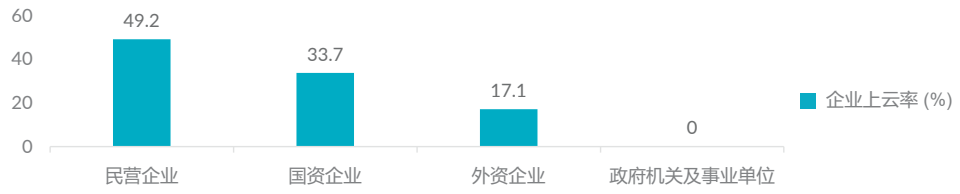
云计算安全挑战及应对之道

敏于知

云计算及安全职责细分

与传统的实体机房部署基础设施不同，云计算是指通过互联网提供集中化的服务和基础设施。云服务器使用虚拟技术在异地托管公司的应用程序。通过这样的方式，数据可以定期备份，无需一次性的营建成本和长期的运维成本支出，公司只需为其消耗的资源付费。

根据《2021 年中国企业上云指数洞察》研究表明，近年来中国云端服务市场快速增长，其中民营企业上云率更是高达 49.2% [1]。而《Gartner 中国云基础设施和平台服务市场指南》预测：到 2024 年，中国终端用户在系统的基础设施和基础设施软件上的支出约 40% 将会转到 “云服务” 上 [2]。随着越来越多的企业选择将云计算技术应用到其生产经营中，以及云计算及相关技术的广泛普及，企业对云安全的需求也随之增加。



2021 年不同企业上云率（来源：亿欧智库《2021 年中国企业上云指数洞察》）

大多数云提供商都试图为客户创建安全的云。他们的商业模式取决于防止违规行为和维护公众和客户的信任。云提供商可以尝试避免他们提供的服务出现底层安全问题，但客户如何使用服务、向其添加哪些数据以及相应的权限控制则由客户自行负责。客户的配置不当、敏感数据保护不到位和访问策略不当都会导致云上的网络安全水平下降。因此，云安全责任将由云服务提供商和云租户共同承担，具体的职责划分会根据使用的云服务类型而变化 [3]。

Infrastructure as a Service (IaaS) – 用户可以在云服务提供商提供的基础设施上部署和运行任何软件，包括操作系统和应用软件。用户没有权限管理和访问底层的基础设施，如服务器、交换机、硬盘等，但是有权管理操作系统、存储内容，可以安装管理应用程序。

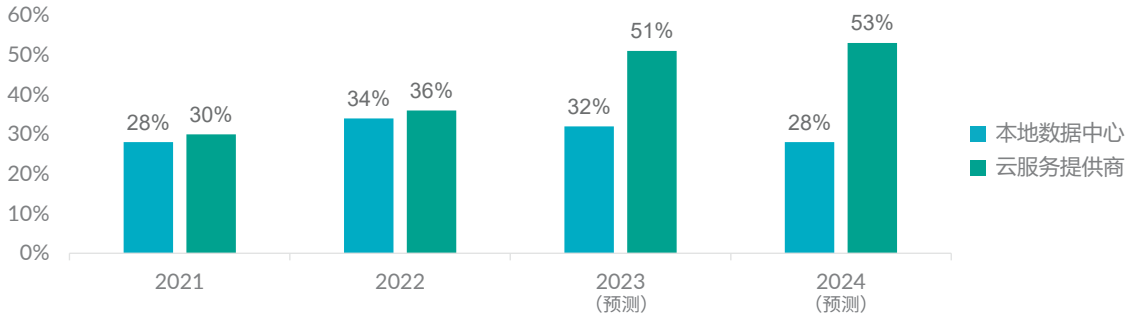
Platform as a Service (PaaS) – 用户使用由云服务提供商支持的编程语言、库、服务以及开发工具来创建、开发应用程序并部署在相关的基础设施上。用户无需管理底层的基础设施，包括网络、服务器、操作系统或者存储。用户只能控制部署在基础设施中操作系统上的应用程序，配置应用程序所托管的环境的可配置参数。

[1] 2021 中国企业上云指数洞察报告：https://www.iyiou.com/research/20220210968
[2] Gartner 发布中文版本《中国云架构和平台服务市场指南》：https://www.skyguard.cn/news/10163.html
[3] 《云计算关键领域 – 安全指南》：https://cloudsecurityalliance.org/artifacts/security-guidance-v4-0-chinese-translation/

Software as a Service (SaaS) – 用户可以使用在云基础架构上运行的云服务提供商的应用程序。可以通过轻量的客户端接口或程序接口从各种客户端设备访问应用程序。用户无需管理或控制底层云基础架构，包括网络、服务器、操作系统、存储甚至单独的应用程序功能 [3]。

为什么需要云安全

受全球企业数字化转型的影响，越来越多的企业依赖云架构为技术基础，采用虚拟分布式存储的方式，在云端管理其数据资产。《Veeam 2022 数据保护趋势报告》调研显示，2022 年，34% 的企业选择把数据备份在本地数据中心，36% 的企业选择把数据备份在云端，还有部分企业暂未确定其数据备份保护方案。该报告还预测在未来两年内会有更多的企业将使用云计算资源进行数据备份 [4]。同时，Gartner 也发现，中国数据库正加速增长并逐步向云端迁移。随着企业持续向云端迁移，针对云计算安全威胁的技术也呈现出复杂、先进的特点，而若未能有效地应对云计算中的威胁及挑战，可能会对企业产生重大影响，因此了解安全要求以及确保云端资产安全就变得至关重要。



企业灾备战略（来源：《Veeam 2022 数据保护趋势报告》）

根据最近的研究，在使用公共云服务的企业中，约 1/4 经历过恶意行为者的数据盗窃，另有 1/5 经历过针对其公共云基础架构的高级攻击。在同一项研究中，83% 的组织表示他们将敏感信息存储在云中。如今，全球有 97% 的组织使用云服务，因此每个人都必须了解企业迁移到云上所面临的安全风险与挑战 [5]。

云计算安全挑战

无论企业是否上云，安全性这一个问题始终适用于所有企业。企业面临的风险通常包括拒绝服务、恶意软件、SQL 注入、数据泄露和数据丢失等等。所有这些风险都会对企业的业务声誉和底线产生重大影响。以下介绍了常见的云安全风险及挑战：

有限的资源能见度及控制

企业在共享责任模型承担了云用户的一些责任，也限制了对云资源的控制。云用户必须依赖提供商来提供资源、调整底层硬件等。因此，云上资产安全在一定程度上取决于云提供商的安全能力。

配置错误

云服务的使用引入了许多需要客户端配置的设置。许多企业存在由于对云上资产的错误配置导致安全事件。

数据安全

我们总能在新闻中看到与云相关的数据泄露趋势。原因从错误配置到网络攻击各不相同。但这一切都取决于与云相关的总体数据保护。

业务停机

尽管云计算具有弹性，但是由于云平台基础架构由云提供商控制，云用户无法阻止其系统业务停机的情况发生。

合规风险

由于企业的基础架构发生改变，很有可能由于对监管要求的疏忽而面临合规风险，例如等保 2.0 对云计算的拓展要求。

[4] 2022 Data Protection Trends Report: https://www.veeam.com/wp-data-protection-trends-report.html?wpty

[5] 调查：采用公共云的四分之一组织的数据被盗：https://www.secrss.com/articles/2481

受限的控制

大多数公司将通过多个设备、由多个部门自不同地区访问云上的资源。在没有适当工具进行管控的情况下，云计算的性质可能会导致公司失去对基础架构访问的控制和审计能力。即，如果没有正确的流程，企业可能并不清楚哪些用户在使用自己的云服务，包括他们正在访问、上传和下载的数据。在这种情况下，由于企业对基础架构缺少能见度，企业无法确保相关数据和资产的安全性，如服务商遭遇意外删除，自然灾害等状况，可能会导致云用户数据的永久丢失；而同时云用户亦无法控制云平台底层的基础架构或备份策略，从而增加了数据泄露和数据丢失的风险。

与自己所在场所的控制服务器和应用程序相比，IT 团队在第三方云服务提供商的环境中对数据的访问权限更少。默认情况下，云客户将获得有限的控制权，并且无法访问底层物理基础架构 [6]。

合规风险

随着监管控制的加强，企业需要遵循一系列合规要求。使用云计算服务为法规和内部合规性增加了另一个维度的风险，即当企业迁移到云时可能会造成的合规风险。根据业务性质的不同，企业的云环境可能需要遵守 HIPAA、PCI DSS 和等保等法规要求，以及其他内部团队、合作伙伴和客户的安全要求。其中，许多法规要求企业了解其数据位于何处、谁有权访问它、如何处理数据及如何保护数据等。此外，云提供商基础架构以及内部系统和云之间的接口等也都包含在合规性检查和风险管理流程中。将数据传输到云端或未在云端按照相应法规要求保护数据，都可能会使组织处于不合规的状态，引发潜在的重大法律、财务及名誉等各方面影响 [6]。

配置不当

云服务的配置不当是另一个潜在的风险。随着服务范围和复杂性的增加，发生配置不当的可能性也随之上升。云服务的配置不当可能导致数据被公开、未授权修改甚至删除 [7]。

CSA 报告称，公共云资源的错误配置是数据泄露的主要原因。这种错误配置的常见示例包括：不安全的数据存储、过多的权限、默认设置中保留的凭据或设置不正确或完全禁用的其他控制功能 [8]。

研究表明，目前只有 26% 的公司可以审核其 IaaS 环境是否存在配置错误。IaaS 的错误配置通常充当云原生漏洞的前门，允许攻击者成功登陆，然后继续扩展和泄露数据。研究还显示，云客户在 IaaS 中忽略了 99% 的错误配置 [6]。

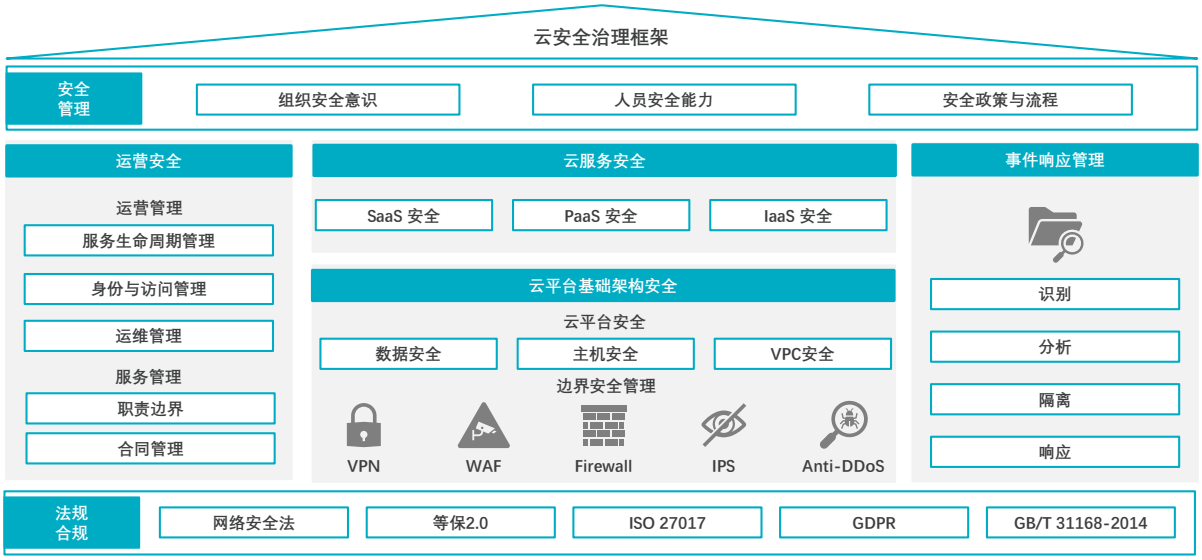
企业的应对之道

当企业选择将其应用 / 系统服务转移到云上，以往的许多安全流程和实践将仍然适用。然而，为了维护基于云的系统和数据安全，企业需要克服云计算相关的一系列安全挑战。甫瀚咨询汇编了云安全治理的最佳实践及建议来帮助企业更好应对基于云的安全风险。

[6] What is Cloud Security: https://www.mcafee.com/enterprise/en-in/security-awareness/cloud.html

[7] A Comprehensive Guide to Cloud Security in 2022: https://kinsta.com/blog/cloud-security/#7-security-risks-of-cloud-computing

[8] Emerging Public Cloud Security Challenges to Watch For: https://cloudcheckr.com/cloud-security/emerging-public-cloud-security-challenges/



选择受信任的云服务商

云安全的基础是建立在选择正确的云服务提供商的基础上。企业希望与提供最佳内置安全协议并符合最高级别行业最佳实践的云提供商合作。目前市场上领先的云服务提供商通常都会将自己的安全合规性及安全认证公开，如此，企业可通过了解服务商的情况来判断该服务商的安全能力，提供的安全防护服务，如 WAF、IPS、Anti-DDoS 等来确保云平台基础架构的安全。

提升组织用户云安全能力

用户是安全中的薄弱环节，云安全也不例外。他们对安全实践的了解和应用是对组织系统进行保护或为网络攻击打开大门之间的区别。企业应确保以安全的云实践培训所有访问组织系统的用户（员工和利益相关者），正确并有效的对相关人员进行网络安全意识培训，包括如何发现恶意软件，识别网络钓鱼电子邮件，以及不安全做法的风险等，这些都是防范相应攻击的有效手段。

对于直接参与实施云安全性的更高级用户（如管理员），企业可考虑为其进行特定于行业的培训和认证，如 CSA 的 Certification of Cloud Security Knowledge (CCSK), Certified Cloud Security Professional (CCSP), 以及阿里云云安全工程师 ACP 认证 (Alibaba Cloud Certified Professional – Cloud Security) 等，帮助企业提升自身对云安全的了解及治理能力。

使用安全治理解决方案提升云安全及合规性

近年来各国政府和权威机构纷纷推出解决威胁个人和组织网络安全问题的举措，如今全球法规、标准日益完善，对企业提出了更高的合规要求。然而，当企业迁移到云上，往往产生难以全面识别复杂的法规 / 标准、合规管理方式高成本低效率、无法量化结果等问题，会给企业的合规遵循带来巨大的压力和挑战[9]。

当企业了解需要遵守的法规 / 标准后，需要研究云服务商如何能够帮助企业满足相应法律要求，如云服务商通过相关认证 (GDPR、HIPAA、PCI DSS 等) 及提供安全合规类产品来帮助用户提升云安全及合规能力。

目前领先的云服务商大多提供了安全合规检查 / 评估类服务，如 Microsoft 的 Compliance Manager 允许用户选择需要合规的法规标准，并将标准拆分成不同的行动计划。用户通过完成相应的改进行动从而达到满足法规标准的相应要求。另外，AWS 的 Security Hub，Microsoft Azure 的 Security Center，阿里云的配置审计，以及华为云的 Compliance Compass 等产品均实现了不同程度的合规要求自动化，通过自动化合规策略 — 策略即代码 (Policy as Code)，尽可能将法规标准条款代码化、策略化，通过周期性、自动化的扫描帮助客户盘点各个云服务的合规情况，并通过可视化看板将风险状况直观呈现，同时提供具体改进建议[9]。

[9] 华为云安全治理云图 Compass 正式公测：https://caijing.chinadaily.com.cn/a/202112/02/WS61a82fd4a3107be4979fafe9.html

达于行

甫瀚咨询可提供的服务

甫瀚咨询为企业提供企业安全治理及架构设计咨询，从治理、合规及技术角度，全面协助企业提升云安全保护水平，达成安全保护从无到有、从弱到强的转变，为优化企业综合安全治理水平奠定基础。我们可提供的安全治理相关服务包括：

云平台安全架构设计

根据行业最佳实践，侧重企业上云的底层设计，包括网络拓扑设计、安全组件使用、安全组和子网设计等。

云安全策略评估及设计

重点关注云计算安全策略的评估与设计，包括角色、权限、SaaS 安全、数据安全、备份、恢复、云安全策略和要求等。

云端配置扫描

对使用的云组件按照指定的法规标准、最佳实践、内部要求进行配置扫描以发现潜在风险，确保与实施和安全设计的一致性。

安全工具实施咨询

评估企业业务、规模、所处行业以及信息资产架构等信息，提供相关安全工具实施建议，如合规评估工具、安全监测工具、安全防护工具等，帮助企业有效管理云端资产安全。

安全意识与能力咨询服务

针对行业 / 企业 / 部门 / 角色等高度定制化的云安全意识与能力培训，提供最大化的效率和安全意识，确保人员管理不再是企业安全的短板。

关于甫瀚咨询

甫瀚咨询是一家全球性的咨询机构，为企业带来领先的专业知识、客观的见解、量身定制的方案和卓越的合作体验，协助企业领导者们充满信心地面对未来。透过甫瀚咨询网络和遍布全球超过25个国家的逾85家分支机构和成员公司，我们为客户提供财务、信息技术、运营、数据、数字化、环境、社会及管治、治理、风险管理以及内部审计领域的咨询解决方案。

甫瀚咨询荣膺2022年《财富》杂志年度最佳雇主百强，我们为超过80%的财富100强及近80%的财富500强企业提供咨询服务，亦与政府机构和成长型中小企业开展合作，其中包括计划上市的企业。甫瀚咨询是Robert Half International Inc.（纽约证券交易所代码：RHI）的全资子公司。RHI于1948年成立，为标准普尔500指数的成员公司。

联系我们

余达丽
项目总监
Angela.Yu@protiviti.com

张甄鑫
经理
Jason.Zhang@protiviti.com

尹必成
高级咨询顾问
Oliver.Yin@protiviti.com

公司地址

北京
朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海
徐汇区陕西南路 288 号
环贸广场二期 1915-16 室
电话：(86.21) 5153 6900

深圳
福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

香港
中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti 甫瀚