

国内外云计算+安全动态报告

2018 年第 5 期

启明星辰云计算安全事业部

目录

目录.....	i
本期云安全动态内容摘要.....	1
国内外云+安全动态报告.....	4
一、云厂商动态.....	4
1. AWS 云安全动态.....	4
1.1 推出 Amazon EC2 队列.....	4
1.2 使用 Amazon CloudWatch 监控 Amazon Kinesis Data Analytics 应用程序.....	4
1.3 随 Lumberyard Beta 1.14 推出 Script Canvas 重大更新.....	5
1.4 Amazon Sumerian 全面开放.....	5
1.5 Quick Start 推出适用于在 AWS 云上运行的 Tableau Server.....	5
1.6 正式发布 Amazon EC2 裸机实例.....	6
1.7 Amazon ECS 服务发现功能支持桥接和主机容器联网模式.....	7
1.8 Amazon Connect 与五大新公司实现了集成.....	7
2. VMWare 云安全动态.....	8
2.1 VMware 助推企业转型，迈向数字化之巅.....	8
3. GOOGLE 云动态.....	9
3.1 Twitter 将部分基础数据移入 Google Cloud.....	9
3.2 谷歌收购云技术创企 Cask Data，构建运行大数据分析工具.....	11
4. 微软 Azure 云动态.....	11
4.1 微软 Build 2018 亮点：AI 与云并驾齐驱 边缘计算高频出现.....	11
4.2 微软与美情报部门达成革命性协议：为美国政府提供云服务.....	12
4.3 微软 OneDrive 成企业最受欢迎云存储.....	12
5. 阿里云动态.....	12
5.1 阿里云营收 133.9 亿元 连续 12 季度规模翻番.....	12
5.2 积微物联携手阿里集团 共建攀钢 ET 工业大脑.....	13
5.3 阿里云推出人工智能猪肉.....	13
5.4 阿里云开发 AI 收银员 上海地铁已运用语音购票技术.....	14
5.5 阿里云发布 Link 生活物联网平台 2.0 支持天猫精灵等三大语音 AI 操控.....	14
5.6 阿里云宣布同贵州的下一个五年计划 八大领域全面突进.....	16
6. 腾讯云动态.....	16
6.1 腾讯云黑石数据中心助推重庆智造.....	16
6.2 CODING 获腾讯云一亿元战略融资，共同开启云端开发时代.....	16
6.3 腾讯云发布数据安全解决方案数盾，解决三大新痛点.....	17
6.4 腾讯携手中科院国家天文台落地 FAST.....	18
6.5 腾讯云重磅发布全新智慧零售产品 全维助力零售业数字化升级.....	19

7.	华为云动态	19
7.1	华为敏捷网络助力宜春市人民医院新北院打造赣西区域医疗中心	19
7.2	阿里云投诉华为靠虚假材料谋取中标，因缺乏证据被驳回	20
7.3	熙菱信息：联手华为打造海淀视频云	20
二、	开源云动态	21
1.	Openstack 动态	21
1.1	OpenStack Summit 2018:浪潮 InCloud OpenStack 5.5 海外首发	21
2.	Easystack 动态	21
2.1	EasyStack 完成 C+轮融资，云计算定义超融合下半场	21
3.	99CLOUD（九州云）动态	24
3.1	九州云赴中国 IT 用户版的“达沃斯”峰会	24
三、	云安全厂商动态	24
1.	启明星辰	24
1.1	启明星辰集团发布工业物联网网络安全解决方案白皮书	24
1.2	启明星辰荣获中国网络安全与信息产业“金智奖”三项大奖	25
2.	山石网科	25
2.1	山石云·格获得 VMware Ready 认证	25
3.	亚信安全	26
4.	绿盟科技	26
5.	360 企业安全	26
5.1	360 企业安全集团 2018 年教育部高等教育司产学研合作协同育人项目	26
5.2	工信部赴 360 企业安全集团调研	26
6.	安恒	27
6.1	教育行业信息安全监测预警管理平台正式发布	27
6.2	安恒信息助力杭州城市数据大脑建设	27
6.3	广州大学与安恒信息正式签约 共建人工智能安全联合实验室	28
7.	安天	28
8.	Fortinet	28
8.1	Fortinet 发布新型光纤连接器扩展了 Fabric-Ready 合作伙伴计划	28
9.	Checkpoint	29
9.1	CheckPoint 公布 2018 年第一季度财务业绩报告	29
四、	容器技术及安全动态	30
1.	整合了 CRI plugin 的 Containerd 1.1 发布	30
2.	Kata Containers 1.0 稳定版问世	33
五、	安全新产品及技术	33
1.	iPhone X IOS 11.3.1 被腾讯 Keenlab 团队成功越狱	33
2.	漏洞导致 Windows 系统崩溃，硬件专家公布 PoC 利用码	34

3.	CNNVD 关于 PHP 输入验证安全漏洞的通报.....	34
4.	Synack 勒索软件利用多种高级技术躲避检测	34
5.	近 400 个政企网站感染 Coinhive 恶意软件, 秘密挖掘加密货币.....	35
6.	邮件形同裸奔, PGP 与 S/MIME 加密协议被曝严重漏洞	35
7.	Telegrab 恶意软件可以获取 Telegram 的密码、cookie 及密钥文件.....	35
8.	FBI 控制感染几十个国家 50 万台路由器和存储设备的 VPNFilter.....	36
9.	Mac 设备遭遇新门罗币挖矿软件入侵.....	36
六、	络安全投融资、收购事件.....	37
1.	收购	37
1.1	StackPath 完成对 Server Density 的收购	37
1.2	KnowBe4 完成对 exploqii 的收购	37
2.	投融资	37
2.1	Namogoo 获得 1500 万美元的 B 轮融资	37
2.2	IronNet Cybersecurity 获得 7800 万美元的 B 轮融资	37
2.3	CUJO 获得未知数额 B 轮融资	37
2.4	Indeni 获得 1400 万美元融资	38
2.5	Runsafe Security Inc 获得 240 万美元种子轮融资	38
2.6	Openpath Security Inc 获得 700 万美元种子轮融资	38

本期云安全动态内容摘要

云厂商方面, AWS 推出 Amazon EC2 队列并发布 EC2 裸机实例, Quick Start、Script Canvas 和 Amazon CloudWatch 实现重大更新实现相应的能力补充, AWS 全面开放托管式的服务 Sumerian, Amazon ECS 服务发现功能现在支持桥接和主机容器联网模式, 而 Amazon Connect 则与五大新公司实现了集成; VMware 在成都举办“迈向数字化之巅”大中华区 CIO 高峰论坛, 助推企业转型; Twitter 正在将部分基础数据从物理数据中心移入 Google Cloud 平台, 谷歌收购云技术创业企 Cask Data, 构建运行大数据分析工具; 2018 微软 Build 全球开发者大会盛大举办, 核心亮点为 AI、云以及边缘计算, 微软/戴尔与美国情报部门达成了一项协议为美国政府提供云服务, 微软 OneDrive 已成为企业最受欢迎云存储; 阿里云营收 133.9 亿元, 连续 12 季度规模翻番, 积极投入 AI 领域推出人工猪肉以及 AI 收银员已成功运作, 在物联网方面发布 Link 生活物联网平台 2.0, 携手积微物联共建攀钢 ET 工业大脑, 并且宣布同贵州的下一个五年计划; 腾讯云黑石数据中心助推重庆智造, 企业级研发管理平台 CODING 获腾讯云一亿元战略融资, 2018 腾讯“云+未来”峰会顺利召开公布多项重要内容, 包括数据安全解决方案数盾、携手中科院国家天文台落地 FAST 和全新智慧零售产品等; 华为敏捷网络助力宜春市人民医院新北院打造赣西区域医疗中心, 阿里云投诉华为靠虚假材料谋取中标因缺乏证据被驳回, 熙菱信息联手华为共同建设海淀视频云。

开源云方面, 2018 OpenStack 温哥华峰会上浪潮发布了最新的 InCloud OpenStack 5.5; EasyStack 完成 C+轮融资, 云计算定义超融合下半场; 九州云赴

中国 IT 用户版的“达沃斯”峰会。

云安全厂商方面，启明星辰集团重磅发布工业物联网安全解决方案——《启明星辰集团工业物联网网络安全解决方案白皮书》；另外启明星辰荣获中国网络安全与信息产业“金智奖”三项大奖。

其他安全厂商，国内方面：山石云•格获得 VMware Ready 认证；360 企业安全集团推进 2018 年教育部高等教育司产学合作协同育人项目；安恒发布教育行业信息安全监测预警管理平台，协助杭州城市数据大脑建设；国外方面，Fortinet 发布新型管线连接器扩展了 Fabric-Ready 合作伙伴计划，为多厂商环境实现自动化安全，Checkpoint 公布其 2018 第一季财报。

容器动态方面，ContainerD1.0 正式版发布，其整合了 CIR plugin；Kata Container1.0 发布，发力容器内核级隔离安全。

安全新技术方面，IOS 11.3.1 系统发布时间仅仅一周时间被腾讯 Keenlab 团队成功越狱；多个系统或软件漏洞被曝，硬件专家公布 PoC 利用码可致 Windows 系统崩溃，CNNVD 收到关于 PHP 输入验证安全漏洞，PGP 与 S/MIME 加密协议被曝严重漏洞；恶意软件和勒索软件的威胁也没有停歇，SynAck 勒索软件的最新变种利用多种新颖且复杂的技术躲避检测，近 400 个政企网站感染 Coinhive 恶意软件秘密挖掘加密货币，Telegrab 恶意软件可以获取 Telegram 的密码、cookie 及密钥文件，Mac 设备则遭遇新门罗币挖矿软件入侵，而恶意软件系统“VPNFilter”已被 FBI 控制。

网络安全公司投融资方面，总共发生 2 起收购和 7 起投资事件。智能网络服务平台 StackPath 完成对基础设施监控方案提供商 Server Density 的收购，安全意识培训与模拟网络钓鱼平台 KnowBe4 完成对德国和中欧安全与合规教育的解释

性视频制作公司和内容服务提供商 **exploqii** 的收购。融资方面，旨在帮助企业对抗网络安全威胁的安全公司 **IronNet Cybersecurity** 以 7800 万美元的 B 轮融资拔得头筹，网络安全公司 **Namogoo** 和网络运营解决方案提供商 **Indeni** 分别以 1500 万美元的 B 轮融资和 1400 万美元融资分列二三位。

2018 年 5 月 30 日

启明星辰云计算安全事业部

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 推出 Amazon EC2 队列

5 月 2 日，Amazon EC2 队列是一项全新的功能，它简化了跨不同 Amazon EC2 实例类型、可用区以及按需、Amazon EC2 预留实例 (RI) 和 Amazon EC2 Spot 购买模式预置 Amazon EC2 容量的方式。现在只需一次 API 调用，即可按照期望的规模、性能和成本，跨 EC2 实例类型和购买模式预置容量。

用户可以创建 EC2 队列规范来定义目标容量、需要的 EC2 实例类型、以及使用按需、预留实例和 Spot 购买模式将填充队列的水平。此外，用户还可以规定 EC2 队列在扩展时是否应当分别考虑每个实例的内核数量或内存量，或者平均考虑所有实例。然后 EC2 队列将根据这些首选项，启动满足目标容量需求的最低价格实例组合。通过 EC2 队列，只需在 AWS 管理控制台几次点击，即可综合使用多种实例类型和购买模式，以成本高效的方式预置容量。

1.2 使用 Amazon CloudWatch 监控 Amazon Kinesis Data Analytics 应用程序

5 月 7 日，现在可以使用新的 Amazon CloudWatch KPU 使用率指标来监控 Amazon Kinesis Data Analytics 应用程序。该指标将显示您的应用程序使用的 Kinesis 处理单元 (KPU) 数量。KPU 是一个流处理容量单元，由 4 GB 内存、1 个 vCPU 计算单元和相应的联网功能组成。通过 KPU 使用率指标，可以更方便地监控随着服务根据执行分析的需要弹性扩展 KPU 数量时，应用程序资源的增加和减少。

Kinesis Data Analytics 是实时处理流数据的一种最简单的方法，采用的是标准 SQL 且无需了解新的编程语言或处理框架。通过 Kinesis Data Analytics，能够使用 SQL 查询流数据或构建整个流式处理应用程序，以便获取可执行的见解并及时响应业务和客户需求。

1.3 Lumberyard Beta 1.14 推出 Script Canvas 重大更新

5 月 11 日, AWS 推出 Lumberyard Beta 1.14, 它包含 200 多项改进、漏洞修复和新功能, 包括对游戏引擎的可视化脚本环境的重大更新、新组件实体等等。其中的一些亮点包括:

- 变量管理器 (Script Canvas): 使用 Variable Manager (变量管理器) 窗格来创建和管理所支持变量类型的变量, 创建或设置变量节点, 以及将变量添加到 Script Canvas 图形以发布声明和进行初始化。
- 书签 (Script Canvas): 添加访问 Script Canvas 图形上具体位置的快捷方式。可以使用 Bookmarks (书签) 窗格或快捷键快速移动到该位置。
- 新组件 (组件实体系统): 包括用于创建受风影响的卷的 Wind Volume 组件; 用于创建现实的详细云影响的 Sky Cloud 组件; 以及用于对卷内的对象施加物理力的 Force Volume 组件。
- 支持 Visual Studio 2017。

1.4 Amazon Sumerian 全面开放

5 月 15 日, AWS 宣布 Amazon Sumerian 全面开放, 这是一种托管式的服务, 允许开发人员快速方便地创建和发布增强现实 (AR)、虚拟现实 (VR) 和 3D 应用程序, 无需任何专门的编程或 3D 图形专业知识。

Amazon Sumerian 为应用程序的设计、开发和部署提供集成开发环境 (IDE)、编辑器、资产库、API 以及虚拟人物 (称为 Sumerian Host)。使用 Sumerian 创建的应用程序在兼容浏览器中发布, 有利于开发人员“一次创建, 广泛发布”。场景可以使用兼容的 VR 头盔 (HTC Vive、HTC Vive Pro 和 Oculus Rift)、兼容 AR 的 iOS 和 Android 设备、笔记本电脑以及数字标牌查看。

1.5 Quick Start 推出适用于在 AWS 云上运行的 Tableau Server

5 月 3 日, 这一更新后的 Quick Start 可以自动在 Amazon Web Services (AWS) 云上的独立或集群环境中部署 Tableau Server。此次更新后, 可以在 Linux 或 Microsoft Windows Server 上进行部署。

Tableau Server 是在线共享和分发在 Tableau 中创建的商业智能内容并针对这些内容展开协作的解决方案。借助 Tableau Server, 可以在 Tableau Desktop 中创建工作簿和视图、控制面板以及数据源, 并将这些内容发布到服务器上。

此 Quick Start 会使用 AWS CloudFormation 模板安装以下某种架构：

- 独立架构。将 Tableau Server 安装到运行 Microsoft Windows Server、CentOS 或 Ubuntu Server 的 Amazon EC2 m4.4xlarge 实例上的默认 Virtual Private Cloud (VPC)。
- 集群架构。将 Tableau Server 安装到至少三个运行 Microsoft Windows Server、CentOS 或 Ubuntu Server 的 Amazon EC2 m4.4xlarge 实例上的全新或现有 VPC。此选项会构建包含 VPC、子网、NAT 网关、安全组、堡垒主机和其他组件的 AWS 环境。

1.6 正式发布 Amazon EC2 裸机实例

5 月 17 日，Amazon Elastic Compute Cloud (EC2) 裸机实例可让应用程序直接访问底层服务器的处理器和内存资源。这些实例非常适合需要访问硬件功能集（例如 Intel® VT-x）的工作负载，或需要在非虚拟化环境中运行以符合许可或支持要求的应用程序。裸机实例基于 Nitro 系统、一系列由 AWS 构建的硬件卸载和服务器保护组件而构建，这些组件相结合可安全地向 EC2 实例提供高性能网络和存储资源。在 AWS re:Invent 2017 大会上，AWS 宣布推出预览版裸机实例，而现在它将以 i3.metal 实例的形式与 EC2 存储优化 I3 实例系列一起正式发布。

使用裸机实例，EC2 客户可运行受益于深度性能分析工具的应用程序、需要直接访问裸机基础设施的专用工作负载、在虚拟环境中不受支持的传统工作负载，以及受许可限制的第 1 层关键业务应用程序。此外，裸机实例还可让客户运行虚拟化安全容器，例如 Clear Linux Containers。裸机实例上的工作负载可继续利用 AWS 云的所有综合服务和功能，例如 Amazon Elastic Block Store (EBS)、Elastic Load Balancer (ELB) 和 Amazon Virtual Private Cloud (VPC)。

裸机 I3 实例自 2017 年 8 月开始投产，可为 VMware 和 AWS 经过 18 个月的联合开发和测试后发布的 VMware Cloud on AWS 服务提供支持。借助这种独特的混合云服务，客户能够使用其现有的基于 VMware 的部署与管理方法将其本地数据中心环境扩展到 AWS 云中。裸机实例使 VMware 能够直接在 EC2 托管的基础设施上运行其包括 vSphere Hypervisor 在内的全套软件。

作为规模新颖、归入 I3 实例系列的实例，裸机 I3 实例与该系列中的其他实例具有相同的特性，包括针对低延迟、极高的随机 I/O 性能以及高顺序读取吞吐量进行优化的

NVMe SSD 支持的实例存储。I3.metal 实例由 2.3 GHz Intel Xeon 处理器提供支持，提供 36 个超线程内核（72 个逻辑处理器）、512 GiB 内存和 15.2 TB 的 NVMe SSD 支持的实例存储。这些实例使用基于 Elastic Network Adapter (ENA) 的增强型网络提供高达 25 Gbps 的聚合网络带宽，从而可提供高网络吞吐量和更低的延迟。

1.7 Amazon ECS 服务发现功能支持桥接和主机容器联网模式

5 月 22 日，可以使用 Amazon Elastic Container Service (Amazon ECS) 服务发现功能发现和连接使用桥接和主机联网模式的 Amazon ECS 任务。用户可以轻松开始使用 ECS 服务发现功能发现在 Amazon ECS 上运行的容器化应用程序。

之前，ECS 服务发现功能仅支持使用 awsvpc 联网模式启动的任务，该模式会为每个正在运行的任务分配一个专用的弹性联网接口。

现在，除了使用 awsvpc 模式启动的任务外，还可以使用 Amazon ECS 服务发现功能处理使用桥接模式和主机联网模式启动的任务。用户可以使用 ECS 服务发现功能处理更多容器负载，而无需对网络做出任何更改。

1.8 Amazon Connect 与五大新公司实现了集成

5 月 22 日，AWS Quick Start 团队、解决方案架构师和联络中心合作伙伴 Segment 团队联合 AWS 合作伙伴，宣布推出五大全新 Amazon Connect 集成，以便提供联络中心解决方案：

- eGain Solve - 全渠道案例管理、分析和人工智能 IVR 与知识管理
- Teleopti Workforce Management (WFM) - 预测联络中心人员需求、配备人员并优化员工队伍
- WEBTEXT Contact Center Messaging - 支持短信、彩信图片、Facebook Messenger 和其他消息收发渠道的发起人交互。
- HERE Location Suite - 位置智能，包括绘图、地理编码、路线选择、交通状况、运输、定位和地理可视化
- 采用 VoiceFoundry 的 ServiceNow IT service management - 实现工作流程自动化，提高员工工作效率，提升客户体验

Amazon Connect 集成自动部署，利用 AWS 合作伙伴提供的热门服务和解决方案扩展了 Amazon Connect 提供的基于云的联络中心功能。

可以使用 Amazon Connect 集成在 AWS 云中轻松设置和管理您的联络中心，并为客

户关系管理 (CRM)、人力资源优化 (WFO)、分析、统一通信 (UC) 和其他使用案例提供关键解决方案。这些解决方案遵循 AWS 最佳实践，以实现最高级别的安全性和可用性。

2. VMWare 云安全动态

2.1 VMware 助推企业转型，迈向数字化之巅

5 月 9 日，全球企业软件创新领导者 VMware 在成都举办“迈向数字化之巅”大中华区 CIO 高峰论坛，聚焦亚太地区 CIO 数字化转型旅程的下一个演进阶段，与业界精英人士畅谈未来的工作、商业和应用，助力 CIO 引领企业的数字化转型进程，同时更深刻地揭示数字化转型的范围和影响，助力数字化业务，帮助企业赢得成功。

VMware 全球副总裁、大中华区总裁郭尊华表示：“当下，各企业机构正掀起数字化转型的热潮，以期带来更好的体验，并推动业务增长。基于业界领先的产品和解决方案，VMware 助力企业通过加速数字化转型之旅实现可能，实践自己对客户的坚定承诺。”



VMware NSX 网络和安全产品组合提供了一致的运维环境连接、保护和运行虚拟云网络。该产品组合拥有面向数据中心、分支机构、云和电信环境的全新增强功能，并推动对传统和现代应用框架的支持。借助 VMware NSX 产品组合，客户将能在私有数据中心、AWS、Azure 和 IBM Cloud 之间进行一致的网络与安全管理。

网络虚拟化：VMware NSX 数据中心是业内部署最广泛的企业数据中心网络虚拟化平台，全球共计拥有逾 4500 位客户。NSX 数据中心助力客户设计、构建与运维由下一代策略所驱动的数据中心，连接、保护传统及现代应用并实现其自动化，并借助该基础架构固有的安全性来保护应用与数据。

软件定义的广域网（SD-WAN）：VMware NSX SD-WAN by VeloCloud 是行业领先的 SD-WAN 解决方案，集成了最佳实时网络覆盖的经济性、灵活性与云端服务的部署速度、规模化和自动化。通过部署 NSX SD-WAN 解决方案，客户可利用全面可视化、指标、控制、所有设备和用户端点自动化以及更低的总成本来提供更好地云与应用性能。NSX SD-WAN 与 NSXData Center 以及 NSX Cloud 的集成，助力客户将一致的网络和安全策略从数据中心拓展到分支机构直至云端，同时提供端到端的操作可视化和控制性。NSX SD-WAN by VeloCloud 为企业和电信运营商提供了一个可扩展平台，在一致连续的业务策略框架下集成本地服务和云端服务。NSX SD-WAN 以三种方式交付给客户：客户可从 VMware 或全球 60 多个通信服务提供商处购买 NSX SD-WAN 服务；NSX SD-WAN 也可作为本地部署解决方案进行购买。目前已有 2000 多名客户采用 NSX SD-WAN。

多云网络：VMware NSX Cloud 为运行在基于 VMware 的私有数据中心以及原生公有云的各种应用提供一致的网络与安全。NSX Cloud 解决了采用多个公有云时面临的运维挑战，如：多个云之间相互矛盾的策略和构造；针对云、区域和 VPC 改变策略要求手工操作；东西向流量的有限运维可视化；以及每个公有云特定的运行工具等。

混合云连接：VMware NSX Hybrid Connect 帮助客户化解混合云的最大挑战之一——一致的网络。借助 VMware NSX Hybrid Connect，客户创建性能卓越、安全性更高的一致软件架构，在丝毫不损监督和控制的情况下，将数据中心和云端相连。NSX Hybrid Connect 支持客户将工作负载从任意 VMware 环境无缝迁移到现代软件定义的数据中心环境，无论其运行于本地、公有云亦或由 VMwareCloud Provider 合作伙伴提供运营。

VMware 帮助客户创建一个完整闭环、基于意图的系统，借助 360 度可视化的运维自动化提供性能反馈，并通过主动与预测性分析实现快速补救。VMware vRealize Network Insight 可在私有云、公有云以及虚拟和物理环境下为客户提供所部署服务内各种组件的完整可视化。VMware vRealize Suite 助力客户获得连续、近乎实时的网络资源健康、性能和容量数据，并为资源和服务编排工作流的闭环式集成提供优先警报。

3. GOOGLE 云动态

3.1 Twitter 将部分基础数据移入 Google Cloud

5 月 7 日报道，Twitter 正在将部分基础数据从物理数据中心移入 Google Cloud 平台。值得明确的是，这个社交公司的大部分基础结构依然会留在其数据中心，但是特定的工作将

会利用 Google 的云计算。



具体而言，Twitter 是在迁移它的冷数据存储和灵活计算的 Hadoop 集群。这样将大大提高 Twitter 的工程团队在使用数据平台时的生产力，对 Twitter 的平均用户体验并无多大的直观影响。

Hadoop 计算机系统是 Twitter 数据平台的核心。这家公司运行着多个 Hadoop 集群，有的甚至达到世界最大水平。Twitter 的 Hadoop 文件系统主机会跨越成千上万的服务器，群集超过 300PB 的数据。换言之，基础数据的处理变得越加棘手，为了跟上发展的速度，Twitter 在找寻能解决该问题的好方法。

不过，此次迁移的速度并不十分迅速，Twitter 方面也并没有做出一个确切的时间安排。但 Twitter 的 CTO Parag Agrawal 还是谈及了 Twitter 对未来收益的希望。

他认为，“一旦迁移完成，我们将更快地满足容量供应、提高灵活性、获得更广泛的工具和服务系统、改善安全措施，并增强重大事件的修复能力。从体系结构来说，我们还将能够将这类 Hadoop 工作负载进行的计算和存储进行分工，这将是一个具有长期性规模和运营效益的举措。”

当然，Google 对 Twitter 这个大客户的到来也是拍手称快的。

Google Cloud 的 CTO Brian Stevens 在申明中表示，“无论是 Twitter 为了满足平台需求而设立的工程战略，还是 Google Cloud 在全球范围内提供的服务，这两者都是具有高度一致性的。Google Cloud 平台的数据方案以及基础架构将给 Twitter 提供其平台所需要的技术灵活性和一致性，我们期待与他们的团队保持长期的技术合作关系。”

3.2 谷歌收购云技术创企 Cask Data，构建运行大数据分析工具

5 月 17 日报道，谷歌正在努力围绕谷歌云构建更深入的企业业务。然而，在涉及企业间的收入和使用情况时，谷歌云继续落后于亚马逊的 AWS 和微软的 Azure。近日，谷歌收购了一家来自 Palo Alto 的创企 Cask Data，该公司专门构建基于 Hadoop 的大数据分析服务的解决方案。

在不到一周前，谷歌刚刚宣布收购 Velostrata，这是一家来自以色列的创企，可帮助企业云环境和混合环境中迁移并运行数据、应用和其他 IT 功能。

4. 微软 Azure 云动态

4.1 微软 Build 2018 亮点： AI 与云并驾齐驱 边缘计算高频出现

5 月 8 日凌晨（美国当地时间 5 月 7 日下午），2018 微软 Build 全球开发者大会在西雅图的微软总部开幕。在今年的 Build 大会现场，微软率先亮出的便是一系列围绕边缘计算的全新服务，包括开源 Azure IoT Edge Runtime 平台；上线首个支持在边缘环境中部署的 Azure 认知服务定制化视觉服务；上线 Project Kinect for Azure 传感器套件……

“人工智能既可以应用于云端，也可以应用于终端。”在接受 21 世纪经济报道记者专访时，微软全球资深副总裁、微软亚太研发集团主席兼微软亚洲研究院院长洪小文毫不讳言边缘计算的趋势。在他看来，云计算对于收集数据和模型训练极为重要，终端则更强调执行能力，也拥有更为独特的应用场景。

数据显示，预计到 2020 年，智能设备总数将超过 200 亿台。这些设备将非常智能，甚至无需一直连接到云端，就能具备看、听、推理、预测的能力。这就是智能边缘计算。

微软 CEO 萨提亚·纳德拉认为，智能云与智能边缘计算近在咫尺，它将为消费者、企业，以及从手术室到工厂车间的各个行业的不同应用场景开启全新机遇。

此外，微软推出全新的 Project Kinect for Azure。它是一组包含微软飞行时间深度摄像头在内的传感器套件，集尺寸小和功耗低于一身，并具备在边缘环境中进行人工智能计算的能力。

当然，在智能云 Azure 和人工智能方面，微软也进行了诸多升级，如新上线针对多声道音源提供高级声音处理的语音设备开发工具包，开放预览用于深层神经网络处理的架构 Project Brainwave，升级 Bot Framework 与认知服务等。

在 Build 2018 开幕式，微软智能语音助手和亚马逊 Alexa 上演了和谐互动的一幕，两个

不同的语音助手正式整合,可以相互“召唤”。在整合的同时,两个助手也开始呈现角色分化:微软小娜主要用于工作和商务交流,亚马逊 Alexa 则接入生活类服务。

这是业内智能语音助手“各司其职”的首个案例。“不同的语音助手拥有自己的特长。小娜基于微软在商业领域的积累,在商务助理上更加擅长,Alexa 则能够对接天气通知、日程、购物、音乐等服务。”洪小文表示,“但对于用户而言,对两者功能的需求都是存在的,因此两个语音助手相互发挥特长,能够为用户带来更好的体验。”

除了在智能语音助手这样的具体产品上更加开放,微软在 AI 资源开放上也走得很远。Build 2018 期间,微软全球执行副总裁、微软人工智能及微软研究事业部负责人沈向洋宣布,向开发者开放微软研究院与人工智能事业部的资源。

4.2 微软与美情报部门达成革命性协议:为美国政府提供云服务

5 月 16 日消息,微软/戴尔与美国情报部门达成了一项革命性协议,为美国政府提供云服务。

4.3 微软 OneDrive 成企业最受欢迎云存储

5 月 25 日报道,数据机构 Spiceworks 对北美和欧洲 544 家企业调查后发现,大多数企业都在使用微软 OneDrive 作为云存储解决方案,远远领先其他竞争对手。该机构称,每个 Office 365 订阅中包含 1 TB 的 OneDrive,使 OneDrive 成为提供独立云存储产品并节省资金的一种方式。

5. 阿里云动态

5.1 阿里云营收 133.9 亿元 连续 12 季度规模翻番

5 月 4 日,阿里巴巴集团公布其最新财报,阿里云在 2018 财年(2017 年 4 月至 2018 年 3 月底)营收达 133.9 亿元,季度营收连续 12 个季度保持规模翻番。

财报数据显示,2018 财年第四季度(2018 年 1 月到 3 月底)阿里云营收规模为 43.85 亿元,比去年同期增长 103%,连续第 12 个季度保持营收规模翻番。财年营收规模来看,阿里云在过去的 12 个月中(2018 财年为 2017 年 4 月到 2018 年 3 月底),阿里云营收规模达到了 133.9 亿元,同比增长 101%。

过去三年,阿里云每个季度以三位数左右的增速在不断扩大自己的市场领先优势。研究机构 IDC 通过销售、市场等渠道得到的调研数据显示,截止到 2017 年上半年,阿里云在中

国云计算 IaaS 市场份额为 47.6%，几乎为市场所有追随者的总和，也是市场第二名的 5 倍。

与亚马逊在美国市场的情况类似，阿里云在中国云计算市场也充当了开拓者的角色。阿里云于 2009 年创立，当时阿里巴巴正在面对极端复杂的商业和技术难题，从购买软件走向了技术自研道路，由此累积的技术产品和方法论，为阿里云的成功创造了历史机遇。经过 18 年的发展，阿里巴巴本身已经成为数字经济体的最佳案例，其在自身业务场景中形成了完善的数字化转型技术和方法论。面对数字化转型的挑战，大中型企业们也纷纷转向阿里云来寻求解决方案。

5.2 积微物联携手阿里集团 共建攀钢 ET 工业大脑

5 月 8 日，积微物联、阿里云、攀钢集团共同签署合作协议，三方将以攀钢集团为场景试点，以阿里云为技术载体，以积微物联为平台，三方共建“钢铁大脑”，深化 ET 工业大脑在钢铁生产领域的应用。



将人工智能深入钢铁生产核心环节，以降低钢铁料消耗，节省生产成本，共同实现攀钢集团智能制造、智慧营销、智慧采购、智慧物流和智能装备的“两化融合”目标，全力打造国家级智能制造试点示范产线，共同赋能国内钢铁行业的智能化发展。

5.3 阿里云推出人工智能猪肉

在 5 月 11 日举行的阿里开放日上，阿里云的人工智能猪肉也正式亮相，同时还展示一款用 AI 技术种出来的陕西阎良甜瓜。



据阿里云方面介绍，这批猪由阿里云与四川特驱集团、德康集团合作养殖。特驱集团是国内农业产业化国家重点龙头企业，年生猪养殖 1000 万头左右。他们在养殖过程中全面引入了阿里云人工智能技术，包括各类猪只数量识别、猪群行为特征分析、疾病识别和预警、无人过磅等。

5.4 阿里云开发 AI 收银员 上海地铁已运用语音购票技术

5 月 23 日，在阿里云栖大会 武汉峰会上，阿里云展示了 AI 点餐技术。客户以每秒 5 个字的速度，向一台机器点单，并频繁更换语句，这台机器对每次对话均作出了精准应答。

阿里巴巴语音交互首席科学家鄢志杰向记者表示，如今机器对人类口语的理解能力带到了新的高度，这完全打破了“语音唤醒+语音指令”传统命令式交互方式，阿里云首创的流式多意图口语理解引擎，极大地提升了对人类随意、自然的口语表达的理解力，“这些模块并非简单级联，而是深度融合而形成了多模态语音交互方案。现在这套解决方案已经在阿里云上开放，开发者开箱即用”。鄢志杰称。

阿里云方面介绍，这项解决方案除了可以做收银员之外，还能在地铁卖票。目前，上海地铁已经部署了这一技术。乘客直接说出目的地，售票机便可选择合适的站点和路线。测试数据显示，普通买票耗时往往超过 30 秒，而语音购票全程只需要 10 秒左右。

5.5 阿里云发布 Link 生活物联网平台 2.0 支持天猫精灵等三大语音 AI 操控

5 月 23 日，阿里云在云栖大会 武汉峰会上推出了全新阿里云 Link 生活物联网平台 2.0，支持亿级设备全球接入、提供多语言语音 AI 交互能力，可帮助中国家电企业快速智能化出海，全球消费者都可轻松获得中国家电产品的智能体验。

阿里云 Link 生活物联网平台 2.0 是阿里巴巴宣布全面进军物联网领域后，开拓智能生活领域的一个标志性平台产品。同时也是阿里云帮助国内智能家电企业走出国门，打开世界市场的利器。



据悉，阿里云 Link 生活物联网平台 2.0 为家电厂商提供了丰富的功能，仅需 5 个步骤，即可快速搭建全球家电智能化平台：

一是语音 AI 控制，一键接入全球 Top3 智能语音平台。基于全球化部署，阿里云打通了全球主流智能语音平台，包括天猫精灵、Amazon Echo、Google Home 等智能音箱都可轻松接入，语音发出指令即可控制智能家电。

二是场景联动，一键接入全屋智能生态，为用户提供最好的生活体验，避免切换遥控器或者多个手机 APP 的繁琐操作。可以控制电动窗帘开、关、停，控制灯光开、关和亮度，或者通过智能音箱进行场景选择或切换，如开启在家模式、切换睡眠模式等。

三是全球洞洞察，实时感知市场需求和趋势，及时调整产品功能开发、销售策略，针对市场需求做出快速反应。

四是软硬结合，云边端一体保障设备安全。在端测提供小于 2K 内存空间需求的 iTLS，兼容 TLS 的同时提供更高的网络效率。同时提供 3 种设备认证模式和 4 种安全等级芯片，为企业提供方便快捷，可自由组合的安全解决方案。

五是公版 APP，提供简单易用的应用开发模板，无需自行重复开发，直接调用账号系统、消息通道、配网界面即可部署一款定制化的智能家居 APP。

目前，阿里云上激活的物联网设备超过 5000 万台，覆盖超过 1000 个品牌，更有大量明星级智能单品，如知名厨卫品牌九牧，平台运营后开发人员投入减少了 50%，上市时间提

前 3 个月；国内销量第一的扫地机器人科沃斯，只用 1 天就完成了语音 AI 配置，5 天完成了地图轨迹功能开发。

5.6 阿里云宣布同贵州的下一个五年计划 八大领域全面突进

5 月 26 日消息，贵阳数博会正式开幕，阿里云在数博会上宣布了了在贵州发展的的下一个五年计划，将从扶贫、农业、旅游、医疗、工业、教育、政务、创业八大领域全面推动贵州大数据产业。同时，贵阳将会成为阿里云的全球备案中心和技术支持中心。

6. 腾讯云动态

6.1 腾讯云黑石数据中心助推重庆智造

5 月 11 日消息，腾讯云重庆黑石数据中心园区的落地，除了满足重庆本地的云计算需求之外，还可进一步辐射到西南乃至全国的应用市场。

根据资料显示，目前重庆中小企业网站 80% 的服务器都放在外地。本次腾讯云黑石数据中心的落地，将有助于吸引企业回归本地，并且助力企业实现低延迟、高速上网。



“高性能计算不仅需要强劲的计算力，还需要从应用层针对性地匹配解决方案。”吴坚坚介绍，在优势基础能力之上，腾讯云联手合作伙伴共同构建 HPC 和工业设计生态，让高性能计算力更好地服务于工业智能化，推动工业智造云端落地。

6.2 CODING 获腾讯云一亿元战略融资，共同开启云端开发时代

5 月 17 日，企业级研发管理平台 CODING 宣布完成 B+轮融资。本轮融资来自 CODING 的战略合作伙伴腾讯云，融资金额一亿元人民币，将用于国内首款云端工作站

Cloud Studio 及后续产品的研发与迭代。双方将在产品与计算资源层面进行更加深度的对接与合作。



CODING 成立于 2014 年，凭借团队优秀的产品基因、扎实的技术根基、所在领域的巨大市场空间，CODING 持续获得资本认可，三年间已经相继获得来自 IDG 和光速资本的两轮投资。本次腾讯云的 B+ 轮投资也是 CODING 首次接受战略投资。CODING 在开发工具领域深耕三年，已经成功推出“CODING 个人版”、“CODING 企业版”、“CODING 私有部署”等产品，为上千家企业的开发部门提供服务，并为超过 80 万开发者提供简洁的开发环境。

6.3 腾讯云发布数据安全解决方案数盾，解决三大新痛点

5 月 24 日，腾讯云数据安全专家研究员彭思翔博士在 2018 腾讯“云+未来”峰会安全分论坛上指出，合规要求、隐私威胁、量子计算将是当下数据安全面临的三大挑战，亟需全新的思维和格局来应对这场变革。同时，彭思翔也结合腾讯云自研的全流程数据保护方案——数盾，分享了腾讯在保护用户数据安全方面的成果。

彭思翔介绍了腾讯云打造的一款以数据为中心的全流程保护方案——腾讯云数盾，通过数据审计，隐私保护，威胁抵御，量子加密等产品构建了一站式全流程的保护体系。

在合规要求方面，彭思翔认为数据库审计是重要基石。目前腾讯云对数据库操作进行监控及记录，均满足在合规审计需求基础上，能够及时发现数据访问异常和风险，并输出多级告警和详尽报表，确保所有的数据操作可被追溯、审查。同时，加持 AI 能力的数据库审计能够更加精准地发现问题，腾讯云独创 AI 黑白双引擎模型综合判断，自动适配用户操作特

点，检出率和精准度都达到 95% 的业界高水平。

针对隐私保护，彭思翔着重介绍了高级隐私保护技术。作为企业级用户常用的数据脱敏，数盾可实现一键智能脱敏，满足生产数据用于测试、开发、培训和大数据分析场景中的数据脱敏需求。此外，腾讯云数盾当前的匿名化处理、交互式差分隐私框架、PSI 算法拥有简单易用，兼容性强、安全等级高等特点，能够满足企业在敏感数据使用/发布场景里的安全性要求。

值得关注的是，数据保护最重要基础的手段是数据加密，目前腾讯云数盾融合了多种加密解决方案，能够应对量子计算破解带来的安全挑战。预估量子计算出现后会严重影响非对称加密算法的安全性，腾讯云数盾还推出了抗量子加密，是基于散列的能够抵抗量子计算攻击的加密算法。

此外，腾讯云数盾也会将抗量子加密算法集成到其他数据安全产品中，用户可根据需要启用抗量子加密算法，提升各类安全产品的安全可靠。

6.4 腾讯携手中科院国家天文台落地 FAST

5 月 24 日，腾讯云+未来峰会在广州举行。在峰会合作伙伴分论坛，中国科学院国家天文台（以下简称“国家天文台”）与深圳市腾讯计算机系统有限公司（以下简称“腾讯”）就 FAST 天眼数据存储与分析、月球与深空探测数据开发应用签署合作备忘录。这也是继今年 1 月双方达成战略合作之后，具体项目的推进与落地。腾讯云副总裁陈平、国家天文台 FAST 工程副总经理张蜀新、国家探月工程地面应用系统副总师左维进行签约，《中国国家天文》社长、原国家天文台书记刘晓群，腾讯副总裁、腾讯云总裁邱跃鹏及腾讯云副总裁谢岳峰共同出席见证本次签约的达成。



6.5 腾讯云重磅发布全新智慧零售产品 全维助力零售业数字化升级

5 月 24 日消息，腾讯“云+未来”峰会智慧零售专场在广州举办。腾讯云现场重磅发布六款新品，分别是智选、优品、优客、优 Mall、优码、优评，提供包括开店选址、商圈洞察、商品管理、门店运营的全维智慧零售解决方案，全面提升消费体验。目前，永辉、绫致时装、必胜客、蒙牛、百丽国际、美克国际家居等知名零售和餐饮企业已经携手腾讯云共同探索零售行业数字化升级之路。

以百丽国际旗下深圳福田 coco Park Nike 店为例，引入智慧零售解决方案后，整体运营数据产生显著提升：门店销量及坪效方面，客群画像有效提升门店女性 SKU 转化率，实现女子区销售额月环比增长接近 40%；门店布局方面，动线分析帮助优化门店布局，有效发掘门店前后场客流量不均等现象并结合门店装修提供优化方案，调整货品陈列，后续显著提升区域整体收入。

此外国内知名的零售企业永辉，也在积极推动数字化变革。目前，腾讯云智慧零售与永辉生活、超级物种等永辉旗下一系列品牌门店进行合作，在落地门店提供基于优图的视觉 AI 技术，结合永辉自主研发的门店自助收银系统通过人脸识别支付，不掏手机轻松完成购物全流程，极大提升用户门店购物体验。同时通过视觉 AI 技术，用户进店即自动识别其会员信息，捕捉用户在店动线及购物偏好。通过腾讯云大数据应用中台，为零售企业提供品类优化和销量预测，实现精准人货洞察，大幅提升门店经营效率。在此基础上，永辉可全面了解门店丰富用户画像及实时交易转化率，实现全景式消费洞察，并通过数据分析运营更好的服务永辉会员。

值得一提的是，必胜客联合腾讯多个工具打造的智慧餐厅 5 月 23 日在上海大宁隆重开业。据悉，该店集成了多种技术，打造更有趣、更个性化的用餐体验，赋予科技以温度，让顾客体验全新用餐感受。

7. 华为云动态

7.1 华为敏捷网络助力宜春市人民医院新北院打造赣西区域医疗中心

5 月 9 日消息，宜春市人民医院是一所集医疗、科研、教学、防保及康复为一体的三级甲等综合医院，新院区网络建设涉及老区、儿科楼、新院多地中心机房资源拉通。华为提供智慧数字医院敏捷网络方案：大二层网络通过多中心 CE12800 的 vxlan 方式打通，云资源按需漂移；汇聚层部署敏捷 ENP 板卡实现纵向虚拟化和随板 AC 能力；接入层采用上行万

兆骨干、千兆到桌面，帮助宜春人民医院用户在医疗服务水平体验上极大提升，优化医疗资源与诊疗环境，拉通多院区就诊信息共享，简化运营管理维护，增强效率。

7.2 阿里云投诉华为靠虚假材料谋取中标，因缺乏证据被驳回

5 月 25 日消息，近日中国政府采购网公布财政部政府采购信息公告（第五百七十号）显示，阿里云投诉华为软件涉嫌提供虚假材料谋取中标，官方给出的结论是“经审查取证，认为投诉缺乏事实依据，驳回投诉”。

这起云计算招标项目名称为“国家税务总局网络学院培训平台转型升级公有云租用项目”，是 2017 年底政府公有云采购项目。2017 年底，国税总局公开招标的形式采购周期为三年的公有云服务。2017 年 9 月 8 日发布招标公告，开标日期是 2017 年 12 月 11 日。最终中标的供应商为华为软件技术有限公司，中标金额为 1050 万元，为三年服务费用，而项目部署实施费用和其他费用均为 0。

而前文提及的这份公告称，投诉人（即阿里云计算有限公司）因对中央国家机关政府采购中心（国采中心）就本项目作出的质疑答复不满，而提起投诉，认为华为软件涉嫌提供虚假材料谋取中标。

经过审核，相关部门认为现有证据不足以证明华为软件存在提供虚假材料谋取中标的行为，投诉事项缺乏事实依据。另外，尽管华为软件投标文件中提供的部分认证证书不符合招标文件有关要求，扣除相应得分后，华为软件仍排名第一，不影响中标结果。

根据此前国家税务总局网站公布的《国家税务总局网络学院培训平台转型升级公有云租用项目合同书》，按照合同的规定，华为软件所需提供服务有：租用部署云服务器、云存储、负载均衡、CDN、云数据库等设备，为网络培训平台提供稳定可靠、动态弹性的硬件支持，保证并发用户、流量带宽等突发增加时，系统弹性调度资源，及时提供稳定可靠的服务等。

7.3 熙菱信息：联手华为打造海淀视频云

熙菱信息联手华为共同建设的北京市海淀区“网格化图像信息系统微卡口（大数据）平台”项目首战告捷。该项目以熙菱信息的视频图侦及车辆大数据分析系统为核心，采用华为视频云“一云一池”的先进理念，全面解决客户图片接入转发及存储、图片二次解析、车辆大数据应用上云与数据整合的需求，最终赢得了客户认可与项目成功。

二、 开源云动态

1. Openstack 动态

1.1 OpenStack Summit 2018:浪潮 InCloud OpenStack 5.5 海外首发

5月21日,在2018 OpenStack 温哥华峰会上,浪潮发布了最新的 InCloud OpenStack 5.5,在大规模交付、易用性、稳定性、智能化运维等方面均有显著提升。目前,浪潮 InCloud OpenStack 已经在某非运营商客户的“两地三中心”方案中率先部署,并实现单 Region 超过 1000 节点、总规模达 1400+节点的先进开源云基础设施。

此次发布的 InCloud OpenStack 5.5 进一步提升了易用性、大规模部署能力和两地三中心方案支持。InCloud OpenStack 5.5 实现了 OpenStack 的容器化部署,基于容器化技术封装各个组件为独立于宿主操作系统的容器化镜像,依靠统一分发实现一键式批量部署和资源图形化编排,显著提升了易用性。同时,实现了对虚拟机、裸机、容器三种计算资源的同平台统一管理 and 对外提供服务,可轻松对三种资源进行并行调度和管理,实现集计算、存储和网络资源的融合共享,降低运维与管理成本。此外,两地三中心方案可对外提供同城 150KM 双中心双活,异地数据中心主备的容灾能力。

2. Easystack 动态

2.1 EasyStack 完成 C+轮融资,云计算定义超融合下半场

2018年5月15日,中国开源云计算的领导者 EasyStack 在北京举行的春季发布会上正式发布公司中文品牌名——易捷行云,并同时宣布完成由多家人民币基金投资的3亿元 C+轮融资,资金将主要应用于核心技术的研发、云计算产品化的开发,以及企业解决方案的生态投入三大方向。C+轮融资不仅意味着易捷行云 EasyStack (以下简称 EasyStack) 将年内完成拆除 VIE 架构,也意味着开源云计算在中国市场的飞速发展以及行业企业用户的广泛认可。

同时, EasyStack 还发布了 ECS Stack 硬件参考架构,曙光作为 ECS Stack 官方战略合作伙伴,将于第三季度上市相关超融合一体机。此外,在生态布局上, EasyStack 已经拥有超过 100 个生态合作伙伴和超过 300 个渠道合作伙伴。作为春季发布会的又一重磅举措, EasyStack 与博学教育宣布战略合作,成立 EasyStack 博学学院,推出 CKA 等全球容器认证

培训课程，培育中国容器人才市场。

正如 2007 年苹果手机的发布成为从功能手机到智能手机的拐点事件，2018 年将成为超融合下半场的分水岭之年。现在的手机都是智能手机，未来的超融合也都是云就绪超融合。且具备支持多云、以应用为核心、微服务粒度升级的三大特征。EasyStack 联合创始人兼 CTO 刘国辉表示，“ECS Stack 的核心设计思想就是实现从硬件基础设施到软件基础设施的抽象，从管理资源到支撑应用的跨越，从单一云平台向多云管理的延伸。”

1，支持多云形态

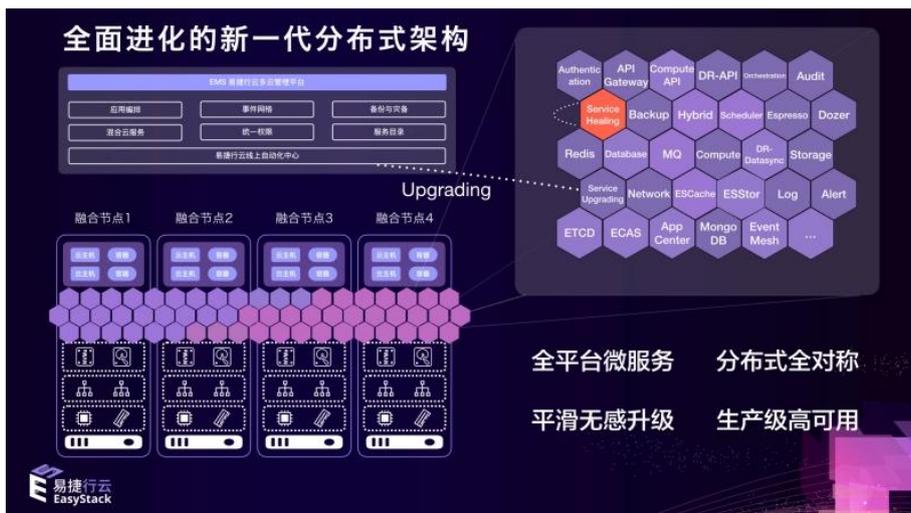
云计算之于超融合，智能操作系统之于手机，这是区别智能机与功能机的基础特征。但下半场的云就绪超融合不仅可以实现对计算、网络、存储的抽象，使用户具备对本地云资源的交付和管控能力，还应当包括多云管理能力。据 IDC 预计，到 2020 年，将有超过 90% 的企业级 IT 组织倾向选择多云架构，可以说多云已经成为大势所趋。



ECS Stack 提供完整的云平台服务能力，不仅具备云主机+容器的双引擎计算服务，还能实现自助式访问 IT 资源，按需申请，敏捷交付；通过多级权限，层级配额，满足用户对于云服务的分配和管控能力，同时支持对云资源使用情况进行精细化计量和可视化呈现。值得一提的是，ECS Stack 还将第四季度引入 EMS 多云管理服务，支持多云形态的业务运营。

2，微服务粒度升级

越来越多的企业客户核心业务上云，传统的平台升级会影响业务连续性，而微服务粒度的升级方式将最大限度地降低这种风险。正如智能手机的 APP 升级，做到新功能升级的平滑无感知，确保以应用为目的的快速迭代。



据悉，ECS Stack 控制平面采用全新设计的微服务架构，基于统一的微服务调度框架实现。不同控制服务之间相互独立，且严格隔离，能够基于微服务的细颗粒升级策略，实现无感知升级。这种微服务粒度的升级特色，便于新功能快速迭代，满足规模企业对业务随需而变的需求。

3. 以应用为核心

云就绪超融合的核心设计思想不是以底层资源分配为目的，而是以支持应用业务为目的，实现从硬件基础设施到软件基础设施的抽象，从管理资源到支撑应用的跨越。



ECS Stack 支持应用中心，目标是让企业级服务的创建、交付、下载如智能手机 App 一样简单。作为面向应用服务提供商和开发者的应用管理和交付平台，用户可与 ECS Stack 的感知式可视化资源编排能力相协同，实现丰富的创建方式、多场景的预置模版、多维的模版管理、灵活的资源调用以及感知式的服务连接关系，以所见即所得的方式规划并构建业务系统，提供可靠、敏捷、高效的服务编排全流程生命周期管理。

用户可以从应用中心选择认证的开源应用软件或商业应用软件，也可以创建和发布自己

的应用到应用中心。不同租户之间的应用可以共享也可以完全隔离，充分保证租户应用的隐私性和隔离性，为构建云时代的新型应用生态系统奠定了基石。

与此同时，EasyStack 还发布了 ECS Stack 和 ECS 相结合的工业互联网场景化方案，并发布 ECS Stack 在教育、医疗、政府、制造行业的行业解决方案。

3. 99CLOUD（九州云）动态

3.1 九州云赴中国 IT 用户版的“达沃斯”峰会

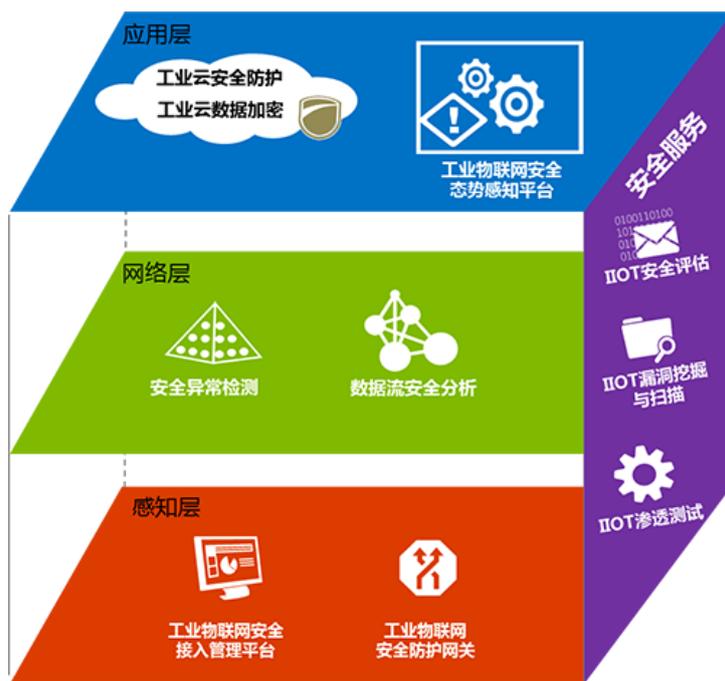
5 月 17 日消息，6 月 2-3 日由 ITSS 数据中心运营管理工作组（DCMG）、双态 IT 联盟主办，ITSS 媒体工作组、OpenStack 基金会金融工作组、中国新一代 IT 产业推进联盟协办的“中国双态 IT 大会乌镇峰会”将在乌镇枕水酒店隆重召开，九州云作为双态运维联盟创始成员单位及大会的赞助商将积极参与其中。

三、云安全厂商动态

1. 启明星辰

1.1 启明星辰集团发布工业物联网网络安全解决方案白皮书

- 在感知层部署物联网端侧设备防护以及管理措施，提供访问控制、安全认证与准入、数据传输加密等安全能力，确保感知层物联网设备的安全性及可视化管理。
- 在网络层部署安全异常检测系统和数据流安全分析系统，实时监测网络层入侵攻击以及流行为异常等网络层威胁。
- 在应用层的主要以云安全防护为基础，云数据加密为保障，通过工业物联网安全态势感知平台实现整体安全的监测、管理、控制和运营。
- 提供工业物联网安全评估、漏洞挖掘与扫描、渗透测试服务，由代码级到业务级安全服务实现安全保障



此解决方案可应用于仓储物流、油气开采、智慧办公、智慧城市、先进制造等多类工业物联网场景，能有效抵御感知、网络和应用各层中典型工业物联网安全威胁，协助用户构建完整动态的工业物联网安全保障体系。

1.2 启明星辰荣获中国网络安全与信息产业“金智奖”三项大奖

5月4日，中国网络安全与信息产业峰会（SCCI）暨金智奖颁奖与《信息安全与通信保密》理事大会在成都隆重召开。启明星辰作为理事单位受邀参加，与来自国内网络安全领域的主管部门领导、专家学者、行业精英齐聚一堂，共同探讨中国网络安全与信息产业健康可持续发展的高质量的发展。

会议最后进行了中国网络安全与信息产业“金智奖”颁奖典礼。“金智奖”的评奖旨在从企业的品牌及智慧价值的角度关注企业的成就与价值，鼓励创新与发展，以推动产业升级，打造产业新格局。

“金智奖”颁奖典礼上，启明星辰荣获三项“金智奖”——2017年度优秀解决方案奖、2017年度优秀产品奖以及2017年度人物杰出成就奖。

2. 山石网科

2.1 山石云·格获得 VMware Ready 认证

近日，经过 VMware 严格、详细的验证测试后，山石云·格 V2.5 获得了 VMware 的最

高认可，并在 VMware NSX 生产环境下得到支持。山石云 格已经达到了 VMware 互操作性标准，并可与 VMware 云基础架构有效地协作。通过山石云 格与 VMware NSX 结合使用，用户可以从全面的威胁可视以及针对数据中心内部和云端的南北向、东西向流量的全自动高级威胁防护中受益。

3. 亚信安全

暂无更新。

4. 绿盟科技

暂无更新。

5. 360 企业安全

5.1 360 企业安全集团 2018 年教育部高等教育司产学研合作协同育人项目

为贯彻落实《国务院办公厅关于深化高等学校创新创业教育改革的实施意见》（国办发〔2015〕36 号）文件精神，深入推进产学研合作协同育人，汇聚企业资源支持高校专业综合改革和创新创业教育，360 企业安全集团（以下简称 360 企业安全）与数十所高校进行产学研合作，提供联合实验室建设、在线实验平台、专业共建、师资培训、资源建设及人才培养等多项服务，助力于高等教育的创新与改革，以产业和技术发展的最新需求推动高校人才培养改革。

根据“教育部高等教育司关于征集 2018 年产学研合作协同育人项目的函”的内容要求，360 企业安全集团拟在“教学内容和课程体系改革项目（精品课程建设）”、“师资培训项目（网络安全师资培训）”、“实践条件建设项目（网络安全实验室建设）”校外实践基地建设项目等四个方面的项目上与高校展开合作，推动高校教学内容更新及课程体系完善，建立体系化的教学资源及应用，支持高校实践教学改革，提升高校在实验教学领域的综合能力，提供学生实习实训岗位，加强管理实习实训管理，提升学习实践能力。

5.2 工信部赴 360 企业安全集团调研

工信部信息化和软件服务业司昨日赴 360 企业安全集团进行调研。调研组参观了工业控制系统安全国家地方联合工程实验室，听取了 360 企业安全集团关于工控安全服务、工业安

全应用实践、工业互联网国内外发展趋势与产业业态等方面的汇报，详细了解了 360 企业安全集团在工业互联网安全生态、工控安全技术趋势、安全保障体系、实验室建设、城市级工业安全监测平台、安全人才培养等方面的实践经验。

6. 安恒

6.1 教育行业信息安全监测预警管理平台正式发布



安恒的风暴中心在教育行业深耕多年，基于对行业的深厚理解和网络安全技术的积累发布了此平台。旨在协助全国各省教育厅、教委、市局明确网络安全责任，加强网络安全监测预警，促进安全通报整改落地，让教育网路空间安全成为常态。

6.2 安恒信息助力杭州城市数据大脑建设

5 月 15 日上午，杭州市政府召开新闻发布会，正式对外发布《杭州市城市数据大脑规划》（以下简称“《规划》”），杭州市数据资源管理局局长郑荣新、杭州市公安局交通警察局副局长孔万峰出席发布会，并对杭州城市数据大脑最新工作进展及发展规划情况进行了整体介绍。安恒信息作为杭州数据大脑建设的参与企业，受邀出席了此次新闻发布会。

郑局长介绍道：“城市数据大脑将散落在城市各个角落的数据（包括政务数据、企业数据、社会数据、互联网数据等等）聚会起来，创新应用云计算、大数据、人工智能等前沿技术，在城市治理领域进行融合计算，打造平台型人工智能中枢，实现城市运行的生命体征感知、公共资源配置、宏观决策指挥、事件预测预警、“城市病”治理等功能。通过这个“大脑”，实时对城市“体检”，感知城市生命体征参数，实现事件的预测预警；优化城市公共资源配置，

将有限的优质资源配置到最为合适的位置，解决入学难、就医难、养老难等问题；为政府的宏观决策提供大数据参考，为市民的生活提供精准化服务；治理“城市病”，缓解交通拥堵、环境污染，降低安全事故发生概率等。”

在城市数据大脑建设中，数据安全问题不容忽视。“城市数据大脑建设始终将数据安全放在首位，建立了多道数据安全屏障。”郑荣新局长在发布会上着重强调了城市数据大脑数据安全性的重要性。并在会上预告了《杭州市政务数据安全保障体系规划》也即将印发，这部规划将对政府各部门的数据安全管理提出明确要求，从源头管控数据安全。

安恒信息作为杭州城市数据大脑建设的参与企业，也将在未来发挥自己在信息安全方面的资源优势，协助用户一起构建杭州城市数据大脑的数据安全保障体系，促进杭州大数据产业的健康发展。

6.3 广州大学与安恒信息正式签约 共建人工智能安全联合实验室

成功签约后，双方将发挥各自的优势资源和特长，通过联合实验室共同开展国家级和省市级重大专项、产业化基金、电子发展基金等项目的立项、申报和项目的执行工作，实现产学研的优势结合。此外，广州大学也可以根据科研需要，将若干需要攻克的关键技术、重大需求通过联合实验室的形式，与安恒信息开展联合研究。

合作双方一致认为，校企联合具有非常强的优势互补关系，将是充分发挥双方各自特长、实现产学研无缝对接、可同时满足核心技术研发和产业化需要的最佳途径。双方将成立联合实验室，以广州大学的网安科研团队力量来推动网络安全的创新技术和产业发展，以安恒信息的人工智能安全研究为抓手，推动联合实验室在相关核心技术方面的研究和积累。安恒信息也将为联合实验室提供最新人工智能安全技术研究成果支撑，实现网络安全科研与工程相结合，与广州大学一同解决国家级网安需求，以及保障广州大学人才培养的实习实训。

7. 安天

暂无信息。

8. Fortinet

8.1 Fortinet 发布新型光纤连接器扩展了 Fabric-Ready 合作伙伴计划

飞塔宣布推出其新型光纤连接器，通过与 Fabric-Ready 联盟合作伙伴技术的开放 API

(应用程序编程接口) 实现多厂商环境中的自动化操作功能。结构连接器提供 Fortinet Security Fabric 解决方案与客户现有安全生态系统的一键连接, 并通过单一玻璃板实现动态操作更改的自动化, 从而缩小安全和合规性差距。初始结构连接器类型包括云, SDN, 威胁智能馈送, ITSM, 自动化工具, SSO / 标识, IaaS 可见性和 Endpoint / CVE。第一套光纤连接器与领先的技术基础架构和解决方案紧密集成, 包括亚马逊网络服务 (AWS), 思科 ACI, 谷歌云平台, 微软 Azure, Nuage Networks VSP, ServiceNow 和 VMware NSX。Fortinet 客户将立即受益于 Fabric Connector 与最新版 FortiOS 6.0 的集成。

9. Checkpoint

9.1 CheckPoint 公布 2018 年第一季度财务业绩报告

总收入: 4.52 亿美元, 同比增长 4%

递延收入: 11.66 亿美元, 同比增长 10%

GAAP (一般公认会计原则) 营运收入: 2.13 亿美元, 占总收入的 47%

非 GAAP 营运收入: 2.39 亿美元, 占总收入的 53%

GAAP 每股收益 (EPS): 1.16 美元, 同比增长 7%

非 GAAP 每股收益 (EPS): 1.3 美元, 同比增长 9%

营运现金流: 4.19 亿美元, 同比增长 18%

业务亮点汇总:

年度新产品之选 – Check Point Infinity: Check Point Infinity 在 2018 年 Network Computing Awards 评选中被评为“年度新产品”。Check Point Infinity 提供一系列广泛的安全技术, 可以保护企业免受最先进的和未知的第五代网络攻击, 现在可以使用 Check Point Infinity Total Protection 进行部署。CheckPoint Infinity Total Protection 是一款突破性全新消费模型, 提供简单全包、基于用户、按年购买的服务。该解决方案提供安全基础架构的关键元素, 包括网络安全硬件和硬件升级、网络安全软件、终端、移动端和云安全软件、安全更新、支持和购买, 这些都在年度购买服务里面。

CloudGuard 产品系列: 帮助企业云应用程序和基础设施免遭第五代网络攻击。CloudGuard 是业界第一套专为软件即服务 (SaaS) 应用程序和基础设施即服务 (IaaS) 解决方案提供高级安全和威胁防护的技术。CloudGuard SaaS 旨在防止账户劫持, 采用正在申请专利的 ID-Guard 技术, 应用于 Microsoft Office365、Google G-Suite、Salesforce、ServiceNow、

Slack、Box、Dropbox、Egnyte 等基于云的应用程序。CloudGuard IaaS 的前身是 vSEC，现在则是 CloudGuard 系列的一员。CloudGuard IaaS 可为所有领先的公共和私有云平台提供第五代高级安全/威胁防护，防御针对基础架构和工作负载的攻击。这些平台包括：Amazon WebServices、Google Cloud Platform、Microsoft Azure、Cisco ACI、OpenStack、VMware NSX、AWS 上的 VMware 云、VMware ESX、阿里云、KVM、Hyper-V 等。

第五代（Gen V）安全管理：最新的 Smart-1 安全设备可以提供第五代安全管理，整合多个控制台并对安全事件进行收集、关联和分析，通过一个单一的设备来监控安全状态以及管理所有规模企业的安全策略。全新的第五代 Smart-1 系列可将性能提升 8 倍，实现高达每秒 100,000 条日志的记录速度，并为安全事件分析提供高存储容量。

“以色列奖”（Israel Prize）：Check Point 创始人兼首席执行官 Gil Shwed 因其在以色列科技行业的突出贡献获得了享誉盛名的“以色列奖”。“以色列奖”是以色列最高的国家荣誉奖项，颁发给在某些领域表现卓越或者对以色列文化和国家做出突出贡献的人。今年的“以色列奖”颁发于以色列 70 周年独立日庆典仪式上，以色列总统、总理、国会议长、教育部长和最高法院院长一同出席了颁奖典礼。

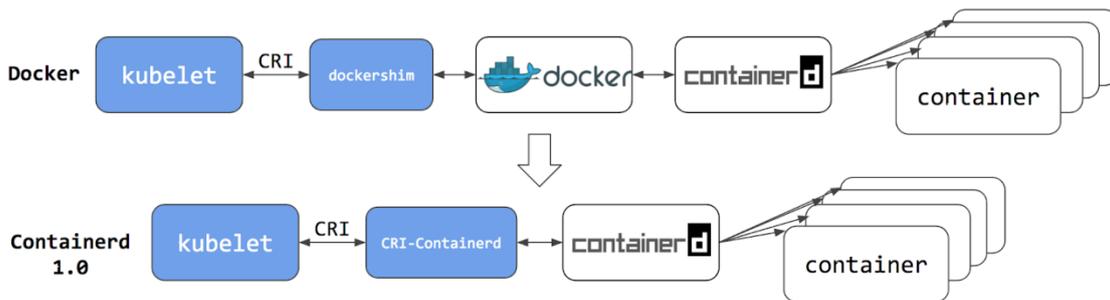
四、 容器技术及安全动态

1. 整合了 CRI plugin 的 Containerd 1.1 发布

containerd 1.1 的发布，将 CRI plugin 整合进了 containerd。简化了结构，提高了集群的性能和稳定。Containerd 1.1 运行在 Kubernetes 1.10 或以上版本，支持所有 Kubernetes 特性。在 Google 云上的 Kubernetes 测试设施，containerd integration 的功能已经和 Docker integration 旗鼓相当。

Kubernetes 的 containerd 架构进化了两次。每次进化使整个体系更加稳定和有效率。

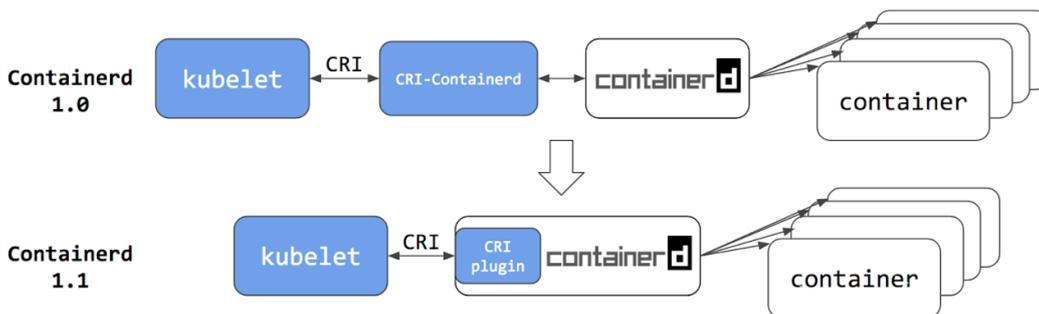
- **containerd1.0**



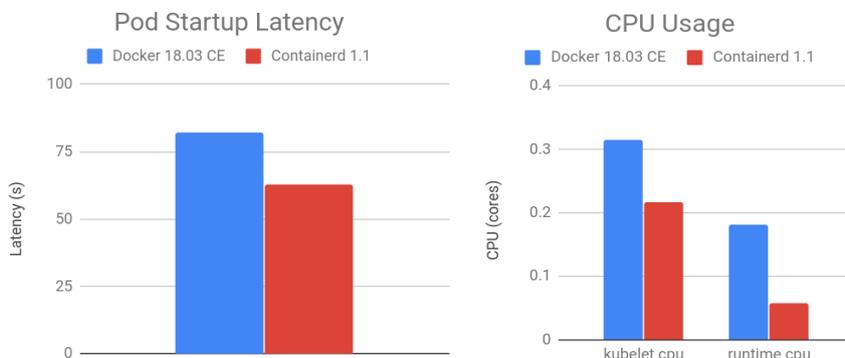
在 containerd 1.0 中，Kubelet 和 containerd 之间的操作使由一个叫做 cri-containerd 的进程来完成的。Cri-containerd 处理来自 Kubelet 的容器运行界面（CRI）服务请求，并且使用 containerd 来管理容器和相应的容器镜像。相比较于 Docker CRI 方案（dockershim），淘汰了体系中一个额外的步骤。

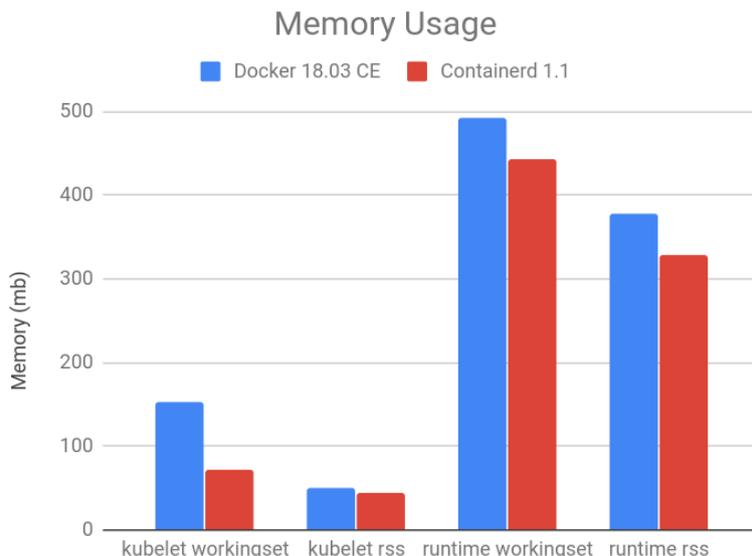
当然，cri-containerd 和 containerd 1.0 仍然是通过 grpc 连接的两个不同的进程。额外的进程使整个流程复杂，用户不容易理解和部署，带来不必要的沟通成本。

● Containerd 1.1 – CRI Plugin（当前版本）



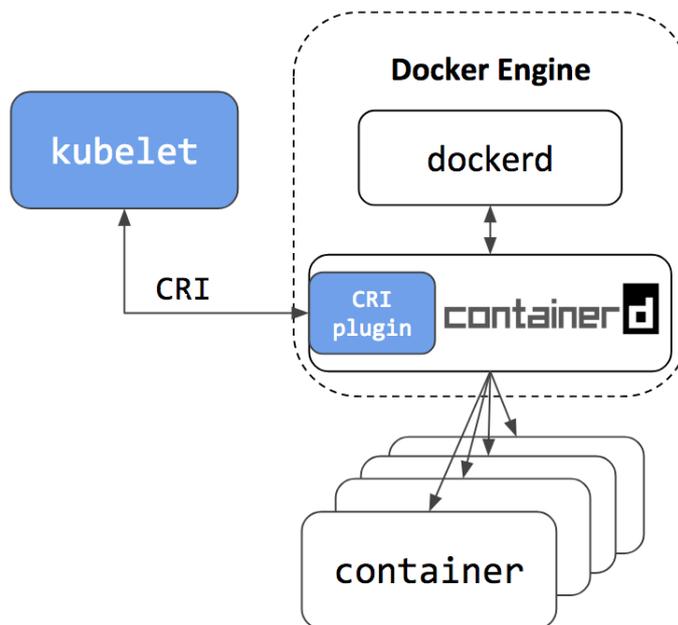
在 containerd 1.1 中，cri-containerd 进程被重构成为 containerd CRI plugin。CRI plugin 被构造进 containerd 1.1，并且默认启用。不同于 cri-containerd，CRI plugin 直接通过函数调用来和 containerd 交互。这个新架构使整合更加稳定和有效，并淘汰了额外的 grpc hop。用户可以直接在 Kubernetes 使用 containerd 1.1。Cri-containerd 进程不再需要了。





● dockerd 的进化

Docker Engine 是构建在 containerd 之上的。下一个 Docker 社区版 (Docker CE) 将使用 containerd 1.1。当然，默认内置和启用了 CRI plugin。这意味着有特定需求的 Docker 用户可以选择继续使用 Docker Engine，与此同时，也能够用内置的，同时也被 Docker Engine 使用的 containerd 来配置 Kubernetes。下图说明了 containerd 同时被 Docker Engine 和 Kubelet 使用：



既然 containerd 同时被 Docker Engine 和 Kubelet 使用，那这意味着用户选择使用了 containerd 后，不仅可以得到新的 Kubernetes 特性，性能和稳定的提升，也将同时为了保留

使用 Docker Engine 的选项以便满足其他的情况。

Containerd namespace 机制是被用于保证 Kubelet 和 Docker Engine 不会看到和进入对方的建立的容器和镜像。这是为了不让二者互相干扰。也意味着：

用户将不能使用 `docker ps` 命令查看到 Kubernetes 创建的容器。请使用 `crictl ps` 替代。反之亦然。用户不能使用 `crictl ps` 命令查看到 Docker CLI 创建的融洽。`crictl create` 和 `crictl runp` 命令只用于故障排除。不建议手动在生产环境下的 nodes 上使用 `crictl on` 来启动 pod 或容器。

用户不能使用 `docker images` 命令查看到 Kubernetes 拉取的镜像。请使用 `crictl images` 命令替代。反之亦然，Kubernetes 看不到 `docker pull`, `docker load` 或 `docker build` 创建的镜像。请使用 `crictl pull` 命令替代，如果你需要载入一个镜像请使用 `ctr cri load`。

2. Kata Containers 1.0 稳定版问世

Kata Containers 整合了 intel 的 Clear Containers 和 Hyper.sh 的 runV，能够提供给虚拟化容器一个独立的运行环境，在运行效率与安全级别上与虚拟机相差不大。

对于 Kata Containers，每一个 container/pod 都是基于一个独立的 kernel 实例来作为一个轻量级的虚拟机。自从每一个 container/pod 运行于独立的虚拟机上，他们不再从宿主机内核上获取相应所有的权限。这种措施简化了您需要采取的安全策略，而且能更好的避免容器攻击宿主机内核的可能性。

Kata Containers 使得容器能够作为 CaaS（容器即服务）在任意的裸机上运行。由于容器之间有硬件来作为隔离，它允许互不信任的租户使用同一个集群。假定还有网络安全策略来提供集群内租户之间的网络隔离。

五、安全新产品及技术

1. iPhone X IOS 11.3.1 被腾讯 Keenlab 团队成功越狱

腾讯 KeenLab 团队成员“Liang Chen”推特上分享图片，其团队成功越狱了一部运行 iOS 11.3.1 系统的 iPhone X。值得一提的是，IOS 11.3.1 系统发布时间仅仅一周时间，团队破解速度相当之快。据悉，在 InfiltrateCon 2018 大会上，腾讯 Keenlab 团队演示了这次越狱，通过分享的图片来看，这台运行 iOS 11.3.1 的 iPhone X 已经成功安装了 cydia 破解组件，底部

文字显示系统版本为 11.3.1。不过需要注意的是，腾讯 KeenLab 并不会发布适合普通用户使用的越狱工具，只是进行了越狱演示。

2. 漏洞导致 Windows 系统崩溃，硬件专家公布 PoC 利用码

Bitdefender 公司的研究员 Marius Tivadar 在 GitHub 上发布了一段 PoC 代码，即便在计算机被锁的情况下也能在几秒内导致 Windows 计算机崩溃。该 PoC 代码利用的是微软处理 NTFS 文件系统镜像过程中存在的一个漏洞，代码中含有格式错误的 NTFS 镜像，用户可提取这个图镜像并将其放在 USB 中，然后将 USB 直接插入 Windows 计算机中就能导致系统在几秒内崩溃，导致蓝屏死机 (BSOD)。Tivadar 详细说明该漏洞情况及其影响时指出，系统的自动播放可被默认激活。即使禁用自动播放功能，只要访问文件还是会导致系统崩溃。例如当 Windows Defender 扫描 USB 或其它工具打开 USB 时就会导致系统崩溃。

3. CNNVD 关于 PHP 输入验证安全漏洞的通报

近日，国家信息安全漏洞库 (CNNVD) 收到关于 PHP 输入验证安全漏洞 (CNNVD-201805-054、CVE-2018-10547) 情况的报送。成功利用漏洞的攻击者，可在用户不知情的情况下，在该用户浏览器中执行任意代码。PHP 5.6.36 之前的版本，7.0.27 之前的 7.0.x 版本，7.1.13 之前的 7.1.x 版本，7.2.1 之前的 7.2.x 等版本均受漏洞影响。目前，PHP 官方已经发布新版本修复了该漏洞，建议用户及时确认是否受到漏洞影响，尽快采取修补措施。

4. Synack 勒索软件利用多种高级技术躲避检测

近日，研究人员发现 SynAck 勒索软件的最新变种利用多种新颖且复杂的技术躲避检测。通常情况下，为了能够在被感染系统中存在更长的时间，攻击者通常会添加多种防御技术来识别检测工具的审查。SynAck 勒索软件就部署了“常用技术”，并为新的变种添加了 Process Doppelgänger 代码注入技术。这种技术最早出现在 Black Hat 欧洲 2017 大会上，利用这种技术的攻击方式对所有 Windows 平台都有效，而且能够攻击主流的安全产品。利用这项技术，SynAck 勒索软件能够伪装成存储在磁盘上的合法程序，最终运行恶意代码，且不会更改可能引发警报的文件。此外，SynAck 还使用混淆技术、常见识别技术，甚至还会测试

目标系统的键盘语言设置，来躲避检测。如果系统默认语言设置为西里尔文，这款软件就不会执行。

5. 近 400 个政企网站感染 Coinhive 恶意软件，秘密挖掘加密货币

来自 Bad Packets Report 的安全研究员 Troy Mursch 发现，使用过时版本的 Drupal 内容管理系统的一些网站正在成为黑客挖掘加密货币的受害者。这次活动袭击了约 400 个网站，虽然主要目标是美国的政府机构和教育机构，但多家科技公司的网站也感染了该病毒。Mursch 收集受影响的网站名单中，包括美国国家劳工关系委员会（NLRB）、中国高科技公司的联想、台湾网络硬件制造商 D-Link 以及加州大学洛杉矶分校（UCLA）。美国、墨西哥、土耳其、秘鲁、南非和意大利的官方网站也受到影响。Mursch 发现所有受感染的 JavaScript 代码都指向相同的域名（vuuwd.com）和相同的 Coinhive 密钥，这意味着它是所有这些攻击背后的单个个体或实体。Mursch 之前的研究发现近 5 万个网站正在进行加密活动，其中许多是不知情的。

6. 邮件形同裸奔，PGP 与 S/MIME 加密协议被曝严重漏洞

由 9 名学者组成的团队向全世界发出警告，OpenPGP 和 S/MIME 电子邮件加密工具中的严重漏洞。该研究小组称，这个代号为 EFAIL 的漏洞如果被利用，将允许攻击者从发送或接收的消息中提取明文内容。Electronic Frontier Foundation（EFF）的研究人员也证实了这些漏洞的存在，他们建议用户卸载 Pretty Good Privacy 和 S/MIME 应用程序，直到发布修复补丁为止。专家们披露了两种被称为 EFAIL 的攻击变体，在这两种情况下，黑客需要处于加密电子邮件拦截的位置，例如黑客攻击目标电子邮件账户或进行中间人攻击（MitM）。“EFAIL 攻击利用 OpenPGP 和 S/MIME 标准中的漏洞揭示加密电子邮件的明文。简而言之，EFAIL 滥用 HTML 电子邮件的活动内容，例如外部加载的图像或样式，通过请求 URL 来渗透明文。”研究人员发表的博客文章中称。“要创建这些渗透通道，攻击者首先需要访问加密的电子邮件，例如通过窃听网络流量，攻击电子邮件帐户、电子邮件服务器、备份系统或客户端。这些电子邮件甚至可能是在几年前收集的。“攻击者操纵受保护电子邮件中的密文，并将包含自定义 HTML 代码的修改消息发送给原始接收者或发件人。

7. Telegrab 恶意软件可以获取 Telegram 的密码、cookie 及密钥文

件

思科 Talos 研究人员发现了名为 Telegrab 的病毒，这个病毒会从 telegram 桌面版中窃取信息。分析这款恶意软件后研究人员发现，软件是由说俄语的黑客开发的，而目标也是俄语用户。恶意代码是 Telegrab 恶意软件的一个变体，Telegrab 首次发现于 2018 年 4 月 4 日功能是收集 telegram 的缓存和密钥文件。Telegrab 恶意软件的第二个版本发现于 2018 年 4 月 10 日，开发团队似乎非常活跃。尽管 Telegrab 的第一个版本只会窃取文本文件，浏览器密码和 cookie，但第二个版本实现了窃取 Telegram 缓存和 Steam 登录密码、劫持 telegram 聊天的能力。

8. FBI 控制感染几十个国家 50 万台路由器和存储设备的

VPNFilter

北京时间 5 月 23 日晚，思科公司发布安全预警称，俄罗斯黑客利用恶意软件，已感染几十个国家的至少 50 万台路由器和存储设备。攻击中使用了高级模块化恶意软件系统“VPNFilter”，这是思科 Talos 团队与多个部门以及执法机构一直追踪研究的恶意软件。尽管目前研究尚未完成，但思科决定提前公布结果，以便受害者及潜在受害者及时防御与响应。就在思科发布报告后不久，美国联邦调查局称已经控制 VPNFilter 的一个关键域名，这个域名被用来与 VPNFilter 僵尸网络中的路由器和其他 NAS 设备进行通信。相关法庭文件显示，攻击与俄罗斯政府支持的黑客组织 Fancy Bear 有关，Fancy Bear 又称作 APT 28、Sofacy 等，指 2007 年开始活跃，曾发起过多次攻击，是一个臭名昭著的黑客组织。

9. Mac 设备遭遇新门罗币挖矿软件入侵

大量 Mac 用户发现，一个名为 mshelper 的进程占用了他们的 CPU 和电池，事实上，这是一款门罗币挖矿病毒。Malwarebytes 的研究人员对 mshelper 恶意软件进行了分析，虽然没能确定传播方式，但假冒的 Flash Player 安装程序，恶意文档或盗版软件应该是主要渠道。程序是一个名为 pplauncher 的文件，由启动守护程序（com.pplauncher.plist）保护进程，程序由 Golang 开发，并且相对较大（3.5 Mb）。

六、 络安全投融资、收购事件

1. 收购

1.1 StackPath 完成对 Server Density 的收购

5 月 14 日，StackPath 完成对 Server Density 的收购，收购价未公开。StackPath 是一家网络安全技术公司，为用户提供安全、快速和规模化的智能网络服务平台。Server Density 是一个 SaaS 产品，它帮助用户管理和监控他们的基础设施。

1.2 KnowBe4 完成对 exploqii 的收购

5 月 22 日，KnowBe4 完成对 exploqii 的收购，收购价未公开。KNOWBE4 是一个安全意识培训与模拟网络钓鱼平台，帮助企业员工加强网络安全意识，避免网络钓鱼的攻击。exploqii 则是德国和中欧安全与合规教育的解释性视频制作公司和内容服务提供商。

2. 投融资

2.1 Namogoo 获得 1500 万美元的 B 轮融资

5 月 1 日，Namogoo 从 Blumberg Capital 和其他 3 位投资者处获得 1500 万美元的 B 轮融资。Namogoo 是一个网络安全公司，其独特的技术可以检测并阻止数字恶意软件，防止未经授权的广告和恶意软件窃取客户信息，影响销售渠道和整体客户的体验。

2.2 IronNet Cybersecurity 获得 7800 万美元的 B 轮融资

5 月 3 日，IronNet Cybersecurity 从 C5 Capial 和其他 2 位投资者处获得 7800 万美元的 B 轮融资。IronNet 成立于 2014 年，旨在帮助企业对抗网络安全威胁。IronNet 表示将会在私营部门的网络安全上继续投入，并声称其技术可以提供实时的全网情况监测，并利用高级的行为学模型和 10 亿兆级别的大数据分析，及时发现异常并进行处理。

2.3 CUJO 获得未知数额 B 轮融资

5 月 17 日，CUJO 从 Charter Communications 处获得未知数额的 B 轮融资。CUJO 是一个为电信运营商和网关制造商提供 SaaS 解决方案的人工智能平台。

2.4 Indeni 获得 1400 万美元融资

5 月 22 日, Indeni 从 RTP Ventures 和其他 2 位投资者处获得 1400 万美元的融资。Indeni 是美国的一家网络运营解决方案提供商, 利用来自专家、机器学习以及自动化社区的帮助, 使企业能够预测到网络中断, 避免出现重大故障问题和宕机所带来的高额成本。

2.5 Runsafe Security Inc 获得 240 万美元种子轮融资

5 月 22 日, Runsafe Security Inc 从 Alsop Louie Partners 和 Center for Innovative Technology 处获得 240 万美元的种子轮融资。Runsafe Security 公司是针对嵌入式系统和设备脆弱性的网络强化技术的先驱。

2.6 Openpath Security Inc 获得 700 万美元种子轮融资

5 月 22 日, Openpath Security Inc 从 Openpath Security Inc 和其他 4 位投资者处获得 700 万美元的种子轮融资。Openpath Security 公司为企业提供了一个移动和云支持的访问控制系统。