国内外云计算+安全动态报告

2018 年第 12 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 推出多项新功能支持，推出适用于 Windows Server 1809 版本的 EC2 AMI,Amazon MQ 推出代理网络功能,AWS Server Migration Service 添加了对多服务器迁移的支持,Amazon EKS 针对 Kubernetes 版本 1.11 推出托管集群更新和支持功能,推出全新 Amazon DynamoDB 密钥诊断库,Amazon EC2 推出分区置放群组，并且 AWS Storage Gateway 宣布提高吞吐量并新增缓存功能，以及 Amazon MQ 目前支持 PCI 和 ISO 合规计划； VMware 与腾讯云携手推出黑石 Stack-V 混合云解决方案；Azure 复原能力提升；阿里则又做调整，蚂蚁金服迎回原阿里云总裁胡晓明；腾讯云发布新一代移动金融开发平台 开发效率提升 200%。

开源云方面，江苏农信上线首个大规模 OpenStack 农信云平台；EasyStack 助力证券行业打造金融云平台，包括中山证券、深圳证券、国泰君安等；九州云亮相全球云计算大会，推动工业物联网升级换代。

云安全厂商方面，启明星辰集团携手天津飞腾打造高性能自主可控网关型产品，成为华为首批终端安全奖励计划合作伙伴，同时多项产品夺得佳绩，启明星辰泰合 TSOC 平台再次入围 Gartner SIEM 魔力象限，启明星辰云子可信助力中小微企业创新转型，启明星辰 VenusEye-威胁情报中心赋能安全渐入佳境；深信服 EDR 助力军工行业信息化；山石网科被 Gartner 评选为亚太地区企业级防火墙全球性厂商；亚信安全入选安全牛威胁情报矩阵、态势感知矩阵；绿盟科技“安全运营+”体系发布；安恒 EDR 新版本正式发布；360 企业安全被 IDC 评为中国威胁情报市场的领导者；赛门铁克携手 Fortinet 推出云安全服务。

容器动态方面，Kubernetes1.13 版本发布，此版本继续关注 Kubernetes 的稳定性与可扩展性；Rancher、ARM 联合推出物联网、边缘计算、K8S 平台；Kubernetes 爆安全漏洞，集群升级是唯一解决之道；微软发布通知，Azure 容器服务 ACS 要暂停，聚力 kubernes 平台，提醒用户做好迁移准备。

安全新技术方面，多项重要安全相关文件发布，公安部网络安全保卫局发布《互联网个人信息安全保护指引（征求意见稿）》，工信部发布 2018 年第三季度网络安全威胁态势分析与工作综述，信通院发布《车联网白皮书（2018）》，网信办发布《金融信息服务管理规定》；多项安全新技术也得到发布，基于 AI 构建的免费恶意软件检测平台 SNDBOX 上线，微软发布针对专业版和企业版 Windows 10 的 Windows Sandbox；与此同时，苹果发布 iOS 12.1.1 更新，修复了密码绕过漏洞、RCE 漏洞等问题，CNNVD 关于微软多个安全漏洞的通报。

网络安全投融资方面，仅分别有 1 起收购事件和 1 起融资事件。安全运营中心即服务公司 Arctic Wolf Networks 收购网络风险平台公司 RootSecure。家为企业提供云端数据安全的技术公司 Avanan 则获得 2500 万美元的 B 轮融资。

2018 年 12 月 29 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 云安全动态

1.1 推出适用于 Windows Server 1809 版本的 EC2 AMI

12 月 4 日，AWS 推出适用于 Windows Server 1809 版本的已包含许可证 (LI) 的 Amazon 系统映像 (AMI)，让客户可以方便灵活地获得和运行最新的 Windows Server 半年频道版本。该版本 Windows Server 包括对容器和 Kubernetes 的改进支持，最适合于构建基于容器和微服务的现代化 Windows 应用程序等使用案例。

通过在 Amazon EC2 上运行 Windows Server 1809 版本，客户可以将 AWS 的规模、性能和弹性与最新的 Windows Server 半年频道版本的新功能完美结合。已包含许可证 (LI) 的 Windows Server 1809 版本 AMI 现已在所有公有 AWS 区域开放，可以从 Amazon EC2 控制台直接启动。运行 Windows Server 1809 版本 AMI 的实例将按标准的 Windows 定价收费。

1.2 Amazon MQ 目前支持 PCI 和 ISO 合规计划

12 月 5 日，可以使用 Amazon MQ 在符合 PCI 规范或需要 ISO 认证的应用程序之间收发消息。Amazon MQ 是一种适用于 Apache ActiveMQ 的托管消息代理服务，能够轻松地在云中设置和操作消息代理。

Amazon MQ 现在符合 PCI DSS，这意味着您可以使用它来处理、存储或传输付款信息。可以在 AWS Artifact 中下载 PCI 合规性文件包，以详细了解如何在 AWS 上实现 PCI 合规性。

此外，Amazon MQ 也通过了 ISO 9001、27001、27017 和 27018 认证。这些认证是全球公认的安全标准，能够证实云的质量和信息安全管理得到保证，且个人身份信息受到保护。

除了满足 PCI 合规和 ISO 认证计划标准之外，Amazon MQ 还符合 SOC 标准，并在 HIPAA 合格范围之内。

1.3 AWS Server Migration Service 添加了对多服务器迁移的支持

12 月 6 日，AWS Server Migration Service (SMS) 现在提供多服务器迁移支持，使应用程序从本地数据中心迁移到 Amazon EC2 更加容易且经济高效。用户可以将一组服务器作为单个单元迁移，而不必费力协调单个服务器的复制或解耦应用程序依赖关系。通过多服务器支持，Server Migration Service 显著缩短了迁移应用程序所花的时间，并降低了迁移过程出错的风险。

AWS Server Migration Service 是一种无代理服务，使用户能够更轻松、更快速地将本地工作负载从 VMware vSphere 和 Microsoft Hyper-V 环境迁移到 AWS。它可让用户自动执行实时服务器卷的增量复制、为其制定计划以及进行跟踪，从而能够更轻松地协调大规模服务器迁移。通过多服务器支持，用户首先可以将服务器划分成多个应用程序组（例如，按 Web 前端、应用程序服务器和数据库服务器分组）。之后，Server Migration Service 同步并一致地复制应用程序中的所有服务器，并且会自动生成 CloudFormation 模板，该模板可随时用于在 EC2 中启动复制的应用程序。

1.4 EKS 针对 Kubernetes 版本 1.11 推出托管集群更新和支持功能

12 月 12 日，Amazon Elastic Container Service for Kubernetes (EKS) 现已可针对 Kubernetes 版本进行托管式就地集群升级。此外，Amazon EKS 现已可支持 Kubernetes 版本 1.11.5。

Kubernetes 目前的发展非常迅速，功能发布及漏洞修复工作开展得十分频繁。之前，要在不同的 Kubernetes 版本之间进行迁移，用户需要手动执行包含多个步骤的更新过程，或创建新的集群，然后再迁移应用程序。由于这些过程耗时冗长，很可能会导致应用程序停机。

现在，借助 Amazon EKS，可以轻松地将集群更新到最新版本的 Kubernetes，而无需管理更新过程。Kubernetes 版本更新可就地完成，因而用户无需创建新集群或将应用程序迁移至新集群。 Kubernetes 版本 1.11.5 适用于所有新集群，而且 Amazon EKS 集群更新支持用户将所有现有集群迁移至版本 1.11.5。

用户可以通过调用 update-cluster-version API 或使用 EKS 控制台中的“更新集群版本”按钮，将新版本的 Kubernetes 应用于集群。 也可以通过调用 describe-updates API，来详细了解正在进行的更新的状态；还可以通过调用 list-updates API，来查看正在进行的更新。

1.5 AWS Storage Gateway 宣布提高吞吐量并新增缓存功能

12 月 12 日，AWS Storage Gateway 面向文件网关发布了多项增强功能，包括提高的性能、选择性刷新网关缓存分区的选项，以及配置 DNS 和 NTP 设置的能力。

文件网关支持本地应用程序通过在虚拟或硬件应用程序上部署的本地网关以访问文件的形式访问 Amazon S3 中的对象。按照以下发布的最佳实践，现在可以实现高达 500MB/s 的写入吞吐量。

1.6 推出全新 Amazon DynamoDB 密钥诊断库

12 月 13 日，Amazon 发布了 Amazon DynamoDB 密钥诊断库，可提供近乎实时的 DynamoDB 密钥使用信息。该库为轻量级客户端实用工具，可帮助用户分析表格流量并显示可视化内容，包括每个分区密钥的读写次数。通过使用该库，可以几乎实时调整到不可预测和不均匀的工作负载。

1.7 Amazon MQ 推出代理网络功能

12 月 19 日，用户现在可以使用 Amazon MQ 设置高度可用的代理网络，跨 AWS 可用区和区域连接多个消息代理。代理网络可提高消息代理的可用性和可扩展性，是受停机时间影响极大的关键任务型应用程序的理想选择。

Amazon MQ 是一种适用于 Apache ActiveMQ 的托管消息代理服务，让用户能够轻松地在云中设置和操作消息代理。消息代理提供企业应用程序之间的通信主干。应用程序使用 Amazon MQ 代理网络连接到网络中的节点，如果某个节点发生故障，可以在几秒

1.8 Amazon EC2 推出分区置放群组

12 月 20 日，AWS 推出了分区置放群组，这是一种全新的 Amazon EC2 放置策略，有助于降低与大型分布式和复制的工作负载（如 EC2 上运行的 HDFS、HBase 和 Cassandra）相关的故障可能性。分区置放群组在逻辑分区之间传播 EC2 实例，并确保不同分区中的实例不共享相同的底层硬件，从而将硬件故障的影响限制在单个分区中。此外，分区置放群组提供了对分区的可见性，并允许拓扑感知应用程序使用此信息，以做出智能数据复制决策，从而提高数据可用性和持久性。

2. VMWare 云安全动态

2.1 VMware 与腾讯云携手推出黑石 Stack-V 混合云解决方案

12 月 5 日，全球企业软件创新领导者 VMware（NYSE: VMW）与全球领先的云计算服务提供商腾讯云宣布达成合作，双方共同打造的混合云服务平台——腾讯云黑石 Stack-V 正式交付使用，且双方合作取得实质性进展。根据合作协议，腾讯云基于黑石 IaaS 基础框架，深度融合 VMware 在计算、网络、存储等方面的领先技术和资源优势，构建更符合中国市场客户需求的服务产品，以强强联合、互补共赢的方式将该混合云解决方案共同推向市场。

黑石 Stack-V 可以直接减轻企业上云的技术障碍，方便用户以更加简单、便捷的方式将业务拓展至公有云，同时也将显著丰富腾讯云的混合云解决方案，提升腾讯云在金融、政府、制造业、传媒业等行业和领域的混合云服务能力。作为领先的云计算服务提供商，腾讯云在国内公有云产品和服务方面拥有深厚的技术积累以及领先的市场优势。目前，腾讯云黑石数据中心已运营数万台黑石服务器，积累了海量运营经验和众多企业客户，在布局上也完成了北京、上海、广州等全国核心节点的覆盖。

3. GOOGLE 云动态

暂无消息。

4. 微软 Azure 云动态

4.1 机器学习+在线迁移=Azure 复原能力 UP

微软 Azure 团队致力于确保用户部署在 Azure 上的业务得以持续可靠地运行。为了优化 Azure 的可靠性，他们和微软亚洲研究院合作，利用机器学习来预测潜在的故障，并使用在线迁移技术提前缓解故障的影响。

自 2018 年初以来，Azure 一直采用在线迁移技术来应对各种各样的故障场景， 比如硬件故障、机架维护和软件/BIOS 更新等常规操作过程中出现的错误等。借助在线迁移，Azure 能够从容处理故障，并将故障的影响降低了 50％。

尽管如此，想要进一步拓展在线迁移的应用领域，仍需要探究如何利用系统中的有效预测信号来挖掘在线迁移的用武之地。基于集群管理系统的各种监控数据，微软研究员实现了基于机器学习的故障预测模型，通过与自动在线迁移技术相结合，该故障预测模型被应用在了磁盘故障、IO 延迟和 CPU 频率异常等多种硬件故障情况的处理中。

微软 Azure 团队与微软亚洲研究院联袂打造的高精度故障预测的机器学习模型，能够在出现故障迹象之前就把正在运行的任务从“有风险”的机器上迁移出去，这也就意味着在 Azure 上运行的虚拟机比底层硬件还要可靠。

利用这个模型，在线迁移对虚拟机的影响被控制到了最低。从客户的反馈来看，虚拟机在线迁移从未引发任何问题。在线迁移的过程中，虚拟机的状态和所有网络连接能够都保持正常。迁移的最后阶段，虚拟机会暂停几秒，继而迁移至新的主机。只有极少量对性能敏感的任务可能会在虚拟机暂停前的几分钟内受到轻微影响。

5. 阿里云动态

5.1 阿里又做调整，蚂蚁金服迎回总裁胡晓明

本周一张勇通过内部信的形式宣布了集团 CTO 张建锋担任阿里云智能事业群总裁，同时对原阿里云总裁胡晓明的去向卖了个关子。结果周四晚间就正式宣布阿里云原总裁胡晓明出任蚂蚁金服集团总裁，向董事长兼 CEO 井贤栋汇报。井贤栋在邮件中热烈欢迎胡晓明回归，并表示胡晓明的回归是蚂蚁金服组织架构的重大升级。之所用用“回归”二字，是因为颜值堪称阿里领导团队 TOP10 之一的胡晓明，在 2005 年加入阿里巴巴时，任职的就是蚂蚁金服首席风险官，他对支付宝、蚂蚁金服的创建及发展功不可没。

6. 腾讯云动态

6.1 腾讯云发布新一代移动金融开发平台 开发效率提升 200%

12 月 20 日，腾讯云在北京正式发布了新一代移动金融开发平台 TMF（Tencent Mobile FinTech Platform），整合腾讯在移动产品开发、测试、发布、运营上的成熟技术能力，能够为多场景下的移动金融应用开发提供全生命周期的支撑和管理，帮助金融机构低成本、高效率地构建移动金融服务。

腾讯金融云总经理胡利明介绍，腾讯云新一代移动金融开发平台 TMF 针对移动金融产品体验差、玩法少、渠道单一等痛点问题打造，将着力帮助金融机构打造真正高价值的移动金融服务应用。

腾讯云新一代移动金融开发平台 TMF 会在底层提供囊括开发框架、运维系统、运营体系、安全组件在内的统一开发平台，并在此基础上提供丰富的传播、场景以及 AI 工具箱。银行、保险、证券以及互联网金融等机构可以在统一的开发平台下，以一套代码打造覆盖多端的金融服务应用，避免 App、微信公众号、小程序、H5 多端重复功能开发。开发过程中还能灵活调用平台中丰富的组件库和即插即用的工具箱，避免基础组件的二次开发。

7. 华为云动态

暂无消息。

二、 开源云动态

1. Openstack 动态

1.1 江苏农信上线首个大规模 OpenStack 农信云平台

江苏省农村信用社联合社(简称江苏农信)是经中国人民银行批准成立的江苏地区最大的金融机构。目前省联社在全省共有法人单位 62 家，营业网点 3257 个。

自 2016 年始，江苏农信一直在开源云计算领域不断探索进取，期望构建——用于大幅提升开发测试效率，并逐渐实现 Devops 开发测试云，旨在提高整体生产效率的作业云，基于高效云服务的“互金产品”生产云，以及覆盖全省二级农商行的 OpenStack 农信共享行业云。

两年前，江苏农信正式进入大规模云计算环境规划阶段，并充分考察了市场上多种技术类型和几乎所有云厂商的私有云解决方案。最终敲定开源路线，是因为江苏农信更看重开源生态的繁荣，开源技术的先进性，以及开源产品的兼容性。在厂商选择方面，最终江苏农信选择携手易捷行云 EasyStack，打造中国首个服务三农的大规模 OpenStack 农信云，拥抱以 OpenStack、Ceph 等为基础的开源云计算技术，成为金融行业最佳实践的标杆案例。

2. Easystack 动态

2.1 EasyStack 助力中山证券打造金融云平台

作为证券行业首个采用 OpenStack 生产云的企业，中山证券选了 ECS 易捷行云企业云，该私有云平台也是金融行业首家采用 Neutron AZ 实现物理分区的云平台。

随着云计算的不断深入，证券行业对信息技术的研究和探索从原有的概念到实际应用都取得了实质性的发展，越来越多的证券公司开始考虑将传统 IT 基础设施迁移到私有云上，纷纷启动云平台建设项目。

从 2017 年开始，中山证券就启动了以 OpenStack 技术为基础的生产云平台建设，成为中国第一家在生产数据中心应用 OpenStack 构建私有云的证券公司。同时，在生产云建设中，中山证券采用了 Neutron Availability Zone(Neutron AZ)技术，也成为中国金融行业内首家采用 Neutron AZ 实现物理分区的企业。可以说，在尝试创新技术方面，中山证券两次开创了业界先河。

2.2 EasyStack 助力深圳证券信息构建私有云平台

深圳证券信息选择 EasyStack 的 ECS 易捷行云企业云构建金融私有云平台，深圳证券信息也是中国证券行业最早一批构建私有云的企业。

作为国内唯一具备主板上市公司、中小企业板上市公司等多层次资本市场信息披露业务资质的信息服务机构，深圳证券信息是国内最早的证券信息服务专业公司。同时，作为掌握中国证券行业风向标的机构，深圳证券信息也是中国证券行业最早一批构建私有云的企业。

伴随金融科技及业务创新的发展，证券行业快速步入数字化转型时代。作为国内证券业的发源地，深圳证券交易所已成为中国最具代表性的证券交易平台，截至 2018 年底，交易规模达到 1350 亿元。其中，经深圳证券交易所授权，国内最早的证券信息服务公司——深圳证券信息有限公司（深圳证券信息）承担着深圳证券交易所证券交易实时行情、上市公司信息公告的发布、经营和管理等关键业务。

未来，深圳证券信息将会把更多的工作负载将迁移到云平台上，不断将云计算技术融入业务环境之中，满足公司对业务创新的需求，实现公司数字化转型。

2.3 国泰君安借 EasyStack 打造金融云平台

国泰君安作为中国证券业全面领先的综合金融服务商，多年来始终以客户为中心，深耕中国市场，为个人和机构客户提供领先的综合金融服务。与此同时，国泰君安高度重视对信息科技的战略性投入，持续推进数字化转型创新，在信息技术推动证券业务发展上有着长远规划和思考。

国泰君安证券金融产品交易综合服务平台具备技术自主化、智能化、降低成本三大特色。

首先，在技术自主化及先进性方面，国泰君安证券采用 OpenStack 开源事实标准技术路线，积极参与社区，培养自主技术团队。国泰君安证券背靠高度活跃的开源技术社区，为公司云平台的技术架构先进性提供保障。

其次，国泰君安证券金融产品交易综合服务平台实现了智能化运营，打通资源编排与自有自动化运维及监控平台和工作流平台，实现资源智能开通及回收。同时，通过深度融合 OpenStack 与 Kubernetes 打通云数据中心新一代应用交付的最后一公里。

最后，通过 EasyStack ECS 易捷行云企业云，国泰君安证券大幅度提升了上海来安路、外高桥和东莞南中心 3 个数据中心的资源管理效率，减轻运维压力。同时，构建应用快速交付闭环，大大缩短了应用上线及回收时间，有力支撑了创新型业务的增长。

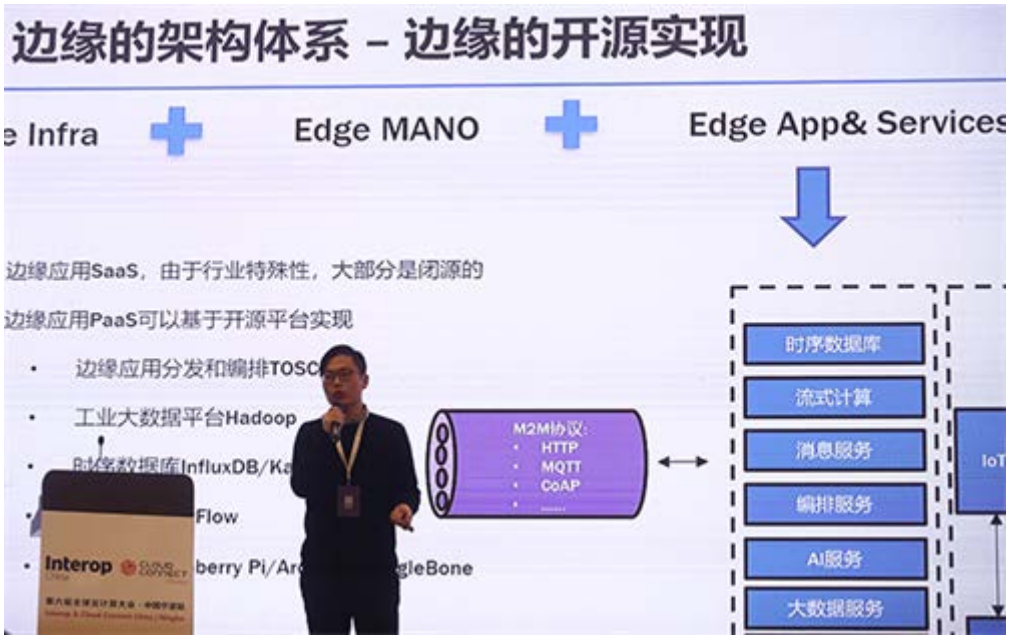
未来，国泰君安与 EasyStack 就构建应用快速交付闭环、混合云管理、契合国泰工作模式的资源生命周期管理、PaaS 服务与应用集市 SaaS 服务等方面继续合作，共同打造服务自愈、可持续进化、保持技术先进性的新一代金融云平台，持续提供更优质的金融服务。

3. 99CLOUD（九州云）动态

3.1 亮相全球云计算大会，九州云推动工业物联网升级换代

12 月 12-14 日，由宁波市人民政府指导，博闻中国主办的云计算行业年末盛典——第六届全球云计算大会•宁波站在泛太平洋大酒店隆重开幕。作为开源云的领军企业，九州云受邀出席本次会议，并携手中移杭研、诺基亚两大合作伙伴展开了精彩的主题演讲，共同助推宁波智能制造、智慧城市的快速发展。

在分论坛“5G 时代的云计算应用场景”上，九州云就工业边缘云发表了精彩演讲，并特邀中移杭研、诺基亚两大合作伙伴同场分享了“边缘计算”方面内容，为工业制造转型升级提供最佳解决方案。



在该论坛中，九州云边缘计算技术总监蒋暕青以《工业边缘云的商业模式、架构设计和开源实现》为主题展开了分享。工业往往要面对包含多个层次的应用系统，按照“人、机、料、法、环、测”等要素，包含 ERP、WMS、EMS、MES 等诸多系统，在打造工业边缘云的过程中，需要决定这些系统中哪些应用适合放在边缘、核心网和客户数据中心，这些不同的部署如何协同工作，需要一个从商业可行性到技术框架的设计过程，在本次演讲中，蒋暕

青重点分析了不同应用的特色，提出合理的部署方式，如何基于开放技术工业 IOT 和其他技术结合，实现一个符合 ETSI MEC 标准、兼容开放工业应用、软件和硬件解耦、厂商中立的工业 MEC 平台。

三、 云安全厂商动态

1. 启明星辰

1.1 启明星辰集团携手天津飞腾打造高性能自主可控网关型产品

12 月 5 日，启明星辰集团携手天津飞腾公司在北京召开“网御星云高性能自主可控网关型产品发布暨启明星辰集团 • 天津飞腾战略合作签约仪式”，宣布双方达成战略合作伙伴关系，同时发布网御星云高性能自主可控网关型产品。启明星辰集团总裁严立、天津飞腾公司总经理窦强、启明星辰集团副总裁/网御星云总裁胡晓峰、启明星辰集团副总裁高鹏等领导出席本次发布会。

没有网络安全，就没有国家安全。当前，信息安全已上升到国家安全的高度，对于信息安全产业而言，自主可控的网络安全已经上升为国家战略。天津飞腾公司是国内具备自主研发能力的集成电路芯片设计和生产领军企业，启明星辰集团是中国信息安全领军企业，自 2016 年率先发布商业化自主可控防火墙整机产品后，目前已经形成全系列自主可控网关型产品格局。

本次发布的网御星云高性能飞腾系列网关型产品，其核心处理器、操作系统、网络处理器，内存等均实现了自主化，凸显了网御星云在自主研发领域的积累和实力。值得一提的是，飞腾系列网关型产品具备 80G 的高速边界处理能力，彻底改写了国产自主安全产品性能的传统认知。

1.2 启明星辰成为华为首批终端安全奖励计划合作伙伴

近日，华为在北京举行 2018 华为终端安全奖励计划大会，启明星辰受邀出席本次大会，并成为华为终端安全奖励计划首批合作伙伴。华为对外披露“漏洞奖励计划”，向受邀安全研究者提供最高 100 万元人民币的漏洞发现奖励和荣誉致谢。启明星辰助理总裁孙薇受邀参加圆桌论坛环节，在终端安全奖励计划、终端漏洞挖掘成本、移动安全领域威胁等方面和嘉宾展开了深入探讨交流。

启明星辰积极防御实验室（ADLab），成立于 1999 年，是中国安全行业最早成立的攻防技术研究实验室之一，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、桌面主流应用、Web 及开源库／软件等领域均有前瞻性技术研究成果。

启明星辰积极防御实验室（ADLab）自 2015 年起已与华为在终端安全领域展开合作，仅去年已提交十余个终端安全漏洞研究成果。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。截至目前，积极防御实验室（ADLab）已通过 CNVD/CNNVD/CVE 累计发布原创漏洞近 1500 个，连续三年在 CNCERT 组织开展的年度政府部门网站安全专项检测工作中荣获第一名，受到国家与各行业客户的大力认可。

1.3 启明星辰泰合 TSOC 平台再次入围 Gartner SIEM 魔力象限

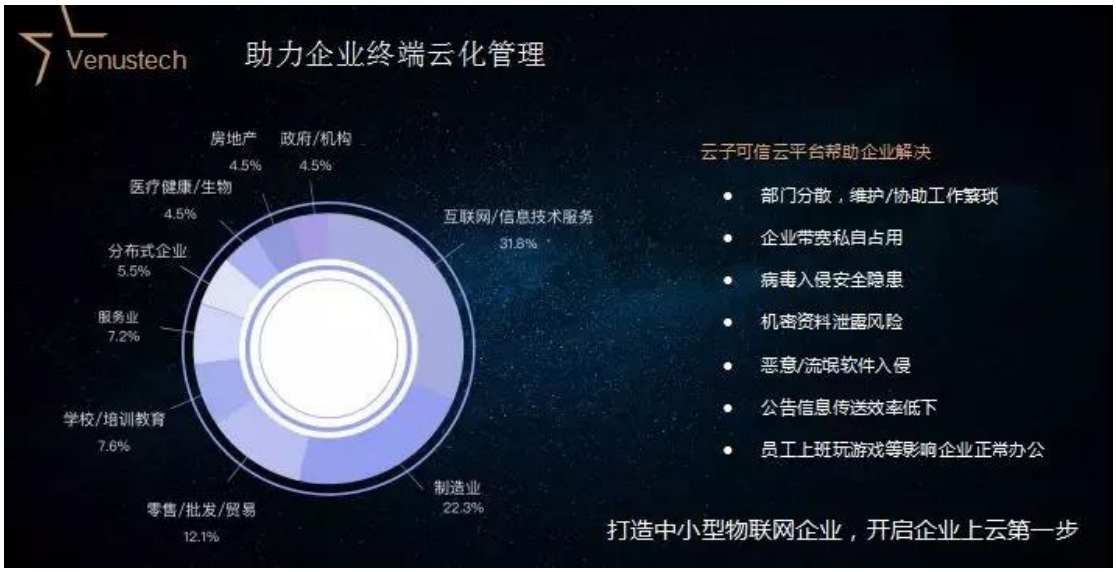
近日，国际知名的 IT 咨询机构 Gartner 发布了 2018 年《Magic Quadrant for Security Information and Event Management》的报告，启明星辰泰合 TSOC 平台再次入围 Gartner SIEM 魔力象限，启明星辰已连续两年成为亚洲唯一入围 Gartner SIEM 的安全厂商！

2018 年，Gartner 大幅提高了 SIEM 产品的入围门槛，从往年的 200 多项考核指标增加到了近 330 多个考核指标，考核重心更加聚焦于安全厂商产品在新技术领域 ABC（AI、Big Data、Cloud）的发展、全球市场战略以及客户满意度等方面的综合实力。 泰合 TSOC 平台采用大数据架构，基于机器学习的多维度智能关联、用户实体行为分析（UEBA）等技术，在多年的研究实践中积累了大量的高级安全分析场景。 启明星辰泰合 TSOC 平台在国内拥有超过 2000 家行业用户，上百个国家/部省级重大案例，在网络安全法、等级保护 2.0、欧盟 GDPR 法案、ISO27001 等各种标准的合规要求下，启明星辰泰合 TSOC 平台将在用户的信息安全建设中发挥不可或缺的作用。

1.4 启明星辰云子可信助力中小微企业创新转型

12 月 13 日，由工业和信息化部、四川省人民政府指导，四川省经济和信息化厅主办的全国首届中小微企业云服务大会在成都盛大举行。启明星辰旗下企业终端安全云平台-云子

可信精彩亮相，获得了中小微企业用户的青睐好评。



据 CERT 报道，有 90% 以上的企业安全问题是计算机终端安全防线薄弱造成的。 云子可信是启明星辰自主研发的面向中小微企业的终端安全安全云平台。无需购买服务器、带宽、也无需配备专业安全运维人员，只要接入互联网，即可获取该平台的所有安全服务。

1.5 启明星辰 VenusEye-威胁情报中心赋能安全渐入佳境

启明星辰威胁情报中心（VenusEye）是由启明星辰集团倾力打造的集威胁情报收集、分析、处理、发布和应用为一体的威胁情报服务平台，是启明星辰多年网络安全研究经验积累的集中体现，是国内为数不多的“领航者”之一。

启明星辰威胁情报中心（VenusEye）综合运用沙箱集群、同源性分析、大数据、知识图谱、人工智能等先进技术，生产和提供高质量的威胁情报信息。基于启明星辰威胁情报中心（VenusEye）可以提供威胁情报数据、系统、技术和专业分析能力；启明星辰威胁情报中心（VenusEye）Portal 站面向公众提供服务和运营，提供 SaaS API、离线情报库、威胁情报标准、私有威胁情报中心系统（TIC）等多种威胁情报数据、产品和服务解决方案；在检测探针类、分析感知类、攻击回溯类、运营服务类、解决方案类等多种威胁情报应用场景中广泛应用。

2. 深信服

2.1 深信服 EDR 助力军工行业信息化

深信服受邀在国家国防科技工业局信息中心主办的“第四届军工行业信息化推进大会”

发表“军工行业终端安全检测与响应——利用人工智能有效应对终端未知风险”的主题演讲。

深信服 EDR 以终端资产为核心，通过预防、防御、检测、响应赋予终端更为精准、持续的检测和快速处置能力；在应对高级威胁的同时，可实施联动协同、威胁情报共享、多层级响应机制，帮助用户快速检测、处置终端安全问题，构建全新轻量级、智能化、响应快的下一代终端安全系统。 深信服 EDR 具备下一代人工智能检测引擎、创新微隔离、流量可视化等特点。

3. 山石网科

3.1 山石网科被 Gartner 评选为亚太地区企业级防火墙全球性厂商

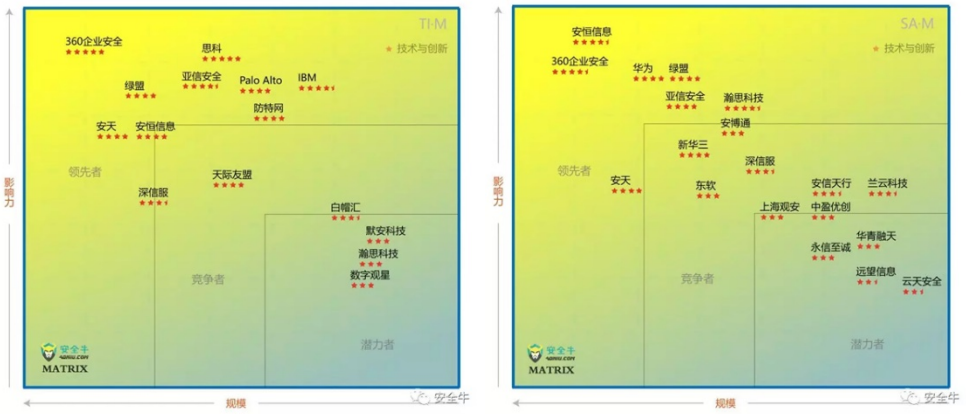
近日，全球知名咨询机构 Gartner 发布了亚太地区企业级防火墙魔力象限。山石网科入围全球性厂商”(中国厂商仅山石网科和华为入选“全球性厂商”)。山石网科拥有多项中国专业认证，如：计算机信息系统安全产品销售许可证，中国信息安全认证中心(ISCCC)认证，信息安全产品测评认证(EAL3+)证书等。

除硬件防火墙外，山石网科虚拟化防火墙山石云·界，是专门为云计算环境设计的虚拟化网络安全产品，以虚拟主机形态，All In One 的理念继承了山石网科下一代防火墙产品的精髓，适用于 VMware、KVM、hyper-V、XEN 的虚拟化平台下的各种网络部署场景，为用户提供云计算网络之间的安全隔离和安全防护。山石云·界支持 AWS，Azure，AliCloud，腾讯云，京东云，华为云，浪潮云，曙光云等主流公有云平台。山石云·界是国内首个 OSM

兼容虚拟防火墙产品。

4. 亚信

4.1 亚信安全入选安全牛威胁情报矩阵、态势感知矩阵

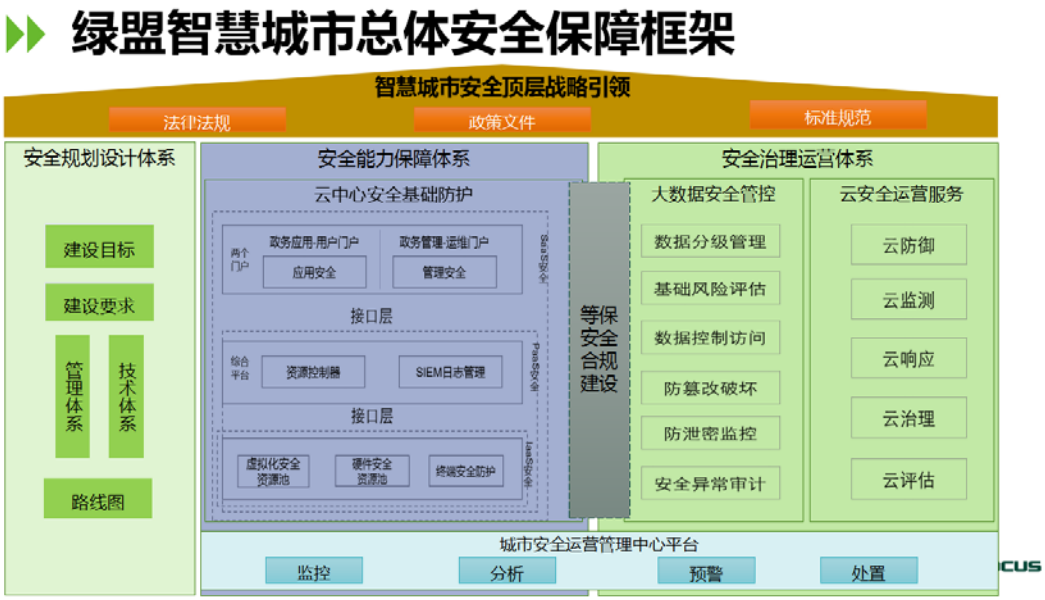


安全牛近日首次推出《中国网络安全细分领域矩阵图》(Matrix 2018.11)。本次调查数据的时间区间为 2017 年全年。亚信安全成功入选威胁情报矩阵、态势感知矩阵领先者。

5. 绿盟

5.1 绿盟科技“安全运营+”体系发布

12 月 5 日，在“安全运营+”媒体沟通会上绿盟科技发布“安全运营+”体系。这标志着绿盟科技在战略转型的发展道路上向前迈出了更为坚实的一步。



此次绿盟科技发布的“安全运营+”体系，旨在为智慧城市、云计算及政企等领域客户提供一体化的安全运营服务解决方案。

其中绿盟云安全解决方案主要是将资源池安全能力和端点防护相结合，提供丰富的云安全服务，可帮助用户从网络、主机、应用和数据等多个维度进行防护，形成安全服务闭环；利用图形化的界面帮助用户快速了解整个云平台的安全态势，及时发现未知威胁，同步到相应安全服务，协同防御；整个安全服务采用自动化的交付模式，可快速完成安全服务交付，提升业务响应速度和运维管理效率。

6. 安恒

6.1 安恒 EDR 新版本正式发布

近日安恒主机卫士 EDR2.0.7 正式发布，明御®主机安全及管理系统是一款集成了丰富的系统防护与加固、网络防护与加固等功能的主机安全产品。明御®主机安全及管理系统通过自主研发的文件诱饵引擎，有着业界领先的勒索专防专杀能力；通过内核级东西向流量隔离技术，实现网络隔离与防护；通过流量画像，实现全网流量可视化且支持一键阻断；拥有补丁修复、外设管控、文件审计、违规外联检测与阻断等主机安全能力。目前产品广泛应用在服务器、桌面 PC、虚拟机、工控系统、国产操作系统、容器安全等各个场景。实现功能包括资产指纹、病毒查杀与防御、漏洞管理、主机网络防御（支持南北向违规外联可视化及一键阻断、东西向威胁横向扩散可视化及一键阻断；支持自定义规则配置主机通信关系）、存储对象访问控制、 Web 应用防护、安全运维管控、威胁分析及日志检索

新版本增加的功能包括：病毒查杀增强、黑白名单双模式违规外联防护、微隔离与防暴力破解自动联动和出入站双向微隔离配置等。

7. 360

7.1 360 企业安全被 IDC 评为中国威胁情报市场的领导者

11 月 30 日，国际权威咨询公司 IDC 发布了 2018 中国威胁情报安全服务市场研究报告。报告显示，360 企业安全成为中国威胁情报市场的领导者，与半月前安全牛发布的威胁情报产品矩阵分析显示的结论一致。

截至目前，360 已经发布了 Alpha 威胁分析平台、威胁情报系统平台——TIP、监管行业威胁情报平台——威胁雷达、高级威胁情报分析服务、云端 SaaS API 等多个威胁情报产

品，全面覆盖了国内威胁情报服务的四种主流模式（威胁情报数据应用程序编程接口、威胁情报平台、威胁情报软件即服务、安全产品赋能），360 天眼、NGSOC、态势感知、360 智慧防火墙、EDR、云安全、虚拟化安全等核心安全产品和服务均集成了威胁情报能力，并且能够为不同客户提供定制化的行业解决方案，交付成功率居业内领先地位。未来，360 威胁情报中心还将以联盟的方式向第三方输出威胁情报能力，提升业界整体的安全防护水平。

IDC 认为，360 企业安全在威胁情报安全服务领域拥有独特且丰富的数据优势。基于国内庞大的安全终端软件装机基础，能够提供海量终端样本库、主动防御数据、文件信誉情报、各类安全产品（如网站安全、防火墙、态势感知、高级威胁发现等）的攻击发现日志，通过整合关联实现威胁来源的判定和画像，提供信息有用且维度全面的 IP 信誉，实现各种流行性及高级定向攻击的发现、评估与跟踪。同时作为批量生产机读情报的基础数据，能够实现本地化流行攻击 IOC 覆盖。

8. 安天

暂无消息。

9. Fortinet

9.1 赛门铁克携手 Fortinet 推出云安全服务

近日，网络安全厂商赛门铁克与集成自动化网络安全解决方案商 Fortinet 宣布达成合作伙伴协议，将 Fortinet 业界领先的下一代防火墙（NGFW）功能集成到赛门铁克云安全服务 Web Security Service（WSS）中，并且将赛门铁克行业领先的端点保护解决方案集成到 Fortinet Security Fabric 平台中。

赛门铁克 Web Security Service（WSS）是一种易于使用的云交付网络安全服务，能够防御高级网络威胁，确保访问控制，为云应用和网络上的关键业务信息提供安全保护，并且满足合规要求。行业领先的 Fortinet FortiGate 下一代防火墙与赛门铁克 WSS 集成后，新产品将成为市场中提供最全面云端威胁防护功能的单一解决方案。双方还计划将赛门铁克行业领先的端点保护解决方案集成到 Fortinet Security Fabric 平台中，为用户提供实时威胁情报，并且实现对漏洞和高级恶意软件攻击的自动响应。不仅如此，Fortinet SD-WAN 技术的互操作性也将通过赛门铁克技术集成合作伙伴计划（TIPP）的认证，以兼容赛门铁克 Web Security Service 网络安全服务。作为合作伙伴协议的一部分，双方将携手推进市场推广活动。此次

强强合作将能够为用户提供跨云、网络和端点的企业级安全防护功能。

10. Checkpoint

暂无消息。

四、 容器技术及安全动态

1. Rancher、ARM 联合推出物联网、边缘计算、K8S 平台

2018 年 12 月 11 日，企业级 Kubernetes 管理平台 Rancher Labs（以下简称 Rancher）宣布与英国芯片设计公司 Arm 合作，以满足客户对物联网和边缘计算的部署需求。今后，Rancher Kubernetes Engine (RKE)以及 Rancher OS 可移植到 Arm，增强后的 Rancher 服务器可以管理运行在数据中心的 x86 集群，以及运行在边缘计算和数据中心节点的 Arm 集群，为同时运行在 Arm 和 x86 上的 Kubernetes 集群提供了全球首个解决方案。无论用户选择使用哪种架构，Rancher 将提供在企业中运行 Kubernetes 的端到端解决方案。除此之外，Rancher 和 Arm 还将联手为中国的智慧城市项目提供基于 Kubernetes 的解决方案。

“Arm 自主研发的 Neoverse 处理器为扩展可以容纳万亿连接设备需求的计算能力提供了极大的优势”，Arm 软件生态系统解决方案高级总监 Kevin Ryan 表示：“Arm 与 Rancher 的合作让成千上万的组织拥有了从云端到边缘计算的 Neoverse 生态系统的强大力量。”

2. Kubernetes 1.13 版本发布

Kubernetes 在 2018 年年内第四次也是最后一次发布新的版本-Kubernetes1.13 版本！

此版本继续关注 Kubernetes 的稳定性与可扩展性，其中存储与集群生命周期相关的三

项主要功能已经逐步实现普遍可用。此版本中的核心更新包括：利用 kubeadm 简化集群管理、容器存储接口（简称 CSI）以及将 CoreDNS 作为默认 DNS。

这些稳定的功能设计代表着我们为用户以及运营人员设定支持期望方面实现的重要里程碑。此外，我们还在持续推出一系列内部改进及新的 alpha 测试功能，这些也将在本版本当中供社区使用。

值得注意的其它功能更新：

- ✓ 对第三方设备监管插件的支持已经进入 alpha 测试阶段。这意味着从 kubelet 当中删除现有与特定设备相关的知识，从而将未来一切可能要求特定设备知识的用例排除在外。
- ✓ Kubelet 设备插件注册表已经正式毕业并迎来稳定版本。其建立起一套通用的 Kubelet 插件发现模型，能够利用不同类型的节点级插件（例如设备插件、CSI 与 CNI 等）与 Kubelet 之间建立起通信通道。
- ✓ 拓扑感知分卷调度功能目前正式进入稳定阶段。其使得调度程序能够识别出 Pod 分卷的拓扑约束条件，例如区域或者节点等等。
- ✓ APIServer DryRun 正逐步进入 beta 测试阶段。这项功能将对象管理的“应用”与声明从 kubectl 转移至 apiserver，旨在修复大量目前无法得到解决的现有 bug。
- ✓ Kubectl Diff 正逐步进入 beta 测试阶段。其允许用户运行一条 kubectl 命令以查看本地声明的对象配置与活动对象的当前状态之间的差异。
- ✓ 使用持久分卷源的原始块存储设备正逐步进入 beta 测试阶段。其通过一个持久分卷源使得原始块存储设备（非联网）转化为可供用户的资源。

3. Kubernetes 爆安全漏洞

近期 Kubernetes 爆出安全漏洞，Kubernetes 产品安全团队表示，近日在 Kubernetes API Server 存在权限扩张漏洞，该漏洞由 Rancher Laba 首席架构师 Darren Shepherd 发现，漏洞编号为 CVE-2018-1002105。

s

攻击者可通过伪造的请求，在已建立的 API Server 连接上提权访问后端服务。更加糟糕的是，没有简单的方法可以检测是否已使用此漏洞。由于未经授权的请求是通过已建立的连接进行的，因此它们不会出现在 Kubernetes API Server 审核日志或服务器日志中。解决此漏洞唯一方式是尽快升级你的 Kubernetes。

目前 Kubernetes 已发布新版本，来解决该漏洞带来的风险，Kubernetes 安全团队 Google 高级工程师 Jordan Liggitt 建议，Kubernetes 企业用户应该尽快选择对应版本进行更新；

CVE-2018-1002105 漏洞受影响的版本：

Kubernetes v1.0.x-1.9.x

Kubernetes v1.10.0-1.10.10

Kubernetes v1.11.0-1.11.4

Kubernetes v1.12.0-1.12.2

修复补丁版本：

Kubernetes v1.10.11

Kubernetes v1.11.5

Kubernetes v1.12.3

Kubernetes v1.13.0-RC.1

影响的配置:

集群启用了扩展 API server，并且 kube-apiserver 与扩展 API server 的网络直接连通；

集群开放了 pod exec/attach/portforward 接口，攻击者可以利用该漏洞获得所有的 kubelet API 访问权限。

4. 微软 Azure 容器服务 ACS 要暂停

最近，微软宣布将于 2020 年 1 月正式暂停其 ACS（Azure Container Service）服务，并鼓励 ACS 用户将其分布式基础架构转移到新推出的 Azure Kubernetes Service 服务上，这对微软来说是一个合乎逻辑的举动。虽然 ACS 将继续支持 Docker Swarm 和 Mesosphere 的 DC/OS 替代编排选项，但将不再运行它们。相反，微软正集中精力改善 Azure 中的 Kubernetes 支持以及相关工具。

虽然 ACS 即将退役，但基于此的应用不会立即停止，用于管理的 API 将被停止，因此无法控制且无法使用 Azure 工具添加新集群或更新和扩展现有服务。尽管代码可以运行，但如果不能使用自己的工具管理，功能还是会受到限制。用户会被锁定在目前使用的旧版本框架中，并且无法依赖自动安全更新。

五、 安全新产品及技术

1. 公安部网络安全保卫局发布 《互联网个人信息安全保护指引（征求意见稿）》

为深入贯彻落实《网络安全法》，指导互联网企业建立健全公民个人信息安全保护管理制度和技术措施，有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益，公安机关结合侦办侵犯公民个人信息网络犯罪案件和安全监督管理工作中掌握的情况，组织北京市网络行业协会、北京邮电大学和公安部第三研究所相关专家，研究起草了《互联网个人信息安全保护指引（征求意见稿）》。

为凝聚各界共识和智慧，进一步完善防护措施，更好地为互联网企业和广大网民保护个人信息提供指导指引，现面向社会广泛征求意见。公众可以登陆“全国互联网安全管理服务平台”（http://www.beian.gov.cn）查阅征求意见稿，有关建议可通过电子邮件方式发送至 syjyc@vip.126.com，或传真至 010-66262319。

2. 工信部发布 2018 年第三季度网络安全威胁态势分析与工作综述

工信部发布 2018 年第三季度网络安全威胁态势分析与工作综述的公告。公告显示，第

三季度公共互联网网络安全形势依然严峻，发生多起严重危害用户合法权益的网络安全事件。其中，用户数据泄露事件多有发生、云计算平台相继发生故障。今年三季度全行业共处置网络安全威胁约 3397 万个，包括恶意 IP 地址、恶意域名等恶意网络资源约 653 万个，木马、僵尸程序、病毒等恶意程序约 2611 万个，网络安全漏洞等安全隐患约 4.8 万，主机受控、数据泄露、网页篡改等安全事件约 127 万个，其他网络安全威胁约 1 万个。

工信部同时对下一步工作作出部署，除了完成相关既定工作外，工信部将联合多企业、多单位开展移动恶意程序专项治理工作。及时发现和消除移动恶意程序等网络安全威胁，维护广大网络用户的合法权益。

3. 苹果发布 iOS 12.1.1 更新，修复了密码绕过漏洞、RCE 漏洞等问题

Apple 发布了其核心产品的更新，涵盖 iCloud、Safari、iTunes、macOS Mojave、High Sierra、Sierra、iOS 2.1.2 快捷方式、tvOS 12.1.1 以及 iOS 12.1.1。本次发布的更新修复了大量安全问题，包括代码执行、权限提升和信息泄露漏洞。因此，如果您是上述任何产品的用户，则应尽快更新。

此外，iOS 12.1.1 还修复了面容 ID 可能临时无法使用的问题，修复了在“信息”中使用中文键盘或日文键盘键入时，可能无法显示预测文本建议的问题，并且解决了“语音备忘录”录音可能无法上传至 iCloud 的问题。

4. SNDBOX 上线：基于 AI 构建的免费恶意软件检测平台

在 Blackhat Europe 大会上推出了一款名为 SNDBOX 的新恶意软件分析服务，该服务利用人工智能和强化虚拟环境对恶意软件样本进行静态和动态分析。静态分析部分允许上传者查看提交文件的信息，如文件元数据、表单信息等。使用许多不同的工具和站点已经可以获得这些信息，SNDBOX 提供的也差不多。动态分析部分是 SNDBOX 的真正力量发挥作用的地方。执行分析时，SNDBOX 将跟踪创建的所有文件和进程以及任何系统 API 调用、注册表查询和更改以及 WMI 请求。

“网络”部分允许上传者查看运行示例时执行的所有网络流量。AI 将查找任何异常信息并将其列在网络指示器下，这使地上传者可以快速发现罕见或不常见的网络流量。并非所有 SNDBOX 收集的信息都会显示在网站上。例如，HTTP 请求的 POST 数据不会显示在仪表

板中。不过上传者可以下载包含 SNDBOX 收集的所有信息的完整 JSON 报告。总的来说，SNDBOX 是那些经常进行恶意软件分析的人或者那些在他们的计算机上发现可疑文件的人的理想工具。

5. CNNVD 关于微软多个安全漏洞的通报

近日，微软官方发布了多个安全漏洞的公告，包括 Microsoft Internet Explorer 安全漏洞（CNNVD-201812-458、CVE-2018-8619）、Microsoft Excel 安全漏洞（CNNVD-201812-466、CVE-2018-8597）等多个漏洞。成功利用上述漏洞可以在目标系统上执行任意代码。微软多个产品和系统受漏洞影响。目前，微软官方已经发布漏洞修复补丁，建议用户及时确认是否受到漏洞影响，采取修补措施。

6. 微软发布针对专业版和企业版 Windows 10 的 Windows Sandbox

微软针对专业版和企业版 Windows 10 发布了一个轻量级的桌面环境 Windows Sandbox，以安全运行可执行文件。Windows Sandbox 是一个隔离的临时桌面环境，用户可以放心地运行不信任的应用程序，不用担心会对主机系统造成影响。安装在 Windows Sandbox 中的应用只会留在 Sandbox 里，一旦 Sandbox 关闭，里面的所有文件都将会永久删除。用户要想启用 Windows Sandbox，首先要有 Windows 10 Pro 或 Enterprise build 18305 或更高的系统版本，还需要在 BIOS 里启用虚拟化功能（物理机器），然后打开 Windows Features 寻找到 Windows Sandbox，打开开始菜单寻找到 Windows Sandbox 运行。

7. 信通院发布《车联网白皮书（2018）》

2018 年 12 月 19 日，中国信息通信研究院连续第十一年在京召开 “ICT 深度观察大型报告会暨白皮书发布会”，会上发布了《车联网白皮书（2018）》。这是中国信通院第二次发布《车联网白皮书》。本白皮书从技术、产业和政策措施三个维度对车联网国内外发展现状及趋势进行分析。技术部分包括单车智能化相关汽车电子技术和 V2X 无线通信、多接入边缘计算、车路协同平台等网联化相关技术，以及信息安全等共性关键技术；产业部分从专利布局、产业链协同重点剖析产业发展新趋势，探索新生态和新模式等；政策措施部分包括

顶层设计规划、协同推进机制、法律法规等；最后总结全文，对车联网融合创新发展提出“1+3”举措建议，包括构建一个跨行业协调机制和技术创新、产业融合、安全管理三个发展体系。

8. 网信办发布《金融信息服务管理规定》

国家互联网信息办公室 2018 年 12 月 26 日公布《金融信息服务管理规定》（以下简称规定）。规定主要是为了加强金融信息服务内容管理，提高金融信息服务质量，促进金融信息服务健康有序发展，保护自然人、法人和非法人组织的合法权益，维护国家安全和公共利益。在中华人民共和国境内从事金融信息服务，应当遵守该规定。规定要求金融信息服务提供者应当履行主体责任，配备与服务规模相适应的管理人员、建立信息内容审核、信息数据保存、信息安全保障、个人信息保护、知识产权保护等服务规范。同时还规定了其他相关责任和禁止事项，明确了监管部门与责任主体。

六、 网络安全投融资、收购事件

1. 收购

1.1 Artic Wolf Networks 完成对 RootSecure 的收购

12 月 12 日，Artic Wolf Networks 完成对 RootSecure 的收购，收购价未公开。Arctic Wolf Networks 是一家安全运营中心（SOC）即服务公司，业务模式对于中小企业来说更有吸引力，中小企业无力支付那些能够给诸多安全事件“降噪”的高端方案，而 Arctic Wolf 的服务能帮助这些企业缩小调查范围，减少全职安全专家的编制。RootSecure 是业界领先的网络风险平台，提供信息安全、遵从性和风险分析解决方案。

2. 投融资

2.1 Avanan 获 2500 万美元 B 轮融资

12 月 17 日，Avanan 从 Greenfield Partners 和其他 2 位投资者处获得 2500 万美元的 B 轮融资。Avanan 是一家为企业提供云端数据安全的技术公司。