内容摘要

云厂商方面，Amazon Connect 和 Amazon Cloud Directory 均已通过 ISO 相关认证，Amazon 网络负载均衡器在欧洲区域开通，并且 AWS 推出洞察功能。VMWare 则完成对 CloudCoreo 的收购，同时戴尔确认正在考虑和子公司 VMware 合并作为上市公司返回股市。Google 向第三方开放自研 AI 芯片 TPU，按小时收费。微软与小米签署合作备忘录，助其打入国际市场。阿里云在 MWC 发布 8 款云计算 AI 产品，并在 2018 冬奥会亮相阿里云 ET 奥运大脑。联通联合腾讯云全面启动 31 省合作。华为在 MWC 上展示 5G 云 VR 解决方案。

开源云方面，Gartner 官方声明从未评选 OpenStack 八大厂商。经济学人新年关注 EasyStack 等四家中国云厂商，九州云 2017 年营收过亿。

云安全厂商方面，启明星辰集团受邀出席 2018 ITS CHINA 年度盛典，并作《智能交通行业大数据平台安全》的主题演讲。其他安全厂商，国内方面：360 企业安全宣布与 VMware 在云计算和虚拟化领域展开全面合作，并参与支持“第十七次计算机和移动终端病毒疫情调查活动”。安恒信息举办高校教师网络安全技能精讲班，助力网络空间安全一级学科专业建设。国外方面：Fortinet 推出 100Gbps+的 NGFW 硬件防火墙，应对企业上云所产生的更高加密数据带宽需要，同时和 Google 云合作推出支持 BYOL（自带证书）的 VM 防火墙，还被阿联酋电信服务提供商选定为其提供云统一威胁管理（UTM）托管安全服务；CheckPoint 推出三款全新安全管理设备防御“第五代”威胁和攻击，并推出 CloudGuard 主

动防御的云安全解决方案。

容器动态方面，Subtree 发布 Dotmesh，实现容器应用和微服务状态的捕获、组织和共享；Rancher 2.0 里程碑版本发布，支持添加自定义节点。

安全新技术方面，当用户处于隐私浏览模式时，Firefox 59 将从 URL 中去除引用信息以防止用户意外泄漏敏感信息；新技术利用 X.509 数字证书建立隐蔽数据交换通道传输数据。移动安全方面，三星与 KoolSpan 合作实现三星智能机安全通信；以色列移动取证公司 Cellebrite 已经找到了可以解锁几乎所有 iPhone 设备的方法，其中可能包括最新的 iPhone X；旨在保护用户加密货币安全的防黑客智能手机 SIKUR Phone 出现。

网络安全市场方面，二月发生了 3 起收购和 7 起融资事件。其中 Splunk 以收购价 3.5 亿美元完成对 Phantom 的收购。国内自适应安全服务商青藤云安全融获 2 亿 B 轮融资。国外方面，实时网络安全防护管理厂商 Vectra Networks、运营网络可视化公司 CyberX 和移动目标防御解决方案厂商 Morphisec 公司均获得超过千万美元的融资金额。

2018 年 3 月 1 日

启明星辰核心技术研究院云安全研究组

目录

国内外云+安全动态月报

一、 云厂商动态

1. AWS 云安全动态

1.1 Amazon Connect 现已通过 ISO 认证

Amazon Connect 是目前通过 ISO 9001、ISO 27001、ISO 27017 和 ISO 27018 等标准认证的 AWS 服务之一。AWS 通过对其控制措施实施广泛的审计以维持认证，确保影响公司和客户信息保密性、完整性和可用性的信息安全风险得到恰当管理。您可以直接下载 AWS ISO 证书的复印件使用，无需另行认证：AWS ISO 9001 证书、AWS ISO 27001 证书、AWS ISO 27017 证书和 AWS ISO 27018 证书。

Amazon Connect 现已在所有开放此服务的 AWS 区域通过 ISO 认证。首次使用 Amazon Connect 的客户可以选择 AWS Free Tier 以试用此服务。如需了解 Amazon Connect 这一自助式云联系中心的更多信息，请访问 Amazon Connect 网站。

1.2 Amazon Cloud Directory 通过 SOC 和 ISO 认证

现在可以使用 Amazon Cloud Directory 来管理有系统和组织控制(SOC)、ISO 27001、ISO 27017、ISO 27018 或 ISO 9001 合规性要求的应用程序层级数据。

利用 Cloud Directory，您可以搭建灵活的原生云目录，从而沿多个维度组织数据层级，例如组织结构图、课程目录和设备注册表等。例如，您可以创建能在报告结构、位置和成本中心的单独层次结构中导航的组织结构图。

SOC 和 ISO 27001、ISO 27017、ISO 27018 和 ISO 9001 合规性支持也在所有开放 Cloud Directory 的 AWS 区域提供。您可以使用 AWS Artifact 下载 AWS SOC 报告和 ISO 证书。

1.3 Amazon RDS 和 AWS Database Migration Service 支持从 SQL Server 复制

Amazon RDS for SQL Server 现已支持变更数据捕获 (CDC)，从而可复制到不同的目标数据库。所有 Enterprise Edition 版本以及 SQL Server 2016 SP1 及以后的 Standard Edition 版本均支持 CDC。

CDC 可以结合 AWS Database Migration Service (DMS) 使用，将来自 SQL Server 源数据库的变更复制到 DMS 支持的任何目标数据库。DMS 将自动检测 RDS 上的 SQL Server 实例。

1.4 网络负载均衡器现已在欧洲 (巴黎) 区域开放

网络负载均衡器旨在确保以超低的延迟实现每秒处理上百万条请求的能力，现已在 AWS 欧洲 (巴黎) 区域开放。网络负载均衡器还经过了优化，能够处理不稳定的流量模式，同时在每个可用区使用单个静态 IP 地址。它在连接级别 (第 4 层) 运行，根据 IP 协议数据将连接路由至 Amazon EC2 实例、容器和 IP 地址。此外，它还保护客户端侧的源 IP，允许应用程序查看客户端 IP 地址以便应用程序用于进一步的处理。

在该地区推出后，网络负载均衡器现已在如下 15 个 AWS 区域开放：美国东部 (弗吉尼亚北部)、美国东部 (俄亥俄)、美国西部 (加利福尼亚北部)、美国西部 (俄勒冈)、欧洲 (爱尔兰)、欧洲 (法兰克福)、欧洲 (伦敦)、欧洲 (巴黎)、亚太区域 (孟买)、亚太区域 (首尔)、亚太区域 (悉尼)、亚太区域 (新加坡)、亚太区域 (东京) 和南美洲 (圣保罗)。

1.5 AWS 账户活动实时洞察功能推出

AWS 账户活动实时洞察是一种解决方案，它可帮助您更轻松地实时监控您的 AWS 账户活动。此解决方案自动预置必要的服务，以记录和可视化显示您 AWS 账户的资源访问和使用指标。AWS 账户活动实时洞察旨在提供一个实时指标可视化显示的框架，让您只需注意添加新的指标，而非相关的基础设施操作。

对于没有办法记录和可视化显示账户活动指标的客户而言，这一解决方案可以提供宝贵的洞察，了解谁在访问您的资源以及资源的使用方式。这一洞察可以帮助您做好更好的决策，提高安全性和效率，促进合规性审计，以及优化成本。

此解决方案部署 AWS CloudTrail 来记录账户活动，使用 Amazon Kinesis Data Analytics 来实时计算指标，并使用 Amazon DynamoDB 可靠地存储计算所得数据。此解决方案还提供可自定义控制面板功能，以可视化的方式实时显示账户活动。计算的指标适用于创建、修改和删除 60 多种支持的 AWS 服务的 API 调用。

1.6 Amazon AppStream 2.0 现在支持跨 AWS 区域复制映像

现在，您可以跨 AWS 区域复制 Amazon AppStream 2.0 映像。在多个 AWS 区域中使用相同的映像可以在 AppStream 2.0 上更轻松地管理应用程序的全局部署。通过在靠近您

用户的 AWS 区域部署您的应用程序，您可以为他们提供响应更迅捷的体验。

要将映像复制到另一个 AWS 区域，请启动 AppStream 2.0 控制台并选择包含现有映像的区域。在导航窗格中，依次选择 Images (映像)、您的现有映像，然后单击 Actions (操作)，选择 Copy (复制)，再选择您的目标 AWS 区域。您还可以使用 CopyImage API 以编程方式复制映像。

2. VMware 云动态

2.1 VMWare 完成对 CloudCoreo 的收购

2 月 14 日，VMWare 完成对 CloudCoreo 的收购，收购价未公开。CloudCoreo 是一家云基础设施管理安全公司，其目标是希望能够让企业客户随时随地的部署、管理以及防护云应用。

2.2 戴尔确认：我们或是公开上市或是让 VMware 吃掉我们

科技巨头戴尔在向美国金融监管机构提交的文件中证实，戴尔正在考虑和子公司 VMware 合并作为上市公司返回股票市场，否则的话，就什么都不会做。VMware 于 1 月 31 日提交的时间表 13D SEC 备案今天公开，其中称：戴尔科技公司正在评估各种潜在的商业机会，包括考虑戴尔科技普通股的潜在公开募股或戴尔技术公司与股票发行者之间的潜在业务合并。戴尔科技公司也在考虑维持现状。戴尔科技目前评估的潜在商业机不包括将戴尔科技出售给第三方或股票发行者。

3. GOOGLE 云动态

3.1 苹果 iCloud 竟用谷歌公共云存储用户数据

2 月 26 日据国外媒体报道，苹果上个月在其网站上更新的一份文件中首次承认，使用了谷歌的公共云来为旗下的 iCloud 业务提供数据存储服务。

3.2 谷歌向第三方开放自研 AI 芯片 TPU：每小时 6.5 美元

谷歌在一篇博客文章中正式宣布，将以“有限数量”向谷歌云客户开放张量处理器（Tensor Processing Unit，简称 TPU）服务。TPU 是谷歌为机器学习而设计的人工智能定制芯片。将 TPU 开放，对于选择在谷歌云平台上运行机器学习模型的客户来说，可谓好事一桩。但谷歌这次开放的 TPU 数量有限，而且按时收费，每小时成本为 6．50 美元。

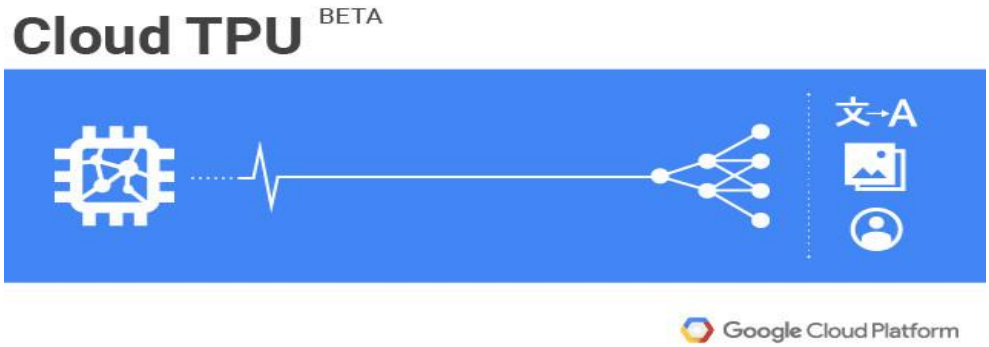
谷歌在 2016 年低调推出了 TPU 项目，并在去年 5 月的年度开发者大会上推出了第二代 TPU。这次更新让谷歌进入了更为复杂的深度学习培训阶段。

TPU 专用于人工智能和机器学习，可为谷歌带来两大好处：

首先，利用自主研发的芯片，谷歌可以在核心的计算基础设施方面更便宜、更有效地减少对英特尔、英伟达等芯片制造商的依赖。拥有自己的硬件使谷歌能够更快地进行实验。

其次，新的 TPU 也为谷歌的云计算业务带来额外收入，现在，谷歌云平台（GCP）和谷歌的业务应用程序 GSuite 每季度可超过 10 亿美元收入。

谷歌目前允许公司租用单个 TPU 板卡，今年晚些时候，将允许企业租用多个板卡，并连接成名为 TPU pod 的超级计算机网络。



4. 微软 Azure 云动态

4.1 小米与微软签署合作备忘录 助推小米进国际市场

2 月 23 日报道，微软在云计算、人工智能等领域的技术储备将与小米在移动智能设备上的储备进行结合，帮助小米产品进入国际市场。

参考消息网-出海记记者从小米获悉，根据双方签署的战略合作备忘录，小米与微软将主要围绕以下几个方面展开合作：

云服务支持：随着小米不断进军国际市场，小米用户已经遍及全球各地。小米与微软正在共同探索，进一步利用微软智能云 Azure 平台和服务，在更广阔的国际市场上为小米提供用户数据存储、带宽、计算，及更多创新服务。

笔记本电脑类设备：小米与微软正在讨论进一步深化双方在笔记本电脑类设备上的合作，在联合市场推广、渠道支持和小米未来笔记本及笔记本类产品研发等方面，微软将大力推动小米产品进入更多全球市场。

微软小娜与小米智能音箱：双方正在讨论将微软小娜（Cortana）与小米智能音箱整合进军国际市场的更多可能。小米与微软的工程、产品及业务推广团队之间将进行经常性的高层交流，进一步推进此项合作。

广泛的人工智能合作：围绕人工智能技术的研发和应用，双方将进一步拓展多层次的广泛合作，其中将涉及计算机视觉、语音、自然语言处理、文本输入、对话式人工智能、知识库、搜索等微软人工智能技术，以及 Bing 搜索、Edge 浏览器、微软小娜、微软小冰、SwiftKey、微软翻译 Translator、Pix 相机、认知服务、Skype 等微软产品及服务。双方围绕人工智能技术及产品展开的深度合作，加之小米所拥有的全球最大的 IoT 网络平台以及业内领先的人工智能产品优势，将更好地整合小米硬件、软件和互联网产品，为小米用户带来更完善的全新体验。

5. 阿里云动态

5.1 阿里云 MWC 发布 8 款云计算 AI 产品，和微软 Azure 开始缩小差距

阿里云刚刚在西班牙巴塞罗那 MWC 展会上，同步发布了 8 款云计算和人工智能产品，包括图像搜索、智能客服云小蜜、大数据 PaaS 产品 Dataphin 等，并表示中国数字化转型正在进入快车道，新零售、新制造、ET 城市大脑等产业 AI 实践已经快世界一步。

5.2 阿里云 ET 奥运大脑亮相 2018 冬奥会 百年赛事向数字时代进化

2 月 11 日报道在牵手奥运一年之后，2 月 10 日，阿里巴巴在 2018 年冬季奥运会上全面展示了科技将为这项百年赛事带来的改变。阿里巴巴首席市场官董本洪向外界系统阐释了“云上奥运”理念，并发布阿里云 ET 奥运大脑，推动奥运向数字时代的升级进化。

据悉，现场发布的阿里云 ET 奥运大脑是面向奥运等大型体育赛事推出的人工智能系统，在阿里云强大的计算能力基础上，阿里巴巴将计算机视觉、机器学习、IoT、大数据等技术与体育赛事相结合，从数字化运营、数字化体验、数字化竞技、数字化传播四个方面推动奥运进化。

5.3 阿里云助特驱集团全面 AI 养猪

继交通、工业、航空等之后，阿里云再次将产业 AI 推进到了农业领域。2 月 6 日，阿里云与四川特驱集团、德康集团宣布达成合作，将对 ET 大脑进行针对性训练与研发，最终全面实现 AI 养猪。在前期的理论验证阶段，ET 大脑提升了母猪年生产能力 3 头，死淘率降低了 3%左右。

6. 腾讯云动态

6.1 腾讯云与创梦天地达成合作

2 月 6 日，腾讯云在深圳腾讯滨海大厦召开发布会，称与创梦天地达成战略合作。腾讯云方面称，通过此次合作，他们将联手创梦天地通过技术赋能、数据赋能、生态赋能提升运

营能力、服务能力，为行业注入新的发展动力，赋能泛娱乐技术新生态。

腾讯云方面称，技术服务是他们最主要的能力之一，多年来，他们基于 QQ、QQ 空间、腾讯游戏、微信等业务的技术锤炼，已经能够提供集云计算、云数据、云运营于一体的云端服务体验。而在腾讯云当中，腾讯游戏云则已经覆盖了五大洲的 36 个全球服务节点，并与与腾讯开放平台、应用宝、手机 QQ、玩吧、QQ 浏览器和腾讯外部平台资源对接，为游戏厂商构建游戏生态；

具体来说，创梦天地的游戏业务将通过腾讯游戏云的计算能力、网络资源和云端托管 Hadoop 服务，为玩家带来更好的游戏体验；并通过腾讯云的海外节点和全球互联网络，助力乐逗游戏出海。

6.2 联通混改项目落地 联合腾讯云全面启动 31 省合作

日前中国联通与腾讯云云服务合作平台正式发布上线，该平台将为国内外客户提供“腾讯云+联通”的公有云及混合云服务。

未来，腾讯云与中国联通将继续携手，进一步广泛聚合内容与应用，在公有云、混合云、行业云等多领域全面合作。

7. 华为云动态

7.1 MWC 2018：华为 xLab 展示 5G 云 VR 解决方案

在 MWC 2018 位于 4 号馆的华为 xLab 展台，展示了华为与 TPCAST 共同开发的 5G 云 VR 解决方案。

不论是 HTC Vive、Oculus Rift 还是 PSVR，数据线一直是困扰消费者和 VR 开发商的一大难题。此前，HTC 联合 TPCAST、英特尔发布了基于 60Ghz 传输技术的无线 VR 解决，但是受到基站、成本等因素的限制，这项技术并没有快速在消费级 VR 设备中普及。而高传输速率、低延迟的 5G 网络的商用化，也许能解决无线 VR 的难题。

7.2 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 Gartner 官方声明：从未评选 OpenStack 八大厂商

近日，互联网媒体开始纷传一篇文章，标题为《Gartner 评选出的八大 OpenStack 公司》，由于该文章的指向性，部分行业客户对此提出了质疑。针对此事，Gartner 特别做出了阐述和澄清，Gartner 表示从未以任何形式组织或参与 OpenStack 八大厂商评选。

2017 年，在 OpenStack 正值发展七周年之际，国际权威咨询机构 Gartner 发布了《2017 年 OpenStack 分销与支持服务市场竞争格局》分析报告（Competitive Landscape: OpenStack Distributions and Support Services Market, 2017），报告分析了 OpenStack 分销与支持服务市场格局，从市场、产品、技术三个方面为 OpenStack 未来的发展方向提出了建议与意见，成为众多目光焦点，引发业内众多讨论。

对于 Gartner 的这份报告，各家媒体众说纷纭，莫衷一是。但市场上出现的《Gartner 评选出的八大 OpenStack 公司》之类的报道和 Gartner 做这份市场调查的初衷违背，因此特别在 Gartner 官方微信网站（Gartnerinc）上，由 Gartner 研究总监张毅先生撰文，阐述这份报告的调查初衷、方法和结论，披露报告的核心内容，指出“报告及文中提及的厂商名录并非完全涵盖整个市场，仅代表市场中某些典型类型的厂商“，并特别强调“其他相关文章 Gartner 均不予认可”。

Gartner 亦在这份声明结尾重申”中国 OpenStack 市场既包括华为、华三、浪潮、中兴、大型系统集成商的身影，也有海云捷迅、有云（现同方有云）、优铭云、九州云、EasyStack、及云途腾等明星初创公司的身影”， Gartner 认为 OpenStack 的发展离不开行业内各大小玩家与广大用户的贡献与参与，并没有评选所谓的“八大厂商”。

2. Easystack 动态

2.1 经济学人新年关注 EasyStack 等四家中国云计算企业

《经济学人》刊登的“中国云计算行业发力赶超西方”的报道中，作者曾来到中国实地采访，并着重选择了四家中国云计算的代表企业——阿里云(中国最大的公有云企业)、EasyStack(中国开源云计算领导企业)、兴业数金(中国金融行业云的领导者)、UCloud(中国估

值最高的独立公有云企业)进行了面对面沟通和关注。

3. 99CLOUD（九州云）动态

3.1 99Cloud 年营收近亿

99Cloud 主要帮助企业解决开源技术最后一公里的难题。基于 OpenStack 和相关开源技术，打造适合企业级使用的智能计算/存储融合架构云平台，从而简化数据中心管理运维，降低企业数据中心成本支出。

整个 2017 年，99Cloud 的营收近亿元；

在资本方面，99Cloud 也曾获得 2 轮投资：

A 轮：5000 万人民币，英特尔领投，上海仪电跟投；

B 轮：1.5 亿人民币，华泰领投、泰达、徽瑾创投。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰集团受邀出席 2018 ITS CHINA 年度盛典

近日，以“智启新时代 智联通未来”为主题的第六届 ITS CHINA 年度盛典在北京成功举办。此次盛典由智能交通网主办，邀请了多位行业领导及学术领袖等重量级嘉宾，共享智能交通领域年度成果，探讨我国新时代背景下智能交通的发展理念和方向。作为国内网络安全领军企业，启明星辰集团受邀参加大会，并作《智能交通行业大数据平台安全》的主题演讲。

启明星辰于波表示：“随着大数据技术在智能交通行业中的应用越发广泛，其所暴露出来的数据安全问题不容忽视。数据平台在平台安全、服务安全、数据安全、数据确权问题、APT 攻击防御、个人隐私保护、大数据聚合分析等方面都可能存在安全风险，一旦重要数据遭到泄露，将严重危害国家、企业乃至个人的切身利益，造成无法估量的损失。因此，在推广大数据应用的同时，大数据的安全问题更是重中之重。”

启明星辰大数据安全主要包括：认证，授权，审计，脱敏，加密等方面的安全管控。实现用户账号进行统一管理；数据资源操作权限的策略管理；所有用户对大数据平台的操作行为都会留下审计记录，包括：用户对数据资源的操作、用户对 DSM 的配置管理、用户对访

问策略和授权策略的配置管理。

2. 山石网科

暂无更新。

3. 亚信

暂无更新。

4. 绿盟科技

4.1 绿盟科技获 2017 年度中国反网络病毒联盟“优秀安全企业称号”

2018 年 2 月 2 日，中国互联网协会反网络病毒联盟（以下简称“ANVA”）在北京外国专家大厦隆重召开 2017 年年会，绿盟科技作为联盟首批成员单位，因在恶意程序样本共享、计算机应用程序安全检测等方面表现突出，荣获 2017 年度中国反网络病毒联盟“优秀安全企业称号”。

本次会议上，工信部网安局对《公共互联网网络安全威胁监测与处置办法》进行宣贯，联盟秘书处对 2017 年联盟的工作进行了总结汇报，并对 2017 年表现突出的成员单位进行了表彰，充分肯定了受表彰单位的技术实力和模范作用。绿盟科技、华为、阿里巴巴、猎豹等十三家公司被授予 2017 年度中国反网络病毒联盟“优秀安全企业称号”。

5. 360 企业安全

5.1 360 企业安全宣布与 VMware 在云计算和虚拟化领域展开全面合作

360 企业安全集团宣布，将与全球云基础架构和移动商务解决方案的领导厂商 VMware 在云计算及虚拟化领域展开全方位技术合作，利用 360 领先的网络安全能力及方法论与 VMware 云计算技术优势，共同致力于为中国用户提供安全高效的计算环境。

作为中国最大的企业网络安全厂商，360 企业安全集团是 VMware 在中国市场重要的安全合作伙伴。基于其雄厚的攻防、大数据等安全技术积累和对“数据驱动安全”技术思想的创新实践，成为中国企业级安全市场技术领导者，为包括中央部委和大型央企在内的超百万家企业级客户提供了全面有效的安全保护。

360 企业安全集团旗下 VMware 平台无代理杀毒产品获得了 VMware Ready™认证。360 企业安全集团可支持 VMware 最新版本 vSphere 和 NSX®，全面兼容 VMware vSphere®5.0/5.1/5.5/6.0/6.5、NSX6.2.4/6.3.0 版本。通过与 VMware 合作，360 企业安全集团将为中国政企客户提供基于 vSphere、NSX 平台的基础安全解决方案，为用户的虚拟化环境提供安全保护。

VMware 大中华区合作伙伴及业务拓展总经理王冰峰表示：“作为全球云基础架构和移动商务解决方案的领导厂商，VMware 致力于与 360 企业安全集团这样的一流企业合作，为中国客户提供更先进的安全解决方案，帮助企业提升安全性能和业务灵活性，加速其业务转型。”

360 云安全事业部总经理刘浩介绍，360 企业安全的无代理防火墙和 IPS 的产品也将很快面世并投放市场，后续还有陆续推出更多、更丰富、更完整的云安全解决方案，保护客户云安全。

5.2 360 企业安全参与支持“第十七次计算机和移动终端病毒疫情调查活动”

2018 年 2 月 1 日，“第十七次计算机和移动终端病毒疫情调查活动”正式启动。活动由公安部网络安全保卫局主办，国家计算机病毒应急处理中心承办，包括 360 企业安全在内的 21 家国内外反病毒产品生产厂商参与活动并提供支持。

为全面了解和掌握我国信息网络安全和计算机病毒疫情现状，推动我国计算机病毒防治工作的发展，进一步宣传、普及信息网络安全知识，提高广大用户网络安全防范意识，同时给国家有关部门制定网络安全及计算机病毒防治策略提供准确参考和有力依据，公安部已经连续十六年组织全国性的计算机病毒年度疫情调查活动，并一直由国家计算机病毒应急处理中心承办。中央电视台、新华社、腾讯网、《信息网络安全》、《中国信息安全》、新浪、搜狐、网易、北方网、天津电视台及当地多家媒体作为支持媒体参与此次调查活动。

调查范围为全国企业及个人用户在使用联网设备过程中的网络安全状况，包括计算机设备、智能设备、移动设备以及网络支付等联网应用安全情况。此次调查活动将面向公众、政府机构、企业用户进行深入调查，以了解计算机和移动终端病毒疫情状况。

6. 安恒

6.1 安恒信息举办高校教师网络安全技能精讲班，助力网络空间安全专业建设

网络空间安全专业被定义为一级学科，各大相关高校、职业院校纷纷开设相关课程。教

师是支撑学科建设的主要力量，这不仅体现在教师的理论基础上，更加体现在网络安全攻防实战中。

安恒信息于 2018 年 2 月 1-3 日如期举办了 “高校教师网络安全技能精讲班”。精讲班通过与导师面对面交流探讨、实验实操、参观企业等形式促进专业教师的互动交流，增强科研兴趣，拓展学术视野，明确研究方向。

参加此次培训的学员主要来自于全国各地的本科院校、高职院校中的计算机或网络安全专业负责人、教研室主任、实验室人员以及网络中心安全维护责任人。这些院校都已经开设或者计划开设网络空间安全等相关专业，安排人员参加此次培训，是为了更好完成专业建设的前期筹备工作。

7. 安天

暂无信息

8. Fortinet

8.1 Fortinet 推出业界最快的 100 Gbps +下一代防火墙设备

多云环境以及越来越多的使用物联网和移动设备访问关键任务应用程序正在急剧增加企业边缘网络上的加密数据量。这些技术的采用也在增加带宽，吞吐量和会话容量要求。

在此背景下，Fortinet 推出了其 FortiGate 6000F 系列下一代防火墙（NGFW）。FortiGate 6000F 采用了全新的硬件处理架构，可在紧凑型 Fortinet 机箱设备中提供经过验证的性能，为指数级增长的企业流量提供高级安全性，非常适用于企业边缘网络。能够实现高密度，高能效和简单部署的威胁防护和加密检查吞吐量。

高速和灵活的接口：高密度 zSFP +和 QSFP28 接口支持 10G，40G，100Gbps 和 25G 新数据速率，以便在企业迁移到更高密度设计时提供高速连接和更高的灵活性。

安全结构集成：FortiGate 防火墙作为 Fortinet 安全结构的基础，运行全球部署最广泛的网络安全操作系统 FortiOS。 Fortinet 安全架构提供广泛的，集成的和自动化的安全性。

Fortinet 的下一代硬件架构是业界首个针对安全设备的产品，它利用了紧凑型内部处理卡，这些卡是通常用于尖端模块化安全机箱的小型刀片式服务器。每个处理卡将多个 12 核 CPU，安全处理单元（SPU）和内容（CP9）和网络处理器（NP6）组合为一个独立单元。在 3U 设备中，FortiGate 6000F 系列可支持多达 10 个独立处理卡。这种创新设计实现了传

统的机箱式的优势，如高弹性和会话规模，同时还以突破性的速度提供先进的安全功能，这在紧凑型设备中是前所未有的。该架构提供了额外的好处，例如使用新的自定义分发处理器（DP3）的硬件负载平衡功能，可以在分立处理卡之间智能分配任务。

8.2 Fortinet FortiGate 虚拟机现在可用于 Google 云平台

Fortinet 宣布，其 FortiGate 虚拟机（VM）现已面向 Google 云平台客户，提供按需消费，同时为动态企业云网络提供多层安全。

FortiGate VM 下一代防火墙可在 Google Cloud Launcher 市场上以 BYOL（带自己的许可证）的形式提供，从而使企业能够通过一致的自动化安全策略更安全地将他们的工作负载和应用程序迁移到 Google Public Cloud。

FortiGate 虚拟机可以帮助 Google 云客户安全地实现公共云的规模和弹性，并具有内部部署基础架构的集成安全性，控制和可视性。

Fortinet 正在与 Google Cloud 等合作伙伴合作，帮助企业通过云计算加速他们的数字业务，同时确保云中客户和组织数据的一致安全性和隐私。通过 Fortinet 安全架构，Fortinet 为企业客户提供了一个单一的玻璃视图，可以查看谷歌云，本地以及混合云环境中的 FortiGate 虚拟机和其他安全应用。

8.3 阿联酋电信服务提供商（EITC）选择 Fortinet 的云网络安全解决方案

阿联酋电信服务提供商（EITC）选择 Fortinet Security Fabric 解决方案作为其基础 云统一威胁管理（UTM）托管安全服务。此方案是专门为企业宽带用户和中小型企业设计的。

电信服务公司计划提供基于云的清洁管道服务，同时提供细粒度的安全服务以及客户的单点管理以实现自助服务和可视性。同时还需要安全基础架构的功能，如 Web 内容过滤，病毒防护，入侵防御，应用程序控制，数据丢失防护和远程 VPN 访问等。

FortiPortal 云端集中管理控制台能提供企业客户互联网流量的安全可见性和控制，实现从任何位置全面管理 FortiGate 企业防火墙。FortiAnalyzer 集中式网络安全日志记录和报告以及 FortiManager 集中式安全管理解决方案被部署用于向客户提供完整的管理和报告。

“对于我们干净的管道互联网产品，我们审查了几家供应商，Fortinet 满足了我们严格的评估标准，该标准基于专用客户门户的可用性，安全特性，报告功能，连接选项和可用协议，并提供最优惠的价格性能解决方案“，EITC ICT 解决方案副首席执行官 Farid Faraidooni 说。

9. Checkpoint

9.1 Check Point 推出三款全新的 Smart-1 安全管理设备防御“第五代”威胁和攻击

CheckPoint 推出这三款安全管理设备全部基于 Check Point Infinity Total Protection，这是一种独特的全新安全模式，可防御“第五代”威胁和攻击。新设备可以为企业级实时安全监控和控制提供集中、统一的策略管理以及高级日志和威胁分析，从而实现第五代网络防护。

目前所有业务领域都面临着第五代网络攻击，其定义是跨越移动、云端和本地网络，大规模且快速移动的攻击。这些复杂的攻击可以轻松绕过如今大多数组织正在使用的常规静态检测防御。全新的 Smart-1 设备可提供高达 48TB 的管理存储容量，记录速度高达每秒 10 万条，性能比之前的型号提高 8 倍。这样可以在网络、云端和移动环境中达到前所未有的安全管理性能，实现高效的第五代网络防护。

三款新设备 Smart-1 525、Smart-1 5050 和 Smart-1 5150 可以帮助企业 IT 团队实现全面的单一控制台安全管理，同时对数以千计的网络设备的大量新数据和历史数据进行关联、存储和分析。这将简化和加速安全管理流程，强化组织的安全状况，以应对目前的第五代网络攻击形势。

9.2 Check Point CloudGuard 整套方案为云安全提供主动防护

根据 2017 Check Point 网络安全的一项调查，81% 的组织对其公有云的安全性存有顾虑。共享责任模型（Shared Responsibility Model）和云端安全性专业知识的不足，意味着云端资料和资产很容易受到攻击。

由 Check Point Infinity 网络安全架构提供支持，Check Point® CloudGuard™提供一整套方案，可为云数据、工作负荷、网络和应用程序提供主动防护。Check Point CloudGuard 不仅覆盖 vSEC 的所有产品(IaaS)，而且新增了产品 CloudGuard SaaS，为客户提供更为强大的安全威胁防护。

这个全面的产品组合可与各类云基础设施和应用程序无缝集成，并且可以快速轻松保护所有云服务安全，甚至可以防护最复杂的第五代网络攻击。CloudGuard 的另一个特点是一键式和灵活部署模式，配合云服务的方便快捷。

四、 容器技术及安全动态

1. Subtree 发布 Dotmesh，实现应用状态的捕获、组织和共享

Subtree 发布了 Dotmesh。Dotmesh 是一种容器友好的应用状态快照工具，它提供了与 git 类似的命令行接口（CLI），操作并共享的捕获的应用状态数据。Dotmesh 主要从云原生和基于微服务的应用中捕获、管理和共享状态，便于调试和探索在 QA 和生产环境中发现的有问题状态。

应用状态在“datadot”中捕获，并通过一种集中式的“dothub”仓储进行存储和共享。Dotmesh 可以在一次原子提交中捕获多种数据库的状态，每种状态在一个“subdot”中。该工具非常适用于在任一时间点上捕获基于微服务的应用状态。在基于微服务的应用环境中，应用状态分布于多个组件间，例如多个数据存储、缓存或队列。

2. Rancher2.0 里程碑版本发布，支持添加自定义节点

Rancher 是一个开源的全栈化企业级容器管理平台，用户在 Rancher 可视化界面上以点选的方式，即可一键完成所有容器基础设施（网络、存储、负载均衡等）的对接与部署，确保容器在任何基础架构上（公私有云、虚拟机、物理机等）无缝运行，简单直观的操作，即可搞定在生产环境中使用容器的一切工作。

从 Rancher 2.0 开始，Rancher 中的每个集群都将基于 Kubernetes。用户可以充分利用 Kubernetes 的强大性能及其迅速壮大的生态系统，而通过 Rancher 平台上基于 Kubernetes 的、简单直观的用户体验，Rancher 2.0 将加快 Kubernetes 在企业中的普及。

新版本可以统一纳管来自不同基础设施的 K8s 集群。Rancher 2.0 提供对用户认证、监控和健康检查的集中管理，IT 管理员拥有更高的可见性和控制力。Rancher 2.0 充分利用了 K8s 中复杂的基于角色的访问控制(RBAC)功能，为用户提供共享集群和主机访问。更新之前的版本只支持 DigitalOcean 和 AWS，而最新版本，用户可以在创建 RKE 集群时添加自定义节点。通过 SSH / IP 或 docker run 的方式均可实现自定义节点添加。

五、 安全新产品及技术

1. Firefox 59 将添加新的隐私功能，从 URL 中删除敏感数据

当用户处于隐私浏览模式时，Firefox 59 将从 URL 中去除引用信息。该措施旨在防止用户意外泄漏敏感信息。Referrer 信息是当用户点击链接时由浏览器发送的信息。例如，如果用户点击网站 1 上的网站 2 链接，则网站 2 的网站管理员将知道登陆其网站的新用户来自网站 1。发生这种情况是因为 HTTP 请求带有一个名为“Referrer 值”的字段，用于存储 HTTP 请求的来源。Referrer 是网络工作的关键要素，帮助网站管理员了解他们的流量，帮助网络分析公司研究互联网站点之间的流量。但“Referrer”也被认为会引起问题。例如，在 2015 年 1 月，电子前沿基金会（EFF）发现 HealthCare.gov 已经在网址中嵌入了关键的患者信息。任何用户访问他们的网站，然后跳转到其他网站时，就会暴露他们的个人信息。

2. 新技术利用 X.509 数字证书建立隐蔽数据交换通道传输数据

2017 年 7 月的 Bsides 大会上，来自 Fidelis Cybersecurity 公司的安全研究员 Jason Reaves 演示了利用 X.509 数字证书秘密传输数据的过程，现在他发布了相关的 POC 代码。X.509 是一项标准，用于定义常用网络协议（TLS/SS）公钥证书的格式。例如 TLS 在建立加密会话的握手过程中使用 X.509 进行证书交换,Reaves 正是利用这一点，设计了隐蔽通道使用 X.509 扩展中的字段来传输数据。攻击者可以利用这个秘密通道窃取目标组织的数据，并逃避检测。 一般来说隐藏在 X.509 元数据中的数据无法被检测到，Reaves 发布的 PoC 代码在 TLS 协议中传输了 Mimikatz 后期利用工具。Reaves 认为可能有效的应对方法是禁用自签名的证书，并检查证书中的可执行文件。

3. 三星与 KoolSpan 合作实现三星智能机安全通信

面向手机的加密安全语音和信息解决方案提供商 KoolSpan 宣布与三星合作，在三星智能手机上实施安全通信。KoolSpan 支持企业常用的主流电话，可帮助公司所有内部呼叫和文本提供端到端加密服务。 KoolSpan 与三星合作开发了三星版本的 TrustCall Native，可在三星设备上与本地拨号器、手机本机、信息和联系人等三星原生功能集成到一起，并自动实现加密。 TrustCall 本地安全通信适用于拥有三星企业联盟计划（SEAP）帐户和订购 KNOX 配置的客户，主要是应对移动通信攻击的增长，既能实现安全又能确保易用。

4. 以色公司 Cellebrite 发现解锁任何 iPhone 设备的方法

据报道，以色列移动取证公司 Cellebrite 已经找到了可以解锁几乎所有 iPhone 设备的方法，其中可能包括最新的 iPhone X 。 Cellebrite 成立于 1999 年，为其客户提供手机数字取证工具和软件，同时它是美国执法机构重要的安全承包商。他们声称已经开发出一种全新的黑客工具可用于解锁运行 iOS 11 以及更早版本的所有 iPhone 设备。在披露的文件中，该公司所提供的 “高级解锁与数据提取服务” 可以适用于 iOS 5 至 iOS 11 的所有版本 iOS 设备，除了 iPhone 还可以应用在 iPad 和 iPod touch 上。此外，Cellebrite 还能够解锁谷歌安卓系统的三星手机（如 Galaxy 和 Note 系列），Alcatel，Nexus, HTC, 华为等其他设备。 目前具体技术还不明确，苹果方面回应称，正在敦促用户及时更新到最新 iOS 版本以避免潜在安全隐患。

5. 防黑客智能手机出现，旨在保护用户加密货币安全

网络安全公司 Sikur 在西班牙巴塞罗那的移动世界大会上推出了价值 799 美元的 SIKUR Phone。 SIKUR Phone 内置加密货币钱包，旨在保护比特币等数字货币的安全。 该公司声称，它通过黑客对设备进行测试，且这些黑客无法破解该设备。 SIKUR Phone 将于 2 月 27 日以 799 美元的价格预售，第一批将于 2018 年 8 月交付，且公司以该优惠价格售卖的 SIKUR Phone 仅提供 20,000 部。

六、 网络安全投融资、收购事件

1. Attivo Networks 获得未知数额的公司轮融资

2 月 6 日，Attivo Networks 从 Bain Capital Ventures 和其他 3 位投资者处获得未知数额的公司轮融资。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. Infocyte 获得 520 万美元 B 轮融资

2 月 9 日，Infocyte 从 Feik Enterprises 和其他 2 位投资者处获得 520 万美元 B 轮融资。Infocyte 是一家网络安全技术公司，能够帮助企业主动识别网络威胁。

3. CryptoMove 获得 600 万美元 A 轮融资

2 月 12 日，CryptoMove 从 408 Ventures 和其他 5 位投资者处获得 600 万美元 A 轮融资。CryptoMove 是一家信息安全技术公司，采用主动防御技术，帮助用户数据免遭威胁。

4. VMWare 完成对 CloudCoreo 的收购

2 月 14 日，VMWare 完成对 CloudCoreo 的收购，收购价未公开。CloudCoreo 是一家云基础设施管理安全公司，其目标是希望能够让企业客户随时随地的部署、管理以及防护云应用。

5. Morphisec 获得 1200 万美元 B 轮融资

2 月 19 日，Morphisec 从 Deutsche Telekom 和其他 3 位投资者处获得 1200 万美元 B 轮融资。Morphisec 主要从事移动目标防御解决方案。

6. Vectra Network 获得 3600 万美元 D 轮融资

2 月 21 日，Vectra Network 从 Accel Partner 和其他 8 位投资者处获得 3600 万美元 D 轮

融资。Vectra Networks 成立于 2011 年 1 月是一家安全技术提供商，主要为企客户提供实时网络安全防护管理。

7. CyberX 获得 1800 万美元 B 轮融资

2 月 27 日，CyberX 从 ff Venture Capital 和其他 4 位投资者处获得 1800 万美元 B 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。

8. Splunk 完成对 Phantom 的收购

2 月 27 日，Splunk 完成对 Phantom 的收购，收购价 3.5 亿美元。Splunk 是一家企业数据智能分析软件提供商，其软件可用于监控、分析实时的机器数据以及 TB 级的历史数据，且数据来源不限。Phantom 是一家智能化网络安全技术公司，为企业提供基于社区的安全自动化编排平台。该平台可以对安全操作进行自动化编排，可以在数秒钟之内实现手工操作需要数小时甚至数天才能完成的事情。而 Phantom Apps 则可以充当结缔组织，将企业部署的各个分散的安全产品集成到一起。 所谓自动化编排，就是将多个安全应用按照一定的逻辑配合，实现多种安全业务功能，自动化编排进而提高安全运营效率，减少企业各项成本。

9. 安全意识培训公司 PhishMe 以 4 亿美元市值被收购

PhishMe 是一家专注于培训员工如何识别和举报网络钓鱼攻击的安全意识培训公司，该公司已被一家私募股权收购，这笔交易价值 4 亿美元。在收购完成后该公司将重新更名为 Cofense。该公司表示，目前它们已在全球拥有超过 1700 家客户，其 PhishMe Reporter 已安装在 1000 万以上的端点上。在过去的四年里，它的复合年增长率约为 80%，并且在澳大利亚，新加坡，迪拜和沙特阿拉伯开设了新的办事处。

10. 青藤云安全融获 2 亿 B 轮融资

青藤云安全近日宣布获 2 亿 B 轮融资，由红杉资本中国基金领投，A 轮投资人宽带资本，红点投资、真格基金继续跟投。青藤云安全是国内首家自适应安全服务商，与 Symantec 赛门铁克、McAfee 等国际知名安全公司并列成为 Gartner 全球安全市场指南代表厂商。青

藤云安全技术方案依据自适应防御系统从预测—防御—监控—回溯的四个阶段理论，构建了 Analyzer、Monitor、Builder 三个产品来完成企业自适应安全防御能力。