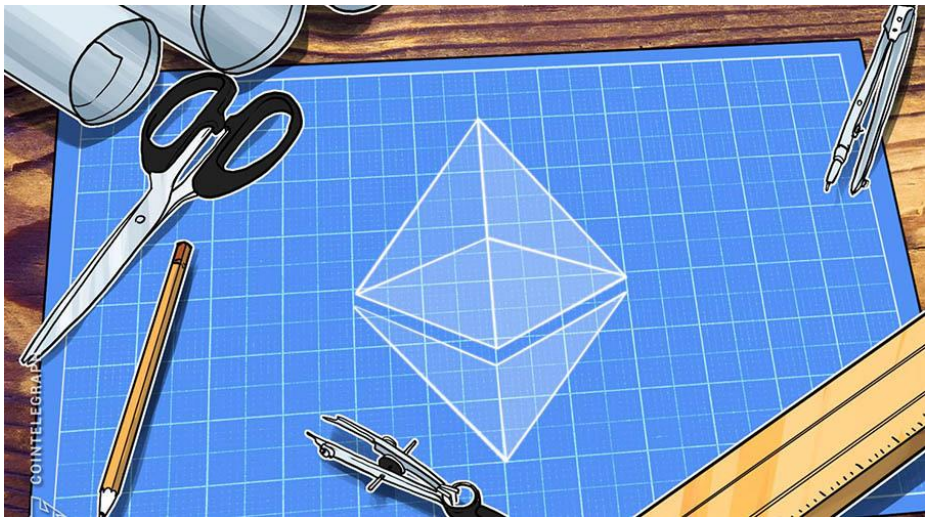
该服务是一个参考架构，旨在让开发人员利用谷歌云的机器学习来扩大市场。

综上所述，AI 云服务可能将与企业软件供应商所采用的典型垂直销售方式迥然不同。AI 将是横向部署。通过这种方式，云供应商将会发展得更好，企业也将可以更好地开展定制化服务。

4. 微软 Azure 云动态

4.1 微软在 Azure 上推出以太坊授权验证算法

8 月 7 日发布的一篇博客文章显示，微软的云平台 Azure 在其以太坊（ETH）区块链产品中引入了授权验证（PoA）算法。



据报道，新的以太坊网络算法将为私人或联盟网络提供一种“更有效”的方式来构建去中心化应用程序（DApps），而“所有共识参与者都要知名且信誉良好”。与工作量证明（PoW）这一 Azure 现有协议相比，PoA 算法基于区块链上已批准的身份或验证器原则，并且在完成交易时不需要竞争。

Azure 上的新以太坊产品具有如身份租赁系统，Parity 的网络组件支持，Azure Monitor 和治理 DApp 等许多功能，可确保其正常运行和安全性保证。身份租赁系统旨在确保当每个成员拥有“冗余共识节点”时，没有两个节点可以携带相同的身份。即使在虚拟机（VM）中断的情况下，系统也会提供身份保护，因此新节点“可以快速启动并恢复先前节点的身份。”Parity 的网络组件支持旨在简化构建智能合约的过程，使客户能够使用比 ETH 区块链上现有的 Solidity 编程语言更熟悉的语言来进行编写。博客文章指出，开发人员现在可以用 C、C ++ 和 Rust 等语言编写 DApp。治理 DApp 解决方案旨在简化参与联盟过程中的投票和验证者授权。通过启用此功能，开发人员可以为客户提供抽象级别，允许程序员隐藏除对象之外的所有相关数据，以降低复杂性并提高效率。

博客文章写道，治理 DApp 还将确保每个联盟成员都能控制自己的密钥，从而允许对用户选择的钱包进行完全受保护的签名。Microsoft 于 2015 年底首次宣布，将推出基于以太坊的 Azure 云计算平台。Azure 成立于 2010 年，提供由 Microsoft 管理的数据中心组成的全球网络，用于开发、测试、部署和管理应用程序和服务。6 月早些时候，R3 区块链联盟宣布，该公司与 39 家全球金融公司一起成功测试了客户了解（KYC）应用程序，在 Microsoft Azure 上运行了总共 45 个节点。

5. 阿里云动态

5.1 中国联通与阿里成立云粒智慧科技，关注金融生态等领域

8 月 3 日消息，中国联通与阿里巴巴宣布，双方将成立云粒智慧科技，注册资本 3.53 亿元人民币。中国联通表示，云粒智慧将依托联通在政企市场场景、通讯基础设施等能力，借助阿里巴巴在大数据、云计算、物联网、人工智能等方面优势，重点关注政务、金融、生态环境、公安、制造等领域。中国联通总经理梁宝俊将出任新公司董事长，阿里云总裁胡晓明担任副董事长。

企查查客户端显示，云粒智慧科技有限公司在北京市工商行政管理局西城分局登记，于今年 6 月 29 日核准成立，股东有联通系统集成有限公司、阿里巴巴（中国）网络技术有限

公司和杭州佳世云网络科技合伙企业，分别占股 51%、34%和 15%。据专家分析，这次作为云粒智慧最大股东的联通，以后在云计算，大数据和人工智能上发力会逐步使用关联公司的方式，而联通本身逐步成为一个纯粹的管道和仓库。

5.2 阿里云新发布九款云产品 与 AWS 等展开竞争

8 月 22 日消息，近日阿里巴巴旗下阿里云推出了 9 款新产品，将与亚马逊 AWS 和微软 Azure 在海外市场展开竞争。

在数据技术和 AI 方面，阿里云准备推出两个关键产品：无服务器化（Serverless）的云上交互式查询分析服务 Data Lake Analytics（数据湖泊分析）和专有的机器学习平台——PAI。Data Lake Analytics 是 Serverless 化的云上交互式查询分析服务。无需 ETL，就可使用标准 SQL、现有的商业智能（BI）和 ETL 工具，以极低成本与高效地轻松分析与集成在云上及 TableStore 上的数据。PAI 是阿里云独有的机器学习平台，适用于不熟悉人工智能的客户。物联网的平台和软件包也会进入到全球市场。

阿里巴巴也宣布推出基础设施和安全产品。Anti-Bot 服务旨在避开网络黄牛和网络搜索器。Hybrid Backup Recovery 是一款用于关键业务数据备份的工具。独立主机可用于需要遵守数据本地化规范的公司和需要处理大流量的公司。除上述以外，阿里巴巴还发布了更多工具，如 Apsara Stack 和 Elasticsearch。

在印度，阿里云与塔塔通信及其子公司 GCX 合作，并在孟买设有数据中心。阿里云提供虚拟计算、CDN、数据库服务和云安全应用等云解决方案。该公司表示将专注于整个印度的中小企业，允许企业在云上托管他们的应用程序、软件和原始数据。

数据中心业务只是阿里巴巴发掘不断增长的印度互联网用户的战略之一。到 2021 年，印度互联网用户预计将达到 8 亿人。今年 1 月，阿里巴巴集团表示将在未来 2 年内为其印度和印度尼西亚业务投资近 200 亿卢比，特别是其内容和媒体业务。当时阿里巴巴推出了一个博客平台，该平台为产生内容的用户付费。阿里巴巴为该平台预留了 5 亿卢比的预算。

除了核心的 B2B 电子商务部门外，阿里巴巴还运营其门户网站 UC Web，包括 UC 头条和 UC 浏览器。2016 年 6 月推出的 UC 头条宣布，截至 2017 年 2 月，UC 头条已拥有超过 1 亿印度用户。截至今年 2 月，UC 浏览器月活跃用户数为 1.3 亿。

5.3 阿里云栖大会：云服务拿下数字重庆，还要布局区块链服务

8 月 24 日，阿里巴巴 2018 云栖大会·重庆峰会在重庆悦来国际会议中心举行，本次峰

会沿用了“驱动数字中国”的主题，重点聚焦在 IoT、智能制造、云计算、大数据、人工智能等领域的探讨，峰会主论坛的重点也是着重推进阿里云与重庆地区城市交通、企业、产业等数字化升级相融合的深入合作，以及打造代表性落地案例。

智慧城市是阿里的重要战略方向之一，而阿里每下一城，手笔可谓都不小，以期实现资源的全面联动，在重庆亦如此。阿里云总裁胡晓明在主论坛现场一一揭晓了具体合作项目，包括智能交通、智能制造、智能汽车、智能金融、智能服务、智能人才等方面，胡晓明说：“在 2018 年 1 月份，阿里巴巴跟重庆市签订了全面的战略合作协议，我们希望能够把我们的互联网技术落户重庆，并且以重庆为辐射点向周边开始辐射，我们希望共同参与打造智能重庆。我们甚至给自己定了一个目标，我们希望能把重庆打造成以互联网、大数据、云计算、人工智能为主的亚洲最智能的大型城市，这是我们很纯朴的一个想法。”

这里还有一个概念提的很有意思，那就是阿里会作为“城市合伙人”的角色参与重庆的城市建设。

首先是智慧交通，主要技术依托便是阿里城市大脑。重庆不仅是山城，同时有两江，港口、高铁、地铁、轻轨、航空等等资源聚合起来非常具有代表性，胡晓明表示，重庆有近 350 万辆车，从整个城市规模来看，在中国是居前的，此外，重庆又有较好的城市升级改造，无论是摄像头还是线圈等等，当这些基础数据有了以后，加上地图、云计算和人工智能技术便能激发巨大想象空间。“阿里已在杭州已经打造了世界上第一个城市大脑，整体把杭州的通行效率提升了 15.3%，因为杭州本身的城市物理条件限制，杭州原来的拥堵指数在中国排名是非常靠前的，如何优化交通，提升整个交通的通行率是一个非常复杂的问题。我们通过城市大脑实现了交通本身的顺畅率提升 15%。”

杭州作为样板案例，阿里也希望把这样的技术方案带到重庆，主论坛上，阿里云和重庆市城市管理委员会宣布第一步先共同打造重庆市公共停车智能化管理服务平台，这个平台将借助 ET 城市大脑聚集全市实时全量的停车资源信息，进行区域泊位信息监控和预测，并结合城市动态交通信息与交警联动，提供出行规划、流量引导、停车诱导等多种服务，为政府进行区域泊位规划优化提供辅助支撑，从静态交通层面提升城市交通畅通度。预计明年能把重庆市主城区的所有停车位进行聚集，至 2020 年完成全市联动。

“我们希望 2020 年能把重庆整个停车位跟地图定位结合在一起，能够提供给所有的驾驶员、出行人员有这样本身停车位的搜索，马上可以便利付费，马上可以进行有效的就近停车，这些是我们要去做的。”胡晓明说。

除了停车场，还有机场，阿里云和重庆机场打造智慧机场的建设。旅客分级安检、人脸

识别一证通关、会员合作、机场智能营销等领域展开全面合作，提升机场智能化运行能力及旅客满意度。据了解，重庆机场目前数据自动采集率超过了 70%，例如，通过云计算和人脸识别，实现了对航站楼重点区域的人数统计和密度分析，以及针对值机和安检区域旅客的排队情况，适时的增开柜台和安全通道，减少旅客的排队时间在 20%以上，可以根据旅客等候出租车的情况，及时调配车辆，可以方便旅客便捷换乘。还可以通过客流的密度分析，及时发现航站楼里边异常的人群聚集情况，以便于及时采取针对性的措施，加强现场管控，确保航站楼秩序等等。

重庆是一个制造大市，智能制造升级的背后支撑则是阿里的工业大脑。这个环节的案例是阿里和攀钢集团的合作，对钢铁产业来说成本控制也很重要，其中最重要的就是在炼钢环节成本的控制，对炼钢的原料来说会涉及到铁水，也会涉及到废钢，也会涉及到生铁还有一些活金，这些成本的投入会直接影响整个钢厂的效益。目前攀钢在西昌的一个基地一年有 400 万吨的钢铁产量，基于阿里云工业大脑每吨可节约 1 公斤原料，每年节约 400 万公斤的炼钢原材料合计一千多万元的成本，接下来将进行能源消耗的进一步优化以及对生产设备的稳定运行进行预测性的监控维护等合作。

另外，在未来 3 年，阿里云 IoT 将联合工信部赛迪研究院、重庆南岸区政府三方打造“飞象工业互联网平台”。据悉，飞象平台预计 3 年内将接入 100 万工业设备，5 年内将助力重庆 4000 家制造企业实现“智造”，胡晓明表示，通过该平台的应用有望把用工减少 20%，把故障的停机减少 50%，把产品品质提升 5%以上，管理效率提升 20%，所以这是我们希望在整个重庆打造的一个“飞象”工业互联网平台。

阿里在重庆瞄准的另外一个机会是汽车，重庆一年生产汽车超过 300 万辆，占全国产量 11%，阿里在重庆跟东风小康、长安福特、长安汽车等一起合作，推进旗下 AliOS 斑马智行系统在汽车产业的渗透，背后基于智能网联系统提供更多的地图、语音、导航、操控等增值服务。

拿下智慧城市、智能制造、智能汽车这几块大蛋糕大工程之外，在智能金融方面，跟重庆银行合作共建移动智能银行平台，实现全行的一体化数据整合，把企业的数据、理财的数据、零售的数据进行集中，提升银行内部数据运营的一体化效率，以及智慧办公。智能服务方面，胡晓明透露盒马鲜生今年年底会入驻重庆，打造一个三公里的便利生活圈，并希望将之前与海底捞、小薇家智能披萨店的技术合作经验在重庆进行复制推广，提升服务业的水准和质量。最后，拉拢一把人才，胡晓明表示将跟重庆市一起合作打造智能人才之城，在未来三年联合重庆的 14 家高校，为重庆打造超过 3000 名以上的大数据人才。

值得关注的一点是，在技术解读环节，除了阿里云产品总监何云飞介绍当前阿里云的技术与服务优势之外，阿里云资深专家易立提到阿里云推出了区块链服务，构建在阿里云的公共云、专用云的弹性计算能力基础之上，以及可靠的存储以及安全网络互联，将能为企业提供安全稳定的区块链服务。同时支持开源区块链技术以及阿里自研的蚂蚁区块链，将进一步和合作伙伴一起构建行业解决方案，提供业务中间界，而不是停留在技术本身，目前已经有商品溯源、供应链金融以及数字资产管理等应用落地。天猫、蚂蚁、阿里云还联合推出了基于区块链的跨境溯源平台，这个系统是基于公开透明的区块链技术构建，生产商、运输商、海关、质检等各个部门共同参与到共识的确认，从而打造出一个更具公信力的平台，可以在生产、运输、入库等过程中进行有效的溯源和质量监控，加强消费者的信任。

6. 腾讯云动态

6.1 腾讯云、腾讯 WeTest 和英特尔合作布局云游戏

8 月 5 日，ChinaJoy 作为中国泛娱乐产业年度风向标，受到全球业界的高度关注。在本届 ChinaJoy 上，腾讯云、腾讯 WeTest 和英特尔，合作为游戏玩家、游戏开发者等业界人士联合展出了云游戏解决方案 Demo。未来，该联合方案的应用将让原本只能在高端配置设备上才能体验的大型游戏，也能流畅运行在入门级设备中。即，游戏玩家能够随时随地，通过手机、平板电脑、台式电脑、电视等任何联网设备，获得一致的高品质游戏体验。

6.2 腾讯云企业客户数据丢失 赔偿意见存千万元分歧

8 月 6 日，云计算规模快速扩张，可靠性仍存挑战。腾讯云发布声明称，平台用户“前沿数控”所存储的数据损坏。原因是数据所在物理硬盘固件问题，在极小概率下触发静默错误，发生数据写入和读取不一致。腾讯云尝试修复数据未果，现已将有问题的硬盘全部下线。

腾讯云提出赔偿约 13.6 万元，客户方要求赔偿约 1100 万元。“前沿数控”伍姓负责人向财新记者表示，腾讯云工作人员在积极与其沟通当中，希望能达成和解，但双方仍未就赔偿方案统一意见。公司已经在做相关材料公证等准备工作，若协商未果，不排除起诉。华为云动态

6.3 长亮科技携手腾讯云发布“银户通” 助银行提升用户连接力

8 月 16 日，长亮科技携手腾讯云发布一站式智能金融服务银户通。基于银户通，银行能够便捷应用到腾讯云及长亮科技提供的优势金融科技能力，并对接腾讯丰富的生态资源，以更广泛地触达用户；银行用户也将能更快捷地获取到银行提供的智能化金融服务工具及其他增值服务。

7. 华为云动态

7.1 华为发布云管理网络 2.0，即日起免费试用

8 月 21 日，华为在北京举办主题为“云网融天下，智简赢未来”的云管理网络发布会，宣布华为云管理网络 2.0 正式入驻华为公有云，即日起可登录 Huawei Cloud 申请免费试用。同时，华为宣布与上海文骋、新网程和汉朔科技等各行业伙伴进行合作。合作伙伴可以基于华为云管理平台为企业开发行业方案，也是华为的专业服务提供商。华为致力于提供智简的园区网络、一站式云服务的平台、和拥有专业行业伙伴的云管理网络服务，帮助中小企业在云时代成功数字化转型。

华为云管理网络搭载了华为全系列的高品质网络产品，包括企业交换机、WLAN、接入路由器、防火墙等 200 多款产品，可以覆盖从几十人的小型办公场景到大型的商超场景网络服务。华为的全系列网络产品服务过北京鸟巢、深圳机场等复杂场景，品质得到市场的印证。其中华为 WLAN 产品 60%的算法和天线技术，源自 30 多年的技术积累，所有产品均经过业界最专业的无线实验室的测试，确保了产品的品质。

华为云管理网络服务真正将线下网络规划、部署、运维、调优的繁杂、耗时、耗人力的网络管理工作迁移到云端，提出从云网规、云部署、云运维到云安全的端到端全生命周期云管理服务，同时提供全面的云端自动化工具以及移动管理 APP，实现极简网络管理。

在生态方面，华为提出了专业生态伙伴的概念。华为会选择与不同行业的专业 MSP（行业服务提供商）合作，在华为云管理服务平台之上，开发不同的行业应用，并且 MSP 可以基于此提供面向行业客户的增值服务。此次发布会上，面向零售行业为例，华为与文骋、新网程、汉朔科技达成合作。上海文骋总经理张珈表示：“希望携手华为，为更多连锁用户提供一站式的线上线下 ICT 运维解决方案。”上海新网程希望通过与华为的合作，让无线生活更安全更规范更美好。汉硕科技表示愿与华为通力合作，共同打造云管化的、面向未来智能零售应用场景的完整解决方案。

二、 开源云动态

1. Openstack 动态

1.1 SUSE OpenStack Cloud 助力 TCS 企业云平台

8 月 22 日消息，SUSE 宣布跨国 IT 服务、咨询和商业解决方案机构 TataConsultancyServices（TCS）已选择 SUSE OpenStack Cloud 作为 TCS 企业云平台的标准基础。

通过密切合作，TCS 和 SUSE 的团队成功设计出兼具功能性和灵活性的企业云平台。该平台集成多项技术，包括针对软件定义组网的 Cisco ACI、KVM 和 VMware 虚拟机管理程序，以及采用 SUSE OpenStack Cloud 的 EMC 存储后端。TCS 和 SUSE 联合开发了这个强大并且可复制的架构，可通过快速部署满足客户需求。

面向企业用户的 SUSEOpenStackCloud 支持多种虚拟机管理程序，将为 TCS 客户提供灵活性、选择性和高可用性。TCS 提供的 TCS 企业云平台是依据其战略路线图推出的产品，旨在帮助客户转变他们的 IT 基础架构。这个平台能够帮助企业提高开发和推出商业应用的便捷性。

TCS 企业云基础架构业务部门云销售和解决方案全球总监 Rajesh Srinivasan 博士表示：“随着企业纷纷开始采用混合云，由 SUSE OpenStack Cloud 提供支持的 TCS 企业云平台可以快捷、安全地在云端运行商业应用，还能让工作负荷在不同的云环境之间无缝迁移。我们与 SUSE 的合作为双方共同的客户带去企业级的可靠性、互操作性和灵活性。”

SUSE 销售总裁 Ronaldde Jong 表示：“SUSE 服务的客户遍布全世界，他们希望通过转变自身的 IT 基础架构来推动增长并获得竞争优势。我们与 TCS 的协作将扩大这个范围，让 SUSE OpenStack Cloud 的开源创新服务于更广泛的客户群体。现有和潜在客户的需求推动我们与 TCS 这样的公司建立战略合作伙伴关系，并且为我们的创新指明方向。”

SUSE OpenStack Cloud 为客户打造灵活、可自定义并且可扩展的云，进而加快软件定义基础架构的部署。另外，它还能提高互操作性、可扩展性和灵活性，帮助企业客户打造面向未来的 IT 基础架构，进而在竞争激烈的当今市场上脱颖而出。除了在 TCS 企业云平台中集成 SUSE OpenStack Cloud，今后 TCS 的解决方案路线图还将纳入更多 SUSE 产品，例如 SUSE Cloud Application Platform，包括其内置的 SUSE CloudFoundry。

2. Easystack 动态

2.1 京东云战略投资 EasyStack

8 月 9 日消息，捷行云 EasyStack 日前宣布完成 C++轮融资，本轮融资由京东集团战略投资，融资金额则未公布。

据易捷行云官方消息，C++轮融资由京东云主导，京东集团投资，并没有宣布其他投资者的消息。借由本轮投资，EasyStack 和京东云将成为企业云战略合作伙伴，为企业用户提供私有云、公有云、跨多云的一站式云服务体验，进一步扩大双方的云计算市场，为更多企业用户的数字化转型提供更好的云服务。不仅如此，EasyStack 也将与京东集团各项业务紧密合作。

合作达成后，京东集团副总裁、京东云投资负责人邓天卓表示，“值得信赖”是双方洞察用户需求，打磨极致产品的信仰，面临企业云计算市场的爆发，EasyStack 为企业级客户提供开放、稳定可靠、高性能的云计算产品与服务的理念与京东云一致。“开放包容，不懈地推动生态发展，以促进行业发展为己任，会让京东云在未来布局方面走得更稳健。”

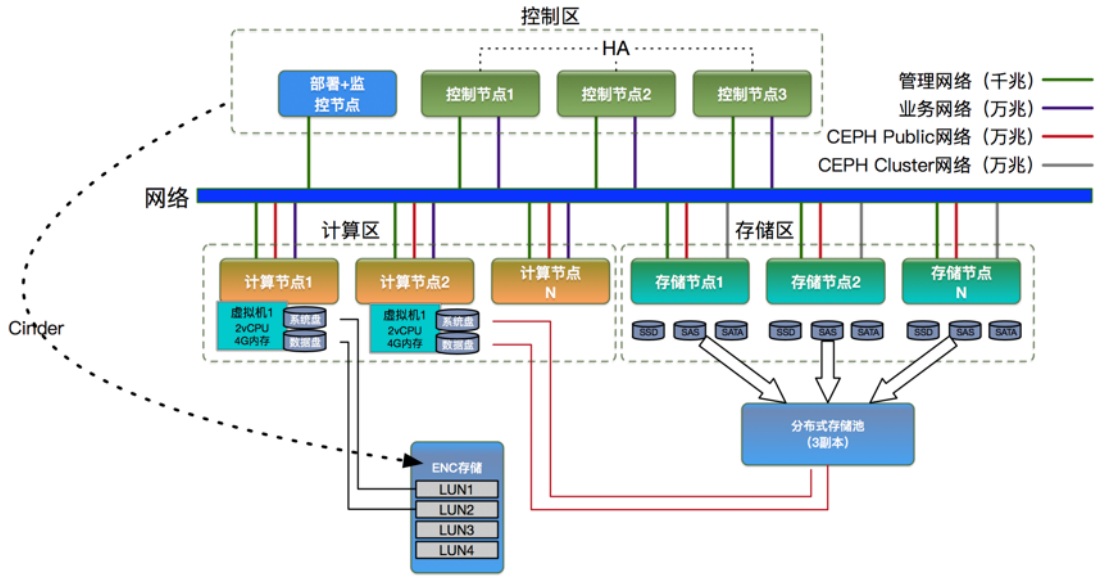
EasyStack 创始人兼 CEO 陈喜伦则透露，公司正在向“以开源生态为基础的世界级云计算企业”的长期战略目标迈进。此次 C++轮战略投资，EasyStack 将与京东实现从技术、产品到市场的全面战略合作；与此同时，EasyStack 仍将保持公司独立发展，持续进行核心技术的研发投入，云计算产品化的开发，以及企业解决方案的生态建设，为企业用户打造从基础架构到应用的跨多云的一站式云计算平台。

3. 99CLOUD（九州云）动态

3.1 牛商网携手九州云,构建新型互联网业务平台

8 月 23 日消息，结合自身 IT 的信息化建设现状、需求以及其整体的标准要求，牛商网最终联合九州云构建私有云平台，对计算、存储、网络资源进行较彻底的云化，通过建设云平台以满足各方面的要求。

牛商网云平台整体解决方案如下。



通过计算虚拟化、存储虚拟化、网络虚拟化实现资源利用率提高；通过热迁移、多副本冗余、分布式技术等手段等实现高可用。通过 Nova、Cinder、Neutron 等技术实现资源的统一管理。

通过多租户技术、VPC 网络等实现资源的逻辑隔离；通过云管理协同实现平台的统一调度。通过模板标准化，实现单一计算、存储、网络元素的标准化。通过 Heat 等编排技术，实现针对应用的标准化。

通过对计算 Flavor、存储 Volumn Type、网络 QoS 等定义，实现不同资源的标准化；通过对项目资源和可以使用模板的映射，实现资源针对不同等级项目的匹配。通过流程机制保证资源的按需分配和回收，通过租户配额计中计保证资源在额度内的快速发放。通过虚拟化和按需资源分配，提高资源的利用率，降低总体成本。

通过底层分布式技术，实现资源的横向扩展。通过容器化 IaaS，实现底层的平滑升级和弹性伸缩，结合虚拟化热迁移等技术，实现平台的的按需规模设计。

提供资源审批、工单流转、运维监控、日志审查、大屏展示等功能，支持平台的运维和运营，提升管理效率。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰受邀参加中国网络安全年会，多项新技术研究成焦点

作为信息安全产业的领军企业，启明星辰始终立足于网络安全领域，现阶段已在云计算、大数据、人工智能、物联网、工业互联网、关键信息基础设施保护、移动互联网等新技术布局，帮助城市全面提升安全能力。

未来，启明星辰将继续坚守初心，以保障国家网络空间稳定与客户业务健康运营为己任，持续致力于提供具有国际竞争力的自主创新的安全解决方案和优秀的实践服务，为建设网络强国贡献力量。

1.2 启明星辰携手守护者计划抵制网络诈骗

启明星辰作为中国信息安全产业的领军企业，加入“守护者计划 2018 公益行动企业联盟”的正能量阵营中，共同对抗网络威胁、抵制网络诈骗，竭力全方位守护公众的网络安全。

去年，启明星辰积极防御实验室（ADLab）与电信云堤联手，成功打击黑产。通过对僵尸网络黑产的分析中发现“黑吃黑”攻击行为——黑雀攻击，使相关安全部门可以分析评估该黑雀的攻击影响力，及时采取应对措施，使受控制网络失效，有效抑制黑色产业发展。

未来，通过“守护者计划 2018 公益行动企业联盟”这个窗口，守护者计划将联合社会各领域企业积极应对网络威胁。启明星辰还会与联盟在产品、技术等方面展开深度合作，在个人信息保护、金融安全保护等领域提供更多优质服务和安全保障，共同守护用户安全，提升社会公众的幸福感。

2. 东软

2.1 东软 RealSight APM 云应用性能监控提案纳入 TOSCA 标准

东软参与全球信息化产业顶级标准化组织 OASIS 的 TOSCA 国际行业标准制定，提交云应用性能监控方案并被纳入标准。

该方案基于东软 RealSight APM 应用管理套件，专门用于解决企业云应用的监控和管理等问题，为企业业务的顺利运行，实现数字化转型保驾护航。

TOSCA（云应用拓扑编排标准，Topology Orchestration Specification for Cloud

Applications）是由 OASIS 组织制定，多家全球知名的 IT 公司联合参与，并经过多年的推行和完善，已经成为国际通用的行业规范。该标准重点关注云服务中的应用程序和结构的互操作性描述、云服务中各个部分的关系及这些服务的操作行为（例如，如何部署，打补丁，关闭），目标是增强云应用程序和云服务的移植性，即重复使用性，以便于客户灵活选择云提供商，搭建可控、可定制的完整云应用管理体系。

3. 山石网科

3.1 山石网科发布新版 OS，全面支持 IPV6

山石网科正式发布了 StoneOS 5.5R6 版本，山石网科下一代防火墙功能可全面支持 IPv6，涉及到的产品包括：下一代防火墙、智能下一代防火墙、数据中心安全防护平台 X10800、数据中心防火墙、ABG 应用负载网关、山石云·界等等。

此次版本升级，山石云•界支持新型号 VM04，VM01\VM02\VM04 多型号采用统一镜像，无需重装可进行型号间升级切换。

3.2 山石网科、瑞星、VMware 共推云计算安全整体解决方案

山石网科“未来已至- AI 定义的云计算数据中心安全技术发展峰会”在长沙举行，瑞星、山石网科、VMware 在会上主要讨论了未来的合作模式，瑞星将在 VMware 提供的 NSX 安全平台及开放的安全 API 接口提供终端防病毒安全防护，由山石网科提供网络安全防护，三方共同发力云计算安全，帮助企业用户提升安全性能和业务灵活性。

4. 亚信安全

4.1 亚信安全与新华三合作，发力“更安全的数据中心”

亚信与新华三合作，双方将在产品创新、技术服务、渠道营销等领域展开全面的战略联盟合作，积极提升云计算应用安全管理水平，共同帮助企业级用户应对不断演化的网络威胁。

亚信安全服务器深度安全防护系统(Deep Security)已经通过亚信安全实验室与 H3C 云计算实验室的联合验证测试，并且获得了 H3Cloud Ready 认证证书。

亚信安全服务器深度安全防护系统(Deep Security)将作为 H3C CAS 虚拟化系统的标准化服务模块，对采用 H3Cloud 解决方案的用户提供按需服务。

4.2 亚信安全发布 2018 年第二季度安全报告

亚信安全发布《2018 年第二季度安全威胁报告》，报告显示，挖矿病毒仍然是不法分子利用最为频繁的攻击方式，并伴有大幅度增长。此外，不断更新的勒索软件攻击与感染方式，以及高度专业化、组织化的 APT 攻击事件也是本季度值得关注的安全动态。

5. 绿盟科技

暂无消息。

6. 360 企业安全

暂无消息。

7. 安恒

7.1 安恒信息与派盾科技签订战略合作协议

安恒信息与派盾科技签订战略合作协议，与派盾科技一起，共建区块链产业安全全生命周期整体解决方案，推动区块链行业安全问题的防御能力提升和安全保障，更好地保障区块链产业安全。

在此次协议签订后，安恒信息在区块链领域的布局，也将全面展开。

8. 安天

暂无信息。

9. Fortinet

9.1 Fortinet 获得 NSS Labs 的 SD-WAN 测试推荐级别

Fortinet 的 FortiGate SD-WAN 解决了安全 SD-WAN 部署中诸多的挑战，并且是唯一一个在 NSS Labs 首次软件定义的广域网报告中获得“推荐”评级的 NGFW 安全厂商。

10. Checkpoint

10.1 CheckPoint Check Point 发布《网络攻击趋势：2018 年中报告》

仅去年一年，全球有 51%的组织遭遇过基于云的攻击，包括联邦快递(FedEx)、英特尔(Intel)和本田(Honda)。

一些基于云的攻击，主要是那些涉及数据过滤和信息披露的攻击，这些攻击是由于糟糕的安全应用。

一些凭证被遗留在公共源代码存储库中，或使用弱密码，这只是威胁者如何访问和控制云中托管的未受保护资源的一些例子。

另一个正在崛起的威胁正在席卷云环境，那就是臭名昭著的加密货币挖矿器，他们将目标对准云基础设施，以利用云所提供的巨大计算能力，并为威胁者带来巨额利润。

在 2018 年上半年，目睹了针对云的核心组件的两个挖矿器——Docker 和 Kubernetes 系统。

四、 容器技术及安全动态

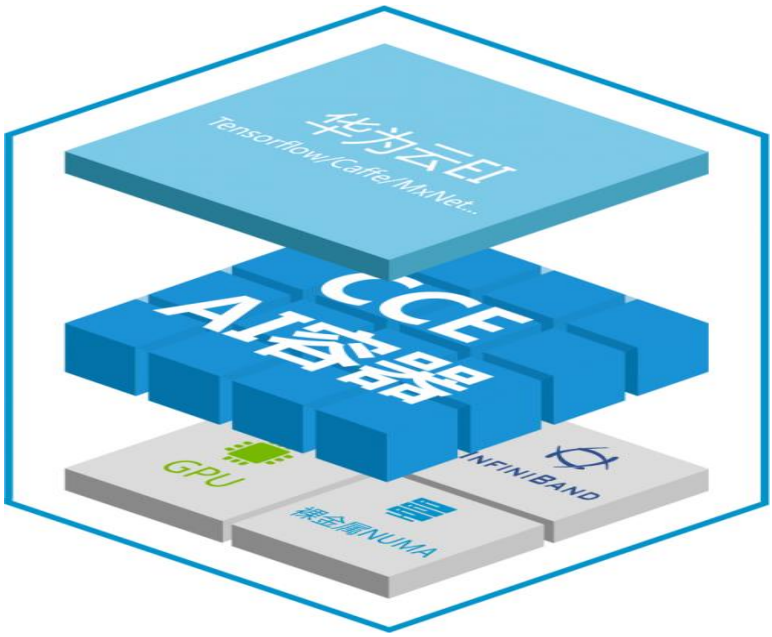
1. 华为云全球首发 GPU 共享型 AI 容器 加速“普惠 AI”落地

8 月 28 日,“AI 上有信仰的云——华为云中国行 2018”成都站如期举行。华为云全球首家推出了 GPU 共享型高性能 AI 容器,这是继裸金属容器、Windows 容器等重大特性之后,华为云在容器领域的又一次技术突破,将极大地推动 AI 技术的普及,助力“普惠 AI”策略加速落地,为广大用户提供“用的起、用的好、用的放心”的 AI 云平台

华为云 AI 容器是全球首款支持共享 GPU 的高性能容器产品,在业界首家实现了多容器共享 GPU 资源,大幅降低了 AI 计算的成本,并在 AI 计算性能上比通用方案提升了 3-5 倍以上。

华为云 AI 容器已完成多款主流 GPU 的适配,包括 Nvidia Tesla P4/P100/V100 等产品系列,客户可根据不同应用场景灵活选取,以达到最高的性价比。

华为云 AI 容器支持 Tensorflow、Caffe 等主流深度学习框架,并在华为云 EI 的深度学习、推理平台、人脸/图像/文字识别等多个服务得到广泛应用与验证。目前正式面向华为云客户提供该项服务,让客户轻松获得强劲、高效的 AI 计算引擎。



目前 AI 容器已在华为云的 CCE 容器服务中开展公测,您可以访问以下地址申请试用:

https://console.huaweicloud.com/cce2.0/#/app/resource/cluster/list?type=GPU

HUAWEI CONNECT 2018 作为华为自办的面向 ICT 产业的全球性年度旗舰大会,将于 2018 年 10 月 10 日-12 日在上海隆重举行。本届大会以“+智能,见未来”为主题,旨在搭建一个开放、合作、共享的平台,与客户伙伴一起共同探讨如何把握新机遇创造智能未来。

2. Istio 1.0 正式版发布，可用于生产环境

北京时间 7 月 31 日晚上 24 点，Istio 宣布推出 1.0 正式版本，并表示已可用于生产环境。

Istio 是一个由谷歌、IBM 与 Lyft 共同开发的开源项目，旨在提供一种统一化的微服务连接、安全保障、管理与监控方式。Istio 项目能够为微服务架构提供流量管理机制，同时亦为其它增值功能（包括安全性、监控、路由、连接管理与策略等）创造了基础。这款软件利用久经考验的 Lyft Envoy 代理进行构建，可在无需对应用程序代码作出任何发动的前提下实现可视性与控制能力。Istio 项目是一款强大的工具，可帮助 CTO/CIO 们立足企业内部实施整体性安全、政策与合规性要求。

值得关注的更新：

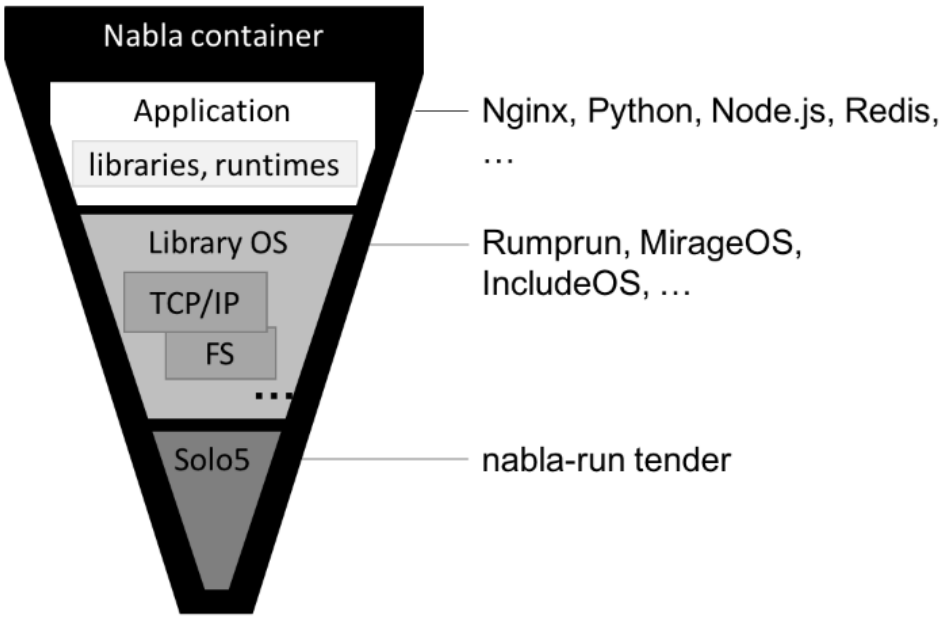
- 现在可以将多个 Kubernetes 集群添加到单个网格中，并启用跨集群通信和一致的策略实施。多集群支持功能现在是 Beta 状态。
- 通过网格实现对流量的细粒度控制的网络 API 现在是 Beta 状态。使用网关显式

建模关于 ingress 和 egress 的关注点，允许运维人员控制网络拓扑并满足边缘的访问安全要求。

- 现在可以增量上线双向 TLS，而无需更新服务的所有客户端。这是一项重要的功能，可以解除在现有生产环境部署方面采用 Istio 的障碍。
- Mixer 现在支持开发进程外适配器。这将成为在即将发布的版本中扩展 Mixer 的默认方式，使得构建适配器变得更加简单。
- 现在，Envoy 在本地完全评估了控制服务访问的授权策略，从而提升了它们的性能和可靠性。
- 通过 Helm chart 进行安装 现在是推荐的安装方法，它提供了丰富的自定义选项，以便根据您的需求配置 Istio。
- 在性能改进方面投入了大量精力，包括连续回归测试、大规模环境模拟和目标修复。

3. IBM 发布专为安全性设计的容器-Nabla

IBM 声称其新的容器设计比 Docker 或其他容器更安全，通过将操作系统调用降至最低限度，从而尽可能减少其攻击面。



James Bottomley 是一位 IBM 研究杰出工程师和顶级 Linux 内核开发人员，他概述了存在两种基本类型的容器和虚拟机（VM）安全问题：被描述为 Vertical Attack Profile (VAP) and Horizontal Attack Profile (HAP)。

VAP 描述的是全部代码，通过遍历代码可以提供完整的服务，包括从数据输入，更新

到输出等。像所有代码一样，这段代码也存在漏洞，而且漏洞的密度差异性随机，但遍历的代码越多，发现安全漏洞的概率就越大。堆积起来的安全漏洞的集合——应用可能从容器内跳出到物理主机或虚拟化主机层面——就是 HAP 集。

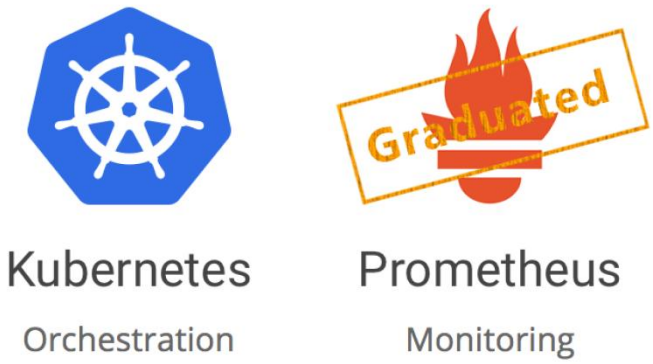
定量方法测量 HAP=Linux 内核代码的缺陷密度*代码遍历产生的代码数量。

即先测出一个 VM 或容器裸系统的代码有多少行数，然后用这系统去运行一个指定的应用。系统的代码行数越多，就越有可能存在 HAP 级别安全漏洞。

4. CNCF 宣布 Prometheus 项目于 CNCF“毕业”

8 月 9 日，管理 Kubernetes 和 Prometheus 等云原生开源技术的 Cloud Native Computing Foundation（CNCF）在 PromCon（年度 Prometheus 会议）上宣布 Prometheus 是继 Kubernetes 之后的第二个 CNCF 毕业项目。Prometheus 已成为构建现代云原生应用程序的企业首选的开源监控工具之一

在 CNCF 管理的项目中，要从’孵化’转为’毕业’的成熟水平，项目必须被社区广泛的采用，有结构完整的治理过程文档，以及对社区可持续性和包容性的坚定承诺。



5. Microsoft 宣布正式发布 Linux on ASE

Microsoft 宣布正式发布（GA）用于 ASE（应用服务环境，App Service Environment）的 Linux。该服务使客户可结合使用 Linux 上的应用服务（App Service）特性与 ASE。在正式发布版之前，Microsoft 曾于今年五月发布了支持客户在 ASE 中部署 Linux 和容器化应用的公开预览版。

使用 Linux on ASE，客户可以独立选用 Microsoft 预构建镜像上的容器或代码，将自己的 Linux Web 应用部署到 Azure virtual network（VNet） (VNet)。客户的容器可以来自于

DockerHub、Azure Container Registry，或是自己的私有注册容器。Microsoft 提供的预构建镜像支持 Node、PHP、Java、.NET Core 等编程技术栈，并将进一步支持更多编程语言。

Linux Web 应用可驻留在使用 Windows、其它 Linux 或容器化 Web 应用的 ASE 中。所有容器共享同一 VNet，但 Windows 和 Linux Web 应用必须各种具有应用服务计划（App Serive Plan）。据宣布 Linux on ASE 正式发布的 MSDN 技术博客帖子介绍，客户可以使用具有 Dv2 虚拟机的独立 SKU（可提供服务单元，Stock Keeping Unit），并添加额外的扩展能力（在一个 ASE 中可扩展到合计 100 个 Windows 和 Linux 应用服务计划）。

部署流程：要在新的 ASE 中创建一个 Web 应用，客户只需新建一个 Web 应用，选取 Linux 为操作系统（内建镜像），选取 Docker 容器（或用户自定义容器），或是新建一个用于容器（或用户自定义容器）的 Web 应用。在新建一个应用服务计划时，记住应选取一个独立 SKU。

6. 谷歌推出 K8S 二进制授权

为强化 Kubernetes 的安全性，Google 引入了二进制授权（Binary Authorization），确保使用者只能将受信任的 workload 部署到 Kubernetes 中。二进制授权是在 Kubernetes 中部署 API 的安全性功能，提供使用者策略性的控制手段，让授权的镜像在环境中运作。

Google 提到只要使用开源项目 Grafeas 的自订策略，并根据要求允许或阻止 Pod 创建，使用者也可自行进行二进制授权。作为二进制授权测试版发布的一部分，Google 更新了开源引擎 Kritis。

Kritis 与开源 Grafeas 整合就可以在 Google Kubernetes 引擎部署中使用容器注册表分析 API 和二进制授权。这样使用者可以自行使用开源软件建立控制流程。

7. 谷歌云移交 Kubernetes CI/CD 所有权给社区

8 月 29 日，在北美开源峰会上，云原生计算基金会（CNCF）宣布 Google Cloud 已开始转让 Kubernetes 项目的云资源的所有权和管理给 CNCF 社区贡献者。 Google 云计划将通过 900 万美元的 Google Cloud 信用补助金（分为三年）来支持此项举措，以支付与 Kubernetes 开发和分发相关的基础架构成本，例如运行持续集成和持续交付（CI / CD）管道并提供容器镜像下载存储库。

通过此举，CNCF 和 Kubernetes 社区成员将负责所有日常 Kubernetes 项目运营。职责包

括开发 Kubernetes 的操作任务，例如测试和构建，以及 Kubernetes 分发的维护和操作。Google Cloud 信贷补助金将主要用于资助可扩展性测试和维护运行 Kubernetes 开发所需的基础架构，确保项目继续经过反复测试和企业就绪。

五、 安全新产品及技术

1. 8 月 Android 安全补丁发布，共计修复 43 处漏洞

在发布 Android 9.0 Pie 正式版之后，Google 今天还发布了针对所有支持设备的 Android Security Patch for August 2018，修复了很多安全漏洞和用户报告的其他问题。其中包括 2018-08-01 和 2018-08-05 两个安全补丁级别，修复了包括框架、多媒体框架、系统、内核、高通组件、高通闭源组件等共计 43 处安全漏洞。

2. 顺丰上线下单“隐址件”，收寄双方均看不到对方信息

随着《快递暂行条例》的出台和落实，快递信息安全议题持续引发关注。近日，顺丰推出了可隐匿收/寄件人地址的产品——“隐址件”，收寄件双方只需分别填写自己的地址即可完成下单。使用时，寄件人在填写好寄件信息后，将收件信息填写页面分享给收件人，收件人补充收件信息后，寄件人则可在线上完成下单，在此过程中，收寄双方都通过第三方平台进行信息交互。第三方平台对收寄双方的姓名、手机号、详细地址进行隐匿处理，不会在快递单上显示。在寄递全流程中，仅收派员拥有通过巴枪扫描获取相关信息的权限，可明显提高信息安全保密性。

3. PhishPoin：一种绕过 Microsoft Office 365 保护的新技术

PhishPoint 是一种新型的 SharePoint 钓鱼攻击，在过去的两周内，大约有 10%的 Office 365 用户受到了这种攻击的影响。安全专家警告称，已经有很多网络诈骗份子开始使用这种新型的攻击技术来绕过目前大多数电子邮件服务商所部署的高级威胁保护（ATP）机制了，其中受影响的就包括 Microsoft Office 365 在内。

根据 Avanan 发布的安全报告显示：“在过去的两周内，我们检测到并成功阻止了一种新型的钓鱼攻击，目前全球大约有 10%的 Office 365 用户受到了此次攻击的影响。PhishPoint

是一种升级版的网络钓鱼攻击，攻击者主要利用电子邮件和 SharePoint 来收集终端用户的 Office 365 凭证信息。在攻击的过程中，攻击者会使用 SharePoint 文件来托管钓鱼链接，通过向 SharePoint 文件插入恶意链接（而不是向电子邮件中插入），攻击者将能够绕过 Office365 的内置安全机制。”

4. 微软 Cortana 出现漏洞，即使系统锁定也能使用浏览功能

实际上，Windows 系统会默认开启锁屏状态下调用 Cortana 数字助手的功能，用户无需解锁即可向 Cortana 提问，而 Cortana 也会通过语音或文字等形式回答你的问题，即使这名用户没有进行身份验证。在这种状态下，Cortana 主要依赖于 Edge 浏览器或个别版本的 IE 11 浏览器来实现这种问答功能。

而来自 McAfee 的研究人员近日发表报告称，如果攻击者能够物理访问到目标设备的话，攻击者将能够利用这种存在安全缺陷的功能来窃取用户存储在浏览器缓存中的数据。通过向 Cortana 提问恰当的问题，攻击者就可以在不解锁屏幕的情况下让 Cortana 直接访问一个由攻击者控制的域名地址，由于该域名地址所指向的资源内容是攻击者控制的，所以他们就可以直接在目标用户的浏览器中运行恶意 JavaScript 脚本了。

McAfee 的研究人员也已经在这篇研究报告中提到了攻击者如何利用 Cortana 获取目标用户的数据、运行恶意代码，甚至是修改锁定 PC 的密码，感兴趣的用户可以深入阅读了解详情。

值得一提的是，Cortana 可以根据用户具体提出的问题和提问的方式来给出更加详细的回应，甚至可以直接返回互联网中的某条资源。比如说，如果你想查询某个官方网站的话，Cortana 将会直接返回维基百科里的条目。

5. 英特尔处理器曝出新漏洞

近日，两名德国安全研究员发布了名为《ret2spec: Speculative Execution Using Return Stack Buffers》的论文，披露了英特尔处理器的新漏洞“逆 spectre 攻击”。攻击者可利用这个新漏洞，在未经授权的情况下读取数据。新漏洞是“运行时优化返回地址”的 CPU 预测导致的。如果攻击者能操纵这一预测，就能控制预测执行编程代码，通过旁路读取本应该禁止访问的数据。研究人员称，他们在五月份通知了厂商，90 天的保密期已过，所以他们现在公开了论文。他们认为，ARM 和 AMD 的处理器可能也受到该漏洞的影响。

六、 网络安全投融资、收购事件

1. 收购

1.1 Cisco 完成对 Duo Security 的收购

8 月 2 日，Cisco 完成对 Duo Security 的收购，收购价 23.5 亿美元。Cisco 是全球最大的网络设备制造商。Duo Security 是一家企业级移动认证安全服务商，推出了自主登记用户双重安全认证服务，支持 iOS、安卓和黑莓等主流移动操作系统，而且不需要任何硬件认证就能生成安全密码。在用户端，用户下载移动应用之后可以和平时一样输入用户名和密码，一旦首次身份认证成功，他们就会提供第二种认证方式，并且无缝同步到服务器和企业内部网络中，这种解决方案不仅安全性能得到保障，还加速了身份认证速度。

2. 投融资

2.1 HYAS InfoSec 获得 620 万美元的 A 轮融资

8 月 2 日，HYAS InfoSec 从 205 Capital 和其他 5 位投资者处获得 620 万美元的 A 轮融资。HYAS InfoSec 是从事威胁研究，情报分析和检测的安全公司。

2.2 RiskRecon 获得 2500 万美元的 B 轮融资

8 月 7 日，RiskRecon 从 Accel 和其他 5 位投资者处获得 2500 万美元的 B 轮融资。RiskRecon 是一个第三方软件风险评估工具，能够帮助用户获得对每个第三方安全实践的可验证评估，然后建立基础信任水平，并确定具体领域的风险管理。

2.3 HYAS InfoSec 获得 47.5 万美元的未知轮融资

8 月 14 日，HYAS InfoSec 从 Western Economic Diversification Canada 获得 47.5 万美元的未知轮融资。HYAS InfoSec 是从事威胁研究，情报分析和检测的安全公司。

2.4 AttackIQ 获得 550 万美元的 A 轮融资

8 月 14 日，AttackIQ 从 Index Ventures 和其他 3 位投资者处获得 550 万美元的 A 轮融资。AttackIQ 是一个自动验证平台，可以完成对安全控制能力的准确检验。

2.5 Twistlock 获得 3300 万美元的 A 轮融资

8 月 15 日，Twistlock 从 Dell Technologies Capital 和其他 5 位投资者处获得 3300 万美元的 C 轮融资。Twistlock 是一家针对虚拟容器提供安全技术的初创企业，其产品能帮助企业解决主机和容器应用内的安全威胁。