云安全

云安全

云计算的概念越来越流行，而且云计算被认为是一种强大的商业模式，使用云计算，可以根据需要购买计算能力、磁盘存储、协作应用开发资源、客户关系管理（CRM），而且它非常灵活。但是采用云计算仍然存在很多的安全隐患和管理难题，例如确我们需要定没有把企业数据或者任何个人信息或其它机密信息至于风险之中。

云计算的安全问题

云计算被认为是一种强大的商业模式，使用云计算，可以根据需要购买计算能力、磁盘存储、协作应用开发资源、客户关系管理（CRM），而且它非常灵活。但是 Forrester 在《你的云有多安全？》（How secure is your cloud?）的报告中题诗考虑使用基于云的服务的公司需要明白云计算存在的安全问题。

- “云”究竟是什么
- 云计算的机遇与风险
- 云计算需要考虑的三个风险
- Forrester 建议谨慎采用云计算服务
- 云和虚拟化服务器向 PCI 提出挑战
- 2010 年云计算：请准备好迎接风险管理的挑战

云计算的安全优势

IT 行业进入云计算的一种方式是通过向内部用户提供的企业主导的 IT 人员控制的应用服务。这就让 IT 人员有能力监控使用模式并减少营业费用。应用服务的关键功能是向

终端用户发送适应的应用和桌面，而他们的性能和在本地安装的应用上所感受到的性能类似。

- 应用服务云可以推进安全性
- 云中的网络安全服务的优势
- Web 安全策略：使用云安全服务

云计算的安全防护

安全分析家和从业人员一般会说要使用云计算，但要谨慎行事。云计算会遇到与外包有关的敏感的公司数据所能遇到的所有风险。当你和第三方已知或未知的转包商交易时，特别是在全面范围内时，执行安全策略和遵从法规要求就很困难。再加上云模糊的特性以及非传统厂商进入这个市场，就更增加云的危险。

- 如何确保云计算的安全性
- 加密专家说云计算可以被保护
- 私有云：创建自己的云安全等级
- 为云计算的实施做好网络准备
- 实施云计算之后如何保证安全

云计算安全联盟

云安全联盟（Cloud Security Alliance）是一个非赢利性组织，成立于 4 月 21 日旧金山的 RSA 大会上。成立的目的是计划为采用云计算产品的公司提供安全建议，它会提出安全云计算的最佳实践并教育用户云计算如何保护其他的计算形式。然而如果他们想进行关于云计算的有深意的讨论并为计划采用云计算的企业提供有用的数据还需要克服很多困难。

- 安全云计算联盟成立
- 云计算联盟前路挑战重重
- 云计算安全团队报告安全难点

“云”究竟是什么

一家日志管理软件即服务厂家，AlertLogic 的创始人兼 CTO，Misha Govshteyn 最近在他的博客中写道，在 RSA2009 大会上有些厂家使用的云计算概念不太精确。

Govshteyn 指出 Netgear 使用“云”来描述他们的统一风险管理（unified threat management - UTM）产品线。Netgear 声称它有一个“云中复合安全架构”。终端安全厂家 Prevx 则用“云”来描述他们的终端代理使用了“云的能力”。

“这些是比较荒谬的例子，”Govshteyn 说。“云的真正意义在于把复杂的运算量从机房转移，而将其以服务形式提供。归根结底，云的核心是其性价比和简单性。”

连 IBM 也在偷换概念。蓝色巨人把它的新 WebSphere SOA 产品称为 WebSphere CloudBurst Appliance。它是安装在机房内的，这也没能阻止 IBM 将其称为 SOA Appliance，它在私有云中实施和管理 SOA。

和 Govshteyn 一样，其它的安全专家和业界观察家也认为云概念的不严格使用已经引起对它的真正含义的迷惑。

“我听很多最终客户说他们已经听厌了云这个名词，因为和供应商的每次对话都会谈到它。”Forrester Research 的高级研究员 Chenxi Wang 说道。“业界已经对又一个热门字眼感到厌倦了，但是云计算和云服务还是会存在的。

基于 Web 提供的服务是云的主要组成部分。在 Forrester 的最新报告中，Wang 描述了三种和云计算相关的市场：应用部件即服务，软件平台即服务，以及虚拟基础架构即服务。

应用部件即服务市场包括基于 Web 的 email，以及其他由提供商所有的社交网络应用。Google 的基于 Web 的文字处理和电子表格软件就属于这一市场。

Salesforce.com 和其他通过 Web 出售软件的厂家则可归为软件平台即服务这一市场类别。据 Wang 的观点，微软的 Azure 服务平台和 Amazon 的 S3 数据存储服务也属于这一市场。

最后的第三个基于云的服务市场包括虚拟基础架构即服务市场。这一领域包括传统的外包服务，例如当公司在远程数据中心中托管 Web 服务器，而服务提供商提供维护和升级服务。

对不同的公司来说，对云的真正组成的完全理解也有所差异。Wang 说，实际上，有些公司可能还没有意识到他们的一个小部门已经在一个特定的业务流程中使用了云计算。

Wang 说："有些才刚刚开始试水，而这些公司通常不太精通于其优势和风险，甚至其功能"。

连国家技术标准局（National Institute of Standards in Technology - NIST）也在权衡一个官方的定义。在 4 月发布的讨论稿定义中，NIST 说云计算是一个"演化的范例"。他们将这个名词细化为五种关键特点，三种交付方式和四种实施模型。

"云计算是一种可用的、方便的、按需的对一个共享的可配置计算资源池的网络访问的按次付费模型，这些资源可以包括网络、服务器、存储、应用和服务，可以快速实施并投入使用，而需要极少的管理工作或服务提供商的介入，"NIST 说道。

Cloud Security Alliance（云安全协会，一个非盈利组织）的安全顾问和主管，Jim Reavis 正在寻求使云服务更安全的办法，他说"云"这个概念应该被简化以便普通用户的理解。

"在我看来，云计算就是将按需使用的信息技术以订阅服务的形式提供给用户，"Reavis 说。"客户则不知道这些共享的资源的内部运行机理。

据 AlertLogic 的 Govshteyn 所说，如果客户不知道共享资源的内部机理，他们可能就不应该在意云的定义。

"理解云的定义和如何做出购买决定没有必然联系。"Govshteyn 说。

（作者：ROBERT WESTERVELT　译者：李博文 来源：TechTarget中国）

云计算的机遇与风险

不久前，Eli Lilly 制药公司的研究员需要快速地分析大量数据。如果结果能证明他的想法，该公司可能会产生出一种世界一流的药物。

唯一的麻烦是，研究人员将需要 25 个服务器以应对大量的数据，他知道这可能需要长达 3 个月才能使这一投资获得批准。在一个由于产品拖延上市而带来约每秒 150 美元损失的公司，三个月的等待确实是非常的昂贵。

Adrian Seccombe 是这家公司安全部门的全球领导，他解释说：“他找到一位长期以来一直从事云计算业务的 IT 人员，这位 IT 人员能够用信用卡向 Amazon 支付费用，以开动 25 台服务器运行一小时。”

然后，他们意识到他们没有正确地建立服务器，所以不得不考虑关闭然后重启。他们花了 40 分钟，使服务器启动并运行。

“在两个小时内他们处理了数据。这项研究所花的时间从 3 个月突然之间减少到两个小时 ”， Seccombe 说。

事情还没完。当研究人员发现以现在的速度在下班之前不能完成对数据的分析时，他们可以增加他们的权限，使用更多的服务器加快处理这些数据。“他们希望得将云中的数据取回来，因为他们觉得将数据留在云中过夜不太合适。”

他们完成了任务，并向 Amazon 支付了 89 美元。然而，以每秒 150 美元的损失计算，3 个月的等待成本将超过 10 亿美元。

成本的比较是令人难以置信的，体现了云计算这一概念的强大力量。但是，对于 Seccombe，这一事例也反映出这一模式的一些问题。

“他们取回了数据结果，并且是在 Amazon 端到端的安全线之上进行的。这是安全和快速的。 ”

如果事实不是这样呢？他们怎么能够证明没有在 Amazon 的云中留下他们的数据的任何痕迹？ 他们不得不接收亚马逊的说辞。

随着云计算、SaaS 和新的基于公司之间共享数字资产的协作模式的到来，这只是其中一个问题。

这就是为什么 Seccombe， 作为 Jericho Forum 的成员，最近一直致力于与该组织的其他成员合作推出一些框架，以说明如何有效安全的进行工作。Jericho Forum 是一个安全方面的智囊团。

这项工作的结果是一个三维立方体，预计在 3 月份正式推出，试图以图形的形式描绘出关键决策，公司需要做出这些决策，以决定哪项工作交给云计算可以安全地完成，哪项工作须在保密状态下完成，及如何让不同的完成方式相互协调。

过去五年 Jericho 论坛已对传统的信息安全思想做出了挑战，规划出了没有防线的世界的要求，这一世界中移动和合作代替了企业之间原有的硬性边界。

去年，Jericho 发布了合作导向的架构，这一架构定义系统如何共同努力，同时又不损害安全。现在正在进一步筹划云计算的安全要求。这一最新工作的结果向安全产业发起了挑战，但也为具有眼光的聪明人士描绘了一些有趣的机会。

这一组织的主要信息是，根据企业对整个过程的控制要求，利用云计算可以实现多种方式的合作。

云协作模型看起来像魔方，每面有四个图，因而分割为代表不同类型工作的八个小立方体。

魔方的三个维度分别是：

- 开放（open）/专有产权(proprietary)
- 有边界限制（Perimeterized）/ 无边界限制（deperimeterized ）
- 内部（Internal）/外部（external）

该模型的目的是帮助企业对他们的业务流程进行分类，并最终选定他们需要推进的系统架构。

“将云视为一件事物是一个错误”，Seccombe 说，“你可以把内部的、专有产权、有边界限制的云，也可以有外部的、开放的、没有边界限制的云。

他说：“在 Eli Lilly 公司，我们正在确定在什么地方开展哪种业务流程。例如，收集药品的成分的工作不会放在一个开放的、没有边界限制的云中。而是可能放在一个内部的、专有产权、有边界限制的云中，仍然会使用云技术，但我需要对这一流程施加更多的控制。”

展望未来，关键是在各种各样的子云之间建立有效和安全的接口，以使部署在云中的业务可以无缝连接，并创造必要的服务做到这一点。

比如，检查在云中完成计算的任务返回的所有数据可以成为一种独立的服务。“这并不是说我们不信任 Amazon，但它是一个职责分离的问题”，他说。“你不想正在为你提供服务的人员同时又审计员。”

在云中开展工作

鉴于在云中开展工作的巨大的优势，现在的目标是看您可以放心地将多少工作整个委托给云。

Jericho 预计如下一系列工作具有这种的潜力：

- 价值/成果
- 进程

- 软件
- 平台
- 基础设施

当公司提升到这一层次，并将基础设施、平台、软件等委托给基于云的服务时，他们可以做到 Seccombe 所描述的“抽象”：“抽象意味着你并不在乎具体是怎么回事，因为有人为你照顾这些事情，并会以负责的态度处理问题。”

他承认，大多数云活动在基础设施和平台的水平（如亚马逊网络服务），或与软件合作（如 Salesforce 或 NetSuite）。 但他引用了一个来自个人的经验的例子：Value-as-a-service。

当为他的黑莓手机寻找一个新电池时，他点击了亚马逊网站，亚马逊网站给出了五个出售电池的商店。 他选择了一间店铺并下了定单，电池很快用亚马逊的包装盒送到。“亚马逊带给了我得到电池过程中的价值体验，但是我不记得是从哪家商店买的。这是我第一次经历价值作为一项服务。我只有一次点击，并于第二天获得了电池。”

这一例子突显了云中的合作增进了以客户为中心的计算支持。这不仅仅用于购物。

Seccombe 列举了 www.patientlikeus.com 网站，有各种投诉人们可以相互比较别人留下的投诉。对于一个制药公司，一些同类的设施可以用来收集病人的反馈意见，只要有合适的控制措施。

当然，还有最难哨的骨头。云是非常有吸引力，但在没有正确的安全级别时，进入云中将导致灾难。正如 Seccombe 所说，你不能在发生安全事件之后再提安全措施。“如果你天真地进入云中，然后你丢失了数据。你也就失去了对数据控制，”他说。“这就是为什么我们正在努力将这些工作在前期做好。”

下一步如何？

云计算可能会对我们如何做 IT 产生巨大的影响。即使公司将继续在内部运行自己的系统，他们也应在云中开发和测试应用系统，而不是有意购买他们独占的系统。

云为基础的服务提供必要的备份而不需巨额的前期费用时，异地灾难恢复中心也将开始变成浪费金钱的行力。

但是，服务必须更容易使用。 例如， Eli Lilly 公司的研究人员现在必须手动配置服务器，但在未来，这种服务会由顺序而来的应对这一需求的服务自动完成。

当在云中发生的合作增多，且合作的持续时间可能很短（几分钟，而不是几年）时，身份验证和访问管理重要性将会提升。

“旧模式中假定在你的关系网中的每一个人都是值得信赖的，你为这些用户建立一个 Active Directory 方便他们使用本组织内的资源，这种模式已经死亡或是正在死亡。我们必须找到一种方式设法改变它”，Seccombe 说。

（作者： Ron Condon 译者：陈志辉 来源：TechTarget中国）

云计算需要考虑的三个风险

“云”过去常被用于对各类基于 Web 应用的通称。现在它普遍用于指网格或实用新型计算模式，在这点上它取代了本地硬件和存储器输入/输出。企业正在纷纷向云这个方向发展，只是一些企业比另一些发展的要快。然而，转向云这个方向使企业面临许多需要去考虑的风险。这些风险的核心，是许多云/ Web 2.0 的供应商无力满足法律与规章的要求。以下是三大主要风险：

1．安全：对于许多企业来说，信息的安全性是最主要的风险。这或许是受到了保护知识产权、商业秘密、个人可识别信息或其他敏感信息这些需要的驱动。要使这些敏感信息在互联网上可用，就需要在安全控制以及内容访问和信息途径的监测上有重大的投资。一些供应商提供的日志记录和审计控制还不能像企业内部及企业应用程序所提供的日志记录一样健全。在这个方向上的困难是，要确保在事故发生后，企业能够知道是谁访问了文件以及可能对文件所做的操作是什么（如编辑，下载，更改访问等）。

2．电子化搜寻（E-discovery）：电子化搜寻当前的趋势大多是假设企业已经明确知道它的信息存储在哪里，这些信息如何备份，以及如何保护。这些规则也假设企业能够实际地检查存储设备，并且在必要时，能够检查存储介质来获取擦除及/或删除文件的证据。在云环境中，企业可能很少或者根本不知道存储和备份的过程，也很少或根本不会亲自去访问存储设备。而且，由于来自多个客户的数据可能存储在单个存储库中，对存储介质的取证检查以及对文件存取和删除的正确认识将是一个重大的挑战。

3．计算机取证（Computer forensics）：对许多企业来说，计算机取证是电子化搜寻和内部调查的关键组成部分，而且经常需要实际地访问存储设备或计算资源。从计算机操作系统存储在物理和易失性存储器里的信息中，我们可以了解到很多东西：存储在计算机的随机存取存储器中的信息在关闭计算机后几乎会立即消失。当数据和应用程序脱离本地个人计算机时，取证调查人员可能就不能再访问某个案例的关键信息。一个特定的文件或此文件最后被访问时的地点，通常在决定该文件如何被使用以及被谁访问时起着关键性的作用。假设数据存储转移到云，而数据又没有完全消除的话，那么获得未受污染的证据数据副本的能力可能会降低。

预先准备

虽然这些问题可能不会是云环境中移动数据存储和应用的绝对障碍，但它们已明显妨碍了工作的正常运行，这导致企业需要认真审查其合同义务、风险预测、安全基础设施和监督能力。企业应该准备好向供应商提出适用于自己商业需要以及存储和交易信息种类方面详细的安全和法律要求。

今天的一个主要挑战是，几乎不存在涉及到在云环境中存储信息的法案（case law）。企业必须采取措施来依法保护知识产权和信息的安全。由于这一领域缺乏相关的判例法，法律部门也可能会担心云环境中知识产权，商业秘密和合法的特权信息（privileges information）。在任何情况下，企业必须保证将其安全和法律规定作为合同的一部分，并进行定期审计，从而确保供应商能够满足这些要求。

（作者： Patrick Cunningham 译者：Sean 来源：TechTarget中国）

Forrester 建议谨慎采用云计算服务

Forrester Research Inc.发布了新的报告，督促企业在检查基于云的服务时要小心警惕。早期的采用者遇到了一些路障，包括不知道他们数据的位置、当做出决定更换服务的时候数据上的活动以及服务提供商保护客户隐私的方式。

据 Forrester 发布的名为《你的云有多安全？》（How secure is your cloud?）的报告称，考虑使用基于云的服务的公司需要在和服务提供商签合同前清楚地明白安全、隐私和法律后果。这份报告敦促企业制订数据安全和法规优先顺序检查表，并比较企业需求和云服务提供商的策略和程序。

报告的作者 Forrester 的首席分析师 Chenxi Wang 说：“凭经验，当你把内部开发的需求外包的时候，厂商笔记至少和要你一样安全。”

公司必须理解法规问题的影响、服务提供商处理数据安全的方式以及公司的知识产权是否存在风险。在很多情况下，合同应该详细地列出灾难准备程序、适合的数据处理和泄露事件中服务提供商的角色。

Wang 说：“还要特别注意云服务中部明显的操作细节，例如数据位置、事件日志、复制方式以及架构。”

Wang 称，很多公司都在转向云服务，来降低成本，提高效率。Forrester 最近关于企业和中小型业务的调查发现，47%的软件决策者在 2009 年没有使用或者没有考虑使用 SaaS。

据 Wang 所说，云计算经常会使数据安全和隐私变得复杂。企业失去了可见性和控制，因为公司数据可能存在于其他网络上。Wang 说，有些公司中有的员工在没有 IT 安全的同意前就使用云服务。

“在很多情况下，不通过 IT 或者其它集中权威的参与而设置一项服务很简单。在很多情况下客户就可能出现在某人的桌面上，但是内容的位置是在企业之外。”

在最近的采访中，Eastman Kodak Co.的 CISO，Bruce Jones 说他的公司正在考虑在某些进程上使用云服务，但是他补充说，他的公司很谨慎，担心公司数据会有风险。

Jones 说：“总是有人问我‘我们可以把这个移到云中吗’，在这一点上我很难处理。我没有发现巨大的利益。”

Jones 说 Kodak 的研究和开发部门的计算程序在云计算中可能存在价值。他说，公司有时在按需计算能力上需要高性能来执行大型的计算。

“云可能在这时候提供一些好处，但是我想要确定我们没有霸 IP 数据或者任何个人信息或其它机密信息至于风险之中。”

Wang 说，对云服务提供商的全面评估应该包括对它的审计，来获取内部操作的能见度。云提供商可能不会允许内部审计，但是他们应该提供“架构和网络的某种形式的外部审计。”目的是理解这项服务使用事件日志的方式以及谁可以访问后门的数据。

据 Wang 所说，法规问题也会阻碍云服务的采用。服务提供商的数据处理和业务连续性实践也应该在法规问题的解决中考虑。另外，公司应该主动记住他们行业内的特殊法规。

Wang 建议客户谨慎地仔细检查安全等级以及合同条款。尽管大部分是相当标准的，有些公司可能会在合同的某些条款上协商，使其仅针对企业的业务程序和数据处理的程序。Wang 说，在很多案例中，除非你是大型企业，云服务提供商不会特别华时间协商 SLA 或者合同条框。

她说：“如果你是小客户，他们就不会注意，但是如果是大型客户，他们就会为你拼命。这是他们工作的方式。”

Wang 说，合同中应该包括如果没有遵守 SLA 的后果、当服务合同到期时数据的处理防洪四、回归到公司的数据类型以及在指定的时间内云服务提供商应该把他们网络上的所有数据删除。

“我们发现有些公司被厂商的禁闭惹火了。更改服务不是很容易。如果正在更换，祝你好运，希望他们可以为你工作；如果合同没有要求为你扩展末端服务支持，那么他们就什么也不会做。”

(作者：Robert Westervelt 译者：Tina Guo 来源：TechTarget中国)

云和虚拟化服务器向 PCI 提出挑战

特别兴趣小组和新技术的研究都可以帮助支付卡行业安全标准委员会（PCI SSC）解决云中的支付卡数据的法规问题。

PCI SSC 有一个关于虚拟化安全的特别兴趣小组（SIG）。它的终极目标是什么？这个团队要考虑哪些问题呢？

Troy Leach：退后一步，我们有一个无线特别兴趣小组，一直在提交新的无线实施指导。它是一个现象文件，我迫不及待要把这些文件放在市场上。它为环境中含有无线的企业、正在做出变更的企业或者正在实施无线的企业都提供了指导。这是很强大的指导，我们希望可以在虚拟 SIG 中看到同样的效果。

我可以假定（虚拟化团队）将围绕虚拟服务器中的保管、规则和责任一系列问题。他们可能会讨论云计算。他们可能讨论虚拟本地网（VLAN）以及网络的虚拟分割是否合适等。它和我们上个月成立的另一个关于作用域（scoping）的 SIG 很相似。所以当谈到虚拟化的时候应该会有一些重叠。

关于作用域（scoping）的 SIG 只和虚拟化问题有关吗，还是和所有的网络分段问题有关呢？

Leach:都是关于作用域（scoping）的问题。这是由商家和特别组织以及他们呢想要如何覆盖这些话题来决定的。他们在分割和减少 PCI 评估的不同方面有着广泛的兴趣。

如果有人走过来对你他他们正在进行运计算，在这个标准中你能给他们指出他们要遵守规则给他们指导吗？

Leach:这是个较难的问题。我们有一种 RFP 所要求的新技术，可以探究这些问题，我们将会研究虚拟化中怎么应用。我们想要对这种技术保密，但是我们认识到有时不能发出一些要求。

我们确实有些挑战性的技术。我认为大部分人需要的技术之一是“服务器的主要功能”，以及虚拟化是否在这些操作系统内部创建了足够的分割，然后在每个服务器上实现这种功能。对于很多企业来说这都是很大的挑战。管理程序从一个操作系统转移到另一个操作系统上以及这种层面的杀毒软件是否合适中都存在一些新的工作。这种技术还存在很多挑战，我们希望在今年夏末可以出具一份关于 RFP 新技术的意见书。

在网络分段中存在哪些问题？

Leach:我认为很多厂家在分段的时候面对的第一个挑战就是他们不知道他们的持卡人数据存储在哪里。持卡人信息的发现阶段，特别是如果你不熟悉这种发现，就是一种挑战。作为前任首席技术官，我可以说有时我确实不知道市场团队是如何收集信息的，也不知道业务部是服务收集系统管理员和数据库管理所不知道的信息的。我们正在向这个方面努力。很多企业都认识到了安全的重要，并且需要进行一些实践，而不是一年一次的确认。

PIN Entry Device (PED)安全项目是正在扩大，将要包括 UPT 和 HSM。这两种新标准是什么？

Leach: PED 标准现在是一个群，我们有很多这些设备的标准，可以记录 PIN 交易。这个项目中和无人监看支付设备（unattended payment terminals，UPT）相关的部分关注这类设备的另外的安全要求，例如染料泵和电影售票厅。这些交易都是在没有出纳员的情况下完成的，我们认识到在这类设备上需要有附加的物理和逻辑的安全控制。

另外， 硬件安全模板（HSM）是在设备内部的。它管理设备处理 PIN 的方式。例如，它可以从设备上进入处理器或者 acquiring bank（接受信用卡转帐的银行）的时候加密 PIN。

如果我是个商人，而且我已经安装了这些设备，那么会发生什么呢？

Leach:这些要求和 PED 的要求类似。在这些要求中，这些设备的制造商有责任通过这些要求的验证。很多这些制造商都非常了解这些标准。他们也参与了审查这些标准。所以我们可以预料这些厂商将会很快在实验室中通过这些过程。

（作者：Robert Westervelt 译者：Tina Guo来源：TechTarget中国）

2010年云计算：请准备好迎接风险管理的挑战

随着信息安全项目经理开始新一年的工作，他们通常会找出那些能够影响企业安全策略的关键主题。

然而，毫无疑问有一个主题比其他主题都突出：云计算。艰难的经济环境确实令云计算很有说服力。因为按需（on-demand）资源是动态可扩展的以及动态灵活的；按需资源已经是2009年的热点了，它总是吸引着大型或者小型的企业。不管2010年的经济状态如何，云计算肯定会继续改变着我们的IT方式。

对于那些想要保护企业的网络用户和数据的人来说，往云计算转变将会是一个很大的改变和挑战。规则遵从最有可能阻止企业把所有的数据和操作都转向云，所以除了保护现有的网络基础设施以外，这个转变实际上是另一个在安全领域上的挑战。转向云计算意味着需要把数据以及应用程序都放在外围防御保护和物理访问控制之外，越来越多的用户将不受HR的控制，比如供应商、客户端以及合作伙伴等，人们将通过基于网络的协作工具来访问你的数据。IT管理员对于保护那些能够访问公司网络的移动用户的安全已经很头疼了，但是这一点对于云计算而言是一种完全不同的规模。

对我来说，关键的安全挑战之一是：怎样才能有效的管理和执行处于企业防火墙以外的员工、顾客以及合作伙伴的访问控制。云计算让我们都成了远程工作人员，而根据定义，云的应用程序和数据也处于企业的外部。这就意味着你不能再依靠那些多重认证技术、防火墙以及其他的外围防护措施了。

从战略上讲，管理这些挑战需要采取若干行动。HR的安全政策必须重新复查并且加强，以确保这些这些政策可以执行强有力的用户周期管理。你还必须有一个详细的身份识别以及访问管理策略，这个策略要能够充分利用联合的身份识别管理，它是一个能让用户通过自己的安全域安全地访问数据或者系统。我建议在你自己的企业应用程序中能够使用单点登录（SSO），并利用这个结构来简化云提供商的集成和实施。

云计算将更多的依赖于互联网连接，因此，就算是比较小的操作也需要建立某种形式的冗余以确保数据和应用程序在任何时候都可用。尽管进行了大肆宣传，但是云服务还是相当的不成熟，很多人都经历过某种形式的中断或者其他的毛病。有些云很容易失败，它只是糟糕的经

济环境中出现的一个新行业。多重服务提供商将向你通过更好的网络多样性以及业务连续性，所以任何基于云的工程都应该包含供应商中立的应用程序和数据结构。这包括以独立的云形式进行备份，以及一个独立的机器镜像（machine image）。你需要尽可能直截了当的进行这一转变，或者执行必要的应急计划，准备随时把所有的操作都拿回到内部云中进行处理。尽管云计算会减少一定的连续性问题，但是它永远不可能避免对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将会受到更多、持续时间更长的攻击，因为它们是黑客和网络恐怖分子喜欢的目标。因此，建立一个数据加密策略并且实现某种技术对它进行支持是最好的主动防御措施。从本质上讲，加密了的数据是受到保护的，这也是为什么许多法律法规都要求这样做的原因。所有的数据和网络通信都应该加密，即便是其他的服务会对它们进行保护。加密还可以让你将角色（roles）和数据分开，因为加密密钥可以控制着对数据进行访问的权限。

在新的一年，我们一定会看到许多新的基于云的服务上线，很多服务会给企业带来实质性的经济利益。有些服务无疑将会改变过去长期建立的风险回报关系，所以当你评估转向基于云服务的投资回报率（ROI）时，你需要重新检查企业的风险业务策略和承受能力。云计算正在改变 IT，所以在 2010 年，请认真考虑如何把安全嵌入到新的业务程序中去，以便基础设施、数据和用户都能得到保护。

（作者：Michael Cobb 译者：Sean来源：TechTarget中国）

应用服务云可以推进安全性

IT 行业进入云计算的一种方式是通过向内部用户提供的企业主导的 IT 人员控制的应用服务。这就让 IT 人员有能力监控使用模式并减少营业费用。应用服务的关键功能是向终端用户发送适应的应用和桌面，而他们的性能和在本地安装的应用上所感受到的性能类似。

虚拟化数据中心的著名的优势是集中的应用密度——每个服务器上应用的数量越多，在电力、冷却、地产和 IT 管理上的合成节约所需要的服务器数量就越少。巩固数据中心和减少服务器数量的能力是 VMware ESX 的主要市场驱动和 VMotion 的功能。但是，端点虚拟化时间把有此那个程序转化到了数据中心服务器中，所以成本节约和服务器虚拟化存在差异。刚刚出现的端点虚拟化的好处主要是从数据中心控制端点、安全方法提升的主要好处、端点管理的节约和终端用户选择设备的自由。让终端用户不关设备或者或位置，总是运行 Windows 应用的安全副本的能力是 Citrix Delivery Center 和 Microsoft Terminal Services 的主要市场驱动。

Citrix Receiver 和 Citrix Dazzle 出现建立企业创建企业应用服务方式的切实的例子。IT 中有一些基于 iTunes 外表的应用选择服务，而且是从用户选择 IT 提供的应用包和他们工作需要的桌面的方式上取得感受的。Receiver 软件很明显是为用户运行应用选择最好的机制，决定应用是否应该本地处理或者可以被虚拟化在数据中心中以本地用户界面运行。对安全团队来说最重要的是，不管用户使用的是在公司笔记本电脑、家庭电脑还是个人 iPhone，用户都可以运行 Windows 应用的经过同意的复制版本。IT 完成了对应用的认证访问控制、桌面的安全意识配置、应用和浏览器、敏感数据的控制以及集中审计来监控可接受的用户策略，而不需要从微观管理端点。虚拟化可以改变传统的安全方式——就是 IT 和安全团队的分裂的概念。

大部分的企业采用应用服务都是考虑远程用户和重复任务的工作人与，例如数据进入位置、银行出纳员和在家工作的员工，而家里端点是共享的或者相反不容易被管理的。应用服务的方法放大了对办公室工作人员和远程工作人员的吸引力。

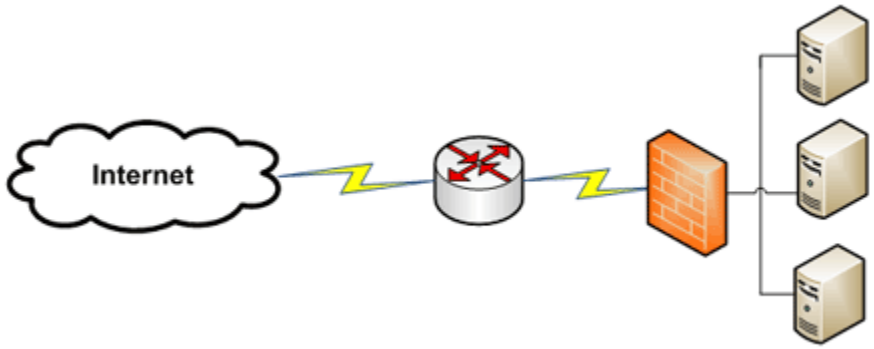
VMware vSphere 很好，而且是数据中心的推荐应用，但是虚拟桌面和端点应用上很令人失望。中层的企业发现 Microsoft Terminal Services 是个很优秀的容易管理的基本应用远程显示功能的选择。SMB 企业在设备室中为应用安全、不定和升级分配服务器；终端用户点击图像远程执行应用。技术熟练的员工使用 Parallels Virtual Desktop Infrastructure 建立自己的端点安全工具。Citrix 安装基础现在开始向用户资料发送应用服务上存在一些问题。在安全资料中，端点被视为最弱的一环。通过应用服务虚拟化端点可以让 IT 不需要再管理和保护端点。

（作者：Eric Ogren　译者：Tina Guo来源：TechTarget中国）

云中的网络安全服务的优势

问：云网络安全服务的优势和劣势是什么？请您提供一些这种服务的例子。

答：“云”这个词是指在外部提供商或者管理安全服务提供商（MSSP）所运行的外包的管理安全服务。这些服务被这么认为的原因是大部分的网络图表使用云的图片代表公司边界路由器之外的一切，例如下面的图表：



云中提供的服务包括管理防火墙到入侵检测/防御服务（IDS/IPS）到反垃圾邮件/杀毒过滤。

应该使用“云中”的服务吗？这是个复杂的问题。他们要比自己动手的方法贵了很多，但是这样的安排可以使自我管理服务中的技术复杂性降低。

管理安全服务可以可利用安全专家和他们大量的专家意见，但是你会失去了解“安全人员”的舒适感，这些了解并熟悉你的业务的人就在附近。

我个人相信管理安全服务可以在“深度防御”策略中起很大的作用，这种策略在安全中强调分层的方法。如果这种方法适合企业的安全计划，就立即采用管理服务吧，但是需要向他们提供保护服务期和桌面的端点安全产品。

(作者：Mike Chapple　译者：Tina Guo 来源：TechTarget中国)

Web 安全策略：使用云安全服务

如果你从未留意过企业内的 Web 安全策略，那现在就是时候重新审视一番了。可以肯定地说，你的公司有各种部门正在使用 Web 应用和云计算架构或服务，而现在是在他们周围建立安全策略的时候了。

最近的思科系统 2009 年度安全报告指出了做好 2010 年切实计划的必要性。基于云的工具和使用云的生产力软件可能已经在你的公司里应用了，而黑客也已准备好猛扑上去。

传统的 Web 安全主要包括 URL 过滤、HTTP 协议校验和单一登录访问控制。然而，恶意软件作者感染正规网站或者改变域名的速度要超过信誉系统能够适应的速度，这使得 URL 过滤的作用从反恶意软件安全手段变成了保证允许使用策略的强制执行。

协议校验已经被集成进防火墙中，以便在下游系统受到影响之前就在网络边际查出异常流量。而 Web 安全被留给终端，这使更新签名定义和软件功能对 IT 来说代价高昂。

给 IT 的好消息是因特网流量可以通过基于 Web 的安全云重定向，且性能仍可接受。云安全服务可以使处理和管理任务集中化，使得在控制成本的同时将有效的安全扩展到企业更加简单。

入流量可以被检查是否有恶意软件并强制执行经验证的访问控制；出流量可以被检查是否有受限数据以及是否依策略进行了传输加密。从管理上讲，集中的 Web 安全控制可以为新的基于 Web 的应用增加额外的应用层安全，并提高检查能力以达到更好的性能，而不需要把管理的负担大范围分布出去。

Web 安全有多种实现方式，可以将他们混合以适合网络架构的需求。类似微软的 TMG 或者 Check Point 安全公司的 Web 安全软件刀片网关这样的设备很适合支持分公司，或者需要一个专用设备进行高性能过滤的情形。安全云服务，包括趋势科技和 Zscaler 公司等提供的服务，可以在不需要大规模分发签名来给占用网络带宽的低优先级应用限速的前提下，有效地过滤已知的恶意软件，同时使得所有用户可以立即享有新增的安全功能带来的好处。

企业安全云可以遵循相同的模式。那些希望被阻断的消息和数据存在站内的系统上，而不是在一个安全服务商的数据中心的企业，可能对数据外泄保护功能特别有兴趣。虚拟桌面基础

架构项目也给了 IT 一个机会，来以一个独立的安全云的形式来部署安全。IT 团队可以把出去的流量都通过安全产品来路由，以保护业务，而不需要在每个虚拟机或者虚拟的服务器上安装 Web 安全软件。例如，Xceedium 公司允许 IT 对数据中心内的因特网访问进行颗粒状的控制，而 HyTrust 则可以提供对虚拟数据中心内的经授权的用户操作的控制——两者都是将应用和桌面与安全策略执行相分离的重要能力。

在安全团队考虑用 Web 安全云保护业务的可行性的时候，他们也可以考察虚拟化帮助台服务的能力。Citrix 系统公司和 Bomgar 公司这两个公司提供可以轻松从因特网下载的“可降解”的代理软件，使得 IT 可以通过 Web 支持远程用户。这种方式要依靠 Web 安全来降低服务台的运营成本（例如，更少的系统软件更新），并通过更快地解决安全和配置问题来提高用户满意度。在审视将 Web 安全责任赋予安全云的同时，IT 可以通过集中化管理远程支持软件来理顺帮助台运营。

还没有动作的公司应该预留 2010 年的资源来重新审视 Web 安全的趋势、其对业务的影响和满足普遍的 Web 访问安全需求的其它方法。

（作者：Eric Ogren　译者：李博文　来源：TechTarget中国）

如何确保云计算的安全性

云计算是有吸引力的，充满诱惑的，也许也是不可抗拒的。其优点是令人信服的，尤其是 pay-as-you-go 模式，与买电非常相似（或者说，如果你愿意，可以只买一杯饮料，而不是一整瓶）。

这是一种强大的商业模式：根据需要购买计算能力、磁盘存储、协作应用开发资源、客户关系管理（CRM）。云计算是灵活的，可伸缩的，而不必购买更多的服务器和磁盘或扩大或部署昂贵的基础设施和程序。它可满足短期创意和要求，也可以应对商业周期中的高峰和低谷。

但是，如何在这一过各程中确何安全呢？安全分析家和从业人员一般会说要使用云计算，但要谨慎行事。云计算会遇到与外包有关的敏感的公司数据所能遇到的所有风险。当你和第三方已知或未知的转包商交易时，特别是在全面范围内时，执行安全策略和遵从法规要求就很困难。，。再加上云模糊的特性以及非传统厂商进入这个市场，就更增加云的危险。

IDC 去年秋天公布的一份调查报告中指出， 在 244 个 IT 主管/ CIO 中，75%的受访者认为对于云计算，安全性是重要或非常重要挑战。 相比之下，63%十三关注后两项---性能和可用性。因此，与商业伙伴在业务上进行竞争之前，你最好克服云计算的风险。

Craig Balding，一家财富 500 强企业的技术安全领导说：“我建议安全人员要关注这个问题，因为 CFO（他只关心数字）或者听 CFO 陈述的 CIO 会来问：‘云计算到底是什么，我们可以用云计算做什么？’”

让我们研究一下云计算的风险与收益，做哪些事情可以使公司减轻这些风险并收获一些好处。

安全不是提供商的专利

现在，云计算提供商不过多谈论安全并不奇怪。现在正是宣扬云计算是即将出现在商业领域的下一个“重大事件”的时候。

大部分公开的讨论来自安全专家和分析师，这些讨论推动了厂商采取主动行动。正如 Balding 所举的例子，亚马逊在亚马逊网络服务(Amazon Web Services ,AWS) 网站上并没有太多的安全措施，谷歌的企业应用套件也一样没有。没有明显的程序或明确的承诺可以，比如应付想要报告漏洞的研究人员。

“谷歌和亚马逊都有非常精明的安全人员，”Balding 说，“但是，当你与在每次关于云计算的会议上都很显眼的亚马逊的人讨论安全问题时，不会有太多的交谈。如果他们把可以讨论安全问题的人员也带到社区，那这将更有意义。”

问题不在于云计算厂商对安全问题都漠不关心，显然他们并非如此。 相反，问题是强安全性对于他们的商业模式有多重要，他们在这个问题上会走多远，他们愿意为这个问题花多少钱？问题还在于，一个商业模式是否支持这样一种安全计划，这一安全计划不仅强有力而且能足够灵活地满足用户独特的安全和法规需求，特别是大型跨国公司？

“云计算为性能进行优化，为资源消耗进行优化，为可扩展性进行优化，”Forrester 的分析师 Chenxi Wang 说，“但不针对安全进行优化。”

在这一市场的早期阶段，你必须关注的是现在的安全问题在哪，厂商是否从开始就可以突破到服务中来，或是从客户的方面向服务施加压力。这是一个新的市场，公司必须在进入市场之前对安全问题有足够的准备。

“现在，一切都没有确定，” Gartner 的分析师 Mark Nicolett 说，“这是一个早期采纳者所遇到的情况。你不可以在云计算中才拥和传统外包商的安全性一样的的安全等级。”

云计算的高度风险性

对于云计算，你必须处理所有在“正常”外包服务中所遇到的风险因素。但是，云计算也带来了其自身固有的安全问题，这使得它不仅难以为你的公司提供它完成所需功能的保证，而且，在某些情况下也会使服务提供商难以满足你所要求的所有服务。

“云计算的不同之外在于控制，”Balding 说，“控制意味着可见性。你无法看到的东西是无法控制的。”

考虑数据安全的三个主要要求：可用性，完整性和保密性。

第一个要求对于你的业务和你的服务提供商的业务是核心的。数据泄露已经够糟糕了，但如果服务中断，业务也就中断了。例如，Amazon 的 Simple Storage Service（S3）去年曾两次中断过几个小时。如果您的第一项要求是接近 100 %的正常运行时间，那么这是一个很好的选择，几乎每个厂商将其做为优先考虑的事情。

数据完整性和保密性是另一回事。 完整性要求只有授权用户进行经过授权的更改。保密性是指只有授权用户才能读取数据。人们会期望应用强有力的控制加强对授权用户访问、认证、隔离数据等方面进行管理。如果已经有传统的合作伙伴和服务供应商可以接触你的敏感数据，你就可以扩展这些控制。但是，云计算条件下，作为一个实际问题，你不知道你的数据在什么位置。你不知道哪一台服务器为你计算，不知道它通过哪些网络传输，甚至不知道它存储在什么位置，因为提供商的系统动态的响应你和其他成千上万的客户时增时减的需求。云计算的灵活性和可扩展性，使云计算具有吸引力的同时也使得它难以预测。

“外包给 Amazon、或 IBM、或戴尔、或微软做云计算与外包给 AT&T 没有差别，”杰夫阿尔法软件首席安全专家 Kalwerisky 说。“现在的差别是你确实不知道数据在哪。”

此外，很难保证数据的隔离，因为这些网络和服务器共享来源于数以千计的客户的数据。 所以你必须要关注的是你的服务供应商的工作人员和一些来自其他企业的人由于不当授权或认证可以读到这些数据。

Forrester 的王提到了一个相关的问题，即传递信任，因为云计算供应商必须依靠第三方供应商提供的计算和基础设施资源。那么如果我与我的供应商之前存在值得信赖的关系，我该如何扩展这一信赖关系呢？

“这些第三方基础设施资源接触到我的机密数据”，王说。“我是否应当允许这种我已经与我的供应商，比如亚马逊，建立的信任关系传递到第三方，以及如何对此进行评估？传递信任的问题没有明确的说法。”

所以，你的供应商并不知道在特定时间你的数据在何处，这就难以确定你的数据是否正在以保密和隐私的方式进行处理。

谨慎地采用云计算技术

这些并不这意味着你的公司应该排除使用云计算开展业务的计划；你也不应该为安全问题妥协。

Alpha Software 的 Kalwerisky 说：“你现在唯一能做的就是在应用云计算之前慎重考虑合同”。他说，大客户可以利用主要的云计算提供商保证更好的安全性和透明度。毕竟，有选择的余地。

“如果一个供应商做不到，我可以去其他的供应商”，他说，“市场将推动它。”

Gartner 公司建议你对外包商坚持坚定的安全要求，即使云计算环境是比较大的问题。你的数据的风险仍然存在。

在名为“评估云计算的风险” 的报告中，Gartner 公司强烈建议引入第三方安全公司进行风险评估。它警告说，即使是习惯自己进行评估的大型高端的企业，如主要金融机构，也最好聘请第三方评估提供云计算的商业伙伴。

云计算分布式的性质使得这种评估变得更加困难。而且，与传统的外包合作伙伴将良好的安全性视为一个有竞争力的竞争标准不同，云计算供应商可能会对外人审计他们的运作有所保留，或至少是限制其访问。它们不太可能允许审计和评估小组接触自己的数据中心，但进行日志检查和审查审计跟踪也就是可以商量的了。

Forrester 公司的 Wang 说：“显然，审查不可能很具体。例如，对谷歌进行漏洞评估（是不合理） 。他们不会让你这样做。你必须看是否有可能做某种程度的外部审计。目前，这是非常困难的。”

大型企业当然不应该迁就供应商的标准服务协议，但规模较小的公司是另一回事。他们通常缺乏充分评估服务的安全性的专业知识或机能，所以他们更倾向于依靠具备专业知识或机能的供应商。

“我接触过的大多数小公司，除非它们是高度专业化的，往往将性能、减少资源的开销置于安全之前考虑，” 王说，“但是，这并不意味着云计算供应商不应该做更多的工作，满足他们的需求，而且更加透明化。 ”

不论公司大小，最重要的考虑是暴露给了服务供应商的数据的敏感度。如果服务不必把敏感数据暴露在风险中或不会危及你的操作，对供应商的安全性要求也可以不那么严格。另一方面，如果机密的客户信息、知识产权或其他敏感的数据处于危险之中，公司也不应该对安全性要求妥协。

“企业所需要做的是在风险与商业利益之间做出选择，确定那些商业利益相对高于风险的业务，” Gartner 公司的 Nicolett 说，“那些业务现在是最适合云计算的。”

公司也应坚持对数据进行加密，无论是传输过程还是静止数据。加密传输过程中的数据是可以保证的；所有服务供应商都使用 SSL 或其他一些强大的加密功能。静止数据更加复杂，并且你可能必须依靠自己的资源进行加密。关键的问题是：谁拥有密钥？

如果供应商控制密钥，加密则变得不现实。这又会回到一个信任和核查的问题，要核查该供应商不管什么人、在什么情况下接触密钥都严格遵循规定。如果你的公司持有密钥，这一机制就更复杂，但是安全显然是在你的手中，因为只有你的工作人员可以解密数据。

Gartner 公司的 Nicolett 将漏洞管理服务提供商 Qualys 公司视做一个很好的模式。客户的数据是混合的，但它是加密的，由客户控制的解密密钥。

“敏感的安全数据存放在外部，而企业感到放心，这是能力”，他说。

坚持规定

容易获得是云计算的优势，也是它的风险。一个部门、工作组甚至个人可以轻易进入云计算中。只需要出示企业卡

“这是从安全的角度来看民主化的负面影响，” Balding 说，“除非你已有优秀的 DLP，你可能甚至不知道云正被使用。”

考虑一组开发人员，他们可以绕过公司的规定和流程--也许事情比他们所希望的要慢很多。他们不是坏人，他们只是试图要完成自己的工作，并做他们想做的：为公司创建一流的软件。

或是业务部门可以作出决定，签定合同开发应用程序或是购买 CRM，如 salesforce.com 。他们完成任务，但绕过所有他们应该遵守的控制规定。

“这可能是一个有效的商业决定，但值得担心的是这是一种无意识的决定”，Gartner 公司的 Nicolett 说，“这样，就没有对安全性、规定和风险程度进行评估，因为了解这些风险的人员并没有参与这项决定。”

同时这也有经营风险，他说。 工作流程可能会被损坏或破坏，因为应用程序之间的联系进入云中，内部程序不明确，流程的完整性可能会退化。

你仍然可以将应用迁移到云计算中，他说，但是你必须制定有意识的、计划周密的决定，这些决定可以解决这些将要出现的潜在的问题。

解决的办法很简单。如果你的公司有良好管理规定，员工遵守进行风险评估的规定和流程，在签约前为服务进行规划和审查。从高层传递来的消息应该是肯定的：外包的措施适用于云计算。因此，在这走完这一流程前，不要急于付钱。

标准化--下一步吗？

评估云计算供应商的主要障碍之一是缺乏用于比较的标准。没有标准对数据如何存储、访问控制、性能指标等进行衡量。

这引起了商业和安全问题。例如，如果我将我的销售系统外包给一个供应商，但要与收帐款业务指定另一个供应商，我怎么在他们之间共享数据？更进一步，这种方案可行吗？

供应商、分析师和安全领导人正在讨论标准化的必要性，例如，SLA。

“我的客户在与其他的 SLA 对比时遇到了问题，因为语言是不同的；他们承诺的特性不同”， Forrester 公司的王说。“你真的要花费大量的时间确保你拿来做比较的是两个苹果，而不是一个梨和一个苹果。”

下一步可能会由一个行业联合会达成一项协定，并最终由一些公认的标准化组织进一步认可这一协定。使竞争者服从一个标准从历史上看是很困难的，这一协定也不可能会例外。

“没有一个供应商希望做出改变以符合其他一些供应商的标准”，阿尔法软件公司的 Kalwerisky 说。 “但是，一旦我们有了关于数据存储、安全问题和许多其他事情的标准，那么云计算就成为了不可阻挡的选项，因为你会拥有你在数据中心所拥有的一切，但会减少麻烦和资本投入。”

(作者：Neil Roiter 译者：陈志辉 来源：TechTarget中国)

加密专家说云计算可以被保护

云计算的进步可能已经是不可避免的了，但是这不表示相关的安全问题不可避免。

据 2009 年 RSA 大会上的加解密专家称，云计算安全问题和任何新技术的问题都很类似，安全研究人员可以发现更好的保护云中的敏感数据的方式。

Sun 的副总裁兼首席安全官 Whitfield Diffie 说“我认为云计算将会达到这种转态，任何程序或者主要的行业设计都不能在公司使用云计算的电脑上进行。这次我认为应该是比我年轻的人来发现解决方案。”

Whitfield 是参加周二 RSA 年度加解密专家团的五个著名的加解密专家之一。

马萨诸塞洲的技术研究所的电机工程和电脑可以专家 Ronald Rivest 说，他对研究人员可以聚在一起解决云计算的安全问题感到很乐观。

在最近几个月中，已经成立了一些安全组织研究如何保护云中的数据。这样的组织之一，云安全联盟，就在本周的 RSA 上启动了。它还将发布一份安全报告，流出了十多项需要解决的云计算安全问题。

Rivest 说：“确保满足所有的安全目标非常困难。”

相关的安全问题，行业观察员注意到随着企业在降低成本的新方法，他们越来越多转向云计算。研究公司 Gartner 估计，到 2011 年，早期的技术采用者将把他们的 IT 基础架构的 40%以服务的形式购买，“把应用从特殊的架构中分离出来”。

安全厂正在准备对这种趋势作出回应。周一，VMware 在 VMsafe 项目中发布了 针对安全厂商的 APIs。他们还发布了云计算操作系统的下一个版本。赛门铁克、McAfee、趋势科技和其他厂商也正在整合安全工具解决虚拟化问题。

至少有一位加解密专家警告说云计算可能导致威胁的增加。Weizmann Institute of Science 的计算机科学专家 Adi Shamir 说安全一直是阻挡造不成大祸的小灾难。他说云计算引入了这样一个世界：大型计算是有很少的由微软、Amazon、Google 等主导的大型数据中心处理的

Shamir 说：“我认为我们正在面对真正的危险，黑客将可以使其中一个这样的数据中心不能工作，然后我们就会面对灾难性的后果。”

但是，BT Counterpane 的首席安全技术官 Bruce Schneier 说他没有看到云计算和目前的软件中的风险之间有很多基本的区别。

Schneier 说：“我们仍然要相信我们的厂商。”。

（作者：Robert Westervelt 译者：Tina Guo 来源：TechTarget中国）

私有云：创建自己的云安全等级

维护你对云中的数据的控制的方法之一是对它的所有权。这是财富 500 强之一的技术安全领导者 Craig Balding 所说的。

他说，大型企业都已经在数据中心的作了巨大的投入，所以商业的活跃性以及新商业的主动性都是他们投入云计算的不得不接受的驱动，迫使其节约硬件成本的投入，至少现阶段是这样。所以提到私有云的概念，也就是完全是在大型企业内部的云（称为“企业云”），但是更可能包括第三方，例如将向云服务迈进的主要提供商之一。

区别在于私有云不能向公众开放。企业客户可以获得云计算的安需的最大化的利益，但是可以获得和常规的外包服务相同的安全和法规控制。由于主要提供商可以依据领域——防御、金融服务等等分割数据，并且已经习惯于维护对每位客户的信心的强大的访问，他们可以在合适的位置支持这种类型的云。

Balding 说：“有了私有云，攻击界面就很少了。”因为在这世界上，不是有了信用卡就可以注册的。

（作者：NEIL ROITER 译者：Tina Guo 来源：TechTarget中国）

为云计算的实施做好网络准备

云计算给企业的运行方式带来了巨大的变化，而企业的 IT 基础设施也就需要相应的改变。这个变化对那些保护企业数据以及企业网络用户安全的网络管理员们来说影响最大。

共享数据、应用程序以及 IT 基础设施能够给企业带来巨大的成本优势和生产效益，但也会给公司的防火墙和物理环境带来麻烦。作为网络管理员，你在公司实施云计算过程中需要做的工作就是在把数据、应用程序、基础设施这些内容发送到云计算时，确保用户和数据的安全。尽管云计算提供商也承担了保护企业数据安全的部分责任，但是最终还是得由企业自己的安全工作人员来负责。在这篇文章中，我们将讨论一下在把网络基础设施延伸到云计算的时候，该怎样做好企业网络安全方面的准备工作。

在把数据或者应用程序发送到云端之前，评估当前企业内部网络的安全状态非常重要。此时是进行网络审计的理想时刻，因为你可以查清楚公司的网络防御是否跟公司的数据安全性、完整性、可用性政策相一致，是否符合监管规则的要求和行业最佳做法。

这个审计的好处是多方面的。使用网络审计工具（免费的、或者市场上可以买到的）肯定会发现一些不理想的配置和实践做法。一旦用更好的安全控制以及改进的程序将这些缺点进行修正之后，你就能建立起一个可以接受的网络设备、网络用户以及应用程序的安全基准。这个基准可以作为今后审计工作和安全配置检查的参考，以确定在转移到云计算的过程中网络安全是如何受到影响的。

其次，了解云计算提供商的安全政策和程序也非常重要。你应该寻找那些安全水平能够跟企业遵从标准相符合的、安全内容跟企业防火墙内容相一致的服务提供商。为了避免安全领域各个方面（比如备份、访问、数据破坏）的责任混乱，我推荐在合同中明确指定哪一方去负责相关政策或者标准的遵从事宜。

防火墙的设置可能需要调整，这取决于云计算服务是怎样进行的。为了确保防火墙系统和其他的周边防御（比如 IDS/IPS 系统）得到正确的调整，你需要跟服务提供商密切合作，因为他们理应具备处理可能出现的网络安全配置问题的经验。如果需要对防火墙规则进行修改并且要开放额外的端口，请确保这些变化被更新到网络安全基准上，并对网络再次进行扫描检

查。你可以使用像 Nmap 这样的工具，它可以保证只开放正确的端口，并且保证不会有不被信任的关系或者连接来破坏安全政策。

当在网络中添加一个新的服务时，请保证有足够的职责分离以及足够的访问授权，以保证没人能够恶意或者无意的破坏公司数据。根据人力资源部门的雇佣登记表来复查用户帐户以及帐户特权必不可少，这样可以确保访问权的正确性，确保那些不再使用的帐户已经被停止。如果由于转移到云计算的需要，你给第三方（比如提供商和客户）开启了网络访问权，那么还应该对网络访问控制系统（NAC）的全部设置进行复查。请确保目前的 NAC 产品能够应对用户数量急剧增加的情况。许多企业实际上正在考虑使用基于 SaaS 的 NAC 方案来保证可扩展性和协同工作能力。

云计算在某种程度上模糊了静止数据、传输中的数据以及使用中的数据之间的区别，这使得数据加密成为最重要的防御手段之一。加密的数据自己就能够保护自己，因此即便是其他的服务会保护数据和网络通信，这些数据和通信也需要全部加密。另外，加密可以让数据不可读，减少了存储在云计算中的数据遭到破坏的风险。加密技术还允许角色和数据的分离，因为加密密钥控制着数据的访问权。我会用一种分析程序（比如 wireshark）对网络进行定期检查，以确保网络通信通道是加密的。

最后，请通过使用内部云或者混合云的开发以及实验来对网络安全进行测试，不要害怕麻烦。这项测试包括在企业内部网络使用一个应用程序服务进行测试，这跟云计算供应商所提供的一样，还包括通过一个有限制的、非关键任务的云计算来测试云计算提供商的能力。我推荐大家阅读一下云安全联盟的指南，它能帮助你理解企业采用云计算时需要考虑的主要问题。

然而，为云计算准备好网络只是第一步。为了让云计算的实施能够真正成功，一旦你开启了云计算服务，你就需要确保网络的基础安全长期稳定。你还需要调整并且升级你的防御措施和安全控制来处理新的威胁。我们将会在下一篇文章中对这方面的挑战进行讨论。

（作者：Michael Cobb　译者：Sean　来源：TechTarget中国）

实施云计算之后如何保证安全

如果你已经成功地把你们公司中使用的应用程序和数据接入了云的话，那么别人就会说你完成一件非常棒的工作。但是你和我都知道，这些应用程序和数据的安全维护工作才刚刚开始。在这里，我将谈一谈在云计算实施后，或者实施方案已经确立并开始执行时，哪些技术和程序必须要开启、监督并保证其安全。

身份识别和访问管理（IAM）

云计算把我们大家变成了可以远程办公的工作者，但这也使得身份认证和访问管理（IAM）成为了迁移到云计算后的主要挑战之一。拥有一个健全的、关于用户以及用户访问周期性的管理方案很重要，因为它可以使得用户的账户、证书和访问权限都能适用并能进行更新，还能够禁用那些已经离职的用户的账户。我们还期待着建立这样一种机制，它可以充分利用联合身份管理，从而使得用户可以跨越相对独立的安全域安全地访问数据或者其他系统。

更具体一些来说，就是要企业应用程序中加入单点登录（SSO）功能，并且要利用这一架构来简化云提供商的工作。对于那些已经使用 SSO 的用户来说，他们会感觉到更加无缝迁移到云计算中，这会使得跨越不同类型云计算服务的信任管理简单一些。你还将会得到作了日志记录的基准数据，这些记录可以帮助你监控和评估由于迁移到云计算所带来的变化。

SSO 产品应该采用联合实施普遍标准中的某个标准，比如安全声明标记语言（Security Assertion Markup Language）和自由联盟统一联合框架（Liberty Alliance ID-FF）。这些标准扩展了现有的从内部网络越过防火墙到外部云的访问和身份策略，同时仍然可以按照你的信息保护和数据分类规定来执行适当的认证强度。

带宽

云计算不仅使得互联网的使用增加，而且还增加了网络堵塞瓶颈的风险。Web 应用程序对延迟极其敏感，网络太忙会导致很多程序的运行非常吃力。停机或者处理缓慢将会大大降低雇员效率，并可能导致他们不遵守相关的策略。比如，文件或着数据传输慢可能会导致员工使用那些相对不安全的方法，这会破坏公司所规定的安全政策。

解决这个问题的一种方法是使用 WAN 优化产品，这种产品可以通过“改进应用程序流量管理、消除多余的传输”来缓解企业应用程序网络流量的拥塞问题。比如，Citrix 系统公司推出的 Ctrix Netscaler 软件，它提供一个 Web 应用程序的防火墙，并且结合了第 4-7 网络层负荷均衡的流量管理。其它 WAN 优化厂商还包括 Riverbed Technology 和 Blue Coat 系统公司。

防火墙

内部网络和云之间的连结当然应该被加密；在互联网上用明文来回地发送任何敏感或者关键数据就像是主动邀请攻击者来窃取信息一样。作为网络工程师，你一定要确保网络设备可以应付那些在 SSL 加密通信中大量占用处理器时间的公钥加密算法，你可能需要将那些处理所有 SSL 操作的 SSL 加速卡或者代理添加到基础设施中去。但是，加密本身并不能阻止恶意软件或者其它方面的网络攻击。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

在云计算实施后，另外一个重要的任务是对所有安全策略进行审计，以确保它们仍然适用。此外，还需要对故障恢复和业务连续性的计划和程序进行更新和测试。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：Sean　来源：TechTarget中国）

安全云计算联盟成立

一个新的组织计划为采用云计算产品的公司提供安全建议。

The Cloud Security Alliance 本周发出了这样的声明。这个非赢利性组织将在 4 月 21 日旧金山的 RSA 大会上正式启动。它会提出安全云计算的最佳实践并教育用户云计算如何保护其他的计算形式。

这个联盟的联合创始人之一、安全咨询师 Jim Reavis 说联盟想要提供对采用云计算的公司提供安全教育和指导。他说，联盟还将帮助云计算厂商解决软件发送模式中的安全问题。

Reavis 说：“在企业管理信息和所使用的工具之间总是存在联系，但是使用云计算，所负责信息的分离和这种工作就会由第三方负责。”

云计算是按需访问信息技术服务。虚拟化是公司用于访问这些服务的方法。Reavis 如是说。根据 Gartner 的调查，到 2011 年上半年，技术采用这将把 IT 基础架构的 40%以服务的形式购买，“把应用和特殊架构分割开”。安全厂商要在 VMware 的 VMsafe 项目下重组他们的应用。赛门铁克、McAfee、趋势科技和其他厂商都在整合他们的安全攻击，解决虚拟化的问题。

这个新联盟将在 RSA 上发布名为“云计算关键领域指南（Guidance for Critical Areas of Focus in Cloud Computing）”的技术论文。这篇论文列出了云计算用户和提供商必须解决的问题。Reavis 说论文很全面，涵盖了和云计算相关的法律、技术和管理问题。

他说：“我们派出了一些这个领域的主题专家，去看看云计算的风险和机遇，以及我们可以为云服务用户提供哪些指导。我们想要提供实用的资料。”

在这一年中，联盟还计划为不同行业的用户提供专家建议，提出公司采用云计算产品的最佳实践建议。

联盟是由云计算和安全专家领导的，并由 PGP Corp.、 Qualys 和 Zscaler 等公司支持。安全专家兼博客撰写人 Chris Hoff 将在联盟中担任技术指导。

最近还有一个组织启动，也是解决和云计算相关的安全挑战，并支持这种技术的市场增长。这个名为 Open Cloud Manifesto 的组织列出了行业中需要解决的问题：安全、数据和应用写作性和便携性、管理和治理、以及测量和监控。它的支持者有 EMC Corp.、IBM Internet Security Systems、Novell Inc 和 Sun Microsystems Inc.等。

（作者：Robert Westervelt 译者：Tina Guo 来源：TechTarget中国）

云计算联盟前路挑战重重

新成立的云安全联盟（Cloud Security Alliance，CSA）如果想进行关于云计算的有深意的讨论并为计划采用云计算的企业提供有用的数据还需要克服很多困难。这个组织在本月初宣布成立，并计划在 RSA 大会上正式启动的时候发布白皮书。

CSA 的成员都是在安全和互联网企业中已经成功的专家和有兴趣的人员。他们建立这个组织的使命是“促进云计算安全系数的最佳实践的应用，并提供云计算的使用的培训，帮助保护其它形式的计算。”

这不是第一次，也不会是最后一次，成立安全联盟以走在可能阻碍新技术增长的安全问题之前。关于“安全联盟”的搜索可以快速发现很多相似的组织，包括 nternet Security Alliance、Voice over IP Security Alliance、Document Security Alliance 和 Radio Frequency Identification (RFID) Security Alliance。安全从业人员都可以很好的讲出新技术中潜在的安全缺陷，并提出最佳实践建议。

决定 CSA 影响力的首要问题是关注点。随着如此之多的会员的各种情趣和远大的目标，可能会出现沸腾的场面。可能最后的结果是结论太模糊而不能转化成 IT 的实际步骤。CSA 的最初的使命声明和最佳实践研究草案范围个别宽。

现在还没有对“云”的普遍可接受的定义。云计算的市场规模和宣传也各不相同，IDC 预计在 2012 年市场会打到 420 亿美元；而 Gartner 则认为在 2009 年收入将增加 21.3%，达到 563 亿美元；Merrill Lynch 则认为在 20011 年将会有 1600 亿美元的市场。每个公司使用不同的云计算定义，这也解释了市场规模和估价的差异。

更进一步的案例是最近宣布含有 159 个成员的 Open Cloud Manifesto group，他们想要研究云计算的六种模式：

1. 终端用户和云
2. 企业和云和终端用户
3. 企业和云（综合）
4. 企业和云和企业
5. 企业和云（便携式）
6. 私有（内部）云

不管云是什么，数据存储和应用处理都是在企业网络之外操作的，也就是说安全将会是关键的性能。在这个组织提出了云计算的使用案例的同时，安全联盟则是在关注 15 个“焦点领域”，而每一个都可以成为安全联盟组织的重点：

1. 信息生命周期管理
2. 政府和企业风险管理
3. 法规和审计
4. 普通立法
5. eDiscovery
6. 加密和密钥管理
7. 认证和访问管理
8. 存储
9. 虚拟化
10. 应用安全
11. 便携性和互用性
12. 数据中心操作管理
13. 事故响应、通知和修复
14. “传统”安全影响（商业连续性、灾难恢复、物理安全）
15. 体系结构

和云一样，期待云安全联盟开始广泛，然后发现专注的领域。这是一个没有大量用户经验可用的重大承诺。CSA 可能在开始的时候关注两到三个领域，以及集中云的模式，从

而获得 IT 人员的反馈。IT 人员应该关注 CSA 的工作，并随着企业要求的进步，提出 RFP 和 RFI 的建议。云计算联盟和 Open Cloud Manifesto 都有连接的团队，可以获得帮助，特别是从在服务提供商级别网络的大型企业内部工作的安全专家 的帮助。

(作者：Eric Ogren 译者：Tina Guo 来源：TechTarget中国)

云计算安全团队报告安全难点

云计算安全联盟周三发布了一份文件，列出了它认为需要解决的十多处问题以更好的保护云计算环境。

这份 83 页的文件“云计算主要关注领域的安全指南（Security Guidance for Critical Areas of Focus in Cloud Computing）”列出了 15 个需要解决的领域，其中有两个需要特别关注：治理和云中的操作。

报告流出了组成很多云计算体系的架构，然后确定了三种传输模式：基础架构即服务（Infrastructure as a Service，IaaS），平台即服务（Platform as a Service，PaaS）和软件即服务（Software as a Service，SaaS）。它还解决了公司和服务提供商遇到的治理和风险管理问题。它建议服务提供商执行定期的第三方风险评估，并把结果告知客户。

这份报告解决的其他问题包括法规和审计，推荐服务提供商使用 SAS 70 Type II 审计以及 SO 27001 证书，还有要取得更多同样而全面的证书。加密和密钥管理、存储问题、应用安全关注点和虚拟化安全问题也都有细节的说明。

这个初出茅庐的组织是在本周的 2009 年 RSA 大会上启动的，目的是提高对云计算安全问题的了解。在周三的发言中，Reavis Consulting Group LLC 的总裁兼这个非赢利组织的联合创始人 Jim Reavis 说这份报告可以向采用虚拟化或者正在选择云计算提供商的企业提供指导。

Reavis 说：“我们是选择的这些领域是以虚拟化是阻碍构建云计算的战略战术痛处位基础得到，治理领域更加宽广、更具策略性。”

在过去的几年中，企业竞相采用虚拟化并把数据移交给云服务提供商，希望可以削减服务器管理成本。Reavis 说云安全联盟计划在今天主办几次会议，提供云安全问题的专家建议，以及云计算实施的最佳实践报告。

eBay Inc.的全球信息安全副总兼 CISO，Dave Cullinane 是这个组织的顾问之一。在 RSA 的发言中，Cullinane 说他们公司是于计算的早期采用者，而且遇到了缺乏保护云中数据的信息和最佳实践的问题。

Cullinane 说：“我认为我们应该走在这些问题之前，至少要从安全的方面查看这些问题。我们想要做的是把我们可以接触到的专家意见结合在一起。”

这个组织的另一位顾问 Jerry Archer 是 Intuit Inc.的副总兼 CISO。Archer 说 Intuit 看到云计算是不可避免的，并目前正在企业中研究和配置。

Archer 说：“现在它还在试验阶段，但是如果有一定数量的亲自确认的信息和事务数据，确保它的安全毋庸置疑非常重要。确保你可以了解在云中进行的豁动并管理突发事件和正在进行的其它事件非常重要。”

Reavis 说这个组织将会包含一切，目前成员包括从对云安全问题非常有热情的个人到微软、PGP Corp.、Qualys Inc.、Zscaler Inc.等厂商。

Reavis 说：“我们不是把头埋在沙子里等待问题过去的安全人员。我们认为这是在计算方面不可避免的转变。”。

（作者：Robert Westervelt 译者：Tina Guo 来源：TechTarget中国）