Microsoft

白皮书

# 可信在云端

Microsoft Azure 由 世纪互联 运营

Office 365 由世纪互联运营

根据 Forrester Research 最近的一项研究，公有云服务支出预计在 2016 年达到 1060 亿美元，比 2015 年的预计支出水平增长 21%。《2015 年电脑世界预测研究》（ComputerWorld Forecast Study 2015）发现，云计算项目是如今多数 IT 部门最重要的项目。向云端转移，存在诸多原因：现买现付成本模型、可以从任何位置或通过任何设备进行全球访问、根据业务需求变化调整规模、内置的灾难恢复、和为 IT 部门提供更大的灵活性，以满足整体发展和规模化经营的需要。随着这些承诺得以兑现，各公司正在认识到如何将其云业务上升到一个新的水平，并将云纳入其整体业务战略。

但与此同时，出于对安全、隐私和合规问题的关切，许多首席信息官仍然对云的使用心存疑虑。由于网络安全存在对公司品牌、市场份额和营收产生负面影响的潜在可能，因此已经得到首席执行官和董事会层级的关注。采取统筹兼顾方法、对客户和监管机构保持透明的外部云服务提供商能够提供比企业内部更多的风险保障。

# 转型云端

今天，各个组织正在超越云计算的早期承诺，利用其速度、规模、和经济效益转型业务，重塑与客户沟通的方式，提高员工的工作效率，推动新的、更快的创新来源。例如，云的规模和范围正在帮助企业利用海量数据，以改善其对业务的认识。营销人员正在利用这些认识加强与客户的协同。移动办公的员工正在共享数据和应用，以提高协作效率和整体工作效率。管理人员正在开发新的商业模式，并创造新的基于服务的收入流。

根据国际数据公司（IDC）最近的报道1，云服务市场正在进入"一个将在云上产生海量新型解决方案和价值创造的创新阶段"。云的规模和范围将使这一情况成为可能，并以我们重新定义全球经济的方式来改变企业和政府单位。

***"把云计算做为纯粹节约成本方法的公司正在失去更多的机会。"***

*Tom Lamoureux*
*技术媒体和电信部门风险咨询负责人*
*毕马威*

# 风险和脆弱性

更多的机遇也带来了新的风险和复杂的挑战。威胁形势不断发展，网络犯罪分子正在寻找新的方法来破坏商业和政府活动。隐私是和管控人们最关心的问题，采用云来实现其业务现代化的公司正在要求在其数据管理

[1] 《国际数据公司（IDC）预测公共 IT 云服务支出》，2014 年 11 月

和使用方面拥有更多的控制权和参与权。微软最近在对全球 2600 多个 IT 决策者进行的调查中发现：对于利用公有云而言，安全、隐私和数据控制位居最迫切的业务考量之首。

# 安全仍是主要顾虑

安全漏洞的消息继续主导头条新闻，而非法侵入的规模和范围也在不断增长。仅在 2014 年，数据泄露比上年同期增长了 49%，网络犯罪分子在 1500 多个漏洞中窃取了超过十亿的数据记录[2]。在世界经济论坛[3]的 2014 年报告中，麦肯锡预计网络攻击风险“可能实质性减缓技术和业务创新的步伐，总影响高达 3 万亿美元”。在任何安全攻击中，目标组织的安全程度仅与其最薄弱环节的安全性相当：如果任何环节没有得到保护，那么整个系统将处于危险之中。虽然 IT 领导者承认云可以提供更高的数据安全性和管理控制权，但他们仍担心：从他们目前的内部解决方案迁移到云，将使他们更容易受到黑客攻击。

**威胁来源的类型和攻击方法[4]**

| 威胁来源 | 目的和动机 |
|---|---|
| 公司 | 搜集商业情报，提高竞争优势 |
| 国家 | 锁定国家机密、军事情报、关键基础设施 |
| 黑客行动主义者 | 意识形态，或者寻求媒体关注 |
| 网络恐怖分子 | 寻求危害国家安全和社会 |
| 网络犯罪分子 | 寻求通过网络空间的非法活动谋利 |
| 网络斗士 | 受民族感召的公民，受到政治、民族或宗教价值的推动 |
| 在线社交黑客 | 使用社交媒体，利用社会目标的心理 |
| 雇员 | 不满或沮丧的内部人员 |
| 业余黑客 | 年轻的技术达人，寻找目标证明自己的技能 |

## 隐私挑战

由于公有云在多租户环境中运行的规模，云服务对企业提出了新的隐私挑战。公司希望利用云来节省基础设施成本并提高灵活性和敏捷性，同时也担心失去对其数据存储、访问、和使用等方面的控制权。

[2] Gemalto，《2014 年漏洞水平指数报告》

[3] 麦肯锡公司，《世界经济论坛》，2014 年 1 月

[4] 欧盟网络与信息安全机构；《欧洲网络与信息安全局（ENISA）2014 年威胁形势》，当前和新兴网络威胁概述

即使在积极利用云部署更多创新的解决方案的过程中，企业仍对数据的控制权、所有权、以及对其控制能力以外的事情负有责任而忧心忡忡。因此，许多企业都在选择其数据在云端的存储地点，并对能够访问其数据的机构设限。在微软最近一次的调查中，75%的 IT 受访者表示他们的首要义务是保护其客户的隐私。

# 基于微软技术的可信云

微软的云基础架构支持分布在 140 多个国家超过十亿企业和消费者客户，并且支持 10 种语言和 24 种货币。在中国，借鉴微软独特的经验和规模，基于微软技术由世纪互联独立运营的 Microsoft Azure 和 Office 365 为客户提供安全、隐私、合规、透明的可信云服务。

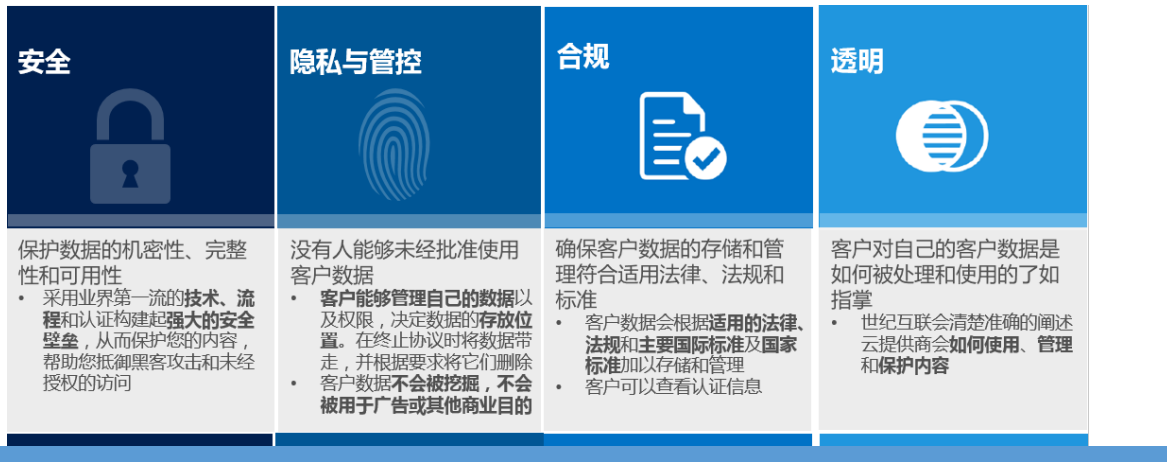
**200 多**项云服务
**100 多**万台服务器
**超过150 亿美元**的基础设施投资

**10 亿**客户
遍布**90个国家/地区**的云服务
**80%的500强企业**


客户需要捍卫自己对于安全和私有数据的权利，并设置客户可以信赖的安全性、合规性和数据隐私性标准。我们相信：这样的需求不仅需要确保安全的技术来支撑，也需要能跟上云时代创新和转型步伐的最新监管要求和标准，来对执行过程和方法的透明度进行适当的审计。

## 可信云的基本原则

基于微软服务与全球的同源技术，由世纪互联独立运营的 Microsoft Azure 和 Office 365 云服务基于一套安全可信的理念来实现我们的云安全。例如，在数据方面，我们认真对待我们的承诺：帮助保护客户数据、保护客户对有关数据的的控制权和决策权、帮助客户满足其数据的合规性要求、以及企业云服务保持透明。以下四个可信云的原则表达了我们认为企业组织可从可信的云服务提供商获得的服务。



# 安心地迁移到云端

## 投资您的安全

**现场事件响应：**世纪互联配备了全天候事件响应团队，帮助消除攻击和恶意活动的威胁。事件响应团队由有经验的安全专家领导，负责提供安全响应，提高客户的安全性，推进安全领域的技术创新，提供权威的安全指导。事件响应团队时刻保持警惕，以识别、调查、解决安全事件和安全漏洞。检测安全事件会调动技术团队和沟通团队，技术团队和沟通团队在此过程中通力协作，由技术团队对问题展开详细调查并制定解决方案，由沟通团队为客户制定指南。

**安全的设计：**做为云服务的技术提供商，微软创建、实施、并不断提高其软件开发和威胁缓解实践的安全性。由世纪互联运营的 Microsoft Azure 和 Office 365 是基于微软技术，而微软许可给世纪互联的技术应用遵循安全开发生命周期（Security Development Lifecycle）进行开发。SDL 流程旨在降低 Azure 和 Office 365 中漏洞的数量和严重性。自 2004 年起，SDL 就将对安全的需求嵌入整个软件开发生命周期中。

**持续的测试和改进安全性：**威胁建模、静态代码分析和安全测试都有利于列举、减少和管理攻击表面，但它们并不能消除所有安全隐患。为了发现不可预见的漏洞和改进检测和应对能力，Azure 和 Office 365 采用持续的漏洞测试。专业的团队密切监测并确保云基础设施、云服务、产品、设备和内部资源，在不断模拟真实世界中每一个级别的漏洞。

**威胁检测、缓解和响应：**随着网络威胁的数量、种类和严重程度的增加，我们在威胁检测和响应中的努力也在增加。集中监控系统为管理我们云服务的团队提供持续的可见性并适时发出警报，而额外的监测、记录和报告功能为客户提供可见性。安全补丁的普遍应用和更新有助于保护系统免受已知漏洞的威胁。入侵和恶意软件检测系统用于检测和减轻外部攻击的风险。在恶意活动的情况下，我们的全天候事件响应小组遵循既定的事件管理、通信和恢复流程。该团队使用业界最佳实践方案，以提醒内部团队和客户。最后，安全报告监控访问模式，以帮助主动识别和缓解潜在的威胁。

***75％的攻击利用商业软件中众所周知的漏洞，而我们可以通过定期打补丁来防止这些漏洞入侵。***

*CyberEdge 集团*
*《2014 年网络威胁防御报告》*

**数据保护：**数据是数字经济的货币，我们承担着保护客户数据的重任。加密通信和操作流程这两种技术保障措施都有助于保全客户数据。在云端，来自多个客户的数据可以存储在相同的物理硬件上。基于微软技术由世纪互联运营的云服务使用逻辑隔离，把每个客户的数据与其他人的数据隔离开来。对于传输中的数据，Azure 和 Office 365 在用户设备与数据中心之间以及数据中心内部使用行业标准加密传输协议来保护客户数据安全。为了加强对加密数据的用户控制，我们致力于为客户提供云服务使用的加密密钥的控制，使客户能够灵活地选择最能满足其需求的解决方案。客户拥有选择权，可以防止世纪互联拥有其加密密钥的副本，但这样一来，如果出现问题或产生安全威胁，世纪互联无法排除故障或修复该问题，就有可能限制客户对云服务的充分使用。

**网络保护：**网络威胁正变得越来越复杂，使我们有责任提供安全连接，无论是在我们的云基础设施中，还是您的数据中心与我们的数据中心之间。我们从隔离多种部署模式的网络开始进行设置，这使我们能够防止在同一硬件上不需要的跨租户通信。由世纪互联运营的 Microsoft Azure 和 Office 365 使用多种技术阻止发往数据中心以及数据中心内部的不良通信，例如防火墙、分区局域网（ LANs ）以及后端服务器与公共接口的物理分离，虚拟机不接收来自互联网的传入流量，除非客户配置它们接受阻断发往数据中心的以及 Azure 和 Office 365 数据中心内部的未经批准的流量。我们提供虚拟网络，使客户能够在订阅中指定多个部署，并且使这些部署通过私有 IP 地址相互通信。每个虚拟网络与其他虚拟网络相互隔离。内建的 SSL 和 TLS 的加密技术使得客户能够对同一部署内部，不同部署之间，从 Azure 到内部部署数据中心，以及从 Azure 到管理员和用户的通讯进行加密。客户还可以使用可选的 Azure ExpressRoute 在 Azure 数据中心与本地的基础结构之间创建专有连接。ExpressRoute 使用专用 WAN 直接连接，相比互联网连接更可靠，更快速，更安全。

> *“您大可不必出于安全考量抗拒云计算了。”*
>
> *弗雷斯特研究公司（Forrester Research）*

**身份和访问：** 对于访问权限、访问级别、访问信息、访问位置和设备的管理是客户安全策略的关键要素。Azure 和 Office 365 可以很容易地定义和管理一个或多个云服务的身份和访问控制。Azure Active Directory 提供了云端的全面的身份和访问管理解决方案，使开发人员可以在他们的应用程序中轻松构建基于策略的身份管理，在多个设备上使用。多因素身份验证可同时用于终端设备和云应用，降低组织风险，并有助于在用户的帐户凭据以外提供额外的一层身份验证，从而能够遵守法规，以确保员工、客户和合作伙伴访问。在多个云服务的工具还支持基于用户角色的授权，简化了跨界定用户组的访问控制。管理操作

（包括系统的访问）都进行了记录，从而为意外或未经授权更改的情况提供审计线索，可按客户要求向其提供有关用户访问其环境信息的报告。

**可见性和控制：**保护客户数据和系统是一个共担的责任，我们认识到：客户了解自己在分布式基础架构中的安全状况对业务稳定至关重要。世纪互联提供不同级别的监控、日志和报表，为客户提供可见性。在 Azure Management Portal 中，客户可以浏览使用情况和资产报告，例如异常登录事件报告、特定用户报告及活动日志等，使客户对安全策略有更多控制权，并提供可见性，在威胁到来之前做好准备。

# 保护客户数据的隐私

**清晰的指引和选择客户数据的位置：**对于许多客户而言，了解和控制他们的数据位置可能是数据隐私合规和治理的一项重要内容。我们与客户共享有关客户在数据存储设施中存储其数据的地理位置的高层次的信息。数据存储位置公开透明，客户拥有灵活的选择权。数据可以在相互冗余的中国东部和北部的数据中心之间进行复制，但不会发送到中国以外的地区。

**严格访问权限：** 世纪互联工作人员被限制访问客户数据。Lock box 控制着世纪互联工作人员及其分包商访问您的数据所需要的授权。世纪互联采用最小化数据块技术，分层决定哪个内部团队可以访问数据。客户数据只能在必要时被访问，以支持客户使用我们的云服务。这可能包括故障排除，旨在防止、检测或修复影响服务运行的问题、或保护和检测免受安全威胁（如恶意软件或垃圾邮件）的功能改进。当被授权时，访问权限被严格控制并记录，并且这些报告要进行审计。强大的身份验证（包括使用多因素身份验证）有助于把访问权限于经授权的工作人员。访问权在不再需要时将立即撤销。我们不会为了任何广告或类似的商业目的而获取、维护、扫描、索引或挖掘客户数据。

**执法机关或第三方请求：**当执法机关或其他第三方依法强制要求披露世纪互联存储的客户数据时，我们会坚持透明的原则，并最小程度的披露数据。世纪互联认为，客户应控制自己存储在本地或云服务中的信息。相应地，我们也不会向第三方（我们的供应商和分包商除外）披露客户数据，除非您指示我们这样做或适用法律和法规要求我们这样做。如果我们必须向某一第三方披露客户数据，我们将采用商业上合理的努力立即通知您并提供相应要求的副本，除非法律禁止我们这样做。

**隐私声明：**由世纪互联运营的 Microsoft Azure 隐私声明和由世纪互联运营的 Office 365 的隐私声明介绍了对客户使用 Azure 及 Office 365 服务适用的隐私政策和惯例。

**控制数据销毁：**当客户删除客户数据或离开云服务时，世纪互联会遵循严格标准：在重新使用之前覆盖存储资源，并且对退役的硬件进行物理销毁。世纪互联应客户要求立即或在服务终止或到期之后 90 天执行彻底的数据删除。客户有权在他们离开服务时带走他们的数据。数据便携性和可转移性是我们服务的关键属性，以避免厂商控制的担忧。

**特定服务的控制选项：**Office 365 服务提供额外的控制，使客户能够管理安全和隐私选项，包括反病毒、反垃圾和反恶意软件保护的电子邮件设置、在线会议控制、法律限制从而有选择地保留电子存储信息，以及 e-Discovery 允许客户为了法律调查的目的而查找和检索整个 Office 365 服务的内容。

# 使您的组织满足合规标准

世纪互联致力于通过第三方审核机构不断的验证，并且与客户共享审计结果和合规方案，帮助他们履行自己的合规义务。

**认证和验证：**由世纪互联运营的 Microsoft Azure 和 Office 365 满足广泛的国际国内和特定行业的合规性标准，如 ISO/IEC 20000 和 ISO/IEC 27001，公安部制定的信息系统安全等级保护定级三级备案，GB 18030 信息技术中文编码字符国家标准以及可信云服务认证（TCS）。世纪互联遵循这些标准中的严格的安全控制，通过严格的第三方审计进行验证，达到世界一流的行业标准、认证、验证、授权。请登陆**信任中心**查看云服务合规性的详细信息。

**合规性框架：** 由世纪互联运营的 Microsoft Azure 和 Office 365 的合规性框架映射到多个监管标准的控制。这使得世纪互联能够使用一套通用的控制设计和搭建服务，简化今天及其未来对于一系列法规的合规性。世纪互联合规流程也更容易为客户实现跨多个业务合规并有效地满足不断变化的需求。安全合规框架包括测试和审核阶段、安全分析、风险管理最佳实践和安全标杆分析，以实现认证和验证工作。

# 保持透明度

由世纪互联运营的 Microsoft Azure 和 Office 365 基于微软云技术，建立在与客户保持透明度的坚定信念之上。当您的数据托管在我们的云服务中时，我们以清楚、通俗易懂的语言来解释我们用它做什么。我们的

操作对您是可见的，您可以监控服务的状态、跟踪问题、回顾过往服务可用性及服务的任何更改。我们以清楚、通俗易懂的语言来解释世纪互联如何使用、管理、并保护您的企业数据。

**审计标准认证：**严格的第三方审计验证了世纪互联坚持这些标准所要求的严格安全控制。作为世纪互联承诺的透明度的一部分，客户可以向认证第三方请求审计结果，来验证世纪互联对许多安全控制的执行情况。

**执法请求：**当执法机关或其他第三方依法强制要求披露世纪互联存储的客户数据时，我们会坚持透明的原则，并最小程度的披露数据。

**漏洞通知：**在客户数据被泄露的事件中，世纪互联将通知其客户。我们有全面的、透明的政策，管控事件响应流程，从事件识别直到经验教训。

# 总结

世纪互联不会把客户的信任当作理所当然。我们知道，信任对于云服务尤为重要。我们郑重承诺：将在当今移动为先、云端为先的世界中保护我们的客户。这些信条是我们提供云服务和技术的基础。我们的可信云（Trusted Cloud）原则将继续指导我们的拓展云业务，使客户能够安心地迁移到云端。

# 更多资源

**信任中心：**更多关于可信云的信息，请访问 https://www.trustcenter.cn