

# 国内外云计算+安全动态报告

2018 年第 11 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.....	3
一、    云厂商动态.....	3
1.    AWS 云安全动态.....	3
1.1    Amazon S3 管理控制台现在支持五种新语言.....	3
1.2    Amazon Inspector 将 EC2 实例详细信息添加到安全检测结果中.....	3
1.3    现已可在 AWS Deep Learning AMI 上使用 Chainer 5.0.....	3
1.4    Amazon API Gateway 新增对 AWS WAF 的支持.....	4
1.5    Amazon RDS for Oracle 现在支持扩展数据类型.....	4
1.6    Amazon Inspector 推出了无代理网络评估.....	4
1.7    AWS Secrets Manager 支持 CloudFormation 以安全方式自动预置资源.....	5
1.8    Amazon RDS for Oracle 现在支持 Oracle 12.2 数据库.....	5
1.9    Amazon ECS 和 AWS Fargate 现支持资源标记.....	5
2.    VMWare 云安全动态.....	6
2.1    VMware 收购 Kubernetes 核心创始团队 Heptio.....	6
3.    GOOGLE 云动态.....	7
3.1    Google 云业务 CEO 换将 甲骨文前高管接任.....	7
4.    微软 Azure 云动态.....	8
4.1    微软与纳斯达克将在区块链技术上展开合作.....	8
5.    阿里云动态.....	8
5.1    阿里云管控工具-云命令行（公测）发布.....	8
6.    腾讯云动态.....	8
6.1    中国商飞上飞公司与腾讯云签订战略合作协议.....	8
6.2    腾讯微瓴亮相物联网论坛,助力建筑空间的数字化.....	9
7.    华为云动态.....	10
7.1    华为蝉联 OpenStack 全球用户调查第一名.....	10
二、    开源云动态.....	10
1.    Openstack 动态.....	10
1.1    《2018 OpenStack 用户调查报告》出炉.....	10
2.    Easystack 动态.....	13
2.1    Ceph 基金会正式成立 EasyStack 作为创始会员加入.....	13
2.2    EasyStack 位列 2018 OpenStack 用户调研报告全球三甲.....	15

3.	<b>99CLOUD (九州云) 动态</b> .....	<b>15</b>
3.1	九州云入驻中国移动集团边缘计算开放实验室 .....	15
3.2	九州云黄舒泉当选 StarlingX 首届 TSC.....	15
三、	<b>云安全厂商动态</b> .....	<b>16</b>
1.	<b>启明星辰</b> .....	<b>16</b>
1.1	启明星辰集团助推天津市打造一流网络强市 .....	16
1.2	IoT-VBox: 刚刚面世, 防护物联网终端就超 50 万! .....	16
1.3	郭启全总工关于等保 2.0 等五项工作内容的重要讲话 .....	18
1.4	启明星辰亮相 CERNET 华中地区 2018 年学术论坛.....	19
2.	<b>东软</b> .....	<b>19</b>
2.1	华为和东软携手完成首次 C-V2X 互联互通应用测试.....	19
3.	<b>山石网科</b> .....	<b>21</b>
3.1	山石网科参与 GITC 2018 北京站.....	21
4.	<b>亚信</b> .....	<b>21</b>
4.1	亚信科技为智慧交通疏导提供新方案 .....	21
5.	<b>绿盟</b> .....	<b>21</b>
5.1	绿盟科技荣获“2018 年度中国用户体验创新示范企业” .....	21
四、	<b>容器技术及安全动态</b> .....	<b>22</b>
1.	云原生计算基金会宣布 Envoy 项目正式“毕业” .....	22
2.	Aqua Security 在 AWS 市场上发布首个容器安全解决方案.....	22
3.	微软智能云 Azure Kubernetes 容器服务落地中国, 开启预览.....	23
4.	AWS 开源安全且快速的新概念微虚拟机 Firecracker .....	24
五、	<b>安全新产品及技术</b> .....	<b>25</b>
1.	25 个欧盟成员国将开展电子作战领域合作 .....	25
2.	谷歌安卓应用防护增强: 号称一个应用也不漏过.....	25
3.	西门子修复防火墙漏洞, 确保运营商安全通报 .....	26
4.	大疆身份识别系统漏洞允许攻击者将无人机变成间谍工具.....	26
5.	2018 Q3 Android 新恶意样本数量达 320 万个 同比增加 40%.....	26
6.	英特尔超线程 CPU 出现新漏洞 .....	27
7.	谷歌发布新安全功能, 若禁用浏览器 Java Script 则无法登录 .....	27
六、	<b>网络安全投融资、收购事件</b> .....	<b>27</b>
1.	<b>收购</b> .....	<b>27</b>
1.1	Threat Stack 完成对 Bluefyre 的收购.....	27
1.2	ForeScout Technologies 完成对 SecurityMatters 的收购.....	27
1.3	SolarWinds 完成对 8MAN 的收购 .....	28
1.4	BlackBerry 完成对 Cylance 的收购 .....	28

<b>2.</b>	<b>投融资 .....</b>	<b>28</b>
2.1	Shape Security 获得 2600 万美元的 E 轮融资 .....	28
2.2	Netskope 获得 1.68 亿美元的 F 轮融资 .....	28
2.3	Automox 获得 930 万美元的 A 轮融资 .....	29
2.4	Duality 获得 400 万美元的未知轮融资 .....	29
2.5	XM Cyber 获得 2200 万美元的 A 轮融资 .....	29
2.6	Alcide 获得 700 万美元的 A 轮融资 .....	29

## 本期云安全动态内容摘要

云厂商方面，AWS 提供多项功能支持，包括 Amazon S3 管理控制台现支持五种新语言、Amazon API Gateway 新增 AWS WAF 支持、Amazon RDS for Oracle 现支持 Oracle 12.2 和扩展数据类型、AWS Secrets Manager 支持 CloudFormation 以安全方式自动预置资源、AWS ECS 和 AWS Fargate 现支持资源标记、AWS Deep Learning AMI 上使用 Chainer 5.0，同时 Amazon Inspector 推出了无代理网络评估并将 EC2 实例详细信息添加到安全检测结果中；VMware 收购 Kubernetes 核心创始团队 Heptio；Google 云业务 CEO 换将，甲骨文前高管接任；微软与纳斯达克将在区块链技术上展开合作；阿里云管控工具-云命令行（公测）发布；中国商飞上飞公司与腾讯云签订战略合作协议，腾讯微瓴亮相物联网论坛,助力建筑空间的数字化；华为蝉联 OpenStack 全球用户调查第一名。

开源云方面，OpenStack Summit 在德国柏林开幕，《2018 OpenStack 用户调查报告》同时出炉；Ceph 基金会正式成立 EasyStack 作为创始会员加入，EasyStack 位列 2018 OpenStack 用户调研报告全球前三甲；九州云入驻中国移动集团边缘计算开放实验室，并且九州云黄舒泉当选 StarlingX 首届 TSC。

云安全厂商方面，启明星辰亮相媒体融合技术研讨会 探讨网络安全体系化运营，防护物联网终端就超 50 万，关注郭启全总工关于等保 2.0 等五项工作内容的重要讲话。华为和东软携手完成首次 C-V2X 互联互通应用测试，山石网科参与 GITC 2018，在前沿技术聚集地，亚信科技为智慧交通疏导提供新方案，绿盟科技荣获“2018 年度中国用户体验创新示范企业”。

容器动态方面，云原生计算基金会宣布实现服务与边缘代理功能的 Envoy

项目正式毕业；Aqua Security 在 AWS 市场上发布首个容器安全解决方案，租户创建容器服务时可直接购买；微软智能云 Azure Kubernetes (AKS) 容器服务在中国世纪互联运营的 Microsoft Azure 落地，开启预览，大大简化 Azure 平台上 Kubernetes 的部署和运营，让开发者可靠、灵活地自由伸缩应用架构。AWS 开源用于 Serverless 计算的安全且快速的新概念微虚拟机 (microVM) Firecracker。

安全新技术方面，安全合作与安全补强增加，25 个欧盟成员国将开展电子作战领域合作、谷歌安卓应用防护增强、西门子修复防火墙漏洞确保运营商安全通报、谷歌发布新安全功能控制登录；与此同时，大量漏洞爆出，大疆身份识别系统漏洞允许攻击者将无人机变成间谍工具、2018 Q3 Android 新恶意样本数量达 320 万个同比增加 40%、英特尔超线程 CPU 出现新漏洞。

网络安全公司投融资方面，共发生 4 起收购和 6 起投融资事件。收购方面，通讯公司 BlackBerry 以 14 亿美元的价格完成对网络安全技术公司 Cylance 的收购，企业级网络安全公司 ForeScout Technologies 则以 1.13 亿美元的价格完成对 SecurityMatters 的收购，其他 2 起收购事件收购价均未公开。投融资方面，云业务安全接入代理公司 Netskope 以 1.68 亿美元的 F 轮融资拔得头筹，专注于阻止自动化网络攻击和移动攻击的 Shape Security 和全自动 APT 仿真平台公司 XM Cyber 分别以 2600 万美元的 E 轮融资和 2200 万美元的 A 轮融资位列二三。

2018 年 11 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 云安全动态

#### 1.1 Amazon S3 管理控制台现在支持五种新语言

11 月 2 日, Amazon S3 管理控制台现在支持五种新语言: 西班牙语、意大利语、德语、繁体中文和葡萄牙语, 将 S3 管理控制台支持的语言数量增加到了十种。支持语言的增加让用户可以用本地语言更轻松地配置和管理自己的 S3 存储桶和对象。S3 管理控制台还支持英语、法语、日语、韩语和简体中文。

Amazon S3 在世界上最大的全球云基础设施上运行, 是一项全新构建的服务, 可提供 99.999999999% 的持久性。此次发布的 Amazon S3 增加了对欧洲、亚太地区和美洲的国际客户的支持。客户可以通过管理控制台底部的语言选择器, 用本地语言与 S3 管理控制台交互。

#### 1.2 Amazon Inspector 将 EC2 实例详细信息添加到安全检测结果中

11 月 5 日, Amazon Inspector 安全检测结果中现在包括具有漏洞或不安全配置的 Amazon EC2 实例的 Amazon 系统映像 (AMI) ID、实例标签、Auto Scaling 组、主机名、IP 地址、DNS 名称以及子网 ID。当用户在管理控制台中查看检测结果时, 只需单击“显示详细信息”按钮即可查看这些字段。此外, 当用户通过 AWS API 和 CLI 描述检测结果时, 也可使用这些字段。

Amazon Inspector 会自动评估应用程序的漏洞或者相较于最佳实践的偏差。执行评估后, Amazon Inspector 会生成按严重程度确定优先级的安全检测详细列表。这些附加字段可以帮助您根据易受攻击的 EC2 实例的映像、网络位置、标签或其他属性对安全检测结果进行筛选、分组和优先级排序。

#### 1.3 现已可在 AWS Deep Learning AMI 上使用 Chainer 5.0

11 月 5 日, 适用于 Ubuntu 和 Amazon Linux 的 AWS Deep Learning AMI 现在提供支持 Python 3.6 和 iDeep 2.0 的 Chainer 5.0。与其他框架一样, Deep Learning AMI 提供经过

微调 and 进行了完善配置的优化版 Chainer 5.0, 支持在 Amazon EC2 CPU 和 GPU 实例上进行高性能深度学习。

此外, AWS Deep Learning AMI 还支持 TensorFlow、PyTorch 和 Apache MXNet 等其他常见框架, 所有这些都已预先安装好并进行了完善配置, 让用户在几分钟内即可开始开发深度学习模型, 同时充分利用 Amazon EC2 实例的计算能力。

#### 1.4 Amazon API Gateway 新增对 AWS WAF 的支持

11 月 5 日, 现在可以在 Amazon API Gateway 中为您的 API 启用 AWS WAF, 从而更轻松的保护用户的 API 免受常见 Web 攻击。

AWS WAF 是一种 Web 应用程序防火墙, 允许配置规则, 根据自定义规则和定义的条件允许、阻止或监控 (计数) Web 请求, 从而帮助保护 Web 应用程序和 API 免受攻击。

用户可以将 AWS WAF 用于用户的 Amazon API Gateway API, 以防止 SQL 注入和跨站脚本 (XSS) 等攻击。此外, 还可以使用规则根据 IP 地址、地理区域、请求大小和/或字符串或正则表达式模式筛选 Web 请求。可以将这些条件放在 HTTP 标头或请求本身的主体上, 从而允许创建复杂的规则来阻止来自特定用户代理、恶意机器人或内容抓取器的攻击。还可以利用 AWS Marketplace 上的托管规则, 即时保护 API 免受常见威胁, 例如 OWASP 前 10 大安全风险和常见漏洞 (CVE)。

#### 1.5 Amazon RDS for Oracle 现在支持扩展数据类型

11 月 6 日, Amazon 宣布, 当用户使用自定义参数组并将 MAX\_STRING\_SIZE 参数设置为 “EXTENDED” 时, Amazon RDS for Oracle 支持扩展数据类型。扩展数据类型允许用户将 VARCHAR2、NVARCHAR2 和 RAW 列的最大大小增加到 32767 字节。用户可以将扩展数据类型与使用 Oracle 12c 主要版本的数据库实例结合使用。

#### 1.6 Amazon Inspector 推出了无代理网络评估

11 月 8 日, Amazon Inspector 现在使用 “网络可访问性” 规则包提供无代理网络评估, 该规则包可识别能从用户的 VPC 外部访问的 Amazon EC2 实例上的端口和服务。只需在 Inspector 控制台中单击几下, 就可以分析 AWS 账户的网络配置, 以识别可通过 Internet 或私有网络 (如 VPN、Direct Connect 或对等 VPC) 访问的资源。

使用网络可访问性规则包的 Amazon Inspector 评估可帮助验证 AWS 网络配置的运作情况是否符合预期。评估会生成详细的结果, 显示 EC2 实例上的可访问端口以及允许访问



这些端口的网络配置，以帮助用户轻松按最初的计划限制访问。网络可访问性规则包使用 AWS 的可证明的安全性计划中的最新技术，该计划包含一套使用自动推理的 AWS 技术。无代理评估会分析 Amazon Virtual Private Cloud (VPC)、安全组、网络访问控制列表 (ACL) 和路由表等 AWS 网络配置，以查找可访问的端口。

使用网络可访问性规则包时，可以在 EC2 实例上安装 Inspector 代理以获取其他信息。强化结果包括用于识别在可访问端口上侦听的进程的信息。通过使用 Inspector 主机评估规则包（如常见漏洞和泄露 (CVE)），还将获得有关 Amazon EC2 实例上漏洞的信息。该规则包可以显示对托管应用程序的 EC2 实例的可能访问路径以及这些实例中的漏洞和不完全配置，便于用户更加全面地了解潜在安全风险。

### 1.7 AWS Secrets Manager 支持 CloudFormation 以安全方式自动预置资源

11 月 12 日，通过与 AWS CloudFormation 集成，AWS Secrets Manager 让用户能够更轻松以安全方式自动预置 AWS 资源。可以通过这项集成来预置创建和访问 AWS 资源所需的密钥，例如数据库凭证。

AWS Secrets Manager 可帮助用户创建和保护访问应用程序和 IT 资源所需的密钥。通过集成 AWS Secrets Manager 与 AWS CloudFormation，用户可以使用 CloudFormation 来预置 IT 资源以及访问这些资源所需的密钥。这些密钥存储在安全的位置并经过自动加密，可以进行配置来实现安全轮换。详细了解如何配合使用 AWS Secrets Manager 与 AWS CloudFormation。

### 1.8 Amazon RDS for Oracle 现在支持 Oracle 12.2 数据库

11 月 13 日，现在可以启动在 Oracle 12.2 上运行的 Amazon RDS for Oracle 实例。要在 AWS 管理控制台中单击几下创建新的 Oracle 12.2 数据库实例，请使用“启动数据库实例”向导，并选择数据库引擎版本“12.2.0.1.ru-2018-10.rur-2018-10.r1”。

此版本推出了新的引擎版本控制方案。Oracle 提供版本更新 (RU) 和版本更新修订 (RUR)，而不是补丁集更新 (PSU)。RU 包含优化程序更改、功能添加和安全修复。RUR 仅包含针对接下来的两个季度修补周期的安全修复。这一新的版本控制系统使用户可以更好地控制在每次更新时安装的功能。

### 1.9 Amazon ECS 和 AWS Fargate 现支持资源标记

11 月 15 日，现在用户可以标记 Amazon Elastic Container Service (Amazon ECS) 和 AWS

Fargate 资源，例如服务、任务定义、任务、集群和容器实例。这让用户可以更好地分配成本、提高工作负载的可见性、轻松搜索和识别容器化应用程序、实施程序化基础设施管理操作，并定义精细的资源级权限。

许多 ECS 客户都管理着数千种资源，例如任务定义、服务、任务和集群，这些资源分布在不同的团队、产品、业务部门和环境。如果没有标记，他们很难以系统的方式管理整个基础设施和基础成本。现在，用户可以使用 ECS API 和控制台在创建或运行 ECS 资源时对其进行标记。使用 AWS Fargate 启动类型的客户现在可以使用标签轻松分配其 ECS 任务的成本。对于使用 EC2 启动类型的客户，ECS 已在“成本和使用情况报告”中提供了详细的 ECS 任务使用数据，客户可以使用这些数据来分配基础 EC2 实例的成本。

要使用标记功能，用户需要为任务、容器实例和服务选择新的 Amazon 资源名称(ARN)和资源标识符 (ID) 格式。要使用新标记功能及其所有潜在好处，这些新的 ARN 和 ID 是必备条件。

## 2. VMWare 云安全动态

### 2.1 VMware 收购 Kubernetes 核心创始团队 Heptio

11 月 8 日消息，VMware 计划收购西雅图创企 Heptio。Heptio 由 Kubernetes 联合创始人 Joe Beda 和 Craig McLuckie 共同创立，致力于帮助企业构建和运行基于 Kubernetes 的容器式体系架构。

Beda 和 McLuckie 以及他们的团队都将根据此次交易，加入 VMware。

这笔交易的具体条款尚未被披露。但 VMware 表示，这些条款对公司来说并不重要。根据 PitchBook 的数据，Heptio 于 2017 年完成 2500 万美元 B 轮融资，估值达 1.17 亿美元，投资者包括 Lightspeed、Accel 和 Madrona。

鉴于 Heptio 创始人的出身，VMware 的此次收购成为在 Kubernetes 押下重注的信号，也预示着 VMware 将成为企业服务的重要基石。VMware 已经在全球拥有超过 50 万名客户和 7.5 万名合作伙伴。目前我们尚不知晓 Heptio 的客户有多少，但其可以确定其中包括雅虎日本等大型科技前沿企业。

这也是对开源的持续崛起及其在云架构中的地位的一次认可，这种模式在 10 月底因 IBM 以 340 亿美元收购 RedHat 而获得了巨大的关注，IBM 的这次收购也是有史以来最大的技术收购之一。

Heptio 为采用或已经使用 Kubernetes 的企业提供专业服务，为管理 Kubernetes 和相关容器集群的特定方面提供培训、支持和建设开源项目。VMware 将利用更广泛的云、本地和混合存储与计算服务，帮助扩大 Kubernetes 的业务渠道和利润。

“Kubernetes 正在成为一个开放的多云基础设施框架，以便企业组织能够运行各种应用，” VMware 相关负责人 Paul Fazzone 在一份声明中表示。“Heptio 产品和服务将加强和扩展 VMware 与 PKS 的合作，将 Kubernetes 确立为跨云基础架构的事实标准。”

VMware 及其 Pivotal 业务已经通过 PKS 提供了与 Kubernetes 相关的服务，这使得组织可以运行不受云限制的应用。Heptio 将成为更广泛投资组合的一部分。

“Heptio 团队一直专注于 Kubernetes，创造了一些产品，使得跨多个云管理多个集群变得更加容易，” Heptio 的首席执行官兼联合创始人 Craig McLuckie 表示。“现在，我们将利用 VMware 的云原生资源和经验证的执行能力，扩大我们的影响。VMware 对 Heptio 的兴趣承认了开源领域有如此多的创新。我们共同致力于社区做出更多贡献，包括资源、想法和支持。”

根据 Crunchbase 的数据，VMware 总共进行了约 33 次收购，但这似乎是第一次明确提升其在 Kubernetes 领域的地位。

VMware 表示，这笔交易预计在 2019 财年第四季度完成。

### 3. GOOGLE 云动态

#### 3.1 Google 云业务 CEO 换将 甲骨文前高管接任

11 月 17 日消息，三年前创建谷歌云计算业务的黛安-格林(Diane Greene)将被甲骨文前高管托马斯-库里安(Thomas Kurian)取代。Kurian 将于 11 月 26 日加入谷歌 Cloud，并将于 2019 年初接任该公司的领导职务。在那之前，格林将继续担任谷歌云业务的 CEO。格林自 2012 年以来还一直担任谷歌母公司 Alphabet 的董事。

对于格林来说，这是一个艰难的任期，他为谷歌带来了强大的企业实力，此前他曾联合创立并运营 VMware，她还组建了强大的企业销售团队，并从 Spotify 和 Snap 等公司那里赢得了业务，但谷歌未能追上亚马逊在这一领域的巨大领先地位，在云计算市场上，亚马逊和微软目前分别位列第一、第二位。根据 Synergy Research 的数据，Amazon Web Services 控制着 34% 的云基础设施服务市场。微软以 15% 的市场份额位居第二，其次是 IBM(第三)和谷歌(第四)，市场份额均为个位数。Alphabet 上月的财报电话会议上对云计算部门的规模和增长

速度方面提供的信息少的可怜，这也大大出乎各分析师意料之外。

## 4. 微软 Azure 云动态

### 4.1 微软与纳斯达克将在区块链技术上展开合作

10 月 31 日消息，微软表示，其 Azure 区块链服务将与纳斯达克的金融框架（Financial Framework）进行整合，后者向交易员、证券交易所以及清算所提供相互之间沟通交流的软件。

双方的合作将打造一个新的区块链系统，该系统允许客户在一个共同的交互界面上使用不同的区块链技术。

纳斯达克金融框架计划，使其客户能够通过一个共同的交互界面使用不同的区块链技术。该公司希望这将简化和加快区块链的使用，并让客户针对不同的情境选择最佳方案。

这两家公司表示，这将使买卖双方之间的匹配更容易，且交易的交付、支付和结算管理也将会更为简便。

## 5. 阿里云动态

### 5.1 阿里云管控工具-云命令行（公测）发布

11 月 19 日消息，阿里云管控工具-云命令行（公测）发布。阿里云云命令行是一个网页版的管控工具，当通过浏览器启动云命令行后，阿里云会自动提供一个安全的，预装 CLI、Terraform 等多种云管理工具和 ssh、vim、jq 等系统工具的操作环境，帮助用户在浏览器内直接用命令行管理阿里云资源。

## 6. 腾讯云动态

### 6.1 中国商飞上飞公司与腾讯云签订战略合作协议

11 月 6 日，中国商飞上海飞机制造有限公司（简称“上飞公司”）与腾讯云签订战略合作协议。协议的签订标志着双方在民机智能制造领域达成重要共识，将共同推进云计算、大数据、人工智能和 5G 等前沿技术在航空工业及相关上下游领域的广泛应用和推广。

上飞公司总经理余泽民，副总经理卢小安、王飞，党委副书记、工会主席曹印诺，腾讯云副总裁徐翊鸣、腾讯云企业业务总经理蔡毅出席签约活动。卢小安、蔡毅分别代表双方签

订战略合作协议。

余泽民说，飞机是高度复杂的产品，也是高度智能的产品，智能制造是飞机制造的必由之路。腾讯公司的研究成果将有助于推动我们在商用飞机智能制造领域的建设和部署。

徐翊鸣表示，腾讯公司将与上飞公司携手打造基于云平台、应用人工智能、物联网、5G 等新技术的试点项目，共同推进“云大物智”在工业领域的应用。

## 6.2 腾讯微瓴亮相物联网论坛,助力建筑空间的数字化

在 11 月 19 日举办的首届中国建筑物联网高峰论坛上,腾讯云副总裁王涛发表主题演讲,他介绍了腾讯云在智慧办公、智慧社区、智慧商圈等场景下的建设成果,及一套深度适配智慧建筑场景的物联网类操作系统——腾讯微瓴,并提出腾讯云将持续输出产品与技术能力让建筑学会思考,让空间更有温度,为建筑空间的数字化升级助力。



作为腾讯的技术出口,腾讯云为微瓴提供包括存储、计算、分析、系统分发以及微信开放接口等基础能力,整合物联网数据接入平台、大数据开发应用平台、人工智能与应用、大数据分析可视化等空间大脑,提供统一身份、统一支付、统一触点、运营推广等核心业务服务,为智慧办公、智慧社区、智慧商圈输出民生应用、无人商超、身份识别等丰富的空间应用产品和解决方案。

## 7. 华为云动态

### 7.1 华为蝉联 OpenStack 全球用户调查第一名

11 月 13 日，OpenStack Summit 在德国柏林开幕，《2018 OpenStack 用户调查报告》同时出炉。华为蝉联 2017 年和 2018 年两次全球用户调查第一名。

## 二、 开源云动态

### 1. Openstack 动态

#### 1.1 《2018 OpenStack 用户调查报告》出炉

11 月 13 日，OpenStack Summit 在德国柏林开幕，《2018 OpenStack 用户调查报告》同时出炉。

作为由 OpenStack 基金会发起的第 11 次全球 OpenStack 用户调查项目，报告汇总了 2017 年 8 月至 2018 年 8 月期间提交的 1483 份调查问卷，来自全球 63 个国家和地区的 858 个项目部署和 441 个用户组织。根据这些数据，报告对 OpenStack 在全球的发展状况、演进趋势、生态系统、以及供应商排名等做了全面的分析与解读，是 2018 年全球开源云计算市场的用户调查权威报告。

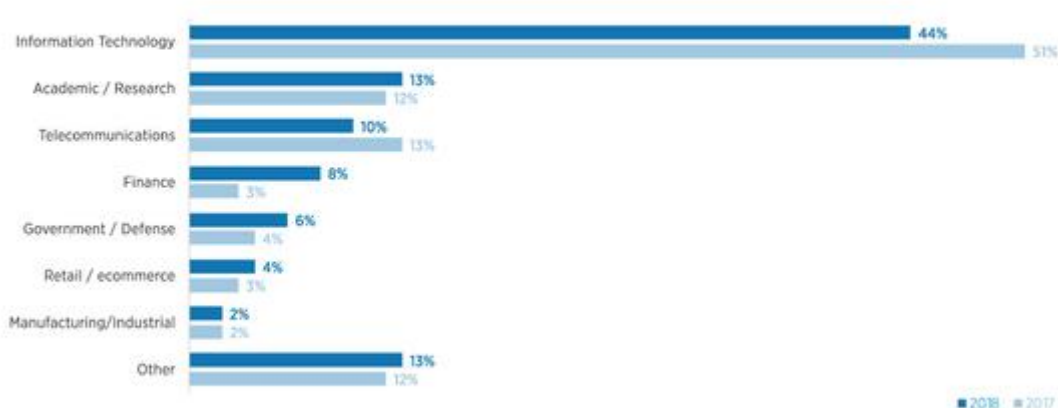
用户调查报告发现，75% 的 OpenStack 云是本地私有云，这一数据相较于 2017 年 3 月有 5% 的提升。OpenStack 云的用户包括各种规模的组织，其用户的组织规模呈正态分布，大约一半的受访者受雇于 999 名或更少员工的组织。

用户调查报告还认为，OpenStack 是高速发展企业和成熟企业的强大基础架构解决方案。采用 OpenStack 不仅能够提升企业运营效率，还能加速企业的创新能力，同时可以避免供应商锁定，这是用户采用 OpenStack 平台的 TOP3 要因。

- OpenStack 用户在 IT 之外的行业持续增长

报告显示，OpenStack 在 IT 以外的行业正得到广泛部署，并形成增长趋势，IT 行业 OpenStack 部署比例从 2017 年的 51% 下降到 2018 年的 44%。

### Which industries use OpenStack?



2017's sample size of 499, and 2018's sample size of 685.

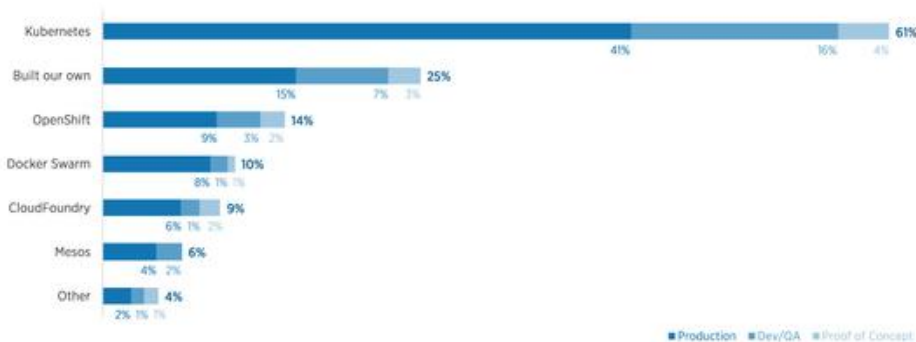
虽然 IT 行业仍然是报告中整体占比最大的行业类别，但 OpenStack 在金融行业的部署占比增幅最大，从 2017 年的 3% 飙升至 2018 年的 8%。这其中代表用户就包括 Banco Multiva、eBay Classifieds Group、Progressive 保险、SBAB 银行和大众汽车金融服务等大型金融机构。此外，政府/国防（从 2017 年的 4% 上升至 2018 年的 6%）和零售/电子商务（从 2017 年的 3% 上升至 2018 年的 4%）行业的 OpenStack 部署量也有显著增长。

- Kubernetes 持续占据 OpenStack 容器编排框架首位

在 2018 年的用户调查报告中，61% 的参与者采用 Kubernetes 作为管理 OpenStack 之上应用的 PaaS 及容器的工具。代表用户包括 BBVA、欧洲核子研究委员会（CERN）、中国银联、大众汽车以及沃尔玛实验室。

可见，Kubernetes 在 2016 年取得领先后，持续占据 OpenStack 容器编排首要框架地位。这表明，OpenStack 和 Kubernetes 越来越多地作为互补技术部署，特别是在多云场景中——在这些采用 Kubernetes 的受访者中，70% 的用户表示他们正在运行多云环境。

### What PaaS and containers orchestration tools are used to manage applications on OpenStack deployments?



Sample size of 359.

● Kubernetes 应用增长推动 OpenStack 裸机云增长

在 2018 OpenStack 用户调查报告中，OpenStack 的裸机云服务 Ironic 的采用比例快速增长，24%的生产级部署都依赖 Ironic，而 2016 年这个比例仅为 9%。Ironic 毫无疑问成为所有 OpenStack 生产级部署中应用增速最快的 OpenStack 组件之一。对于那些在 OpenStack 上运行 Kubernetes 的用户，Ironic 的使用比例更高，达到 37%。作为 OpenStack 上 Kubernetes 的 CNCF 认证安装工具，Magnum 也被广泛使用，应用比例达到 16%。

● OpenStack 多云用户更依赖 OpenStack

调查报告强调了 OpenStack 在多云环境中的主导地位以及用户对使用 OpenStack 来管理云计算基础架构的强烈依赖。

在此次调查中，78%的 OpenStack 用户为多云用户。其中，44%的用户多云架构的公有云服务选择的是 AWS，28%选择了 Azure，24%选择了 Google。另一方面，这些用户在 OpenStack 上运行的整体云基础架构的占比为 58%。

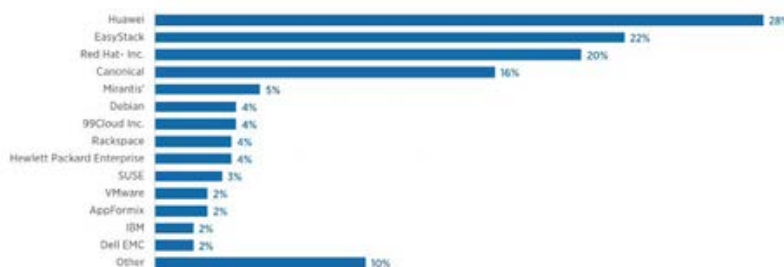
● OpenStack 供应商排名，TOP3 亮了

在 2018 OpenStack 用户调查中，为了让部署 OpenStack 的用户参与者更好地了解业界生态，OpenStack 基金会将以往调查问卷中“你采用的是哪家供应商的 OpenStack 产品？”细分为两个问题：一个是“使用了哪家软件供应商的 OpenStack 产品来构建云计算平台？”；另一个是“OpenStack 云平台的硬件产品供应商是谁？”。

**EasyStack Joins Huawei and Red Hat Among Top Ranking OpenStack Software Vendors**

When looking at the responses from participants who indicated they are working with a software vendor, EasyStack joins the Top 3 OpenStack vendors in 2018, placing second behind Huawei, who retains its No. 1 spot from 2017. Red Hat ranks third among software vendors named by survey respondents.

**Which vendor's OpenStack-related software products power users' clouds?**



Sample size of 454



排名	OpenStack软件供应商	参与调查用户占比
1	HUAWEI	28%
2	EasyStack	22%
3	Red Hat Inc	20%
4	Canonical	16%
5	Mirantis	5%
6	Debian	4%
7	99Cloud Inc	4%
8	Rackspace	4%
9	Hewlett Packard Enterprise	4%
10	SUSE	3%
11	VMware	2%
12	AppFormix	2%
13	IBM	2%
14	Dell EMC	2%
15	Others	10%

在参与调查的用户中，关于 OpenStack 软件供应商排名的报告显示为：“EasyStack（易捷行云）与华为和红帽一起成为本次用户调查报告的前三甲 OpenStack 软件供应商，排名第二；华为蝉联 2017 年和 2018 年两次全球用户调查第一名，红帽排名第三。”

值得关注的是，这也是中国企业第一次占据 OpenStack 基金会用户调查报告供应商排名榜单的前两名，充分反应出中国新一轮客户在 OpenStack 技术选择上的持续看好，OpenStack 已经成为中国私有云的事实标准。

作为中国云创业企业和专业的私有云，EasyStack 首次进入前三甲，反应了软件和服务正在成为中国私有云市场的主要推动力量，软件定于计算、存储、网络决定了私有云平台的整体架构，从而影响硬件和服务的选择。

作为全球最具影响力的开源企业，红帽在 10 月被 IBM 以近 340 亿美元价格收购，联系今年微软收购 Github, VMware 收购 Kubernetes 核心创始人公司 Heptio 等系列开源收购案，反应出在云计算的大潮下，开源被全球市场空前看好。

在硬件供应商方面，Dell EMC、华为和 HPE 分列以 33%、29% 和 27% 占据榜单前三甲。值得一提的是，作为软硬兼具的 IT 巨头，华为在 OpenStack 软硬两个榜单中都位居全球 TOP3。

## 2. Easystack 动态

### 2.1 Ceph 基金会正式成立 EasyStack 作为创始会员加入

11 月 12 日，Linux 基金会在德国柏林“Ceph Day”上宣布，正式成立 Ceph 基金会，以

支持 Ceph 开源项目社区。易捷行云 EasyStack 与其余 30 余家全球技术领袖作为创始会员共同加入 Ceph 基金会。



Ceph 项目是一个统一的分布式存储系统，提供了对象、块、和文件存储功能。Ceph 高效，灵活且可大规模扩展，显著降低了在私有云中存储企业信息的成本，并为任何对象、文件和数据块提供高可用性，广泛被世界各地的云计算供应商和企业使用。Ceph 基金会将以一种协调的、与供应商无关的方式组织和分配财务捐款，以使社区立即受益，也将有助于促进整个 Ceph 生态系统的快速发展与壮大。

作为中国开源云计算的领导者，易捷行云 EasyStack 不仅一直深度参与 Ceph 项目，积极贡献 Ceph 代码，推进 Ceph 产品化应用，还将 Ceph 作为云计算基础架构平台的重要组件，持续进行产品化创新，不断优化 Ceph 在 EasyStack 云平台上的性能和可靠性，广泛为金融、政务、制造等企业级客户提供稳定、敏捷、灵活且高效的云计算产品。

Linux 基金会执行董事 Jim Zemlin 表示：“Ceph 在帮助企业有效管理高增长和扩展数据存储需求方面有非常丰富的经验，在 Linux 基金会下，Ceph 基金会将能够利用更多资源来帮助完善 Ceph 生态系统建设。”

Ceph 联合创始人 Sage Weil 表示：“Ceph 基金会的成立证明了一个多元化的开源社区的力量所在，各方共同联合起来致力于解决数据存储和数据服务的爆炸性增长。”

易捷行云 EasyStack 联合创始人兼 CTO 刘国辉表示：“作为中国开源云计算的领导者，EasyStack 一直持续贡献开源社区，推动开源技术的产品化。作为 Ceph 基金会的创始成员，EasyStack 将继续基于 Ceph 技术推动构建更加广泛的生态系统，为企业级客户提供开放、稳定可靠、高性能的云计算产品与服务。”

## 2.2 EasyStack 位列 2018 OpenStack 用户调研报告全球前三甲

11 月 13 日, OpenStack Summit 在德国柏林召开, OpenStack 基金会在会上发布《2018 年 OpenStack 用户调查报告》。在参与此次调查的 OpenStack 用户中, 有 22% 采用了易捷行云 EasyStack 的 OpenStack 软件产品构建云平台, EasyStack 也因此在本次调研报告中位列全球 OpenStack 软件供应商第二名。

作为由 OpenStack 基金会发起的第 11 次全球 OpenStack 用户调查项目, 报告汇总了 2017 年 8 月至 2018 年 8 月期间提交的 1483 份调查问卷, 来自全球 63 个国家和地区的 858 个项目部署和 441 个用户组织。根据这些数据, 报告对 OpenStack 在全球的发展状况、演进趋势、生态系统、以及供应商排名等做了全面的分析与解读, 是 2018 年全球开源云计算市场的用户调查权威报告。

调查报告显示, OpenStack 是发展中公司和成熟企业的强大基础架构解决方案, 并适用于任何规模的用户, 其中 75% 是本地私有云项目。用户采用 OpenStack 的 TOP3 要素依次是: 第一, 能够提升企业运营效率; 第二, 加速企业的创新能力; 第三, 可以避免供应商锁定。

## 3. 99CLOUD (九州云) 动态

### 3.1 九州云入驻中国移动集团边缘计算开放实验室

10 月 30 日, 由中国移动和中国通信学会联合主办的"2018 边缘计算技术峰会"在京隆重召开。峰会获得了中国信息通信研究院、工业互联网联盟(AII)、SDN/NFV 产业联盟、边缘计算产业联盟(ECC)等机构及组织的响应和支持。来自产业各方的专家学者, 以及互联网界、工业界、电信界的近 400 名代表集聚一堂, 共同探讨边缘计算产业生态的构建和协同发展。会上, 九州云携最新的解决方案亮相, 联合中国移动全力布道边缘计算产业。

### 3.2 九州云黄舒泉当选 StarlingX 首届 TSC

11 月 14 日, OpenStack 全球峰会进入第二天的议程, Keynote 上, StarlingX 社区正式对外宣布第一届八位 Technical Steering Committee 技术指导委员会(以下简称 TSC)委员名单, 九州云技术总监黄舒泉作为唯一的华人和中国公司代表位列其中, 传递更多中国声音。

不可否认, 边缘计算已成为云技术的最新趋势, 尤其随着 5G 移动网络的出现, 边缘计算将为供应商们带来全新的商机。StarlingX 已逐渐发展成为边缘计算领域的重要项目之一, 备受业界关注, 并成功吸引了英特尔、华为、爱立信、风河、九州云等重量级厂商的参与。今年 10 月底, OpenStack 基金会更是发布了 StarlingX 的首个版本, 该版本为分布式边缘提

供了功能齐全的云。

### 三、 云安全厂商动态

#### 1. 启明星辰

##### 1.1 启明星辰集团助推天津市打造一流网络强市

启明星辰安全运营中心随着新技术而变化,并在变化中不断融合世界最先进的安全技术,整合国内最优秀的安全人才,为智慧城市未来发展持续赋能。如今,启明星辰北斗安全运营中心已在全国各地落地开花,为智慧城市、城市云、大数据中心及其他城市关键信息基础设施建立网络安全监测、信息通报和应急处置机制,实现“全天候、全方位”的网络安全态势感知、运维服务、应急响应能力。



启明星辰集团以“第三方独立安全运营”为核心的 I<sup>3</sup> 新战略,立足于自身在云计算、大数据、物联网、工业互联网、关键信息基础设施保护、移动互联网等领域的安全技术发展,以具备全面实战对抗能力的安全运营团队为核心,打造标准化、体系化、实战化的安全交付模式,从而提供覆盖全行业全技术的安全能力,解决新技术带来的安全挑战,帮助融媒体全面提升安全能力。

##### 1.2 IoT-VBox: 刚刚面世,防护物联网终端就超 50 万!

在“物联网+”背景下,形成了智慧城市、智慧电力、智慧交通、智慧安防等新行业模式,推动了电力、公安、市政、交通等行业的深度变革。在产业背景和技术日新月异的当下,

启明星辰全面布局城市安全运营，同时在无锡建立物联网安全总部，聚焦物联网安全。

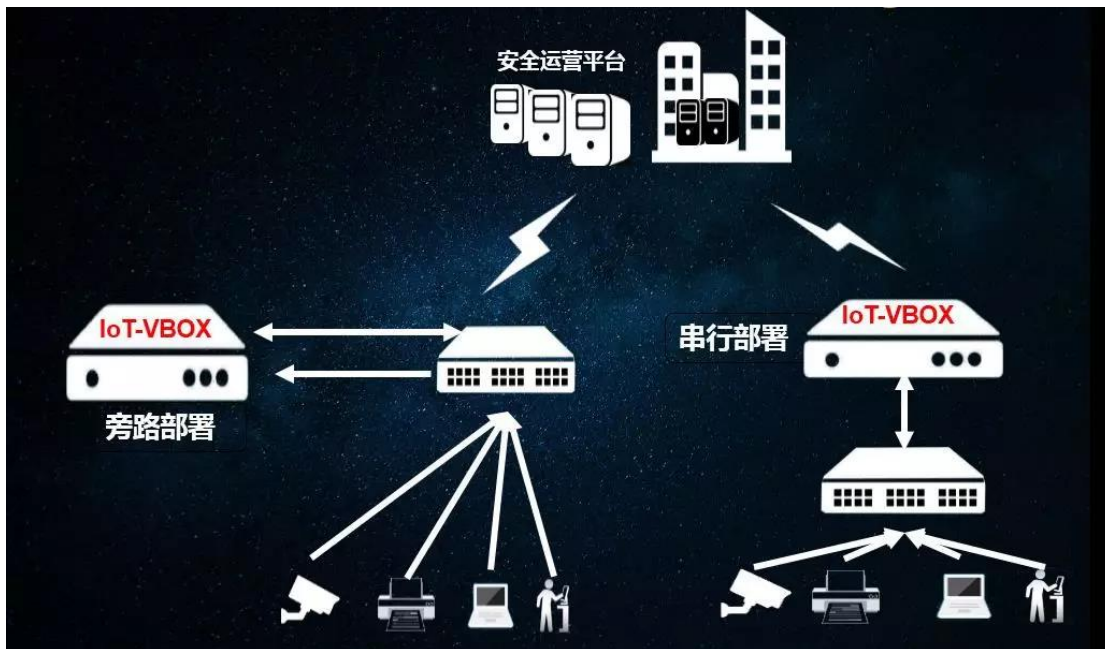
在集团的物联网安全战略议题下，物联网安全接入防护系统 IoT-VBox 面世，定义“物联网+”场景下物联安全新路线，为智慧城市的物联安全赋能。

IoT-VBox 正是围绕着“物联网+”场景下的安全需求，基于发现(Discover)、保护(Protect)、可视化(Visibility)和管控(Control)技术路线来构建物联网安全防护架构。



产品实现按需通断的访问控制。物联网终端碎片化的现状决定了其有无穷的安全漏洞，无限的补丁，按需通断访问控制则有效减少物联网终端的攻击平面，是最简洁有效的防护手段。





产品实现在线物联网终端行为学习。对于终端的数据流内容（Payload）行为建模，当终端被植入木马行为变化时，进行阻断报警防护。

### 1.3 郭启全总工关于等保 2.0 等五项工作内容的重要讲话

等保 2.0 时代也下调了等级测评周期，原来“第三级网络的运营者一年测评一次，第四级半年一次”，改为“第三级以上网络的运营者应当每年开展一次网络安全等级测评”。



这些诸多细粒度的变化，从制度层面给用户带来了一次知识更新的要求，同时也是为用户构建更加强大的安全能力提供了体系化的制度保障，可以说，等级保护 2.0 是一次网络安全的重大升级。

等保 1.0 时代	VS	等级 2.0 时代
<ul style="list-style-type: none"> <li>■ 五个规定动作： 定级、备案、建设整改、等级测评，监督检查。</li> </ul>	<p>工作内容</p>	<ul style="list-style-type: none"> <li>■ 满足等保 1.0 时代 5 个规定动作。</li> <li>■ 增加了：风险评估、安全监测、通报预警，案事件调查、数据防护、自主可控、供应链安全、效果评价、综治考核等方面。</li> </ul>
<ul style="list-style-type: none"> <li>■ 传统的网络和信息系系统。</li> </ul>	<p>保护对象</p>	<ul style="list-style-type: none"> <li>■ 从传统的网络和信息系系统，向“云大物智移”上扩展。</li> <li>■ 等保 2.0 则把云计算、大数据、物联网、工业控制、物联网、基础信息网络、其他信息网络等新业态也纳入了监管。</li> </ul>
<ul style="list-style-type: none"> <li>■ 十个安全控制域。</li> <li>■ 总体控制要求：（以三级为例）控制数量为 290 个点。</li> </ul>	<p>保护力度</p>	<ul style="list-style-type: none"> <li>■ 缩减为八个安全控制域。</li> <li>■ 总体控制要求：（以三级为例）控制数量从 290 个点，调整为 231 个点（以 GB/T-22239&lt;信息安全等级保护基本要求&gt;为对比点）。</li> </ul>

关键信息基础设施的定义：面向公众提供网络信息服务或支撑能源、通信、金融、交通、公用事业等重要行业运行的信息系系统或工业控制系系统；且这些系系统一旦发生网络安全事故，会影响重要行业正常运行，对国家政治、经济、科技、社会、文化、国防、环境以及人民生命财产造成严重损失。

#### 1.4 启明星辰亮相 CERNET 华中地区 2018 年学术论坛

由 CERNET 华中地区网络中心、河南省教育科研计算机网 HERNET 网络中心及 CERNET 湖南省主节点主办的，中国教育和科研计算机网 CERNET 华中地区 2018 年学术论坛在河南省驻马店成功召开。郑州启明星辰信息安全技术有限公司应邀出席，围绕“融合·创新·教育信息化 2.0”这一议题，与参会人员广泛的学术交流和分享。未来，启明星辰将继续通过‘平台+服务’式的安全新运营方式，为高校教育部门提供持续、及时、定制化的网络安全服务，助力高校教育信息化 2.0 建设。

## 2. 东软

### 2.1 华为和东软携手完成首次 C-V2X 互联互通应用测试

近日，基于中国标准的 LTE-V2X “三跨”互联互通展示，也即跨通信模组（芯片）、

跨终端提供商、跨整车厂商的互联互通展示在上海汽车城成功进行。在这次活动中，华为和东软携手完成首次 C-V2X 互联互通应用测试，成功实现了多种品牌车型的网络通信功能。

这次测试在 11 月 6 日-8 日中国汽车工程学会年会期间举行，由中国智能网联汽车创新联盟、IMT-2020 (5G) 推进组 C-V2X 工作组、上海国际汽车城(集团)有限公司共同举办。测试基于采用 3GPP R14 LTE-V2X PC5 直连通信技术底层通讯技术，使用工信部《车联网(智能网联汽车)直连通信使用 5905-5925MHz 频段的管理规定(暂行)》的工作频段；采用《合作式智能运输系统 专用短程通信 第 3 部分：网络层和应用层规范》《合作式智能运输系统 车用通信系统 应用层及应用数据交互标准》等 LTE-V2X 网络层和应用层中国标准；从 LTE-V2X 技术的不可替代性出发，选取了 7 个典型的车与车、车与路应用场景：包括车速引导、车辆变道/盲区提醒、紧急制动预警、前向碰撞预警、紧急特殊车辆预警、交叉路口碰撞预警和道路湿滑提醒。

### 演示场景方案 (必选+可选)

注：左转辅助场景，由于公园道路限制，难以实现。建议换成其他可选场景。

- G 道路湿滑提醒
- H 前方急弯提醒
- I 行人横穿预警

- A 车速引导
- B 车辆变道/盲区提醒
- C 紧急制动预警
- D 前向碰撞预警
- E 紧急特殊车辆预警
- F 交叉路口碰撞预警



华为携手东软共同在演示车型上顺利完成各项测试。华为 LTE-V2X 车载终端基于 Balong 765 芯片，具备以下特点：充分考虑 C-V2X 独特场景和性能要求，LTE uu 和 PC5 并发、应用处理器高度集成，支持二次开发，按照车载行业前装质量要求进行管控。在本次三跨测试中，上述优点已经得到充分验证和认可。这些特点将在后续的商用成本，可靠性，开发周期上持续体现。

东软 VeTalk 是国内首款基于 DSRC 和 LTE-V 通信技术的 V2X 产品，可以为整车厂商、一级供应商、运营商、智能交通行业提供一站式的解决方案，包括硬件开发套件、面向量产的 V2X-ECU、网络协议栈、SDK、应用示例、标准一致性测试与仿真模拟测试平台、V2X



Server 等等，全面支持中国市场以及美国、欧洲、日本 V2X 标准。

### 3. 山石网科

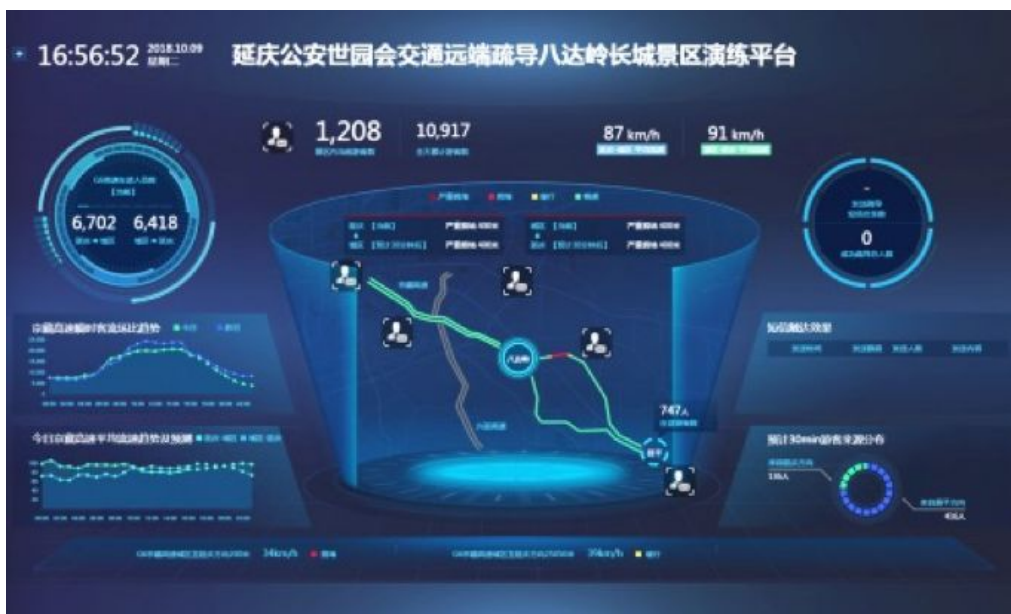
#### 3.1 山石网科参与 GITC 2018 北京站

以“知者创物”为主题的 2018 GITC 全球互联网技术大会于 11 月 22 日-23 日，在北京国家会议中心盛大开幕。“知者”，即互联网领域中，一群本着创新精神为核心，以开发协作，通过迭代创新方式推动行业前进的人。作为“知者”之一，山石网科很荣幸受邀参加大会。山石网科虚拟化防火墙山石云·界获颁“互联网最具技术创新奖”。

### 4. 亚信

#### 4.1 亚信科技为智慧交通疏导提供新方案

亚信科技将其电信级解决方案能力向其他行业输出，在智能交通、车联网相关领域，也取得了不错的应用效果。今年十一，亚信科技联合延庆公安合作部署了“智享大数据公共安全平台”，有效解决了八达岭景区道路的拥堵问题。



### 5. 绿盟

#### 5.1 绿盟科技荣获“2018 年度中国用户体验创新示范企业”

绿盟科技以用户体验助力数字工控工具建设、网络安全数据可视化能力建设等成功实践，

荣获“2018 年度中国用户体验创新示范企业”称号。。

## 四、 容器技术及安全动态

### 1. 云原生计算基金会宣布 Envoy 项目正式“毕业”



云原生计算基金会（简称 CNCF）日前宣布，Envoy 代理已经成为其继 Kubernetes 与 Prometheus 之后第三个正式毕业的项目。

Envoy 项目旨在实现服务与边缘代理功能，通过管理微服务之间的交互以确保应用程序性能，从而协助简化云原生架构的过渡与运营流程。该项目提供的超时、速率限制、断路、负载均衡、重试、统计、日志记录以及分布式追踪等高级功能，可以帮助用户以高容错性以及高可靠性方式处理各类网络故障问题。

Envoy 的进程外架构适用于任何应用程序、任何语言或者运行时；其支持的协议与功能包括 HTTP/2、gRPC、MongoDB、Redis、Thrift、外部授权、全局速率限制以及一个富配置 API 等等。

得利益于其活跃的维护者团队以及近 250 位贡献者的支持，Envoy 被 InfoWorld 网站评为 2018 年云计算最佳开源软件之一。该项目的用户社区目前仍在不断增长，其中包括 Airbnb、Booking.com、eBay、F5、谷歌、IBM、Lyft、Medium、微软、Netflix、Pinterest、Salesforce、Square、Stripe、腾讯、Twilio、Verizon 以及 VSCO 等等。截至目前，项目提交量已经超过 3000 份。

### 2. Aqua Security 在 AWS 市场上发布首个容器安全解决方案

Aqua Security 在 AWS Marketplace for Containers 上推出其云原生和容器安全平台，以及 AWS Marketplace 上的其他几个 Aqua 产品，使得 Amazon 原生应用程序的企业级安全性可

访问且易于使用服务（AWS 客户），并强调 Aqua 致力于支持客户对混合云解决方案的需求。

AWS Marketplace for Containers 允许 AWS 客户使用 Amazon Elastic Container Service（Amazon ECS）控制台和 AWS Marketplace for Containers 来发现、生成和部署容器解决方案 - 包括 Aqua Container Security Platform，满足客户工作负载保护需求。

### 3. 微软智能云 Azure Kubernetes 容器服务落地中国，开启预览

2018 年 11 月 13 日，由 Linux 基金会主办的年度开源云原生社区大会 KubeCon + CloudNativeCon 2018 在上海举行，Kubernetes 开源项目联合创始人、微软杰出工程师 Brenda Burns 在主题演讲中展望了 Kubernetes 项目的最新进展和未来，同时宣布 Azure Kubernetes Service(AKS)已登陆由世纪互联运营的 Microsoft Azure，在中国市场开放预览。

2016 年 4 月，微软在全球运营的 Microsoft Azure 上推出 Azure Container Service。于 2017 年 2 月整合 Kubernetes 容器调度编排平台，并于 11 月更名为 Azure Kubernetes Service（AKS）。这项服务能大大简化 Kubernetes 的部署和运营。让开发者可靠、灵活地自由伸缩应用架构。

**轻松部署和管理 Kubernetes:** 通过 Azure 门户和 Azure CLI 轻松创建群集，还可通过基础架构即代码工具（如 Azure 资源管理器模板和 Terraform）进行配置；可自动升级和弹性伸缩、简化群集维护；用户能随时了解 Kubernetes 托管环境的运行情况，在 Azure 门户中查看控制面板监控、日志及容器运行状况；

**自由伸缩和运行容器应用:** 内建应用程序自动扩展功能，以满足不断增长的用量需求；借助遍布全球的 Azure 区域数据中心，AKS 可实现容器化应用的跨区域部署；Azure 流量管理器能将流量路由到最近区域，提升应用程序性能；借助 Virtual Kubelet 的支持（预览版），在流量出现峰值时，可使用 Azure Container Instance 服务对 AKS 群集中的容器实现弹性扩容；

**Kubernetes 环境安全管控:** 利用 Azure Active Directory 帐户和用户组，控制对 Kubernetes 群集的访问；将 Azure Active Directory 与 Kubernetes 角色访问控制集成，可对 Kubernetes 资源访问实现精细控制；使用 Key Vault 保护 Kubernetes 主节点和代理节点所用的密码和其他密钥；通过自定义虚拟网络、Azure 容器网络接口 (CNI) 和网络策略执行保护容器网络通信安全；

**加速容器化应用的开发：**有效降低应用开发复杂度，使用 Helm 轻松定义、安装和升级复杂的 Kubernetes 应用程序，并自动构建和容器化应用程序；使用 Azure Dev Spaces 和 Visual Studio、Visual Studio Code 或 Azure CLI 加速开发、测试和调试容器；共享 AKS 群集并协同工作，无需复制或模拟依赖项；在几秒内便可通过 HTTP 路由访问已部署的应用；

**充分利用开源工具和 API：**AKS 基于完全开源的 Kubernetes，可让用户充分利用 Kubernetes 生态系统中的服务和工具；使用常用的开源工具（如 Helm、Draft 和 Brigade），可自动执行软件交付流水线；使用 Open Service Broker for Azure，轻松将 Kubernetes 与受 SLA 支持的 Azure 服务（如 CosmosDB）集成；

**轻松实现持续集成/持续部署（CI/CD）：**借助 Azure DevOps Project（预览版），只需三步即可使用完整的 CI/CD 流水线和应用监控，将应用程序部署到 Kubernetes。使用 Azure 容器镜像仓库，可简化容器开发并管理需要跨多个区域复制的容器镜像仓库；Azure 容器镜像仓库中的异地复制允许以单个实例的形式管理全局的镜像仓库，简化操作和管理。

#### 4. AWS 开源安全且快速的新概念微虚拟机 Firecracker

AWS 开源了用于 Serverless 计算的安全且快速的微虚拟机（microVM）Firecracker。

项目基于 Apache 2.0 开源：<https://github.com/firecracker-microvm/firecracker>

Firecracker 是一种专门用于创建和管理多租户容器和基于函数的服务的虚拟化技术，使用 Rust 开发，旨在加快 AWS Lambda 和 AWS Fargate 等服务的速度和效率。它是一种虚拟化技术，提供 Serverless 操作模型，专门用于创建和管理多租户容器与基于函数的服务。Firecracker 在轻量级虚拟机中运行工作负载，AWS 将其称为 microVM，它结合了硬件虚拟化技术提供的安全性与隔离性和容器的速度与灵活性。

Firecracker 的主要组件是虚拟机监视器（VMM），它使用 Linux 内核虚拟机（KVM）来创建和运行 microVM。Firecracker 采用极简设计，它剔除了不必要的设备和面向客户的功能，以减少每个 microVM 的内存占用和攻击面积，这可以提高安全性、缩短启动时间并提高硬件利用率。

Firecracker 目前支持 Intel CPU、AMD 与 Arm，同时它还将与流行的容器运行时集成。

Firecracker 开源原则如下：

- **内置安全性：**提供计算安全隔离，以支持多租户工作负载，并且用户无法失误禁用。用户工作负载同时被视为具备神圣（不可触及）与恶意（应予以防备）两种属性。

- 轻量级虚拟化：专注于短期或无状态工作负载而不是长期运行或持久性工作负载。Firecracker 的硬件资源开销是已知且有保证的。
- 极简主义：如果任务没有明确要求，将不会创建。仅维护每个功能的单个实现。
- 计算资源超额订购：Firecracker 向用户公开的所有硬件计算资源都可以安全地超额订购。

## 五、安全新产品及技术

### 1. 25 个欧盟成员国将开展电子作战领域合作

综合美国国防新闻周刊、政客及 MeriTalk 网站 2018 年 11 月 20 日以来报道，11 月 19 日，来自欧盟的 25 个国家的防长共同签署了一项军事协议，旨在加强联合电子作战能力。该协议由除丹麦、马耳他和英国以外的所有欧盟成员国签署。

根据 2017 年欧盟启动的永久合作架构（PESCO）防务协议，除一年前公布的最初的 17 个项目外，此次签署的军事协议中还包括了另外 17 个新项目。新的项目包括训练、能力发展，以及陆、海、空作战准备和网络防御等。PESCO 协议使欧盟成员国能够在安全和国防领域进行更紧密的合作。它允许有意愿和有能力的成员国共同发展能力，对共同项目进行投资，并加强其武装部队的作战准备。

### 2. 谷歌安卓应用防护增强：号称一个应用也不漏过

谷歌表示，用于扫描用户手机所安装应用的服务 Google Play Protect 已经大大增强。这一服务已经不止于能扫描用户从 Play 商店安装的应用。

谷歌官方博客中介绍称，Play Protect 已经可以分析它能在互联网上找到的每一个应用程序。Google Play Protect 会在互联网上搜寻 Google Play 商店外的所有安卓应用。之后会扫描这些第三方应用程序的恶意行为，然后在其数据库中对其进行分类和索引，这补充了谷歌的恶意指标数据库与其他数据集。

也就是说，在用户安装每一个非 Play 应用的时候，Google Play Protect 就已经了解它了。这样就可以立即提醒用户，设备上是否安装了恶意软件。

此前在 2017 年度的安全报告上，谷歌称 Google Play Protect 已可自动禁用大约 100 万台设备的 PHA（Potentially Harmful Application，潜在恶意应用），并且可以通过日常扫描，

更快地识别、删除大约 3900 万个 PHA。

### 3. 西门子修复防火墙漏洞，确保运营商安全通报

西门子公司周二发布了一系列解决方案，修复了其工业产品线中的八个漏洞。最严重的漏洞包括西门子 SCALANCE 防火墙产品中的跨站点脚本漏洞。该漏洞允许攻击者未经授权访问工业网络，使得运营商面临严峻风险。SCALANCE 防火墙用于保护安全工业网络免受不受信任的网络流量影响，并允许以不同方式过滤传入和传出网络连接。西门子 S602、S612、S623、S627-2M 和 V4.0.1.1 之前的软件版本的 SCALANCE 设备受到影响。

发现该漏洞的 Applied Risk 的研究人员表示，攻击者可以通过制作恶意链接并欺骗管理员（登录到 Web 服务器）来单击该链接来执行攻击。管理员执行此操作后，攻击者可以代表管理员在 Web 服务器上执行命令。“如果管理员被误导访问恶意链接，集成的 Web 服务器就会允许跨站点脚本攻击，” Applied Risk 研究员 Nelson Berg 在对该漏洞的分析中表示。“漏洞利用成功的话可会导致绕过防火墙提供的关键安全措施。”

### 4. 大疆身份识别系统漏洞允许攻击者将无人机变成间谍工具

大疆是世界最大的消费者无人机制造商，美国政府曾对大疆无人机发出警告，担心它收集的美国基础设施信息会提供给中国政府。现在 Check Point 的安全研究人员在大疆身份识别系统中发现了一个漏洞允许任何攻击者将无人机变成一种间谍工具。漏洞已经修复，它允许攻击者完全控制用户的账号，访问储存在云端的飞行记录，航拍照片，用户的信用卡信息，以及无人机摄像头和麦克风的实时信息。

### 5. 2018 Q3 Android 新恶意样本数量达 320 万个 同比增加 40%

根据 G DATA 近日公布的 2018 年第 3 季度报告，新 Android 恶意样本数量达到了 320 万个，与 2017 年同期相比增长了 40%。在分析报告中写道：“移动设备日益成为网络犯罪分子的攻击目标，特别是 Android 设备。其中最重要的原因是全球每 10 个人中就有 8 人使用 Android 设备。”

报告中指出平均每天会发现大约 11700 个新 Android 恶意软件样本，Android 平台的威胁程度日益加深，很多用户面临着设备被攻击的风险中。此外由于全球 80% 的手机均为 Android 系统，因此 Android 平台也是黑客重点攻击的目标。

## 6. 英特尔超线程 CPU 出现新漏洞

安全人员近期发现了一个新的英特尔超线程 CPU 漏洞，是一个非常严重的旁注漏洞。

该漏洞可使攻击者从同一 CPU 内核中运行的其他进程中找出受保护的敏感数据（如密码和加密密钥），并启用 CPU 的多线程功能。该漏洞被命名为 PortSmash(CVE-2018-5407)，现在已被列为与 Meltdown 和 Spectre 等漏洞同等级别。

## 7. 谷歌发布新安全功能，若禁用浏览器 Java Script 则无法登录

据外媒 ZDNet 报导，谷歌近日宣布了四项用于保护 Google 账户的新安全功能，不仅用于加强用户登录账户前后的保护，也适用于在受到黑客攻击后恢复的情况。第一项：如果用户在浏览器中禁用 JavaScript，那么 Google 将不允许用户登录。Google 使用 JavaScript 对访问登录页面的用户进行风险分析，如果将 JS 禁用，那么入侵者便能够逃过检查。第二项：谷歌将在官方 Google Play 附带的安全扫描程序 Google Play Protect 中列出安装在用户手机上的所有恶意软件。第三项：Google 将在安全检查中列出所有已授权可以访问用户 Google 数据的第三方应用和网站，用以提醒用户。第四项：针对账户被入侵后的恢复环节。它是一个重新获得访问权限并重新保护受损配置文件的新程序，除了帮助用户重新获得帐户访问权限外，还可以帮助他们查看与 Google Pay 帐户相关的财务活动，查看添加到 Gmail 或云端硬盘的新文件，以及保护其它服务的其它帐户与主 Google 帐户绑定的内容。

# 六、 网络安全投融资、收购事件

## 1. 收购

### 1.1 Threat Stack 完成对 Bluefyre 的收购

11 月 8 日，Threat Stack 完成对 Bluefyre 的收购，收购价未公开。Threat Stack 公司的云安全平台，旨在检测并告知用户云环境的变化情况。Bluefyre 帮助开发者部署能够事实检测和防御威胁的安全、Cloud Native 应用。

### 1.2 ForeScout Technologies 完成对 SecurityMatters 的收购

11 月 8 日，ForeScout Technologies 完成对 SecurityMatters 的收购，收购价 1.13 亿美元。

ForeScout Technologies 创立于 2000 年 4 月，总部位于美国加州 San Jose，是一家企业级网络安全公司，提供一种无代理的网络安全保护措施确保设备安全。SecurityMatters 是一家网络安全技术公司，致力于开发先进的网络监控，网络智能和网络保护技术。

### 1.3 SolarWinds 完成对 8MAN 的收购

11 月 15 日，SolarWinds 完成对 8MAN 的收购，收购价未公开。SolarWinds 提供网络安全管理软件产品，SolarWinds 正在改变各类规模的企业监控和管理其企业网络的方式。8MAN 是一家提供集成接入权限管理解决方案的公司。

### 1.4 BlackBerry 完成对 Cylance 的收购

11 月 16 日，BlackBerry 完成对 Cylance 的收购，收购价 14 亿美元。黑莓公司是加拿大的一家通信公司，主要产品为手提通讯设备黑莓手机。Cylance 是一家网络安全技术公司，其结合人工智能、算法科学和机器学习技术，提高公司、政府和终端用户解决最棘手的安全问题的能力。

## 2. 投融资

### 2.1 Shape Security 获得 2600 万美元的 E 轮融资

11 月 1 日，Shape Security 从 Baseline Ventures 和其他 8 位投资者处获得 2200 万美元的 E 轮融资。Shape Security 是一家互联网安全技术公司，专注于阻止自动化网络攻击和移动攻击。

### 2.2 Netskope 获得 1.68 亿美元的 F 轮融资

11 月 13 日，Netskope 从 Accel 和其他 6 位投资者处获得 1.68 亿美元的 F 轮融资。Netskope 是领先的云业务安全接入代理（Cloud Access Security Broker, CASB）。Netskope 的云规模安全平台能够让用户自由使用云化业务时，满足安全需求和相关的合规性监管要求。重点包括：1. 能够对所有的 APP/SaaS 的业务风险进行发现和评估，并且能够给出一个评价指标。用户可以根据这个评价指标选择是否采用该 APP/SaaS 服务。2. 能够提供基于身份的接入控制管理。很方便的将云及 SaaS 服务与认证系统对接，对不同的接入用户赋予不同的操作和访问权限。提供比 SaaS 服务商更丰富的访问控制功能。3. 能够对用户和管理员的操作、访问、内容、文件等进行监控和回溯，并且在重要事件发生时自动告警。例如可以设置文件密级，当高密级文件发生不合规操作时，自动阻断该操作，并记录、告警，从而实现数据防泄



密。也可以对登陆环境进行要求，防止非法设备登陆。4. 可以防止来自云服务商本身的数据泄密。例如，在用户输入过程中对数据进行加密，使得云端数据都处于加密状态，保障数据安全。5. 能够对云上的恶意软件进行监控和发现，防止来自云内部的恶意软件。

### 2.3 Automox 获得 930 万美元的 A 轮融资

11 月 13 日，Automox 从 Blue Note Ventures 和其他 3 位投资者处获得 930 万美元的 A 轮融资。Automox 是一个基于云的自动化补丁修复平台，可以在 Windows、Linux、Mac 和第三方软件之间自动化修复补丁。其简单易管理的流程可将修补时间和资源减少 90%。Automox 还可以管理系统配置和持续监控基础设施，提供系统安全性。

### 2.4 Duality 获得 400 万美元的未知轮融资

11 月 13 日，Duality 从 Team8 处获得 400 万美元的未知轮融资。Duality 的突破性创新技术使安全的数字协作成为可能。有了 Duality 的技术，企业可以在数据加密的同时安全协作，将高级分析和人工智能应用于数据，生成洞察，而无需暴露原始数据。

### 2.5 XM Cyber 获得 2200 万美元的 A 轮融资

11 月 13 日，XM Cyber 从 Macquarie Capital 和其他 4 位投资者处获得 2200 万美元的 A 轮融资。XM Cyber 提供了首创的全自动 APT 仿真平台以连续暴露所有攻击矩阵并实施补救。

### 2.6 Alcide 获得 700 万美元的 A 轮融资

11 月 19 日，Alcide 从 CE Ventures (CEIIF)和其他 2 位投资者处获得 700 万美元的 A 轮融资。Alcide 为混合和多计算数据中心提供专用的网络安全平台，以任何规模加快运营速度。Alcide 使 DevOps、安全和工程团队能够通过简单自主的控制来管理和保护不断发展的数据中心和混合云。Alcide 提供实时可见性和应用的微观视角，确保数据中心免受网络攻击，包括恶意的内部活动和数据泄露。