内容摘要

云厂商方面，AWS 公布了 Amazon Inspector 对 Amazon Linux2 的支持，同时 Amazon Connect 通过 SOC 认证，以及 AWS Server Migration Service 现已在 AWS 亚太区域 (新加坡) 开放；VMware 发布新边缘计算解决方案以加强企业物联网能力；Google 方面，原 Amazon 首席 AI 研究员跳槽 Google，并且有消息称，谷歌正自行开发分布式数字分类账本以支持云服务。微软为各级政府提供本地云服务，发布 Ethereum On Azure 简化企业级以太坊区块链部署体验；阿里云首个全球数据中心开始运营，并与深圳大学合作成立大数据学院；腾讯云联合未来媒体发布国内首家 4K 全景实验，在香港增开第二个数据中心，并在美国增设 2 个数据中心，同时腾讯云印度数据中心也开服了；华为云则与拓斯达展开工业物联网方面合作。

开源云方面，OpenStack 发布 Queens 版本，增加众多功能；中国信通院发布《开源治理白皮书》，联合包括 EasyStack 在内的多个国内项目和公司编写；九州云在 OpenStack 核心功能贡献位列全球第五，并且上榜杭州首发准独角兽企业名单。

云安全厂商方面，启明星辰发布 2017 年报-数据安全高速增长，运维业务持续推进；荣获了首批国家信息安全服务最高资质；集团工控产品成功入编《石油化工仪表自动化技术国产化推荐目录（一）》，并加入华为安全商业联盟，协同打造健康网络安全空间。

其他安全厂商，国内方面：亚信中标交通银行态势感知项目，并与青云携手提升云端深度防护能力。360 企业安全集团的三大战略中心落户绵阳；并与建行共建“新一代”反欺诈解决方案。安恒明御 EDR 安全产品获公安部销售许可证。国外方面：Fortinet 发布 2018 年全球威胁态势预测，并获得 NSS 入侵防御系统测试报告的推荐评级；CheckPoint 发布《Check Point 威胁情报 0312——攻击与漏洞榜单》。

容器动态方面，Kubernetes 1.10 发布：更趋稳定的存储、安全与网络功能；SmartX 与 Rancher Labs 联合，共同打造用于容器的超融合基础架构平台。

安全新技术方面，新的面部识别技术 Face Flashing 面世，有报告称约 90% 的企业到 2020 年都会使用生物认证技术；Google 实验室公布了最新一代 72 位量子处理器，错误率只有 1%；微软发布了在 Windows 10 上运行任何 Linux 操作系统的工具。网络攻防方面，两个针对 Memcached 放大攻击的 PoC 代码公布，荷兰警方公布了打击 Hansa 暗网的细节。Linux 基金会官方宣布了一个名为 ACRN 的新项目，该项目将为物联网设备创建虚拟机管理程序通用代码，谷歌云宣布将新增包括区块链技术在内的 20 多项功能加强安全性。G20 将加密货币定义为资产而非货币。IETF 已正式批准 TLS 1.3 作为传输层安全（TLS）协议的下一个主要版本，未来其将成为客户端和服务器之间的通信标准，也就是 HTTPS 的标准。

网络安全公司投融资方面，总共发生 3 起收购和 6 起投资事件。安全意识培训与模拟网络钓鱼平台 KnowBe4 和 IT 安全解决方案公司 CyberArk Software 均完成了未知数额的收购，而美国网络安全公司 Palo Alto Networks 则以高达 3 亿美元的价格完成了对云安全技术公司 Evident.io 的收购。投融资方面，网络安全

公司 Virsec、混合云接入公司 Luminate Security 和入侵检测公司 Solebit 分别获得 2400 万美元、1400 万美元和 1100 万美元的融资，其余 3 家公司所获融资均为超过千万美元。

2018 年 4 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 AWS Server Migration Service 现已在 AWS 亚太区域 (新加坡) 开放

3 月 1 日， AWS Server Migration Service (SMS) 可轻松将工作负载迁移到 AWS，现已在 AWS 亚太区域 (新加坡) 开放。AWS Server Migration Service (SMS) 可轻松将工作负载迁移到 AWS，现已在 AWS 亚太区域 (新加坡) 开放。

1.2 Amazon Connect 现已通过 SOC 认证

3 月 5 日，Amazon Connect 现已通过 SOC (系统与组织控制) 认证。SOC 报告是独立的第三方检查报告，阐明 AWS 如何达成关键合规性控制和目标。AWS 通过对 AWS 控制执行广泛的第三方审核来确保 SOC 合规性。这些审核能够确保采取适当的安全措施和程序，防止出现安全风险，影响客户和公司数据的机密性、完整性和可用性。第三方审核的结果会发布在 AWS SOC 合规性网站上，审核人员可以查看已发布的报告，详细了解为 AWS 运营和合规性提供支持的既有控制措施。

1.3 Amazon Inspector 现在支持 Amazon Linux 2

3 月 13 日，Amazon Inspector 现在支持对适用于通用漏洞披露 (CVE) 的 Amazon Linux 2、安全性最佳实践和运行时行为分析进行安全评估。要运行安全评估，只需在所需的 Amazon EC2 实例上安装 Amazon Inspector 代理，在 Inspector 控制台中配置您的评估，然后即可运行评估。

Amazon Inspector 是一项按需安全评估服务，可帮助 AWS 客户验证其 Amazon EC2 环境中部署的应用程序和操作系统的安全配置。Inspector 可让客户灵活检查 EC2 实例是否存在漏洞，并随时根据安全基准按需评估其实例配置。Inspector 提供规则包，允许客户选择他们希望执行的安全评估类型，以便细致评估所发现的问题，并提供提高实例安全性的建议。

Amazon Inspector 现已可在以下区域使用：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 (法兰克福)、欧洲 (爱尔兰)、亚太地区 (孟买)、亚太地区 (首尔)、亚太地区 (悉尼) 和亚太地区 (东京)。

1.4 Lambda@Edge 增加 S3 源支持，以根据请求标头自定义内容分发

3 月 20 日，Lambda@Edge 允许访问面对源的事件中的额外白名单标头，包括自定义表头，从而进一步自定义 Amazon S3 存储桶中所存储内容的分发。例如，可以将 Amazon CloudFront 配置为缓存国家/地区标头并转发至 S3 源，然后根据访客的位置，使用 Lambda@Edge 动态将访客重定向至网站的具体国家/地区版本。CloudFront 还会缓存应答以进一步提高后续对您网站请求的性能。

此前，仅可以使用 S3 源将 Amazon CloudFront 配置为根据三个标头转发并缓存对象：Access-Control-Request-Headers、Access-Control-Request-Method 和 源。但在此次发布后，可以使用 S3 源将 CloudFront 配置为缓存和转让多个额外的标头，例如 CloudFront-Viewer-Country 或 CloudFront-Is-*-Viewer，然后再使用 Lambda@Edge，根据这些标头自定义内容，以较低低延迟向访客分发。

2. VMware 云动态

2.1 VMware 发布新边缘计算解决方案 加强企业物联网能力

3 月 1 日新闻，VMware 在 MWC 全球移动通信大会上继续推进企业物联网（IoT），发布了一系列新的边缘计算解决方案，以解决资产管理和监控中的使用案例。这些解决方案是通过与 Axis Communications、Wipro Limited 等公司的行业合作开发的。VMware 专注于边缘计算的这些解决方案能够让企业用户以更轻松的方式，安全且有效地利用物联网产生的数据。

在 VMware 看来，VMware vSAN 超融合基础设施（HCI）软件、VMware vSphere 和 VMware Pulse IoT Center 等产品都将在新解决方案中发挥作用。因此，该解决方案将满足工业和制造业以及某些实体零售店的特定需求。

3. GOOGLE 云动态

3.1 亚马逊首席 AI 研究员跳槽谷歌，成为云部门 AI 技术总监

3 月 1 日，根据 Ashwin Ram 的领英资料显示，日前他已经正式从亚马逊离职，转而加入搜索巨头谷歌，并且担任云计算部门 Google Cloud 人工智能技术总监。

在亚马逊就职期间，Ram 最大的贡献就是创新性地设立了 Alexa Prize 大奖赛。在这一比赛中，用户需要尽可能长时间地与 Alexa 对话，目标时长为 20 分钟。

在最新一篇宣布加入谷歌的博文中，Ram 表示：“可以说，在人工智能这一块，谷歌有着最为优质的发展资源和最为强劲的研究实力。而接下来，我的主要工作就是发挥自己的专长，帮助谷歌的人工智能进一步升级完善，让日常生活中的每一个人都能享受到人工智能技术带来的便利。”

3.2 谷歌自行开发分布式数字分类帐本，用以支持云服务

3 月 22 日，据知情人士透露，谷歌正在研发与区块链相关的技术，以支持其云业务和阻止来自新兴创企的竞争。

公司使用区块链和其他所谓的数字分类账来安全地记录交易，并通过互联网处理其他数据。例如，谷歌可以使用这项服务来向客户保证，他们的信息存储在巨大的计算机服务器网络上时，是受到保护的。虽然产品的发布时间尚不明确，但该公司计算利用这项服务，将其云服务与竞争对手区分开来。它还将提供白标版本，其他公司可以在自己的服务器上运行这一版本。

4. 微软 Azure 云动态

4.1 微软将为各级政府提供本地版云服务 与亚马逊争夺政府客户

3 月 5 日，微软宣布，公司将很快让政府客户在自己的服务器上运行 Azure 云服务，这是该公司为了提高 Azure 的吸引力而采取的最新举措之一。

微软将其本地化云产品 Azure Stack 和它专为政府部门量身定制的云产品 Azure Government 整合在一起是为了更好地与亚马逊竞争，争夺公共领域的主要客户。

微软 Azure 全球基础设施主管汤姆-基恩（Tom Keane）表示，这款新服务将于 2018 年中期推出，旨在吸引对本地服务器有需求的政府部门和相关机构，比如军事行动指挥部或海外大使馆等等。

4.2 微软首次发布 Ethereum on Azure 产品升级 简化企业级以太坊区块链部署体验

3 月 21 日， 微软首次发布了 Ethereum on Azure 产品升级，以支持适合企业应用场景的“准投产”联盟区块链网络。

微软公司本次推出了以下三大改进措施：

- 区块链网络存在的高可用性：作为去中心化网络的参与方，在共识流程中，企业的节点存在对于实现一个公平且安全的网络至关重要。为了确保高可用性，微软合并了跨区域 Azure VM Scale Sets (Azure VMSS) 和 Azure Managed Disks。在这种情况下，如果某个节点出现了故障 Azure VMSS 将自动恢复该阶段，并将其重新加入到以太坊网络中。由于活动节点可能会随时间而改变，因此微软会非常小心维护准确的引导节点列表，允许其他成员加入网络。
- 简化部署体验：对于企业而言，选择适合应用场景的网络拓扑可能比较困难。微软投入了大量精力将各种以太坊网络拓扑整合到了一个体验之中，使用户可以遍历所有部署选项，而且只显示对你企业重要的信息。
- 健康和运营支持：在开发运营环境中，区块链网络不能成为企业应用程序架构中的忙点。微软需要监控、记录和分析网络运行状况和区块链指标。现在，微软可以支持部署一个个性化的监测控制台，和你的区块链网络一起来监测区块链基础架构。现在，你可以在矿工和交易阶段上监控 CPU、内存和磁盘容量，而且还可以自定义创建警报功能。

4.3 微软 Azure 云服务在以太坊区块链上完成全球首个区块链投资产品

3 月 25 日， 英国 Nivaura 公司与微软 Azure 云服务在一次测试案例中证明了公有账本能够用于支持受监管的资产。区块链正在成为一个越来越有吸引力的选择，因为支付行业正在不断拥抱加密货币，甚至数字法定货币。

5. 阿里云动态

5.1 中国联通推动云网协同 打通阿里云、腾讯云

3 月 9 日，中国联通副总经理梁宝俊在北京发布了云联网、云组网、云专线、云宽带等七项联通新服务，阿里巴巴、腾讯、中国工商银行等成为首批合作伙伴，将推动云端与网络一体化。

随着信息化的发展，企业大量数据上云。中国联通政企客户事业部总经理李广聚表示，这对网络负载能力和稳定性提出了更高的要求。对运营商来说，机会与挑战共存。

5.2 瑞萨电子将 AliOS 嵌入 MCU，就物联网平台开发与阿里巴巴展开合作

3 月 15 日，全球领先的半导体解决方案供应商萨瑞电子株式会社宣布，与阿里巴巴旗下云计算科技公司阿里云合作，加速以阿里物联网操作系统 AliOS 为基础的物联网解决方案的开发，为中国物联网发展做出贡献。双方将通过由双方工程师组成的联合团队展开合作开发，将阿里物联网操作系统 AliOS 嵌入瑞萨电子丰富的微控制器产品线，由此轻松创建物联网节点和网关，无缝连接阿里云。

通过嵌入 AliOS 的物联网解决方案,瑞萨电子将持续为中国的智慧城市、智能家居、智能工厂等领域做出贡献。特别是在拥有丰富技术积累的智能家居领域，瑞萨电子将提供极具魅力的解决方案。

5.3 阿里云首个全球数据中心开始运营，将协助印尼企业转型和发展

3 月 15 日，阿里巴巴集团云计算部门阿里云宣布，其在印度尼西亚的首个数据中心开始运营。该数据中心可以提供从弹性计算、数据库服务、网络、安全和中间件到分析和大数据的全套云产品和服务，将满足电子商务、媒体、金融科技、游戏、物流、运输和制造等各行业本地企业的急速需求。

据悉，该数据中心是我国第一个全球公共云平台，它将通过提供功能强大、可靠且具有成本效益的云产品和服务，为印度尼西亚企业，特别是中小企业和初创企业提供服务。它还将帮助印度尼西亚客户提供低延迟或数据驻留要求，以帮助他们方便得在该国境内存储和处理数据。

其中，大数据服务平台“MaxCompute”允许用户进行大量 TB 级甚至 PB 级别的结构化数据存储，以带来复杂的数据智能服务（如数据处理、分析和机器学习），这将推动印度尼西亚企业的创新和业务转型。

“作为源自亚洲的唯一全球云服务提供商，我们拥有独特的文化和环境优势，为本地区的客户提供创新的数据智能解决方案和计算能力。”阿里云亚太区总经理 Alex Li 评价道。

据了解，数据中心的启动是阿里云承诺持续支持印尼政府计划，即在 2020 年前创建 1000 家初创公司，的一部分。为了培育本地的互联网相关生态系统，阿里云还宣布将把阿里云认证专家（“ACP”）计划带到印度尼西亚，在一年内，该计划旨在培训 300 名并认证印尼的 100 名云精明专业人员，为企业家和本地人才带来有关云计算，大数据和安全方面最佳技术的知识。

5.4 阿里抢攻 IoT 新赛道 未来 5 年连接 100 亿台设备

3 月 28 日，阿里巴巴集团资深副总裁、阿里云总裁胡晓明宣布：阿里巴巴将全面进军物联网领域，IoT 是阿里巴巴集团继电商、金融、物流、云计算后新的主赛道。

胡晓明是在今日召开的 2018 云栖大会 • 深圳峰会上透露这一消息的。他表示，阿里云 IoT 的定位是物联网基础设施的搭建者，阿里云计划在未来 5 年内连接 100 亿台设备。此外，为应对物联网带来的新挑战，阿里云将在 2018 年战略投入“边缘计算”这一新兴的技术领域，打造全世界第一朵“无处不在的云”。

对于阿里云在 IoT 战略中的定位，胡晓明指出，阿里云在物联网领域的核心价值就是去解决这三个问题：1、提供开放、便捷的 IoT 连接平台；2、提供强大的 AI 能力；3、实现云、边、端一体的协同计算。

据介绍，早在 2014 年，阿里云就开始启动物联网研发，并已经完成了城市、生活、制造、汽车四大物联网领域的核心技术布局。例如，阿里云将与雄安合力打造“世界物联网中心”，为数字中国打样。在智能汽车领域，AliOS 已与上海汽车、神龙汽车、福特汽车实现战略合作，已有超过 50 万辆搭载 AliOS 的智联网汽车跑在路上。

5.5 深圳大学•阿里云大数据学院成立

3 月 28 日，在云栖大会 • 深圳峰会上，深圳大学与阿里云宣布启动粤港澳大湾区数据智能人才培养战略合作，依托政产学研创五位一体的校企合作模式，面向粤港澳大湾区建设云计算、大数据、人工智能等方向联合培养新工科融合型跨界创新人才。据介绍，双方更将共同推动建设深圳大学 • 阿里云大数据学院，计划三年培养 1000 名本科生。

6. 腾讯云动态

6.1 VR 视频迎来新变革，腾讯云联合未来媒体发布国内首家 4K 全景实验

3 月 19 日，以“云聚融合、智创未来”为主题的腾讯云广电融合大会在北京召开，大会上，来自广电行业、终端行业、媒体平台的众多大咖就有关广电跨界融合的趋势以及数字时代 4K 视频的前景问题展开了讨论与分享，并共同成立了中国 4K 全景实验室。

4K 全景（中国）实验室由腾讯云与北京未来媒体发起，实验室成员由包括新疆广电网络股份有限公司、电广传媒影业（北京）有限公司、中广电传媒有限公司等诸多广电行业先锋组成。

据了解，针对 4K 全景这一新视听体验，4K 全景（中国）实验室各成员单位之间已经进行了诸多的探索和尝试。北京未来媒体科技股份有限公司（简称未来媒体）推出了全国首个大屏 4K 全景视频应用——“4K 全景”，其作为 4K 全景内容集成、分发、运营平台，依托腾讯云在视频云领域专业、安全、强大的服务已经实现了全网全终端的变现运营，覆盖用户超 1000 万。

此外，新疆广电网络已经率先上线“4K 全景”平台，重庆有线、广州番禺有线、酷开电视等也正在逐步落地中。内容层面，广东弘视数字传媒有限公司、电广传媒影业（北京）有限公司、中广电传媒有限公司、重庆视讯传媒有限公司已经开始 4K 全景内容的拍摄与制作。硬件层面，以海思为代表的芯片厂商已有多款芯片支持 4K 及全景播放。

6.2 腾讯云在香港增开第二个数据中心，助力云上粤港澳大湾区建设

3 月 26 日，腾讯云在香港的第二个数据中心正式对外开放服务。该数据中心延续了腾讯云在香港第一个数据中心中采用的金融级基础架构技术标准，腾讯云也因此在香港率先实现了金融级双可用区的部署。

依托香港区域与资源优势，腾讯云香港数据中心打造了覆盖香港本地以及连通东南亚乃至整个亚太地区的优质网络，还提供了通向腾讯云全球数据中心的国际链路选择，能够帮助用户快速实现全球业务布局。

此前，主营港股美股业务的互联网券商富途证券便基于腾讯云香港数据中心部署业务。依托腾讯云的技术支持，富途证券为用户提供了稳健可靠的股票交易服务，实现业务的快速增长，成长为业界独角兽。

而香港本地知名金融工程技术公司 eBroker 也基于腾讯云香港数据中心优质的计算资源能力，为金融机构提供创新性、高性能的交易和风险管理解决方案。东海国际、富通投资管理等香港金融企业也基于腾讯云香港数据中心上部署了包括行情系统在内的多项业务。

此外，腾讯云香港数据中心还吸引了游戏、O2O 等行业的大量用户入驻。

6.3 腾讯云在美国新增两个数据中心，实现两地三中心覆盖

3 月 27 日，腾讯云位于美国东部弗吉尼亚区域和美国西部硅谷区域的两个新增数据中心同时开放服务，将向用户提供计算、存储、网络、数据库、安全以及大数据、人工智能等全系列云计算产品。

这是腾讯云继去年在硅谷开放首个数据中心之后，再次扩大在美国的基础设施覆盖范围。目前，腾讯云已实现全美东西海岸两地三中心布局。这将为企业在北美乃至全球进行业务拓展提供更加丰富而可靠的云计算产品和服务保障。

此次新增的腾讯云硅谷数据中心将配备高性能的计算基础设施，能够为高运算负荷 AI 提供强大的计算环境；而在弗吉尼亚的数据中心则直扎美国东部最大的网络枢纽，汇集了北美丰富密集的网络接入及互联资源，能够让用户快速连通全球业务，在获得高可用的云计算服务的同时，还能大幅降低成本。

此前，腾讯云在美国已经获得了来自互联网、视频直播、移动支付、共享单车、网络游戏等行业的许多用户信任。

6.4 腾讯云印度数据中心开服，用云计算激发古文明新活力

3 月 28 日，腾讯云印度数据中心正式开放服务。这是腾讯云在南亚区域布局的首个大规模数据中心，将为印度本地企业以及在印度开展业务的中国企业，提供计算、存储、网络、安全等优势基础云计算产品和大数据、人工智能等先进技术平台。还将把腾讯云在视频、金融、电商、社交、游戏以及工业制造等领域的完善解决方案带到印度，帮助用户大幅节省成本和时间，在南亚市场实现业务创新和商业成功。

在此之前，腾讯云已经在印度部署了 CDN 节点，帮助用户加速业务分发，打造良好产品体验。全球知名社交媒体音乐公司 Smule 旗下 APP《Sing!》也已从中获益。基于腾讯云在印度的 CDN 产品，Sing!以流畅的 K 歌体验迅速获得印度用户青睐，在印度 APP 市场长期排名前列。随着腾讯云印度数据中心的开服，Sing!将从计算层面再次获得就近部署优势，用户体验将进一步得到保障。

目前，腾讯云已经在全球范围内的 23 个地理区域运营着 42 个可用区，帮助数百万家企业依托云计算实现业务快速发展。按照规划，腾讯云还将在一年内在印度开放第二个数据中心，届时，腾讯云将在印度实现双中心格局。

7. 华为云动态

7.1 拓斯达：与华为云展开工业互联网方面的合作

3 月 5 日，拓斯达在互动平台表示，公司目前在工业机器人及核心零部件控制器等方面都具备自主研发能力，因此具备终端数据采集条件。公司也有为客户做 MES 系统，同时与华为云正展开工业互联网方面的合作。

二、 开源云动态

1. Openstack 动态

1.1 OpenStack Queens 发布

万众期待的 OpenStack Queens 于 2 月 28 日正式发布，这是该开源云平台 7 年以来的第 17 个版本。OpenStack Queens 增加了多项新功能，也优化增强了多项旧功能，包括虚拟 GPU(vGPU)支持和容器集成的改进。几个新项目也在 OpenStack Queens 这一里程碑中露面，

包括提供管理硬件和软件加速资源框架的 Cyborg。

OpenStack 的“女王”最令人期待的功能恐怕就是在 Nova 上对虚拟 GPU(vGPU)的支持了。伴随着人工智能、机器学习等新技术对于算力的苛刻要求，GPU 已经成为这些新技术领域的标配软硬件。顺应这个潮流，在此次的 Queens 版本中，增加了对虚拟 GPU(vGPU)的支持。

而 vGPU 的出现，则催生了另一个 OpenStack 用户急需的功能，即对于 vGPU、FPGA 和 DPDK 等软、硬件加速设备的统一管理。而在 Queens 中，通过 Cyborg 项目，实现了对这些软硬件加速设备的灵活统一管理;Cyborg 项目起源于 NFV 加速管理、ETSI NFV-IFA 004 参考架构和 OPNFV DPACC 项目，旨在为专用加速设备(如 FPGA，GPU，NVMe SSD)以及各种加速器(例如 iNIC，ip-sec 卡，DPDK)提供 Nova 之外的一个资源管理框架。Cyborg 在电信 NFV 领域、高性能计算、甚至是边缘计算都至关重要。由于这些领域需求特殊，通常它们场景都需要大量的专用设备做 offloading，或需要加速硬件或软件提高性能，所以 Cyborg 的发布，使 OpenStack 为这些要求实时性和高性能的场景领域填补了空白，同时 Cyborg 也支持 Standalone 的部署方式或与 Nova 或 Ironic 结合使用。

另一个在 Queens 版本中值得注意的是“Zun”，这是一个新的 OpenStack 项目，提供容器服务，旨在通过与 Neutron，Cinder，Keystone 和其他核心 OpenStack 服务集成来提供容器的快速部署，无缝地将先进的企业网络、存储和身份验证功能添加到容器中。

而在 Queens 的新功能中，最实用的应该是非 Cinder Multi-Attach 莫属，Multi-Attach 功能是构建高可用企业级应用的必备功能之一，具有非常广泛的应用范围。Cinder Multi-Attach 能够将相同的 Cinder 卷加载到多个 VM 中。如果一个节点关闭，另一个节点能够接管并访问该卷。

此外，OpenStack-Helm 也是 Queens 的一个亮点，它其实是 Helm 图表和工具的集合，在 K8S 的基础上管理 OpenStack 的生命周期，可以将 OpenStack 项目作为独立的服务来运行。

LOCI 是另外一个全新的项目，LOCI 可以让兼容 OCI 的 OpenStack 服务镜像，既可以放到像 OpenStack-Helm 这样的重量级部署工具，也可以用来独立部署像 Cinder 块存储这样的服务。

这两个服务主要强化了部署和管理的灵活性，能帮助 OpenStack 更好地在任意地方构建基础设施构建模块，这使得 OpenStack 能够支持边缘计算。虽然目前对于边缘计算基础架构的支持还处于早期阶段，但是边缘计算和云计算在一定程度上架构是趋同的。因此，Queens 版本对边缘计算的支持表明了 OpenStack 基金会希望能够引导 OpenStack 社区以及其他开源社区参与边缘计算的工具开发和标准制定，为后续更广泛的边缘计算应用提供支持。

当然，此次 Queens 中的新功能和新特性还有许多，诸如 Ironic 修复模式的引入、 新增 Kuryr CNI 守护进程等也是各具特点，限于篇幅，这里就不一一展开来讲了。

2. Easystack 动态

2.1 中国信通院发布《开源治理白皮书》

3 月 22 日上午，“OSCAR 云计算开源产业大会”在北京国家会议中心如期举办。会上，中国信息通信研究院云计算与大数据研究所风险管理&开源运营业务主管郭雪现场发布《开源治理白皮书》，白皮书不仅仅关注用户如何开源，还关注开源风险，开源的商业模式，定位是开源小白的使用指南。

开源治理在整个开源生态中占据非常重要的位置，尤其是开源生态在蒸蒸日上的同时，开源治理同样要引起人们的关注。为此，中国信息通信研究院着手这个问题，联合国内开源相关企业腾讯、中兴通讯、ZStack、华为、阿里云、IBM、红帽、EasyStack、中国移动、烽火通信、甲骨文、上海思华、中联润通、Mesosphere，编写国内首个开源治理白皮书。围绕怎么做开源，商业模式是什么，如何使用开源技术，以及开源风险等多方面来展开。

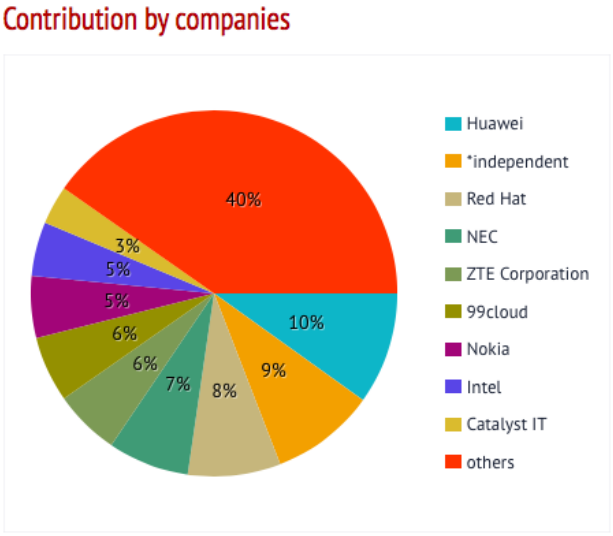
3. 99CLOUD（九州云）动态

3.1 九州云张雷当选 OpenStack 社区容器项目 Kolla PTL

九州云工程师张雷（Jeffrey Zhang）当选为 OpenStack 社区 Kolla 项目 PTL(Project Team Lead)。这是继九州云 CTO 龚永生获选 Tacker 项目 PTL 以来，九州云在 OpenStack 社区又新添的浓墨重彩的一笔。截止目前，九州云在 OpenStack 社区已有 2 个项目 PTL 和 5 个 Core。在 2017 年的 OpenStack 贡献中，九州云在核心模块贡献跃居全球第五。

3.2 OpenStack Queens 版本发布，九州云核心功能贡献全球 TOP5

截止 3 月 6 日，在 Queens 代码贡献中，共有 200 多家企业和组织上榜，其中九州云在核心功能贡献排名全球 TOP5，继续保持整体社区贡献全球前十。



Show 10 entries Search:

#	Company	Completed Blueprints
1	Huawei	29
	*independent	27
2	Red Hat	24
3	NEC	21
4	ZTE Corporation	17
5	99cloud	17
6	Nokia	16
7	Intel	14
8	Catalyst IT	10
9	NTT	10

在最新版本 Queens 的正式项目 Official 中，九州云 Completed Blueprints（完成蓝图数）、Commits（提交代码次数）、Resolved Bugs（修复缺陷数）及 Reviews（代码审阅数）的全

球排名均保持了稳步上升态势，四项指标皆挤进全球 TOP10。同时，九州云在 Kolla、Tacker、Packaging-Rpm、Freezer、Sahara、Solum、Telemetry、Watcher、Horizon、Cloudkitty 等模块成为主要的贡献力量，再次突出了九州云在网络、应用发布、集群服务、容器部署、容灾、计费等多个领域的努力和积累。核心功能贡献稳居全球 TOP5，Commits 贡献跃居全球 TOP6

根据 stackalytics.com 统计的 Completed Blueprints 的数据可以看到，在 Queens 版本九州云共完成 BP 数 17 个，整体贡献排名全球第 5，这也是九州云继 Ocata 版本之后连续稳居第 5。Completed Blueprints 代表的是一个公司希望在 OpenStack 项目里实现的功能和需求，反映了其推动 OpenStack 发展的想法和贡献程度，是衡量一个公司技术实力的一个重要指标。除九州云外，在该项指标中挤进前十的中国企业仅有华为和中兴。

从 Queens 版本的 Commits 排名来看,九州云共提交了 794 次代码，跃居全球第 6 位。与 Ocata、Pike 版本相较而言，九州云在此项指标的进步比较突出，已经以稳定的贡献排名稳居中国 OpenStack 专业公司第一。Commits 代表的是一个公司的代码贡献次数，也是被广泛使用的一个指标。这也是九州云多年来践行 Upstream First 理念，坚持社区共享与贡献回馈的不懈努力成果。

3.3 杭州首发准独角兽企业榜单，九州云上榜

3 月 12 日，在第二届万物生长大会上，杭州市创业投资协会、微链共同首次发布了《杭州一亿美金以上公司（准独角兽）榜单》，九州云凭借自身的优异表现成功上榜，与又拍云、才云科技等共同构成杭州 105 家“准独角兽”阵营。

三、 云安全厂商动态

1. 启明星辰

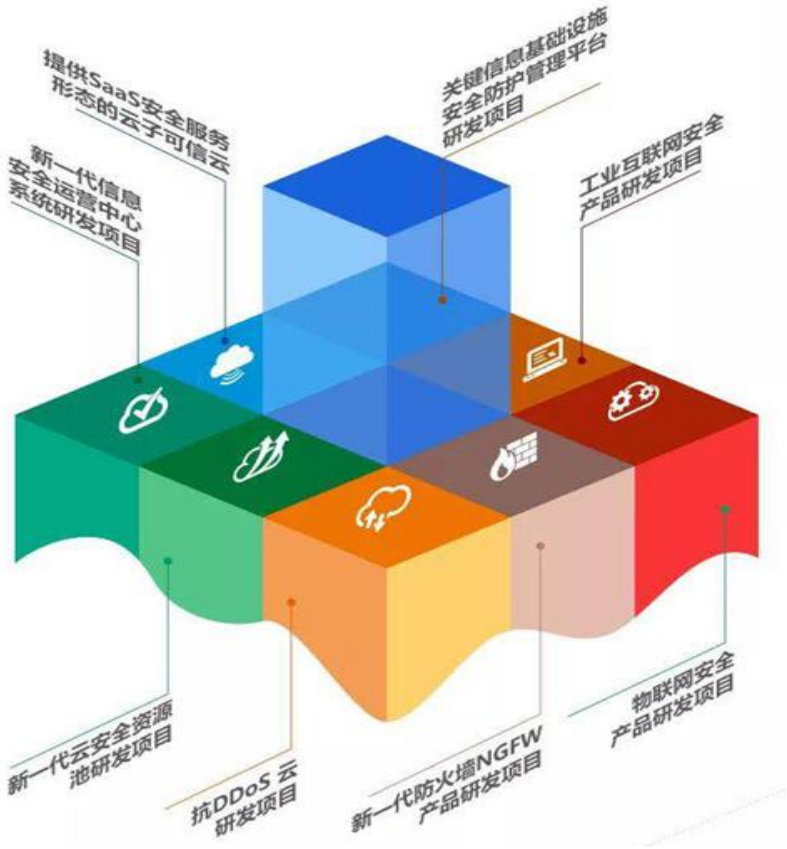
1.1 启明星辰发布 2017 年报-数据安全高速增长，运维业务持续推进

公司的经营情况良好，业绩也实现了稳定增长，全年完成营业收入 22.79 亿元，营业利润 3.58 亿元、归属于上市公司股东的净利润为 4.52 亿元，分别比去年同期增长 18.22%、168.75%和 70.41%。同时，归属于上市公司股东的扣非净利润为 3.21 亿元，同比增长 29.52%。业绩增长的主要原因是报告期内公司业务增长及新增并表损益所致。公司曾于三季报公开披露过对全年的业绩预测，最终实际经营业绩符合业绩预测。

公司召开的"网络安全产业展望及启明星辰战略说明会",董事长王佳女士表示启明星辰进入新的 I3 发展阶段：独立运营(Independence)、互联(Interconnect)、智能(Intelligence),同时各业务负责人就智慧城市安全运维、大数据与人工智能、态势感知、工业互联网安全等新兴领域公司的战略布局。

公司成立于 1996 年，是国内最具实力的、拥有完全自主知识产权的网络安全产品、可信安全管理平台、安全服务与解决方案的综合提供商。在产品方面，公司在北京、上海、广州、杭州、成都、南京等多地拥有研发机构，同时拥有完善的专业安全产品线，横跨防火墙/UTM、入侵检测/防御、安全管理、网络审计、终端安全、加密认证等技术领域，共有百余个产品型号，并根据客户需求不断增加。其中，入侵检测与防御(IDS/IPS)、统一威胁管理(UTM)、安全管理平台(SOC)、数据安全、数据库安全审计与防护、堡垒机、网闸均取得市场占有率第一的成绩，同时在安全运维、专业安全服务方面保持市场领先地位，其它还包括防火墙(FW)、Web 应用防火墙、漏洞扫描、互联网行为管控、防病毒、终端安全管理、数据防泄密、无线安全引擎、应用交付、数据隔离与安全处理、大数据处理/安全、电子印章/签名、工控安全、Vetrix 云安全资源池等多个产品领域。随着云计算、大数据时代的到来，公司已完成大部分产品的虚拟化、云化工作，并推出满足政务云/行业云、运营商云平台、大数据应用、智慧城市、态势感知、移动互联安全、关键信息基础设施保障等新需求的新产

品与解决方案；



在营销方面，公司在全国各省市自治区设立了三十多家分支机构，拥有覆盖全国的渠道和售后服务体系。公司在政府、军队/军工、电信、金融、制造、能源、交通、烟草、教育、传媒等行业是企业级用户的首选品牌，在政府和军队拥有 80%的客户覆盖率，为世界五百强中 60%的中国企业客户提供安全产品及服务，对政策性银行、国有控股商业银行、全国性股份制商业银行实现 90%的覆盖率，为中国移动、中国电信、中国联通三大运营商提供安全产品、安全服务和解决方案。

公司拥有代表国内最高水准的技术团队，包括积极防御实验室(ADLab)、核心技术研究院、产品研发中心、泰合团队、北斗安全运营中心、VenusEye 金睛监测团队、VF 安全咨询专家团、Vetrix 云安全团队、安全系统集成团队等，构成了公司重要的核心竞争力。公司在系统漏洞挖掘与分析、恶意代码检测与对抗等上百项安全产品、管理与服务技术方面拥有完全自主知识产权的核心技术积累。在此基础上形成了较为全面的安全产品线和安全服务模式。此外，公司还是国家认定的企业级技术中心、国家规划布局内重点软件企业，拥有最高级别的涉及国家秘密的计算机信息系统集成资质，并获得国家火炬计划软件产业优秀企业、中国电子政务 IT100 强等荣誉。公司拥有我国规模最大的国家级网络安全研究基地，创造了百余项专利和软件著作权，参与制订国家及行业网络安全标准，填补了我国信息安全科研领域的

多项空白，完成包括国家发改委产业化示范工程、国家科技部 863 计划、国家科技支撑计划、核高基重大专项等国家级科研项目上百项。

1.2 启明星辰荣获首批国家信息安全服务最高资质

近日，中国信息安全测评中心给企业颁发了一份资质证书，启明星辰成为首批获得国家信息安全服务资质三级的网络安全企业。

这个证书是衡量我国信息安全服务企业在风险评估、方案设计、安全集成、安全运维等综合服务方面能力的最高级别证书。也是我国颁发时间最早、覆盖范围最大、最具权威性的国家级资质证书，年审核通过率不足 60%。目前，一级获证企业有 500 余家、二级获证企业有 50 余家，而此次获得三级资质的企业仅有四家，升级比例不足 10%。其他三家是网神，安恒，绿盟。

1.3 启明星辰工控产品入编《石油化工仪表自动化技术国产化推荐目录（一）》

2018 年 3 月 20 日，石油化工仪表自动化技术国产化推进研讨会在北京成功举办。作为唯一一家受邀出席会议的信息安全企业，启明星辰集团工业防火墙和工业网闸两款产品成功入编《石油化工仪表自动化技术国产化推荐目录（一）》。

随着网络主权概念的逐渐明晰、安全威胁形势的愈加严峻，“自主可控”已经成为信息化部署的关键词，推动国产安全设备在各行业、领域的应用也成为安全工作的重中之重。本次《石油化工仪表自动化技术国产化推荐目录（一）》的编写，就是为了提升石油化工企业仪表自动化技术国产化水平、加强民族品牌推广与宣传，引导用户的正确选购符合行业应用的国产化产品。

网络安全之所以重要，是因为其对国家、企业、个人都将产生不可替代的影响。作为信息安全领军企业，启明星辰集团将持续致力于打造自主化的网络安全产品、为石油化工企业装备国产化添砖加瓦。

1.4 启明星辰加入华为安全商业联盟 协同打造健康网络安全空间

3 月 23 日，华为生态合作伙伴大会正式拉开帷幕。启明星辰集团常务副总裁张晓东应邀出席会议并与各产业领导企业、科研机构共同参加华为安全商业联盟揭牌。

当今互联网业务趋近云化，软件定义安全成为常态，企业用户网络安全边界逐渐模糊，在这样的背景下，面对黑产越来越成熟多样、隐秘持续的攻击时，企业用户安全防护亟需从被动响应转变为主动防御，需要高自动化实现检测和处置的协同安全解决方案。

而由于信息安全的特殊性，导致安全问题从来不是一个人、一件设备、一家厂商等这些单独个体能解决的问题。企业、厂商、科研机构必须从单打独斗的“一支箭易折”的模式，向多箭捆绑“一捆箭难折”的模式转变，华为安全商业联盟服务用户、协同防护、合作共赢、产业进步的服务宗旨，深度符合企业用户与安全行业发展的迫切需求。

启明星辰集团拥有安全网关类、威胁管理类、应用监管类、安全服务、安全工具类、管理平台类、云安全七个大类产品，近 40 种产品解决方案。此次加入华为安全联盟，将启明星辰的安全产品解决方案与华为的 SDSec 软件定义安全架构结合，从而形成一个全网协同安全防御生态系统，为客户建立全网协同的立体防御体系。

启明星辰战略布局智慧城市安全运营建设，率先提出“第三方独立安全运营”模式，并已经在成都市、杭州市、济南市、昆明市、郑州市等地开展安全运营中心业务，为智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制，实现“全天候、全方位”的网络安全态势感知、运维服务、应急响应能力。

2. 山石网科

暂无更新。

3. 亚信安全

3.1 亚信安全加入“华为安全商业联盟”，共建全网协同立体防御体系

3 月 22 日，华为生态合作伙伴大会在青岛召开。作为中国网络安全产业领跑者，亚信安全受邀参加了此次大会，并加入由华为主导发起的“华为安全商业联盟”，将亚信安全网络安全产品、解决方案与联盟伙伴的领先产品相互结合，为广大企业客户提供整体安全解决方案和服务，共同构建全网协同立体防御体系。

在大会的分论坛《智简网络 云领未来》峰会上，亚信安全副总裁刘科出席了“华为安全商业联盟发布仪式”，并作为唯一联盟伙伴代表发言。刘科表示：“由华为发起的安全商业联盟，有助于发挥联盟成员各自的能力和资源优势，共享网络防护经验，一方面避免了整网设备无法联动和统一管理所导致的难集成、难维护；另一方面，将带给客户更加高效的攻击防御体验，是一次非常有益的尝试。我们相信，亚信安全加入华为安全商业联盟，能使联盟更加有效地应对恶意攻击带来的网络威胁，同时也能进一步提升亚信安全在业界的竞争力，拓展业务空间。”

3.2 亚信安全中标交通银行态势感知项目

交通银行态势感知采购招标结果近日揭晓，亚信安全凭借业内领先的网络安全态势感知技术及其长期服务银行用户所积累的丰富经验，最终成为交通银行新一代网络防御系统的服务商。交通银行将引入基于亚信安全态势感知技术的沙箱产品及威胁情报系统，部署到关键节点，并通过“动态检测+静态检测”的处理方式，实时监测跨“外-内”网传输的数据安全，规避“僵木蠕”风险，全面提升交通银行的整体安全水平。

亚信安全态势感知平台采用了自适应、内外一体的态势感知框架，能够实现行业化与平台级的安全运营新模式，具备了高级威胁侦测和分析、宏观安全状态展示趋势分析、海量安全事件智能建模分析、全局安全信息深度挖掘等相关创新特性。同时，亚信安全还凭借其 APT 威胁治理、大数据安全、机器学习、勒索软件治理等领域的行业领导力，在长期服务银行、证券、保险等金融用户的项目中拥有优秀口碑。正因如此，亚信安全才能从众多竞争厂商中脱颖而出，最终成为交通银行态势感知项目的建设服务商。

在国内，亚信安全在金融领域拥有庞大的用户基础，其中涵盖了 75%的银行、80%的证券、69%的保险客户。交通银行在部署相关产品后，可以通过采集企业内所有 IT 基础设施数据，利用机器学习、数据建模、行为识别、关联分析等方法对企业内所有机器数据进行统

一分析，实现对网络攻击行为、安全异常事件、未知威胁的发现和告警，并最终达成“合法合规、见到威胁、看懂风险、抓到隐患、主动出击”的建设目标。同时，交通银行与亚信安全合作展开的新一代网络风控项目实践，其影响力对于金融行业用户关注、研究、部署态势感知等先进技术也必将起到推波助澜的作用。

3.3 青云 QingCloud 携手亚信安全 提升云端深度防护能力

企业级云服务商青云 QingCloud（qingcloud.com）日前宣布，与中国领先的云与大数据安全技术服务商亚信安全达成合作，亚信安全服务器深度防护系统 Deep Security 正式入驻 QingCloud AppCenter。基于此次与亚信安全的合作，双方将在云端安全防护领域深度集成，共同为企业用户打造更安全、更便捷、更可靠的云应用环境。此外，QingCloud 还将联合更多安全领域的合作伙伴，携手构建全方位的服务体系，以及完整的云安全生态体系。

青云 QingCloud 一直以来非常重视云端安全。为了加强资源和数据的安全性，QingCloud 构建了一个多维安全架构。DDoS 防护、SSL 证书服务、WAF 等服务，确保用户能够防御来自互联网的攻击，为用户提供安全的第一道防线；QingCloud SDN 构建的虚拟私有网络，实现 100%的二层隔离，保障了网络层的安全；实时副本、灾难自动恢复机制、块设备级别的备份与恢复，确保了云平台底层的数据安全性。随着亚信安全的 Deep Security 在 QingCloud AppCenter 上线，用户可以在云端主机层面获得增强的安全防护能力，功能覆盖网络层、系统层、应用层等的病毒攻击、漏洞攻击、恶意软件攻击，以及系统完整性保护等，全方位提升云端系统的安全防护能力。

与亚信安全 Deep Security 达成合作后，青云 QingCloud 将在 QingCloud AppCenter 平台为用户提供更多安全层面应用的选择。除亚信安全之外，QingCloud 还与长亭科技、安全狗、360 企业安全、上元云安全、昂凯科技、云安宝、中安星云、盛邦安全、中安威士等安全厂商达成了合作。作为云计算环境中的应用交付与运营管理平台，QingCloud AppCenter 以业务的视角重新定义 IT 使用模式，显著降低云端应用开发、部署及运维复杂度，为企业提供一个应用交付与消费的新模式。

4. 绿盟科技

暂无更新。

5. 360 企业安全

5.1 360 企业安全集团三大战略中心落户绵阳

3 月 29 日，360 企业安全集团三大战略中心在绵阳落地举行启动仪式。

此次在绵阳落地的360企业安全集团三大战略中心分别是360企业安全集团安全运营服务总部、360 企业安全集团网络安全人才培养绵阳基地、网络空间安全军民融合创新中心绵阳分中心。

其中，人才培养基地和运营服务总部将致力于网络空间安全专业人才的培养和面向全国的安全运营服务，计划 3 年培养 5000 人以上，全力打造四川省信息安全服务产业，助力绵阳科技城建设；网络空间安全军民融合创新中心绵阳分中心的设立将进一步落实国家网络空间安全和军民融合两大国家战略，推动网络安全能力建设和产业发展，助力网络空间国防建设。

5.2 建行与 360 企业安全共建“新一代”反欺诈解决方案

近日，中国建设银行与 360 企业安全达成合作协议。双方将在数据、算法、产品、生态四大方面携手创新，共建“新一代”反欺诈解决方案。

此次合作中，建行相关业务和技术部门将与 360 企业安全大数据金融团队组成虚拟团队。一方面，基于双方的大数据资源，运用目前业界前沿的人工智能算法，探索更多角度分析，使反欺诈的效果更为出色；另一方面，依托双方特色产品，建立协同防控机制，共建反欺诈生态圈，使用户的满意度更高。

5.3 航天二院七〇六所携手 360 企业安全 共建网络空间安全

3 日，中国航天科工二院七〇六所(以下简称“七〇六所”)与 360 企业安全集团签订网络空间安全领域合作框架协议，双方将在技术、业务、人才等方面开展全方位合作。

在技术合作方面，七〇六所与 360 企业安全集团将围绕移动互联网安全、云计算安全、虚拟化安全、安全态势感知、工控安全和新一代网络信息系统安全等网络空间安全技术领域进行深度合作，联合开展技术研究、产品研发和应用工程建设等。

在实验室建设合作方面，七〇六所与 360 企业安全集团将共同推进“大数据协同安全技术国家工程实验室”军工行业试点建设工作。在此基础上联合成立攻防实验团队，并对外提供安全服务。

在产品合作方面，七〇六所与 360 企业安全集团将以双品牌模式共同开发终端安全防护

类和网络安全态势感知类等产品，并合作研制与推广系列自主可控安全防护产品。

6. 安恒

6.1 安恒明御 EDR 安全产品获公安部销售许可证

EDR(Endpoint Detection and Response)终端检测与响应；在终端安置"Agent"，感知威胁信息，在云端或企业内网搭建数据处理中心，聚合感知到的威胁信息。

一个安全事件，无论在网络中经过多少环节，使用了多少高级技术，其最终目的都是为了代替人完成某些未经授权的工作，比如窃取数据、破坏系统、潜伏下来以备后续使用，而这些动作的完成，必须通过某个终端才能完成。终端是大多数安全事件的目标和发生地，终端安全毋庸置疑成为了安全的主战场。

6.2 安恒参加《华为中国生态伙伴大会》

3 月 23 日，《华为中国生态伙伴大会》在青岛国际会展中心举行。在以《网络安全：构筑智能防御体系，防患于未然》为主题的分论坛中，安恒大客户总监吴伟京发表了主题演讲。吴伟京在会上表示，安恒与华为在 2016、2017 连续两年的合作中，服务的客户覆盖了政府、金融、运营商、企业、医疗等多个领域，金额超过 1000 万元。此次安恒受华为安全商业联盟的邀请，成为联盟的一员，在今后将共同为用户提供领先的安全产品解决方案和服务。

7. 安天

暂无信息。

8. Fortinet

8.1 Fortinet 发布 2018 年全球威胁态势预测

近日，Fortinet FortiGuard 威胁研究与响应实验室基于多年的威胁研究与分析，就 2018 年全球威胁态势作出预测，指出越来越多的犯罪分子正在利用数字社会提供的新机会进行攻击，企业机构需要利用机器学习、人工智能等创新技术增强防御能力，以便保护企业的数据资产。

监督与无监督学习可能带来网络风险

专家预测，如果没有适当的控制，真正自主的自学习人工智能将能够通过我们超级连接的数字世界自由移动，适应新的数字环境，并访问几乎所有的数字资源。

针对这种智能和自动化威胁的最佳防御措施是集成、协作和高度自适应的安全架构。利用机器学习和人工智能等技术，将会有一个高度智能的主动安全防御系统，防御自学习的网络攻击。

黑客利用自动化和机器学习

他们会利用自动化前端挖掘信息和漏洞，并通过 AI 分析大量被窃取的结构化和非结构化数据。为了获得自动化与机器学习所需要的计算能力，网络犯罪分子正在使用云服务和公共基础设施来发起和管理攻击活动，并使用高性能计算（HPC）进行 CPU 密集型攻击。

我们很可能会开始看到完全由基于自动化漏洞检测和复杂数据分析的机器编写的恶意软件，然后根据检测到的弱点的独特特征开发漏洞。下一代的“形态恶意软件”将使用全新的自定义攻击，这些攻击不仅仅是基于静态算法的变体，而且将采用自动化和机器学习将它们定制到一个独特的目标，同时使它们更难以检测。

预测：HIVWNETS 与 SWARMBOTS 的上升

Fortinet 预测，网络罪犯将开始使用围绕群技术构建的智能攻击设备集群，取代传统的僵尸网络，以创建更有效的攻击。蜂巢网络(Hivenets)和机器人集群(Swarmbots)将更为普遍，Hivenets 将能够使用群集的受感染设备或 Swarmbots 来同时识别和处理不同的攻击媒介。随着 Hivenet 识别并攻陷更多的设备，它将能够以指数级增长，从而扩大其同时攻击多个受害者的能力。

要保护网络和服务不受群体攻击的影响，需要基于识别网络中潜在的攻击媒介和工程漏洞的系统方法，未来，利用集成安全设备的自适应安全结构将替换现有的安全工具。

云服务提供商 - 目标松散和单点故障

勒索软件的下一个大型目标很可能是云服务提供商，这首先是因为随着云服务市场的增长，针对云服务商的攻击会带来明确的金钱利益。此外，集中式的云服务会出现巨大的潜在攻击面，一旦犯罪分子渗透到单个云环境，将可能有权访问数十个或数百个组织的数据，窃取大量的数据资产。随着新的云产品的出现，犯罪分子还可能通过攻击获得商业数据、PII（个人身份信息）等高价值的数据，以便在黑暗网络出售。

我们预测，网络犯罪分子将开始将 AI 技术与多向量攻击相结合，以扫描、检测并利用云提供商环境中的弱点，对云服务商进行攻击。这会削弱许多组织对云服务的信任，并可能对数字经济产生毁灭性的影响。

医疗及关键基础设施 – 安全能力的“装备竞赛”

在所有可能受到网络犯罪技术进步影响的行业中，医疗行业和关键基础设施提供商在风险方面继续位居榜首。为了满足消费者需要，很多医疗与关键基础设施服务提供商牺牲了安全能力，这使他们变得脆弱。

由于这些网络的价值很高，如果这些网络被破坏或者被迫离线，可能会造成破坏性的后果，关键的基础设施和医疗服务提供商现在正在与网络犯罪组织进行“装备”竞赛。一方面相信新的互联系统提供了更多的智能和安全，另一方面面临的风险是真实存在的。

响应： 系统将更趋向于智能与整合 ——“专家级系统”的出现

对恶意软件和网络犯罪技术进步的一个关键反应是开发“专家系统”。 专家系统是一个集成的软件和编程设备的集合，使安全架构能够协同工作，从而消除和阻止高级威胁。除了集成多云和移动设备之外，还需要对未分割的和不安全的网络进行主动监视和保护。

最大的挑战之一将是最后一公里的安全 —— 建立自动化基础安全环境，跨越物理和虚拟环境的复杂的多云生态系统和超融合网络使得执行这些基本的安全实践非常困难。人工智能和自动化需要填补这个空白，用集成的专家安全系统来执行确定设备漏洞、跟踪和修补设备执行、监控安全设备和网络设备的配置、根据信任对设备进行排名等基本安全功能和日常任务。

响应：高级网络威胁情报的利用

IP 地址、恶意软件、流量行为和域名是网络攻击的基本组成部分，他们可以很容易地改变和移动，使他们更难以发现，大多数传统安全解决方案很快就会过时。

威胁情报需要将 IP 地址和文件哈希之外的信息关联，并将重点放在网络犯罪分子难以改变的事情上。通过来自遍布分布式网络的紧密集成架构解决方案的智能与来自全球威胁源的实时数据进行汇总和关联，复杂的分析将能够提供可以快速识别和跟踪恶意行为。最后，

所有威胁行为者都有独特的行为、签名和模式。 一旦能够根据犯罪活动的行为识别和隔离不同的威胁行为者，企业将能够根据历史趋势预测恶意行为，并制定相应对策。

8.2 Fortinet 获得 NSS 入侵防御系统测试报告的推荐评级

Fortinet 的 FortiGate IPS 3000d 和 FortiGate IPS 7060e 在总体拥有成本和安全效益的综合测试上，获得了 NSS 的“推荐”评级。Fortinet 的 FortiGate 解决方案是专为今天的弹性和分布式数据中心提供高吞吐量和颗粒安全有效性要求。为了实现这一目标，FortiGate 解决方案利用专利设计的安全和网络处理器，通过单位应用流量的延迟技术，对 IPv4 和 IPv6 的流量提供高性能的安全保护。

9. Checkpoint

9.1 发布《Check Point 威胁情报 0312——攻击与漏洞榜单》

一种名为“RottenSys”的新型移动僵尸网络广泛肆虐，感染近 500 万台 Android 设 备。RottenSys 恶意软件系列最初被用于在用户设备上强行显示广告。作为目前正在组织的僵尸网络的一部分，RottenSys 包 含广泛的功能，例如毫无迹象地安装其他应用程序以及 UI 自动化。

与俄罗斯关联甚切的 Sofacy APT 针对使用新版本 Flash Player 的欧洲政府机构，开发名为“DealersChoice”的漏洞平台。新 版 DealersChoice 已通过钓鱼电子邮件进行发送，该钓鱼邮件引用内容为本月于英国举行的“水下防御与安全”会议。

利用 Monero 加密货币挖掘软件对 PostgreSQL 数据库系统发起新的攻击活动。该加密货币挖掘软件嵌入好莱坞女星“斯嘉 丽?约翰逊”图片的二进制代码末尾，并已为其运营商获利约 65000 美元。

“Dofoil”恶意软件，又名 Smoke Loader，其在 12 小时内利用 Electroneum 加密货币挖掘软件感染近 40 万台 Windows 计算 机。该攻击针对名为“MediaGet”的 BitTorrent 流行客户端开发出后门程序。

Check Point 研究人员对勒索软件即服务 GandCrab 进行了深入研究。报告显示，GandCrab 的开发者通过采用 AGILE 开发 流程不断改进其恶意软件。

FakeBank Android 银行木马病毒的新变种暴发，目前活跃于韩国。该恶意软件能够拦截受害者与银行有关的呼入和呼出电 话，并将其重定向至诈骗者以窃取受害者的银行信息。

四、 容器技术及安全动态

1. Kubernetes 1.10 发布：更趋稳定的存储、安全与网络功能

新版本的推出不断提升 Kubernetes 的成熟度、可扩展性与可插入性。本次最新版本提升了三大关键性功能的稳定度，分别为存储、安全与网络。另外，此次新版本还引入了外部 kubectl 凭证提供程序（处于 alpha 测试阶段）、在安装时将 DNS 服务切换为 CoreDNS（beta 测试阶段）以及容器存储接口（简称 CSI）与持久本地分卷的 beta 测试版。

容器存储接口（简称 CSI）在 Kubernetes 中的实现方案终于迎来 beta 版本：如今，安装新的分卷插件就如同部署 pod 一样简单。这反过来又使得各第三方存储供应商能够在核心 Kubernetes 代码库之外独立开发自己的解决方案，从而进一步延续了 Kubernetes 生态系统的可扩展性。

在本版本中，持久（非共享）本地存储管理也迈向 beta 阶段，这意味着本地连接（非网络连接）存储可作为持久分卷源使用。如此一来，分布式文件系统与数据库的性能将进一步提升，而使用成本则有所降低。

此版本还包含对持久分卷的多项更新。Kubernetes 如今可以自动防止某一 pod 正在使用的持久分卷声明遭到删除（beta 阶段），同时亦可防止删除与持久分卷声明绑定的持久分卷（beta 阶段）。这将有助于保证用户以正确的顺序删除存储 API 对象。

安全——外部凭证供应方（alpha 阶段）

各云服务供应商、厂商以及其他平台开发者现在能够发布二进制插件以处理特定云供应商 IAM 服务的身份验证，或者与 Active Directory 等并非天然受到支持的内部身份验证系统相集成。这一调整补充了 1.9 版本当中新增的云控制器管理器功能。

网络——利用 CoreDNS 作为 DNS 提供程序（beta 阶段）

新版本允许您在安装过程中将 DNS 服务切换为 CoreDNS，这一功能目前处于 beta 阶段。CoreDNS 的移动部件更少——仅拥有单一可执行文件与单一进程，且可支持更多其它用例。

2. SmartX 与 Rancher Labs 联合，共同打造用于容器的超融合基础架构平台

Rancher Labs 宣布与国内领先的超融合产品与解决方案供应商 SmartX 达成战略合作，

Rancher Labs 将加入“SmartX 生态合作伙伴计划 / SmartX Ecosystem Partnership Program（SEPP）”，与 SmartX 强强联合，共同打造用于容器的超融合基础架构平台。

SmartX 和 Rancher Labs 将联手，将超融合技术与容器技术相结合，由 Docker、KVM、操作系统和持久化存储服务组成一个完整的、可用于容器的超融合基础架构平台，基于最新的高性能硬件架构，充分发挥容器先天的高资源利用率、高部署速度的优势，降低企业用户的运营工作复杂度及成本，提供一个高效、轻量、灵活的基于容器的超融合解决方案。

3. Docker Cloud 要关闭集群服务了

Docker 云集群和应用管理服务将会在五月廿一日关闭。用户在此之前须迁移至其他平台并注销 Swarms 服务。

Docker 云服务将会永久关闭，意味着基于 Docker 云的节点，Swarm 集群和应用都将不可用。为了保护用户应用，必须将他们迁移至其他平台，并从 Docker 云注销 Swarm 服务。

五、 安全新产品及技术

1. 新的面部识别技术 Face Flashing 面世

研究人员近期设置一种新的面部识别系统 Face Flashing，可以利用光影模型对人脸的反射来识别不同的人，并根据系统读取反射光线的速度来判断是否是伪造的人脸在尝试识别。这个系统的主要组成是计算机，并与 LCD 屏连接（可以是电脑显示屏也可以是手机屏幕，甚至是安全入口处的认证面板）。系统会向人脸投射一种灯光模型，旁边的照相机会拍下并记录灯光对人脸的反射方式，并将数据传输到内部的实时检测模型，然后转成实际面部识别特征。在这个系统中，最重要的因素就是反射的光影。这与之前的生物识别方式不太相同，算是一个进步。不过也有专家认为仅仅依赖光影模型可不如声称的那么安全。

2. 谷歌 72 位量子计算机来了，比特币有可能被破解

在近日的美国物理学会上，Google 实验室公布了最新一代量子处理器 Bristlecone，Bristlecone 是一款 72 位量子位处理器，错误率只有 1%。这款处理器不仅能够帮助科学家们进行量子模拟的探索，还能够在量子机器学习上有所应用。最为重要的是 Google 实验室谨

慎且乐观的认为：如果一切运行良好的话，量子霸权将在未来几个月到来。目前量子计算机只在科研领域有所应用，但如果真如 Google 实验室所言 Bristlecone 能达到量子霸权，那么比特币等基于区块链技术的虚拟货币可能将被破解。

3. 两个 Memcached DDoS 攻击 PoC 发布

Memcached DDoS 攻击 – 全球最大的 DDoS 攻击达到 1.7Tbps 后几天，有人公布了两个针对 Memcached 放大攻击的 PoC 代码。Memcached DDoS 攻击背后的漏洞是最热的话题之一。世界上最大的 DDoS 攻击记录只持续了几天，本月早些时候，一家美国服务提供商遭到 1.7 Tbps 的 memcached DDoS 攻击。而现在有人已经发布了两段 PoC 代码，两端代码都可以利用 Memcached 进行 DDoS 放大攻击，任何人都可以使用它们来发起 memcached DDoS 攻击。其中一个 PoC 代码漏洞用 Python 脚本语言编写，依靠 Shodan 搜索引擎 API 获取存在漏洞的 Memcached 服务器列表，然后进行 memcached DDoS 攻击。第二个漏洞利用代码是用 C 编程编写的，并使用了存在漏洞的 Memcached 服务器列表。作者还发布了 memecache-amp-03-05-2018-rd.list 文件，该文件是截至 03-05-2018 的存在漏洞的 memcached 服务器列表。

4. 荷兰警方公布打击 Hansa 暗网的细节

Hansa 黑暗网络市场已经完全得到移除，荷兰警方在全国电视上公开了案件的细节，详细介绍了他们是如何做到的。2016 年，荷兰警方从 Bitdefender 处得到消息，了解到最受欢迎的暗网市场 Hansa 服务器运营在荷兰。 该暗网市场和其他一样，出售毒品，窃取信用卡数据并用逃脱监管。“我们希望全世界都知道，你不能指望在网上匿名匿名并犯下罪行 - 即使在黑暗的网络上，”荷兰国家高级科技犯罪部门负责人如此说道。到了 2016 年 10 月，警察仿造了服务器，并重构站点。通过一些列深入研究，他们进入了管理员页面并找到了聊天记录，最终确定了网站运营者。警方成功地对涉案人员进行了窃听，并找到了大量信息，其中包括 Hansa 服务器的流量数据，四位网站管理员的姓名以及他们使用的私人聊天服务的详细信息。

5. 约 90% 的企业到 2020 年都会使用生物认证技术

国外公司 Spiceworks 近期发布一项调查报告，称到 2020 年 90% 的企业将会采用生

物认证技术。大部分情况下，人们采用的还是多因素验证方法。目前为止，指纹验证是最常用的生物认证方式（57%），人脸识别排第二（14%），其他的还有手部姿势识别（5%）、虹膜扫描（3%）、语音识别（2%）和手掌静脉识别（2%）等。此外，企业组织最常在智能手机上进行生物认证（46%）、其次是笔记本电脑（25%）和平板设备（22%）等。很多 IT 专家认为，在未来两到三年内，生物认证还不会完全替代文本密码，但依然会成为比较重要的验证方式。

6. Linux 基金会宣布开启物联网 ACRN 项目

Linux 基金会宣布了一个名为 ACRN 的新项目，该项目将为物联网设备创建虚拟机管理程序通用代码。Linux 基金会表示，它将 ACRN 构建为完全可定制的项目，由两个主要组件组成：管理程序本身和用于与底层硬件交互的设备模型。ACRN 将为物联网领域带来帮助，特别是智能工业设备的开发。ACRN 团队希望硬件供应商将他们的项目作为在物联网设备上固件运行的基础，使他们能够在虚拟机 VM 上运行的各种客户操作系统之间轻松切换和更新系统。

7. G20 将加密货币定义为资产而非货币

阿根廷担任二十国集团（G20）主席国后的首次 G20 财长和央行行长会议日前在阿根廷布宜诺斯艾利斯举行，周小川最后一次以中国央行行长的身份率团出席了该会议。周小川在会上表示，中国支持就加密资产和数字货币问题在 G20 下加强政策协调。据了解，本次会议形成了 G20 联合公报，公报将加密货币定义为资产而非货币，承认其提高金融经济效率和包容性的优势，但也对其逃税、洗钱、恐怖融资等问题表示关注。

8. 谷歌宣布将新增包括区块链技术在内的 20 多项功能加强安全性

据 SC Media US 报道，谷歌宣布将增强其安全系统，包括括 DDoS 保护、高透明度、区块链技术等一系列特点。据悉，谷歌将会发布超过 20 份与安全相关的新声明，将涵盖整个 Google Cloud 产品。

9. IETF 批准 TLS 1.3 为互联网标准

互联网工程任务组（IETF）已正式批准 TLS 1.3 作为传输层安全（TLS）协议的下一个主要版本，IETF 组织是专门批准互联网标准和协议的组织。这个决定是在经过四年的讨论和 28 项协议草案之后提出的，第 28 个草案被选为最终版本。TLS 1.3 将成为客户端和服务器之间的通信标准，也就是 HTTPS 的标准。该协议与其以前的版本-TLS 1.2 相比有几个优点。最大的特点是 TLS 1.3 将旧的加密算法和散列算法（如 MD5 和 SHA-224）替换为较新较难破解的方案（如 ChaCha20，Poly1305，Ed25519，x25519 和 x448）。其次，在谈判客户端和服务器之间的初始握手时，TLS 1.3 也快得多，从而减少了延迟。第三，TLS 1.3 还将支持 TLS False Start 和零往返时间（0-RTT）等功能，有助于缩短与客户段与之前通信的主机建立加密握手所需的时间。第四，TLS 1.3 具有抵御降级攻击的功能，防止攻击者欺骗服务器使用较旧版本的协议，从而利用以前的漏洞。

10. 微软发布了在 Windows 10 上运行任何 Linux 操作系统的工具

微软发布了一款工具帮助 Linux 爱好者将他们最喜爱的 Linux 发行版移植到 Linux 子系统（WSL）上，该子系统是一个 Windows 10 组件，用于在现代 Windows 10 PC 上装载 Linux 发行版。微软已经发布了针对 Ubuntu、SUSE、Kali Linux 和 Debian 的官方镜像，所有这些都可以通过官方 Windows 商店获得。但尽管微软做出了最大的努力，OS 开发商将永远没有足够的时间和资源来移植所有 Linux 发行版来运行其 WSL 实现，这里有太多的 Linux 发行版，其中大部分是为特定目的创建的小众发行版。

六、 网络安全投融资、收购事件

1. 收购

1.1 KnowBe4 完成对 Popcorn Training 的收购

3 月 5 日，KnowBe4 完成对 Popcorn Training 的收购，收购价未公布。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。Popcorn Training 是提供一种易于理解、高效和娱乐化的网络安全培训方案。

1.2 CyberArk Software 完成对 Vaultive 的收购

3 月 12 日，CyberArk Software 完成对 Vaultive 的收购，收购价未公布。CyberArk Software 是新的 IT 安全解决方案的引领者和先驱，它保护公司免受网络攻击，即时这些攻击已经在网络范围内攻击企业的核心。而 Vaultive 的云安全和治理控制则可以对企业云服务提供持续性保护。

1.3 Palo Alto Networks 完成对 Evident.io 的收购

3 月 14 日，Palo Alto Networks 以 3 亿美元价格完成对 Evident.io 的收购。Palo Alto Networks 是美国一家网络安全公司，由 Nir Zuk 先生于 2005 年创立，公司主要专注于防火墙的创建。Evident.io 则是一家云安全技术公司，主要为为政府和企业提供公共云安全监控服务，通过原生 Evident 软件平台，企业可以实时监控旗下云基础设施负载上的安全风险，并且能在第一时间内将问题通知给运维人员，让他们及时采取补救措施。

2. 投融资

2.1 MedStack 获得未知数额的种子轮融资

3 月 1 日，MedStack 筹得未知数额的种子轮融资。MedStack 通过安全云托管、HIPAA、预定义策略和人工配置，将医疗应用程序交付到市场的速度提高 60%。

2.2 Snyk 获 700 万美元 A 轮融资

3 月 6 日，Snyk 从 Boldstart Ventures 和其他 4 位投资者处筹得 700 万美元的 A 轮融资。Snyk 是一家开源库漏洞的解决方案提供商，帮助开发人员在投入生产之前找到并修复开源代码中的漏洞。

2.3 Bitt 获 300 万美元 B 轮融资

3 月 8 日，Bitt 从 Medici Ventures 处筹得 300 万美元的 B 轮融资。Bitt 是一种电子货币，其核心业务是提供进入新兴市场的加密货币。

2.4 Solebit 获 1100 万美元 A 轮融资

3 月 14 日，Solebit 从 ClearSky 和其他 2 位投资者处筹得 1100 万美元的 A 轮融资。Solebit 采取了一种非行为的方法来检测和预防 APT 攻击以及 0Day 攻击。

2.5 Luminate Security 获 1400 万美元 A 轮融资

3 月 14 日，Luminate Security 从 Aleph 和 U.S. Venture Partners 处筹得 1400 万美元的 A 轮融资。Luminate Security 的主要产品是一个可以快速设置和易于管理的公司资源混合云接入平台，名为 The Secure Access Cloud。

2.6 Virsec 获 2400 美元 B 轮融资

3 月 20 日，Virsec 从 Amity Ventures 和其他 4 位投资者处筹得 2400 万美元的 B 轮融资。Virsec 成立于 2014 年，是一家专注于网络安全的公司，提供了一种全新的方法来保护企业免受高级攻击。