内容摘要

云厂商方面，首先 AWS、GOOGLE 和微软都发布第三季度财报，AWS 同比上一季度增长持平，微软 Azure 同比上一季度增速放缓；在技术和方案进展上，AWS 推出 4TB 内存的虚拟机，VMware 和山石发布微隔离可视化方案，谷歌和思科形成混合云联盟，阿里联合量子研究所发布量子云计算平台，华为云发布了三款安全产品：安全体验服务、WEB 漏洞扫描、主机安全服务。

开源云方面，九州云加入 ONF 基金会。

云安全厂商方面，首先，国内安全厂商赞助各类安全技能大赛，其中安恒信息协助举办山东省第三届安全职业技能大赛，360 企业安全协助“湖湘杯”2017 网络安全技能大赛；其次，国内各安全厂商 10 月份继续宣传自身安全产品，安恒在阿里云栖大会上宣传自己的信息安全综合保险业务和“天池”云安全管理平台；再次，国内厂商亦积极开展相关合作，其中 360 企业安全与太极股份签署战略合作协议，安恒信息参与阿里“数据安全合作伙伴计划”。

容器安全方面，CNCF 增加了容器安全开源项目 Notary 和 The Update Framework；Datadog 正式推出实时容器监控功能；CIR-O 1.0 发布的容器标准使得 Kubernetes 兼容了 OCI；另外在 DockerCon2017 Euro 大会上，Docker 宣布同时支持 Swarm 和 Kubernetes。

安全新技术方面，研究人员研制出新的双因素认证技术；能在文字识别上超越神经网络方法的全新概率生成模型方法研究技术出现；NetBSD, OpenBSD 加

强了内核安全机制以及为了有效应对 BGP 劫持，美国出台了新的 SIDR 标准。

网络安全公司投融资方面，10 月国内安全领域没有涉及资本变动情况，而国外总共具有 8 起包括 IPO 和融资的相关事项。从事网络准入控制的美国安全厂商 ForeScout 在 10 月完成了公开 IPO 和正式纳斯达克上市，IPO 总共筹集超过 1 亿资本。8 家美国从事网络安全的公司均获得至少 2000 万美元以上的融资，其中 IT 行业安全风险分析服务提供商 Skybox Security 从 CVC Capital Partners（私募投资公司）和 Pantheon（磐石基金）以私人股本的形式获得最高融资额 1.5 亿美元。

2017 年 10 月 31 日

启明星辰核心技术研究院 云安全研究组

目录

本期云安全动态内容摘要..... i

目录.....iii

国内外云+安全动态报告 1

一、 云厂商动态..... 1

1. AWS 云安全动态 1

1.1 AWS 发布第三季度财报，同比上一季度增速持平 1

1.2 AWS、诺基亚合作致力于提高云计算、5G 和 IoT 覆盖 1

1.3 Salesforce 公司使用 AWS 数据中心为澳大利亚客户提供服务 2

1.4 AWS 推出 4TB 内存的虚拟机..... 2

2. VMware 云动态..... 2

2.1 华云与 VMware 达成战略合作 2

2.2 VMware 与 F5 联手，打造无缝跨云环境..... 2

2.3 山石网科与 VMware 发布基于 NSX 平台的微隔离可视化方案 3

3. GOOGLE 云动态 3

3.1 谷歌和思科结成混合云联盟 3

3.2 谷歌母公司 Alphabet 发布了第三季度财报..... 3

4. 微软 Azure 云动态..... 4

4.1 微软企业云年收入超 204 亿美元提前达到并超出两年前目标预期..... 4

4.2 微软推出 Azure 与亚马逊 AWS“云服务地图”对比工具 4

4.3 通用电气软件平台与微软云展开深入合作 4

4.4 微软基于区块链的 Azure 云服务为美国政府安全问题保驾护航 4

4.5 微软打造绿色云服务，买下通用电气在爱尔兰 15 年风能..... 5

4.6 超级计算机制造商 Cray 宣布与微软达成了一项全新的合作 5

4.7 微软 Azure 宣布支持 OpenBSD..... 5

5. 阿里云动态 5

5.1 阿里云宣布将携手 NVIDIA 提供人工智能培训计划 5

5.2 阿里云发布 Link 物联网平台..... 5

5.3 阿里云联合中科院量子创新研究院发布量子计算云平台..... 5

6. 腾讯云动态 6

6.1 腾讯云发布生物基因解决方案 6

7. 华为云动态 6

7.1 华为云发布三款安全服务 6

7.2 华为云企业智能推出 Elasticsearch 搜索服务 6

7.3 哈尔滨市与华为战略合作，共同推进云计算产业发展..... 7

二、 开源云动态..... 7

1. Openstack 动态..... 7

2. Easystack 动态 7
3. 99CLOUD（九州云）动态 7
3.1 九州云应邀加入 ONF 基金会,助力开源 SDN 技术落地 7
三、 云安全厂商动态 8
1. 山石网科 8
1.1 山石网科携手 VMware 发布基于 NSX 平台的微隔离可视化方案 8
2. 亚信 8
3. 绿盟科技 8
3.1 绿盟科技漏洞管理市场第一 8
3.2 “赛尔绿盟安全云”促进高校网络信息安全建设 9
4. 360 企业安全 9
4.1 360 企业安全助力“湖湘杯”2017 网络安全技能大赛启航 9
4.2 太极股份与 360 企业安全集团签署战略合作协议 10
5. 安恒 10
5.1 安恒信息参与阿里“数据安全合作伙伴计划” 10
5.2 安恒信息协助举办山东省第三届安全职业技能大赛 10
5.3 安恒信息亮相 2017 年云栖大会 10
6. 安天 11
7. Fortinet 11
7.1 Fortinet 最新的沙盒解决方案获 NSS 实验室推荐 11
7.2 Fortinet 在工业物联网中扩展安全防护和安全可视化架构 11
7.3 Fortinet 在 Oracle 云市场中推出其 FortiGate 虚拟机 12
8. Checkpoint 12
四、 容器技术及安全动态 12
1. CNCF 新增项目 Notary 和 The Update Framework 12
2. Datadog 正式推出实时容器监控功能 12
3. CRI-O 1.0 版本发布 13
4. Docker 宣布同时支持 Swarm 和 Kubernetes 13
五、 安全新产品及技术 14
1. 研究人员研制出新的双因素认证 14
2. 全新概率生成模型方法能在文字识别上超越神经网络方法 14
3. NetBSD, OpenBSD 加强内核安全机制 15
4. 美国出台新的 SIDR 标准，可有效应对 BGP 劫持 15
六、 网络安全投融资、收购事件 16
1. IPO 16
1.1 ForeScout Technologies IPO 上市 16

2. 投融资 16
2.1 Skybox Security 获 1.5 亿私有股本资金 16
2.2 KnowBe4,LLC 获 3000 万美元 B 轮融资 16
2.3 CrowdStrike 获 2500 万美元 D 轮融资 16
2.4 Duo Security 获 7000 万美元 D 轮融资，估值超过 10 亿 17
2.5 SecurityScorecard Inc.获 2750 万美元 C 轮融资 17
2.6 Attivo Networks 获 2100 万美元 C 轮融资 17
2.7 Contrast Security 获 3000 万美元 C 轮融资 17

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 AWS 发布第三季度财报，同比上一季度增速持平

亚马逊发布第三季度财报，报告显示，亚马逊营收为 437.4 亿美元，同比增长 34%，净利润 2.56 亿美元，而分析师平均预期为 421.4 亿美元。亚马逊 AWS 云计算业务的营收为 45.7 亿美元，高于分析师预期的 45.1 亿美元。从亚马逊 AWS 的增长速率上来看，同比上一季度保持持平，约 42%。

1.2 AWS、诺基亚合作致力于提高云计算、5G 和 IoT 覆盖

AWS 与诺基亚本周宣布达成了战略合作关系，将共同致力于提高云计算、5G 和 IoT 的覆盖面。

- 诺基亚计划向服务提供商提供与 AWS 部署计划相关的基础设施和应用程序的咨询、设计、集成、迁移和运营帮助。
- 诺基亚的 Nuage Network 软件定义广域网（SD-WAN）服务的客户将能够集成到 AWS 的云端，并且他们将能够使用集成的用户界面来管理混合环境中的连接。
- 此外，两家公司正在推出 5G 和边缘云策略，包括通过诺基亚和 AWS 开发的参考设计为客户提供指导。
- 计划通过将 AWS 的 Greengrass 和机器学习工作与诺基亚的多接入边缘计算（MEC）和所有连接事物的智能管理平台（IMPACT）相结合，目标是抢占新兴的物联网领域。
- AWS 于 6 月推出了 Greengrass 软件，旨在帮助边缘设备处理数据并与 AWS 云进行通信，该软件利用了 AWS 的 Lambda 项目，该项目已经成为近来无服务器计算激增的基础，诺基亚是该项目的初始成员之一。

1.3 Salesforce 公司使用 AWS 数据中心为澳大利亚客户提供服务

Salesforce 公司与 AWS 在今年 3 月宣布的战略合作伙伴关系，Salesforce 公司在澳大利亚的客户可以访问 Salesforce 客户平台，其中包括销售云，服务云，Salesforce 平台，社区云，分析云，金融服务云等。Salesforce 公司已经注册使用 AWS 悉尼地区的服务，Telstra 公司是 Salesforce 公司的澳大利亚第一家客户，可以访问 AWS 悉尼地区的 Salesforce 客户平台。

1.4 AWS 推出 4TB 内存的虚拟机

AWS 推出了最新的 EC2 实例——x1e.32xlarge，它是目前最大的 EC2 实例，提供了 4TB DDR4 内存、Intel Xeion E7 8880 v3 Haswell 处理器和 2.3GHz（128 vCPU）L3 缓存。根据 AWS 官方文档所述，它的网络带宽最高可以达到 25Gbps。

x1e.32xlarge 目前仅在四个 AWS 区域可用：1.美国东部（北维吉尼亚州）2.美国西部（俄勒冈州）3.欧盟（爱尔兰）4.亚太地区（东京）。

微软 Azure 最大的实例拥有 2TB 内存，Google 为 416GB，所以从内存方面来看，AWS 拥有目前内存最大的实例。不过其成本也很高，在美国东部区域每小时费用为 26.688 美元，在东京为 38.688 美元。

2. VMware 云动态

2.1 华云与 VMware 达成战略合作

华云与 VMware 达成战略合作，加速 VMware vCloud Air Network 计划在中国的落地。

目前华云已经成为了 VCAN 的核心战略伙伴，将 vCAN 作了本地化的开发和应用结合，更在市场营销端，制定了 vCAN 未来的发展规划。已在华云自建数据中心搭建了 vCAN 节点，同时，华云利用在私有云、混合云、大数据方面的技术优势，已经成功找到了业务的切入点。

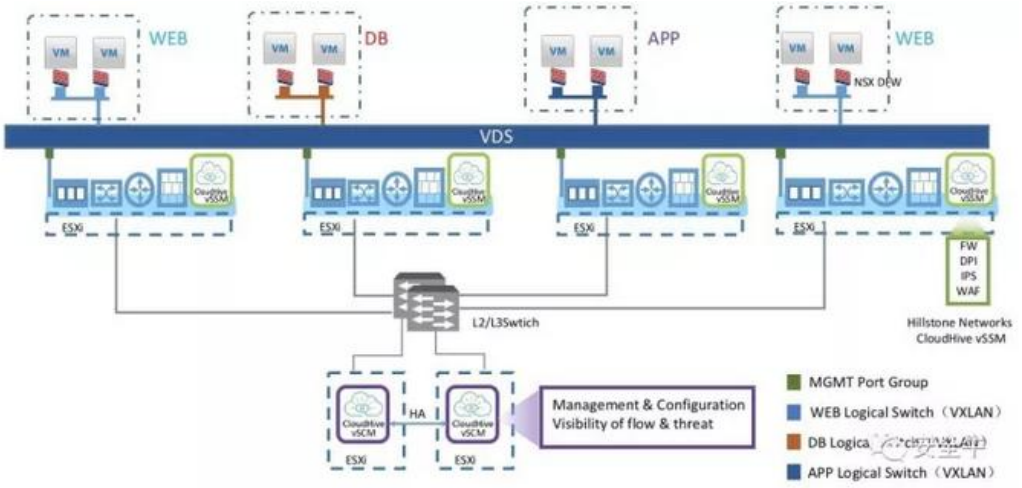
2.2 VMware 与 F5 联手，打造无缝跨云环境

为提升双方用户的使用体验，VMWARE 与 F5 公司持续保持着开发级合作模式。

通过合作，用户在部署环境时，只需要考虑自身业务需求与发展方向，而无需顾虑兼容问题即可快速、安全的部署，从而保证了核心业务延续性。

2.3 山石网科与 VMware 发布基于 NSX 平台的微隔离可视化方案

2017 年 10 月 24 日，山石网科携手 VMWARE，发布支持 NSX 的网络虚拟化平台的全新山石云.格微隔离可视化方案。虚机的虚拟网卡(vNIC)接入在 NSX 的分布式防火墙(DFW)上，DFW 再接入虚拟交换机，相当于为每个虚机的网卡都配备了一个防火墙。根据管理员的设置，DFW 会将选择了深度防护的数据包，重定向给部署在每台 ESXi 的云·格的 vSSM 卡，最后云·格再把通过安全审核的数据包送到虚拟交换机上。



3. GOOGLE 云动态

3.1 谷歌和思科结成混合云联盟

Google 和思科宣布企业混合云的合作，让思科私有云环境得以介接 Google 公有云端。这项合作结合思科的网管、安全、服务管理技术，以及 Google 的容器丛集管理系统 Kubernetes、微服务管理框架 Istio 及 API 管理平台 Apigee 等技术，让思科企业客户有扩充需求时，更容易将其现有部署的应用及资料搬移或扩展到 Google Cloud Platform 上，企业开发人员还能以熟悉的开发工具、runtime 及生产环境来开发新的云端及本地部署应用。

3.2 谷歌母公司 Alphabet 发布了第三季度财报

谷歌母公司 Alphabet 发布了第三季度财报中，Alphabet 第三季度总营收为 277.72 亿美元，比上年同期的 224.51 亿美元增长 24%；Alphabet 第三季度净利润为 67.32 亿美元，比去年同期的 50.61 亿美元增长 33%。

据相关数据统计，在这个季度里，包含谷歌云计算业务的“Google other ”营收为 34.05 亿美元，同比增长 40%；上一个季度里这部分业务营收是 30.9 亿元，增长速度为 42%。根据外媒分析师预计，谷歌云平台占据了其它营收的大约 15%。

4. 微软 Azure 云动态

4.1 微软企业云年收入超 204 亿美元提前达到并超出两年前目标预期

微软发布了截至 2017 年 9 月 30 日的 2018 财年第一季度财报。报告显示，微软第一财季营收 245 亿美元，与去年同期相比增长 12%；净收益为 66 亿美元，比去年同期增长 16%。其中，企业级云业务表现尤其出色，按照第一财季的收入水平，微软的企业级云业务年收入超 204 亿美元。

在第一财季里，微软企业云（微软把 Office 365 commercial, Azure, Dynamics 365,和其他云业务统称“商业云”）的各部分业务都保持了快速增长，其中 Office 365 commercial 业务营收同比增长 42%，Dynamics 365 业务营收增长 69%，Azure 业务营收增长 90%。

Azure 业务实现 90%增长，但是增长速度在过去的季度里确实是在放缓。过去四个季度里，Azure 的营收增长速度分别是：93%、93%、97%和 90%。

4.2 微软推出 Azure 与亚马逊 AWS“云服务地图”对比工具

微软推出了一款名叫“云服务地图”（Cloud Services Map）的对比工具。其旨在帮助客户更好比对 Azure 和 AWS 的差异利弊，从而凸显自身的优势。

“云服务地图”，极大地简化了分析的过程，明确地列出了各项利弊，有助客户规划跨云环境和迁移。根据 RightScale 公司发布的 2017 年度云计算报告，企业平均在 1.8 个公共云上运行他们的业务。

4.3 通用电气软件平台与微软云展开深入合作

通用电气和微软将宣布一项更深入的合作，此次合作涉及通用电气的 Predix 工业互联网平台和微软的 Azure 云平台。

4.4 微软基于区块链的 Azure 云服务为美国政府安全问题保驾护航

在华盛顿举行的微软 Government Cloud Forum 2017 论坛上，微软宣布正在启动 Azure Government Secret 服务，该服务为政府机构提供云计算服务。这个进展将极大地拓展微软区块链技术的服务范围。微软还为目前的政务云（Government Cloud）用户提供区块链即（blockchain-as-a-service）服务套装。

微软的 6 个数据中心已经被“隔离”了，并且获得了国防部临时的“Level 5”授权。另外，还获得了包括联邦风险和授权管理计划（FedRAMP）和国防情报系统局的证书。

4.5 微软打造绿色云服务，买下通用电气在爱尔兰 15 年风能

微软公司已经与通用电气公司签署了一份 15 年协议，购买通用电气的新 37 兆瓦风力发电厂生产的所有风能。这座风力发电厂位于爱尔兰西南部的凯里郡（CountyKerry）。

4.6 超级计算机制造商 Cray 宣布与微软达成了一项全新的合作

全球领先的超级计算机制造商 Cray 宣布与微软达成了一项全新的合作，让 Cray 系统无缝整合到 Azure 数据中心，为微软云服务提供加持。本次合作主打人工智能、全规模建模仿真、高级分析领域（比如生物技术 / 自动驾驶汽车 / 航天工程）等运算密集型应用。

4.7 微软 Azure 宣布支持 OpenBSD

微软的云平台现已支持 OpenBSD 6.1 系统。OpenBSD 是一款开源的操作系统，被很多安全专家认为是最安全的类 UNIX 操作系统。该系统的运作方式及其不间断且全面的源代码审核使得其被广泛应用于创建防火墙，OpenBSD 还适用于构建分布式环境中的隐私网络服务。

5. 阿里云动态

5.1 阿里云宣布将携手 NVIDIA 提供人工智能培训计划

NVIDIA 深度学习学院（DLI）将联手阿里云培训与认证平台阿里云大学以及云栖社区，基于阿里云异构计算平台合作推出人工智能相关的在线培训。阿里云将充分利用云端 NVIDIA GPU 的强大优势为遍布全球的客户提供人工智能动手实验培训课程。此外，双方还将合作开发针对人工智能领域的培训内容，为 NVIDIA 深度学习学院及阿里巴巴大学提供更多前沿的人工智能内容支持。

5.2 阿里云发布 Link 物联网平台

阿里云在 2017 杭州·云栖大会上宣布正式发布 Link 物联网平台，未来还将借助阿里云在云计算、人工智能领域的积累，使物联网具备智能而成为智联网。

阿里云 Link 物联网平台将战略投入物联网云端一体化使能平台、物联网市场、ICA 全球标准联盟等三大基础设施，推动生活、工业、城市三大领域的智联网。

5.3 阿里云联合中科院量子创新研究院发布量子计算云平台

2017 杭州·云栖大会期间，——阿里云联合中国科学院量子信息与量子科技创新研究

院（上海）共同宣布了“量子计算云平台”上线。

6. 腾讯云动态

6.1 腾讯云发布生物基因解决方案

在第四届全国功能基因组学高峰论坛上，腾讯云与百迈客生物科技宣布达成战略合作，并正式发布生物基因解决方案，开放腾讯云计算、存储、人工智能等各项 IT 能力，助力生物基因行业发展。

7. 华为云动态

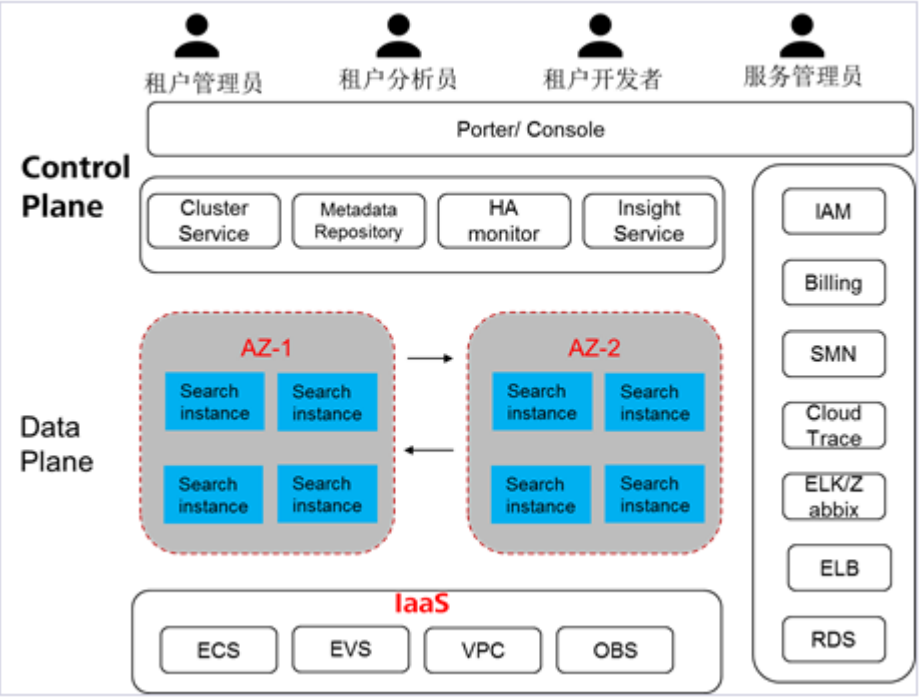
7.1 华为云发布三款安全服务

10 月 20 日，在华为云中国行.昆明站，华为云发布了 3 款新服务：

- 安全体验服务：由安全专家对云用户的系统、应用等进行深度检测，发现其存在的安全漏洞、风险，并给出修复建议和安全解决方案。
- Web 漏洞扫描：则类似自动化的安全体验，主要针对用户的 Web 站点和应用，进行自动化检测，发现安全问题，无需用户操心，无需安装和部署任何软件，一键即可开启。该服务还可以提前检测出网站的漏洞并且提供修复建议，提升网站的总体安全性。
- 主机安全服务：在用户授权下，可在云主机上一键安装主机安全插件，为用户提供账户破解防护、弱口令检测、恶意程序检测和网页防篡改等功能，降低主机被入侵的风险。

7.2 华为云企业智能推出 Elasticsearch 搜索服务

华为云企业智能重磅推出 Elasticsearch 服务，目前已开放公测。



7.3 哈尔滨市与华为战略合作，共同推进云计算产业发展

2017 年 10 月 23 日，哈尔滨市政府与华为公司共同签署云计算产业战略合作协议。同时，哈尔滨经济技术开发区也和华为公司达成战略合作。哈尔滨和华为将充分发挥各自优势，在灾备数据中心、软件开发云、城市产业云等领域进行全方位合作。

二、 开源云动态

1. Openstack 动态

暂无更新。

2. Easystack 动态

暂无更新。

3. 99CLOUD（九州云）动态

3.1 九州云应邀加入 ONF 基金会,助力开源 SDN 技术落地

九州云应邀正式加入开放网络基金会(Open Networking Foundation)，简称“ONF 基金会”，

参与 OPENCORD 项目建设。这也是继加入 Linux 基金会与 CNCF 基金会之后，九州云在开源技术领域的进一步深入探索。通过积极参与全球 SDN 标准制定，将有力地推动开源 SDN 技术在中国的落地应用，打造持续发展的开源软件公司。

三、 云安全厂商动态

1. 山石网科

1.1 山石网科携手 VMware 发布基于 NSX 平台的微隔离可视化方案

山石网科发布支持 VMware NSX 网络虚拟化平台的全新“山石云.格”微隔离可视化方案。该集成解决方案可以保护数据中心内外的工作负载。通过采用该解决方案，客户可以获得以下收益：

- 从网络到应用，实现数据中心流量的全面威胁可视化，有效抵御一切潜在威胁；
- 数据中心内部及云端的全自动化的先进安全防护；
- 有效编排以便实现安全扩展。

其余信息可见云厂商动态 VMware 部分。

2. 亚信

暂无更新。

3. 绿盟科技

3.1 绿盟科技漏洞管理市场第一

据 IDC 最新发布的《2016 年中国 IT 安全市场份额报告》显示，绿盟科技的漏洞管理产品以 23.3%的市场份额连续第六年领跑中国区市场。

绿盟远程安全评估系统（NSFOCUS RSAS）提供系统漏洞漏洞扫描、配置核查、web 漏洞扫描、弱口令扫描四合一功能，可部署在传统机房和虚拟化云环境，满足风险合规要求。目前绿盟 RSAS 支持的系统漏洞数已超过 20000+。同时，绿盟 RSAS 已实现在纯国产化 CPU 和纯国产化操作系统硬件平台上的运行。目前绿盟 RSAS 在金融、运营商、政府、能源等行业大中型企业覆盖度已超过 70%。

针对分布式部署场景，绿盟科技推出新一代集中漏洞管理平台—基于威胁情报的绿盟威胁和漏洞管理平台（NSFOCUS TVM），跟踪分析漏洞披露事件，将结果推送到客户侧平台，评估漏洞影响范围，协助漏洞应急响应工作，并结合对安全漏洞情报的分析，帮助客户提高漏洞加固效率，推动漏洞管理工作的落实。

3.2“赛尔绿盟安全云”促进高校网络信息安全建设

“赛尔绿盟安全云”是由赛尔网络有限公司（简称赛尔网络）和北京神州绿盟信息安全科技股份有限公司（简称绿盟科技）共同运营的教育行业安全云，旨在促进教育网络信息安全事业的发展，打造教育行业安全绿色的网络环境。

“赛尔绿盟安全云”运营中心依托 20 台虚拟机组成的处理集群（vCPU 容量达到 320 核，内存容量达到 400G B，存储容量达到 20T B）以及 10 套脆弱性检测引擎，为用户提供网站安全监测服务、远程漏洞扫描服务和可管理安全服务。

4. 360 企业安全

4.1 360 企业安全助力“湖湘杯”2017 网络安全技能大赛启航

由湖南省委网信办、湖南省教育厅、湖南省经信委等 8 家省直相关部门共同主办的 2017 年“湖湘杯”网络安全技能大赛将于 11 月 12 日开始第一轮初赛环节，360 企业安全为大赛提供技术保障。

360 企业安全将为初赛竞赛平台提供技术支持，并全程参与初赛、复赛、决赛的试题设计，参与比赛规则设计、试题评审，监督比赛结果等。

4.2 太极股份与 360 企业安全集团签署战略合作协议

360 企业安全集团与太极计算机股份有限公司达成战略伙伴关系，360 创始人、360 企业安全集团董事长齐向东与太极计算机股份有限公司总裁刘淮松代表双方签署战略合作协议。齐向东表示，通过加强与太极的战略合作，将有助于 360 产品服务覆盖更加广阔的行业用户领域，助推中国企业和客户的转型和快速成长。360 企业安全集团将积极推动与太极的进一步合作，争取在更大范围取得合作效果。

5. 安恒

5.1 安恒信息参与阿里“数据安全合作伙伴计划”

安恒信息成为首批参与阿里“数据安全合作伙伴计划”公司之一。阿里宣布将基于数据安全能力成熟度模型（Data Security Maturity Model， 简称 DSMM）推出“数据安全合作伙伴计划”，希望通过与合作伙伴的协同，共享阿里在数据安全方面的经验与能力，帮助各企业、行业建立和提升体系化的数据安全能力，以实现全行业生态的可持续发展。

5.2 安恒信息协助举办山东省第三届安全职业技能大赛

10 月 14 日至 17 日，由山东省人力资源和社会保障厅、共青团山东省委指导，山东省信息网络安全协会主办，山东国维信息安全培训中心承办，杭州安恒信息技术有限公司协办的山东省第三届“安恒杯”技能兴鲁职业技能大赛（网络安全）团体赛，在济南举行。大赛由杭州安恒信息技术有限公司提供信息安全竞赛平台和技术支持。安恒为本次比赛搭建了的攻防竞赛平台。

5.3 安恒信息亮相 2017 年云栖大会

在阿里 2017 年云栖大会上，安恒信息和众安保险联合首次推出了信息安全综合保险的互动体检活动。该活动是将线上网站体检与线下打印报告的智能融合，来访嘉宾可在现场体验“网站安全免费体检”大屏互动。

其次，安恒信息在本次云栖大会上，由高级产品经理郑赳带来《纵深解读：等保 2.0 时代，云安全的思考与实践》的主题演讲，内容涉及安恒信息基于多年的安全攻防经验完全自主研发推出的云安全产品——天池云安全运营管理平台。该平台提供了云监测、云防御、云审计、云服务，构建了统一管理、弹性扩容、按需分配的云安全资源池，提供整体的云安全综合解决方案。

6. 安天

暂无信息。

7. Fortinet

7.1 Fortinet 最新的沙盒解决方案获 NSS 实验室推荐

Fortinet 宣布了 NSS 实验室（NSS Labs 是独立安全研究和评测机构，总部设在美国）入侵检测系统(BDS)组最新的测试结果，其中 Fortinet 新的沙盒解决方案 FortiSandbox 2000E 赢得了 NSS 实验室的“推荐”评级。

FortiSandbox 2000E 针对中型企业和服务提供商的 APT 攻击，提供了灵活的部署选项，包括网络边缘、数据中心核心，甚至内部网络。FortiSandbox 2000E 是整体安全解决方案的一部分，其提供的沙箱功能能够结合威胁情报并与多安全产品互动，包括下一代防火墙(NGFW)，入侵预防系统(IPS)、安全邮件网关，web 应用程序防火墙(WAF)和终端安全解决方案。

7.2 Fortinet 在工业物联网中扩展安全防护和安全可视化架构

以 IoT 为目标的攻击已经揭示出，数以十亿计的 IoT 设备可能被用于非法攻击，以破坏全球数字经济、关键基础设施和数百万用户的数据。为此，Fortinet 提出了自己的 IoT 安全架构——FortiGuard Industrial Security Service (ISS)使得企业拥有全面的安全解决方案。ISS 是建立在威胁情报的基础上，通过提供应用控制和签名防御，实现安全防护，其适用范围包括各关键基础设施和工业部门，如公用事业，石油和天然气，运输和制造。另外，ISS 架构

也集成了 Fortinet 广泛的安全产品和解决方案，覆盖整个物联网攻击的链条，提供机器学习、隔离和安全保护功能，期望抵御针对物联网的各种攻击，其包含的产品包括 FortiOS，FortiGate， FortiSIEM， Secure Access， FortiGuard Threat Intelligence， Advanced Threat Protection 等。

7.3 Fortinet 在 Oracle 云市场中推出其 FortiGate 虚拟机

Fortinet 作为 Oracle Partner Network(OPN)的黄金级成员，宣布其的 FortiGate 虚拟机(VM)现在可以在 Oracle 云平台上使用。

FortiGate 虚拟机(VM)防御系统可以通过 BYOL 向 Oracle Cloud 客户提供，使企业可以安全地将工作负载和应用程序转移到公共云上，并通过站点到站点的连接实现安全策略的一致性。另外，FortiGate 虚拟机(VM)能够协助客户是细粒度的控制、满足安全需求以及本地基础设施的可见性。

8. Checkpoint

暂无信息。

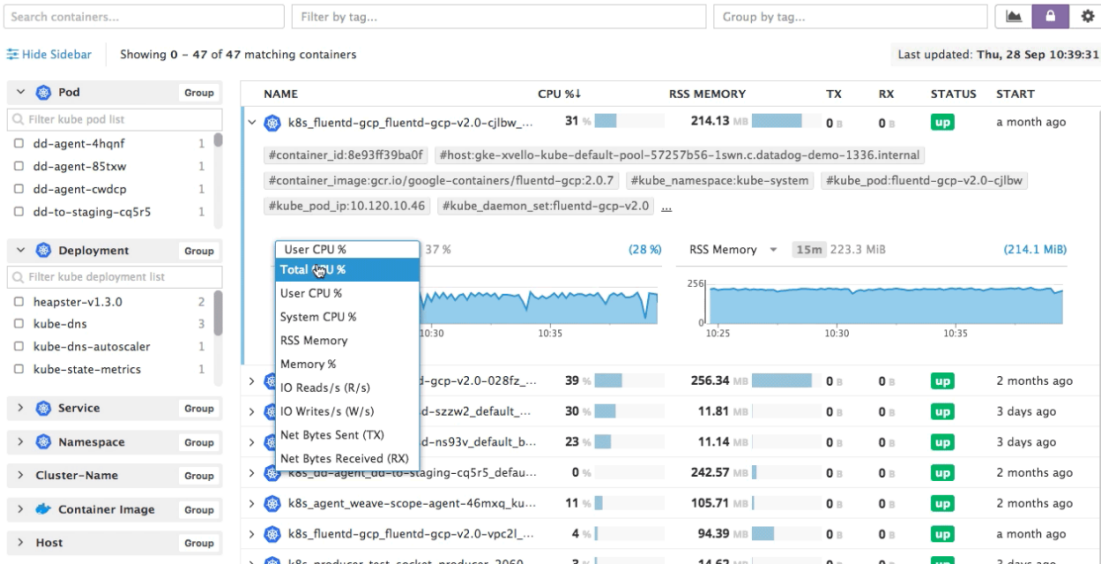
四、 容器技术及安全动态

1. CNCF 新增项目 Notary 和 The Update Framework

近日 CNCF 在项目的花名册上增加了两个开源安全项目：Notary 容器信任项目和 The Update Framework 更新安全框架，提供了密码验证的软件完整性。Notary 用于解决互联网内容发布的安全性。该项目不局限于容器应用，但在容器场景下可对镜像源认证、镜像完整性等安全需求提供很好的支持。

2. Datadog 正式推出实时容器监控功能

提供基础架构监控服务的 Datadog，近日正式推出实时容器监控功能，让企业可以实时监控基础架构中容器运作的状况，像是 CPU 使用率、I/O 等数据。其监控范围涵盖整个基础架构中的容器，以 2 秒钟为单位持续地更新讯息，像是容器的健康状况、资源使用率、部署状况等。目前此功能已经支持 Docker、Kubernetes 及 AWS ECS 容器服务等技术。



3. CRI-O 1.0 版本发布

CRI-O 项目旨在同时支持基于 Kubernetes 容器运行时接口（CRI）和 Open Container Initiative（OCI）标准的容器。其另一个目标是能够提供一个比其它的容器运行时更轻的环境，占用更小的内容空间，以及相比其他容器运行时环境对 Kubernetes 提供更好的性能表现。CRI-O 以 daemon 方式运行，更像另一个形式的 Containerd。

4. Docker 宣布同时支持 Swarm 和 Kubernetes

DockerCon2017 Euro 10 月 16-19 日在哥本哈根举行，Docker 宣布同时支持 Swarm 和 Kubernetes，一个 Docker Compose 模板可以同时部署于 Swarm 中和 Kubernetes 中，并且 Docker EE(Enterprise Edition)也全兼容 Swarm 和 Kubernetes。2018 年 Q1 将正式可用，目前想试用 beta 版的可访问 www.docker.com/kubernetes 尝试。

五、 安全新产品及技术

1. 研究人员研制出新的双因素认证

来自佛罗里达里达州国际大学和 Bloomberg 的科学家研制出一种定制化的双因素认证系统 Pixie，需拍摄用户私人物品进行验证。与传统的硬件安全密钥（例如，YubiKey 设备）加密或输入验证码（通过 SMS 或语音呼叫接收）验证相比，这种新的拍照验证方式省了一些麻烦。 如果用户选择用 Pixie 认证，则初次登录时，需要拍下身边物品的一张初始照片。以后每次登录都需要拍下照片，并由手机内安装的 APP 对比两张照片，进行验证。由于只有用户自己知道验证的物品到底是什么，所以黑客很难通过截取 SMS 短信或利用 SS7 协议的漏洞来劫持这个验证过程，因此研究人员认为，Pixie 比以前的验证系统更加安全。 据了解，Pixie 的错误验证率仅为 0.09%。目前研究人员仍在对这个系统进行研发改进，不过用户已经可以在 GitHub 中下载并试用。

2. 全新概率生成模型方法能在文字识别上超越神经网络方法

AI 在图像识别和文本处理上的才能正在日新月异地变化着。Science 杂志上有一篇论文显示 AI 已经可以破解 CAPTCHA 验证码所提出的挑战了。正如大家所知道的这样 CAPTCHU 在很多站点是用来检验人类与机器的一种验证机制。研究者是来自一家加州的初创 AI 企业 Vicarious，他们运用的是一种全新的概率生成模型方法（该论文表示，在场景文字识别任务

上这种方法已经超过了深度神经网络，甚至可能帮助人类），可以较高的准确度将扭曲的随机文本转换成精确输入。

3. NetBSD, OpenBSD 加强内核安全机制

NetBSD 最近发布了它们针对 64 位 AMD 处理器的的内核 ASLR 机制。KASLR 中国年会针对 NetBSD 内核随机分配内存。这样攻击者就无法简单地猜测并获取进入内存的权限，在漏洞利用上会比以前更难。 开发者 Maxime Villard 表示，目前的机制会在 bootloader 与 kernel 之间增加一个特别层“prekern”。而 OpenBSD 在早些时候也已经具备了相似的 KARL 机制。

4. 美国出台新的 SIDR 标准，可有效应对 BGP 劫持

日前，美国美国国家标准与技术研究所下属的国家网络空间安全卓越中心以及国土安全部的科学与科技政策局联合制定了一套新的标准，以保护主要互联网实体（如互联网服务提供商、托管提供商、云提供商、教育网络、研究网络和国家网络等）之间的信息路由传输过程。这套标准实际上是安全域间路由（SIDR）的标准集合。SIDR 是第一个旨在提高边界网关协议（Border Gateway Protocol）安全性的标准。边界网关协议是一种用于在大型互联网之间路由信息的互联网协议，开发于 20 世纪 80 年代后期，当时互联网环境没有现在这么复杂，因此没有考虑到安全问题。此次两个部门联合发布的标准主要应对 BGP 劫持问题，且符合 IETF 门户标准。

这套防御措施将使用加密方法来确保路由数据沿着网络之间的授权路径传播。IETF SIDR 主要由三个基本组成部分：资源公钥基础设施（RPKI），让互联网地址块（通常是公司或云服务提供商）的持有者有能力规定可直接连接到其地址块的网络；BGP Origin 验证，允许路由器使用 RPKI 信息来过滤掉未经授权的 BGP 路由通告，阻止恶意来源劫持 BGP；BGP 路径验证（也称为“BGPsec”），是 IETF 刚刚发布的标准草案（RFC 8205 至 8210）中的规定。其创新之处在于使用每个路由器的数字签名来确保整个互联网上的路径只能在授权网络中传输。

六、 网络安全投融资、收购事件

1. IPO

1.1 ForeScout Technologies IPO 上市

10 月 26 日，网络安全初创公司 ForeScout Technologies Inc 在纳斯达克交易所正是上市，股票代码“FSCT”，IPO 筹得款项$116,000,000，此前该公司在风险投资中融得超过 1.20 亿美元的资金。ForeScout 是一家专业从事网络准入控制的美国安全厂商，拥有 300 多人的专业团队。其网络准入控制产品 CounterACT 采用最新的无客户端访问控制技术，以快速高效的方式无缝集成到任何网络环境，已经为全球 500 多大型企业和政府机构提供全面的网络接入保障。

2. 投融资

2.1 Skybox Security 获 1.5 亿私有股本资金

10 月 25 日，IT 安全风险分析服务提供商 Skybox Security 从 CVC Capital Partners （私募投资公司）和 Pantheon（磐石基金） 以私人股本的形式筹得$150,000,000。Skybox Security（美国）是一个 IT 行业安全风险分析服务提供商，使用从建模和仿真中提取的数据，其为用户提供了如何最有效地解决威胁风险的决策，从而将运营效率提高了 90％。

2.2 KnowBe4,LLC 获 3000 万美元 B 轮融资

10 月 24 日，KnowBe4,LLC 从 Goldman Sachs 和 Elephant 筹得$30,000,000 的 B 轮融资。KNOWBE4（美国）是一个安全意识培训与模拟网络钓鱼平台，帮助企业员工加强网络安全意识，避免网络钓鱼的攻击。

2.3 CrowdStrike 获 2500 万美元 D 轮融资

10 月 19 日，CrowdStrike 筹集$25,000,000 的 D 轮融资。CrowdStrike（美国）是一个网络安全服务提供商，由反病毒公司 McAffee 的前 CTO George Kurtz 及前副总裁 Dimitri Alperovitch 创建成立于 2011 年，总部位于加州 Irvine。其 Falcon 平台是一个基于大数据分析的端点主动防御平台，可监控企业的数据，侦测零日威胁，并防止定向攻击造成的破坏。平台还可以识别未知恶意软件，学习攻击者特征，然后形成一套响应措施，提高对方攻击的

风险和代价。这些先进的识别机制与传统靠特征库为基础进行恶意软件侦测的手段有很大的不同，为越来越多先进安全公司所采用。

2.4 Duo Security 获 7000 万美元 D 轮融资，估值超过 10 亿

10 月 18 日，Duo Security 从 Lead Edge Capital 和其他 6 位投资者处总共筹得$70,000,000 的 D 轮融资。Duo Security（美国）是一家企业级移动认证安全服务商，推出了自主登记用户双重安全认证服务，支持 iOS、安卓和黑莓等主流移动操作系统，而且不需要任何硬件认证就能生成安全密码。在用户端，用户下载移动应用之后可以和平时一样输入用户名和密码，一旦首次身份认证成功，他们就会提供第二种认证方式，并且无缝同步到服务器和企业内部网络中，这种解决方案不仅安全性能得到保障，还加速了身份认证速度。

2.5 SecurityScorecard Inc.获 2750 万美元 C 轮融资

10 月 12 日，SecurityScorecard Inc.（美国）从 Nokia Growth Partners (NGP) 和其他 8 位投资者筹集总共$27,500,000 的 C 轮融资。SecurityScorecard 是一家网络安全风险监控技术公司，公司主要面向企业客户，为各种组织提供安全基准测试和评估服务。

2.6 Attivo Networks 获 2100 万美元 C 轮融资

10 月 11 日，2.6 Attivo Networks 从 facebook customer service phone number 和其他 2 位投资者总共筹得 $21,000,000 的 C 轮融资。Attivo Networks（美国） 是一家网络安全公司，其采用诱骗技术来检测、调查和帮助缓解已存在网络中的攻击，帮助用户网络、数据中心、云端、SCADA、物联网和销售终端组织恶性攻击，消除网络隐患。

2.7 Contrast Security 获 3000 万美元 C 轮融资

10 月 19 日，Contrast Security 从 General Catalyst 和其他 2 位投资者筹集总共$30,000,000 的 C 轮融资。Contrast Security（美国）是一家信息安全技术公司，目的是开发一种更快、更透明的自动化应用安全平台，帮助企业提升应用安全水平。