Microsoft

安全与合规性

由世纪互联运营的 Office 365

发布日期：2016 年 6 月

最新信息请访问 信任中心：http:// www.trustcenter.cn

简介

对于全球任何 IT 机构来说，信息安全都是一个重要的考虑因素。除了各种信息技术的流行，针对数量日益增加的设备、平台和地点提供对服务的访问，使得信息安全成为最重要的事。您的用户可以通过多种设备的访问获益，尤其在 IT 消费化的大背景下更是如此，但更广泛的访问途径也意味着潜在攻击面的增多。与此同时，组织还将面对来自全球，不断进化的网络威胁，这些威胁多以可能无意中丢失或外泄敏感数据的用户为目标。

在考虑为组织使用云服务存储数据和各种生产力服务时，需要额外注意安全方面的顾虑。首先需要注意信任问题。您必须能够信任自己的服务供应商在处理和管理您的数据时，能够满足您的重要预期，即安全、隐私，以及合规。

由世纪互联运营的 Office 365 的安全、合规，以及隐私功能，有两个同等重要的维度。第一个维度是服务级别的能力，包括技术、运营规程，以及客户在使用服务的过程中默认启用的策略；第二个维度是必要的客户控制，包括能使您根据组织的具体需求对您的 Office 365 环境进行定制的功能。

Office 365 中的安全保护是一种持续的过程，而非某种恒定不变的状态。这些措施会由具备娴熟技能和经验，训练有素的人员进行持续不断的维护、增强，以及验证。我们会尽力确保软件和硬件技术时刻保持最新状态，并会通过强大的设计、构建、运营，以及支持过程对其进行优化完善。为确保 Office 365 具备业界领先的安全性，我们使用了诸如 安全开发生命周期，流量限制，以及针对入侵活动的预防、检测和缓解等过程。若要详细了解有关 Office 365 安全与合规性的最新详情，您可以访问信任中心。

服务级安全性

在云安全领域，即便针对最为复杂的组织，我们的策略和控制也处于行业领导者地位。我们的团队在持续不断地学习并更新自己的服务，借此为用户提供高度安全的云生产力服务，并在合规性方面满足最严苛的行业标准要求。

在服务层面上，我们使用深度防御策略，通过服务中不同的安全层（分别位于物理、逻辑，以及数据层）保护您的客户数据。

从较高角度来看，这些防御层可以通过下图的结构体现：

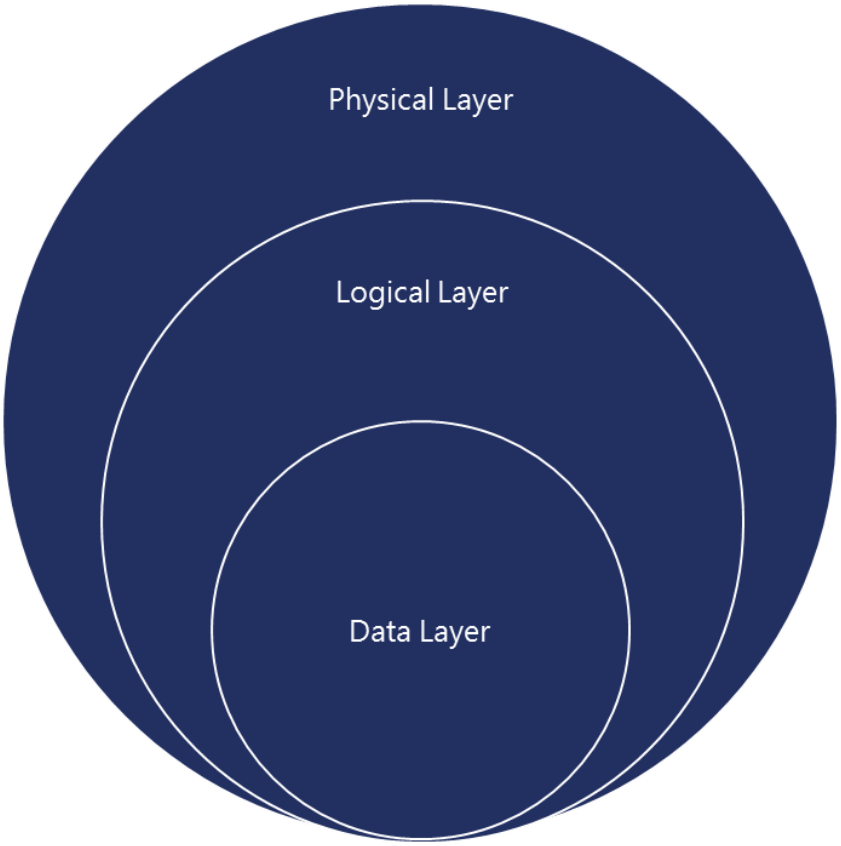

图 1 深度防御

纵深防御策略确保了服务中的诸多层面均具备安全控制，并可确保即使其中某一层被攻破，依然可以通过相应的补偿性控制措施维持服务的安全性。

这个策略还包括在安全入侵事件发生之前对其进行检测、预防、缓解的措施。这些措施会持续对服务层面的下列安全功能进行持续不断的完善：

- 端口扫描和修补

- 边界弱点扫描
- 操作系统安全补丁安装
- 网络级 DDOS（分布式拒绝服务）检测和预防

由世纪互联运营的 Office 365 会借助最新技术和最佳运维实践，通过下列方式防范人员和过程中可能存在的违规情况：

- 对所有运维/管理人员的访问和操作进行审计
- 对服务管理员实行 非持久权限
- 服务排错过程实施“即时 (Just-In-Time, JIT) 访问和提升” 策略（也就是说，按需提升，且仅在需要的时段内提升）
- 员工电子邮件环境与生产访问环境之间进行隔离
- 高特权访问进行强制的背景核查。这是一种非常详尽，需要手工批准的过程
- 客户数据只存储在中国境内的数据中心

为了防范违规情况，我们还会在员工离职、部门变动，或帐户过期前已不再需要使用该帐户的情况下，自动删除所有不必要的帐户。我们会尽可能地使用基于工具的自动化过程取代需要人工介入的操作，包括部署、调试、针对收集，以及服务重启动等例行职能。

我们会对系统自动化机制进行不断的投入，借此帮助我们发现异常和可疑的行为，并通过快速响应措施缓解安全风险。我们还会持续完善高效率的补丁部署系统，为监控系统发现的问题生成并部署解决方案—这一切都无需人工介入。这样的做法极大地增强了服务的安全性和敏捷性。我们会定期进行内部审计和测试，以便对事件响应规程进行持续不断的改进。这些内部测试可以帮助我们的隐私专家和工程师创建出井然有序、可复用，并且逐步优化的响应过程和自动化机制。

物理层—设施和网络安全

设施

考虑到数据存储区域问题，存储在 Office 365 数据中心内的客户数据在地理位置上是分布式的。我们会与中国顶尖的数据中心服务供应商携手合作，保护服务和数据防范自然灾害或未经授权访问所造成的损失。对数据中心的访问会依照工作职责进行全天候限制—只允许必需的人员访问客户应用程序和服务。物理访问控制会使用多种身份验证和安全过程，包括设施内部安全人员的徽章、持续的视频监视，以及双重身份验证。我们会使用动作传感器、视频监视设施，以及安全入侵警报等措施监视数据中心。对于自然灾害，我们还尽可能实施了自动化的火灾预防和灭火系统，以及地震支撑系统。

网络

通过在网络边缘以及网络中的不同节点使用受控设备，我们实施了周边防护措施。对我们来说，网络安全的首要原则是只允许系统执行必要的连接和网络通讯，所有其他端口、协议，以及连接都会被阻止。我们在路由器上使用分层式访问控制列表(ACLs) 实施了 ACLs，在主机上应用了 IPsec 策略，并在网络中使用防火墙规则和基于主机的防火墙规则对网络通讯、协议，以及端口号进行限制。边界路由器的安全措施使得我们能够在网络层面上检测入侵和代表弱点的特征。Office 365 数据中心内部的网络还进行了进一步的隔离划分，借此对关键的后端服务器和存储设备以及对外接口进行物理隔离。

逻辑层—主机、应用程序、管理员用户

逻辑层的安全防护涉及很多控制和过程，这些措施可对主机，这些主机上运行的应用程序，以及需要针对这些主机和应用程序执行任何操作的管理员提供安全保护。

自动化操作

管理员针对主机和应用程序执行的大部分操作都是自动实现的，借此将人工介入的情况降至最低，并降低了产生不一致配置或恶意行为的可能性。这种自动化的方法通过扩展，已经应用于数据中心内部系统的部署工作。

对客户数据的管理访问

管理员对 Office 365 以及您的客户数据的访问会受到严格的控制。这一过程的核心原则是基于角色的访问，以及只为人员提供执行特定操作所必须的最小量服务访问特权。无论访问物理（例如数据中心或服务器）或逻辑资产，均应遵守这些原则。这一过程可形象地称之为“锁箱流程”，管理员需要通过这样的流程申请提升自己的访问特权。

访问控制机制会在不同层面上进行：

1. 人员层面的控制确保了需要进行适当的背景核查和严格的帐户管理，确保只有任务必须的人员可以执行这些任务
2. 基于角色的访问控制
3. “锁箱流程”可实现：
    a. 使用高熵密码（high entropy password）的即时帐户（Just-in-time account）
    b. 受限的访问时间

c. 根据角色访问特定的任务

4. 运行 Office 365 服务的服务器可以使用 Applocker 运行预设的一系列过程。
5. 对所有访问进行审计和审查。

安全开发生命周期

安全开发生命周期 (SDL) 是一套完善的安全保障过程，已融入包括 Office 365 在内的很多软件和服务的设计、开发，和部署等每个阶段。通过设计要求、攻击面分析、威胁建模等手段，SDL 可以帮助开发者从服务发布前一直到服务的整个生命周期过程中预测、发现、缓解弱点和威胁。Office 365 服务会使用最新数据和最佳实践持续更新 SDL，借此确保与 Office 365 有关的新服务和软件从问世的第一天就是高度安全的。

反恶意软件、补丁安装，以及配置管理

反恶意软件程序的使用是保护您存储在 Office 365 中的资产防范恶意软件的重要机制。这些软件会检测并预防计算机病毒和蠕虫感染服务系统，并隔离被感染的系统，确保采取补救措施前不会造成进一步损失。反恶意软件程序可针对恶意软件提供预防和检测控制。

我们会详细记录针对服务器、网络设备，以及其他 Microsoft 应用程序所应用的基线配置要求标准，这些标准中会列出所用的标准程序包。我们会使用安全控制对这些程序包进行预测式和配置。

针对生产环境所进行的，诸如更新、热修复，以及补丁安装等变更需要遵守相同的变更管理过程标准。我们会按照发布补丁的公司所指定的时间框安装补丁。在实施变更前，我们的审阅团队和 变更管理团队 会对变更的适用性、风险，以及资源的分配进行审查和评估。

数据层—数据

Office 365 是一种高度可扩展的多租户服务，这意味着您的数据会与其他客户的数据一起，以一种安全的方式共用某些共同的硬件资源。在设计过程中，我们确保了 Office 365 能够通过数据隔离机制，在服务中以一种高度安全的方式托管多个客户。每个租户的数据存储和处理都会通过 Active Directory，以及针对多租户环境的构建、管理和保护等具体需求开发的功能进行隔离。Active Directory 会使用安全边界隔离您的数据。您的数据将受到妥善保护，不会被共置租户所访问或威胁。

数据完整性和加密

为了保护数据的机密性和完整性，我们的 Office 365 服务使用了行业加密标准，例如 TLS（传输层安全）和 AES 等。

为了保护传输过程中的数据，客户直接访问的所有服务器会通过与客户端计算机协商，使用 TLS（传输层安全）建立安全的会话。这一机制适用于多种协议，例如 HTTP(S)、POP3 等，并被很多客户端使用，例如任何设备上使用的 Lync、Outlook，以及 Outlook Web App (OWA)。TLS 技术的使用可以在客户端与服务器之间建立高度安全的连接，保障桌面和数据中心之间所传输数据的机密性和完整性。

在其他某些适用的场景中，我们会使用文件级别的加密。例如，当会议参与者上传了文件和演示文稿后，这些内容会被 Skype for Business Online 的 Web 会议服务器进行 128 位 AES 加密。

借助最新的加密功能，传输至 OneDrive for Business 和 SharePoint Online 存储的内容会使用一种名为*每文件加密*的措施进行加密。借此，Office 365 中的加密技术远远超越了“每磁盘一个加密密钥”的加密方式，而是使用独一无二的“每文件一个加密密钥”方式。在这种技术的帮助下，SharePoint Online—包括 OneDrive for Business 文件夹—中存储的每个文件都会使用自己专用的密钥加密，后续对每个文件进行更新时也需要使用该文件专用的密钥进行解密。我们并不会将您的组织所存储的文件集中存储在一个数据库内，而是将其分散保存在多个 Azure 存储容器中，每个容器都需要专门的凭据。通过将加密后的文件分散保存到多个存储位置，对文件位置分布图本身进行加密，并将内容和文件分布图的主加密密钥进行物理隔离，这种全新的加密存储技术使得 OneDrive for Business 和 SharePoint Online 为您的数据提供了一个高度安全的环境。

保护防范安全威胁

Office 365 的威胁管理策略由发现潜在威胁的意图、能力，以及成功利用相应弱点的可能性等控制措施组成。用于保护防范此类行为的控制机制很大程度上建立在相应安全标准基础之上。通过独立审计机构对 Office 365 按照 ISO/IEC 27001 和 信息系统安全等级保护第三级等标准实施的控制机制进行验证，您将可以评估我们部署的这些控制机制的效果。

网络威胁的整体大环境已经从传统的机会型威胁进化为包括持续顽固型攻击在内的更高级形式。为了防范从常见的“黑客活动”到网络犯罪在内的各种威胁，我们为您提供了深度防御的方法。

我们的 Office 365 安全策略建立在一种动态的策略基础上，包含四大主旨。为了让我们的防御更有效，更加与时俱进，我们转变思路使用了一种通常被称之为“假定违反”的思维方式，会假定环境中已经发生违反的情况，只是暂时未知。基于此思维方式，世纪互联的安全团队会持续尝试检测并缓解并未广为人知的安全威胁。为此我们所做的一种实践是人为地制造一种安全威胁，并让另一组成员响应和缓解这个威胁。这些练习的主要目标是让 Office 365 更具适应性，以便快速检测并缓解新出现的弱点。

安全策略的第一个主旨可称之为“防止违反”。我们在这方面的投入包括对内建的安全功能进行持续的改善。例如端口扫描和修补、边界弱点扫描、操作系统修补、网络层面的隔离/违反边界、DDoS（分布式拒绝服务）检测和预防、即时访问、适用于服务访问的实时站点渗透测试。

第二个主旨称之为“检测违反”。为此，我们会通过大量内部分析系统收集并汇总各种系统和安全警报。警报系统会分析来自系统内部以及外部（例如来自客户事件）的信号。根据机器学习技术，我们可以快速引入能够触发警报的新模式，并根据系统异常自动触发警报。

第三个主旨称之为“响应违反”。如果有组件受到威胁，可以通过该主旨缓解威胁造成的后果。我们为事件准备了尽职尽责的事件响应过程和标准的操作规程，能够拒绝或阻止对敏感数据的访问，并会通过鉴定工具迅速确定涉及方，确保事件得到成功的缓解。

第四个主旨称之为“从违反中恢复”，其中包含标准操作规程，可顺利恢复服务的正常运作。该主旨还使得我们能够更改环境中的安全主体，自动更新受影响的系统，并对部署状态进行审计以发现可能存在的任何异常情况。

独立验证

Office 365 将运营安全全面融入到一个可扩展的过程中，可快速适应安全趋势和特定行业的需求。世纪互联会定期进行风险管理审查，制定并维护一套能够满足最新标准的安全控制框架。Office 365 服务的生命周期内还包括内部审查和可信赖机构进行的外部审计。世纪互联内部其他团队之间的密切合作关系确保我们可以通过完善的方法保护云中应用程序的安全。

我们会通过独立审计，并对 ISO/IEC 27001、信息系统安全等级保护 (http://www.djbh.net/) 以及 可信云服务认证 (http://www.kexinyun.org) 等标准的遵守情况进行验证，借此让 Office 365 安全技术和最佳实践获得您的信任。

客户的安全控制

Office 365 将您熟悉的 Microsoft Office 套件与 Exchange Online、SharePoint Online，以及 Skype for Business Online 等下一代通讯和协作云服务有机结合在一起。这些服务中每一个都提供了可由您控制的各类安全功能。这些控制可以帮您符合合规性要求，为组织中的个人分配对服务和内容的访问，配置反恶意软件/反垃圾邮件控制，以及加密数据。

数据完整性和加密

虽然 Office 365 在服务层面已经实施了加密技术，并由世纪互联负责管理，世纪互联还为您提供了各种技术，可供您在自己的 Office 365 租户中实施和配置。这些技术可以让您针对不同工作负载用不同方法加密数据，并能让您对存储后和传输中的数据进行加密。这些技术包括：

- 安全多用途互联网邮件扩展 (S/MIME)
- 针对合作伙伴，提供适用于 SMTP 邮件的传输层安全 (TLS)

安全多用途互联网邮件扩展

S/MIME（安全/多用途互联网邮件扩展）是一种适用于 MIME 数据的公钥加密和数字签名标准。

S/MIME 可供用户 (1) 加密电子邮件，(2) 为电子邮件添加数字签名。S/MIME 为电子邮件应用程序提供了下列加密安全服务：身份验证、邮件完整性、发送方不可抵赖性（使用数字签名）、隐私和数据安全（使用加密）。

您可以在内部部署环境中使用公钥基础结构 (PKI) 为最终给用户生成公钥和私钥。公钥证书会发布到您内部部署的 Active Directory 中，并存储在两个属性内，随后即可复制到您在 Office 365 中的租户内。私钥证书需要分发给最终用户，可能存储在用户的设备、智能卡，或其他应用程序内。您需要在自己的 PKI 基础结构中维持对主密钥的控制。

此外，Office 365 还为身处同一个组织内部的两位最终用户提供了使用 Outlook、Outlook Web App (OWA)，或 Exchange ActiveSync (EAS) 客户端撰写、加密、解密、读取电子邮件，以及为电子邮件添加数字签名的能力。

使用 S/MIME 加密的电子邮件只能用邮件收件人的私钥解密。因此如果邮件在传输或存储后被拦截，除了邮件收件人之外的任何人均无法解密邮件中包含的信息。

反恶意软件/反垃圾邮件控制

您还可以配置服务中的反恶意软件/反垃圾邮件控制。您可以选择性地使用自己的反恶意软件服务，通过第三方服务队 Office 365 收发的内容进行双向中转。Office 365 会使用多引擎反恶意软件扫描技术扫描入站、出站，以及内部收发的邮件，防范通过电子邮件传播的恶意软件。

您的管理员可以使用 Office 365 管理中心管理反恶意软件/反垃圾邮件控制，包括高级垃圾邮件选项和针对整个组织应用的安全和拦截发件人列表。每个用户可以在自己的 Microsoft Outlook 或 Microsoft Outlook Web App 收件箱中管理自己的安全和拦截发件人列表。

内容控制和多引擎恶意软件扫描技术还有助于消除文档中包含的恶意代码。根据文件名扩展，Office 365 可以阻止用户通过服务上传或接收某些可能包含恶意代码的文件类型。Office 365 会使用智能即时消息筛选器 (IIMF) 保护服务和您的网络防范通过即时消息软件传播的恶意软件和垃圾信息。

传输层安全

您可以设置到受信任合作伙伴的 SMTP 连接，并使用传输层安全(TLS)协商确保连接的安全。这样的连接器可设置为使用 Opportunistic TLS 或强制 TLS 发送邮件。

如果一家公司需要向业务合作伙伴发送电子邮件，通过加密的 SMTP 通道发送，可以防止邮件数据因为中间人攻击而外泄。

保护最终用户的访问

Office 365 的数据和服务在数据中心、网络、逻辑、存储，以及传输层面的安全性都是有保障的。但用户需要能对数据的访问和使用方式进行控制。在 Office 365 服务中，可以使用 Azure Active Directory 作为底层身份平台。这样您的租户就可以通过强大的身份验证选项，更为细化地控制 IT 专业人员和用户访问和使用服务的方式。Office 365 还能与内部部署的 Active Directory 或其他目录仓库以及身份系统，例如 Active Directory Federation Services (ADFS) 或第三方安全令牌系统 (STS) 进行集成，让服务获得安全的，基于令牌的身份验证。

联合身份和单一登录的安全设置

您的管理员可以将内部部署的 Active Directory 或其他目录仓库与 Azure Active Directory 联合在一起。配置联合后，所有身份基于联合域的 Office 365 用户就可以在 Office 365 的身份验证过程中使用现有的企业登

录凭据。通过联合可实现安全的，基于令牌的身份验证。这样也可以让管理员创建额外的身份验证机制，例如：

- 基于客户端的访问控制，可以让组织控制用户使用不同设备或在不同位置如何访问信息，或将这两者结合在一起（例如对通过公用计算机，或公众 Wi-Fi 热点进行的访问进行限制）
- 基于角色的访问控制 (RBAC)，与上文“自动化操作”一节所描述的数据中心访问控制规程类似

借助即时信息的联合，Skype for Business Online 用户可以在一个高度安全的环境中，与其他组织中同样使用 Skype for Business Online、内部部署的 Skype for Business Server 2010，甚至 Skype 公众 IM 网络的用户进行即时信息交流。所有联合通讯的 IM 系统都会使用访问代理服务器进行加密。此外 Skype for Business Online 还可以让管理员保存即时信息对话内容。

隐私设计

当您将自己的客户数据托付给 Office 365 后，客户数据的所有者不会有任何变化：对于存储在 Office 365 中的客户数据，您依然具备相应的权利、资格，以及利益。

我们正是通过这种清晰的原则确保能够保护您的隐私，并且会在运营在线服务的过程中坚持下列几项重要原则：

- 除了为您提供所购买的服务，我们不会出于广告或任何其他用途挖掘您的客户数据。
- 如果您任何时候选择停用服务，可以随时带走自己的完整数据。
- 我们会告诉您客户数据的存储位置，以及何人在何种情况下可以访问。
- 对您客户数据的访问会受到严格限制，这样的访问不会破坏您的客户数据，并会被记录和审计。

此外，我们的隐私控制可供您精确配置谁能访问您组织中的什么信息。严格的控制和设计元素可以防止您的客户数据与使用 Office 365 的其他组织的数据混合在一起，并防止 Office 365 数据中心的人员访问您的客户数据。

客户的隐私控制

除了服务级别的功能，Office 365 可以让您使用透明的策略和强大的工具进行协作，同时依然能对信息的共享进行清晰的控制。

- **Office 365 中的权限管理**—可以让个人和管理员对文档、工作簿，以及演示文稿设置访问权限。这样即可应用智能策略，防止敏感信息被未经授权人员打印、转发，或复制。
- **适用于网站、文档库，以及文件夹的隐私控制**—作为 Office 365 的重要组件服务，SharePoint Online 提供的协作功能具备诸多隐私控制。例如 SharePoint Online 网站默认被设置为“私密”。另一个例子是，在用户明确设置权限以及要共享给的人身份前，上传至 OneDrive for Business 的文档是不被共享的。
- **适用于通讯的隐私控制**—在 Office 365 中另一个提供实时通讯功能的重要组件服务 Skype for Business Online 中，除了有各种管理员级别的控制外，还有很多用户级别的控制，可以启用或阻止与外部用户和组织的通讯。例如阻止对 Skype for Business 联合功能的访问。类似的，整个服务中都有这样的控制，可供管理员和用户保障自己内容和通讯的隐私。

服务合规性

全球云基础结构的运营需要满足合规性义务并通过第三方的审计。可审计的需求来自政府和行业的指令、内部策略，以及行业最佳实践。持续合规是指我们对 Office 365 的控制不断进行完善，符合最新 IT 标准和监管要求的承诺。

因此 Office 365 获得了包括 ISO/IEC 27001 在内的独立验证。为了帮助无需受制于相关法或控制的客户满足这些标准，Office 365 扩展了所实施的控制。

ISO/IEC 27001

Office 365 的服务可满足 ISO/IEC 27001 标准，同时也是第一个在物理、逻辑、过程，以及管理控制等方面，实施了一整套严格的全球标准的大型主流业务生产力公有云服务。

信息系统安全等级保护定级 (DJCP)

根据《GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南》，公安部授权的测评机构依据《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》对由世纪互联运营的 Office 365 进行测评，信息安全保护等级均被评定为第三级，并且获得备案证明。

可信云服务认证

在由数据中心联盟发起的第四批可信云服务认证评选中，世纪互联运营的 Office 365 在线应用服务获得企业级电子邮件 (Exchange Online)、 文件共享 (SharePoint Online)、共享日历与视频电话会议 (Skype for Business) 3 项可信云服务认证。在第五批可信云服务认证评选中，世纪互联运营的 Office 365 在线应用服务获得企业级电子邮件 (Exchange Online)、文件共享 (SharePoint Online)、共享日历与视频电话会议 (Skype for Business) 新增的“安全性、用户体验性能” 2 项指标的认证。

在 2015 可信云服务大会上，由世纪互联运营的 Office 365 云服务还获得了“可信云 2014-2015 年度行业云服务奖”的办公应用奖，进一步印证了 Office 365 拥有业内一流可靠的技术、安全稳定的运维以及完善规范的服务体系。

测试结果发布于可信云服务认证网站。

客户的合规性控制

通过 Office 365，我们提供了一系列合规性功能，包括数据防丢失 (DLP)、电子数据展示，以及审计和报表功能。提供的这些功能并未影响用户体验和生产力，因此获得了出色的用户接受度。

数据防丢失 (DLP)

虽然恶意软件和针对性攻击会导致数据外泄，但对大部分组织来说，用户的人为错误往往是数据外泄更主要的原因。Exchange Online 提供的数据防丢失 (DLP) 技术可以识别、监视、保护敏感数据，帮助用户了解并控制数据风险。例如，DLP 可以主动发现电子邮件中的敏感信息，例如社会安全号或信用卡号，并在用户发出邮件之前，通过“策略提示”通知用户。您的管理员可以为自己的组织完整控制并定制限制的级别。例如，可以只在发送前提醒用户邮件中包含敏感数据—若要发送敏感数据可能需要进行授权，或者用户可能被彻底禁止发送这样的数据。DLP 功能可以扫描电子邮件正文和附件，您的管理员可以通过完善的报表了解谁发送过哪些数据。

此外您可能会遇到这样的场景：组织中的某人会在日常工作中处理各种类型的敏感信息。文档指纹功能使您可以识别整个组织中所用敏感信息的标准格式，轻松保护这些信息。

不远的未来，这种数据防丢失功能通过扩展还可应用与 SharePoint Online 等其他服务。

审计和保留策略

使用 Office 365 审计策略，您的用户可以记录事件，包括邮件信息、文档、任务列表、问题列表、讨论组，以及日历等内容的查看、编辑、删除。当按照信息管理策略的需要启用审计功能后，管理员可以查看审计数据，并对当前使用情况进行汇总。管理员可以使用这些报表确定组织内部的信息是如何使用的，并可管理合规性，调查需要关注的领域。

出于业务、法律，或制度等原因，您可能需要保留组织内部用户收发的电子邮件信息，或者可能希望删除无需保留的电子邮件。Office 365 中名为邮件传递记录管理 (MRM) 的记录管理技术可以帮您控制用户收件箱中的内容需要保留多长时间，并可定义对于保存超过一定时间的内容所要采取的操作。

Office 365 中的 MRM 是通过使用 *ion tag* 和 *保留策略* 实现的。MRM 整体策略基于下列操作：

- 为默认文件夹，例如收件箱和已删除邮件分配 *保留策略标记*。
- 为邮箱应用 *默认策略标记*，以管理所有未添加标记内容的保留。
- 允许用户为自定义文件夹和个别项目分配 *个人标记*。

用户的收件箱管理和归档操作可以使用不同的 MRM 功能。用户无需按照保留要求对受管文件夹中的邮件进行归档。个别邮件可以设置与所在文件夹所应用的标记完全不同的保留标记。

电子数据展示

新增的电子数据展示中心简单易用，可以委派给专门的用户—例如合规性负责人，或人力资源专员—他们可以在无需求助 IT 部门的情况下轻松完成电子数据展示任务。通过使用电子数据展示，合规性负责人可以跨越 Exchange Online、SharePoint Online，以及 Skype for Business Online，轻松获取各种内容。通过集成式的 Office 365 电子数据展示，您可以通过一个位置搜索并保留电子邮件、文档，以及网站收件箱。您可以指定要搜索和保留的内容。由于可以只差找需要的内容，不会显示无用数据，数据展示工作的成本可大幅降低。电子数据展示过程并不会增加用户保留和搜索数据的负担，因为所有这些过程都是在后台执行的。

数据溢出管理

如果您的组织需要管理数据“溢出 (spillage)”，也可以通过 Office 365 的合规性功能获得支持。例如，如果联邦政府机构有可能需要将机密数据存入 Office 365，组织可以通过多种方式自行移除这些数据。具备相应 RBAC 特权的合规性或安全负责人可以使用电子数据展示功能搜索邮件或文档，并对其执行硬删除。用于存储“溢出”数据的硬盘绝对不会重新用于其他用途或进行修理，也不会离开 Office 365 数据中心的物理安全边界范围。如果 Office 365 基础结构不在使用这样的硬盘，这些硬盘会被彻底销毁。

数据删除

客户数据的隐私是我们对云服务的重要承诺之一。对于 Office 365，一旦服务合约终止或到期，我们会为您的管理员提供 90 天的时间（协议另有规定除外），供您确认所有数据迁移工作均已完成，随后您的数据会以无法恢复的方式彻底销毁。此外如果需要，我们会为您的管理员提供指南，帮助他们自行销毁数据。您可以执行电子化搜寻操作以确认所有数据均无法恢复。

结论

今天的企业需要能够帮助用户随时随地顺利完成工作的生产力服务，同时面对日益进化的威胁，需要维持足够的安全性。Office 365 高度安全的云生产力平台可以同时满足这些要求。若要了解有关 Office 365 安全、隐私、合规、透明，以及服务连续性等方面的更多信息，请访问 信任中心。从应用程序的开发到物理数据中心，再到最终用户的访问，Office 365 平台的每个层面都融入了完善的安全保护。今天，能够以合理的成本在内部部署环境中维持类似程度安全保护的组织已经越来越少了。

重要的是，Office 365 应用程序提供的内建安全功能可以简化数据保护过程，并能让管理员根据独特的业务需求，对安全保护进行灵活的配置、管理和集成。选择 Office 365，意味着企业获得了一个真正懂得自己业务安全需求的合作伙伴，这个合作伙伴已经得到几乎每个行业和每个地区不同规模企业的信任。