云安全技能让您的职业发展前景无限(甚至更远)

云安全形势

云计算是无处不在的。企业正在迅速将工作负载从其内部数据中心迁移到云中，利用无服务器、容器和机器学习等新技术来获得云带来的好处：灵活的容量和可扩展性、改进的可用性和更高的灵活性。

随着对内容、应用程序和设备的不断访问——所有这些都相互无缝连接，没有中断——云计算已经成为我们日常生活中不可分割的一部分。泰雷兹公司最近的一份报告[1]表明，98%的全球组织在云中存储某种敏感数据。95%使用软件即服务（SaaS）应用程序，67%使用基础设施即服务（IaaS）平台，65%使用平台即服务（PaaS）环境。

尽管采用云计算后有许多优势，但组织也面临着新的挑战和担忧。其中，安全仍然是一个关键问题。[2]事实上，94%的网络安全专家确认他们至少对云安全有一定的担忧。

随着越来越多的网络攻击以云工作负载为目标，各组织需要对其云安全态势增加信心。所有行业和部门的组织都在雇用云安全认证的专业人员，以应对不断扩大的威胁环境所带来的挑战。但采用有效的云安全并非没有障碍。《2020年云安全报告》显示，组织面临的最大挑战与技术无关，而是与人和流程有关。调查显示，员工的专业知识和培训（55%）是最大的障碍，其次是预算挑战(46%)，数据隐私问题（37%），以及缺乏与企业内部平台的整合（36%）。

根据《2020年网络安全人力研究报告》尽管今年劳动力短缺的情况有所减少，但为填补网络安全人才缺口，该领域的就业人数在美国仍需增长约41%，全球需增长89%，而云计算安全是迄今为止最受欢迎的技能组合[3]。

重新思考云环境中的安全问题

云很便捷，但也可能会成为一个漏洞。云安全技能的差距意味着公司正在争相填补云安全职位。事实上，最近的调查显示，企业正在寻求培训和认证有兴趣过渡到网络安全的IT人员，以确保他们不断发展的安全需求得到满足。因此，40%的行业专业人士计划在未来两年内进行云安全培训。随着企业转向基于云的解决方案而非企业内部的传统解决方案，这一比率将继续增长[4]。

随着越来越多的组织采用云服务、平台和环境，专业人士需要重新思考安全问题。2020年，近三分之一的组织遇到了一个挑战，即如何找到能够管理融合基础设施的专家，将传统系统和云系统融合到一个连贯的网络环境中。安全专业人员必须确保对云安全采取全面和有效的方法。

为了成功地保护组织，从业人员必须重新考虑安全问题，将关键组件包含到云中：

- 数据
- 用户
- 应用
- 连接性
- 基础设施

云安全专业人员应管理和保护所有的云组件，以避免安全漏洞，保证用户和数据的安全。为了实现这一目标，从业人员需要：

- 保护任何用户在任何地方、任何设备上对网络内容和云应用程序的访问
- 在整个组织内拥有可见性和控制力，以推动云安全战略
- 在数据移入和移出云时保护其安全
- 为用户和网站实现直接到云的连接，无需回传
- 优化基础设施和工作流程
- 防范高级威胁，包括零日漏洞

从业人员经常落入的一个陷阱是使用传统的安全实践和工具来保护云工作负载。不幸的是，大多数传统安全工具不是为云的动态、分布式虚拟环境设计的。82%的2020年云安全调查[5]受访者表示，传统的安全解决方案要么在云环境中根本不起作用，要么功能有限。

缺乏足够的安全保护就会产生一些漏洞，被不良分子急于利用。根据《2020年云安全报告》，最大的安全威胁是云平台的错误配置（68%）、未经授权的访问（58%）、不安全的接口（52%）和账户被劫持（50%）。泰雷兹《2020年数据威胁报告》[6]指出，49%的全球受访者遭遇过影响云数据的入侵。

企业越来越多地投资于雇用或培训安全专业人员来解决这些漏洞。在对云安全专业人员的需求如此之大的情况下，展示对云安全原则和实践的正确理解，打开了各种各样的前景，并预示着光明的未来。

云安全技能

保护一个组织在云中的资产不受配置错误和外部威胁的影响并不是一件容易的事。网络安全专业人员必须知道如何计划和实施安全战略，以减少风险和加强保护；了解与信息安全、隐私和数字权利相关的法律和道德问题；并具备云计算和安全最佳实践的核心知识。

扎实的技术技能基础和对云中威胁的背景理解尤为必要，因为网络安全专业人员今天遇到的攻击是对手利用昨日设计不良的系统和漏洞进行攻击的结果。拥有强大基础的人将能够理解云中新兴攻击的潜力，并指导安全团队采取缓解措施。如果没有这些云安全方面的基础知识，从业者也许能够在日常工作中生存，但无法保证他们能够应对安全事件。

因为网络安全是一个如此受欢迎的领域，选择这一职业道路的专业人士有着光明的未来。根据劳工统计局的数据[7]，网络安全行业在2029年之前预计将增长31%，而所有行业的增长率为4%。此外，根据一些估计[8]，到2021年，全球网络安全工作队伍将有超过350万个空缺职位。

随着企业持续重视安全，以及对手继续挑战云系统中数据的完整性和保密性以及为保护它们而采取的安全措施，网络安全行业将持续需要熟练的专业人士。对云安全的扎实理解对任何个人来说都是一笔巨大的财富，因为他们可以从同龄人中脱颖而出，获得更多的职业机会。

共同责任模式

对云安全的技能和基础知识的需求是基于这样一个事实，即云安全功能是云供应商和使用它们的组织之间的共同责任。无论您是使用IaaS、PaaS、SaaS还是混合平台，主要的云供应商，如AWS[9]、Azure[10]和Google Cloud[11]，都规定云安全要遵循共同责任模式：

» 云供应商对云**的**安全负责。

» 云客户对云**中的**安全负责。

云供应商有责任保护运行其提供的服务的基础设施。这种基础设施包括运行云服务的硬件、软件、网络和设施。另一方面，云客户对他们存储在云平台上的数据、他们的应用程序和操作系统、更新和安全补丁，以及网络和防火墙配置承担全部责任。此外，客户还负责实施身份和访问管理控制，以验证和授权对数据的访问，并负责对静止和传输中的数据进行加密。

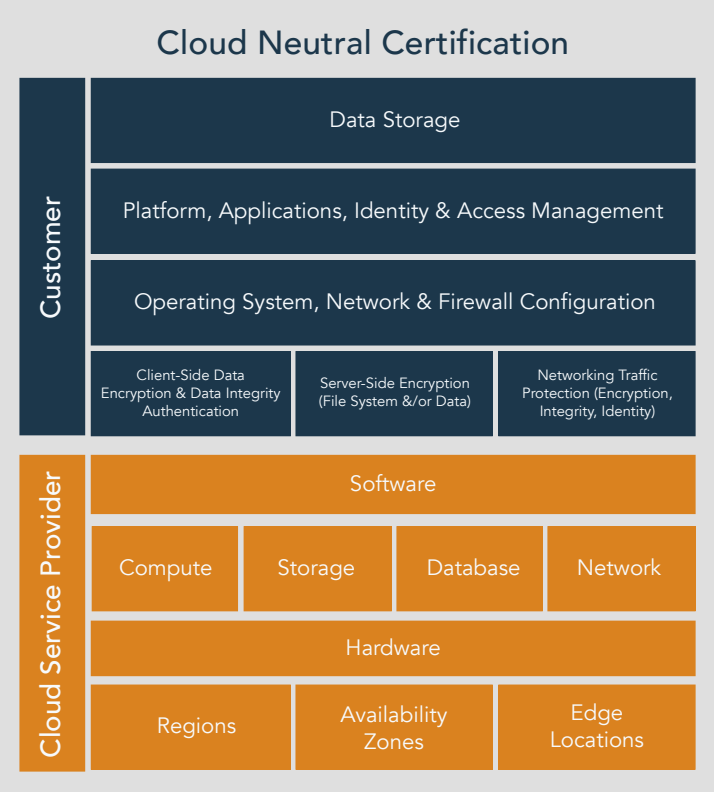

图1:共同责任模式。

共同责任模式是云安全的基础。云安全专业人员需要对他们的角色和责任有一个扎实的了解。错误理解他们在云中的职责级别可能会导致错误配置和糟糕的安全控制。

技术技能

安全专业人士需要具备正确的技术和软技能组合，才能在云安全领域蓬勃发展。虽然技术技能组合证明了您具备应用最佳实践来保护云环境的基础知识，但软技能使云安全专业人员能够成为真正的领导者，无论他们在组织的层级结构中处于何种位置。

技术技能涵盖了广泛的知识范围。首先，云安全专家应该了解云计算的构件，比如定义、角色和技术。同时，他们还具备云环境相关安全和设计原则的基础知识，如加密、访问控制、虚拟化 安全和供应商锁定。

此外，他们需要具备实施与云平台相关的数据发现和分类技术的知识，并为云中的个人和敏感数据设计和应用数据保护，以满足法规遵从性要求，如GDPR、HIPAA和CCPA。云安全专业人员必须识别和分类关键信息，并计划和执行以数据为中心的措施，以消除或减少对手利用的可能性。

除了保护云中的数据，安全专业人员还需要了解云基础设施组件（物理和虚拟）的风险和威胁，以及减轻这些威胁的控制措施。

除了保护云中的数据，安全专业人员还需要了解云基础设施组件（物理和虚拟）的风险和威胁，以及减轻这些威胁的控制措施。

最后，云安全专业人员应该了解各种道德和法律约束以及技术，以便能够确定犯罪行为并保护云中数据的完整性和机密性。

这些特定于云的技术技能可以帮助云安全专业人员在任何行业垂直或监管框架中满足业务和安全需求。

软技能

除了技术技能，软技能对于希望在云安全领域出类拔萃的专业人士也很重要。解决复杂问题的能力至关重要，有助于正确分析问题，与同事清楚地沟通技术问题，并快速得出结论。做出有效的业务和安全决策也是现代商业环境中所有专业人员的核心价值。

安全专业人员需要战略思维来领导业务运营、观察趋势、平衡长期和短期目标，并确定优先级。此外，他们还需要能够有效沟通，倡导云安全原则和最佳实践。由于有大量可用的解决方案和技术，能够选择和实施适合目的的技术并获得其所有好处也同样重要。

在不断变化的全球和商业环境中，专业人员必须灵活地适应变化，他们需要对环境有一个整体的看法，从技术细节中抽象出来，并将运营业务目标视为一个实体。

云安全知识提升您的职业发展

为了获得作为云安全专业人员打下坚实基础所需的特定技能，行业培训和认证创造了一条行之有效的成功之路。云安全培训特别关注配置平台和避免代价高昂的错误所需的操作知识。认证拓宽了知识面，为您提供了有关云计算和安全的大局。

云安全认证将帮助您理解法律合规性、角色和责任等概念，以及安全目标与组织目标的一致性。通过认证过程获得的知识，加上您的背景和经验，可以将您的职业生涯提升到新的高度。

在任何阶段对您的职业生涯都有好处

通过云安全认证获得的知识和技能在职业生涯的任何阶段都很重要。无论您是处于早期开发阶段、从IT转型、改变职业道路还是担任高级管理人员，都有很多关于这种快速发展的技术的知识需要学习。

云安全是业务运营中不可或缺的一部分，在获取云安全认证的过程中获得的结构化和纪律性知识只会增强您在组织中思想领袖中的前景。

确立职业道路

随着您职业生涯的发展，云安全认证将帮助您成为团队和经理的宝贵财富。正确的认证使您能够将有效的云安全策略转化为成熟、可靠的实践和解决方案，以保护组织的数据免受网络犯罪分子的窥探。

打造云安全专家的职业生涯

另一方面，如果您已经致力于成为一名杰出和熟练的IT或安全从业者，云安全认证将为您提供独特的云相关知识和技能，专业人士越来越需要具备这些知识和技能。这些严谨的知识将帮助您将业务目标与安全解决方案结合起来，并成为提高生产力和成功的推动者。

实现对云的掌控

作为一名安全专家，从云安全认证中获得的基础知识可以帮助您制定策略，推动您的组织向创新和成功迈进。了解安全的云计算如何推动企业增加业务收入，将有助于您做出正确的决策，让您成为公司现在和未来的领导者。

随着云安全职位空缺率创下历史新高并不断增长，获得云安全认证的时机前所未有地优越。获取云安全认证带来了无数好处，现在的挑战是选择一个能够满足您所有需求的认证。

获取CCSP，掌控云主动权

ISC2 注册云安全专家(CCSP)认证可以将您的职业生涯带向云端并不断超越。CCSP是云安全认证的基准，并多次被公认为是最有价值和最全面的云安全认证[12]。

获取CCSP认证有利于从业者，并使他们在竞争日益激烈的环境中获得竞争优势。CCSP具有权威性，是确保云安全全面融入每一个云解决方案所必需的指挥领导力的典范，它利用了庞大的知识库和严谨的技能组合。

一个厂商中立的认证

CCSP是一个与厂商无关的认证，确保认证从业者具备安全知识，从而成功保护任何云环境。

随着越来越多的组织选择厂商中立的云安全解决方案以避免供应商锁定，CCSP认证的中立性对于寻求在各种平台上应用有效控制、策略和配置最佳实践的云安全从业者来说是一项巨大的奖励。厂商中立认证的最大优势在于，它为从业者提供了一个平衡的方法和云计算安全各方面的知识基础，包括这些技术的优势和局限。供应商的认证只为其自己的平台提供培训，这限制了所获知识的范围和适用性。

即使已经拥有一个特定的供应商的认证，您仍然可以获取CCSP认证，构建有效的云安全所需的端到端基础知识。CCSP可以扩展您的技能，并允许您将您的安全专业知识应用于多个云计算环境，展示在云架构、设计、运营、数据安全、风险和合规方面的能力。通过获得CCSP认证而获得的厂商中立的知识，可以确保您有能力在任何云环境中保护敏感数据。

一个市场差异化标准

CCSP独特的标准将其提升到了一个标准，使其成为首屈一指的云安全认证。众多原因被认为是其独特之处，使其与其他认证相比具有不可逾越的优势，它也为其认证持有人提供了好处，使其在日益激烈的竞争中获得竞争优势。

能胜任岗位的知识。CCSP被定位为云安全方面的专家，证明其精通新的技术、发展和威胁。

坚实的基础。CCSP认证提供了建立云安全最佳实践、不断发展的技术和缓解策略所需的高级知识和技能。

职业发展机会。CCSP认证提供了多种就业机会，因为现在几乎所有组织都在一定程度上在云中运营，而强大的云安全态势是允许它们创新并获得竞争优势的关键因素。

行业认可。云安全从业人员通过CPE活动的持续专业发展，不断扩展他们在云服务及其安全方面的知识，获得那些寻求安全地转移到云和创新的组织的认可。

更高的薪酬。CCSP认证可以帮助增加您的收入。拥有CCSP认证的专业人员在认证薪资调查榜上排名第5位[13]。

专业信誉。CCSP认证通过展示对网络安全职业的承诺和奉献精神，有助于提高职业信誉。经过认证的专业人员传达知识并激发信任，提高他们未来进入领导岗位的的市场竞争力。

同行人脉。获得CCSP认证可以增强与其他经过认证且技术娴熟的云安全专业人士的交流机会，他们可以在需要时成为宝贵的知识和信息库。

将新知识与商业目标相融合。通过CCSP考试获得的知识有助于专业人士了解云部署的所有领域，以及云服务和安全如何与业务目标、风险容忍度和监管合规性相关。云技术和安全与企业战略目标的一致性是一个市场差异化因素，也是认证投资的巨大回报。

了解云环境的证明。CCSP认证是了解云平台背后技术的证明，可以帮助您在预算、人员配置、组织结构和外包方面做出更好的决策。

提高工作绩效。了解新兴的云技术和安全原则可以通过利用云环境为增强协作提供的所有好处，帮助您提高工作绩效。

指导新生代。获得终身职位的专业人员可以根据安全协作和集成方面的知识及经验指导下一代IT安全专业人员。传承智慧有助于创造一种安全文化，培养强大的云安全态势。

获得CCSP证明您处于云安全的最前沿。我们询问了获得CCSP认证的网络安全专业人士，他们如何从获得这一认证中受益，他们说：

"完成CCSP的最大好处之一是得到雇主的行业认可。随着更多的组织正在进行现代化和云迁移工作，为确保这些环境的安全，它们对网络专业人员的需求很强烈。CCSP让我了解了围绕各种云部署和服务模型的安全问题，这使我能够创建一个路线图，以克服安全控制实施过程中的常见挑战。迁移到云环境或消费云服务的组织必须意识到潜在的安全风险。作为一名CCSP，我有信心成为云部署安全方面的安全倡导者和值得信赖的顾问。"
—Hunter Sekara, CISSP-ISSAP, ISSEP, ISSMP, SSCP, CCSP, CAP, CSSLP

"获得CCSP有助于提高我的专业信誉。它有助于证明我对该行业的承诺和奉献，并为我的职业生涯带来重要价值，包括晋升机会。"
—Babatunde Falode, CISSP, CCSP

"它使我能够赶上新一代的年轻IT专业人士，他们还没有从大型机到云的经历。"
—Paul Oor, CISSP, CCSP

CCSP如何脱颖而出

该认证在其他云安全认证中脱颖而出，有许多出色的原因。认证杂志称CCSP是 "迄今为止云保护领域最全面的认证[14]"，并将其列为他们调查对象计划获得的首个认证。CCSP是唯一要求有云经验的云安全认证。候选人必须有至少5年的IT工作经验，其中3年必须是信息安全方面的经验，1年是云安全方面的经验。CCSP知识的通用性和中立性使其成为国际公认的云计算标准的可靠标准，如ISO/IEC 17024、17788、17789、27017和27018。

通过持续的专业教育和发展计划，获得CCSP认证的专业人员能够及时了解新出现的威胁、技术、法规、标准和实践，确保他们在全球环境中保护敏感数据的能力。

CCSP为您的职业生涯提供竞争优势

在您职业生涯的任何阶段，CCSP都是您在云安全领域出类拔萃的重要合作伙伴。掌握了云安全技能，您将能够更好地管理云计算的能力，同时保证关键资产的安全。有了CCSP，天空才是您的极限。

CCSP表明您拥有先进的技术技能和知识，能够使用ISC2 制定的最佳实践、政策和程序来设计、管理和保护云中的数据、应用程序和基础设施。

通过CCSP认证获得的结构化知识是您职业生涯成功的必经之路，也是您的组织在不断变化的全球环境中获得竞争优势的必经之路。CCSP认证可以让您的职业发展无极限并且更超越。

要了解更多关于CCSP认证如何帮助您获得专业知识并推动您的职业生涯，请访问
www.isc2china.org/ccsp
并下载我们的电子书 《安全云迁移的20个技巧》。

关于ISC2

ISC2是一个国际非营利性会员组织，专注于启迪构建一个安全可靠的网络世界。因其广受赞誉的注册信息系统安全专家（CISSP®）认证而最为人熟知，ISC2提供了一套认证组合，作为整体的、程序化的安全方法的一部分。我们的候选人、准会员和会员人数超过50万，由经过认证的网络、信息、软件和基础设施安全专业人士组成，他们正在发挥作用并帮助推动行业发展。我们以慈善基金--网络安全和教育中心™对教育和普及大众的承诺而践行我们的愿景。有关ISC2 的更多信息，请访问我们的 网站 在微信和微博
上关注我们。

参考文献

1 Thales Data Threat 2020 Report, Global Edition, available at https://cpl.thalesgroup.com/data-threat-report

2 Cybersecurity Insiders 2020 Cloud Security Report, available at https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

3 ISC2 2020 Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study

4 ISC2 2020 Cybersecurity Workforce Study https://www.isc2.org/Research/Workforce-Study

5 Cybersecurity Insiders 2020 Cloud Security Report, available at https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

6 Thales Data Threat 2020 Report, Global Edition, available at https://cpl.thalesgroup.com/data-threat-report

7 Bureau of Labor Statistics, Occupational Outlook Handbook, Information Security Analysts, available at https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

8 Cybercrime Magazine, Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021, available at https://cybersecurityventures.com/jobs/

9 Amazon Web Services, Shared Responsibility Model, available at https://aws.amazon.com/compliance/shared-responsibility-model/

10 Microsoft, Shared responsibility in the cloud, available at https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

11 Google Cloud Platform: Shared Responsibility Matrix, available at https://services.google.com/fh/files/misc/gcp_pci_srm__apr_2019.pdf

12 Cybersecurity Insiders 2020 Cloud Security Report, available at https://www.cybersecurity-insiders.com/portfolio/2020-cloud-secuity-report-isc2/

13 Certification Magazine, Salary Survey 2019: Certification leads to improved performance, increased earning power, available at http://certmag.com/salary-survey-2019-certification-leads-improved-performance-increased-earning-power/

14 Certification Magazine, Salary Survey 2019: Certification leads to improved performance, increased earning power, available at http://certmag.com/salary-survey-2019-certification-leads-improved-performance-increased-earning-power/