内容摘要

云厂商方面，Amazon EFS 现已支持传输中数据加密，同时 Amazon EC2 现在提供 Ubuntu 和 Amazon Linux 2 上的 Microsoft SQL Server AMI，并且推出 AWS 区块链模板，以及 AWS Config 增加 AWS Elastic Beantalk 支持；VMware 最新研究表明 APJ 地区企业在多云部署时认为成本与安全性优先于创新；Google 使用 AI 进行篮球比赛胜负预测，并且开始在日本和澳大利亚之间铺设 9600 公里海底电缆以满足包括云在内的网络业务需求；微软公司重组加码云计算，并携手联想发布混合云解决方案，同时业绩显示 Azure 云收入翻倍；阿里云将加速广东智造转型升级和与福州合作打造“数字中国”福州样本，并且进军土耳其市场，同时发布区块链解决方案，以及在将 ET 医疗大脑应用于妊娠糖尿病预测；腾讯云“超算中心”落户重庆；华为发布 2017 终端云服务白皮书和区块链白皮书，并在 2018RSA 上发布 SDSec 解决方案。

开源云方面，OpenStack 宣布腾讯云 TStack 成为其白金会员；九州云发力边缘计算产业，并且九州云金融案例入选“2017 年度中国 SDN、NFV 优秀案例”。

云安全厂商方面，启明星辰正式发布信息安全领域首款电子签章产品：启明星辰电子签章系统；另外，公司牵头组织并实施的 2016 年北京市科委科技计划及课题顺利通过验收，联合申报的“交通运输网络安全技术行业研发中心”正式启动。

其他安全厂商，国内方面：亚信安全产研院与眉山市公安局签署战略合作协

议，共建网络空间平安示范城市。绿盟科技联合前海财险推出网络安全险，发布了新一代云计算安全解决方案。360 在 RSA 大会上展示了基于大数据、人工智能、云计算技术的全网威胁实时监控系统和三大杀毒引擎。安恒在 RSA 大会上首发玄武盾全新版，发布资产安全和漏洞管理解决方案。国外方面：Arista Networks 加入 Fortinet Fabric-Ready 合作伙伴计划，推动跨数据中心和云网络的安全自动化；CheckPoint 和 CloudPassage 整合并发布。

容器动态方面，Cilium1.0 发布，将 BPF 革新引入 Kubernetes 网络和安全系统；Docker 发布企业版 2.0，着力提升 Kubernetes 的支持能力和安全性。

安全新技术方面，研究人员发现 PDF 文件可被恶意攻击者利用，在无需用户交互的情况下，只需打开文件就能窃取 Windows 凭证（NTLM 哈希）；近期区块链安全问题增多，SMT 项目现安全漏洞，火币 Pro 暂停所有币种充提币业务，MongoDB 服务器漏洞泄漏加密货币用户信息；微软布为 Office 365（基于商业订阅的办公工具套件）推出新的反勒索软件功能，同时宣布推出 Windows Defender System Guard runtime 认证，该新的安全技术可以为杀毒软件厂商提供额外的帮助，并且可以检测到内核篡改，rootkit 和漏洞利用，微软为 Linux 子系统提供了 Windows Defender 防火墙。

威胁情报公司 AlienVault 宣布推出免费终端扫描服务 OTX Endpoint Threat Hunter，新产品让企业和安全专家识别其网络中的威胁；谷歌、微软和 Mozilla 的浏览器很快将为用户提供由 FIDO 联盟和万维网联盟构建的全新无密码认证标准，目前正处于最终审批阶段。Ubuntu 18.04 LTS 版发布， Ubuntu 18.04 LTS 在云计算领域效率极高，特别适用于机器学习这样的存储密集型和计算密集型任务，该版本的 Linux 内核支持一些全新的特性，如 AMD 安全内存加密，以及针对

SATA Link 电源管理的改进等。

网络安全公司投融资方面，总共发生 3 起收购和 7 起投资事件。专注于防火墙的网络安全公司 Palo Alto Networks 以 1 亿美元的价格完成对自动化安全平台提供商 Secdo 的收购。云服务提供商 Evolvo IP 则以未知价格完成对统一云通信业务商 thevoicefactory 的收购。RSA 将收购行为分析公司 fortscale。融资方面，SaaS 运营管理平台提供商 BetterCloud 以 6000 万美元的 E 轮融资拔得头筹，身份管理和云安全解决方案的创新公司 Saviynt 和网络安全解决方案商 Onapsis Inc. 分别以 4000 万美元的 A 轮融资和 3100 万美元的 C 轮融资分列二三位。

2018 年 5 月 2 日

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 EFS 现已支持传输中数据加密

4 月 1 日， Amazon Elastic File System (Amazon EFS) 现在允许加密在文件系统及其客户端之间传输的数据。Amazon EFS 传输中数据加密使用行业标准的 Transport Layer Security (TLS) 1.2 来加密发送至连接的客户端和从连接的客户端发送的所有数据。为进一步简化 EFS 的使用，AWS 发布了一款挂载帮助程序，可用于建立加密客户端至静止加密的或未加密文件系统的连接。通过这项发布，Amazon EFS 现在提供全面的加密解决方案，允许客户加密静止和传输中数据。

1.2 Amazon EC2 现在提供 Ubuntu 和 Amazon Linux 2 上的 Microsoft SQL Server AMI

4 月 19 日，Amazon EC2 现在提供 Ubuntu 和 Amazon Linux 2 上已包含许可证 (LI) 的 Microsoft SQL Server 2017 的 Amazon 系统映像 (AMI)。这些 AMI 将添加到以前使用 Windows Server 和 Red Hat Enterprise Linux 启动的 SQL Server 2017 AMI 列表上，从而可以更加灵活地在 Amazon EC2 上利用需要的操作系统运行 SQL Server 工作负载。

1.3 推出适用于以太坊和 Hyperledger Fabric 的 AWS 区块链模板

4 月 19 日，AWS 区块链模板提供了一种使用开源框架快速轻松地创建和部署安全区块链网络的方法。借助 AWS 区块链模板，可以使用经过认证的托管 AWS CloudFormation 模板部署以太坊和 Hyperledger Fabric 框架。使用 AWS 区块链模板，可以专注于构建区块链应用程序，而不用花费时间和精力手动设置区块链网络。

AWS 区块链模板将选择的区块链框架作为容器部署在 Amazon Elastic Container Service (ECS) 集群上，或直接部署在运行 Docker 的 EC2 实例上。区块链网络是在自己的 Amazon VPC 中创建的，因此，可以使用 VPC 子网和网络访问控制列表。可以使用 AWS IAM 分配精细的权限，以限制 Amazon ECS 集群或 Amazon EC2 实例可以访问的资源。

1.4 AWS Config 增加支持 AWS Elastic Beanstalk

4 月 24 日，现在可以使用 AWS Config 来记录 AWS Elastic Beanstalk 资源类型的配置更改。AWS Elastic Beanstalk 服务可以部署和扩展以多语言开发的 Web 应用程序和服务。只需上传代码，Elastic Beanstalk 将自动处理包括容量预置、负载均衡、自动扩展和应用程序运行状况监控在内的部署工作。使用 Config，您可以跟踪对 Elastic Beanstalk 应用程序、应用程序版本、环境以及该环境中配置的所有资源的更改。例如，可以查看环境平台版本、部署和扩展策略、运行状况策略以及标签等方面的更改。

2. VMware 云动态

2.1 VMware 最新研究表明 APJ 地区企业在多云部署时认为成本与安全性优先于创新

4 月 24 日，VMware 联合 MIT Technology Review Custom 公布了一项旨在分析亚太及日本地区（APJ）企业多云部署的最新调研结果。该调研着重指出，在云端部署人工智能方面，虽然 APJ 地区的受访者比全球同行更加乐观，但他们在使用多家提供商推动创新方面落后于潮流。同时，在多云部署过程中，安全仍是首要考虑和担忧的因素，尤其是在欧盟《通用数据保护条例》将于 2018 年 5 月生效之际。

该项名为《部署风暴后，多云环境雨过天晴》的调研分析了全球大型企业的 1300 多位 IT 决策者对云部署的态度——其中包括来自澳大利亚、中国、日本与印度的 750 多位高管。

该调研结果表明，在利用多云实施创新推动业务增长方面，APJ 地区仍比较滞后，而成本则是云部署过程中主要的影响选择的因素：

- APJ 地区的受访者未将改进创新视作多云部署的一项主要优势，这表明使用多家提供商推动创新在该地区仍处于相对初期的阶段。
- 就采用人工智能等技术而言，各企业机构仍处于学习阶段。APJ 地区受访者表示，他们目前正在使用人工智能或机器学习，包括人工智能驱动型云。
- 来自中国与印度的受访者即将采用人工智能，近半数表示其所在公司将在未来 3 年内采用人工智能。来自印度的受访者意愿最为强烈，认为云将很快由人工智能所驱动。

3. GOOGLE 云动态

3.1 谷歌使用人工智能技术来预测篮球比赛胜负结果

4 月 2 日，根据国外媒体报道，谷歌表示将在本赛季的 NCAA 美国大学生篮球联赛总决赛阶段充分利用自己的数据科学人工智能技术。谷歌云计算部门会使用人工智能和机器学习技术来展示谷歌的最新成果，通过对比赛上半场的表现数据进行分析，在中场休息的时候给出下半场比赛结果的预测。

谷歌表示，在今年的 NCAA 联赛中合作，专注于比赛统计和数据分析，并且充分利用谷歌云平台的优势。在所有谷歌能够识别的信息中，包括不同该运动员的以往的表现、稳定性等数据都会被考虑在内。“这个团队想要看看人工智能和分析工具在比赛中是如何表现的，因此将会在周末的比赛场次中上半场结束后进行预测，然后对下半场的表现或数据进行分析和总结。”

这一实验在美国国内观众中也引起了关注。在进入到中场休息时间后，谷歌会对其数据进行分析并且做出预测，然后制作出电视广告，在下半场比赛开始之前播出。谷歌表示：“这可能是自己首次使用实时预测分析技术在直播的体育赛事中投放广告。”

3.2 DeepMind 或成谷歌未来盈利利器

4 月 2 日，根据报道，上周，谷歌云计算部门宣布了一项新服务：将文本转换为自然语音，这也是第一款包含 DeepMind 代码的产品。Google Cloud 提供的文本至语音应用程序接口可提供男声和女声的转换，每转换一百万文本字符的成本是 16 美元。

Alphabet 同时还运营其他 AI 研究团队，但 DeepMind 一直担任着更多充满未来主义的工作，例如 Alpha Go。DeepMind 是 Alphabet 的大手笔投资之一，同时还将技术不断转化成商业应用程序。在 Facebook 和微软，A.I.研究小组已经将技术转化为可销售的产品。

3.3 谷歌开始在日本和澳大利亚之间铺设 9600 公里海底电缆

4 月 4 日，谷歌表示已开始在日本和澳大利亚之间铺设长 6000 英里（约合 9600 公里）的海底电缆，以满足该公司云计算业务迅速增长的网络需求。日本和澳大利亚之间的谷歌电缆由两部分组成。一部分将从日本延伸到关岛，另一部分从关岛延伸到悉尼。

4. 微软 Azure 云动态

4.1 微软公司重组加码云计算

4 月 1 日，据媒体报道，微软公司施行重大重组，将新设“AI 与云计算”和“体验与设备”两大部门。这意味着，微软正在削弱其 Windows 产品系的重要性，将云计算放在更高的层级。

4.2 联想携手微软发布混合云解决方案

4 月 19 日，联想发布了 ThinkAgile SX for Microsoft Azure Stack 混合云解决方案。ThinkAgile SX for Microsoft Azure Stack 是首批在国内上市的支持 Azure Stack 的集成系统。Azure Stack 是 Azure 公有云在本地数据中心的延伸，它使用相同的 Azure Resource Manager 应用部署模式、自助服务门户和 API，定期更新，保证与 Azure 一致的混合云平台和体验。

4.3 微软业绩超预期 Azure 云收入翻倍

4 月 27 日，微软发布截止于 3 月 31 日的财报，该季度营收为 268 亿美元，同比增长 16%，其中 Azure 云业务同比增长 93%。净利润为 74 亿美元，同比增长 35%。营收和净利均超过分析师预期，微软股价盘后上涨 2.27%。

5. 阿里云动态

5.1 阿里云将加速广东智造转型升级

4 月 2 日，2018 中国（广东）数字经济融合创新大会在广州举办，阿里云总裁胡晓明回顾了阿里巴巴同广东的十年之约，并表示下一个十年之约将加速广东制造向“广东智造”转型升级。阿里云

在广东服务的企业已经超过 10 万家。这份名单包括：珠江啤酒、OPPO、珠江钢琴、金立、美的等知名企业。即便是顺德地区的中小工厂也在广泛使用阿里云的技术。据了解，除了工业之外，阿里云的人工智能已经在城市、航空、金融、司法、农业、环保等多个领域规模化落地。

5.2 阿里云进入土耳其市场

路透社 4 月 9 日发布的快讯称，阿里云于 4 月 9 日正式进入土耳其市场。据悉，此前，阿里云已经在欧洲、北美、东南亚、中东等全球 18 个地区建设了 43 个可用区，成为亚洲最大的云计算平台；此次和 E-Glober 达成深度合作，意味着阿里云进一步将中国市场的领先优势拓展到“一带一路”沿线地区。

另据美国商业资讯网站 4 月 9 日报道，当天阿里云和 E-Glober 宣布建立伙伴关系，为土耳其市场带来强大、可靠、成本效益高的云计算产品和服务，以帮助当地企业捕捉数字化转型带来的机遇。报道称，E-Glober 是阿里巴巴集团在土耳其的唯一授权代理商。而将阿里云强大的云计算能力、全球基础设施与 E-Glober 本地网络结合在一起的广泛合作，将为满足土耳其本土公司的数字化和国际化扩张需求提供一个强有力的工具。

5.3 阿里云发布区块链解决方案

4 月 10 日，阿里云发布区块链解决方案，支持天猫奢侈品平台 LuxuryPavilion 推出全球首个基于区块链技术的正品溯源功能。该方案旨在帮助进一步打造和拓展奢侈品供应链应用生态。

据阿里云官方介绍，借助阿里云区块链技术，天猫会将奢侈平台 Luxury Pavilion 上商品的原材料生产过程、流通过程、营销过程信息整合写入区块链，使得品牌的每条信息都拥有特有的区块链 ID“身份证”，附上各主体的数字签名和时间戳，供消费者查询和校验。

阿里区块链项目统计

时间	项目名称	具体内容
2016 年 7 月	公益善款追踪	与中华社会救助基金会合作，在支付宝爱心捐赠平台上线区块链公益筹款项目“听障儿童重获新声”，让每一笔善款可被全程追踪。
2017 年 3 月	跨境食品供应链	阿里巴巴与普华永道达成合作，宣布将应用区块链打造透明可追溯的跨境食品供应链，搭建更安全的食品市场。此次合作在澳大利亚、新西兰这两个全球最大的食品、乳制品出口国开始试水。
2017 年 8 月	“医联体+区块链”试点项目	阿里健康与江苏常州市合作推出我国首个基于医疗场景的区块链应用——“医联体+区块链”试点项目。该项目旨在将最前沿的区块链技术应用于常州市医联体底层技术架构体系中，实现当地部分医疗机构之间安全、可控的数据互联互通，用低成本、高安全的方式，解决长期困扰医疗机构的“信息孤岛”和数据安全问题。
2017 年 10 月	“BASIC”战略	“BASIC”战略，其中的 B 应的就是区链(Blockchain)，技术实验室宣布开放区块链技术，支持进口食品安全溯源、商品正品溯源等。蚂蚁金服风控团队宣布开放风控云服务，帮助解决各行业面临的业务安全风险问题，比如羊毛党，信贷欺诈，黄牛党，刷单等等风控问题。
2017 年 11 月	数字雄安区块链实施平台	阿里巴巴集团、蚂蚁金服集团与雄安新区签署了战略合作协议，阿里巴巴与蚂蚁金服将承建数字雄安区块链实施平台。
2018 年 4 月 12 日	奢侈平台 Luxury Pavilion	助阿里云区块链技术，天猫会将奢侈平台 Luxury Pavilion 上商品的原材料生产过程、流通过程、营销过程信息整合写入区块链，使得品牌的每条信息都拥有特有的区块链 ID“身份证”，附上各主体的数字签名和时间戳，供消费者查询和校验。

数据来源：网贷之家整理

5.4 阿里云 ET 医疗大脑预测妊娠糖尿病准确率 83% 发病率或降 65%

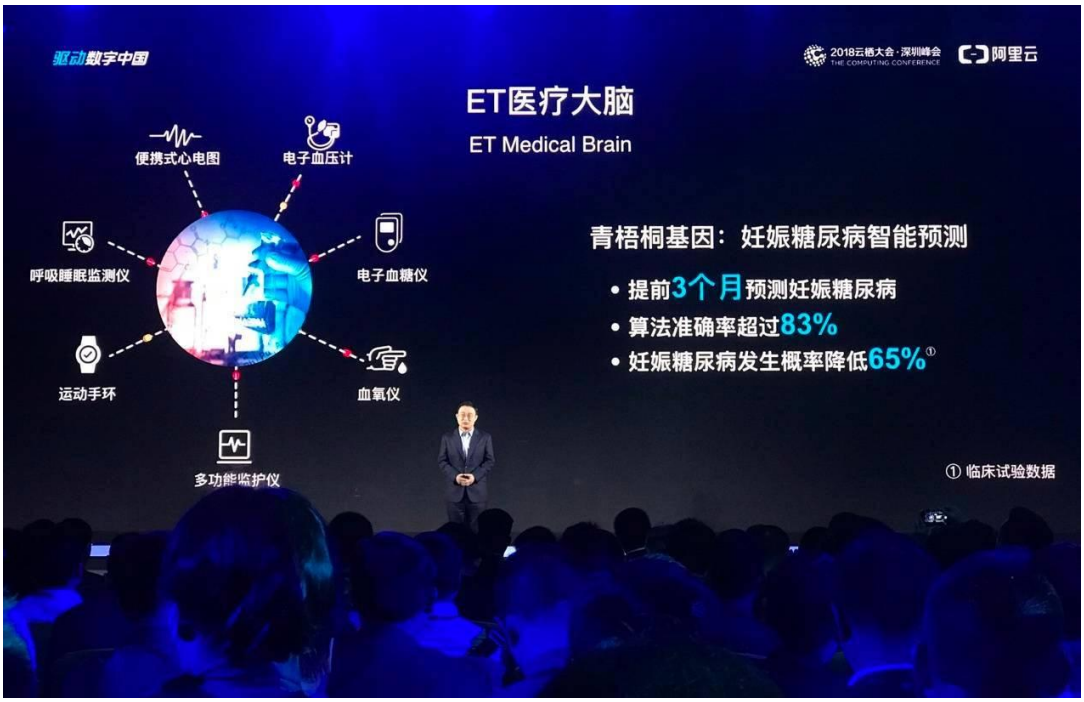
4 月 20 日，阿里云对外披露了 ET 医疗大脑的新突破。他们联合青梧桐基因研究团队，对临床数据、检验数据、基因数据结合孕妇生活方式，用机器学习算法实现了对妊娠糖尿病（简称：GDM）的精准预测，准确率达到 83%。在孕早期积极干预后有望将实际发病率下降 65%以上。这项技术填补了国内尚无准确预测工具的空白。

阿里云 ET 医疗大脑的最新成果则可以根据孕 8-12 周的临床检查数据和基因数据，来预测个体的发病概率，目前准确率能达到 83%，为高风险孕妇赢得了 12－16 周的干预时间。

“之前的筛查方法大多是基于高危因素进行判别，或者结合临床检查数据，如相关生化指标等进行人工智能机器学习，缺少个体的基因数据，预测结果并不理想。”阿里云精准医疗科学家顾斐表示，我们首次将高危因素数据、体检和化验数据、基因数据、生活方式数据综合使用，随着项目的开展，机器学习算法会越来越聪明，准确率有望进一步提升。

目前，此项目已经完成在吉林省妇幼保健院、长春市妇产医院等十余家三甲医院部署，已经与北京协和医院、中国疾控中心营养与健康所等国内权威临床科研机构开展合作，拟将上述系统用于妊娠期糖尿病高危人群提早干预对母胎结局影响的研究。

未来，阿里云将联合青梧桐基因，在准确预测妊娠糖尿病的基础上，建立妊娠糖尿病高风险人群的精准干预算法模型，通过精准预防，降低妊娠糖尿病发病率。



5.5 阿里巴巴、蚂蚁金服与福州合作打造“数字中国”福州样本

4 月 22 日，首届数字中国建设峰会于 22 日在福建福州开幕。在本次峰会开幕前夕，福州市政府与阿里巴巴集团、蚂蚁金服集团达成战略合作，全方位打造“数字中国”的福州样本。三方将深化在互联网产业服务、互联网政务服务、城市大脑以及公共信用体系等智慧城市建设领域的合作。同时，阿里云将和福州市长乐区共建“工业互联网”，推动当地工业制造业升级。

6. 腾讯云动态

6.1 腾讯云“超算中心”落户重庆

4 月 12 日，腾讯云（重庆）工业互联网智能超算中心项目 12 日完成签约。本次项目合作是腾讯云携手重庆市经信委、两江新区管委会、长安汽车四方联合推出，是由腾讯根据长安汽车对企业工业设计仿真计算的需求投资建设的创新项目。据介绍，基于超算中心，腾讯云将与长安汽车合作共建智能汽车工业设计云、长安系营销大数据项目，并为长安汽车智能网联、新能源等领域项目提供资源和服务支撑。

7. 华为云动态

7.1 华为发布 2017 终端云服务白皮书：用户数已超 3.4 亿

4 月 18 日，第十五届全球分析师大会期间，华为发布了 2017 终端云服务白皮书。白皮书显示，2017 年华为终端云服务全球用户数超过 3.4 亿，注册开发者超过 35 万。

根据华为发布的 2017 终端云服务白皮书（以下简称白皮书）显示，华为终端云服务用户平均每天使用手机 6.6 小时，涵盖通讯、消费、理财、娱乐、拍照、游戏、阅读、资讯获取、旅行出游、教育、运动、就餐、数据管理等多个生活场景。

截至 2017 年底，华为终端云服务的全球用户数已经超过 3.4 亿，海外用户数突破 3000 万，国内外用户数量分别增长了 56%和 372%。

同时，华为注册开发者数量超过了 35 万，提交应用数量相比 2016 年上升 36%，合作伙伴获得的收益上升 60%，其中游戏开发者收益上升 99%，主题开发者的收益上升 135%。为了更好的激励开发者，2017 年华为终端云还发布了“耀星计划”，设立 10 亿元基金从人才培养、开发支持、创新支持、营销辅助等多方面激励和扶持创新。

7.2 华为云发布区块链白皮书 加速区块链技术行业落地

4 月 18 日，在 2018 华为分析师大会(HAS2018)期间，华为云 BU 总裁郑叶来在云专场发布《华为区块链白皮书》。该白皮书的发布，对加快区块链技术的快速落地，推动行业数字化转型，有着积极的助力作用。

7.3 SDSec：今年 RSA 华为的主打解决方案

4 月 26 日，今年的 RSA 2018 大会上，华为则着重介绍了自己的 SDSec（软件定义安全）

解决方案。

华为认为，在新的互联网环境下，企业需要应对三大挑战：未知威胁更善于伪装，难被发现；新型恶意软件传播速度加快，难被响应；安全部署效率低下，难以适应发展。可以说三大问题，都能总结为一个“慢”字。然而，天下武功，唯快不破。华为 SDSec 解决方案通过三大关键能力，构筑主动防御体系，达成先敌一步的“快”。

检测智能：发现“快”

SDSec 解决方案采用人工智能进行检测。不只是使用打分制的直线模式，而是将威胁判断扩展到类似人脑神经网络的多维立体空间，更加立体化地对样本进行更精细的判断。对于加密流量，SDSec 结合机器学习算法，在加密流量中提取多个行为特征，在不解密流量，不损耗网络性能的情况下，检测加密流量中的恶意流量。

处置智能：处理“快”

华为的 SDSec 对 SDN 进行了升级，在控制层实现对网络、安全以及第三方上安全能力的统一调度管理，从而以全网的角度进行了联动防御。而华为自身拥有的产品系列，可以为用户提供端到端的完整安全解决方案。用户可以使用厂商预设的自动化响应模板针对不同的情况预先制定处置方案，从而提升响应效率。用户也可以根据自己不同的应用需求自定义模板。另外，由于全网协防，使得整个系统能快速感知被感染主机，并且进行切断隔离，防止病毒进一步扩散。

运维智能：部署“快”

华为的一个改变是不再基于一个固定的网络安全框架，而是针对应用来采取相对应的安全配置。通过安全控制器提供的场景化自助业务模型，用业务模板去匹配需要的业务安全需求；将应用安全策略自动应用到对应的安全资源池，实现业务敏捷要求；同时协同、联动 SDN 网络控制器，在业务变更扩展时对安全策略自动调整以及适应；最后简化对信息的读取，不再依赖于了解繁冗的网络信息，而是通过图形化的形式去读取安全业务的常用信息。SDSec 帮助运维人员极大程度地减少了运维的难度与复杂度。

二、 开源云动态

1. Openstack 动态

1.1 跻身 OpenStack 白金会员，腾讯云 TStack 助力构建高稳定云平台

北京时间 2018 年 4 月 25 日 OpenStack 官方正式公布腾讯成为 OpenStack 基金会白金会员。这是继腾讯云 TStack 斩获 OpenStack 2017 年度 Superuser 大奖之后，在 OpenStack 技术领域的又一重大突破。腾讯云 TStack 团队一次性通过答辩，成为互联网领域首家 OpenStack 白金会员。

腾讯云 TStack 是腾讯云基于自身强大技术能力和海量运营经验推出的私有云平台，具备高稳定性、统一管理、可视化运营等特点，可提供集 IaaS、PaaS 和 SaaS 为一体的综合云服务解决方案，助力政府、企业构建稳定安全的云环境和健康的云生态。长期的经营和技术迭代，让腾讯云 TStack 在同类产品中极具竞争力，在行业已取得重要的成绩。

目前，腾讯云 TStack 在腾讯内部的使用已经涵盖 4 个地区(深圳、上海、天津、成都)、7 个机房、14 个集群，服务于腾讯内部多种线上环境，300 多条业务线;TStack 平台同时也承载着腾讯内部各产品线的开发测试服务，比如微信，QQ，浏览器，游戏等

此外，腾讯云已将 TStack 平台以及运营服务经验推广到中国政企市场，截至目前，腾讯已与全国 15 多个省、50 多个城市签署合作协议，涉及智慧公安领域、智慧交通领域、智慧人社等诸多领域。

2. Easystack 动态

本月暂无重要动态。

3. 99CLOUD（九州云）动态

3.1 九州云亮相 2018 中国 SDN/NFV 大会，发力边缘计算产业

4 月 17-18 日，由 SDN/NFV 产业联盟主办的“2018 中国 SDN/NFV 大会”在北京召开。国内三大电信运营商、英特尔、华为、九州云、中兴通讯、新华三、腾讯、百度等 20 余家企业的技术专家以及国外诸多联盟基金会代表均出席本次会议。会上，九州云携 CORD 解决方案首次亮相，全力布道边缘计算产业。

3.2 “2017 年度中国 SDN、NFV 优秀案例”诞生，九州云金融案例入选

4 月 17 日，为了更好地推动中国 SDN/NFV 产业的商业化落地，在业界分享成功的商用部署案例，在由 SDN/NFV 产业联盟指导，IT168 和 C114 联合主办的“2017 年度中国 SDN、NFV 优秀案例评选”活动中，九州云凭借“基于 SDN 下一代金融云网络联合研究与应用实践”案例从 45 家案例中脱颖而出，被评为“2017 年度中国 SDN、NFV 优秀案例”。

九州云也成为此次获得该奖项厂商中唯一一家开源领域专业综合云服务厂商。该奖项既是对九州云在 SDN/NFV 领域持续创新成果的肯定，同时也为推动开源技术 OpenInfra 在垂直行业集成落地提供了借鉴。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰牵头组织并实施的 2016 年北京市科委科技计划及课题顺利通过验收

近日，由北京启明星辰信息安全技术有限公司牵头组织并实施的 2016 年北京市科委科技计划——网络威胁情报安全分析与协同系统研发项目（D16110100330000）及课题网络威胁情报安全分析系统（D161100003316001）均顺利通过了北京市科委组织的验收会，得到了科委技术专家组的高度认可，项目和课题信用评定结果均为 A。

项目成果“网络威胁情报安全分析系统”是基于大数据和人工智能的下一代安全分析平台，填补了国内此领域空白。平台实现了海量存储（每天安全大数据采集量 10TB 级以上）、安全数据资源统一管理、基于机器学习建模分析、实时流分析、交互分析的组件式集成等技术创新，而基于互联网开源工具的整合更是具有借鉴意义和探索价值。

该平台适用于网络安全运行中心，可作为目前安全事件监控系统的升级版。通过扩展数据采集范围，还可用于企业移动应用监控、工业控制系统监控、物联网系统监控等领域，也适用于网络威胁态势感知项目、智慧城市网络安全监控项目等，行业范围包括不限于能源、银行、交通、政府、电信、医疗等客户,具有明显的社会价值、经济价值以及推广应用价值。

1.2 启明星辰联合申报的“交通运输网络安全技术行业研发中心”正式启动

为贯彻全国交通运输科技创新暨信息化工作会议精神，实施《交通运输科技“十三五”发展规划》，推进交通运输科技创新体系建设，由交通运输部公路科学研究院推荐的北京中交国通智能交通系统技术有限公司联合启明星辰等单位共同申报的“交通运输网络安全技术行业研发中心”正式启动。

此次交通运输网络安全技术行业研发中心的正式启动，其主要研发方向之一就是落实国家关于提升网络安全的政策和技术要求，有效运用现代信息技术发展的新方式、新手段，推进技术成果和产品的有效转化，提升交通运输网络安全技术防范能力和保障水平。

作为联合申报方，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、云安全七大类产品，近 40 种产品解决方案，此次双方将在交通运输网络安全态势感知与监测预警、交通运输网络信任体系、交通运输关键信息基础设施防

护、交通运输网络安全前沿技术研究等方面进行合作，引入交通行业安全运营中心、工控安全防护、车联网安全防护新理念，形成一个交通行业内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，拓展交通行业的安全蓝海。

1.3 启明星辰电子签章系统正式发布

电子签章是实体印章的网络化和电子化，是企业互联网化、企业印章管理和企业信息系统安全的一个重要环节。2017 年，国务院办公厅发布《“互联网+政务服务”技术体系建设指南》，重点着眼于统一用户认证、电子证照、电子文书、电子印章等关键支撑技术。电子签章技术已经成为互联网+政务服务体系建设的刚需。

互联网+的快速发展，也使得网络安全威胁愈加严峻，电子签章在使用过程中不可避免存在文档被修改无法追踪、签章被仿冒等弊端。因此，一款既能解决使用需求，又能提供全方位安全防护的电子签章产品显然已经成为用户迫切需求。为此，启明星辰集团推出信息安全领域首款电子签章产品——启明星辰电子签章系统。

启明星辰电子签章系统将为用户建立有效的安全策略、管理规范和业务流程，形成综合的、全方位的解决方案。立足于政府、金融、人社、交通、税务、医疗、教育、公检法等众多行业，为客户提供安全、便捷的电子签章整体解决方案，为相关电子政务、电子税务局、电子病历、电子非税、电子证照、电子合同、电子凭证等多个维度提供法律保障和安全保障。

2. 山石网科

暂无更新。

3. 亚信安全

3.1 亚信安全产研院与眉山市公安局签署战略合作协议，共建网络空间平安示范城市

今日，中国网络安全产业领跑者亚信安全与四川省眉山市公安局联合宣布，双方将依托亚信网络安全产业技术研究院，共建网络空间平安示范城市，并将在信息化与网络安全技术研究、网络安全检查和安保等领域开展长期的、全方位的合作与交流，实现警企合作、资源共享、互惠共赢。

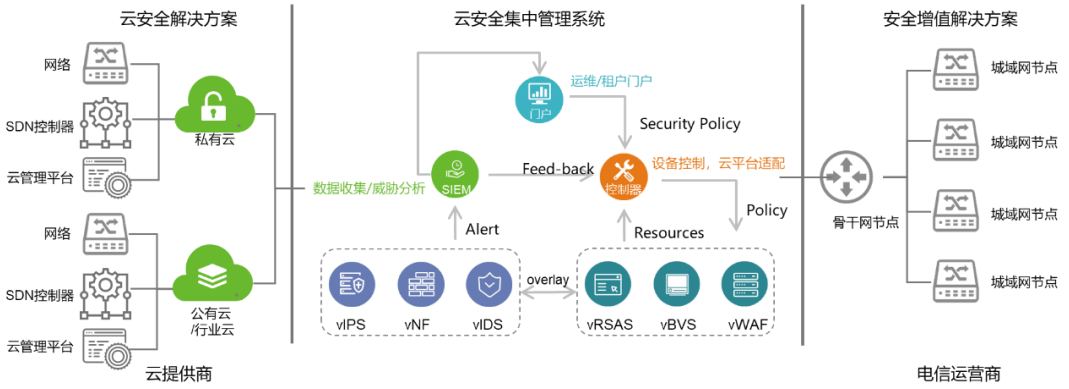
智慧城市的建设是一项巨大的工程，牵涉众多信息化子系统的建设，其中任何一个环节出现问题都可能影响城市的整体安全防护，造成经济损失、社会秩序混乱乃至威胁国家安全。在此背景下，整合各方力量，打造主动式、立体式的网络安全联动防护体系，创建网络空间平安城市，就成为保护智慧城市发展成果的必然要求。

在本次合作中，亚信安全与四川省眉山市公安局将共同建设网络空间平安示范城市，实现“事前监控预警、事中防御处置、事后溯源取证”的城市网络安全一体化全流程管理，促进全天候全方位感知网络安全态势思想的实践。同时，双方共同开展信息化和网络安全研究，在网络安全执法和保卫领域开展合作，提升整体的安全防护能力水平。

4. 绿盟科技

4.1 绿盟科技发布新一代云计算安全解决方案

通过云安全集中管理系统和安全资源池，该解决方案不仅可以帮助客户解决云计算环境下的安全风险，也可以帮助电信运营商构建安全增值服务，拓展 IDC 业务。



提供丰富的安全服务

该方案将绿盟科技传统优异的、丰富的安全产品转化为安全服务，让客户像使用其它云

计算服务一样使用安全服务，可以帮助客户很好的解决业务系统的安全风险。

支持安全服务编排

该方案利用 SDN 技术，自动化的完成客户所使用安全服务的引流和编排，并且客户可以根据业务变化，快速的调整安全服务，及时响应业务变化。

适配多种云计算环境

该方案提供的安全能力可适配 VMware ESXi、KVM 等多种虚拟化软件，以及 OpenStack、HUAWEI Fusionsphere 等云管理平台，让客户在虚拟化、私有云和行业云等环境中，保持安全的连续性。

兼容第三方安全产品

通过 API 接口，该方案可以与第三方安全产品对接，实现统一的服务提供和集中管理，可以为客户提供更多，更优质的安全服务，充分保护已有投资。

4.2 绿盟科技联合前海财险推出网络安全险

伴随金融科技的迅猛发展，金融科技为金融行业插上了腾飞的翅膀，随之也出现了各种各样的网络安全威胁。金融机构在部署各种安全设备、实施各项安全工作后，可以将网络安全风险降低到很低的水平，但网络安全的本质是人与人之间的抗争，是攻与防的对抗，残余风险始终存在。

在经典的信息安全风险模型里，对风险的处置共有四种手段，消除、降低、转移和接受。国内企业应对信息安全风险经历了不同的阶段：最初，企业总是希望将风险消除，后来逐渐接受与风险长期共存的状态，基于风险偏好和成本考量制定合理的风险降低目标，并接受残余风险。但转移，作为风险处置手段始终在网络安全领域没有得到应用。

而在其他传统安全领域，财产险已经是普遍采用的一种风险转移手段。通过购买保险，企业可以将火灾等带来的财务风险转移给保险公司。网络风险无异于企业面临的其他风险种类，国外也在通过网络责任险（Cyber Liability Insurance）来对抗网络风险以及相关的经济损失。现在美国网络安全保险市场保费超过全球总量的 90%。

基于以上的背景，绿盟科技联合前海财险于 4 月 10 日联合发布了这款“网络安全综合保险”产品。

与其他过往网络安全险不同的是，这款保险产品保障内容涵盖大多数当前网络安全风险点。具体包含以下 7 项保障内容：

1. 事故鉴定服务费用

企业聘请专业机构进行事故鉴定需要支付的服务费用。

2. 数据恢复费用

企业为恢复、重建或重新收集电子数据，需要支付的费用。

如：服务器数据恢复、硬件或软件数据恢复费用等。

3. 计算机勒索赎金

由于遭受安全威胁而支付的勒索赎金。

如：黑客攻击并窃取了网站信息，向网站提出赎金要求。

4. 数据泄密责任

因个人信息或公司信息发生泄漏，受害者向泄露信息的企业提出的赔偿要求。

如：酒店泄露客户信息数据，受害者向酒店及数据商提出的索赔。

5. 外包商导致的数据泄密责任

因外包商原因导致信息泄漏，受害方向企业提出的赔偿要求。

如：企业使用外包商维护系统，由于外包商自身的管理原因造成信息泄露。

6. 数据安全责任

企业因疏忽或过失，致第三方财产损失而需要支付的赔偿金。

如：企业被植入恶意代码、窃取口令或硬件被盗而造成其服务的客户遭受损失。

7. 法律服务费用

企业发生数据安全事故而被提起仲裁或者诉讼而产生的仲裁费、诉讼费、律师费等。

4.3 绿盟科技携三大工控解决方案亮相石油石化企业信息技术交流大会

4 月 18-19 日，2018 中国石油石化企业信息技术交流大会暨展示会在京举办，绿盟科技连续三届受邀出席。作为信息安全领域的领航者，本次大会绿盟科技携三大解决方案亮相展会，并承办“网络安全分论坛”，两位安全专家发表专题演讲，与石油石化行业参会嘉宾们共同分享绿盟科技在安全规划与建设实践中的成功经验。

绿盟科技安全专家发表题为《工业大互联下的安全思考》的主题演讲，专家表示，进入工业 4.0 时代，能源行业正逐步进行工业数据化和智能化的转型。正应用 CPS 技术将信息领域的信息化、智能化应用于传统行业，使广泛互联智能化成为现实，智能制造与按需制造成为可能。

专家指出，在传统单点的技术积累转化为私有的协议与工艺的过程中，数据缺乏有效利用，导致大量的沉默数据出现，行业的发展受制于历史沉默数据，发展速度相对缓慢。因此

需要增加数据处理和分析的能力。而工业互联网的发展，将使得大量的历史沉默数据变成有效数据。工业云、工业大数据与智能化装备的结合是工业化智能的显著特点。同时工业互联网安全也面临着新的挑战。

5. 360 企业安全

5.1 360 携核心科技亮相 2018RSA 大会

会上，360 公司集中展示了基于大数据、人工智能、云计算技术的全网威胁实时监控系统，三大杀毒引擎，以及多款国民级安全产品，这些技术和研究成果，代表了当前国内应对网络威胁的最高技术水平。

360 公司认为，如今的网络空间发展呈现出三种新趋势，一是网络攻击造成的损失越来越不可承受，二是各种漏洞成为像石油、稀土一样的国家战略资源，三是网络战争已经引发了全球规模的网络军备竞赛。

在此次 RSA 大会上，360 公司首次集中展示了其“看家法宝”级的威胁情报应对实力，主要包括 DDoSMon、ScanMon 和 DNSMon 三个部分。

其中，DNSMon2018 年新推出的威胁情报处理系统，它可以实时分析海量 DNS 流量，并对流量中的各种异常和关联关系进行分析，从而发现网络上存在哪些恶意代码行为。

ScanMon 可以第一时间感知网络扫描行为，并方便有效地识别对应的攻击者，从而达到追踪溯源的目的。此前，360 网络安全研究院在针对 mirai 僵尸网络出现、发展、新变种的持续跟踪中，就大量借助了 ScanMon 的能力。

DDoSMon 可以实时感知大量的 DDoS 攻击行为和受害者以及对应发起 DDoS 攻击的僵尸网络。目前，已有多个互联网大公司使用了 DDoSMon 监控自身网络遭受攻击的情况。

此外，360 自主研发的世界首个采用人工智能/机器学习技术的反病毒 QVM 引擎；专注于识别脚本、文档等非 PE 文件的 QEX 引擎；有效应对变形木马并全面修复感染型病毒的 AVE 引擎三大引擎，以及专注 APT（高级持续威胁）事件追踪的波塞冬系统等解决方案也在本届 RSA 上集中展示。

5.2 建行 360 企业安全集团携手中科睿光共筑云安全

近日，360 企业安全与中科睿光达成战略合作，双方宣布将在云计算及虚拟化领域展开全面的技术结盟，利用双方优势技术及资源，携手打造面向中国用户的安全高效的云计算环境。

中科睿光副总裁马莉表示，“中科睿光作为国内一流的云计算产品及服务提供商，拥有强大的技术实力和服务能力，在中国城市云、政府、教育、科研、医疗等行业市场拥有领先地位，中科睿光与在安全领域拥有雄厚实力的 360 企业安全集团合作，无疑将会为用户提供更加完善的安全解决方案，助力用户实现业务加速转型。”

360 云安全事业部总经理刘浩介绍，360 云安全解决方案专注于为用户解决云环境下的各类安全问题，凭借 360 自身强大的大数据分析及攻防能力，结合本地安全防护及云端防护，形成全方位立体化防御体系，为用户的云上安全保驾护航。

此次合作意义不凡，双方都本着构建高安全性和可靠性的云基础架构的目的，通过全面保障客户的安全需求，充分发挥软件定义数据中心架构的价值，为客户提供自主、领先的创新型云计算产品与解决方案。

6. 安恒

6.1 安恒信息亮相 RSA2018：玄武盾功能全新升级 创新首发

安恒信息以“云与大数据”为主题，展示了一系列最新的安全研究与技术成果。其中，WEB 安全一站式 SaaS 服务——玄武盾功能也全新升级，并在本次大会中创新首发。

该版本玄武盾，将全面提升云端 WEB 监测防御服务能力，最大的亮点在于提升了防御性能、引入大数据建模与威胁情报提高分析效率与准确度，并为用户提供更清晰的攻击分析结果。

除玄武盾以外，此次大会上，安恒信息也以“云与大数据”为主题，展示安恒的天池云安全平台、风暴中心 SaaS 服务、AiLPHA 大数据分析平台、ICS 安全解决方案等，为大家带来一系列最新的安全研究与技术成果。

6.2 安恒发布资产安全及漏洞管理解决方案

安恒资产安全及漏洞管理解决方案（DBAPPSecurity Asset security and Vulnerability Management Solution ,简称 DBAPPSecurity AVM）提供资产安全和漏洞管理的全生命周期管控，通过量化和闭环的处置，促进资产安全和漏洞管理的持续监控和优化。同时，结合安恒卓越的漏洞挖掘能力及威胁情报库，为企业资产安全提供及时的预警和响应建议，降低资产风险，提高漏洞修复能力。

基于全生命周期的安全资产监控，通过多扫描器扫描发现隐匿资产，同时监控资产的上线、变更、转移、报废信息，通过多扫描器扫描，逐步构建安全资产指纹信息。同时，结合安恒自身卓越的漏洞挖掘能力以及对接国家信息安全漏洞库，结合威胁情报，为企业资产风险提供及时预警及漏洞修复建议和方案。

基于多扫描器引擎统一调度及交叉漏洞验证，提高漏洞发现的准确率。可统一调度企业采购的各厂家的扫描器，实现扫描任务的创建、下发、任务状态监控、任务启停、报告取回、报告归一化等一系列集中管理功能。同时，通过对报告的归一化，将各类扫描器的扫描报告进行统一标准，统一规格的呈现，节省使用成本。

基于企业内部管理流程，实现漏洞闭环管理、持续分析和预控安全风险。整体流程可轻松和企业 CMDB、工单等内部配置管理和流程对接，实现资产风险和漏洞修复的闭环管理

7. 安天

暂无信息

8. Fortinet

8.1 Arista Networks 加入 Fortinet Fabric-Ready 合作伙伴计划，推动跨数据中心和云网络的安全自动化

将 Fortinet Security Fabric 与 Arista 的 EOS（一种网络操作系统）相集成，提供了一种联合解决方案，实现了更好的安全管理和横向扩展架构的自动化，最大程度地映射到网络流

量要求。

Arista EOS 运行在 Arista 交换机上，并与 Fortinet FortiGate 企业防火墙的高级安全功能集成在一起，动态卸载并提供对 FortiGate 网络转发的无缝控制。此集成允许在网络中应用动态安全策略，使数据中心能够以更高的规模和性能满足其安全需求。

此外，Arista Networks 的 CloudVision MSS 将与 FortiManager 集成，实现数据中心高级安全服务插入的自动化。无论服务设备或工作负载是物理还是虚拟，MSS 都提供灵活的软件驱动的网络服务，以将 FortiGate 和其他安全组件插入流量路径。通过合作，Arista 和 Fortinet 将 Fortinet 安全架构扩展到混合数据中心，以实现一致的安全策略编排和实施，并结合高性能的可扩展性，以保护当今最具弹性和动态的环境。

9. Checkpoint

9.1 CloudPassage 和 Check Point 发布整合版

CloudPassage 和 Check Point 的整合在 RSA 展台（N 3635）上展出。这种集成可实现与云的灵活性和动态性相结合的云安全性。

用于保护物理网络的相同原则 - 例如最小特权原则和深度防御原则 - 也适用于保护云。但云与物理网络有着非常重要的区别：云远远更加自动化，因此云安全解决方案需要发展并“表现得更像”他们所保护的本地云服务。

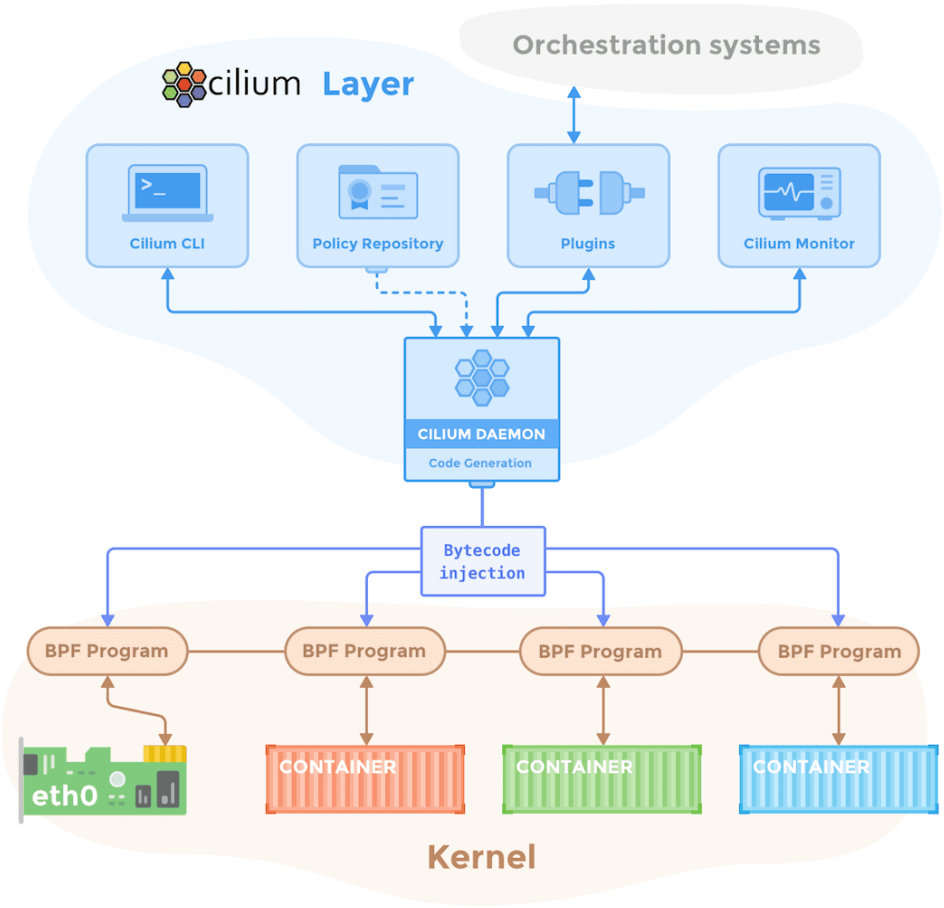
共享责任模式应该如何包含第三方安全解决方案。最值得注意的是，利用开放 API 进行增强集成的解决方案支持各种云环境，并提供有关威胁，用户，配置等的相关背景。

CloudPassage 一直是高性能应用程序开发和部署环境中云安全自动化和合规性监控的领先创新者。他们的旗舰安全自动化平台 CloudPassage Halo 可以在云端，服务器和容器上快速和规模地自动化工作负载安全性和合规性，从开发到部署。Halo 利用广泛的安全控制来保护各种类型的服务器和工作负载，包括虚拟机和容器以及公共和混合云（AWS，Azure，Google Compute Engine 等）。

同样，Check Point CloudGuard IaaS 为公共和混合云环境带来了全面的威胁预防安全，访问，身份认证，强认证，合规性报告和多云连接。CloudGuard IaaS 与领先的云平台和编排工具无缝集成，使其能够在几分钟内部署，同时支持动态安全策略和弹性可伸缩性。这些强大的功能使客户能够弹性扩展其云安全性，同时保持与动态环境不断变化的容量保持一致。

四、 容器技术及安全动态

1. Cilium 1.0：将 BPF 革新引入 Kubernetes 网络和安全系统



高效 BPF 数据通道：BPF 通过提供高性能内核沙箱可编程性，在数据通道层处理繁重工作，在 Linux 底层提供的超强动力。

全分布：所有数据通道元素在集群内都是全分布的，在每个集群节点上都运行在操作系统最有效的层级上。

Service Mesh 数据通道：BPF 允许用户为快速增长的 Service Mesh 空间建立合理的数据平面。Cilium 1.0 已经提供了例如 Envoy 的透明内部代理。未来 Cilium 版本会提供 Sidecar 代理加速。我们已经发布了一些早期 Sidecar 代理的基准指标。

CNI 和 CMM 插件：CNI 和 CMM 插件可以整合 Kubernetes、Mesos 和 Docker，提供网络，负载均衡和容器安全功能。

数据包和 API 层面的网络安全：Cilium 整合了基于数据包的网络安全以及透明 API 认

证，为传统部署和微服务架构的安全性。

基于身份：Cilium 将负载和身份信息在每个包内都打包在一起（而不是依靠源 IP 地址），提供高可扩展安全性。这一设计使得身份可以被嵌入任何基于 IP 的协议，而且与未来的 SPIFFEE 或者 Kubernetes 的 Container Identity Working Group 兼容。

基于 IP/CIDR：如果基于身份的方式不适用，那么可以采用基于 IP/CIDR 安全方式控制安全访问。Cilium 建议在安全策略中尽量采用抽象方式，避免写入具体 IP 地址。其中一个实例就是定义基于 Kubernetes 服务名的策略。

API 自感知安全机制：HTTP/REST、gRPC 和 Kafka 广泛使用暴露出基于 IP 和端口的服务，其安全机制明显不足。内置自感知 API 和数据存储相关协议在相关粒度上允许强制使用最小特权级别安全。

分布式可扩展负载均衡：高性能 3-4 层负载均衡器在服务连接间使用 BPF，具有流哈希和加权 round-robin 功能。基于哈希实现的 BPF 提供 O(1)复杂度的性能，也就是性能随着服务数量增加性能并不下降。

简化网络模型：将安全从地址层解耦出来极大简化了网络模型：一个三层网络空间为所有服务端点提供链接，在其上分段，用策略层实现安全控制。这一简化对扩展和排错很有帮助。网络可以用两种方式配置：

Overlay/VXLAN：此方法是在 IP 协议上负载身份信息的最简单整合方法。VXLAN 使用硬件帮助实现最佳性能。

直接路由：直接路由将路由功能授权给已有网络模块，例如内置 Linux 路由层，IPVLAN 或者云路由提供者。

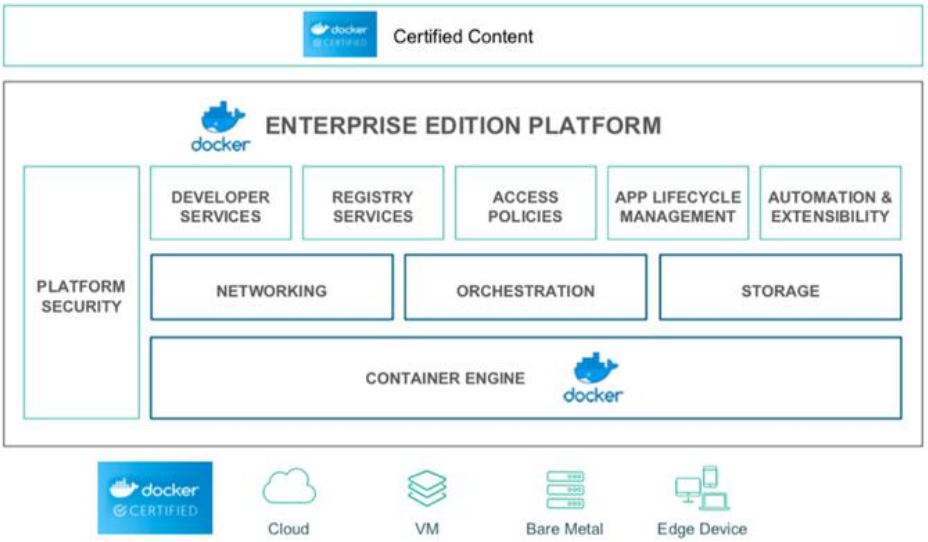
可视化/监测：跟策略类似，可视化也在网络包和 API 调用两个层面实现。所有可视化信息，不仅仅是 IP 地址和端口号，还包括丰富的工作流元数据，例如 container/pod 标签和服务名。

显微镜：显微镜为集群层面提供基于标签，安全身份和事件类型的过滤，提供安全和转发事件的可视化。

基于 BPF 高性能监控：高性能 BPF 性能循环缓冲区（perf ring buffer）的设置，就是为了追踪每秒百万级的应用事件，提供整合 BPF 可编程性的高效通道，允许数据可视化同时增加最小额外负载。

2. Docker 企业版 2.0 发布，着力提升 Kubernetes 支持能力与安全性

Docker 公司于 4 月 17 日正式发布了 Docker EE 2.0 的相关消息，其中增加了 Docker 社区版（简称 Docker CE）版开发中的新功能，并对企业级功能作出进一步增强。而通过 Docker EE 2.0，Docker 将为 Kubernetes 提供新的安全配置选项。



Docker EE 2 还将为 Docker 自家的 Swarm 容器编排系统提供支持。Swarm 当中最为核心的安全功能之一在于相互认证 TLS（传输层安全）概念的引入，其负责为不同容器节点提供密码保护下的数据传输机制。Docker 公司现在已经将同样的相互认证 TLS 安全功能引入 Kubernetes 集成方案。

五、 安全新产品及技术

1. PDF 文件可以被滥用来窃取 Windows 凭据

安全研究员阿萨夫•巴哈拉夫(Assaf Baharav)发布报告称 PDF 文件可被恶意攻击者利用，在无需用户交互的情况下，只需打开文件就能窃取 Windows 凭证（NTLM 哈希）。PDF 的规范特征可以为 GoToE 和 GoToR 远程加载内容。如果用户打开攻击者特制的 PDF 文档，就会自动向远程恶意 SMB 服务器发送请求。由于所有的 SMB 请求都会 包含 NTLM 哈希用于认证，因此远程 SMB 服务器的日志中会记录相关哈希值，使用工具即

可破解并获取密码。 专家表示，几乎所有 PDF 阅读器都可能受到这种攻击。FoxIT 尚未对此作出回应，而 Adobe 则表示不计划修复调整。微软则发布了 ADV170014 修复建议，指导用户关闭 Windows 操作系统中的 NTLM SSO 认证。

2. MongoDB 服务器漏洞泄漏加密货币用户信息

安全研究人员偶然发现了一个 MongoDB 数据库，其中包含超过 25,000 名投资或接收 Bezop（加密货币）的用户的个人信息。据网络安全公司 Kromtech 称，该数据库包含全名、家庭住址、电子邮件地址、加密密码、钱包信息以及扫描的护照、驾驶执照或身份证等信息。数据库存储了与 Bezop 团队在年初开始运行的“ 赏金计划 ”有关的信息，在此期间，它将 Bezop 代币分发给在其社交媒体帐户上宣传货币的用户。

3. Ubuntu 18.04 正式版发布，针对安全性优化

Canonical 于伦敦时间 26 日正式发布了 Ubuntu 18.04 LTS 版，Canonical 的 CEO 称，Ubuntu 18.04 LTS 在云计算领域效率极高，特别适用于机器学习这样的存储密集型和计算密集型任务。据了解，此次 Ubuntu 18.04 LTS 的代号为 Bionic Beaver（仿生海狸），Canonical 将会支持此款操作系统到 2023 年 5 月。Ubuntu 18.04 LTS 采用 4.15 版本的 Linux 内核，支持一些全新的特性，如 AMD 安全内存加密，以及针对 SATA Link 电源管理的改进等。

4. SMT 项目现安全漏洞，火币 Pro 暂停所有币种充提币业务

4 月 25 日火币 Pro 发布公告称，SmartMesh(SMT)项目方反馈今日凌晨发现其交易存在异常问题，经初步排查，SMT 的以太坊智能合约存在漏洞。受此影响，火币 Pro 现决定暂停所有币种的充提币业务，待查明 SMT 异常问题后，再行恢复所有币种的充提币业务。有消息称，SMT 的此次漏洞与前几日 BEC 代币的漏洞相似，可以通过溢出攻击获取大量的代币，目前 SMT 已上线火币、okex 等多家交易所。

5. 微软为 Linux 子系统提供 Windows Defender 防火墙

微软最近发布了 Windows 10 Insider Preview Build 17650（RS5），在这一版本中，微软把 Fluent Design 更新应用到了新 Windows 10 中的 Windows Defender 安全中心应用程序

中。Windows Defender 防火墙现在还支持 Linux Windows 子系统（WSL）进程。用户可以为 WSL 进程添加防火墙规则，整个过程类似于添加任何常用 Windows 过程的规则。此外，还允许用户利用 WSL 的防火墙通知。当 Linux 工具尝试允许从 SSH 或 Web 访问端口时，Defender 的防火墙将授予你访问权限。

6. AlienVault 推出 OTX Endpoint Threat Hunter

威胁情报公司 AlienVault 宣布推出免费终端扫描服务 OTX Endpoint Threat Hunter，新产品让企业和安全专家识别其网络中的威胁。“OTX Endpoint Threat Hunter 是 Open Threat Exchange 中的免费威胁扫描服务，能让你使用 OTX 威胁情报检测关键端点上的恶意软件和其他威胁。你现在可以世界上最大的开放式威胁情报社区来评估您的终端，防止新攻击出现。并且全部免费。“AlienVault 公告提到。OTX Endpoint Threat Hunter 服务是 AlienVault 开放威胁情报交换（OTX）平台的一部分，截至目前，该平台已经为超过 1800 万用户提供了超过 1900 万条威胁情报。 新服务使用轻量级工具 AlienVault Agent，它可以部署在 Windows，Linux 和其他端点设备上。

7. 微软宣布推出新的 Windows 平台安全技术

微软宣布推出 Windows Defender System Guard runtime 认证，这是一个新的 Windows 平台安全技术，将应用到 Windows 所有版本。微软表示，为了缓解软件攻击，运行时证明利用基于虚拟化的安全性（VBS）中与硬件相关的安全技术，与 Credential Guard 相同。新的安全技术可以为杀毒软件厂商提供额外的帮助，并且可以检测到内核篡改，rootkit 和漏洞利用。此外，它还可用于防止游戏中的作弊行为，保护敏感交易（涉及银行等金融交易）以及有条件地提供访问权限（使用特定访问策略）。“软件和服务可以利用这种认证技术来确保系统不受篡改，保证关键进程正常运行。这种基于硬件的“健康检测”可用于识别出电脑有没有被黑，或者对关键云服务限制访问。Runtime 认证可以为各种高级安全应用程序搭建平台，“微软在公告中指出。

8. 安全性升级，主流 Web 浏览器将迎来全新标准

谷歌、微软和 Mozilla 的浏览器很快将为用户提供由 FIDO 联盟和万维网联盟构建的全新无密码认证标准，目前正处于最终审批阶段。W3C 已将新的认证标准 WebAuthn 推进到

候选推荐标准（CR）阶段，这是最终批准 Web 标准之前的最后一步。预计将为全球用户提供更强大的 Web 身份验证，它已经在 Windows，Mac，Linux，Chrome OS 和 Android 平台上实施。

9. 微软 office 365 中新增反勒索软件功能

微软正式宣布为 Office 365（基于商业订阅的办公工具套件）推出新的反勒索软件功能。这项新功能称为“文件恢复”，它是一项 OneDrive 功能，可以让用户把文件回滚到 30 天之前的状态。OneDrive 文件恢复功能可用于意外大量删除，文件损坏或任何其他灾难性事件，但微软将此功能作为保存在 OneDrive 文件夹内重要文件的反勒索软件保护系统。意外删除文件或感染勒索软件的不幸用户可以在 OneDrive Web 仪表板中找到新的“文件还原”选项。此外，微软还调整了 OneDrive 的内部机制，检测帐户的文件是否可能被勒索软件加密。在某些情况下，如果用户安装了 OneDrive 应用程序，公司将向用户手机发送通知。下面的通知 - 图片会在用户发现勒索软件感染后立即提醒用户，并让用户和公司在生产停止前恢复受影响的文件回到之前的状态。

六、 网络安全投融资、收购事件

1. 收购

1.1 Palo Alto Networks 完成对 SECDO 的收购

4 月 10 日，Palo Alto Networks 完成对 SECDO 的收购，收购价 1 亿美元。Palo Alto Networks 是美国一家网络安全公司，公司主要专注于防火墙的创建。而 Secdo 是一家网络安全初创企业，其安全平台能够实现检测过程自动化以及对可疑事件进行自动化调查，从而降低技能障碍，并让企业安全团队更加有效率。

1.2 Evolve IP 完成对 thevoicefactory 的收购

4 月 18 日，Evolve IP 完成对 thevoicefactory 的收购，收购价未公布。Evolve IP 是一家云服务提供商。他们提供的云服务包括，虚拟服务器、虚拟桌面、灾难恢复、IP 电话、统一通信、联络中心等。公司已经基于思科，EMC，VMware 和 Broadsoft 等公司的技术建立了地理多样分布、冗余的数据中心，以及连接各一线运营商创建了一个私有云。

thevoicefactory 则提供托管开放式 API、白标签选项和国际覆盖的统一云通信。

1.3 RSA 将收购行为分析公司 fortscale

RSA 宣布收购 Fortscale，Fortscale 是一家提供行为分析解决方案的公司。该交易的财务条款尚未披露。Fortscale 的技术旨在通过大数据分析和机器学习来预测识别威胁。它会自动识别与正常行为的偏差，并警告安全团队潜在风险，例如共享用户凭据，远程访问异常和滥用特权帐户。RSA 希望通过其 NetWitness 平台向客户提供新的用户和实体行为分析（UEBA）功能。自 2013 年公司成立以来，Fortscale 总共获得资金 2300 万美元，其中包括大约一年前的 700 万美元。RSA 还宣布推出 NetWitness 平台的新版本。版本 11.1 中不仅包含 UEBA Essentials，还包括可帮助组织管理终端的 Endpoint Insights，以及使用动态分析技术提供日志数据的可视化。

2. 投融资

2.1 Red Balloon Security 获得 2190 万美元的 A 轮融资

4 月 3 日，Red Balloon Security 从 Abstract Ventures 和其他 3 位投资者处获得 2190 万美元的 A 轮融资。Red Balloon Security 是一家设备安全技术公司，主要为消费电子、汽车、国土安全、军事等行业提供嵌入式设备系统安全解决方案。

2.2 Storage Made Easy 获得 3000 万美元的 A 轮融资

4 月 4 日，Storage Made Easy 从 Undisclosed Strategic Corporate Investor 处获得 3000 万美元的 A 轮融资。Storage Made Easy(“SME”)提供了一个专注于两个大型新兴市场的企业文件结构。第一个是包含治理和遵从性的云安全，第二个是大型和增长的对象存储私有云市场。SME 的产品解决方案提供了一个“毯子”，在公共云的前提下或者第三方软件供应商的云环境下，企业可以在将所有数据打包在一起。客户使用 SME 进行安全性、加密和控制，并提供数据统一平台。

2.3 BetterCloud 获得 6000 万美元的 E 轮融资

4 月 5 日，BetterCloud 从 Accel Partners 和其他 5 位投资者处获得 6000 万美元的 E 轮融资。BetterCloud 是第一个 SaaS 运营管理平台，使能 IT 进行 SaaS 应用程序定义、纠正和实施管理和安全策略。在 60 多个国家，超过 2500 个客户使用 BetterCloud 进行持续的事件监控，快速地补救威胁，并完全自动化政策执行。

2.4 ObserveIT 获得 1600 万美元的 B 轮融资

4 月 11 日，ObserveIT 从 Bain Capital Ventures 处获得 1600 万美元的 B 轮融资。ObserveIT 是唯一一家提供内部威胁监视和预防解决方案，授权安全团队检测内部威胁，简化调查过程，防止数据过滤，在所有主要垂直领域中有超过 1600 个全球客户。

2.5 OPĀQ Networks 获得 2250 万美元的 B 轮融资

4 月 13 日，OPĀQ Networks 从 Columbia Capital 和其他 2 位投资者处获得 2250 万美元的 B 轮融资。OPĀQ Networks 打破了传统的安全模式，其基于云的服务使组织能够简化、集中和保护他们的网络。OPĀQ Networks 集成了网络和安全的管理平台降低复杂性和成本，并且构建安全控制，同时建立一个真正敏捷的基础设施，允许组织更容易防御新兴威胁和立即适应业务和管理需求。

2.6 Onapsis Inc.获得 3100 万美元的 C 轮融资

4 月 13 日，Onapsis Inc.从 406 Ventures 处获得 3100 万美元的 C 轮融资。Onapsis 是云计算和基于 ERP 和业务关键应用程序的网络安全和遵从性解决方案的先驱。

2.7 Saviynt 获得 4000 万美元的 A 轮融资

4 月 18 日，Saviynt 从 Carrick Captital Partners 处获得 4000 万美元的 A 轮融资。Saviynt 是身份管理和云安全解决方案的创新公司，保障云中应用、数据和基础设施，企业和大数据的安全。Saviynt 的下一代 IGA 平台独特地将数据访问策略、访问控制和使用分析与高级角色和 SOD 管理、基于风险的访问请求和认证结合起来。