思科软件即服务 (SaaS) 访问控制

概述

软件即服务 (SaaS) 是通过云计算模型提供的软件解决方案，对许多组织而言，使用这些解决方案的优势显而易见，包括显著节约成本和提高员工工作效率。然而，采用这些服务也会给 IT 管理员带来一项重大挑战：管理访问控制。

如果没有对用户的身份、访问权限和凭证进行有效的管理（以及无法跟踪哪位用户何时使用何种应用），组织会面临网络和数据安全方面的风险。还可能无法满足合规性监管要求，并且在发生数据丢失事件后妨碍事故调查的顺利完成。这些潜在的负面效应会削弱使用 SaaS 解决方案所带来的优势。

同时，随着企业使用的 SaaS 应用数量的不断增加，他们越来越需要一个高效且易于管理的 SaaS 访问控制解决方案。许多组织的应用数量可能正在迅速攀升，但是管理和 IT 意识却原地踏步。有一个因素还进一步增加了访问控制的难度，即在当今的企业，更多的员工在组织外部的更多地点工作，同时，用于访问各种应用和敏感数据的设备类型也在不断增加。

SaaS 急剧增加

最近的经济衰退促使许多公司开始探索通过云计算和 SaaS 解决方案来控制成本。他们发现，从协作服务（例如 Cisco WebEx™）到联机应用套件（例如 Google Apps 和 Zoho）的各种技术不但可以帮助他们提升收益，还有利于员工交流想法，比以往更高效地完成任务。

员工很快就能接受 SaaS 解决方案，并且认识到这些工具确实有助于改善工作流程和加强与组织内外其他人员的协作。对经济萧条期经历大幅裁员的员工队伍而言，这些优势变得尤为重要。但是，员工往往会在未获得批准，甚至在未通知 IT 的情况下，便注册 SaaS 服务进行“试用”，或者与已在使用此服务的合作伙伴或客户共同处理某项任务。

企业往往不知道企业内正在使用的 SaaS 应用数量，直至经过审计才发现数量庞大惊人。例如，思科® 最近的一项 SaaS 服务审计显示，思科全球 60000 多名员工在整个企业中使用的 SaaS 应用超过 300 个。

在大多数公司，SaaS 应用数量只会不断增加，因为有更多的解决方案可供选择，并且企业希望利用这些解决方案来增加价值和增强竞争优势。事实上，Gartner 预测全球 SaaS 市场在未来四年内将获得蓬勃发展。2009 年企业应用市场的 SaaS 收入共计 75 亿美元，比 2008 年的 64 亿美元增加了 17.7%。Gartner 预计，到 2013 年，这一收入几乎会翻番，达到 140 亿美元 [1]。

移动员工加剧挑战

随着企业采用更多的 SaaS 应用，他们正在寻求有效的方法来控制哪些用户可以访问特定服务，以及这些用户在每项服务中的访问权限。但是，越来越多的用户走出传统企业安全边界迈向“无边界的网络”，使得这项本来已经很艰巨的挑战变得更加复杂。

更多的远程和移动办公员工从机场、家中、咖啡馆等任何需要工作的地点使用智能手机、笔记本电脑、上网本等各种设备访问网络和 SaaS 应用。此外，他们会通过企业支持或不支持的这些设备传输销售信息或客户信息等敏感数据，而且这些数据常常被同时用于工作计算和私人计算用途。

IT 管理员无法将相同级别的安全和控制延伸到不经过企业基础设施而直接访问 SaaS 应用的远程用户。因此，IT 在力争实施访问控制，帮助确保适当的人员拥有网络和相关应用的相关部分的访问权限，与此同时也亟需找到一种快速高效的方式来满足用户远程访问 SaaS 应用的要求。

[1] “Gartner Says Worldwide SaaS Revenue to Grow 18 Percent in 2009”（Gartner 表示 2009 年全球 SaaS 收入将增长 18%），Gartner, Inc.，2009 年 11 月 9 日新闻稿：http://www.gartner.com/it/page.jsp?id=1223818。

对可视性与可控性的需求

为了避免敏感数据丢失，IT 管理员还需要能够及时撤销 SaaS 访问权限，例如当用户从组织离职后。然而，目前的 SaaS 访问权限撤销流程远远谈不上快捷或者高效。

通常，员工从企业离职时仍然保有 SaaS 应用的访问权限，直至下一次在企业用户目录与应用之间进行同步。撤销用户访问权限的这段滞后时间给心怀不满的员工提供了窃取企业数据的机会。再者，由于所有给定组织目前使用的 SaaS 应用数量都很多，他们可能无法确切了解用户在离职前拥有多少个帐户的访问权限，也无法了解该员工能否将关键数据带出去。

IT 管理员还需要一个有关组织正在使用的所有 SaaS 应用的用户访问报告的单一存储库。如果能够查看并记录每个 SaaS 用户的访问历史记录，在数据泄露后的事故调查中，将能节约宝贵的时间。这样还有助于确保组织符合保护某些类型的敏感数据（例如客户的社会安全号码）的合规性监管要求。

因此，随着 SaaS 流量激增，以及从不同设备和非托管终端访问这些应用的远程和移动用户数量不断增加，IT 管理员逐渐发现自己无法以确保企业受保护的方式处理以下对网络和数据安全非常关键的三种活动：

- 管理用户身份。
- 管理用户访问权限。
- 管理用户凭证。

管理用户身份

每个 SaaS 应用都必须在云中复制用户身份数据，以便 SaaS 应用确定向哪个用户授予哪些访问权限。该流程很繁琐，且很容易出错；而且它要求不停进行同步，以便获取最新信息。

为了克服这些问题，一些企业向每家 SaaS 供应商都提供通过“隧道”访问活跃企业用户目录的权限。然而，尽管这种方法对一两个 SaaS 应用易于管理，但随着应用数量的不断增加，这种方法对管理员是一项重大挑战。同时还会造成重大安全隐患，因为供应商可能会滥用用户目录信息。

管理用户访问权限

IT 管理员没有一个单独的地方来实施哪些用户可以访问哪些 SaaS 应用。此外，每个 SaaS 应用存在单独的访问控制。例如，访问 Salesforce.com 的员工使用独立于其企业网络登录凭证的登录凭证直接登录 Salesforce.com。

如果员工离职，组织必须禁用该用户具有访问权限的所有 SaaS 应用的所有相关用户帐户。但是，企业往往不知道员工可能使用了多少个 SaaS 应用。

撤销用户访问权限也正在成为外包或离岸运营的组织所关注的领域；第三方服务提供商的员工和合同工流动性往往较高。此外，正如先前所提到的，IT 无法将相同级别的安全和控制延伸到从非托管终端访问 SaaS 应用的远程用户，而且不经过企业基础设施又是另一个重大安全隐患。

管理用户凭证

不同 SaaS 应用之间的用户名和密码不同，用户难于记住所有用户名和密码。这会导致服务中心收到的服务请求增多，久而久之，会给组织造成很高的成本，尤其是会降低员工和 IT 的工作效率。

另一个关键的风险区域是，用户凭证经过互联网传输，容易受到攻击。

此外，由于每个 SaaS 供应商的密码强度策略不同，并且会发生变更，企业很难遵守企业标准。同时，萨班斯-奥克斯利法案 (SOX) 和支付卡行业数据安全标准 (PCI DSS) 要求实施相关标准，尤其是针对对比较敏感的专利信息或财务报表等数据具有访问权限的用户。

管理 SaaS 访问控制的复杂性显而易见，因此组织无法既保障数据和网络安全没有风险，又充分利用这些解决方案。

为了帮助解决上述挑战和减轻 IT 的管理负担，思科正在为面向 Web 7.0 的 AsyncOS® 解决方案引入一个基于标准的 SaaS 访问控制机制。

利用 Cisco SaaS 访问控制，IT 管理员可以保留对用户身份和相关访问权限的控制权。而用户则可享受流畅的体验，使用一个企业用户名和密码即可访问获得使用授权的所有 SaaS 应用。

解决访问和身份问题

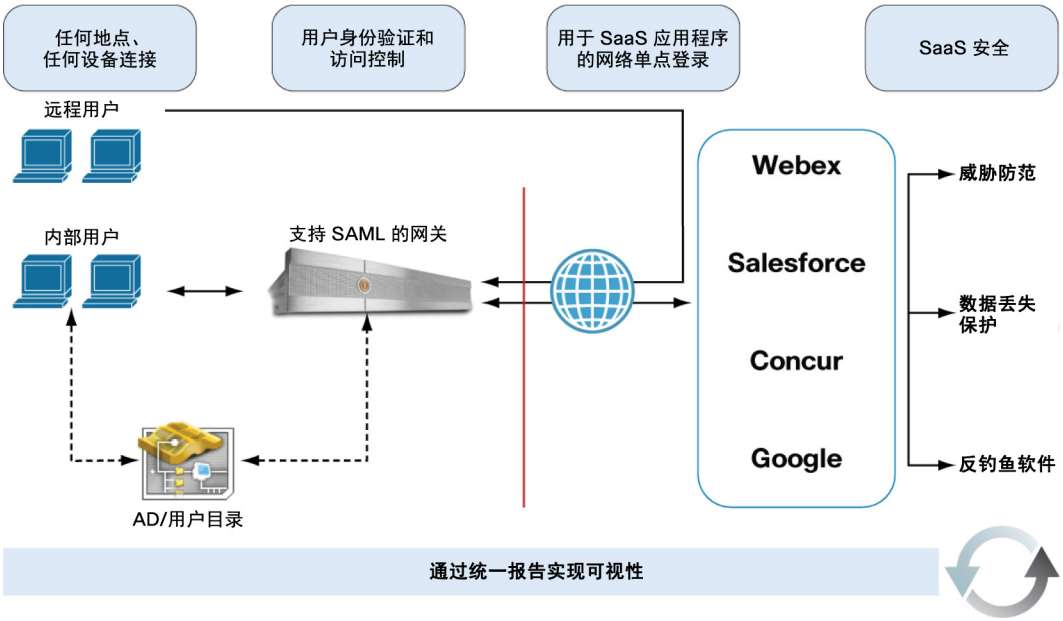
要应对 SaaS 环境中固有的安全与数据管理问题以及员工的高移动性，组织需要具有以下特点的访问控制解决方案：

- **无缝** - 易于实施，且对最终用户透明。
- **安全可控** - 让管理员可控制合法用户的身份验证和授权，可根据需要撤销访问权限，并可通过访问报告了解用户行为。
- **基于标准** - 使用 SaaS 供应商采用的各种技术和语言。
- **支持移动性** - 满足通过移动设备访问 SaaS 应用的用户或企业网络以外的用户的要求。
- **智能** - 向 SaaS 提供商提供与用户访问权限相关的属性（例如：哪些用户具有哪些信息渠道的访问权限）。

Cisco SaaS 访问控制解决方案内置在 Cisco IronPort® S 系列网络安全设备中，可解决采用 SaaS 解决方案所带来的难题，并向 IT 经理提供管理 SaaS 应用访问和实施安全策略所需的控制权。SaaS 访问控制解决方案使用安全声明标记语言 (SAML) 来授权对 SaaS 应用的访问权限。

使用 SAML，IT 管理员可保留对使用 SaaS 解决方案的员工的身份验证和授权的完全控制权；与此同时，用户操作更加便捷，使用单点企业登录即可处理其所有基于 SaaS 的活动。有关 SAML 标准的更多信息，请参阅第 6 页方框中的内容。（要与 SaaS 访问控制解决方案交换信息，SaaS 应用必须支持 SAML 2.0）。

图 1. 使用 Cisco SaaS 访问控制扩展安全和控制



SaaS 访问控制，分步操作

使用 Cisco SaaS 访问控制解决方案，IT 管理员可以轻松安全地管理访问 SaaS 应用的用户身份、访问权限和凭证。管理员和用户均遵循以下所述的流程。

配置解决方案

第 1 步： IT 管理员在 SaaS 应用和 Cisco IronPort 网络安全设备 (WSA) 上通过 SAML 建立用户身份验证和授权。管理员：

- 创建一个供用户访问应用的唯一 URL（例如 http://saas.mycompany.com/SSOURL/GoogleApps），并配置该 URL 以便 Cisco IronPort WSA 能够识别。
- 从 SaaS 应用供应商获取服务提供商元数据，并将文件导入 Cisco IronPort WSA。
- 将企业数字证书上传到 SaaS 应用和 Cisco IronPort WSA，以确保通信安全。

第 2 步： IT 管理员为 SaaS 应用创建各种策略（例如：给定用户组可如何获取访问权限），以及取决于用户位置的访问权限（远程工作员工与网络内部用户）。

第 3 步： IT 管理员可以向所有用户发送上述唯一 URL，也可以在企业内部网上创建一个包含该 URL 的书签。

向用户授予访问权限

第 1 步： 用户通过该唯一 URL 访问 SaaS 应用。如果用户尚未通过身份验证，Cisco IronPort WSA 会对用户进行身份验证。该身份验证可以对用户是无缝的，也可以通过浏览器身份验证提示完成，具体取决于配置。

或者，用户可以访问 SaaS 提供商的网站，并输入企业域名和其他具体帐户详情。随后，SaaS 提供商会将用户重定向至 Cisco IronPort WSA 进行访问控制。

第 2 步： Cisco IronPort WSA 拦截访问、识别用户，并生成表示用户的 SAML 信息。

第 3 步： Cisco IronPort WSA 向 SaaS 应用发送 SAML 声明。其中可以包括用户名等用户身份验证信息，以及位置等配置属性。SAML 声明是使用 WSA 和 SaaS 应用上配置的数字证书安全发送的。请注意，用户密码不会发送给 SaaS 应用。

第 4 步： SaaS 应用对请求的资源作出响应，并向用户授予访问权限。

能够应对所有访问挑战的解决方案

Cisco SaaS 访问控制解决方案可解决 IT 部门在扩展托管应用的使用时所面临的以下三个关键问题。

管理用户身份

使用 Cisco SaaS 访问控制，IT 管理员无需为每个 SaaS 解决方案复制用户身份数据，也无需向 SaaS 供应商授予其通过隧道访问企业用户目录的权限。一旦管理员通过 SAML 配置好身份验证和授权规则，就无需再维护解决方案了。

管理用户访问权限

管理员可以将 Cisco IronPort WSA 作为实施策略的单一位置，用于设置哪些用户可访问哪些 SaaS 应用以及他们可如何访问这些解决方案。例如，管理员可以指定只有销售人员才可以访问 Salesforce.com 中的某些区域，或者只有副总裁 (VP) 级别或更高级别的高层管理人员才可以访问某些信息。

此外，管理员还可以使用企业网络中针对现场员工的安全和控制级别，来管理访问 SaaS 应用的移动用户的访问权限。使用 Cisco SaaS 访问控制，对 SaaS 应用的所有访问，包括移动员工的访问，均由 Cisco IronPort WSA 管理。这样可确保组织的安全策略得到统一实施。

除了统一实施用户访问权限策略外，一旦企业用户帐户被禁用，该解决方案还会立即撤销对所有 SaaS 应用的访问权限，不会因企业用户目录与 SaaS 应用之间的同步问题而出现任何延迟。（请注意，尽管该解决方案能够管理 SaaS 应用的访问权限，但是它没有提供创建或删除 SaaS 用户帐户的功能。）

这种实时控制能减少数据丢失的机会，无论因为疏忽还是有意为之。管理员还可以查看访问报告，获取有关用户行为的信息或者在发生数据泄露后进行取证。

什么是 SAML？

安全声明标记语言 (SAML) 是一项用于在安全域之间，即身份提供者（例如企业）与服务提供商（例如 SaaS 企业）之间，交换身份验证和授权数据的基于 XML 的标准。SAML 的价值正在逐渐被那些需要在保障组织安全的前提下共享身份验证和授权信息的组织所利用。借助 SAML，企业无需向外部供应商授予对其用户目录的访问权限。

包括 Salesforce.com、Cisco WebEx 和 Google Apps 在内的许多 SaaS 提供商都采用了 SAML 2.0 来作为他们的身份验证和授权标准（可访问 http://saml.xml.org/wiki/list-of-organizations-using-saml 查看已采用 SAML 的服务提供商的列表）。鉴于 SAML 的易用性和安全性，思科选择了 SAML 来推动其 SaaS 访问控制解决方案中的用户身份验证流程。请注意，SaaS 访问控制仅帮助管理对符合 SAML 2.0 的 SaaS 应用的访问权限。

思科的优势

Cisco SaaS 访问控制与 Cisco IronPort 网络安全设备集成，可减少 IT 管理难题，同时降低总拥有成本。其他提供联合身份解决方案的供应商需要通过云计算增加设备或附件，因而会将关键控制置于网络边界之外。Cisco IronPort 网络安全设备用独特的方式管理网关内的控制难题。

管理用户凭证

凭借 Cisco SaaS 访问控制，员工只需使用企业用户名和密码即可登录所有 SaaS 应用。这样，企业用户可获得更加快速流畅的体验，不再需要为每个 SaaS 应用管理一个登录名和密码。反过来，这样又能降低对 IT 服务中心的依赖性，同时提高员工的工作效率。

通过采用单个用户名和密码，组织可以统一实施其密码强度和变更策略。这样的统一实施让企业更容易遵守 SOX、PCI DSS 等法规所要求的密码标准。

由于登录过程通过的是企业网络而不是互联网，登录名和密码更安全，遭受攻击或被盗的可能性大大降低。

总结

尚未使用 SaaS 应用的企业所面临的问题并非**是否**采用这些应用，而是**何时**采用。还有，随着他们更多地采用此类解决方案，他们将如何解决管理多个 SaaS 应用的用户访问权限和安全的复杂性？

利用面向 Web 7.0 的 AsyncOS 中的 Cisco SaaS 访问控制机制，组织可以自由地利用 SaaS 应用节省成本、便于使用和提高工作效率的优势，而不会影响安全或合规性。IT 可以从单一集中位置安全地主动管理用户访问，查看与企业正在使用的符合 SAML 的 SaaS 解决方案相关的用户活动。

使用 Cisco SaaS 访问控制，员工还可随时随地从任何设备访问 SaaS 解决方案。当企业调整安全策略并采用新的解决方案以支持新兴无边界企业时，这一能力对组织尤为重要。

美国总部
Cisco Systems. Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte. Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 思科网站 www.cisco.com/go/offices 上列有各办事处的地址、电话和传真。

美国印刷 C11-596141-00 04/10