

国内外云计算+安全动态报告

2019 年第 6 期

启明星辰云计算安全事业部

目录

目录.....	ii
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 云动态.....	4
1.1 AWS Glue 现在提供 VPC 接口终端节点.....	4
1.2 Amazon EC2 宣布推出主机恢复功能.....	4
1.3 Amazon EBS 加密功能现已在中国部分区域推出.....	4
1.4 AWS Organizations 现在支持 AWS 账户的标记和取消标记操作.....	5
1.5 AWS ParallelCluster 现已支持 Elastic Fabric Adapter (EFA).....	5
2. VMWare 云动态.....	5
2.1 Faction 为 VMware Cloud 筹集了 1400 万美元.....	5
3. GOOGLE 云动态.....	6
3.1 谷歌云服务宕机，欧美部分地区无法使用 YouTube 等服务.....	6
4. 微软 Azure 云动态.....	6
4.1 微软 Azure 云服务被用于托管恶意软件.....	6
4.2 Azure SQL Database Managed Instance 正式登陆 Azure.....	6
5. 阿里云动态.....	7
5.1 联手阿里云玖富万卡实现征信维度和数据安全双升级.....	7
5.2 阿里云发布首款 LoRa 室内安防套装产品.....	7
5.3 阿里云实时计算获大数据流计算产品能力评测证书.....	7
5.4 国内首例云服务器案件二审判决 阿里云胜诉.....	7
6. 腾讯云动态.....	8
6.1 腾讯云加码出海市场 输出行业全球化解决方案.....	8
6.2 贝店与腾讯云达成战略合作 加速发展社交电商业务.....	8
6.3 腾讯云数据库再获国际权威机构认可.....	9
7. 华为云动态.....	9
7.1 云+AI+5G 时代，需要多元化云服务架构.....	9
7.2 构建安全可信云服务，华为云全球安全认证再升级.....	10
二、开源云动态.....	11
1. Openstack 动态.....	11
2. Easystack 动态.....	12
2.1 EasyStack 助力福州市第一医院“互联网+医疗”创新.....	12

2.2	EasyStack 助光大证券构建私有云平台	12
2.3	EasyStack 助邮储银行构建中国最大 OpenStack 金融生产云	13
2.4	EasyStack 助兴业数金构建首个 OpenStack 金融行业云	14
3.	99CLOUD（九州云）动态	14
三、	云安全厂商动态	15
1.	启明星辰	15
1.1	启明星辰应邀参加 2019 年中国工业信息安全大会	15
1.2	启明星辰集团《统一安全业务运维管控平台》入选“2019 全国政法智能化建设智慧法院十大创新案例”	16
1.3	华为终端致谢启明星辰 ADLab	17
2.	深信服	18
2.1	深信服桌面云提升至中国桌面云市场第二	18
3.	山石网科	19
3.1	优秀学生获得山石网科网络安全奖学金	19
4.	亚信	21
4.1	亚信科技发布 5G 战略及系列产品	21
5.	绿盟	22
5.1	绿盟科技方案再次入选工信部网络安全技术应用试点示范项目	22
6.	安恒	23
6.1	安恒 AiLPHA 入选 2019 年最具颠覆性创新潜力榜	23
7.	奇安信	24
8.	安天	24
四、	容器技术及安全动态	25
1.	Kubernetes 1.15 发布	25
2.	Docker 迎来 Windows Subsystem for Linux 2	26
3.	Kube-OVN 0.5.0 发布	26
五、	安全新产品及技术	27
1.	macOS Catalina 应用将需要通过认证	27
2.	iOS 13 与 macOS 10.15 不再支持 SHA-1 证书	28
3.	印象笔记扩展被曝严重漏洞	28
4.	国家网信办《个人信息出境安全评估办法（征求意见稿）》	29
5.	谷歌发布面向计算隐私的开源工具	29
六、	网络安全投融资、收购事件	29
1.	收购	29
1.1	Onapsis 完成对 Virtual Forge 的收购	29

2.	投融资	30
2.1	Liongard 获 450 万美元 A 轮融资	30
2.2	Orca Security 获 650 万美元种子轮融资	30
2.3	Expel 获 4000 万美元 C 轮融资	30

本期云安全动态内容摘要

云厂商方面，AWS 添加多项增强，包括 AWS Glue 提供 VPC 接口终端节点、Amazon EC2 宣布推出主机恢复功能等，同时 Amazon EBS 加密功能现已在由光环新网运营的 AWS 中国（北京）区域和由西云数据运营的 AWS 中国（宁夏）区域推出；AWS Organizations 现在支持 AWS 账户的标记和取消标记操作，AWS ParallelCluster 现已支持 Elastic Fabric Adapter (EFA)；Faction 为 AWS 服务上完全托管的 VMware Cloud 筹集了 1400 万美元，Faction 提供了一套针对具有多云和混合云部署的企业的工具，包括混合灾难恢复即服务(HDRaaS)，用于 AWS 上的 VMware Cloud 的数据备份和迁移解决方案；Cloud Control Volumes，适用于 AWS 上的私有云，公共云和 VMware Cloud 的跨云存储平台；谷歌云服务宕机，欧美部分地区无法使用 YouTube 等服务；微软 Azure 云服务被用于托管恶意软件，可控制多达 90 台电脑、微软宣布 Azure SQL Database Managed Instance(SQL Database 托管实例)服务已正式登陆 Microsoft Azure；玖富数科与阿里云达成全面战略合作，双方将共同打造国内首个自主研发的智能数字普惠科技赋能平台、阿里云发布首款 LoRa 室内安防套装产品、阿里云实时计算获数据中心联盟首批大数据流计算产品能力评测证书；腾讯云加码出海市场，输出行业全球化解决方案、贝店与腾讯云达成战略合作，加速发展社交电商业务、腾讯云数据库再获国际权威机构认可；构建安全可信云服务，华为云全球安全认证再升级。

开源云方面，EasyStack 助力福州市第一医院“互联网+医疗”创新，并在广大证券私有云、邮储银行金融生产云和兴业数金行业云上发力。

云安全厂商方面，启明星辰应邀参加 2019 年中国工业信息安全大会，启明星辰集团《统一安全业务运维管控平台》入选“2019 全国政法智能化建设智慧法院十大创新案例”，华为终端致谢启明星辰 ADLab；深信服桌面云提升至中国桌面云市场第二；山石网科东南大学网络空间安全学院优秀学生获得山石网科网络安全奖学金；亚信科技发布 5G 战略及系列产品；绿盟科技再次入选工信部网络安全技术应用试点示范项目；安恒 AiLPHA 入选 2019 年最具颠覆性创新潜力榜。

容器动态方面，Kubernetes 1.15 发布，可扩展性与持续性改进。微软方面刚刚推出的 Windows Subsystem for Linux 2 (WSL2)将 Linux 内核引入 Windows 系统,使 Docker Desktop 版本 2 秒启动。Kube-OVN 0.5.0 发布,支持 NetworkPolicy、用户自定义网卡和 MTU 等。

安全新技术方面，苹果公司提供多项安全性提升，macOS Catalina 应用将需要通过认证，iOS 13 与 macOS 10.15 不再支持 SHA-1 证书；国家网信办《个人信息出境安全评估办法（征求意见稿）》；谷歌发布面向计算隐私的开源工具；印象笔记扩展被曝严重漏洞。

网络安全投融资方面，分别发生 1 起收购和 3 起融资事件。Onapsis 完成对 Virtual Forge 的收购，Virtual Forge 是自动检测和修复 SAP 应用程序网络安全解决方案的服务提供商，Virtual Forge 的技术添加到 Onapsis 屡获殊荣的业务应用程序网络弹性平台上，为利用 SAP 和 Oracle 应用程序运营业务的企业组织提供无与伦比的网络安全、可见性、事件响应和管理等功能。融资方面，配置状态安全检测服务提供商 Liongard 获 450 万美元 A 轮融资；云安全可见性解决方案提供商 Orca Security 获 650 万美元种子轮融资；透明托管云安全服务提供商 Expel

获 4000 万美元 C 轮融资。

2019 年 6 月 28 日

云计算安全事业部

国内外云+安全动态报告

一、云厂商动态

1. AWS 云动态

1.1 AWS Glue 现在提供 VPC 接口终端节点

6月4日消息，AWS Glue 宣布提供 VPC 接口终端节点。

现在可以直接通过 Virtual Private Cloud (VPC) 中的接口终端节点（而非通过互联网连接）直接连接到 AWS Glue。使用 VPC 接口终端节点时，VPC 与 AWS Glue 之间的通信将完全在 AWS 网络中安全地进行。除 AWS GovCloud（美国东部）和 AWS GovCloud（美国）以外，推出 AWS Glue 的所有区域均可使用此功能。

1.2 Amazon EC2 宣布推出主机恢复功能

6月5日，Amazon EC2 宣布推出主机恢复功能。如果专用主机上发生意外硬件故障，Amazon EC2 的主机恢复功能将在新主机上自动重启实例。主机恢复减少了手动干预的需求，尽可能缩短了恢复时间，并降低了专用主机上实例运行的运营负担。此外，与 AWS License Manager 的内置集成可在恢复时自动跟踪和管理许可证。使用主机恢复不会产生额外的 EC2 费用。按标准专用主机费率收费。

1.3 Amazon EBS 加密功能现已在中国部分区域推出

6月6日，Amazon EBS 现已在由光环新网运营的 AWS 中国（北京）区域和由西云数据运营的 AWS 中国（宁夏）区域推出。Amazon EBS 加密功能为您提供块级存储的无缝数据加密支持，能够满足安全性与加密合规性要求，无需任何额外费用。

通过此功能，现在可以创建加密 EBS 卷，其中包含通过 AWS Key Management Service (KMS) 管理的密钥，并将其附加到受支持的实例类型。然后，对所有卷上的数据、磁盘 I/O 和从卷创建的快照进行加密。加密还发生在托管 EC2 实例的服务器上，当数据在 EC2 实例和 EBS 存储之间移动时提供数据加密。

要开始使用，只需在使用 AWS 管理控制台、API 或 CLI 创建新 EBS 卷时启用加密。Amazon EBS 加密功能适用于所有商用 AWS 区域中所有受支持的 EC2 实例。

1.4 AWS Organizations 现在支持 AWS 账户的标记和取消标记操作

6 月 6 日消息，可以将自定义属性或标记分配给使用 AWS Organizations 管理的 AWS 账户。借助将所有者名称、项目、业务组、成本中心、环境和其他值等标记直接附加到 AWS 账户的功能，组织中的人员可以更加轻松地获取有关特定 AWS 账户的信息，而无需参考单独的电子表格或其他带外方法来跟踪 AWS 账户。

AWS Organizations 有助于在 AWS 上增加和扩展工作负载时对您的环境进行集中管理。使用 AWS Organizations，可以根据业务需求自动创建账户，创建账户组，并应用针对这些组的管理策略。还可以通过对所有 AWS 账户设置同一种支付方式来简化账单。

1.5 AWS ParallelCluster 现已支持 Elastic Fabric Adapter (EFA)

6 月 11 日消息，使用 AWS ParallelCluster 设置高性能计算 (HPC) 集群的客户现已可以使用 Elastic Fabric Adapter (EFA)。AWS ParallelCluster 可轻松配置使用 EFA 运行应用程序时所需的所有设置，其中包括带有传入传出规则的安全性组、Open MPI 和 Libfabric 库。

EFA 是一种网络设备，可使用消息传递接口 (MPI) 提高高性能计算 (HPC) 应用程序的速度。EFA 让紧密耦合的 HPC 应用程序具备云的可扩展性、灵活性和弹性。使用 EFA 之后，紧密耦合的 HPC 应用程序可以获得比传统 TCP 通道更低、更一致的延迟和更高的吞吐量，因此能更好地进行扩展。

2. VMWare 云动态

2.1 Faction 为 VMware Cloud 筹集了 1400 万美元

6 月 14 日消息，位于科罗拉多州丹佛市的亚马逊网络服务(AWS)上的 VMware 云管理服务提供商 Faction 透露，它已经筹集了由戴尔科技资本领导的 1400 万美元股权和债务融资，参与现有投资者 River Cities Capital Funds, Sweetwater Capital, Meritage Funds, Charterhouse Strategic Partners 和 Orix Growth Capital。据 Crunchbase 称，紧随其后于 3 月份筹集了 1800 万美元的 B 系列筹款，并将创业总额提升至 4900 万美元，首席执行官兼创始人卢克诺里斯表示，这将用于扩大 Faction 的产品组合并扩大其全球业务。

Faction 提供了一套针对具有多云和混合云部署的企业的工具，包括混合灾难恢复即服务(HDRaaS)，用于 AWS 上的 VMware Cloud 的数据备份和迁移解决方案; Cloud Control Volumes，适用于 AWS 上的私有云，公共云和 VMware Cloud 的跨云存储平台; 和 Bloc，由 VMware 提供支持的托管云。

3. GOOGLE 云动态

3.1 谷歌云服务宕机，欧美部分地区无法使用 YouTube 等服务

6 月 10 日消息, 据 The Verge 报道, 美国时间周日, 欧美部分地区的 YouTube、Snapchat、Gmail、Nest、Discord 等大量网络服务陷入无法访问状态, 其根本原因似乎是谷歌云计算服务出现了问题。谷歌已在其云计算平台上发布了一份状态更新, 指出问题开始于美东时间周日下午 3 点 25 分。谷歌发言人表示, 预计不久就能恢复正常服务。

4. 微软 Azure 云动态

4.1 微软 Azure 云服务被用于托管恶意软件

6 月 3 日消息, AppRiver 安全公司发现, 从网络钓鱼模板到恶意软件以及命令和控制服务, Azure 云服务依然存在安全问题, 研究发现其根源问题存在于微软的 Azure 基础设施中。

自 5 月 10 日以来, Azure App Services 平台上托管的近 200 个网站被用于部署廉价的虚拟主机托管以此维持网络诈骗活动; 5 月 28 日, 一种新形式的钓鱼活动出现在网络中, 攻击者会将钓鱼内容伪装成 Office 365 警告邮件, 声称用户已触发中级威胁警报, 并使用虚假登陆界面将用户信息发送到指定网站。

安全研究人员 MalwareHunterTeam 和 JayTHL 最新发现表明, 上述事件并非独立的攻击行为, 在经过样本分析后, 恶意软件以及稍后上传的其他样本仍然存在于微软的 Azure 基础设施中。

4.2 Azure SQL Database Managed Instance 正式登陆 Azure

6 月 12 日消息, 微软 SQL Server 2008 在今年 7 月 8 日将终止服务, 微软将不再提供补丁包。而最新的微软 SQL Server 2019 预计今年 7 月份上市。面对日益增多的勒索病毒攻击, 企业是升级数据库, 还是将数据库迁移至云端增强数据保护, 微软都提供了解决方案。

作为微软智能云助力客户数据库迁移上云的重要举措, 微软方面今日宣布 Azure SQL Database Managed Instance(SQL Database 托管实例)服务已正式登陆由世纪互联运营的 Microsoft Azure。

据介绍, Azure SQL Database Managed Instance 这项 PaaS 服务以全托管的形式在云端提供了 SQL Server 的几乎全部功能, 能为企业提供将本地部署的 SQL Server 数据库以最低成本迁移上 Azure 云的捷径, 并且可以确保 100%的应用兼容性。

5. 阿里云动态

5.1 联手阿里云玖富万卡实现征信维度和数据安全双升级

6 月 11 日消息，玖富数科与阿里云达成全面战略合作，双方将共同打造国内首个自主研发的端到端、一体化、全流程的智能数字普惠科技赋能平台——“玖富云”，这不仅夯实了玖富数科 T.E 赋能战略的科技基础，也将进一步推动旗下产品功能和服务的全面升级。其中，玖富万卡作为玖富数科集团旗下一款以数字技术驱动、连接用户和场景、提供信用信息服务和管理的平台，将在“玖富云”平台的支持下，实现用户服务的再升级。

5.2 阿里云发布首款 LoRa 室内安防套装产品

6 月 11 日消息，阿里云联合深圳慧联无限科技有限公司发布了基于 Alibaba Cloud LinkWAN 物联网络管理平台的新产品——守护精灵安防套装，这是自阿里云今年提出 LoRa2.0 概念以来，所落地的首款针对于长尾市场的 LoRa 套装产品。该套装主要面向中小企业的防盗需求，可实现店铺防盗、办公场所安全、危险区域人员进出防控、家庭安防、独居人士安全预警等功能。

5.3 阿里云实时计算获大数据流计算产品能力评测证书

6 月 17 日消息，由中国信息通信研究院、中国通信标准化协会主办，大数据技术标准推进委员会承办的 2019 大数据产业峰会在北京国际会议中心隆重举办，阿里云实时计算凭借各项优异测评数据通过数据中心联盟大数据流计算分布式流处理平台基础能力测评，并在现场接受评测颁奖。

“大数据产品能力评测”是由数据中心联盟（DCA）发起的国内首个大数据领域的产品能力评测体系，被誉为大数据产品发展的风向标。本次大数据产品能力评测首次将流计算产品纳入评测体系，阿里云实时计算作为国内首批通过大数据产品能力评测的流计算产品，率先成为被数据中心联盟圈定的国内大数据基础平台第一梯队。

5.4 国内首例云服务器案件二审判决 阿里云胜诉

6 月 20 日消息，对于中国云服务器市场，是非同寻常的日子。国内首例云服务器知识产权侵权案件正式落锤！北京知识产权法院驳回一审原告的所有诉讼请求，阿里云公司不承担法律责任。

2015 年 10 月，《我叫 MT》的游戏所有者乐动卓越发现有游戏公司运营侵权游戏《我

叫 MToonline》。乐动卓越认为阿里云为其提供云服务，也涉嫌构成共同侵权，于是向北京市石景山法院提起诉讼。要求阿里云断开链接，停止为侵权游戏方提供服务器租赁服务，将存储在其服务器上的游戏数据库信息提供给乐动卓越公司。2017 年 6 月，法院一审判决阿里云构成侵权，而在二审则改判，认为阿里云不承担任何法律责任。

6. 腾讯云动态

6.1 腾讯云加码出海市场 输出行业全球化解决方案

6 月 3 日消息，在举办的腾讯全球数字生态大会上，腾讯首次公布了助力国内企业出海的 6 大核心能力和 12 大行业全球化解决方案。

腾讯云副总裁答治茜对此表示：“针对不断增长的市场需求，腾讯云正在战略加码出海市场，并基于自身在云计算领域积累的领先技术能力，为国内出海用户在技术、资源、产品等层面提供全面支持。同时，优先选择在国内有成熟服务经验的游戏、视频、电商、教育等行业重点突破，构建全球云服务差异化优势，持续输出各行各业的出海解决方案，助力国内企业开拓全球市场。”

根据数据统计，目前腾讯云已在全球开放 25 个地理区域，运营 53 个可用区。在可用区之外，腾讯云在全球 50 多个国家和地区，部署了超过 1300 个 CDN 加速节点。

腾讯云正在快速构筑起遍布全球的基础设施服务网。

6.2 贝店与腾讯云达成战略合作 加速发展社交电商业务

6 月 11 日消息，社交电商平台贝店与腾讯云在深圳签署战略合作协议，双方将进一步深化在云计算方面的合作。腾讯云的技术将支撑贝店快速增长的电商业务，助力其新业务发展。此外，贝店还将与腾讯广告、腾讯安全、微信支付等腾讯生态进一步合作，推动社交电商业务高速、可持续发展。腾讯公司副总裁、腾讯云总裁邱跃鹏和贝店总裁顾荣出席签约仪式。

2018 年年中，贝店希望通过“上云”改善计算的稳定性、拓展性等问题。经过多方评估，贝店选择了腾讯云。当年 9 月，双方签约，贝店逐步将服务器迁移至腾讯云。

根据战略合作协议，贝店和腾讯云将在计算与网络、存储与 CDN、云数据库、云安全、监控与管理、域名服务、移动与通信、视频服务、大数据和 AI 等产品和服务方面进行深度合作，加速发展社交电商业务。

6.3 腾讯云数据库再获国际权威机构认可

6 月 17 日消息，国际领先的行业研究与咨询机构 Forrester 正式对外发布全球最新的数据库评估报告《The Forrester Wave™: Database-As-A-Service, Q2 2019》，腾讯云数据库（TencentDB）凭借优异的产品性能以及敏捷、灵活的部署能力，首度成功入选 Forrester 数据库厂商“实力竞争者”领域。

Forrester 是一家被全球认可的可信赖的市场研究与咨询公司。此次，Forrester 通过对数据库厂商的产品矩阵、战略和市场表现三大维度的 27 项指标进行综合评估，最终筛选出市场上最值得关注的 12 家厂商，腾讯云凭借强劲的技术和服务优势进入此次 Forrester Wave™。

据 Forrester 报告显示，腾讯云在性能规模、配置和管理、数据安全、执行力、开源、售后支持、综合收入、客户数量、合作伙伴 9 项细分指标上获得优秀的评分。其中，在用户数量和合作伙伴指标上更是获得了评测范围内的满分。

Forrester 报告指出，腾讯云可以为用户提供可用的数据库即服务产品 DBaaS，支持各种流行的开源和商业数据库，包括 Microsoft SQL Server, MongoDB, MySQL, PostgreSQL 和 Redis。此外，腾讯云还支持 Tcaplus 数据库。除了游戏，腾讯的 DBaaS 还在各行各业得到广泛应用，包括电商、娱乐、零售，社交等等。

据介绍，此次腾讯云数据库获得 Forrester 的认可，一方面表明国产数据库的技术实力得到了国际权威机构的认可，另外一方面也显示，以腾讯云为代表的云厂商在数据库等基础软件领域的迅速崛起，特别是一些垂直领域都有针对性的突破，在一定程度上，也对中国数据库乃至基础软件领域未来的发展起到积极的推动作用。

7. 华为云动态

7.1 云+AI+5G 时代，需要多元化云服务架构

6 月 5 日消息，华为云全球市场总裁邓涛发表主题演讲，邓涛表示，如果将这场全行业的智能化升级比作一条新的赛道，那么云将成为起飞的跑道，而 AI、IoT、5G 将是决定企业发展速度和商业高度的重要引擎，5G 和 AI 将发挥越来越大的作用。

目前，全世界 90% 以上的智能手机、穿戴设备、智能电视、智能驾驶等都基于 ARM 架构，全球一共有千亿级基于 ARM 架构的芯片在运行，可以说 ARM 已经是全球最大的计算生态系统。基于 ARM 的数据中心能更好地满足移动设备的需要，其内核高密度低功耗的优势能更好地实现端云协同。

在算力方面，从“芯”开始，华为云为“云+AI+5G”时代提供高性价比、自主可控的最佳算力。去年 10 月，华为正式发布昇腾 910 和昇腾 310 两款自研 AI 芯片，提供充裕经济 AI 算力；去年 12 月，华为推出“业内性能最高”的基于鲲鹏架构的 7nm 服务器处理器——鲲鹏 920（Kunpeng 920），专为大数据处理以及分布式存储等应用而设计，鲲鹏的高并发低功耗适用于 5G 时代海量终端数据和并发应用场景。

华为云+AI，帮助企业实现智能化升级，由此带来生产力和效率的提升，帮助企业更好地提供智能创新服务，复制专业技能，增加用户粘性。截至 2019Q1，华为云 AI 可以提供从基础平台服务到通用 API、高级 API、预集成方案在内的 59 种服务、159 项功能，融合行业智慧，围绕海量重复、专家经验和多域协同三大场景持续推进 AI 落地。

7.2 构建安全可信云服务，华为云全球安全认证再升级

6 月 11 日消息，全球权威标准机构 BSI（英国标准协会）和 CSA（云安全联盟）宣布，华为云顺利通过 ISO 27001&27017&27018&CSA STAR 四个安全复审和认证。据了解，此次 4 个体系安全认证审核范围覆盖华为云所有机房和一百多项核心云服务，认证云服务数业界领先。华为云以其业界领先的安全保障体系顺利通过所有认证，其中，CSA STAR 的安全评级更是为最高级别 Gold 级。

四大体系安全认证，践行安全可信

ISO 27001 是目前国际上被广泛接受和应用的信息安全管理体系认证标准。该标准以风险管理为核心，通过定期评估风险和对应的控制措施来有效保证组织信息安全管理体的持续运行。此项认证华为云早前已认证通过，此次复审，无论是地域范围、机房数量还是云服务数都得到极大扩充，其顺利通过标志着华为云在信息安全管理体上已达到国际领先标准。

云服务相比普通的 IT 服务/系统有其特殊性，ISO 27017 是针对云计算信息安全的国际认证。ISO/IEC 27017 就是在 ISO/IEC 27002 标准的基础上，保留或者增加了云服务特有的安全实践指南，并提供了额外的控制措施来解决针对于云的信息安全威胁和风险。ISO 27017 的最新认证通过，表明华为云在信息安全管理能力达到了国际公认的最佳实践。

ISO 27018 是专注于云服务个人数据保护的国际行为准则。同 ISO 27001 一样，ISO 27018 也是对地域范围、机房和云服务数量的扩证复审，再次顺利通过表明华为云已拥有完备领先的个人数据保护管理系统。实际上，ISO 27018 是国际上第一个聚焦云计算的个人信息保护国际标准，该标准提供了一套用于公有云中个人信息处理者的个人信息保护实用规则。这些规则让云服务供应商的个人信息安全控制变得标准化和透明化，并能帮助客户选择安全和治

理更好的云服务商。

CSA STAR 认证是由标准研发机构 BSI（英国标准协会）和 CSA（云安全联盟）合作推出的国际范围内的针对云安全水平的权威认证，旨在应对与云安全相关的特定问题，协助云计算服务商展现其服务成熟度的解决方案。加之之前的积累，此次华为云全平台通过 CSA STAR 认证，华为云服务的透明度和客户信任得到进一步证明。

持续构建和提供安全、可靠、稳定的云服务平台

实际上，除了以上四体系安全认证，今年 5 月份，BSI 还宣布华为云新加坡大区获得新加坡 MTCS（多层云安全）最高安全评级的 Level3 等级认证。BSI 表示，华为云获得最高的 Level3 等级认证，意味着华为云在海外有技术强大的安全团队和规范的管理流程，能够为用户提供安全、可靠、稳定的云平台和云服务。

除了安全认证，华为云在构建安全服务上的努力也未松懈半分：为帮助用户防止外部恶意攻击，华为云围绕攻击者可能的攻击路径，发布了基于 AI 的安全解决方案，包括安全 AI 平台米兰达、DDoS 高防、数据库安全等共 20 多款服务产品，让用户像搭积木一样，选择一款或数款安全服务组建符合业务需要的安全体系，堵住攻击；为帮助用户防止内部数据泄露，围绕云上数据的全生命周期，华为云提供了从访问认证、敏感数据识别、防攻击、防泄漏到审计组成的环环相扣的基于 AI 的数据保护解决方案；同时，引入全球最优秀的安全厂商入驻华为云，为用户提供最好的安全服务。

此次华为云一举通过四项国际安全复审扩证及认证，既表明了华为云对国际权威云安全标准规范的遵循，更显示了华为云在云服务安全保障领域的领先实力。华为云将持续致力于为客户提供高度可信的业务运行环境，易获取、按需使用、弹性扩展的云安全服务，帮助客户保护云上的应用系统和重要数据。

二、 开源云动态

1. Openstack 动态

暂无消息。

2. Easystack 动态

2.1 EasyStack 助力福州市第一医院“互联网+医疗”创新

数据联通带来的业务运维挑战等都成为当前医联体信息化建设亟待解决的实际问题。福州第一医院选择主动拥抱下一代云计算创新技术，采用易捷行云 ECS Stack 云就绪超融合的创新解决方案，基于架构更稳定、性能更优的超融合基础设施支撑福州第一医院医联体 IT 建设。在实际项目建设中，助力福州第一医院医联体建设获得以下收益：

业务快速上线、极简部署：ECS Stack 云就绪超融合采用软硬件一体化交付，福州第一医院医联体相关业务项目部署上线，仅 3 天时间就完成了设备加电、平台软件部署和与生产网络连通部署生产应用。

资源弹性扩展、高可靠架构：ECS Stack 云就绪超融合采用创新的全对称分布式微服务架构设计，软硬件去中心化，无单点故障；通过细粒度隔离，多副本机制，集群 HA 功能，机柜级高可靠，故障自愈等功能保障业务连续性；利用超融合平台对多种虚拟资源弹性扩展能力，有效应对医联体不断扩展的复杂业务需求，并满足业务的弹性伸缩要求。

平滑无感升级：ECS Stack 云就绪超融合可实现微服务粒度的平滑无感升级，升级过程保障业务不中断。福州第一医院医联体相关业务平台项目上线以来已分别完成平台大小版本的在线更新操作，升级期间对平台上运行的业务没有造成影响。

智能运维：ECS Stack 云就绪超融合支持智能运维引擎，通过加速故障诊断与运维决策，对硬件、系统、服务、性能全面 360° 监控，可视化多维细粒度监控指标，自动化运维和深度分析，告警/自动巡检报告邮件通知等丰富的功能，有效地降低运维压力，让医院更加专注于业务系统功能扩展和服务优化。

2.2 EasyStack 助光大证券构建私有云平台

在业务层面，光大证券以金融科技为核心，以智能化、数据化运营为支撑，力求实现客户互联网服务深度化，持续推动“金融+科技”产生聚合效应，构建适应未来的金融业务服务体系。因此，光大证券决定首先通过构建完整的私有 IaaS、PaaS 云平台，在新业务的部署上对光大证券两地三中心做到跨域统一交付环境，统一部署与配置流程，集成自动化测试与发布，探索一条金融创新的敏捷之路。

在构建云平台的技术选择上，光大证券认为，证券行业对云平台的安全性、可靠性和稳定性要求极高。同时，为了提升市场竞争能力，公司的新业务必须大规模快速的推向市场，

并且在管理运维方面更加简单、成本更低。

而作为私有云事实标准的 OpenStack 开源技术，不仅能够帮助证券企业实现 IT 系统的敏捷、高效、易扩展以及自主可控的管理需求，同时符合证券企业在新业务方面所需的敏捷开发、快速部署、不断迭代、持续交付的开发模式。同时，开源云平台还可以帮助证券企业实现 IT 建设及维护成本的控制，提升资产利用率，缓解运维管理的压力。

最终，基于对云平台严格的测试与选型，以及看重易捷行云 EasyStack 在金融行业的诸多最佳应用实践，光大证券选择了 EasyStack ECS 易捷行云企业云，进行新业务开发、测试、上线的精细化管理，实践证券企业数字化转型之路。

经过双方共同努力，光大证券携手 ECS 易捷行云企业云构建了高效、安全、稳定、可靠的云基础设施，于 2018 年 6 月正式上线，实现了提供统一的资源与管理路径，自服务资源交付实现轻运维，对接云管平台，实现管控和业务融合。

2.3 EasyStack 助邮储银行构建中国最大 OpenStack 金融生产云

邮储银行采用 EasyStack 易捷行云提供的开源云平台解决方案，构建中国最大的基于 OpenStack 的金融生产云。

邮储银行金融互联网云平台的解决方案亮点如下：

1，国内最大规模基于 OpenStack 部署的金融云

中国邮政储蓄银行规划在三期项目中共部署近千个节点，这也是目前国内金融行业上开源云平台最大的节点规模。在解决方案中充分利用了 OpenStack 的松耦合特性，把可能会造成访问瓶颈的组件独立拆分出来部署在物理服务器上，保证了整体架构的扩展性的同时也保证了高性能的要求。

2，互联网金融业务与云平台深度结合

随着 OpenStack 技术的成熟，客户对于基于 OpenStack 云平台的接受程度已经不仅限于开发测试环境，中国邮政储蓄银行创新地把众多互联网金融业务部署在 OpenStack 生产云平台上，充分利用了云平台的特性，实现了业务快速创新、快速部署、快速上线。

3，灵活的组网方式满足三级等保要求

在解决方案中利用了 OpenStack 的灵活组网技术，通过物理隔离的方式把业务网与管理网隔开，满足了银行互联网业务的三级等保要求，符合银行的信息系统监管规定。

4，纳管集中式商业存储

在邮储银行的生产环境中使用了多家厂商的中高端存储，为了实现云平台的统一管理，

在解决方案中利用 OpenStack Cinder 组件通过集中式存储的 OpenStack 驱动程序，直接对多家厂商(包括 HP、HDS、华为等)的集中式存储实现管理和调度，利用块存储服务的统一接口，为云主机、云硬盘、镜像提供高性能的云存储环境。

2.4 EasyStack 助兴业数金构建首个 OpenStack 金融行业云

兴业数金采用 EasyStack 易捷行云提供的开源 OpenStack 云平台解决方案，构建国内第一个基于 OpenStack 的金融行业云。

兴业数金采用 EasyStack 易捷行云提供的基于开源 OpenStack 云平台解决方案，一期建设互联网金融业务生产云、开发测试云两个云平台，既结合了互联网金融业务的实际需求，又具备行业云的推广扩展能力。方案亮点包括：

1，灵活计费策略支撑金融行业云复杂计费场景

定制开发云平台计费功能，实现资源条目基准价格配置、计费策略配置、计费报表导出、在线或管理员后台充值及欠费处理等功能。这些复杂的计费体系、计费策略、计费管理等功能，为实现金融行业云复杂计费场景提供了业务和技术融合支撑。

2，复杂的组织关系架构契合金融行业云使用场景

考虑到金融行业云的企业用户组织关系架构复杂，兴业数金云在设计之初就在原有 OpenStack Domain、Project 组织架构基础上，增加一级父 Project，实现企业、部门、项目三层组织关系架构契合金融行业云企业用户自有组织架构需求。

3，裸机资源管理实现虚实资源混合使用

考虑到兴业数金云承载的互联网金融业务中需要使用物理节点构建大数据集群，采用 OpenStack Ironic 接入管理裸机资源，并按需提供给数金云租户裸机资源服务。此外，通过对接 SDN 网络方案，亦实现虚拟机和裸机混合组网。

4，统一监控平台

兴业数金云采用 Zabbix 对云平台中物理服务器、网络设备、分布式存储系统、应用系统和虚拟资源统一监控，统一监控平台实现提供监控告警管理功能：包括资源容量、主机性能、虚拟机性能、应用性能监控及告警阈值设置等功能。

3. 99CLOUD（九州云）动态

暂无消息。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰应邀参加 2019 年中国工业信息安全大会

6 月 21 日，由工业和信息化部指导，国家工业信息安全发展研究中心、工业信息安全产业发展联盟联合主办的 2019 年中国工业信息安全大会在北京国际会议中心隆重举行。本次大会是聚焦工业信息安全领域举办的国际性会议，旨在加快推广行业领域最新实践成果，搭建行业领域交流展示平台，促进我国工业信息安全产业全面发展。

大会邀请了工业和信息化部总经济师王新哲、工业和信息化部网络安全管理局副局长杨宇燕、中国工程院院士/工业信息安全产业发展联盟专家咨询委员会主任邬贺铨、中国科学院院士尹浩、国家电网公司大数据中心副主任陈春霖等领导发表演讲。作为信息安全行业领军企业，启明星辰集团应邀参加大会，多角度全面展示启明星辰集团工业信息安全探索、实践及研究成果，同与会人士共商工业信息安全未来发展。



启明星辰集团总裁严立受邀参会并做了《泛在电力物联网与安全中台》的主题演讲。严立讲到，5G+AI+IoT 等技术的深度融合，推动了万物互联迈向万物智能时代的来临，泛在

电力物联网这一具有巨大经济和社会效应的关键基础设施，是工业现代化的重要标志之一，受到了高度关注。以泛在电力物联网为代表的工业互联网实现了网络空间与物理空间的结合，关系着国计民生，一旦遭受网络攻击，其带来的灾难感将远远超过仅存在于网络空间中的危害体会。

随着云计算、大数据、人工智能等技术的产生及发展，企业的后台数据量急剧上升，前端的应用和业务灵活性开放性也急剧放大，启明星辰提出“安全中台”的理念，尝试利用安全中台将灵活、多样、开放的业务前端，与庞大数据能量赋能的后端进行衔接，保障数据安全及业务安全两大核心问题，为驾驭网络安全和工业信息化安全带来一些启示和帮助。

未来，文明的安全如何保障，严立提出了自己的一些思考。信息化、工业化发展到今天，网络安全已经和工业文明对接，一旦爆发网络战，将会对工业文明成果带来反噬，具有灾难性的后果。当今人类社会最大的文明是工业和科技文明，新一代工业革命正在进行，我们要给快速发展的人工智能、基因改造、量子计算……加个定语，那就是“负责任”。科技安全是整个人类命运共同体最大的文明保障，没有科技安全就没有文明的安全。

1.2 启明星辰集团《统一安全业务运维管控平台》入选“2019 全国政法智能化建设智慧法院十大创新案例”

6 月 10 日，由《法制日报》举办的“2019 全国政法智能化建设创新案例征集活动”结果揭晓，通过综合投票及专家评审，启明星辰集团联合河北省高级人民法院参评的《统一安全业务运维管控平台》入选智慧法院十大创新案例。该方案实现了法院信息化应用可管、可控、可审，有效提升司法效率、促进司法公正，为人民群众提供更加高效、便捷的司法服务，也对全国法院系统起到示范作用。

人民法院信息化安全关乎国家、司法、人民群众切身利益，保法院安全就是保国家利益、保司法公正、保人民权益。中国法院正在努力建设全面覆盖、移动互联、跨界融合、深度应用、透明便民、安全可控的人民法院信息化 3.0 版，全面促进信息化建设的同时，仍然存在安全短板：

- ▶帐号独立管理，无法进行有效生命周期管理：各应用系统独立进行帐号的管理，用户身份信息分散于各个系统，形成身份信息的孤岛，维护人员同时对多个系统进行维护，工作复杂度会成倍增加。

- ▶共用帐号、一人多帐号现象突出：由于大部分应用资源中的帐号无法对应到自然人，存在公用帐号和一人多帐号的情况，对员工在应用资源中的访问和操作行为审计及责任追溯

带来困难，并且无法统计访问特定应用资源的所有员工的相关信息，也无法统计特定员工对所有授权应用资源访问的相关信息。

▶各系统认证模块强度不一，改造成本高：各个应用资源独立进行登录认证，采用不同的认证技术和不同的认证强度，在企业范围内采用统一标准提高应用资源的认证安全级别，需要对每个应用资源分别进行改造，改造的成本较大。

▶各系统管理员权限过高：应用资源内的帐号管理、认证管理和授权管理都由管理员完成，管理员权限过于集中和强大，若管理员权限泄露并被用于违规操作，会造成较大影响。

因此，在开展好法院业务信息化 3.0 版的同时，应坚持信息化建设与网络安全并行，实现事件可追溯、责任可定责、使用可管控、维护可审计。

启明星辰集团助力河北法院推出统一安全业务运维管控平台，以用户身份生命周期管理为核心，围绕“人、案、物”等关键因素，多模型多维度实时分析用户业务行为，并基于科学分类、深度聚合、交叉剖析和关联分析业务访问行为模型，通过业务使用量、关键功能以及新业务的使用情况分析，实现多维度业务系统使用情况剖析，整体统筹实现：

- 1) 全局视角资产和用户展现，熟知“家底”情况。及时掌握用户及资源生命周期阶段；
- 2) 业务及运维行为分析展现，通过分析历史数据，了解业务使用及运维过程中的薄弱点和风险点；
- 3) 业务整体安全指数，通过技术手段实现对业务系统整体安全水平进行感知，告警业务面临的风险点；
- 4) 行为、人物的异常画像，清楚而明晰地看清每一个用户的属性信息、行为轨迹以及具体操作。

启明星辰集团联合河北法院自主创新统一安全业务运维管控平台，以规范司法行为、保障司法公正为目标，不断完善信息系统和管理机制，通过全程留痕、动态跟踪、风险预警、公开透明、监督建议等信息化手段，为广大干警提供“监督程序化、司法阳光化”的监督管理手段，为廉洁司法献计献策。目前，该平台已在河北法院全面应用，未来，可应用推广至全国司法领域，为促进阳光司法，推动司法公正贡献力量。

1.3 华为终端致谢启明星辰 ADLab

日前，华为 PSIRT 发布致谢公告，感谢启明星辰 ADLab 在参与华为终端 IoT 奖励“上新活动”计划所付出的努力。

此次活动是华为首次将 IoT 设备安全纳入到漏洞奖励计划中，多家安全实验室和高校参

与了此次终端 IoT 奖励计划上线活动，仅启明星辰 ADLab 提交的漏洞符合本次活动要求，发现并协助华为修复了 IoT 产品中的多个严重安全问题，为其终端 IoT 产品安全提供了有力的支持。

启明星辰 ADLab，致力于网络安全攻防技术研究，在移动终端安全、云安全、工控安全、物联网安全、基础操作系统等领域均有前瞻性技术研究成果。

自 2015 年起，启明星辰和华为开展安全方面的合作。2016 年，启明星辰入驻华为 Cloud DC Open 联合创新办公室，共同开发验证面向云安全的解决方案。2017 年，启明星辰加入华为安全商业联盟。2018 年，启明星辰成为华为首批终端安全奖励计划合作伙伴。

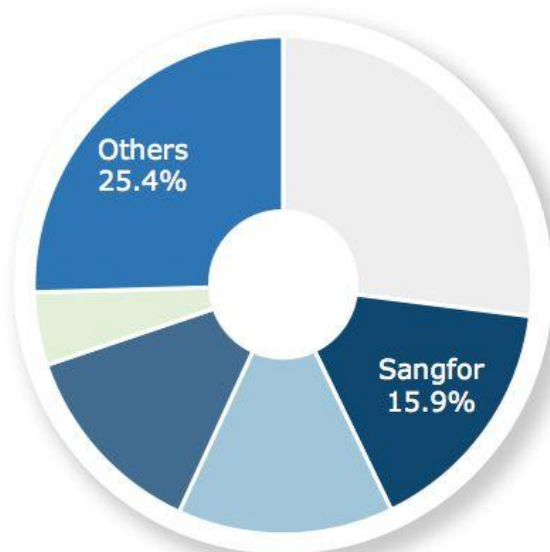
未来，启明星辰在网络安全领域将继续与华为合作，帮助华为提升和完善其产品和业务的安全性。

2. 深信服

2.1 深信服桌面云提升至中国桌面云市场第二

近日，IDC 发布了最新的 2018 年下半年 VCC（虚拟客户端）市场排名报告《PRC VCC Software Tracker, 2018 H2》。报告显示，2018 年，中国桌面云市场增速依旧强劲，深信服桌面云凭借优异的技术、方案与服务，以 15.9% 的占比强势斩获第二名，以全年 53.3% 的高增长率实现增速排名第一。

2018 年下半年中国 VCC（虚拟客户端）市场占有率



借助云计算技术的快速发展，桌面云不断获得市场认可。中国桌面云市场在高速增长的同时，逐渐迈入成熟期。深信服桌面云通过持续的技术创新、产品打磨，完善的方案构建，及优质的服务，实现 75 万+云桌面授权，已经成为全行业 6000+用户新一代云办公模式的一致选择。

持续的技术优化与研发创新，是深信服桌面云获得市场极大认可的根本。深信服桌面云以打造桌面优质使用体验、提升 IT 办公系统运维管理效率，及保障业务安全可靠等用户对终端建设的核心诉求为目标，通过前后端软硬件的深度融合，提供极致体验、更高效、更安全的桌面云，为用户构建可随时随地接入的无边界办公环境。

截至目前，深信服桌面云已完成多次产品升级迭代，通过对虚拟化底层的不断调优，来保障整个平台架构的极致稳定；通过自研的虚拟桌面传输协议，来确保桌面显示的高可靠性，及优越的音频和视频播放体验。如基于新一代高效能桌面图像编码 HEDC 技术，保障用户在窄带环境下，依然能获得高清视频的流畅播放。同时，深信服桌面云支持业界主流的各种操作系统与应用软件，实现对超过 1,000 款外设硬件的全面兼容。针对传统 PC 办公形态固有的安全漏洞，深信服桌面云通过“云-网-端”全方位可视化的安全防护体系，保障办公数据的极致安全。

通过集中的运维平台，深信服桌面云帮助用户建设敏捷高效的 IT 办公系统，远程桌面模板派发、系统升级、软件更新、补丁修护、一键健康检测等，都可以在后台统一完成，实现一位 IT 管理人员可管理 500+云桌面，在满足用户对大规模终端的管理、运维方面，极具优势。

桌面云作为一种平台型产品，需要满足用户在不同场景下的不同需求。基于用户复杂多元的办公业务需要，深信服桌面云针对不同场景打造更加适配的解决方案，并通过不断的生态合作，构建更完善的、差异化的行业解决方案。

日常办公方案、vGPU 方案、广域网方案、软件开发方案、多网隔离方案等，使得深信服桌面云能实现更广泛的行业场景覆盖，在普通办公、公用终端、安全办公、分支办公、移动办公和高端图形处理等各种细分应用场景中，为全行业用户提供专业可靠的终端服务。

3. 山石网科

3.1 优秀学生获得山石网科网络安全奖学金

6月6日，在东南大学建校 117 周年庆祝大会上，东南大学网络空间安全学院的优秀学

生获颁山石网科网络安全



去年 5 月,为了响应党中央和习近平总书记关于建设一流网络空间安全学院的指示精神,助力实施中央网信办等六部委《关于加快网络安全学科建设和人才培养的意见》,山石网科与东南大学网络空间安全学院正式签订战略合作协议。

经过一年的时间,山石网科与东南大学网络空间安全学院共同努力,充分发挥各自的优势,形成专业、产业相互促进、共同发展,实现产学研密切合作。

在上午的奖学金颁奖仪式上,东南大学网络空间安全学院党委书记施畅、党委副书记张璐、副院长曹玖新应邀出席,并对山石网科近年来对学院人才培养工作的大力支持表示感谢,向获奖学生表达祝贺与殷切期盼,希望同学们不断进取,早日成为网络强国的领军人才。

山石网科资深研发总监李校俭、山石网科总裁助理崔清晨为获奖学生颁发了奖学金证书。李校俭表示,网络空间安全专业是为实施国家安全战略而设立的,国家急需网络安全人才,他鼓励同学们要发扬东南大学止于至善的精神,敢于担当时代重任,不断迎接挑战,为国家做出更大的贡献。

山石网科在东南大学教育基金会设立奖学金项目,用于奖励东南大学网络空间安全学院的优秀学生,激励学生勤奋学习、刻苦钻研、开拓视野,为网络安全学科建设和人才培养贡献积极力量。未来,山石网科还将继续加深与东南大学网络空间安全学院的合作,共建产学研结合示范基地,切实落实科教兴国战略,为建设网络强国贡献一己之力。

4. 亚信

4.1 亚信科技发布 5G 战略及系列产品

6 月 20 日，亚信科技控股有限公司在北京隆重举行“原力进化—亚信科技 X for 5G 产品发布会”，全面展示亚信科技构建的“全域虚拟化、全域智能化、全域可感知”的 5G 网络与业务支撑能力，深化与电信运营商和大型企业的合作，共建开放、协同的 5G 生态，共同推动 5G “从流量到价值”的实现。

在发布会上，亚信科技首席技术官欧阳晔博士详细阐述了亚信科技 5G 产品和技术战略，即“全域虚拟化、全域智能化和全域可感知”。

“全域虚拟化”

是指面向 5G 的网络智能化和虚拟化的产品和解决方案，帮助运营商在网络的体系内实现网络和业务功能上的自动化和虚拟化；

“全域智能化”

是借助亚信科技在运营商体系内积累多年的机器学习、数据挖掘和人工智能等能力，帮运营商建立一整套兼容 O 域和 B 域的通用 AI 平台，帮助运营商在通信生态系统内向各个垂直生态系统输出统一的能力；

“全域可感知”

是指亚信科技所有面向 5G 研发的新产品一定是以优化和提升运营商的消费者用户和垂直行业用户在网络业务层面的感知与体验为目的，所有产品的终极目标都是优化 5G 用户的体验和感知。

亚信科技作为中国最大的电信软件和信息服务提供商，2016 年即开始针对 5G 业务模式和场景启动了新一代业务支撑系统的规划和预研工作，并在 5G 网络智能化、人工智能、平台支撑、大数据、场景计费等领域取得突破性进展；发布了 5G 网络智能化产品战略及规划，搭建了系列产品原型，包括客户体验管理产品、网络虚拟化产品、网络智能分析产品等，并已与三大运营商及所属研究机构或省公司展开了试点合作。

“作为中国三大运营商 26 年的长期合作伙伴，亚信科技和运营商在每一代的技术演进上都有高度的战略与技术协同。亚信科技将通过全域虚拟化、全域智能化和全域可感知的技术，竭力帮助运营商实现业务的中立、网络的中立。5G 时代，在技术上，我们希望做运营商网络和业务的编排者；在商业模式上，做运营商和垂直行业的赋能者。”欧阳晔博士表示。

六大 5G 产品体系

基于三个“全域”的理念，亚信科技发布了 6 个方向的产品，即：

5G 全域人工智能产品-AISWare AI²

5G 场景计费产品-AISWare 5G Billing

5G PaaS 平台产品 AISWare AIF

5G 网络智能化产品-AISWare Network Intelligence

5G 大数据产品-AISWare 5G BigData

开源数据库产品 AISWare AntDB。

5. 绿盟

5.1 绿盟科技方案再次入选工信部网络安全技术应用试点示范项目

工业和信息化部日前公布了网络安全技术应用试点示范项目名单，绿盟科技与贵州移动联合申报的《IPv6 网络空间智能安全监控平台》项目以及绿盟科技提供技术支撑的《物联网安全态势感知平台》项目和《山东联通网络信息安全应急处置系统》项目，经单位申报、地方推荐、专家评审、网上公示等环节，成功入选网络安全技术应用试点示范项目。

IPv6 网络空间智能安全监控平台

该平台由贵州移动负责系统平台总体架构的设计、搭建以及系统核心功能、流程实现方法的研究，绿盟科技负责系统的网络搭建、实施以及系统平台软件侧功能的开发和测试、版本的升级和优化，双方优势互补、通力合作，为贵州移动 IPv6 规模部署实施过程中提供了安全配套监控的技术保障手段，在积极推动落实和响应国家 IPv6 网络战略的同时，进一步提高了 IPv6 网络部署实施后资产安全风险的安全管控，降低了企业资产遭受外部攻击和无法及时响应的风险，也为行业 IPv6 环境下暴露面资产基础安全风险管控提供了借鉴和参考。

物联网安全态势感知平台

该项目由中国移动集团公司统一牵头制定整体方案以及项目推进，中移物联网有限公司负责整体架构设计、平台建设和数据分析模型研发，重庆移动公司配合开展省内平台建设，实现物联网卡和行业卡精细化预警并共享数据。绿盟科技为中移物联网有限公司平台侧提供物联网终端和物联网卡安全分析技术支撑，为重庆移动公司省内平台提供整体技术支撑，各方共同为该平台注智注力，全方位提升中国移动物联网安全运营及态势感知能力，为社会营造安全可靠的通信环境，并将为推动物联网行业的健康发展产生重要的社会价值。

物联网态势感知平台主要从物联网卡、物联网终端等维度展开对物联网安全威胁分析和

监控，形式一个完整物联网安全分析、展示和处置平台。通过大数据、人工智能的物联网业务风险预警手段，可对物联卡使用场景、行为特征进行精准分析，让违规用卡无处遁形，为监管单位和发卡单位提供精准的风险预警服务。在使用过程中，有效抑制物联网卡、智能终端的异常使用行为，通过有效的监管手段与体系的建立，可全生命周期了解物联网卡的使用状况，提供完整的证据链进行验证追溯。同时，对于已出售的大量智能终端，需要能够实时掌握终端的异常问题，通过对终端的脆弱性分析、异常行为分析、异常连接等发现终端感染、受控、僵尸网络、异常访问等威胁，为社会营造风清气朗的通信环境。

山东联通网络信息安全应急处置系统

本系统由山东联通负责牵头制定整体方案以及需求确认，绿盟科技负责基础平台承建与技术支持。项目意义在于通过单一的系统平台可以实现网络信息安全对不同领域的处置要求，并且将操作简化成最基本的输入，只需要进行合理的授权，就可以实现可靠快捷的网络信息安全应急处置，可以将不良影响控制在最小范围，满足网络安全法规以及行业主管部门的要求，有效解决事件影响大，活动保障要求高，监控手段效果差，应急处置效率低等问题。同时，填补了态势感知平台在处置方面的空缺，形成从安全威胁监测、分析到处置的闭环管理，以安全事件为驱动，以应急处置为核心，联动态势分析平台及安全设备，实现重要安全事件的快速处置，提升总体安全应急响应效率，特别是满足重保场景下对网络攻击行为的快速阻断，优先消除对重要资产的受害影响，保障重保工作顺利进行，在 2018 年青岛上合组织峰会保障中起到非常大的作用。

6. 安恒

6.1 安恒 AiLPHA 入选 2019 年最具颠覆性创新潜力榜

作为中国科协在 2019 年全国大众创业万众创新活动周期间的重点活动，6 月 14 日，2019 “创世技”颠覆性创新榜发布会成功举办。会上发布“2019 年最具颠覆性创新潜力榜”，安恒信息 AiLPHA 大数据智能安全平台成功上榜！

2019 “创世技”颠覆性创新榜评选活动主要针对节能环保、新一代信息技术、生物、高端装备制造、新能源、新材料和新能源汽车、互联网等八大战略性新兴产业领域评选具有颠覆性创新特征的科研、产品和商业模式。从思想前沿、技术创新、市场孵化、公众关注四个角度展开评选，其中注重技术创新和市场应用价值和发展空间。

安恒信息 AiLPHA 大数据智能安全平台以“AI 驱动安全”为核心理念，创新性地采用

大数据技术和机器学习，集成超大规模存查、大数据实时智能分析、用户行为（UEBA）分析、多维态势安全视图、企业安全联动闭环等安全模块，结合场景分析的自学习建模，具备全网流量处理、异构日志集成、核心数据安全分析、办公应用安全威胁挖掘等前沿大数据智能安全威胁挖掘分析与预警管控能力，实现对整个高级威胁攻击链的全面关联分析和网络系统安全态势感知。

技术创新

安恒信息 AiLPHA 大数据智能安全平台具备多个创新性关键技术，包含基于知识图谱的网络攻击自动化关联推理技术、实时挖掘和分析海量安全数据技术、基于安全场景的行为威胁分析技术、基于机器学习的异常行为风险分析技术、安全事件合规映射技术、基于深度威胁分析的多维态势可视化技术等，很好地解决了市面上现有的安全威胁检测类产品和当前难以实现真正联动分析、态势感知和追踪溯源存在的不足之处。

市场应用

目前，AiLPHA 大数据智能安全平台已被广泛应用于运营商、金融、政府、高校、医疗、公安等各行各业，为用户提供全局安全态势感知能力和业务不间断稳定运行提供安全保障，为用户信息系统安全决策提数据支撑。同时，AiLPHA 大数据智能安全平台获得工信部“2019 年大数据优秀产品和应用解决方案案例”、Cyber Defense Magazine：“2019 年度 SIEM 突破奖”、中国网络安全产业联盟“2018 年网络安全创新产品优秀奖”等荣誉，充分获得行业与用户的认可。

7. 奇安信

暂无消息。

8. 安天

暂无消息。

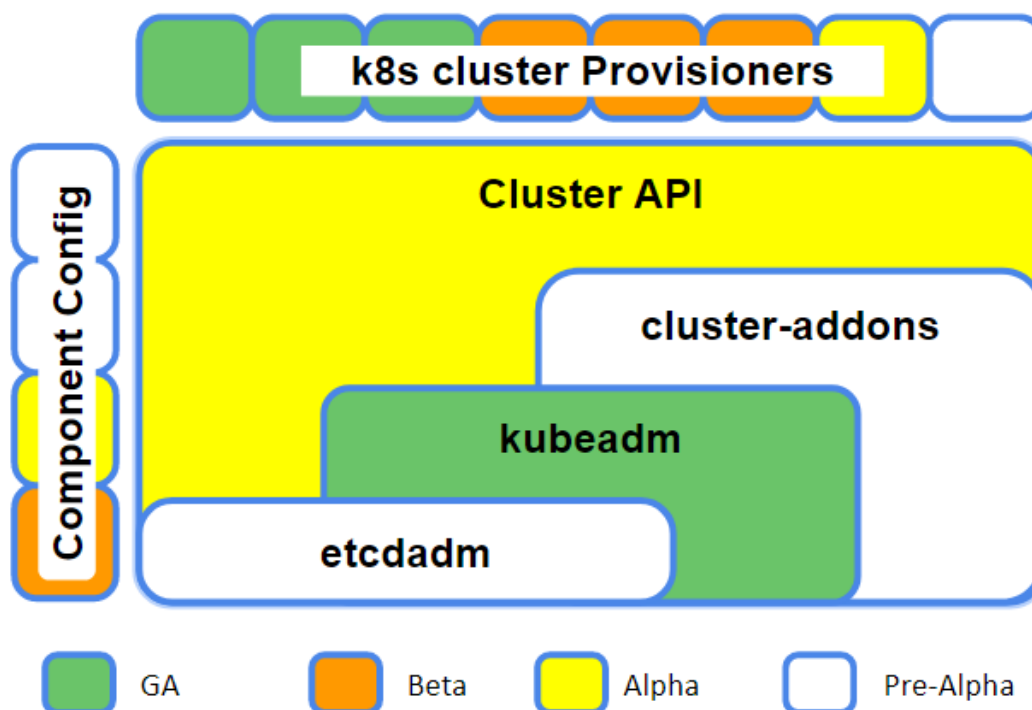
四、 容器技术及安全动态

1. Kubernetes 1.15 发布

2019 年 6 月 20 日，Kubernetes 重磅发布了 1.15 版本，包含 25 项增强功能，其中 2 项为稳定版、13 项为 beta 测试版，另有 10 项为 alpha 测试版。

持续性改进——项目的可持续性水平并不仅仅取决于功能。因此，我们通过多项 SIG 致力于提升测试覆盖率、确保各基础要素的稳定性、改善核心功能集的稳定水平，并努力在完善现有功能的同时处理尚未解决的积压性问题。

可扩展性——社区一直在要求我们进一步提升可扩展性水平，因此本次版本中包含更多与 CRD（Custom Resource Definition）以及 API Machinery 相关的开发成本。本次升级周期中的大多数增强功能来自 SIG API Machinery 及其相关领域。



Kubernetes 近几个版本的变化，我们发现特性主要集中在 Storage、Node、API-Machinery、Network、Scheduling 等 SIG，而这些 SIG 大都致力于可扩展性增强，以便于下游用户在享受稳定核心的同时，轻松扩展定制自己的插件。

2. Docker 迎来 Windows Subsystem for Linux 2

微软方面刚刚推出的 Windows Subsystem for Linux 2 (WSL2)已经将 Linux 内核引入 Windows 系统。

在一篇工程博文当中，Ferquel 解释称，凭借一己之力将容器技术推向主流的 Docker 公司正着手将其 Docker Desktop 开发平台 for Windows 从全 Hyper-V 转换为更加轻量化的 WSL2 Hyper-V 虚拟机。微软“实际上提供了一套能够真正在轻量级虚拟机当中运行的 Linux 内核……其比 Windows 所提供的内核更加轻，与 Windows 集成效果更紧密，Docker 守护程序能够在其中运行良好并获得卓越的性能表现。Ferquel 宣称，冷启动条件下 WSL2 与 Docker 守护程序的速度“迅如奔雷——在我的开发笔记本上能够在 2 秒内完成启动；相比之下，目前的 Docker Desktop 版本启动需要数十秒。”

Docker 还将利用 WSL2 集成包取代原本的 Hyper-V VM。其将具有与当前 Docker Desktop 相同的功能，具体包括 Kubernetes 一键设置、自动更新、透明 HTTP 代理配置、访问 Windows 中的守护程序以及透明绑定 Windows 文件挂载等等。

真正令 Docker 开发者们感到振奋的是，他们将能够同时开发 Windows 与 Linux 版本的容器化程序。Ferquel 宣称这将给面向 Linux 环境的项目或者 Linux 定制型 build 流程的开发者群体带来巨大的推动作用。这意味着大家不再需要分别构建 Linux 与 Windows 版程序的维护脚本！举例来说，Docker 开发人员现在可以与 Linux 平台上的开发者使用相同的一组工具及脚本，并直接在 Windows 之上运行 Linux Docker 守护程序。

他同时宣称，WSL 的绑定挂载还将具有与本机 Linux 设备几乎完全相同的 I/O 性能。这将直接解决 Docker Desktop 面临的主要痛点之一——I/O 密集型工具链。NodeJS、PHP 以及其它 Web 开发工具都将从这一改进中受益。

3. Kube-OVN 0.5.0 发布

Kube-OVN 是一个基于 OVN 的 Kubernetes 开源网络系统。

本次更新主要包含以下内容：

1. 支持 Kubernetes NetworkPolicy

Kube-OVN 0.3.0 的版本起支持子网间的防火墙设置，在 0.5.0 版本开始支持完整的 Kubernetes NetworkPolicy，用户可以实现更细粒度的网络策略控制，更好的对应用级别的网

络访问进行安全控制。

Kube-OVN 在 NetworkPolicy 的实现中没有使用 Iptables 而是使用 Openflow 的流表规则对每个端口进行单独的访问规则设置。并使用 PortGroup 和 AddressSet 等 OVN 中的数据结构对流表进行简化，大幅降低规则的数量，减轻因网络策略对性能的影响。

2. 自定义容器通信网卡和 MTU

针对宿主机多网卡的情况，之前版本的 Kube-OVN 使用默认路由对应的网卡作为容器跨主机通信的网卡。从 0.5.0 开始，用户可以通过命令行参数 `-iface` 选择容器间通信所使用的网卡，方便用户根据自己的网络环境搭建更为复杂的网络系统。

之前版本容器网卡的 MTU 默认为 1400，在新版本中会根据用户选择的网卡 MTU 自动计算出合适的容器网卡 MTU，用户也可以根据自己的情况通过命令行参数 `-mtu` 来指定容器网卡 MTU，实现更好的性能和吞吐量控制。

3. 默认系统参数设置

从本版本开始，Kube-OVN 会自动检查环境系统参数并进行设置，例如：`ip_forward`，`bridge-nf-call-iptables`，`rp_filter` 等，减少因系统参数差异带来的网络问题，避免一些已知问题的出现。

4. 默认网关自动计算

针对 `default_logical_switch` 和 `node_switch` 自动计算默认网关，减少用户手动配置负担。

5. 暴露更多的命令行参数

将开放中的选项参数进行暴露，方便用户进行自定义的设置。

五、安全新产品及技术

1. macOS Catalina 应用将需要通过认证

WWDC 2019 主题演讲期间，苹果宣布了新版 macOS 操作系统的正式名称——Catalina。作为一次重大的系统升级，其对应用开发者也提出了更高的要求。如果你想要打造支持 macOS Catalina 的应用程序，必须交由苹果进行一系列安全认证，否则会在默认情况下被阻止运行。

据悉，这项新措施是现有的 Gatekeeper 流程的进一步延伸，开发者们可以按需提交他

们的应用程序。

2. iOS 13 与 macOS 10.15 不再支持 SHA-1 证书

由于旧版哈希算法不再安全，业内在 2017 年掀起了抛弃 SHA-1 TLS 证书的运动。微软、谷歌、Mozilla 起到了很好的表率作用，并鼓励大家迁移到更安全的 SHA-2 或 SHA-3 证书，然而苹果却迟迟没有采取行动。好消息是，在开发者大会（WWDC 2019）之后，该公司在新版支持页面上写到，iOS 13 和 macOS 10.15 Catalina，已正式抛弃采用 SHA-1 算法签名的证书。

苹果在官方支持页面上写到：

使用 RSA 密钥的 TLS 服务器证书和颁发机构（CA），必须使用 ≥ 2048 位的密钥，TLS 将不再信任使用 < 2048 位的 RSA 密钥证书。

TLS 服务器和 CA 必须使用基于 SHA-2 的哈希算法，TLS 不再信任 SHA-1 签名的证书。

TLS 服务器证书必须在‘主体别名’（Subject Alternative Name）扩展名中显示服务器的 DNS 名称，常用名（CommonName）中的 DNS 名称将不再被信任。

3. 印象笔记扩展被曝严重漏洞

印象笔记 Web Clipper Chrome 扩展中被曝存在一个严重缺陷，可导致潜在攻击者访问用户存储在第三方网络服务中的敏感信息。发现该漏洞的安全公司 Guardio 表示，“由于印象笔记广为流行，该问题可能影响使用该扩展的客户和企业，在发现之时它的用户量为 460 万左右。”

该问题是一个全局跨站点脚本(UXSS)漏洞，编号为 CVE-2019-12592，源自一个印象笔记 Web Clipper 逻辑编程错误，使其可能“绕过浏览器的同源策略，导致攻击者能够在印象笔记域名以外的内联框架中获得代码执行权限。”一旦 Chrome 的站点隔离安全功能崩溃，其它网站账户的用户数据就无法受到保护，从而导致恶意人员能够访问第三方网站上的敏感的用户信息，“包括社交媒体、个人邮件等中的认证、金融、私密会话。”目标被重定向至受黑客控制的且加载目标第三方网站内联框架的网站，并触发旨在强迫印象笔记将恶意 payload 注入所有加载内联框架的利用，而该 payload 将“窃取 cookies、凭证、私人信息并以用户身份执行动作等。”

4. 国家网信办《个人信息出境安全评估办法（征求意见稿）》

为保障个人信息安全，维护网络空间主权、国家安全、社会公共利益，保护公民、法人的合法权益，依据《中华人民共和国网络安全法》等法律法规，国家互联网信息办公室会同有关部门起草了《个人信息出境安全评估办法（征求意见稿）》，现向社会公开征求意见。有关单位和各界人士可以在 2019 年 7 月 13 日前，通过以下方式提出意见：

1. 登录中国政府法制信息网(网址：<http://www.chinalaw.gov.cn>)，进入首页的“立法意见征集”提出意见。

2. 通过电子邮件方式发送至：security@cac.gov.cn

3. 通过信函方式将意见寄至：北京市西城区车公庄大街 11 号国家互联网信息办公室网络安全协调局，邮编 100044，并在信封上注明“个人信息出境安全评估办法征求意见”。

5. 谷歌发布面向计算隐私的开源工具

谷歌发布了一款全新的开源加密工具，旨在提高敏感数据集的隐私性。该工具名为 Private Join and Compute，可帮助那些与机密数据服务商合作的公司。私有计算允许公司在数据库中共享数据，这些数据在各种计算过程中将保持加密状态。然后，他们可以以汇总统计的形式查看解密的最终结果。

六、网络安全投融资、收购事件

1. 收购

1.1 Onapsis 完成对 Virtual Forge 的收购

6 月 17 日，Onapsis 完成对 Virtual Forge 的收购，收购价未公开。Virtual Forge 成立于 2006 年，是自动检测和修复 SAP 应用程序网络安全解决方案的服务提供商。Virtual Forge 的技术添加到 Onapsis 屡获殊荣的业务应用程序网络弹性平台上，为利用 SAP 和 Oracle 应用程序运营业务的企业组织提供无与伦比的网络安全、可见性、事件响应和管理等功能。

2. 投融资

2.1 Liongard 获 450 万美元 A 轮融资

6 月 3 日, Liongard 从 TDF Ventures 和其他 3 位投资者处获得 450 万美元的 A 轮融资。Liongard 专门为 MSP 构建了 Roar 平台, Roar 平台统一了管理方式, 保护了所有客户端。Roar 自动从云、网络和内部部署系统检索配置状态数据, 通过以自动化系统, 检测关键配置项更改并持续评估安全性。

2.2 Orca Security 获 650 万美元种子轮融资

6 月 12 日, Orca Security 从 YL Ventures 处获得 650 万美元的种子轮融资。Orca Security 是一家专注于云安全可见性解决方案提供商, 提供对客户资产的完整可视性, 包括云基础架构、操作系统、应用程序和数据, 帮助全球客户企业安全运营。

2.3 Expel 获 4000 万美元 C 轮融资

6 月 18 日, Expel 从 Battery Ventures 和其他 5 位投资者处获得 4000 万美元的 C 轮融资。Expel 是一家透明托管云安全服务提供商, 专注于调查警报并监控客户的环境, 为用户提供解决方案, 找到发生问题的根本原因, 以免这些问题再次发生。