F5云联合参考架构

通过消除分布式SaaS提供商身份和访问管理系统的缺陷并增强安全性，安全地采用SaaS模式。

白皮书

目录

前言

通过采用基于云计算的服务而非部署和维护内部解决方案，许多企业正在获得切实的优势。利用现成可用、基于订阅的模式，软件即服务（SaaS）提供商能够在经济高效的多租户环境中提供领域特定的专业技术。但是，获得SaaS选项的优势通常以牺牲最先进的访问控制以及可靠的安全策略为代价。如同内部托管服务一样，SaaS提供商维护着自己的身份和访问管理（IAM）系统，以便实施用户名、密码和访问控制，这会带来IAM孤岛和安全管理问题，使得使用多种IAM系统的企业无法进行同步或任何形式的集成。

IAM孤岛会导致潜在的安全隐患并会降低生产力。

- 安全风险是由密码疲劳所引起，更重要的是，由无法及时删除过期账户而引起。
- 生产力降低源于无法及时创建新的用户账户，导致新员工或承包商不能及时访问，以及源于大量IAM系统所需要的管理开销。

F5®云联合避免了这些SaaS缺陷，消除了内部维护的IAM系统与企业外部服务之间的脱节，可以在任何地方提供一致的安全性。

密码疲劳

“使用相同的用户名和密码使账户暴露于黑客攻击的安全隐患下，而不断加剧的复杂选择使得很难记住所有的密码。在某些点上，密码已经太多而无法管理，这就是所谓的密码疲劳。”

-Jon Brody，TriCipher营销副总裁

业务挑战

SaaS的普及

SaaS市场无处不在并且快速增长，为企业提供了大量的优势：

- 因为SaaS基于云环境，所以不需要购置、安装和维护技术。
- SaaS释放了IT资源，使其能够重点关注更具战略意义的项目。
- SaaS有助于实现移动性，通常可从任何位置通过任何设备提供服务。
- SaaS基于订阅，许可成本低于内部购买的现成软件。

- SaaS可通过更新或升级进行维护，而这对于服务用户来说是透明的。

尽管如此，SaaS仍是一项附加服务，不属于企业自行维护和保护的资源，并且这种附加服务还会带来独有的新挑战。

技术孤岛

从数据管理、应用安全以及身份和访问管理方面来说，从企业外部（其私有数据中心外部）提供的任何服务本质上都代表一个技术孤岛。

对于SaaS，数据管理和应用安全都在SaaS提供商的掌控之中，这不是能够轻易改变的。人们有充分的理由认为，SaaS的大多数优势都源自于一个简单的事实，那就是服务交付的复杂性已从服务本身的消费中提取出来。因此，将数据管理和应用安全性向用户开放会将最初的SaaS转型为基础架构即服务（IaaS），这使管理重新回到服务用户的手中，所以马上失去了SaaS模式的所有优势。顾名思义，选择SaaS意味着接受提供商的数据管理和应用安全策略，建立对这些策略的信任。

对于身份和访问管理，SaaS提供商提供自己的解决方案，用户除了维护其内部的IAM系统之外，还要负责填充和维护这些解决方案，再次造成孤立的系统和IAM孤岛。IAM孤岛的增加会带来以下新的风险：

- 数据保护
- 生产力
- 安全完整性

数据保护

数据保护极其重要，企业非常担心（并且有合理的理由担心）委托给外部提供商的数据会被窃取，即便SaaS提供商也不例外。但是，随着每个IAM孤岛增加更多密码让员工管理，这一风险将进一步扩大，因为弱密码使得数据窃取攻击更加容易得逞。在线信用核查提供商Experian在2012年发布的一项调查中指出：“对于平均26种不同的网上账户，用户只有五个不同的密码。”

在2009年的一期《福布斯杂志》中，TriCipher公司市场副总裁Jon Brody指出：“使用相同的用户名和密码会使账户暴露于黑客攻击的安全隐患下，但如果选择使用复杂的密码又难以把它们全部都记住。到了一定的时候，密码将会多得无法管理，这就是所谓的‘密码疲劳’。”。

而比密码强度或黑客攻击更重要的问题是，没有及时注销以前员工和承包商的用户账户将会带来数据保护安全性方面的影响。人力资源（HR）系统每隔多长时间需要跨所有IAM孤岛交叉引用一次？授权变化与在所有IAM孤岛中体现这种变化之间的时差，会带来严重的安全违规风险。然而，在熟练IT资源相当紧俏的情况下，无法及时注销账户将不可避免。

Forrester Research公司预测，IT部门将于2020年销声匿迹。

Forrester Research最近对1000名IT专业人员进行的调查发现，这些专业人员正在转向托管（SaaS）产品，以减轻非关键任务应用的管理工作，例如HR和CRM应用的管理工作。基于订阅的SaaS定价模式还有助于使IT预算成本等同于或低于封装或自主研发的软件。

生产力

如果无法让新员工和承包商及时访问正常开展业务所需的系统和工具，会大幅降低生产力。对新员工的访问进行预配置所花费的时间，会随着所涉及的技术孤岛数量的增加而倍增，因此随着企业更多地利用SaaS的优势，就需要进行更多的访问预配置。

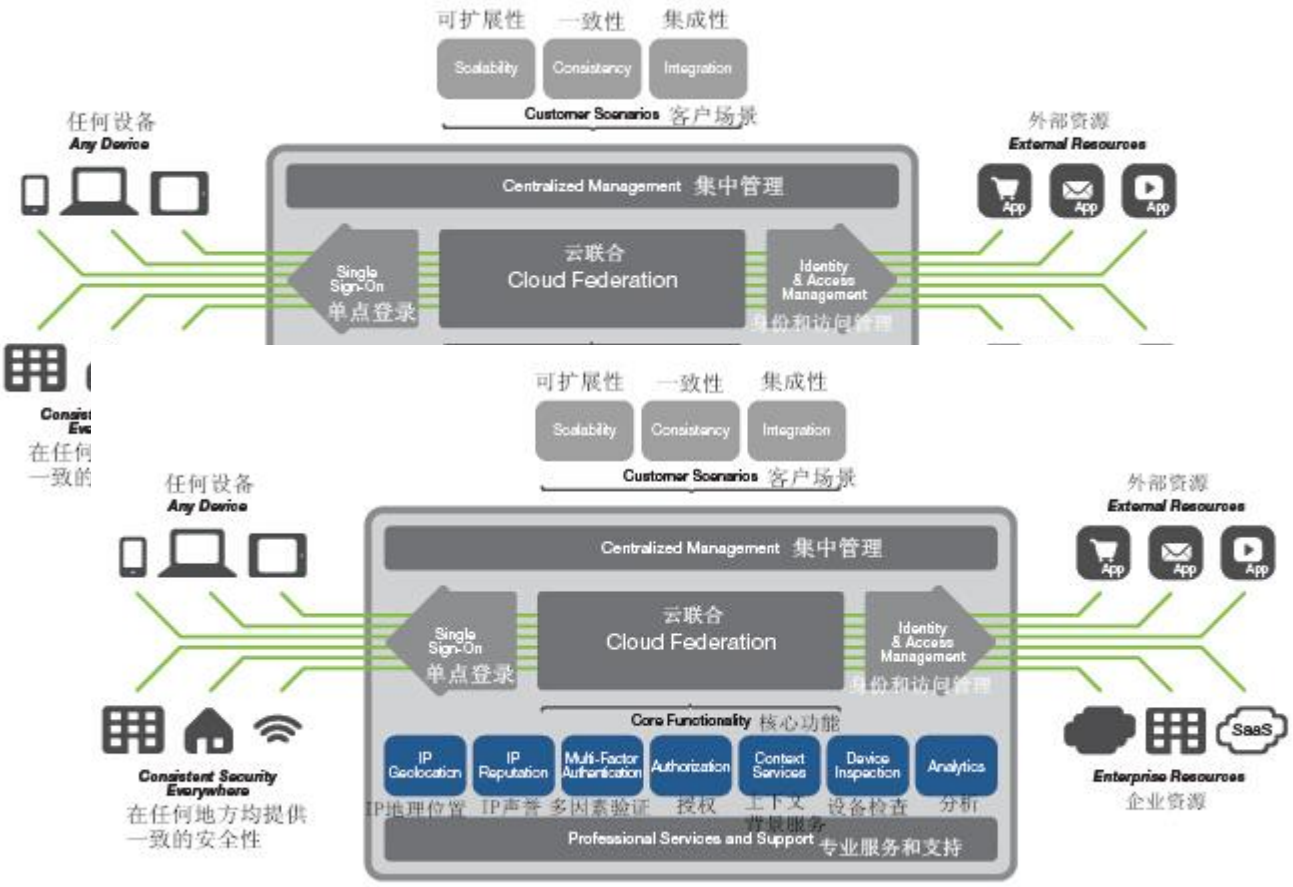
安全完整性

企业投入大量时间和资金为其自行维护的系统研究访问技术，并选择适当的验证和授权解决方案。先进的解决方案采用多因素验证，而这些因素通常包括用户名、密码以及其他验证方式，例如一次性密码或代码等。例如，这些解决方案包括：

- RSA SecureID
- Google Authenticator
- Entrust

这种额外的安全措施日益普及，有助于应对密码疲劳所造成的安全缺陷，例如一次性密码不能写下来，它只能使用一次，然后就失效了。

尽管可以为内部管理的系统实施这种解决方案，但是SaaS提供商并不提供现成可用的多因素验证。如果提供的话，将会是需要单独管理的双因素验证，这虽然可以增强安全性，但仍是一种IAM孤岛。



F5云联合解决方案

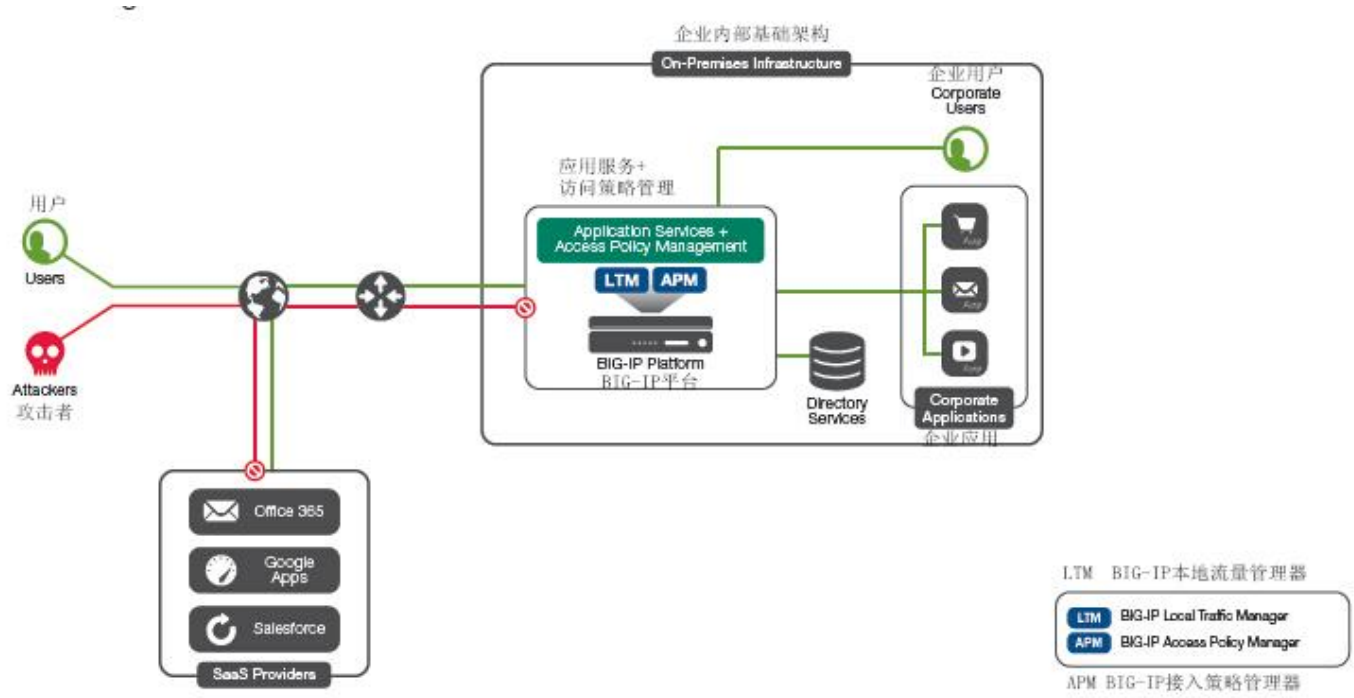
技术解决方案

F5云联合架构可以同时满足这两种需求。它使用安全性断言标记语言（SAML），这是一种基于XML的开放标准数据格式，用于在各方之间交换验证和授权数据。SAML技术无需管理不同SaaS提供商之间的独立用户账户。SAML所解决的最重要的因素是网络浏览器单点登录（SSO）。

此外，F5云联合架构支持部署更加强大的授权解决方案，包括双因素验证、IP地理位置执行以及设备检测等。

F5 BIG-IP®本地流量管理器™（LTM）和BIG-IP®接入策略管理器®（APM）共同提供所需的平台，以支持：

- 企业专用IAM系统与外部SaaS提供商之间的SAML通信
- 对使用BIG-IP设备访问所有系统的所有用户进行一致的多因素验证。



F5云联合架构

业务优势

通过实施F5云联合架构，企业能够：

- 跨SaaS应用实施SSO，消除密码疲劳的根源。
- 在所有系统中执行一致的安全策略。
- 降低启用和注销访问账户的管理成本。
- 降低复杂性并提高生产力。
- 充分利用SaaS的优势，同时更好地管理安全风险。

结束语

以技术孤岛形式运行的孤立系统极大地妨碍企业提高生产力和安全性。它们限制了企业快速响应运营需求的能力，并破坏了经验证的可信安全策略。F5云联合架构可消除SaaS访问孤岛，增强安全性，提高生产力，并支持安全地采用SaaS模式。

F5 公司北京代表处
地址：北京市朝阳区建国路 81 号华贸中心 1 号写字楼 1708 室
邮编：100025
电话：(+86) 10 5643 8000
传真：(+86) 10 5643 8100

F5 公司上海代表处
地址：上海市卢湾区湖滨路 222 号企业天地 1 号写字楼 1119 室
邮编：200021
电话：(+86) 21 6113 2588
传真：(+86) 21 6113 2599

F5 公司广州代表处
地址：广州市天河区珠江新城华夏路 10 号富力中心写字楼 1108 室
邮编：510623
电话：(+86) 20 3892 7557
传真：(+86) 20 3892 7547

F5 公司成都代表处
地址：成都市滨江东路 9 号香格里拉中心办公楼 18 层
邮编：610021
电话：(+86) 28 6606 5210
传真：(+86) 28 6606 5211

Solutions for an application world.