国内外云计算+安全动态报告

2019 年第 5 期

启明星辰云计算安全事业部

目录

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 Amazon EMR 支持在运行 EMR 集群时重新配置应用程序、Amazon Cognito 发布面向管理员的增强型用户密码重置 API 以及 AWS Systems Manager 补丁管理器支持 Microsoft 应用程序修补等，同时 AWS Secrets Manager 支持更多客户端缓存库，以提高密钥可用性并降低成本，AWS IoT Device Defender 支持监控未注册设备的行为； VMware Pulse IoT Center 2.0 正式商用，能够帮助企业应对边缘与物联网系统中的高度分布式、大规模及固有安全性的挑战；先讯美资联合谷歌云为零售商提供实时商业预测；VMware 和微软达成合作，Azure 云可运行 VMware 虚拟化软件；联想和微软携手合作基于 Azure 云的物联网;阿里云首提物联网 LoRa2.0 概念、阿里云 PolarDB 发布更新支持一键迁移、阿里云牵手马来西亚科技公司打造智能交通系统、 阿里云全面拥抱贵州，在八大领域深入合作；优必选与腾讯云就智能机器人达成合作、腾讯云小微牵手优必选，助力智能电视进化、腾讯云推出慢直播方案，低成本打造数字监控系统；华为云存储容灾服务（SDRS）正式商用。

开源云方面，浪潮和英特尔共同分享了 Openstack Rocky 版本的大规模测试数据，推动 Rocky 走向实际生产环境。EasyStack 发布可进化的新一代私有云 ECS，同时开启了 ECS Stack 超融合、ECS 企业云标准版、ECS 企业云场景化版等全系列产品的全新阶段。

云安全厂商方面，启明星辰举行云子可信上线两周年庆典、以最大中标份额入围中国移动漏洞扫描产品集采、发布面向工控领域的无损漏扫解决方案； 深信服承办网络安全等级保护制度 2.0 国家标准宣贯会；山石网科推出满足 NFV 标准的安全网元解决方案山石云•集；亚信出席 C3 安全峰会并发表《5G•云安全》

演讲；绿盟云沙箱成为 VirusTotal 官方合作产品；安恒 AiLPHA 大数据智能安全平台在 2019 数博会上斩获两项大奖；奇安信补天五星计划发布；安天展示智甲终端防御系统方案。

容器动态方面，Helm 3.0 alpha 版本发布，和 kubernetes 完美融合；Docker 发布了 Docker Enterprise 3.0，并称该平台是唯一的桌面到云企业容器平台，使企业能够构建和共享任何应用程序并在任何地方安全地运行它们，从混合云到边缘。KubeCDN 是一个基于 Kubernetes 的自托管 CDN 方案，用户可以完全控制自己的基础设施，不再需要第三方的内容分发网络，重新控制了从服务器到用户设备的数据流。

安全新技术方面，“等保 2.0”正式发布，12 月 1 日正式实施；Windows 再曝“WannaCry”级漏洞，Windows 10 出现新 0day，任务计划进程可用于攻击；英特尔也再曝漏洞，影响 2011 年以来几乎所有产品；同时新指纹识别技术漏洞曝光：可跟踪 Android 和 iOS 设备。

网络安全投融资方面，分别发生 2 起收购和 3 起融资事件。Elevate Security 完成对 Phish5 的收购，Phish5 旨在开发以易用性著称的网络钓鱼模拟软件，能够帮助企业改进和衡量电子邮件安全；KnowBe4 宣布收购 CLTRe，CLTRe 致力于帮助用户评估、构建、维护和衡量的安全态势。融资方面，“网络即服务”的安全厂商 HyperQube 获 50 万美元种子轮融资；SOAR 的服务提供商 Siemplify 获 3000 万美元 C 轮融资； 云安全解决方案提供商 GuardiCore 获 6000 万美元 C 轮融资。

2019 年 5 月 30 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 Amazon EMR 宣布支持在运行 EMR 集群时重新配置应用程序

5 月 1 日消息，Amazon EMR 宣布支持在运行 EMR 集群时重新配置应用程序。

现在可以修改在 EMR 集群上运行的应用程序的配置，包括 Apache Hadoop、Apache Spark、Apache Hive 和 Hue，而无需重新启动集群。EMR 应用程序重新配置功能让您可以即时修改应用程序，而无需关闭或重新创建集群。Amazon EMR 将应用您的新配置，并正常重启重新配置的应用程序。可以通过控制台、软件开发工具包或 CLI 应用配置。

1.2 Amazon Cognito 发布面向管理员的增强型用户密码重置 API

5 月 6 日，Amazon Cognito 针对 Cognito 用户池服务发布了一个新的 API – AdminSetUserPassword，管理员可通过该 API 为其最终用户设置临时或永久密码。即使最终用户经过验证的电话号码或电子邮件地址不可用，此功能对于他们仍然可用。

借助 Amazon Cognito 可以快速轻松地为 Web 和移动应用程序添加用户注册、登录和访问控制功能。Amazon Cognito 可将用户规模扩展到数百万，并支持通过 SAML 2.0 使用社交身份提供商（如 Facebook、Google 和 Amazon）以及企业身份提供商进行登录。

1.3 AWS Systems Manage 补丁管理器支持 Microsoft 应用程序修补

5 月 7 日，可以使用 AWS Systems Manager 补丁管理器在 Amazon EC2 或本地实例中自动选择并应用 Microsoft 应用程序补丁。这会将 Microsoft 应用程序修补功能引入用于修补 Microsoft Windows 的 AWS Systems Manager 解决方案中，从而节约时间并简化修补过程，可以从一个位置管理 Microsoft 操作系统和应用程序补丁。

Systems Manager 补丁管理器通过定义可在预设时间或临时决定应用的操作系统和软件补丁基准来帮助您保持 AWS 和本地实例的合规性，从而确保拥有最新实例。经过此次更新，现在可以使用补丁管理器扫描您的 Microsoft 应用程序，以确认是否缺少基准定义的补丁。此外，还可以将这些补丁应用于 EC2 或本地实例。支持 Microsoft 更新目录中提供

的所有应用程序补丁。要开始使用，只需采取与补丁管理器控制台、CLI 或 API 中的操作系统补丁基准相同的方式创建应用程序补丁基准。

1.4 AWS Secrets Manager 支持更多客户端缓存库

5 月 8 日，可以在 Python、.NET 和 Go 中使用 Secrets Manager 客户端缓存库，从而轻松地在应用程序中使用这些密钥。通过 AWS Secrets Manager，可以在其生命周期内存储、分发和轮换数据库凭证和 API 密钥等密钥。

2018 年，Secrets Manager 在 Java 和 JDBC 中发布了客户端缓存库。客户端缓存可以减少网络可用性问题的影响，例如增加响应时间和网络连接暂时中断，从而帮助提高使用密钥的可用性。它还可以通过减少由 Secrets Manager 发出和计费的 API 请求数来降低使用 Secrets Manager 的成本。这些库定期更新缓存，以确保应用程序使用最新密钥值，可以将密钥值配置为定期轮换。

1.5 AWS IoT Device Defender 支持监控未注册设备的行为

5 月 15 日消息，AWS IoT Device Defender 支持识别未注册 AWS IoT Core 的设备的异常行为。AWS IoT Device Defender 是一项完全托管的服务，可帮助保护 IoT 设备队列的安全。AWS IoT Device Defender 可以持续监控各个设备、云和 AWS IoT Core 的安全指标，验证它们的行为是否偏离了为每台设备所定义的相应行为。如果出现任何异常，AWS IoT Device Defender 就会发送提醒，以便及时采取措施修复问题。

要想使用这项新功能，首先要附加一个定位未注册设备的安全配置文件。AWS IoT Device Defender 能够检测到未注册设备的云指标反常情况，例如身份验证失败次数、连接尝试次数、断开连接次数、消息大小、发送或接收的消息数量以及源 IP。现在，客户还可以监控未注册设备的设备端指标，例如传入/传出字节数、传入/传出数据包数、侦听 TCP/UDP 端口数以及设备连接的目的地 IP 数。

2. VMWare 云动态

2.1 VMware Pulse IoT Center 2.0 正式商用

5 月 7 日消息，VMware 宣布下一代边缘基础架构和物联网设备生命周期管理平台 VMware Pulse IoT Center 正式可用。VMware Pulse IoT Center 2.0 推出更新的功能，旨在为客户提供物联网/边缘设备、互联传感器与应用程序的全生命周期的精细管理。Pulse IoT

Center 2.0 将帮助实现顺畅且更安全的设备注册和配置入网，让启用物联网变得更加简单。

边缘计算和物联网虽已存在，但在物联网领域起步仍然面临诸多挑战。例如：安全连接和编配来自不同设备类型的海量异构数据可能较为困难，不同的操作系统和连接协议经常形成物联网孤岛，不可避免地导致管理成本高昂且效率低下，并拉大 IT 和 OT 团队之间的差距。因此，VMware Pulse IoT Center 2.0 应运而生，它能够帮助企业应对边缘与物联网系统中的高度分布式、大规模及固有安全性的挑战。

3. GOOGLE 云动态

3.1 先讯美资联合谷歌云为零售商提供实时商业预测

5 月 13 日消息，江森自控宣布旗下先讯美资解决方案与谷歌云达成合作，即先讯美资智能库存平台 TrueVUE 将依托谷歌云平台集成零售软件，为零售商提供实时、可执行的商业洞察和预测分析。这也将进一步优化先讯美资业务运营，在实现业务增长的同时，巩固实时洞察分析、店铺运营与绩效管理领域。

智能库存平台 TrueVUE SaaS 采用具有高扩展性和高延伸性的 API-first 设计，提升平台兼容性，简化并加快集成工作，支持零售商使用手机应用程序来提高库存管理效率。TrueVUE 通过抓取实时库存数据、店内商品移动轨迹数据和商品丢失事件等信息，优化库存，为消费者打造卓越购物体验。

4. 微软 Azure 云动态

4.1 VMware 和微软达成合作 Azure 可运行 VMware 虚拟化软件

5 月 1 日消息，在戴尔年度峰会上，一则重磅消息被公布：戴尔子公司 VMware 与微软公司合作，将其基础设施管理软件引入微软 Azure 公有云服务。通过自己的硬件、VMware 基础架构的软件集成和微软 Azure 云服务，戴尔试图在快速增长的混合云市场中取得成功。

进入 Azure 云服务的 VMware 软件有四个主要组成部分，包括 VMware 的旗舰产品 vSphere 虚拟机管理程序，以及添加的 vSAN 存储管理和 NSX 网络管理产品。第四个组件是 vCenter，它允许信息技术团队通过统一界面监控其所有的 vSphere 驱动服务器。

这些管理工具，全球有很多企业和组织机构使用其管理自己的本地应用程序。Azure VMware 解决方案将使这些公司能相对无缝地将本地工作负载转移到微软 Azure 云中，并以与过去相同作为此次合作的一部分，VMware 还将把其 Horizon Cloud 虚拟桌面解决方案与

微软最近推出的 Windows 虚拟桌面服务集成在一起。

5. 阿里云动态

5.1 阿里云首提物联网 LoRa2.0 概念 打造百亿级连接市场

5 月 20 日消息，国内物联网领军企业阿里云率先提出将进入“LoRa2.0 时代”，阿里云方面表示，除了将继续加大在 LoRa 芯片 IP、支撑平台上的投入以外，未来还将全力打造百亿级 LoRa 连接，尽快实现 LoRa 的全面普及阿里云将引领 LoRa1.0 时代走向 2.0 时代，连接数将从 1.0 上百上千，增长到 2.0 的百亿级。相关公司有东土科技、宜通世纪。

5.2 阿里云 PolarDB 发布更新支持一键迁移

5 月 21 日消息，阿里云 PolarDB 发布重大更新，提供传统数据库一键迁移上云能力，可以帮助企业将线下的 MySQL、PostgreSQL 和 Oracle 等数据库上云，最快数小时内迁移完成。据估算，云上成本不到传统数据库的 1/6。目前，已有约 40 万个数据库迁移到阿里云上。PolarDB 是阿里云在 2018 年正式商业化的云原生数据库，目前已是阿里云上增长最快的数据库产品。

5.3 阿里云牵手马来西亚科技公司打造智能交通系统

5 月 23 日消息，中国阿里巴巴集团旗下云计算及人工智能科技公司阿里云宣布，与马来西亚智能交通公司“塞纳交通系统”合作，在马来西亚共同打造智能交通管理系统。

5.4 阿里云全面拥抱贵州 八大领域深入合作

5 月 26 日消息，在贵州数博会上阿里巴巴宣布将在数字政府、教育、物联网、扶贫、科研、零售、工业和农业八大领域持续加大在贵州的投入。以阿里云为依托，撬动经济体的力量，全力推动当地大数据产业发展，重点攻坚技术脱贫。阿里巴巴是最早与贵州开展深入合作的科技公司。早在 2014 年，贵州就与阿里云启动建设“云上贵州”，是全国第一个将所有政务数据上云的省份。而后，阿里云成立本地分支机构，同时在贵州设立全球备案中心和技术支持中心，支持当地数字经济发展。

公开信息显示，目前，“云上贵州”已经形成“一云统揽”新体系，承载省、市、县政府部门全部 9274 个应用系统，实现所有系统网络通、应用通、数据通。在云上贵州“一朵云”的基础上，实现“一网通办”和“一平台服务”。

6. 腾讯云动态

6.1 优必选与腾讯云就智能机器人达成合作

5 月 17 日消息，优必选与腾讯云正式签署战略合作协议。未来，双方将围绕智能机器人终端共同建立服务与内容生态，深化人工智能研发应用。

6.2 腾讯云小微牵手优必选 助力智能电视进化

5 月 20 日消息，腾讯云小微与优必选签署战略合作协议，作为同样驻地深圳的两家科技企业，腾讯与优必选的合作由来已久。本次合作将依托腾讯云小微智能语音等 AI 技术优势及优必选公司在机器人领域的积累，双方将探索人工智能技术、云计算、行业智能化解决方案等领域的深度合作。

根据战略合作计划，双方将围绕智能机器人终端共同打造服务与内容生态，深化人工智能研发应用。双方将共同探索教育、文旅、生活服务、交通、零售等领域服务机器人等应用落地方案，推动 AI 技术的突破与创新，提高行业智能化水平。

未来，腾讯将在 OTT 领域扮演服务提供商的角色，腾讯云小微将把握 TV 产品领域内的合作，与电视牌照方合作打理好产品后进而推送到电视端下游方。

场景用户画像在 TV 端还在演进中，深入到更加具体的用户画像上、实现重度垂直、精细化推进显得尤为重要，这也是腾讯云小微与优必选合作的关键。未来的家庭端产品，都将会建立在 AI 成熟化应用的基础下，如以声音识别、面部识别，实现人机交互。搜索引擎也将越来越准确，进而慢慢带动电视终端的活跃度。

6.3 腾讯云推出慢直播方案，低成本打造数字监控系统

5 月 24 日消息，腾讯全球数字生态大会在云南昆明举行。大会期间,腾讯总裁刘炽平表示,“腾讯与云南省达成了很多合作,其中一个标杆便是‘一部手机游云南’项目”。“一部手机游云南”项目建设一年多以来,广泛受到好评,其中直播板块更是成为云南推广旅游资源的绝佳渠道。通过游云南 APP 及小程序,游客可以观看云南景区实时直播,在出行前做好规划,甚至足不出户遍览云南风光。

与传统的直播方案相比,慢直播具有“上行推流路数多、下行播放带宽小”的特点,通过增加上行推流路数,加速多角度视频画面同步上传,即使多如“游云南”的 1400 路实时画面,也能同时快速上传至云端;同时考虑到此类直播一般观看人数偏少,减少下行播放带宽,在满足少量人稳定流畅观看的条件下降低成本。除了旅游景区直播,慢直播还能广泛应用于安防

监控、阳光厨房、交通路况监测等领域。以阳光厨房为例,慢直播在餐饮后厨部署多个视频采集设备,能够将后厨画面无死角地传至用餐大厅或线上阳光平台,供消费者与监管部门监督食品加工流程,推动食品监管透明化。

基于在音视频、AI 识别、大数据分析等方面的技术能力和经验积累,腾讯云将继续优化慢直播方案,将其拓展到更多领域,助力各行业降低成本、提升效率。当然,慢直播方案仅是腾讯云推出的众多数字产品之一,产业互联网时代下,腾讯将携手众多合作伙伴打造更多面向全行业的解决方案,加速全球数字化发展进程。

7. 华为云动态

7.1 华为云存储容灾服务（SDRS）正式商用

5 月 9 日消息，存储容灾服务（Storage Disaster Recovery Service，简称 SDRS）于华为云杭州城市峰会正式转商发布。SDRS（存储容灾服务）是华为云提供的服务化容灾方案，简单三步操作即可为云上虚拟机提供跨可用区级别的容灾保护，确保数据零丢失（RPO=0），并可在灾难发生时迅速恢复业务，提升连续性、减少损失。SDRS 独家满足第五级容灾标准，助力政企达成容灾监管要求。

SDRS 的三大优点：

（1）更高可靠

SDRS 作为业界独家提供云上跨可用区 RPO=0 的容灾方案，可确保数据零丢失，并在灾难发生后，于分钟级完成从主备切换到容灾端虚拟机运行的全过程（RTO≤30min）。此外，SDRS 可在不影响业务的情况下，无限次执行在线容灾演练，用以检验容灾方案的可行性、有效性。

（2）更低成本

相比传统容灾，SDRS 提供的云上服务化容灾方案可省去硬件、电力、维护等成本，容灾 TCO 下降约 60%。而且在灾难发生前，容灾端虚拟机无需开机，可进一步节省成本。对于某些绑定网卡 MAC 地址的付费应用，由于 SDRS 支持自动网络迁移，故切换后无需加购软件 License。

（3）更易使用

与自建灾备中心所需的各项繁琐操作不同，SDRS 三个步骤即可开启容灾保护，还可以将同一业务内的虚拟机进行成组保护，即以业务为粒度灵活配置保护实例。当灾难发生时，

SDRS 可一键将业务切换至容灾端，用户也可通过容灾大屏，实时查看所有容灾资源、告警等信息。

7.2 华为工业互联网平台 FusionPlant 助力国家电网打造泛在电力物联网

5 月 27 日消息，在 2019 数博会之“工业互联网与智能+”高端对话活动中，华为发布了基于华为云的工业互联网平台 FusionPlant，使能行业伙伴构建行业平台，联合懂行业的应用合作伙伴、有集成交付能力系统集成商等共同提供面向工业全场景的解决方案。当前以云计算、大数据、人工智能、边缘计算、5G 等为代表的新一代 ICT 技术蓬勃发展，正逐渐融入以机、电、工业自动化等为核心的传统工业基础设施架构，构建起工业互联网新型基础设施，帮助电力、煤炭、汽车、钢铁等各行业实现提质降本增效。华为将致力于做工业互联网领域的黑土地，驱动各个行业和企业升级改造。

华为公司高级副总裁张顺茂在主题演讲中分享了华为工业互联网平台 FusionPlant 在电力行业的落地实践。张顺茂认为，当前工业互联网产业还处在探索期，面临两大挑战。首先，相比 2C 的消费互联网，2B 的行业市场更关注知识产权、数据安全隐私等保护，开放性和共享性需要受控保护。所以，2B 市场的生态开放不能一蹴而就，需要先建立基于行业价值链的生态圈，然后逐步扩大开放圈子。其次，工业互联网需要 OT 和 ICT 产业深度融合，而当前 OT 和 ICT 产业有不同的认知、技术和文化背景，双方如何达成跨产业的价值、技术、标准等共识是巨大挑战。

2019 年初，国家电网发布了两网战略——坚强的智能电网+泛在电力物联网。其中，坚强智能电网是第一张名片，目标是打造全球领先的物理基础设施；泛在电力物联网作为第二张名片，则是智能坚强电网在数字世界的孪生，是网上国网的体现。

此前，国家电网已经在输电、变电领域完成多项成功投资，而在配电网数字化发展过程中，面临三大挑战：设备规模大，覆盖全国 440 万个台区，4.3 亿用户表计；数字化程度低，运维手段落后，设备故障停电定位困难，停送电数据发布不及时；三新（新能源、新负荷、新用电）需求多。

为了解决上述问题，“云管边端协同”的华为工业互联网平台 FusionPlant，以华为云为底座，为国家电网引入了物联网、AI、云计算和边缘计算等创新技术，通过五个 1：一套信息模型、一个大脑，一组 App，一种终端和一张网络，将配电网基础设施化繁为简，使能行业开发者灵活开发与扩展 APP 和智能终端功能，助力“泛在电力物联网”战略实施，实现了配电网的数字化、网络化和智能化的部署和运营。

方案试点结果显示，国家电网试点区域电网人均可维护设备数量提升 90%，故障后抢修率下降 50%，新能源新负荷的吸纳和管理提升 100%，平均停电时间下降 20%。为了向国际和国内的全行业推广优秀的创新与实践，推动产业共识，国家电网还联合华为积极参与和主导了多项国际与国内的行业标准，例如编制“配电物联网顶层设计”，编制“智能配变终端技术规范”，共同申报“IEEE 和 IEC 国际标准”等。

关于新技术在行业的落地，张顺茂分享了华为的三点实践：第一，与高校合作建立生态，培养人才；第二，开发和提供简单易用的工具，把各种复杂的技术工具化、平台化，使能各行各业。例如，2019 数博会发布十大“黑科技”之一的 ModelArts 一站式 AI 开发平台。作为华为云打造的一站式 AI 开发工具，ModelArts 可以提供数据处理、智能标注、开箱即用的开发环境，大规模分布式训练，自动化模型生成，及端-边-云模型全场景部署的完整 AI 开发能力，帮助用户快速高效地创建和部署 AI 模型；第三，聚焦场景化问题，将华为的创新技术和生态与各行各业的场景化问题结合起来。华为工业互联网平台 FusionPlant 也正是基于以上经验积累，将 ICT 技术融入到工业企业中，来帮助企业实现数字化、网络化、智能化。

二、 开源云动态

1. Openstack 动态

1.1 浪潮英特尔共同分享 Rocky 的大规模测试数据

在丹佛举行的首届 Open Infrastructure 峰会上，浪潮与英特尔共同分享了基于 Rocky 的 InCloud OpenStack 大规模集群测试数据，为 Rocky 在企业实际生产环境中的部署以及大规模集群支持，提供了先导性技术验证，推动 Rocky 走向实际生产环境。

Rocky 是 OpenStack 基金会非常看重的版本，增加或强化了 OpenStack 对很多新兴技术的兼容，包括人工智能、边缘计算、裸机和软件容器等，在集成能力上有了进一步提升。不过，由于 Rocky 发布时间尚不足一年，产品成熟度依然需要 OpenStack 解决方案提供商做大量优化、改进工作，不断提升高可用、高性能、高效率，才能真正推动 Rocky 在企业生产环境的部署。

实际上，高可用、高效率与高性能正是用户在实际生产环境中，最关注的 OpenStack 特性。此次浪潮与英特尔的测试基于全新升级、优化的 InCloud OpenStack Rocky 版本，在 200+

节点的真实数据中心进行了部署，主要针对上述三个方面进行了全面测试，包括高并发压力测试（2000 并发）、网络/磁盘 IO 与 CPU/内存性能测试、LBaaS/RabbitMQ/Marriadb 测试、稳定性与高可用测试等等。

在实际测试中，浪潮 InCloud OpenStack Rocky 版本展现出良好的高可用特性，可实现控制面和数据面的全方位高可用，包括控制节点的 HA 增强、所有虚拟机的主机 HA 增强、虚拟机 HA 机制增强等。同时 InCloud OpenStack Rocky 版本在效率上也实现显著提升，代码驱动可实现程序化部署/升级，自动化支持持续集成和验证，支持一天高达 500+节点的快速交付，并且无需任何业务中断即可在线轻松扩展。此外，InCloud OpenStack Rocky 版本提供高级虚拟化功能，支持基于时间序列数据库的高 I/O 性能实时监控，并且每个集群每天支持数十亿个细粒度指标，展现出非常优异的高性能。

据透漏，浪潮与英特尔将继续基于第二代英特尔 至强 可扩展处理器以及支持英特尔傲腾 数据中心级持久内存对 InCloud OpenStack Rocky 版本进行更全面、更大规模的测试，并根据今天的测试结果对其进行持续优化和提升。

2. Easystack 动态

2.1 EasyStack 发布可进化的新一代私有云 ECS

2019 年 5 月 24 日，开源云计算企业易捷行云 EasyStack 发布新一代私有云 ECS。它是按照新一代私有云理念和特性交付的云平台，是 EasyStack 研发人员历时 18 个月的研发结晶，同时开启了 ECS Stack 超融合、ECS 企业云标准版、ECS 企业云场景化版等全系列产品的全新阶段。

基于 500+大中型企业客户的私有云的生产实践，新一代私有云 ECS 通过创新的分布式微服务和平台一体化设计，帮助企业客户实现服务能力、产品形态、支撑场景的持续可进化，赋能企业客户数字化转型和业务创新。

技术实现上，易捷行云 EasyStack 新一代私有云 ECS 企业云采用了云平台的微服务化设计。基于远程运维，企业客户无需登录后台，无需输入命令行，完全应用图形化界面化的操作，就可实现云的私有部署、极简运维和高可用的体验保障。通过微服务编排引擎、滚动升级引擎、实时负载导流引擎、服务监控与自愈引擎等技术模块实现了 IaaS 的 SaaS 化，使得新一代私有云平滑无感的持续进化与公有云似的消费级体验成为可能。

3. 99CLOUD（九州云）动态

3.1 荣获 2018-2019 年度 MEC 优异解决方案奖

5 月 16 日-17 日，由中国通信学会主办，北京信通传媒和百卓网络联合承办的“5.17 世界电信日大会”在北京顺利召开。九州云作为边缘计算行业的领先者应邀出席本次大会的“2019 MEC 技术与产业论坛”，与来自电信运营商、设备商、应用方案提供商、研究机构等 200 余人齐聚一堂，共议 5G 与边缘计算发展之关键，畅谈 5G+MEC 的机遇与未来。会上，九州云“基于 ETSI 规范的边缘开放管理平台解决方案”还荣获“2018-2019 年度 MEC 优异解决方案奖”，加速赋能 5GMEC，推动产业发展。

一直以来，九州云始终专注以开源技术为核心进行不断探索和创新，并在开源云和边缘云方面取得诸多新的进展和突破。随着 5G 物联网时代的到来，边缘计算给业界带来了巨大的市场空间。作为边缘计算的积极探路者，九州云凭借自身的技术优势深度参与 CORD,Starlingx,Akraino, OpenStack Edge Group 等边缘计算国际开源社区，并在边缘计算领域广泛拓展合作伙伴和国际客户。在 MEC 领域，九州云携手运营商打造出符合 ETSI MEC 标准规范的、基于开放架构的边缘平台。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰旗下云子可信上线两周年庆典

2019 年，云子可信创立两周年，云子可信已经累计服务中小企业超过 10000+家，终端月增长率达 20% 以上，累计版本迭代 91 次，累计开发新功能 100 个，累计服务行业类型近百种。面对激烈的市场竞争，云子可信运用新一代信息技术提高品牌价值，打造云端一体化管理软件，深耕企业 SaaS 领域。

SaaS 行业蓬勃发展，但时至 2019 年，中小型企业 SaaS 服务依然留有大量空缺。随着全社会信息化程度的不断提高，中小企业也亟需提高信息化和安全水平。早在 2017 年，启明星辰已然针对这一现状做出了努力：2017 年 4 月 27 日启明星辰在北京“429 首都网络安全日”活动上发布了一款保护中小企业信息安全产品——云子可信安全云平台。发布以来，云子可信作为启明星辰倾力打造的第一款 SaaS 产品，致力于为中小微企业提供各种 IT 安全产品和 SaaS 服务，深入解决中小微企业面临的企业终端安全问题，帮助其建立完善的企业 IT 终端安全体系，为企业终端管理、远程桌面、上网行为管理、软件管理、U 盘管控、杀毒防护等方面提供一系列完善的解决方案。

1.2 启明星辰以最大中标份额入围中国移动漏洞扫描产品集采

近日，中国移动公布了 2019 年至 2020 年安全漏洞扫描器产品集中采购中标公告，启明星辰系统漏洞扫描产品凭借过硬的技术实力最终以 70%的份额成功入围。

中国移动在本次集采测试中对主机、数据库、虚拟化设备等的资产发现能力、漏洞识别率及准确率、IPv6 环境扫描能力进行了全方位测试，从多个维度对各厂商漏洞扫描产品的真实能力进行了客观评估，最终启明星辰天镜脆弱性扫描与管理系统通过了严格的测试，以最大中标份额成功入围。

作为国内最早研发脆弱性评估与管理产品的公司，启明星辰不断突破脆弱性评估相关核心技术，在漏洞库覆盖、扫描准确率、结果呈现等多方面持续领先。

全面的漏洞覆盖

漏洞库覆盖了当前网络环境中重要的、流行的主机、数据库、虚拟化设备等漏洞，并且能够根据网络环境的变化及时调整更新，确保漏洞识别的全面性和时效性。

专业的漏洞情报

启明星辰公司作为中国安全行业最早成立的攻防技术研究实验室的企业之一，一直保持着业内一流的漏洞研究水平，能够为客户提持续的、高品质的漏洞库更新。

精准的扫描结果

除了使用常规方法扫描外，天镜可以对于同一漏洞采用多种不同类型的扫描方法进行关联校验，以达到准确判断效果。

丰富的报表呈现

天镜能够生成面向多个用户角色的客户化报表，并以图、表、文字说明等多种形式进行展现，同时支持以 HTML、WORD、Excel、PDF 等多种格式导出结果报表。

根据中国权威调研机构赛迪顾问（CCID）发布的《中国漏洞评估与管理产品市场研究报告（2018）》显示，启明星辰“天镜脆弱性扫描与管理系统”2017 年度以 23.2%的市场占有率拿下漏洞评估与管理市场第一。

启明星辰漏洞扫描产品目前已经为数万客户、亿级别的设备提供脆弱性评估服务，广泛应用于政府、电信、电力、金融、军队军工等行业，适用于传统 IT 网络、工业控制网络、物联网、云计算等各种复杂环境。

1.3 启明星辰发布面向工控领域的无损漏扫解决方案

党的十八大以来，我国确立了网络强国战略，加快数字中国建设，信息经济蓬勃发展，互联网成为国家发展的重要驱动力。如果工业控制领域能搭上互联网技术发展的技术革命，必将极大提升工控领域的生态发展；然而，由于工业控制领域的特殊性，安全问题成为其入网的最大隐患。怎样发现安全风险？怎样解除安全风险？成为工控领域入网首要落实的焦点。

而安全漏洞是安全风险的主要载体，启明星辰顺应时代需求，推出工控无损漏扫解决方案。

工控领域的网络安全风险

- 工控领域的厂商主要在国外，对安全的自主可控具有不确定性；
- 工控领域的安全风险覆盖所有的产品类型，安全无死角；
- 工控领域和传统领域的安全风险一致，甚至更脆弱，降低了攻击者的技术门槛和复杂度。

启明无损漏扫解决方案

工控环境的运行特点是实时性和稳定性，传统的漏洞扫描方式并不能保证工控环境的无损安全评估。这样，工控环境的安全评估需求就出来了：既要保证无损性，又要保证安全性的准确评估。基于这些因素，安全风险可以从两个方面进行评估：静态无损评估和无损动态漏洞扫描。

静态无损评估以被检测资产的指纹信息为分析维度，准确分析资产的安全风险，并定级资产的风险级别。

无损动态漏洞扫描是以可主动调节扫描策略的方式，逐层发现扫描目标的脆弱性，其主要特点可表现为定向性、可控性、无损性；将整个扫描过程逐步深入，确保每个扫描过程的完整性、可递进性，以达到最大限度发现目标脆弱性的目标。

➢无损动态漏扫的产品定位：

➢无损动态漏扫描的技术优势：

保证安全隐患的闭环处理

绝大多数的网络攻击事件都是利用系统未修补的漏洞。许多已经部署安全防护设备和软件的企业仍然饱受漏洞入侵之苦，造成巨大的经济损失。归根结底，其原因是用户缺乏一套完整的漏洞管理机制和平台，未能落实定期评估与漏洞修补工作，忽视了漏洞的管理，最终使漏洞成为攻击者攻击的有效途径，甚至成为蠕虫攻击的目标。工控脆弱性评估在整个工控安全防线中起到了警示和导向的作用，警示工控环境中的安全隐患，引导相关安全防护的部署方式以及对脆弱性的加固，实现对安全隐患的闭环处理。

2. 深信服

2.1 深信服承办网络安全等级保护制度 2.0 国家标准宣贯会

5 月 16 日下午，由公安部网络安全保卫局指导、公安部第三研究所、公安部第一研究所主办，深信服独家承办的“网络安全等级保护制度 2.0 国家标准宣贯会”于北京隆重召开。本次大会由公安部第三研究所副所长刘晓京主持，政府单位、企事业单位、网安企业代表等共 1200 余位到场参会，近 8000 名观众通过线上直播观看大会。

公安部网络安全保卫局郭启全总工程师发言：

郭启全总工进行网络安全等级保护 2.0 国家标准发布并做《网络安全等级保护制度 中国网络安全保障工作的伟大创举》主旨演讲，称网络安全等级保护制度是在以习近平同志为核心的党中央的坚强领导下，是中国网络安全取得的重大成就。是中国网络安全保障工作的伟大创举，是中国网络安全界广大人民的智慧结晶，是中国网络安全的基石，是维护国家安全、社会秩序和公共利益的根本保障。

此外，郭启总工程师在会中提出了要明确实施网络安全等级保护制度的目标和要求：

第一，要落实“分等级保护、突出重点、积极防御、综合防护”的总体要求。

第二，建立“打防管控”一体化的网络安全综合防御体系，提升国家网络安全整体防御能力。

第三，变被动防护为主动防护，变静态防护为动态防护，变单点防护为整体防控，变粗放防护为精准防护，这是理念的变化。重要的理论，重要的理念，重要的思路，指导今后若干年在建设网络安全的时候，按照这几个关键词去落实管理措施和技术措施。

第四，重点保护关键信息基础设施、重要信息系统和大数据，保护其安全。

第五，全力推动网络安全产业、企业快速健康发展，打造世界一流的企业群。

第六，最主要的原则，一定要坚决落实三同步。以后再进行网络系统建设，不能先建设后保护，要坚决落实“同步规划、同步建设、同步运行”网络安全保护措施“三同步”要求。这在网络安全等级保护制度当中进一步明确。

中国工程院院士沈昌祥发言：

沈昌祥在《重启可信革命，夯实网络安全等级保护基础》的主题演讲中提到了等级保护 2.0 的时代特征，以及网络安全等级保护新标准的特点：

第一，将基本要求、测评要求和技术要求框架统一，构建在安全管理中心支持下的三重防护结构框架；第二，将云计算、移动互联、物联网、工业控制等列入标准规范；第三，把可信验证列入各级别和各环节的主要功能要求。

公安部信息安全等级保护评估中心马力副研究员发言：

总结了新标准的三个大特点：

第一，2.0 标准覆盖了新技术、新应用的场景，现在比较流行的云计算、物联网等都被纳入到标准范围。

第二，三个核心标准，基本要求、设计要求和测评要求。形成了完全统一的架构：安全通讯网络、安全区域边界、安全计算环境、安全管理中心，一个中心三重防御技术架构。

第三，把可信计算使用写入了标准范围，从一级开始到四级全部提出了可信验证空间。

深信服 CEO 何朝曦发言：

何朝曦发表《全情投入，践行网络安全等级保护 2.0》主题演讲，强调落实网络安全等级保护 2.0，在各方的协同过程中全情投入，共同为中国广大用户的网络安全保驾护航。

为了保障网络安全等级保护 2.0 的建设工作顺利落地，深信服做了充分的准备工作，包括：

第一，通过宣贯、培训帮助用户理解和应用等保方面的知识。

第二，通过产品的创新，场景的适配，向用户交付真正有效果的等保 2.0 方案。

第三，厂商要和监管部门、评测机构和其他厂商通力协作，推进等保 2.0 工作不断发展。

此外，何朝曦表示，厂商落实网络等级保护 2.0 相关政策当中，最应该做的，也最能够做的就是不断改进产品，改进技术，向用户提供的产品和方案更加符合等保 2.0 要求。一方面提高安全效果，同样是防火墙，不同的产品其实安全效果千差万别，为满足等保 2.0 标准那就需要提供真正拦截新型攻击的防火墙。另一方面，用户需要保护的对象还有场景，随着技术的发展呈现了多样性，这些新场景和厂商提供的产品能很好的适配，才能符合相关标的扩展标准要求。也要根据等保 2.0 要求开发匹配新的产品，包括可信计算相关的安全产品，态势感知这些新的产品。

3. 山石网科

3.1 山石云·集 | 山石网科推出满足 NFV 标准的安全网元解决方案

为了应对云环境下的安全挑战，在“2019 中国 SDN/NFV/AI 大会”上，山石网科正式发布了国内首个面向 NFV 标准的安全网元管理方案——山石云·集。

安全与云、SDN 结合面临三大挑战：

挑战 1：批量化、自动化部署难。不同类型 VNF 部署困难，在线扩容难。现有安全设备无法与新的业务架构融合，没有平滑的升级过渡方案。

挑战 2：多厂家对接难。多厂家、多网元故障定位难，多厂家、多网元、多租户环境标准化低。不同安全厂家间存在技术壁垒，没有标准接口和标准方案，无法实现快速落地。

挑战 3：定制化程度高，运维难。云/SDN 与安全设备间消息易丢失、配置易出错，误操作避免难。虽然进行了安全与业务的对接，但后期运维复杂，导致运维成本升高。

以“中间件”方式管理安全网元

针对上述难题，山石网科认为通过 NFV 部署云计算安全，将成为用户最佳选择。

山石云·集是专门针对需要在云计算和 SDN 环境中部署安全能力的场景，可以实现安全设备及 NFV 的自动化部署与管理，并提供开放的标准接口，能快速与第三方云计算和 SDN 环境进行对接，可针对 VNF、PNF 进行配置与资源的管理，具备对接配置的检查和恢复能力的创新产品。山石云·集的理念是通过部署一个安全的中间件，将安全设备与云平台的对接抽离出来，通过安全设备和中间件对接、中间件和云平台对接的方式，为用户提供安全能力。这样，运维人员可以快速通过山石云·集将软硬件的安全能力/安全资源虚拟化后，与云平台进行对接，大量功能逻辑交由中间件山石云·集进行实现，与云平台最大程度上解耦，让安全在 NFV 环境中部署更简单，融合更灵活，运维更高效。

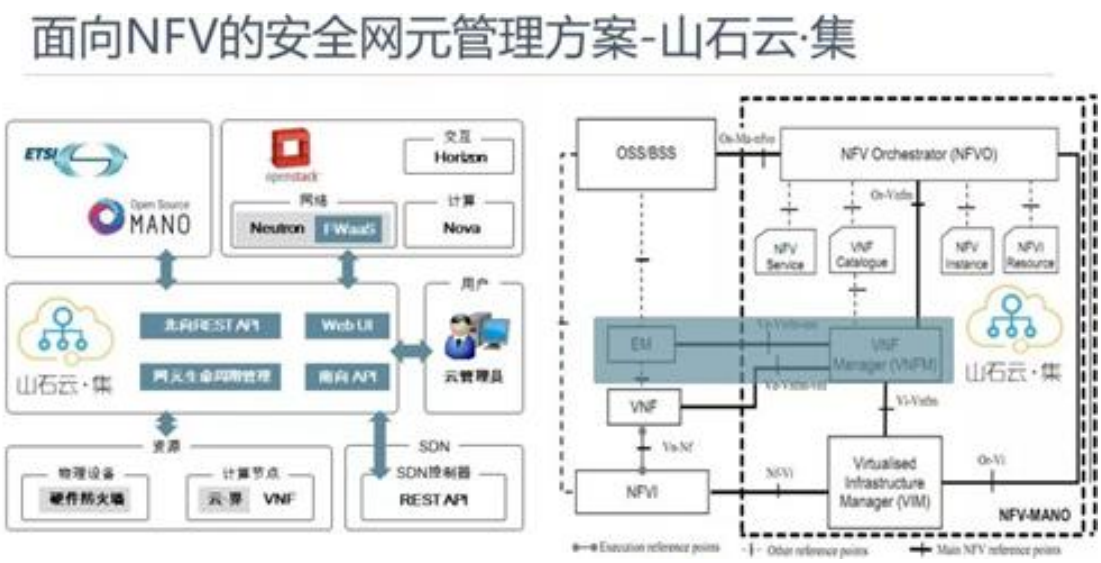
软硬安全资源可灵活调度和管理

山石云·集能够实现全生命周期运维管理：支持多种安全网元初始化方案，解决了安全网元初始化配置问题，使 PNF/VNF 上线更灵活更符合用户需求；配置一致性检测、VPC 互通管理大大减少了运维的工作，使排障更容易，运维更简单；配置备份恢复和网元日志管理，为后期的故障排查和网络优化工作提供了重要依据。

除了可以支持 VNF 网元（vFW 虚拟防火墙）外，山石云·集还可以支持 PNF 网元（硬件防火墙 vSYS）。对于用户重点业务，可以使用硬件防火墙进行安全防护，对于新业务可以使用虚拟防火墙网元进行防护，并且可以支持 PNF 到 VNF 的融合演进。

标准化配置接口是关键

山石云·集在研发过程中的一大挑战是厂商之间对接磨合这个过程，比如与运营商、金融等行业用户一起研究复杂接口如何标准化的问题，最终实现标准化的配置接口。山石云·集遵循 ETSI 定义 NFV 框架及标准，使用 REST API 方式提供服务，易于第三方进行集成，并兼容多个厂家的云计算和 SDN 产品，实现快速对接；兼容标准 OpenStack 的 API 和插件进行对接集成，减少定制化接口，在各厂家 OpenStack 环境间实现解耦，并已与多个厂家的 OpenStack 完成方案对接。



4. 亚信

4.1 亚信出席 C3 安全峰会并发表《5G • 云安全》演讲

作为中国最具影响力、最高规格、聚焦全球视野的国际大型网络安全年度峰会——2019 C3 安全峰会于 5 月 7 日-8 日在成都盛大召开。C3 所代表的 Cyber（网际）、Cloud（云）、Communication（通信）不仅构成了未来网络安全的方向，更象征着 “立体、可控、可视”的安全新机制。

本届峰会以“预建未来——Plan UP”为主题，汇聚全球超过 2500 位 IT 领袖，紧密契合国家网络安全战略，结合 5G、人工智能、物联网、大数据、云安全等新兴技术，针对数字经济发展和产业变革带来的安全需求，分享全球最前沿的安全技术策略展望，深入讨论数字世界面对的各类威胁风险，助力用户打造智能、可靠、安全的网络新场景，共同迎战数字时代下的网络安全风险，一起“预建未来”。

针对 5G 安全的发展与未来，亚信集团董事长田溯宁在《5G • 云安全》的主题演讲中谈到：“在 5G 时代，商业流程会实现从人的连接到物的连接，从知识连接到商业流程的连接将开启产业互联网元年。5G 正在成为产业互联网的基础设施，云网一体化是 5G 时代最重要的特征， IT、OT（Operation Technology，运营技术）与 CT（Communication Technology，通信技术）将实现与 ST（Security Technology，网络安全技术）的深度融合。在实现万物连接之后，开放性、云物一体等 5G 特征也使得网络安全问题变得更加重要。5G 云网是未来所有商业和产业互联网最重要的基础设施。5G 云网时代下需要产业互联网的安全运营商，因为没有安全就没有 5G 云网，就没有未来。”

5G 将开辟移动通信发展的新时代，加速经济社会数字化转型进程。与此同时，5G 网络产生新的信任模型，新的服务交付模式，不断变化的威胁环境以及增加的隐私问题等特征，对安全提出了新的挑战和需求，现阶段亟需加大 5G 安全核心技术研发与突破。

在这种背景下，亚信安全与中国信息通信研究院共同发起，联合中国移动、中国电信、中国联通、中国网安和北京邮电大学成立国内首家 5G 安全协同创新中心。以“产学研用协同创新”模式，面向 5G 安全共性关键技术、产品以及成果转化，搭建创新平台，引领行业发展。建立长效协同创新合作机制，共同进行 5G 安全核心技术联合攻关、共享 5G 安全技术资源、共同编制相关标准、共同申报项目课题、形成联合解决方案并推动场景化应用落地，并对具有市场前景的优势项目进行孵化培育和商用推广。

5. 绿盟

5.1 绿盟云沙箱成为 VirusTotal 官方合作产品

5 月 7 日，VirusTotal 发表正式声明，绿盟科技云沙箱（POMA）成为 VirusTotal 的官方合作产品，旨在可疑文件分析领域强强联合，为客户提供更好的服务。截止目前，VirusTotal 的沙箱合作伙伴，全球仅有七家。

VirusTotal 作为国际知名的安全厂商，以提供可疑文件分析服务著称。绿盟科技云沙箱（POMA）作为绿盟科技威胁情报的重要子产品，对外提供云端威胁分析服务，并为绿盟威胁情报中心持续提供重要的可疑文件情报。

绿盟科技云沙箱（POMA）是由绿盟科技精心打造的一款云端可疑文件分析产品，它可以对 EXE、PDF、Office、JAVA、Flash 等多类型的文件进行静态和动态分析，以发现新型或潜在的攻击行为，并输出完整的分析报告。报告支持 STIX 标准，便于威胁情报的快速共享。

6. 安恒

6.1 2019 数博会 AiLPHA 大数据智能安全平台斩获两项大奖

5 月 26 日，在 2019 中国国际大数据产业博览会上，安恒信息 AiLPHA 大数据智能安全平台斩获“百家大数据优秀案例”，成功入选工信部大数据优秀产品和应用解决方案案例集（2019 年）。 同时，AiLPHA 大数据智能安全平台的核心技术“基于知识图谱的网络攻击自动化关联推理技术”还获得了 2019 数博会领先科技成果奖。

AiLPHA 大数据智能安全平台采用大数据追踪溯源、用户画像、异常聚类和机器学习的智能分析技术，能够有效发现、预警和联动安全设备处置网络安全威胁、异常活动和突发事件，并做到实现全天候重点网站监测，建立智能化的安全大数据搜集、分析、处理体系，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。

针对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，AiLPHA 大数据智能安全平台创新性的采用大数据技术和机器学习，结合场景分析的自学习建模，很好的解决了市面上现有的安全威胁检测类产品和技术的一些难点。

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

7. 奇安信

7.1 补天五星计划发布 跻身全球三大漏洞平台之列

5 月 29 日，2019 补天白帽大会在上海举办。本届补天白帽大会，是奇安信正式成为“国家队”后的首届白帽大会，也是国内规模最大的白帽盛典，大会吸引了国内外上千名网络安全顶尖攻防人才就漏洞技术、安全事件进行了研讨和分享，同时随着“补天五星计划”在大

会上的发布，补天漏洞响应平台跻身全球三大漏洞平台之列，成为国内第一家全面覆盖全品类漏洞的第三方漏洞响应平台。

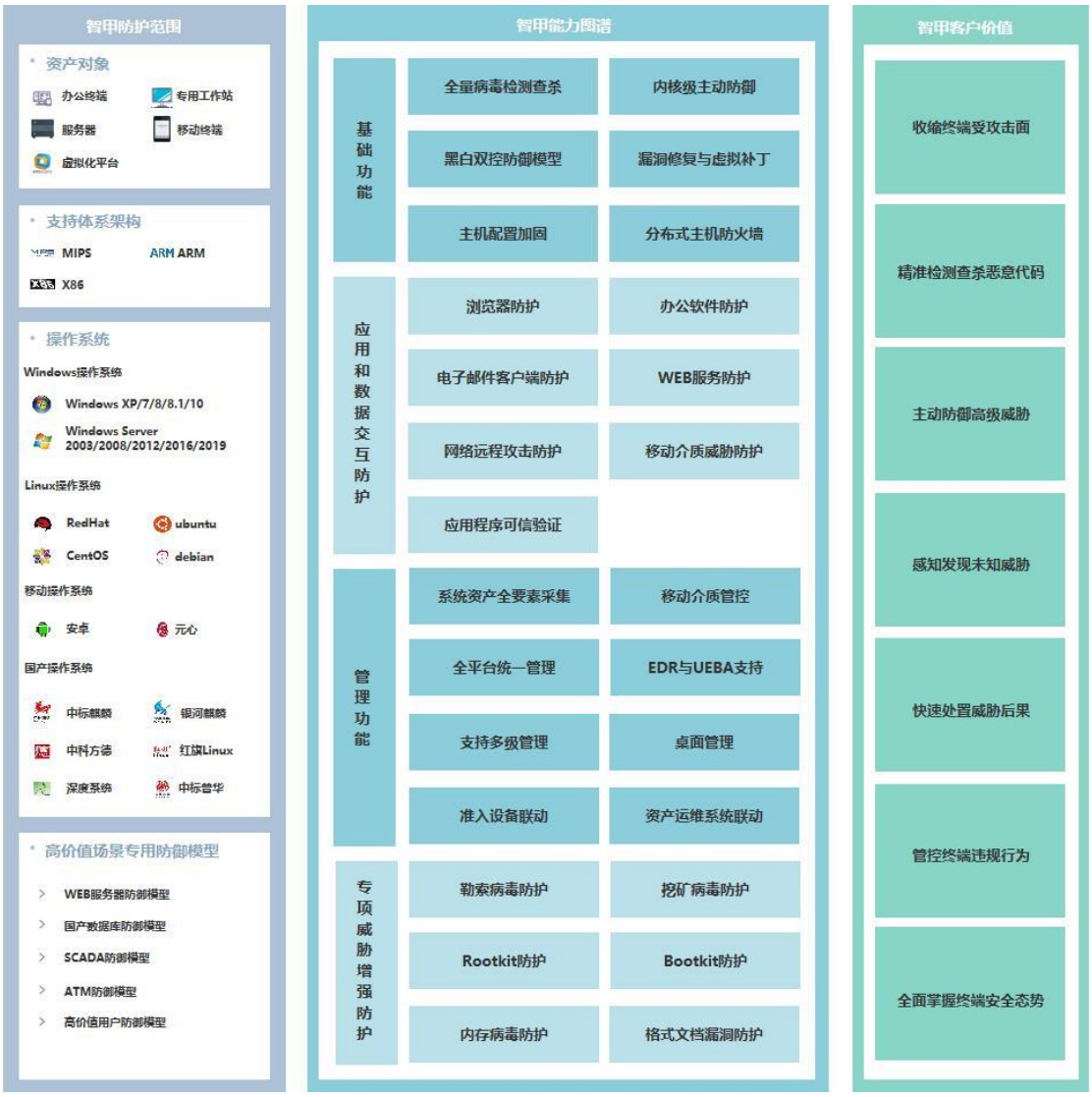
当前，随着物联网、云计算、大数据、5G 等新技术新应用的普及，海量数据大集中的趋势日益明显、企业数据聚集规模快速膨胀，利用漏洞窃取用户数据、加密勒索等网络安全风险日益突出。为此，作为企业和白帽子之间的桥梁，补天漏洞响应平台以“重塑安全属性，再创漏洞价值”为主旨，在 2019 补天白帽大会上隆重发布“补天五星计划”，针对现阶段我国政企机构网络安全所面临的新风险，将漏洞响应范围从原来的 Web 漏洞为主，升级化为 Web、移动 APP、 IOT、工控、操作系统等五大方向，全面覆盖了新一代网络安全环境下的各种漏洞风险，补天平台也由此成为国内第一家覆盖全品类漏洞的第三方漏洞响应平台。

补天漏洞平台致力于做好三件事：维护企业网络安全、降低漏洞被利用的风险、培养网络安全人才。补天漏洞响应平台是中国新一代网络安全公司奇安信集团旗下平台。目前，补天平台目前的白帽子注册数量已经超过 5 万多名，收集的漏洞总数已经突破 34 万，漏洞涉及到的企业多达 7 万多家。”

8. 安天

8.1 安天展示智甲终端防御系统方案

安天集团产品与解决方案全国巡展首站于成都世纪城洲际大饭店成功举办，期间安天展示了全平台终端防御解决方案--安天智甲终端防御系统。



端点系统面临多种流行安全威胁，如勒索病毒、挖矿病毒、内核级木马、格式文档漏洞攻击等。安天智甲终端防御系统支持各种体系结构和操作系统平台，对桌面、工作站、服务器、移动终端、虚拟化等端点场景提供安全防护。为客户提供病毒与恶意代码查杀、威胁主动防御、补丁修复、配置加固等防护功能。对浏览器、电子邮件等入口进行交互防御，对 Office 等软件遭遇的格式漏洞攻击进行特别保护，对 USB 等介质攻击进行保护。具有精准检测防御海量已知威胁的能力和较强未知威胁发现和主动防御的能力，可有效收缩终端受攻击面，有效支撑安天资产运维平台和战术型态势感知的数据采集和响应行动。

智甲采用可信计算与安天下一代反病毒引擎组合构建的黑白双控模式，对引导链和执行对象的行为活动和网络通讯进行检测过滤，针对各种服务器、重要工作站、SCADA 站、ATM 等场景具有专用的防御策略模板。

安天智甲全面支撑各种国产 CPU 和操作系统组合的主机环境防护，参与了专用机病毒防治标准规范的研讨，并率先研发出符合专用机病毒防护要求的产品——安天智甲专用机版，

其在国产 CPU 和国产操作系统的基础架构之上，深度契合专用机的系统特性，从行为、边界、网络等多个层面为涉密专用机提供了全面的安全防护能力。在国产化领域，安天智甲深度结合国产化系统特点，全面覆盖国产化系统平台。

四、 容器技术及安全动态

1. Helm 3.0 alpha 版本发布

经过了长时间的开发，Helm 3 终于发布了第一个 alpha 版本,新版本特性如下：

移除 Tiller

Helm 2 是 C/S 架构，主要分为客户端 helm 和服务端 Tiller；Tiller 用于在 Kubernetes 集群中管理各种应用发布的版本; Helm3 同样在 Release 页面提供了预编译好的二进制文件。差别在于原先的二进制包下载下来你会看到 helm 和 tiller。而 Helm3 则只有 Helm 的存在了。

在 Helm3 中移除了 Tiller 后，版本相关的数据直接存储在了 Kubernetes 中。现在我们直接在一个新创建的集群上使用 Helm3，而不再需要部署 tiller。

Helm 的权限与当前的 Kubeconfig 中配置用户的权限相同，非常容易进行控制。这样也大大增强了使用 Helm 的安全性。

chart 的版本名称现在作用于命名空间

随着 Tiller 的删除，每个版本的信息都必须在某处。在 Helm 2 中，它存储在与 Tiller 相同的命名空间中。实际上，这意味着一旦某个版本使用了某个名称，其他版本就不会使用相同的名称，即使它部署在不同的名称空间中也是如此。

在 Helm3 中，有关特定版本的发布信息现在存储在与版本本身相同的命名空间中。这意味着用户现在可以在两个单独的命名空间中安装 wordpress stable / wordpress，并且可以通过更改当前命名空间上下文来引用每个命名空间列表。

使用 JSONSchema 验证 chart 值

现在可以对 chart 值强加 JSON 模式。这可确保用户提供的值遵循 chart 维护者设置的模式，从而在用户为 chart 提供不正确的值时提供更好的错误报告。会在 helm install、upgrade、template、lint 这几个命令下触 chart 发值的验证。

库 chart 支持

Helm 3 支持一类称为“库 chart”的 chart。这是由其他 chart 共享的图表，和程序开发

中的公共库类似。库 chart 的模板只能声明定义元素。简单地忽略全局范围的非定义内容。这允许用户重复使用和共享可在多个图表中重复使用的代码片段，从而避免冗余并保持图表简洁性。

CLI 命令更新

helm inspect -> helm show

helm fetch -> helm pull

helm delete --purge -> helm uninstall

helm delete -> helm uninstall --keep-history

其他更新

将 requirements.yaml 合并到 Chart.yaml 中；

helm3 执行应用安装时需要名称（或--generate-name）

移除了本地 chart 仓库 helm serve

chart 可推送到 docker registry 仓库（试验状态）

2. Docker 企业版 3.0 发布

近日，Docker 在 DockerCon 2019 大会上发布了 Docker Enterprise 3.0，并称该平台是唯一的桌面到云企业容器平台，使企业能够构建和共享任何应用程序并在任何地方安全地运行它们，从混合云到边缘。

Docker 表示，借助 Docker Enterprise 3.0，开发人员可以直接从桌面构建基于容器的多服务应用程序，并以标准格式打包，可以无缝共享并在任何地方运行。此外，Docker Enterprise 3.0 通过引入自动化生命周期管理和增强安全性的新功能，扩展了其容器平台的领导地位。

Docker Enterprise 3.0 引入了 Docker Kubernetes 服务，这是唯一一款将 Kubernetes 从开发人员桌面集成到生产服务器的产品。这将使 Kubernetes 更容易，更安全，并且更容易被整个企业访问。

运行 Kubernetes 1.14：DKS 包括最新版本的 Kubernetes，包括对容器存储接口（CSI）的全面支持。

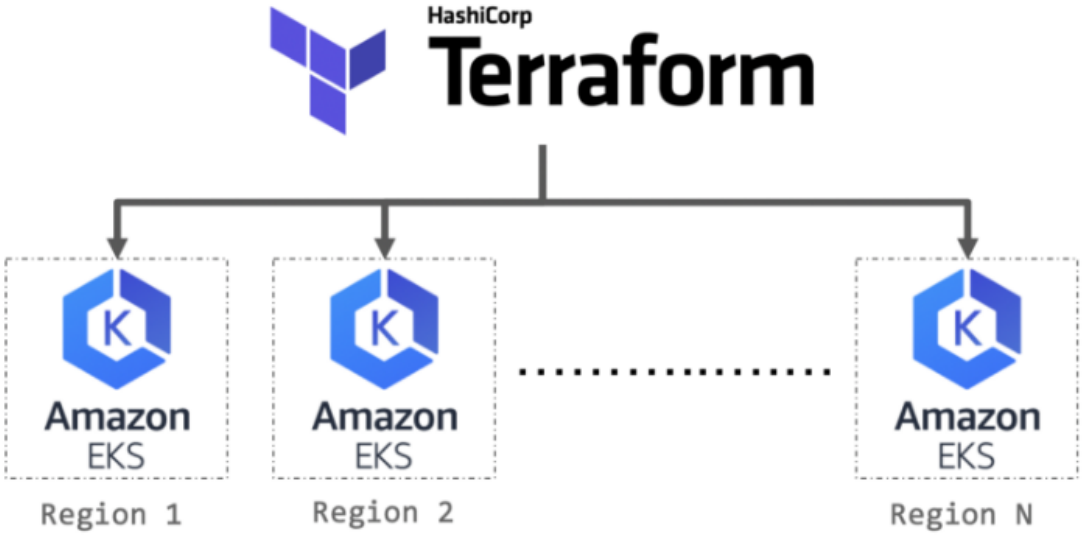
面向开发人员和运营商的单一平台：DKS 是唯一一款在整个开发生命周期内提供一致性的 Kubernetes 产品。通过使用版本包，Kubernetes 开发人员环境与生产环境保持同步，实现完整，无缝的 Kubernetes 体验。

3. kubeCDN：基于 Kubernetes 的自托管 CDN

它是一个基于 Kubernetes 的自托管 CDN 方案，自托管也就意味着我们可以完全控制自己的基础设施。通过 kubeCDN，我们不再需要第三方的内容分发网络，重新控制了从服务器到用户设备的数据流。

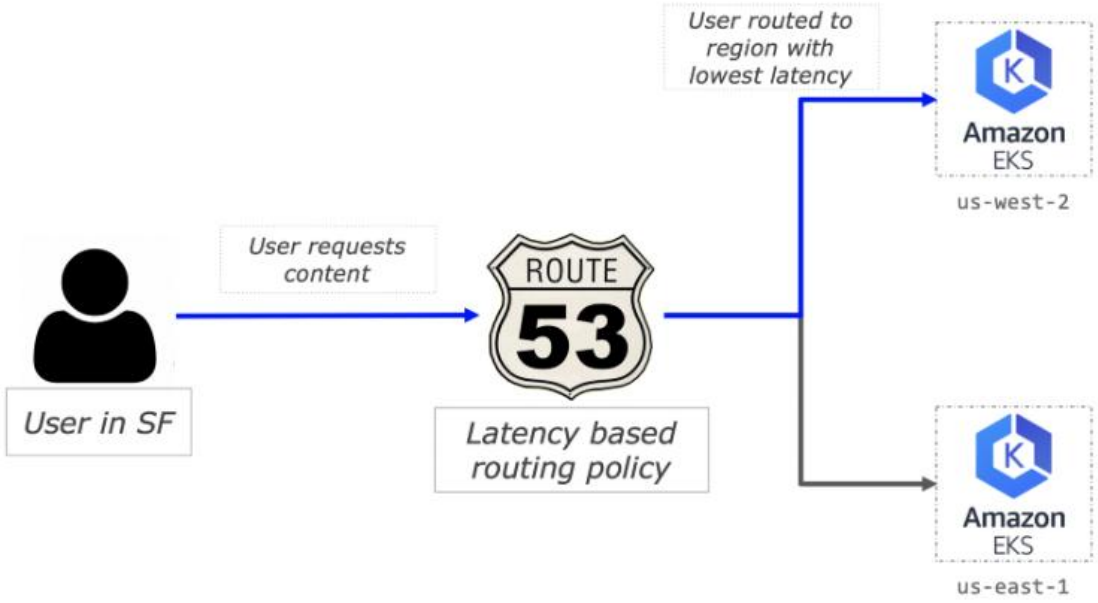
kubeCDN 使用 Terraform 在选定的区域部署 EKS 和其他 AWS 基础设施组件。Route53 是 AWS 提供的云域名系统（DNS），用于多区域用户间的路由；ExternalDNS 用于在部署新服务时自动创建 DNS 记录。

下图演示了如何使通过 Terraform 来部署 kubeCDN。



Terraform 用于部署 kubeCDN 所必需的基础设施，而 Route53 用于将用户流量路由到特定区域。为了演示 kubeCDN，作者在两个 AWS 区域（us-east-1 和 us-west-2）中分别部署了一个视频服务器，然后在 Route53 上设置了一个托管区域，并为集群的每个区域都设

置了 A 记录。作者采用了基于延迟的路由策略，从而将用户路由到能够为他们提供最低延迟的区域。在此演示中，用户总是被路由到地理上最接近的区域。然而，实际情况可能并非总是如此。因特网上的延迟可以随着时间而改变，当采用基于延迟的路由策略时，Route53 可以利用这些监测数据来确定如何路由用户。



kubeCDN 使用 Route53 将用户流量路由到延迟较低的区域。上图演示了 Route53 如何通过两个区域中的集群来路由用户流量。旧金山的用户被路由到 us-west-2 中的集群，因为该区域提供了更低的延迟。

kubeCDN 还可以使用 Route53 中一些别的路由策略，从而满足不同应用程序的需求，详情参阅：https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

五、 安全新产品及技术

1. “等保 2.0”正式发布，12 月 1 日正式实施

2019 年 5 月 13 日下午，国家市场监督管理总局召开新闻发布会，期待已久的等保 2.0 正式发布。根据最新的消息，等保 2.0 将在 2019 年 12 月 1 日正式实施。

“等保 1.0”的时代于 2008 年正式拉开帷幕，经过 10 余年的实践，为保障我国信息安全打下了坚实的基础，但从现实考量已经逐渐开始不适应网络环境的变化。为适应新技术的发展，解决云计算、物联网、移动互联和工控领域信息系统的等级保护工作的需要，由公安部牵头组织开展了信息技术新领域等级保护重点标准申报国家标准的工作，等级保护正式进入

2.0 时代。我们预计，等保 2.0 标准即将正式发布，整个信息安全行业需求将在 2019 年迎来重要的边际改善。

中国工程院院士沈昌祥表示： “等级保护由 1.0 到 2.0 是被动防御变成主动防御的变化，依照等级保护制度可以做到整体防御、分区隔离；积极防护、内外兼防；自身防御、主动免疫；纵深防御、技管并重。”

“等保 2.0”在技术标准上，云计算、大数据等技术列入新标准体系。据中国公安部官员介绍，下周一发布的 2.0 版本将针对新技术提出扩展性要求，在聚焦于等级保护的基本要求时，更多用技术思维解读标准。

中国的网络安全等级保护技术 1.0 版本主要强调物理主机、应用、数据、传输，2.0 版本将在云计算、大数据、物联网、工业控制系统等新技术新应用方面有涉及。

从等保 1.0 到等保 2.0，变化体现在多个方面，差异主要体现在：

（1） 体系框架和保障思路的变化

（2） 定级对象的变化

（3）测评的变化

（4） 等保要求的组合变化

（5）控制点和要求项的变化

“等保 2.0″不仅增加了大量重要要求项， 也将彻底改变我国信息安全市场的面貌。

2. Windows 再曝“WannaCry”级漏洞

在 WannaCry 两周年之际，Windows 再次被曝出存在高危远程漏洞。5 月 15 日，微软发布了针对远程桌面服务的远程执行代码漏洞 CVE-2019-0708 的修复程序。这个漏洞触发无需用户交互，攻击者可以利用该漏洞制作类似于 2017 年席卷全球的 WannaCry 类的蠕虫病毒，进行大规模传播和破坏。只要 POC 放出，就能够在大多数人没来得及更新的情况下重演 WannaCry。不过目前为止，还未发现任何恶意行为利用这个漏洞，GitHub 上出现不少利用这个消息骗 Star、钓鱼或者进行恶作剧。

3. 英特尔再曝漏洞，影响 2011 年以来几乎所有产品

在 Meltdown、Spectre 和 Foreshadow 之后，英特尔处理器又被发现严重漏洞 ZombieLoad，影响 2011 年以来几乎所有处理器。黑客可利用这个漏洞获取英特尔处理器最

近访问过的任何数据，且不会在日志文件中留下记录，普通的安全软件也很难检测到这些攻击。目前，英特尔已经发布漏洞补丁，并联合各计算机厂商分发。英特尔表示，对于大多数 PC 而言，更新补丁对性能的影响很小。

4. Windows 10 出现新 0day，任务计划进程可用于攻击

漏洞开发人员 SandboxEscaper 在微软最近一次安全更新之后的一周，放出了一个 Windows 操作系统的 0day 漏洞。该漏洞于去年 8 月份出现，能够使外部攻击者获取本地权限以及允许访客用户取得 SYSTEM 和 TrustInstaller 等全权限用户的文件。

此次漏洞出现在 Task Scheduler 程序中（即任务计划进程），可通过该漏洞从其他系统中倒入遗留任务。早在 Windows XP 时代，该任务就可以以.JOB 格式存在，至今，仍然可以将其添加到新的操作系统中。

当 Task Scheduler 导入任意具有 DACL（自主访问控制列表）控制权限当 JOB 文件时，在缺少 DACL 的情况下，系统会授予任何用户对文件的完全访问权限。

对此，研究人员解释，通过将遗留任务文件导入 Windows 10 上的任务计划进程中时，从旧系统中复制可执行文件“schtasks.exe”和“schedsvc.dll”并运行，便可导致远程过程调用（RPC）到“_SchRpcRegisterTask”中，这是一种任务调度程序服务公开向服务器注册任务的方法。

Dormann 确认了漏洞利用代码，并且表示它在 2019 年 5 月更新之后的 Windows 10 x86 系统上无需任何修改即可使用，成功率为 100%。

5. 新指纹识别技术漏洞曝光：可跟踪 Android 和 iOS 设备

据美国科技媒体 ZDNet 报道，一项新的设备指纹识别技术可以使用出厂时设置的详细传感器校准信息，跟踪互联网上的 Android 和 iOS 设备的上网情况，任何应用或网站都可以在没有特殊权限的情况下获取这些信息。这种新技术称为校准指纹识别攻击，由于无需获取特殊权限，因此用户无法察觉这种类型的跟踪。用户可以通过网页查询自己的设备是否易受攻击。

六、 网络安全投融资、收购事件

1. 收购

1.1 Elevate Security 完成对 Phish5 的收购

5 月 2 日，Elevate Security 完成对 Phish5 的收购，收购价未公开。Elevate Security 成立于 2017 年，构建一个对员工进行培训和行为分析平台，防止员工违规行为。Phish5 旨在开发以易用性著称的网络钓鱼模拟软件，能够帮助企业改进和衡量电子邮件安全。

1.2 KnowBe4 宣布收购 CLTRe AS

5 月 21 日，KnowBe4 宣布收购 CLTRe，通过 CLTRe 的产品中增加了自身衡量安全态势的能力。CLTRe 致力于帮助用户评估、构建、维护和衡量的安全态势，将继续作为 KnowBe4 的独立子公司运营。

2. 投融资

2.1 HyperQube 获 50 万美元种子轮融资

5 月 8 日，HyperQube 从 Adam Ghetti 和其他 5 位投资者处获得 50 万美元的种子轮融资。HyperQube 是一家专注于“网络即服务”的安全厂商，使企业能够快速和轻松地构建 IT 基础架构。

2.2 Siemplify 获 3000 万美元 C 轮融资

5 月 20 日，Siemplify 从 83North 和其他 3 位投资者处获得 3000 万美元的 C 轮融资。Siemplify 是一家专注于安全编排，自动化和响应（SOAR）的服务提供商，帮助全球客户企业安全运营。

2.3 GuardiCore 获 6000 万美元 C 轮融资

5 月 20 日，GuardiCore 从 83North 和其他 7 位投资者处获得 6000 万美元的 C 轮融资。Guardicore 是一家云安全解决方案提供商，专注于保护大中型企业的数据中心安全，为用户提供安全的云基础架构平台。