cloud security alliance®

云安全现状年度报告

2018

云安全联盟全球企业顾问委员会

序言

随着企业级客户对云安全的需求增加，云服务提供商对云上业务、数据的安全所肩负的责任担子也越来越重。云安全具有广泛的市场空间，但要实现快速发展，还需解决国内外云安全技术创新，标准统一，合规认证，及能力提升等问题，规范市场秩序。目前，国内外云安全相关标准众多，很多国家感到无所适从，不同的企业执行不同的标准，导致市场对安全质量的度量较为混乱，也影响了云计算的应用推广。未来，随着云计算全球化的推进，全球云安全标准将逐渐趋于统一，助力云计算行业快速发展，例如美国政府已与云安全联盟合作将美国联邦云安全标准 FedRAMP 与 CSA CCM 融成一体的 STAR RAMP，德国政府和其它国家也开始效仿。

云安全联盟发布云安全现状报告 2018，给出云安全现状的专业意见，在威胁态势不断演变的背景下，企业和云服务提供商可以为云安全提供的服务。中国云安全与新兴技术安全创新联盟（简称：中国云安全联盟）组织专家进行翻译为中文版本，相信一定会有助云安全在中国的增强。

中国云安全联盟和云安全联盟大中华区非常感谢参与此项目的翻译和支持工作者们。

中国云安全与新兴技术安全创新联盟常务副理事长
CSA 云安全联盟大中华区主席
李雨航 Yale Li

前言

云安全联盟全球企业顾问委员会成立于2016年，是由十多位行业的大型跨国公司的顶尖专家组成的代表团队。该委员会的成立是为了表达大型IT终端用户的观点，并融合云计算使用者信息安全相关的观点。

全球企业顾问委员会的目标是在云技术方面增加企业间的协作，使企业能够采用安全的实践和技术。这些工作旨在促进云服务提供商满足用户对于安全性与隐私的需求，并帮助监管机构不断加强和改进法规来跟上不断变化的云计算新技术和新特性。该委员会发布的报告旨在通过系列的活动，提高对云计算安全的认识以及企业与云服务提供商相互协作重要性的认识。

IT系统的质量和自身的安全能力取决于成熟的大型企业使用者的需求以及他们对行业发展的期待。我们希望您从这份报告中重点了解到的是，云安全是一项需要不断进行的工作，云计算用户社区有责任相互协作和扩大声音，以确保他们的关键安全问题得到倾听和解决。

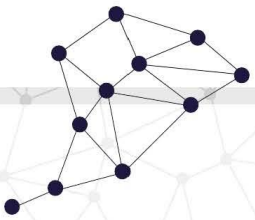
我们欢迎您对该报告的反馈，并鼓励您关注我们的活动，本文中我们概述了在企业、云服务提供商和监管机构之间加快安全地部署云应用的过程。

网址： https://cloudsecurityalliance.org/geab

邮箱： geab@cloudsecurityalliance.org

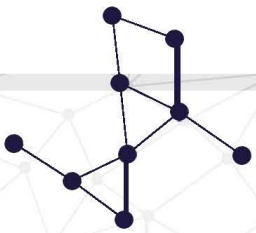
Twitter @csageab

Vinay Patel *Citi Infrastructure, Chair*
Niall Casey *Johnson & Johnson*
Pete Chronis *Turner*
Gurdeep Kaur *Horizon Blue*
Vjay LaRosa *ADP*
Michael Panico *Disney*
Marisa Ruffalo *Chevron*
Joe Zacharias *Caterpillar*



目录

前言
目录
简介
云与相关技术的运用
云服务提供商在安全方面做了什么？
企业在安全发面做了什么？
威胁态势正在演变
和监管者的合作
行业技能差距
摘要
关于云安全联盟（CSA）



简介

多年来，创新者和早期采用者一直在利用云计算技术的更快的部署过程、更好的扩展性和节省服务成本的优势。云计算的发展将继续加速更多的解决方案的产生，包括安全性和附加的特性。在信息数字化和创新的时代，企业用户必须跟上时代的步伐，才能满足基线能力和安全要求。

本文提供了一些最新的企业信息安全从业人员必须知晓的云实践和技术，因为IT和敏感数据的延伸已经超出传统的企业边界。供应商、监管机构和企业必须合作，才能建立跨服务的基准安全要求。了解云和相关技术的使用以及数据安全和所有权的作用和责任，将有助于提高这些服务的采购和长期管理。

云与相关技术的运用

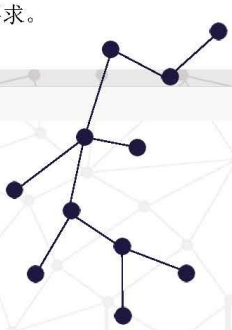
面对当今云服务的广度、范围和丰富性，企业往往不知所措。基础设施即服务(IaaS)领域由三大供应商主导，他们的服务常常与平台即服务(PaaS)产品重叠。新的能力进一步解耦硬件和软件能力。“无服务器”和“功能即服务”的产品允许用户构建他们的应用程序的时候完全依赖于供应商来管理和提供服务器计算资源的分配。此外，软件即服务(SaaS)市场在不断延伸，提供了新的产品来帮助解决数据、安全、网络和身份方面的问题。此外，云访问安全代理(CASB)、软件定义边界(SDP)和安全托管服务 (MSS)等服务在试图超越传统的企业边界进行管理时，造成新的操作复杂性。

由于过去两年IT安全预算有所增加[1]，而且项目在未来五年内持续增长，因此需要在企业用户中进行研究和分享这些服务，以便了解其功能以及如何安全地实施。 许多云服务包含平台原生安全控制，通过添加传统环境中不能满足的安全控制措施，消除传统安全服务中的冗余控制和重叠，帮助公司改进其安全状态。提前规划研究、测试、实施和培训用户使用这些原生安全控制是绝对必要的，以最大限度地提升安全收益。

云服务正在以许多创新的方式被运用。消费者和企业都在利用云在新兴技术方面的优势。 物联网（IoT）设备扩展了计算的边界，允许实地收集和分析数据。人工智能（AI）为数据提供更多的机器学习功能的分析和应用。区块链技术应用使信息和交易所有权透明且安全。应用程序容器和微服务引入了在工程实践中安全、敏捷开发和通信的架构。云已经打开了（以上这些及其它）相关技术的大门。探索实际案例和潜在案例对于跟上市场应用的步伐、建设安全的行业最佳实践非常重要。

为新兴技术建立小型项目可确保大家熟悉新技术，以及如何与现有IT基础架构和工具进行集成。与行业合作伙伴共享成功和挑战，可以让采用者在每个项目中构建功能和安全的模式，从而扩展到更大的工作负载以及整个行业。行业合作伙伴和提供商的合作将确保云供应链中的所有合作伙伴满足基准安全要求。

1. https://www.gartner.com/newsroom/id/3836563

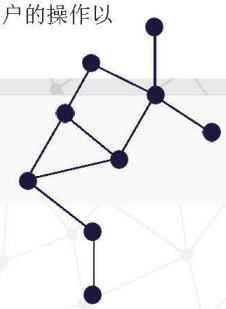


云服务提供商在安全方面做了什么？

随着用户对云提供商安全的信任，用户采用了越来越多的云服务。由于云提供商在云平台安全方面的投资，McAfee的一份调查显示，用户对公有云服务完全信任的比例在2017年增加了76%[2]。但是信任应该基于证据。云提供商正在通过自评估及第三方工具，比如CSA STAR项目[3]、 ISO 27000-series认证[4]、以及 FedRAMP认证项目[5]等方式证明云中的安全。这些平台针对云安全特有风险的安全控制与对策。通过审查通用安全控制集可以对云提供商的通用安全水准进行持续评估。

云提供商的安全水平还与他们快速检测、遏制、减轻攻击的能力相关。云提供商通过参与网络安全信息共享来重点提升威胁应对的能力。这些威胁情报交换机制使得从最小到最大的云提供商之间共享情报更为容易。从最小云提供商共享的威胁行为者情报，可以防止对于大云提供商的破坏。这些实践已经标准化并对包括企业在内的更大型团体开放。鉴于对手迅速协同实施攻击，信息安全团体需要迅速反应，协同在云提供商、企业及用户之间跨行业交换威胁情报。这可以帮助大家维护标准的安全解决方案。

随着威胁态势的演进，云服务提供商持续性的在其平台上添加新的特性功能来解决最新安全隐患。安全以及配置的功能以较快的速度引入平台，但需要最终用户进行良好的沟通。仅仅是培训视频和操作手册还不够，因为企业正在使用多个云服务而且在快速变化。为了帮助企业应对技术的扩展特性，我们的目标是实现更为安全稳定的默认配置，并确保正确运用新的特性。任何一次服务事故，即使是由于用户错误造成的，也会对客户信任度和产品可靠程度产生负面的影响。用户的操作以及行为是和功能本身一样重要需要关注的。



2. Building Trust in a Cloudy Sky: The state of cloud adoption and security https://www.mcafee.com/us/solutions/lp/cloud-security-report.html
3. https://cloudsecurityalliance.org/star
4. http://www.iso27001security.com/html/27017.html
5. https://www.fedramp.gov/

企业在安全方面做了什么？

云技术的采用以及将系统迁移上云对安全提出了不同的挑战。采用云服务仍然需要新的云服务提供商满足企业的合规要求。共享责任模型描述了云提供商/或企业安全控制的归属权。满足这些安全的要求有助于促进企业的合规情况。这种类型的共享安全模型正在鼓励企业将更多的关键业务系统，例如企业资源计划系统（ERP）转移到云上。

许多企业为了云的强大的能力而转向云，其中包括安全性。为了最大程度地利用云的安全能力，企业仍然需要对业务系统进行调整和改进。企业为内网工作流程维护的安全模式不能简单应用于云。迁移工作涉及了解如何为云服务体系正确的重构业务系统，这是利用云安全特性以及平台原生安全工具的关键。针对云的特性和本质，开发和部署的生命周期应当注重使用微服务、应用程序容器和不可变架构，并采用Dev(Sec)Ops方法。自动化的使用将增加我们构建项目的能力以及在开发过程中的安全能力。这些工具集中在云管理面板上，可以帮助企业通过保护API和云平台的原生安全性来限制被攻击的范围。尽管在云上构建新应用程序以及利用云原生工具更加简单，但是将原来内部业务系统迁移上云可能会更加复杂，需要将项目进行分解，并使用多个云服务来获得需要的安全性和可靠性。

威胁情报的共享不应只局限于云服务提供商之间。隐蔽式攻击也好，目标行为攻击也罢，企业内的(数据)传输均是这些攻击行为的目标。应当在企业和云服务提供商生态系统内共享这些常见的威胁行动和线索，便于发现攻击源和制定对应的风险缓解技术。其中，非常重要的是：针对共享的内容、如何共享以及与谁共享来共同努力并制定标准化的方法[6]，以便有效地关联并缓解威胁。在目标明确的情况下，进行共享事件、理解程序和部署策略的协作，信息共享将得到最佳效果。

6. GDPR的准备和意识调查报告 https://cloudsecurityalliance.org/download/gdpr-preparation-and-awareness-survey-report

企业需要了解和评估：所有同云服务的迁移，配置和采纳有关的风险因素。建议采用分阶段的方式迁移敏感数据和关键应用程序。在正确实施的情况下，云可以使数据规范化、可视化、规模化地自动添加到以往的手动过程中。针对企业所使用的云服务来开展适当的培训和教育，将有助于企业企业正确构建云端架构，并充分利用好那些云原生工具和安全性所带来的优势。在做好这一切时，云中的关键数据就会受到云服务提供商和企业安全控制措施的双重保护。

威胁态势正在演变

针对信息系统的攻击和破坏已然成为每日的头条。企业希望与时俱进能够防御新型威胁、风险和漏洞。诸如WannaCry之类的勒索软件在2017年影响了超过250,000台计算机系统。另外，Bad Rabbit、Petya和Not Petya在2017年也如同暴风般席卷了行业。以动态DNS为例的分布式拒绝服务（DDoS）攻击影响了超过70个主要在线服务。 在2016年，诸如Mirai 、botnet之类的有害软件正通过利用不正确的安全实践对信用卡网站发起多次的分布式拒绝服务（DDoS）攻击。错误配置的云服务用法，比如数据分析公司Alteryx[7]因亚马逊AWS S3存储配置错误，导致1.23亿美国人的信息泄露，而Verizon的事故则影响了600百万个人用户。[8]“熔断与幽灵”，这两个CPU处理器漏洞，正在影响几乎所有的现代处理器，使其泄露数据和密码。

企业需要对他们的员工进行基础安全实践方面的培训。防止“钓鱼攻击”和恰当的密码管理策略能够预防许多包括勒索软件和分布式拒绝服务攻击在内的有害攻击行为。针对安全补丁和CVE的快速响应和实施这一响应机制需要进行进一步的调优以防范以上这类有害软件。在补丁机制响应时间和（信息）协调披露方面，云服务提供商也需要对他们的客户保持透明。企业需要意识到并且知道这些最新型的威胁是如何来影响企业的业务，并且做好风险缓解计划并确保相应的技术落实到位。在行业内分享共享情报是一种方式，同时还可通过参考报告和最佳安全实践范例，诸如CSA的“十大威胁报告”，Verizon的数据泄露调查报告， 和OWASP的十大报告帮助企业构建预防、侦测与纠正缓解机制。

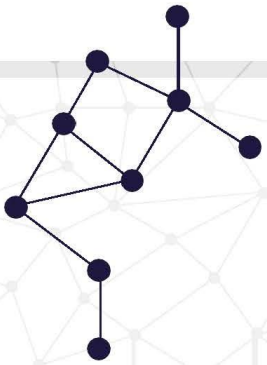
7. http://www.eweek.com/security/cloud-data-leak-exposes-information-on-123-million-americans
8. http://www.eweek.com/security/verizon-won-t-be-the-last-to-leave-data-exposed-in-the-cloud

与监管者的合作

企业在合规时重要的是履行强健的安全原则来实现合规，而不是使用合规来驱动安全要求。安全控制需要具有扩展性，才能灵活地包含新技术实践以及同时满足监管的安全要求。

客户对于隐私的保护意识也在不断提升。任何持有客户数据的组织必须考虑提高其隐私政策的等级，尤其是面对欧盟公民的数据时，需要根据新的《欧洲通用数据保护条例》（简称GDPR）。每个在供应链中负责控制或处理这些数据的合作伙伴必须遵守GDPR的隐私要求。隐私的体系结构、技术的解决方案以及实践均需要切实执行，确保供应链中的各方都满足预期。监管机构和执行这些新规则的人员需要提供清晰的解释和指导，以便负责隐私的人员能够正确应用规则和保护客户数据。

企业、监管者和云服务提供商三方在新技术和提供商能力的教育和培训方面应达成合作关系。法规可以随着云技术等安全技术的应用而发展，为所有人提供更好的安全和隐私保护。行业组织可以在向监管机构提供推动安全性并满足合规的要求的云解决方案和技术的教育时提供支持。



行业技能差距

据研究表明，至少存在100万个网络安全工作岗位的空缺。根据美国网络安全市场研究公司Cybersecurity Ventures发布的2017年度网络犯罪报告，这个缺口到2021年会扩大到三倍。造成这种差距的主要原因是缺乏合格的申请者。因为云技术引导的加速变化改变了周边的安全行业，所以信息安全从业人士在保持技能水平方面面临极大挑战。正确地使用新技术和现有解决方案可以很好地帮助今天的安全从业者。我们的安全教育生态体系需要极大扩张，这将给当今安全行业专业人员增加很多机会。

我们需要集中精力在信息安全领域培养更多合格的专业人员，同时提升现有的专业人士的技能，尤其是与云计算技术相关的技能。

9. http://www.cybersecurityventures.com/jobs

概要

科技发展的速度已远远超越了企业对于新技术的应用速度。为了保证竞争优势，如何安全地应用这些技术给企业带来了前所未有的挑战。随着云技术和其他新兴科技的发展，整个供应链生态环境的每个环节都需要通力合作，来保证大型企业和监管者能够切实理解如何安全地应用现有云服务提供商提供的新技术以及新特性。所有参与方都需要扮演好在保护客户数据安全和分享安全操作最佳实践中的角色。

在云提供商为企业提供服务和新技术的过程中，教育和意识仍待进一步提高。小规模的项目经验应当被共享，这样才能确保安全挑战和安全模型在更大的商业规模乃至整个行业中被更好应用。这一技术差距，特别是云计算和新兴科技，需要通过网络生态中各方的合作和协调方能弥补。

10. http://www.cybersecurityventures.com/jobs