SearchSecurity.com.cn

技术手册

数据安全和云

- ☆ 探索云数据安全
- ☆ 准备迎接风险管理挑战
- ☆ 云计算的风险和优势
- ☆ 如何准备实施云计算的网络
- ☆ 在实施云计算后维护安全

TechTarget
TT中国

数据安全和云

目 录

探索云数据安全

当决定是否采用云服务提供商时，围绕合规性和安全性的问题成为必须考虑的因素。

企业被令人担忧的不断增长的合规要求所包围，从 SOX 法案、PCI DSS 标准到 HIPAA 法案/HITECH 法案（Health Information Technology for Economic and Clinical Health ）以及联邦贸易委员会（ FTC ）的红旗准则（ Red Flags Rules ）。同时，随着可供选择的云服务提供商的数量不断增长，企业有许多的选择权，当然有关云计算合规遵从也有许多需要考虑的问题。

尽管迁移服务到云上可能会有很多好处，但这也没有免除企业的某些责任。值得注意的是，企业仍然被要求遵从各式各样的合规和法律，似乎服务仍然位于公司的内部。

尽管迁移服务到云上可能会有很多好处，但这也没有免除企业的某些责任。值得注意的是，企业仍然被要求遵从各式各样的合规和法律。

在一些情形下，正如 PCI DSS 标准那样，有一个明显的趋势是通过外包某些服务来减少公司的合规遵从范围。值得注意的是，通过大规模地外包信用卡处理流

程给某个第三方提供商，公司的 PCI 范围会显著地缩小（尽管没有完全地消失）。不过，联邦贸易委员会的红旗规则情况不是这样，因为联盟贸易委员会强制要求任何外包的服务必须保持和企业内部实施情形下同等或更好的安全水平。

当你开始评估迁移服务到云时，考虑几个云计算合规遵从的问题十分重要：

1. 迁移到云的数据是否会在任何合规或相关要求之下？这些数据包括如个人可识别信息（PII）、个人健康信息（PHI）或公司财务相关的信息。
2. 如果这些问题一的答案是肯定的话，那么它在哪些合规要求的管辖之下以及需要什么控制措施？
3. 云服务提供商是否真的能提供你组织数据所要求的认可的或等同的控制？
4. 云服务提供商是否有必要的策略、流程和规程来正确地维护这些控制？
5. 供应商是否具备恰当的灾备恢复和业务持续性过程来满足你的组织的业务需要？
6. 如果云服务提供商破产会发生什么？企业的数据会被当作提供商的资产卖给债权人或进行拍卖吗？
7. 如果我决定更换服务提供商，是否容易使用可用的格式导出我的数据？
8. 供应商是否愿意修改它默认的服务条款以便保证或者提供围绕第 3 至第 7 个问题的服务级别协议（SLA）？

最后一个问题特别重要，因为许多云服务提供商拒绝签署默认合同以外的内容。这样一来，就把他们排除在数据相关服务的潜在合规遵从服务商之外了。好几个合作要求，如最为人关注的 HIPAA/HITECH 法案及联盟贸易委员会的准则，特别要求企业必须和它的服务提供商签署合同要求恰当的控制、流程和规程来与每个合规的指导要求保持一致。

类似地，如果提供商无法满足第 3 至第 7 个问题，应该把它们从你组织的业务考虑列表上删掉。无法满足要求是个问题，特别当面对 PCI DSS 标准和 HIPAA/HITECH 法案时。这样一来，你会很快地发现可供选择的云服务提供商是有效的，至少在短期来看是这样。尽管有传闻好几个大型的云服务提供商致力于改造它们的系统来满足这些合规要求。在健康医疗面有少数的云服务提供商已经专门地建立应用来满足医疗行业的需要，但是我还没有看到对这些应用的任何安全性评估，从而可以判断它们的有效性。

在此期间，我推荐你给正在评估的提供商发送上述问题，就像你会为任何其它的外包项目发送信息请求（RFI）那样，选择满足你要求的最佳提供商。

如果没有一家能满足，评估移除或混淆相关数据的方法（例如在迁移数据到云之前对其进行哈希或者加密），从而让你的组织仍能从云获得业务回报。

（作者：David Mortman　译者：Odyssey）

准备迎接风险管理挑战

云计算改变了企业应用信息系统、以及如何达到安全风险管理和合规遵从的方式。

当信息安全规划经理辨认那些会影响企业安全策略的关键主题时，云计算无可争议地从中脱颖而出。

困难的经济环境确实有助于让云计算变得更有说服性。因为按需的资源是动态可扩展的和灵活的，这对于大型和小型的企业来说极具吸引力，且无疑会继续改变我们应用信息系统的方式。

对于每个努力保护组织的网络用户和数据的人来说，迁移到云计算会引起巨大的变化和挑战。合规要求最有可能会妨碍企业迁移它所有的数据和操作到云上，所以，事实上这个转变是额外的安全挑战，位于保护现有的网络基础设施之上。迁移到云上，要求数据和应用放置在已完善建有边界防御和物理访问控制的区域之外。随着不受到 HR 控制的用户数量的增加，如供应商、客户和合作伙伴，都

迁移到云上，要求数据和应用放置在已完善建有边界防御和物理访问控制的区域之外。

会通过基于 Web 的协作工具来访问你的数据。IT 管理员已经疲于确保访问公司网络的移动用户的安全，而云计算又是一个完全不同的规模。

对于我来说，关键的安全挑战之一，是如何对位于企业防火墙之外的员工、客户和合作伙伴进行有效地管理和执行访问控制。云计算把我们都变成远程的工作者，且按定义来说，云应用和数据都位于企业之外。这意味这你不能再依赖多层认证、防火墙和其它边界防护来为你完成工作。

从战略角度来看，管理这些挑战需要很多行动。必须评审和加强 HR 的安全策略以便他们来执行健全的用户管理生命周期。详细的身份和访问管理策略也必须到位，一个能充分利用联合的身份管理，一个能让用户跨自治的安全域安全地访问数据或系统的安排。我建议在你的企业应用内启用单点登录（SSO），并利用这个架构来简化云提供商服务的集成和实施。

云计算同样要求更加可靠的因特网连接，所以即使是微小的操作也会需要建立某种形式的冗余性，来确保数据和应用一直都可用。无论如何炒作，云服务仍然是十分不成熟的，有一些或其它形式的运行中断状况发生。有些可能很容易破产，它是一个处于脆弱的经济环境中的新兴行业。多个服务提供商会提供你更好的网络多样性和业务连续性，所以任何基于云的项目应该采用厂商中立的应用和数据架构。这包括以独立于云方式的备份，和一个独立的机器镜像。你需要尽可能地让这个转

变是简单的，或者有应变计划可以将操作回撤到内部运行的云环境。尽管云计算可能会减少一定的连续性问题，但它永远不会消除行之有效的业务连续性计划的需要。

在不久的将来，基于云的服务和云计算技术会经历激增且长时期的攻击，因为对于黑客和网络恐怖分子来说，它们是具有吸引力的目标。因此，建立一个数据加密策略并实施技术来支持它，是最佳的主动防护措施。被加密的数据本质上是受到

三个主要的风险管理挑战

1. 尽管云计算可能支配 IT 策略向前发展，安全经理还是需要关注其它领域。当然，和云计算紧密相连的是虚拟化技术。这个行业仍然奋力为虚拟化环境定义安全最佳实践，因为应用和数据从单独的服务器迁移到在线的网络上。跟踪事态发展在安全控制方面的发展是重要的，以及对这些系统的威胁。
2. 智能手机是网络环境外安全经理仍在致力于完全控制的另一方面，我们开始看到对移动设备有效的攻击，并且它们会变得更加流行。不会消耗完电池或 CPU 的安全软件会成为必不可少的部分。
3. 最后随着 VoIP 使用的增长，有组织的罪犯们会发起许多攻击。系统管理员需要更加关注 VoIP 隧道的安全，使用加密而不是修补服务的质量。

是的，安全是一份永远不会结束的工作。

——MICHAEL COBB

保护的，这也是为什么这么多法律和合规强制实行这个实践。加密也允许你区分角色和数据，当加密密钥控制访问你的数据时。

不断地，你会看到很多新的基于云的服务上线，许多为企业带来了可观的经济回报。一些无疑会改变长期建立的风险与回报关系。而且当评估转变为基于云服务的投资回报率（ROI）时，你会需要评审组织的业务策略和对于风险的态度。云计算正在改变信息系统，所以要确认考虑到，如何在任何新的业务流程中融入安全，从而使基础设施、数据和用户继续受到防护。

（作者：Michael Cobb　译者：Odyssey）

云计算服务的风险和好处

云提供即时商业利益的同时，风险不容忽视。

企业不久前，Eli Lilly 制药公司的一位研究人员需要快速分析大量数据。如果分析结果像他想的那样，那么该公司就会拥有一种举世无双的药品。

唯一的麻烦是，该研究人员需要 25 台服务器来处理这些庞大的数据，他知道这会花上三个月来申请投资。在一个产品延迟费用很高的行业中，Eli Lilly 公司前任全球安全经理 Adrian Seccombe 表示，该公司药品延迟费用为每秒 150 美元，可以想想三个月的等待将是多么的昂贵。

云计算的好处

Seccombe 继续讲道："该研究人员去找一个 IT 技术员，这个人一直在跟'云'打交道。他掏出信用卡，插进 Amazon 网络服务公司，一个小时之内就在云中启动了 25 台服务器并开始运行。"

随后两个人意识到服务器的建立方式是错误的，所以他们不得不停止运行并重新开始。第二次，他们花了 40 分钟启动服务器并让其运行。

Seccombe 说，"两小时之内他们就开始处理这些数据了。研究时间突然从三个月一下缩短到了两个小时。"

这件事情还没完。当他们意识到分析不能在他们回家之前完成的时候，他们能够做好准备，启动更多的服务器加速数据处理。"他们想把数据从云中带回去，因为他们担心数据在云那里过夜。"

他们完成了任务，需要支付 Amazon 公司 89 美元。如果按每小时 150 美元计算，三个月的等待会花费超过 10 亿美元。

他们完成了任务，需要支付 Amazon 公司 89 美元。如果按每小时 150 美元计算，三个月的等待会花费超过 10 亿美元。

云计算服务：权衡风险和便利

这个成本比较是令人难以置信的，它体现了云计算的绝对能力。但是对于 Seccombe 来说，这个例子也凸显了该模型的某些问题，突出了云计算的某些风险。

“他们用端对端的安全线路（公司——Amazon 云）把数据结果安全地遣送回公司。这样即安全又快速。”

就这样吗？他们如何证明 Amazon 云没有泄露他们的数据？他们只能相信 Amazon 的一面之词。

这只是云计算、软件服务（SaaS）以及新型联合模式（依靠公司分享他们的数字财产）出现后许多问题中的一个。

这是为什么 Seccombe 作为 Jericho 论坛的会员（该论坛是一个安全智囊团），一直跟别人一起工作的原因，他们想提出某种框架，以便描绘出云计算如何才能有效地、安全地进行。

这项该工作的结果是一个三维立方体，用图像方式描述了一些关键的安全决定，当公司要决定哪些任务可以交付给云、哪些任务应该严格管制、以及如何让这些不同的方法协同工作时可以参考这个图像。

过去六年中，Jericho 论坛一直在挑战信息安全的传统思想，并描述了一种“非边缘化(deperimeterized)”世界的具体要求。在他们的新思想中，固定和清晰的边界被企业的流动性和合作所代替。

两年前，Jericho 发布了合作导向架构(COA)指南，定义了系统如何在不影响安全的情况下进行协作。现在，它要进一步描述出云计算的安全要求。这个最新实践的结果为安全行业提出了某些挑战，但是也为那些具有真知灼见的人提供了有趣的机会去克服这些困难。

云的合作模式

该团队的主旨思想是：根据过程所需要的控制级别，云可以联合多种方法。

云合作模式看起来像 Rubik 的魔方立方体，立方体的每一边都有四个面，因此有八个独立的子立方体，代表不同的工作类型。

云合作模式看起来像 Rubik 的魔方立方体，立方体的每一边都有四个面，因此有八个独立的子立方体，代表不同的工作类型。

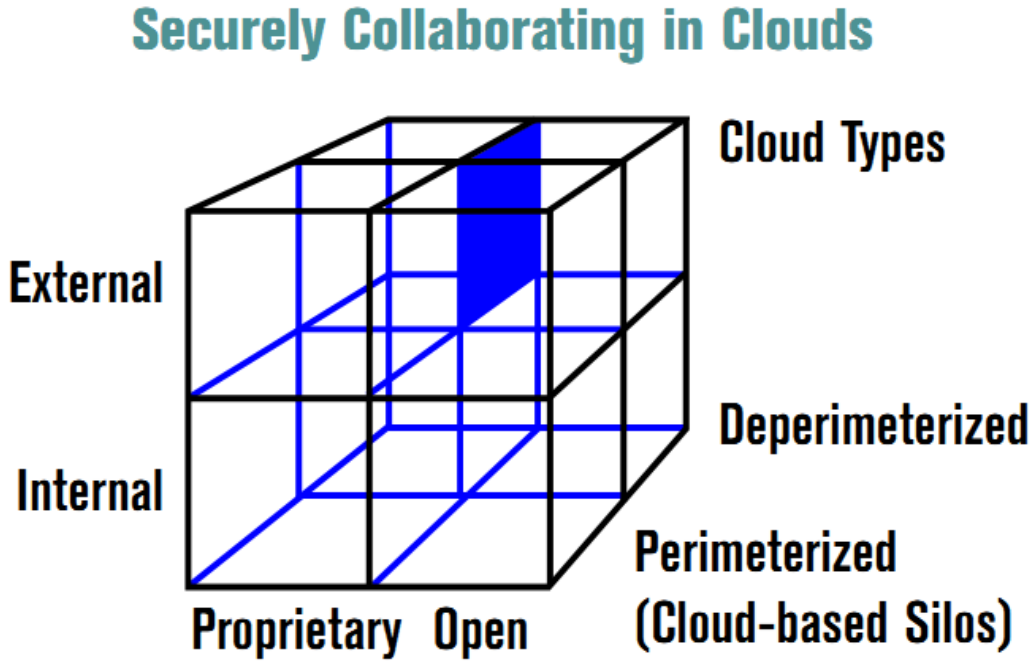
该立方体的长宽高分别是：

- 开放/专用（Open/proprietary ）
- 边缘化/非边缘化（ Perimeterized/deperimeterized ）

- 内部/外部（Internal/external）

该模式的目的是帮助公司对业务过程进行分类，并最终计划所需要的系统架构，以便充分利用云计算服务的好处。

“把云看成一个东西是一种错误，” Seccombe 表示。“你可以使用内部私有的边缘化云，你也可以使用外部的、开放的、非边缘化的云。”



图为云合作模式

“在 Eli Lilly 公司内部，我们要设法决定我们应该在什么地方进行哪些业务过程。比如，把某种药的材料集中在一起，我们可能不会用一个开放的、外部的、非边缘化的云。这更像专用的、边缘化的、内部云，虽然还是使用可能的云技术，但是我要进行更多的控制。”

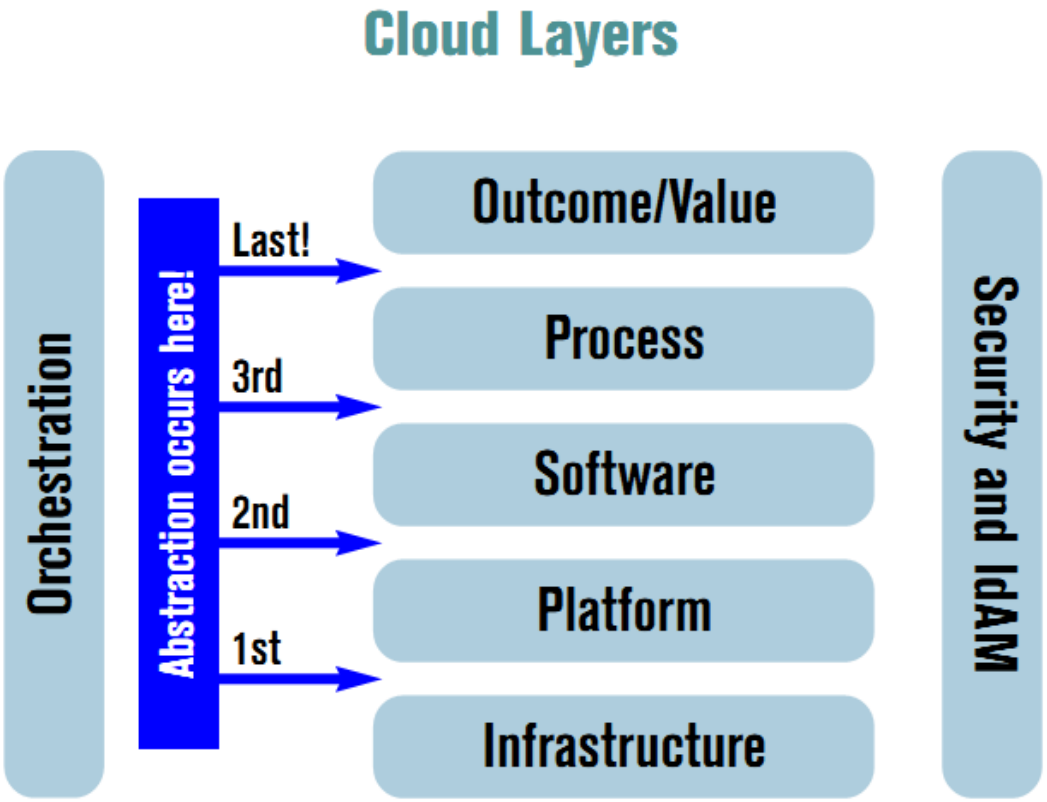
进展的关键是在各种子云之间建立有效的安全接口，以便云中的业务可以无缝对接，并建立必要的服务使之生效。

其中之一，举个例子，可以是独立的数据核查服务，云任务完成以后对返回的数据进行检查。“不是我们不相信 Amazon，这是一种责任的分离问题，”他说道，“你总不会希望审计人员为你提供这种服务吧。”

详细制作 Jericho 的“云层”

鉴于云有巨大的优势，现在的目标就是要看看你有多少工作可以安全地托付给云。

Jericho 设想了一系列可能存在的层，如下所示：



- 价值/成果（Value/Outcomes）
- 过程（Process）
- 软件（Software）
- 平台（Platform）
- 基础设施（Infrastructure ）

随着公司升级堆栈，并把他们的基础设施、平台、软件等等都委托给基于云的服务，他们会达到 Seccombe 描述的那种‘抽象’：“抽象意味着你不必关心任务发生了什么，因为别人正在帮你照看它，而且还是以一种负责任的方式照看。”

他承认，大多数云活动集中在基础设施和平台级别（Amazon 网络服务）或者使用软件（比如 Salesforce.com 或者 NetSuite 公司）上。但是他还引用了一个价值服务的例子，该例来自他的个人经历。

当他想买一块 BlackBerry 的电池时，他点击 Amazon 网站，发现了五个商店。他选了其中一个商店并下了订单，电池很快用 Amazon 的盒子送到。“Amazon 带给我购买电池的价值经历，但是我不记得我从哪家商店买的了。这是我的第一次价值服务经历。我单击一下鼠标，第二天电池就送到了。”

这个例子强调以客户为中心的计算，云中与日俱增的合作也支持这种计算。不仅仅购物是这样。

Seccombe 还列举了一个网站，有抱怨的人们可以在上面交换意见。对于一个药品公司来说，这种资源会有很多机会来获得患者的反馈，但是必须要有适当的控制措施才行。

那么问题就来了。云的确很有吸引力，但是如果没有合适的安全级别就开始与云打交道，会造成灾难。就像 Seccombe 所说的，你不能在出事后再稳固安全。“如果你进入了云，然后你的数据不见了。你就失去了控制，”他说，“这就是为什么我们要提前做这个的原因。”

云计算服务的未来

云计算对我们如何做 IT 工作会产生巨大的影响。即便是公司继续运行自己的系统，他们也可能在云上开发和测试应用程序，不会因为这个目的而购买自己的系统。

如果基于云的服务能够提供必要的备份却不需要前端成本，那么异地灾难恢复中心看起来就像是在浪费金钱。

但是服务要求更容易使用。Eli Lilly 公司的研究人员必须手动配置他们自己的服务器，不过在将来，新服务器可以根据命令自动投入生产，因此这种服务可以自动进行。

云会有更多的合作活动，因此身份和访问管理也呈现出新的重要性。这些合作活动可能非常短，只持续几分钟而不是几年。

“旧模式假设你环境中的每个人都是可信赖的，你在这种模式中建立一个活动目录，让这些

“旧模式假设你环境中的每个人都是可信赖的，你在这种模式中建立一个活动目录，让这些人使用你公司内部的资源。这种模式已经死亡或者濒临死亡。我们必须找到新的方法改变这种情况。”

人使用你公司内部的资源。这种模式已经死亡或者濒临死亡。我们必须找到新的方法改变这种情况，” Seccombe 表示。

政治和法规将会影响我们如何使用云。个人信息要受本地政府管辖，许多情况下存储在其他地方是非法的。就像 Seccombe 浏览 patients-likeus.com 这种网站时发现的那样，他无法处理信息、无法遵从规则，除非他们保证欧洲的病人信息只呆在欧洲。

他表示，这个问题可以这样解决：为数据添加一个元标记，定义它可以呆在哪里，如果数据跑到区域范围之外，这个元标记将强制数据自行毁灭。

（作者：RON CONDON　译者：Sean）

如何准备实施云计算的网络

将你目前的网络安全与云提供商的相融合，实现最平稳的过渡。

云计算代表着业务功能的巨大变化，对一个机构的 IT 基础设施来说更是如此。没有人能比网络管理者更能感受这种变化的影响了，因为他们的任务就是保证机构数据和网络用户的安全。

虽然共享数据、应用程序和 IT 基础设施可以在成本和生产效率上带来显著的优势，但是它们都只发生在企业防火墙和物理环境这一理想区域以外。作为一个网络管理者，你在云计算实现过程中的任务是，在把数据、应用程序和基础设施传输到云端之后，仍能确保用户和数据的安全。虽然云服务提供商需要为企业数据安全承担共同的责任，但最终企业安全的支持者（即网络管理者）要对此负责。在这篇文章中，我们将针对基础设施延伸进入云端的安全性问题，讨论如何构建企业网络。

作为一个网络管理者，你在云计算实现过程中的任务是，在把数据、应用程序和基础设施传输到云端之后，仍能确保用户和数据的安全。

在把任何数据或应用程序移动到云端之前，必须对内部网络安全现状进行评估。这是一个对网络进行检测的好时机，以此观察网络防护性能与你的数据策略（包括安全性、完整性和可用性）、法规要求以及行业最佳标准的匹配程度。

这种检测带来的好处很多。使用一个或多个免费商业网络检测工具肯定会发现实际情况比理想情况要更糟糕。一旦这些被更好的安全技术和改进程序所完善，那么就可以为网络及其它所承载的设备、用户和应用程序以及它所处理的流量确立一个合理的安全底线。在今后的检测和安全配置检查中可以参考这个底线，从而确定网络安全在转到云计算后会受到哪些影响。

其次，这也表明，理解云服务提供商的安全策略和程序是很重要的。关键是寻找一个既能够满足企业的安全要求，又能与防火墙防护能力相当的安全级别。为了避免混淆谁将对你数据安全的各个方面（如备份、访问和数据损坏）负责，我将根据合同，明确应该由哪一方来负责遵守相关政策或标准。

根据云服务的传输方式，防火墙的设置可能需要调整。为了确保包括周边防护（如 IDS / IPS 系统）在内的措施已经得到正确的调整，请与供应商紧密合作，因为供应商肯定具有处理各种可能的网络安全配置问题的经验。如果有必要，修改防火墙规则或者开放其他端口，必须确保每次进行这些改动都进行了另外一次网络检

测，从而更新网络安全底线。可以使用如 Nmap 这样的工具来检查，以确保只有合适的端口被开放，并且没有任何授权或连接违反了安全策略。

每当一项新的服务被添加到网络中，必须确保访问权限和职责的充分隔离，防止个人可能有意无意地损坏公司数据。对账户和人力资源雇佣登记的权限进行审查非常必要，这可以确保权限仍然适当，而那些不再使用的账户也已得到终止。作为云计算的一部分，如果你对第三方（如，供应商和客户）开放网络访问权限，那么任何网络接入控制（NAC）系统配置也必需重新检查。要确保当前 NAC 产品可以应付用户的急剧增加。实际上，许多机构仍在寻找基于 SaaS 的 NAC 解决方案，从而确保可扩展性和互操作性。

因为云计算的应用会在一定程度上消除静态数据和动态数据之间的差异，因此数据加密成为最重要的防护手段之一。

因为云计算的应用会在一定程度上消除静态数据和动态数据之间的差异，因此数据加密成为最重要的防护手段之一。本质上，加密的数据是受到保护的，因此即使受到其他服务的保护，所有的数据和通讯都将需要进行加密。此外，加密的数据不可读取，减轻了对云端数据损坏的一些担忧。数据加密还允许任务和数据的分离，

因为密钥控制着数据的访问。我可能会使用诸如 Wireshark 这样的分析软件对网络进行常规检查，从而确保通信信道正在被加密。

最后，不要因为第一次开发实验内部云和混合云，而害怕测试网络的安全性。你可以采用与云计算供应商相同的方式来提供应用服务，而这只能在网络周边范围内进行，或用有限的、非关键任务的功能来测试云供应商的实力从而进行实验。我还建议你阅读云安全联盟发布的指南，这将有助于你了解云计算组织主要的关注领域。

然而，为云计算构建网络只是第一步。为了使云计算真正成功，你需要确保当你开始运行云服务时，你的安全底线仍然能够得到执行。你还需要适应和发展防御和安全技术，以便处理新的威胁。在下一篇文章中，我们将关注这些挑战。

（作者：Michael Cobb　译者：Sean）

在实施云计算后维护安全

在你完成迁移数据和应用到云之后真正的安全工作才刚刚开始。

你已经成功地把组织选择的应用和数据迁移到云上，并且每个人都说你完成了一项伟大的工作。但是你和我都知道，维护这些应用和数据的安全任务才刚刚开始。本文中，我将回顾在云计算实施完成，或者刚启动且运作后，有哪些技术和流程必须被启用，同时还需要进行监控和安全防护。

身份和访问管理（IAM）

云计算让我们成为了远程工作者，这使得身份和访问管理（IAM）成为云计算迁移后重要的挑战之一。对用户和用户访问来说，拥有健全的管理生命周期是很重要的，以便用户账户、凭证和访问权限总是相关的和保持最新的，包括当员工离职时的账户禁用。同时也要注意，启动一个 IAM 策略能充分利用联合的身份管理，这能让用户跨自治安全域来安全地访问数据或系统。

云计算让我们成为了远程工作者，这使得身份和访问管理（IAM）成为云计算迁移后重要的挑战之一。

更为具体的是，考虑为企业应用引入单点登录系统（SSO）并利用这个架构来简化云服务商的实施。如果你的用户已经习惯了 SSO，那么迁移到云上会显得更加无缝，并且使得跨多个不同类型的云服务管理信任关系不再那么繁琐。同样，会有记录的基线数据帮助你监控和估算由云活动所带来的变化。

一个 SSO 产品应该使用一个常见的标准来实施联合功能，例如安全断言标记语言（SAML）和自由联盟的身份联合框架（Identity Federation Framework、ID-FF）。这些标准将现有的访问及身份策略，从内部网络跨越防火墙延伸向外至云，同时仍然按照你的信息保护和数据分类策略，来强制实行恰当的认证强度。

带宽

云计算所带来的不断增长的因特网使用，同样增加了网络拥塞发生瓶颈的风险。基于 Web 的应用尤其对延迟敏感，如果网络繁忙，许多都会运行吃力。宕机或缓慢的处理阻碍员工工作，并且可能导致违反策略。例如，缓慢的文件或数据传送可能导致员工使用不安全甚至违反安全策略的备选方法。

这个问题的解决方法之一，是部署 WAN 优化产品，该产品通过提高应用流量管理和消除冗余的传输，来缓解企业网络上的应用流量。例如 Citrix 系统公司的 Citrix NstScaler 产品提供了 Web 应用防火墙的功能，并且通过 4 至 7 层的负载均衡融合了流量管理。其它 WAN 优化产品厂商包括 Riverbed 技术公司和 Blue Coat 系统公司。

防火墙

在内部网络和云之间的连接当然应该进行加密，在因特网上以明文的形式来回地发送任何敏感或者业务关键数据就像给攻击者发送邀请函来窃取数据一样。

在内部网络和云之间的连接当然应该进行加密，在因特网上以明文的形式来回地发送任何敏感或者业务关键数据就像给攻击者发送邀请函来窃取数据一样。作为一名网络工程师，确保网络设备能处理涉及到 SSL 加密通信的、大量消耗处理器能力的公钥加密算法。你可能需要在基础

设施中添加能处理所有 SSL 操作的 SSL 加速卡或者代理。然而单独加密不会阻止恶意软件和其它的网络攻击，因此，因此，重要的是要对防火墙进行升级来保护你的内部网络，这样防火墙就可以对 SSL 的流量进行审查。最理想的情况是加密与数据丢失防护产品一起工作，这样可以在执行相关政策的同时还可以对数据进行分类和监管。

审计

在实施完成云计算后另外一个重要的任务是对所有的安全策略进行审计以确保它们保持有效。同样也要审阅、更新和测试灾难恢复和业务持续性计划和流程。既然云计算基础设施是每天系统管理的一部分，所以过程以及更为重要的“人的角色”需要改变。公司内部的 IT 团队一定需要与云供应商紧密合作，这样可以在业务连续性计划中很好的理解另一方的责任，包括数据恢复的哪一方面应该由谁来处理。时刻为服务中断而做好准备，这会对严重安全事件起到缓解作用。

最后，不要把供应商服务品质协议 SLA 里的陈述看作是理所当然的。你需要检查，在商定的时间范围内供应商确实已经对系统进行了备份和修补。你应该要求拥有一份审计结果的副本，并且确保任何建议已经被落实。进行建设性的对话将使得解决双方的安全问题更加容易，所以要保持经常的联系，特别是在应用程序或者

系统更新的时候。这种沟通将有助于减少变化而对相关产业或者政府规定的服从所带来的不利影响。

（作者：Michael Cobb　译者：Odyssey）