IT管理研究、行业分析和咨询

Tivoli. software

设计成就安全:在当今的信息系统中打造基于身份的安全性

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)
白皮书
供IBM使用
2010年3月

目录

执行摘要

长期以来，企业一直将它们的IT投资主要用在新型创新和能力扩展上。但随着数量上让人震惊且不断增加的IT安全事故的呈现，企业还必须在信息安全和IT风险管理上进行类似的战略投资。

大部分组织都投资部署了可加强其环境安全性的工具和技术，以及专注于保护数据本身的技术。但如何实现内置安全性？

如何实现这样一种方法，它据称不会对最新的威胁做出反应，但会建立一个将风险控制融入其核心结构中的更强大的环境？

当今的身份和访问管理技术不仅为此问题提供了有效的答案，它带来的价值还超越了单独的风险控制。可将身份更大部分组织投资部署了可加强其环境安全性的工具和技术。但如何实现内置的安全性？

直接地整合到业务功能中时，IT可交付针对个人进行了更精确调优的各种服务 – 让企业可充分利用在其他时候可能失去的机会。这为其他依赖于身份的安全性和策略控制技术提供了补充，还增添了一种全面的安全性管理方法。其他领域很少提供这样一种直接整合到环境中的业务优化和风险管理组合。

在本文中，ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™)分析师分析了当今直接在信息系统中构建安全性的机会所带来的安全挑战，以及实现这种更主动的方法且更细粒度的身份和访问管理技术的作用。作为一家著名供应商的示例，我们重点展示了IBM，它提供了丰富的身份和访问管理功能，而这些功能是在所有现代IT系统中整合了安全性的庞大安全产品组合的一部分。业务专业人士将全新地认识到，当今的访问管理功能不仅加强了环境对愈加严峻的威胁的防御，还直接在IT中融入了业务价值。

为IT的快速发展保驾护航

最近几年一直不缺乏IT方面的变革。在10多年中，Web已从一种创新演变成一种重要的业务工具。Web本身已变得非常强大且具有很强的适应力，而Web服务等概念也正在改变IT和面向服务的架构(SOA)的实现与整合。虚拟化技术的激增已使IT功能的提供变得更加灵活，让信息系统从许多传统的物理束缚中解脱出来，优化了IT资源的利用率。这进而创造了进一步扩大IT价值的新机会，而云计算等概念使（企业内外的）服务提供商能够按需同时向大量客户提供IT功能。

但是，当创新的速度超过IT安全风险的管理时，会发生什么？组织常常采用新功能来利用新机会并扩大管理范围。但新技术常常会带来新风险，而且如果未能有效地解决这些风险，它们可能在潜在的威胁变为现实时产生重大的影响。

这一形势的证据不胜枚举，而且这些证据都举足轻重。依据Privacy Rights Clearinghouse[1]，单单在美国，自2005年初至今就已有超过3.45亿条个人记录涉及数据破坏，全球的总数肯定要高得多。这已引起全球的组织对可阻止由安全漏洞导致的敏感信息丢失的技术产生巨大的兴趣，如数据授权管理和数据丢失防御(DLP)。

但企业是否应从这里开始解决此问题？看看一下报告:在2009年Verizon Business Data Breach Investigations Report[2]中，身份验证和访问控制的缺陷与漏洞占前5类黑客破坏中的[3]类。再看一看:当Open Web Application Security Project (OWASP) 2007年更新它的前10大最严重的Web应用安全性风险3时，“破坏的身份验证和会话管理”排名第七。而在2010年的OWASP Top 10[4]更新的第一个“版本候选者”中，此类别上升到了第三位。

企业必须重新认识到，企业防御的前线是身份和访问管理(IAM)。它是确定谁有权访问什么的基础技术，没有它，数据授权管理等战术几乎没有实施策略的参照点。

许多组织明显没有认识到随意实现的身份和访问控制使他们面临着安全暴露的风险，或者甚至没有足够严肃地对待风险。

而且，许多组织明显没有认识到随意实现的身份和访问控制使他们面临着安全暴露的风险，或者甚至没有足够严肃地对待风险。一些案例（如2009年照片共享站点RockYou.com上维护的3000多万个密码被破坏）表明，不仅很多站点需要更好地保护用户凭据，而且简单、容易猜测的密码仍在大量使用 – 表明甚至最基本的访问控制策略的实施都失败了。

企业必须认识到这些事实。技术创新的步伐继续在加快，而且在面向服务的架构和云计算等IT部署和交付替代方案的推动下，对更有效的访问控制的需要正成为最首要的需求。业务不能再认为可通过累积越来越多的防御工具来“添加”安全性。当今它必须“内置”到系统中，而且战略性的身份和访问管理方法是这一哲学的主要推动力。

但其价值并不仅限于此。将身份与信息技术相链接，还为企业带来了全新的机会。业务信息系统可更迅速地响应用户的请求，为他们提供最有吸引力的信息，以及在针对特定的个人时最可能成功的机会。很少有其他技术领域可提供这种风险管理与业务优化的组合，这让当今的身份和访问管理技术成为组织可做出的最佳IT投资之一。

1 http://www.privacyrights.org/ar/ChronDataBreaches.htm
2 W. H. Baker et al，2009 Data Breach Investigations Report，Verizon Business，2009年
3 http://www.owasp.org/index.php/OWASP_Top_Ten_Project
4 http://www.owasp.org/index.php/File:OWASP_T10_-_2010_rc1.pdf

设计成就安全

将安全性内置于信息系统中的理念可能并不新鲜 – 但它可能需要转变IT的保护方式，帮助企业更高效地运营的思维。许多组织拥有大量防御性的工具和技术，它们是通过不断向环境中“添加”安全性而积累起来的。在监视环境中的潜在威胁和防御方面，这些工具仍占有一席之地。但它们更多地归类为安全性管理的“响应”方面。

将安全性内置于信息系统中的理念可能并不新鲜–但它可能需要一种思维转变。

另一方面，内置的安全设计所代表的不仅仅是安全性等式的“主动”一端。它不仅需要识别当今新兴的IT和信息保护方法中的风险，还需要直接在IT系统中减轻和管理这些风险的途径。

当今的身份和访问控制技术大大扩展了过去直接在IT中构建安全性的方法，可保证在现代信息架构的各个组件中更加一致地实施策略。访问管理对任何业务变革都至关重要，但它是定义谁可在何种环境下访问哪些信息的策略所不可或缺的。因此，监视并实施控制谁以及个人和小组如何访问或拦截敏感信息的细粒度策略的技术为IAM提供了补充，但必须在DLP工具可将策略与合适的信息访问和使用相匹配之前建立身份和访问控制。

内置安全性:深入剖析当今的IAM功能

DLP对身份管理的补充关系，只是当今IAM技术如何将基本的访问控制概念升级为可部署到所有现代信息架构中的访问保障的一个示例。为了演示这个能力范围，请考虑一个典型的现代应用:

一个需要身份验证的会话常常首先建立一个安全套接字层或可信层安全性(SSL/TLS)连接，为在端点与应用之间交换的信息提供机密性。(这种连接级安全性也可扩展到应用的其他组件)。

身份验证通常在用户提供他们的登录名和识别凭证(密码通常是最简单的情况)时发生，它建立用户的身份。经过验证后，当一个事务在一个整合系统中执行时，可根据需要将用户已验证的信息提供给应用的每个组件。例如，身份联邦技术会传递对每个组件必要(仅对每一步有必要)的身份验证信息。用户名等信息或任何其他个人可识别信息可被抽象化，这有助于确保个人数据具有更高的安全性和隐私。这些技术常常依靠Web服务来摆脱对底层系统的依赖，并且可随意移动身份验证信息。

虽然身份验证和联邦可识别用户，而访问控制技术可针对策略来评估经过验证的访问请求，从而保护访问目标。这意味着可针对特定环境（如各个OS平台、应用、服务器或大型机）或特定需求（如对高度敏感的根或管理员访问的更细粒度控制）来定制访问控制。

就像联邦会抽象身份信息一样，也可抽象访问策略控制，从而更好地满足系统需求，将访问控制转换成为身份验证Web服务提供补充的细粒度权限，或者将访问控制与“单一登录”技术链接来统一身份验证流程。这在调整访问控制，以满足特定环境需求方面提供了高得多的灵活性。

随着事务继续执行，它们的状态会更改。事务状态信息可通过一个应用系统，利用与身份和授权信息相结合的会话管理技术来传递，提供执行事务每一步所需的数据。此信息也可通过Web服务传递。

当今的技术摆脱了对底层系统的依赖，可随意移动身份验证信息。

与当今的信息系统交织在一起的Web服务的灵活性，凸显了专为SOA安全性和策略管理而定制的系统的作用。SOA安全性技术也可验证Web事务的内容，这可能对确保事务完整性至关重要。验证可能包括验证Web服务中SOAP消息的结构和格式等因素。但是，它可能更进一步，包含消息签名的加密验证、敏感内容的加密和解密，或适合某个事务点的其他策略方面的执行。执行这些重要功能的系统也可提供很高的性能，提高现代应用系统的响应速度。

“实时”安全性的优势

由于身份对保证策略的实施非常重要，所以身份的建立很关键。这就需要注册用户并验证身份凭据，让用户在访问授权的服务时可得到正确的验证。用户配备的技术可满足大量策略的需求，提供可简化企业中这些关键流程的工作流。

但面向公众或可能庞大且多样的客户群的应用又如何呢？此处“按需”注册（例如，常常是以前不知道的客户）必须实时执行，以方便应用实现其业务用途。此功能的响应速度对实现企业到用户(B2C)应用在当时当地满足客户期望至关重要。在线客户对应用性能的敏感度以秒来计算，这是众所周知的，而且应用无法承担让他们执行单调的注册过程的风险。在利用率峰值期间或应用负载的周期性变化时尤为如此，这时必须优化所有应用组件来快速响应需求。

实时响应的注册和身份验证可帮助解决这些以及其他挑战。例如，一个验证用户一次（但不会在事务的剩余步骤中重新验证）的系统可能成为一个攻击目标。如果应用不会在流程晚期重新验证用户，可在一次性验证后将自身插入这类事务中的攻击者可能利用用户的凭据。实时验证可在整个事务中重新验证用户，帮助消除这些安全性差距。这种验证可能对用户透明，不需要因为复杂的安全性管理来牺牲客户友好性。

实时用户注册和身份验证也提供了超越安全性的业务收益。它可为应用带来更好的个性化，自定义门户的显示，并在识别用户后提供用户最感兴趣的信息。通过将身份链接到购买偏好等信息，它也可帮助企业应用更好地服务客户，调优用户看到的内容（如通过业务分析而优化的购买建议）。这表明身份技术也可帮助提高应用的业务绩效。

一种综合方法

数据和应用安全性是一个不断变化的领域。因此，组织必须认识到帮助防御不断变化的威胁领域的技术（如入侵防御和漏洞评估）有何作用。这些技术也可帮助组织保护网络、数据和应用环境，以及评估IT环境中的已知漏洞。应用的入侵检测和预防可通过专为Web环境设计的网络防御来进一步增强，而数据库监视和安全性系统可帮助确保对拥有数据本身的资源的掌控。

值得注意的是，为SOA环境提供安全保障和高性能的设备也可防御Web服务被利用。这为网络中的系统和应用级防御提供了直接补充，为SOA事务提供了消息级保障。

威胁领域中的不断变化意味着，必须依据当前威胁来评估应用系统的漏洞。应用的漏洞管理是Web安全性评估工具的目标，这些工具帮助组织理解已部署的应用中所暴露的风险，而源代码安全性分析工具可帮助您识别并修复开发和维护过程中的应用安全性问题。

长远观点:身份和策略生命周期管理

所有这些功能为架构师和开发人员提供了一组强大的工具，从一开始就在IT系统中建立信心。但是，同样重要的是不断维护这种信心。

例如，想象一下个人角色的变化过程。在组织内，个人的工作职能会发生变化，不同的职能在访问信息系统时需要一组不同的特权。具有较高敏感度的资源可能适合在一个角色中访问，但不适合另一个角色。一位客户或合同工可能在某个时刻成为员工，这就需要更改IT中的访问特权。

这些功能为架构师和开发人员提供了一组强大的工具，从一开始就在IT系统中建立信心。但是，同样重要的是不断维护这种信心。

再想象一下，员工也会离开组织，当然原因很多。当他们离开某个角色时，必须转移或终止该角色中的特权。当他们离开组织时，他们以前能访问的信息的敏感度会成为一个安全因素 – 这再次显现了身份和访问管理与数据丢失防御之间的补充关系。诚然，组织可能认识到需要在员工更改他们的状态之前保护这些信息，监视和实施策略来控制在哪些条件下访问哪些内容是可接受的和不可接受的。

对于IAM，这些需求对应于需要一种生命周期方法来进行身份管理。角色管理可帮助组织识别给定角色的合适特权集，而用户管理功能可帮助组织定义不断管理这些身份变化的策略和流程。

这些同样的技术也应适用于访问目标。在访问管理生命周期方法中，组织评估信息资源的访问特权并在需要时细化它们。必须常常更改保护整个组织的访问控制来适应新信息系统的引入或这些系统中的变化。这些更改也必须针对用户中的身份和角色更改而进行调整，确保通过适当调优访问控制来满足用户和策略的需求，从而满足企业的需求。

当按需注册和实时身份验证“在云中”运行时，组织应有能力维持对内部安全策略的控制。

在这些生命周期中，组织需要监视访问情况，在问题和潜在的滥用出现时识别它们。举例而言，这种监视和报告功能可能对遵守制度不可或缺，但它还通过指出可用作更严重问题的早期迹象的潜在异常，支持更有效的安全性管理。

一些案例中涉及到未采用这种综合访问监视和生命周期管理方法的情况，如2008年发生的法国银行Societe Generale的Jerome Kerviel的案例，对后端办公室功能的了解和从前端办公室交易职位对访问权利的滥用为

Kerviel提供了访问交易系统的能力，使他能够隐藏由未授权的交易活动导致的巨大损失。该事故表明，身份和访问管理可直接实施职权分离来控制这些风险，对破坏访问控制的尝试进行早期检测有助于预防重大损失的出现。

服务选项:保护“IT即服务”

这些示例表明，可用于保护现代业务系统的功能范围丰富多样 – 但这种功能丰富性也可能让人却步。主要寻求优化业务绩效的组织也需要控制其IT开发和维护成本，特别是在资源受限时（并且这一需要很少拥有比当前经济气候下更高的价值）。随着组织变得对安全问题越来越敏感，它们还认识到需要可靠的专业技能来将安全性内置到业务技术中。

这就是以服务的形式提供IT具有很高呼声的地方。虚拟化和Web服务等技术提供的灵活性让提供商能够将功能公开为已整合的服务。这样更容易用一种更灵活的整合方法来使用和创建系统组件。云计算更进一步，可将完整的系统传输给服务提供商（无论是组织内部还是外部的提供商）。这允许组织卸下许多开发和维护负担，同时仍然获得现代技术的收益。

在风险管理上，必须智能地采用这些新技术。例如，通过各种服务创建IT需要成功的方向，在保证安全性方面，这就意味着策略。组织必须有能力定义安全性策略来指导服务的安全整合、部署和使用。

同样重要的是组织可在面向服务的环境上运用和保持的控制水平。例如，当按需注册和实时身份验证等运行时元素“在云中”运行时，组织应有能力维持对内部安全性策略的控制。这突出了为外部或托管服务制定策略的内部工具的价值。

IBM:实现“设计成就安全”

作为向所有规模的组织（包括许多全球最大型的组织）提供信息技术的领先提供商，IBM已成为许多组织将这些安全功能直接构建到现代业务系统中时值得信赖的合作伙伴。

IBM定义和配备IT中的用户身份和角色的技术，得到了可对敏感信息资源的访问进行控制的广泛功能的补充。从SOA安全性和数据授权的定义开始，IBM Tivoli Security Policy Manager让组织能够管理SOA安全性和细粒度授权策略的整个生命周期，从创作和发布策略到定义它们在信息系统中的实施，以及根据需要更新策略。Tivoli Security Policy Manager实现了跨复杂系统的多个组件的集中策略协调，集中数据安全性策略控制，提供更一致的策略定义和实施。它还为组织提供了一种方式来维护对分布式运行时服务的内部控制，这些服务可能位于组织内部和外部的托管或云环境中。这有助于确保对服务具有更高的控制水平，无论如何托管服务或托管在何处，消除了采用可减少IT管理负担的面向服务方法的重要阻碍。

IBM已成为许多组织将这些安全功能直接构建到现代业务系统中时值得信赖的合作伙伴。

为策略的定义和管理提供补充的是IBM Tivoli Access Manager产品，它们在运行时、在访问目标（如FileNet、Cognos和Microsoft SharePoint）时实施各种强制策略。Tivoli Access Manager家族的丰富功能提供了跨各种平台和应用的用户身份验证和授权，以及对操作系统环境的特权用户访问。

针对电子商务的IBM Tivoli Access Manager为许多重要的企业业务应用提供了基于角色的访问策略实施。它提供了Web环境的访问控制，包括用于IBM WebSphere和门户环境的Java安全性。而且它将大型机z/OS支持扩展到了WebSphere，让WebSphere环境中的用户能访问关键的大型机应用、数据库和资源。

许多组织面临着简化对大量应用和资源进行访问的挑战，每个组织常常都提供了其自己的访问控制工具。这需要个人记住大量登录名和密码，这可能降低总体安全性。IBM Tivoli Access Manager for Enterprise Single Sign-On提供了使用单个登录名访问多种资源的能力，同时提供了对所管理的每个目标资源的细粒度访问控制。这通过单一密码为用户提供了对广泛的企业应用、Web和遗留环境、桌面和网络资源的更加简化但安全的访问。

Tivoli Access Manager for Enterprise Single Sign-On还简化了登录过程，自动化了通常在身份验证时执行的常见任务，包括应用登录、驱动器映射、应用启动、单一登录、导航到首选屏幕、多步登录和其他典型任务。这不仅有助于让单一登录变得更加无缝，还在自动执行策略时变得更加安全。它可在一个工作站上调整任何用户的身份验证和登录顺序。也可在工作站空闲或无人值守时自动注销用户，在需要时满足此功能的合规性要求。

这些功能为与许多系统整合的访问控制提供了补充。例如，IBM大型机常常受到了一些设施的保护，如著名的资源访问控制设备（Resource Access Control Facility, RACF）。RACF通过验证已授权的系统用户、分类和保护系统资源、控制访问方式，以及记录和报告授权和未授权的访问尝试，为保护大型机环境提供了长期的帮助。当今，Tivoli Access Manager家族提供了将企业级访问管理与RACF整合的能力，这让对大型机资源的访问变得更加无缝，甚至在整合Web或其他应用时，同时确保全面的安全性策略实施。

将这些功能编织在一起的是IBM Tivoli Federated Identity Manager等技术，它支持基于标准的身份联邦，而后者将身份和身份验证从对复杂应用或SOA环境中任何一个系统的依赖性中抽象出来。它支持用更细粒度的方式，根据需要在事务的每一步中充分利用身份验证信息。它可为各个事务流程提供确保获得授权而不暴露个人信息所需的信息。这有助于确保整个事务中的安全性，改善对寻求利用系统中一次性身份验证（其中从不会重新验证授权）的威胁进行防御。它还让组织无需构造高风险的架构，例如这样一种架构:其事务依赖于一个系统“信任”另一个系统，而不会将安全性内置于当今的方法中，以实现更可靠的身份和访问管理。Tivoli Federated Identity Manager对用户自行注册的支持对B2C应用具有很高的价值，提供了能够以极低的用户或客户影响扩展业务范围的按需注册。

将安全性内置于现代环境中的意义不仅仅是整合合适的身份验证与访问控制。它还意味着“深度防御”。

一旦在环境中内置了一种综合的身份和访问管理方法，IBM解决方案就可支持保持最新安全状态的能力。整合到IBM产品组合中的身份生命周期管理功能支持组织管理人员、合作伙伴和客户的移动和终止。它提供了角色评估和角色特权变更管理，使访问控制保持最新，而IBM监视和报告功能提供了确保适当管理访问控制所需的可视性和洞察。

将安全性内置于现代环境中的意义不仅仅是整合合适的身份验证与访问控制。它还意味着“深度防御”，其中架构师会认识到威胁领域中的不断变化。全面的IBM安全产品组合支持向当今的环境提供这一保护水平所必需的警戒性和防御型功能，提供了支持更全面的方法的入侵检测和防御、SOA安全性、数据库监视和网络Web应用保护技术。IBM还提供了通过漏洞评估和更安全的开发来加固应用的应用安全性技术，帮助开发人员将安全性内置于当今的环境中，超越身份和访问控制。

随着组织越来越多地寻求面向服务的IT交付选项，IBM也认识到了这一战略方向，并且有望推动其增值客户采用它的战略来实现面向服务的方法。该公司已提供了Web应用漏洞评估功能作为一项托管服务，为IBM声名卓著的托管安全性服务提供补充并为组织带来丰富的选择。在用于远程或托管服务安全性策略内部管理的Tivoli Security Policy Manager等资产的补充下，IBM为组织提供了丰富的选择来将基于服务的选项与内部偏好相整合，让客户能够制定最适合业务和策略需求的方法。

EMA前景

我们不可能过分强调一个错误的严重性，审视这个长长的身份和访问管理功能列表，而只需将它视为一连串的创新。必须要理解的是，当今的身份技术让系统比过去安全得多，只要这些技术得以正确实施。

众多遗留系统仍在使用陈旧的技术验证用户是否具有他们所声明的身份，它们依靠简单、一次性的身份验证技术，仅仅因为一个机器“信任”另一个机器，就允许后端系统（其中常常包含敏感数据）毫无疑问地接受来自“前端”HTTP服务器的连接。攻击者可依靠像这样的低级复杂性来攻击IT系统中的架构缺陷。

众多遗留系统仍在使用陈旧的技术来验证用户是否具有他们所声明的身份。当今更细粒度且分布式的身份和访问管理方法有助于填补这些风险空白。

当今更细粒度且分布式的身份和访问管理方法有助于填补这些风险空白，使系统设计人员能够将安全性构建到当今更复杂的IT环境的每个方面中。借助它得到全球最大型且最严格的组织认可的业务技术创新方面的悠久历史，IBM已证明了它对此方法的承诺。这一传承在IBM的身份和访问管理产品组合中显而易见，从大型机环境的访问控制开始已进行了30多年的创新。

当今的身份技术已彻底变革了细粒度地控制身份和策略来满足特定用途，同时保护个人隐私的方式。它们还变革了可靠共享信息的方式，统一了一种更加无缝且更深度整合的方法，可扩展到组织中的许多资源。它们可在事务中的每一步之后提供细粒度的身份验证和授权，全面增强安全性、隐私和策略控制。而且它们可对用户透明地提供这种一致性，还提供了注册用户和管理访问的技术来帮助业务应用更迅速地响应业务需求。

此功能不仅在当今是必需的。攻击代码、公开的漏洞和成功的攻击中的趋势很明显:对手比以往更加强大。当今的系统必须建立一定的安全性水平来匹配它们提供的创新，从而减轻当今更严重的风险。

关于IBM

IBM提供了一个完备的安全性、风险和合规性管理解决方案组合，可帮助组织应对保护动态基础设施的各种挑战。这些产品提供了丰富的安全性功能，解决了IT环境中的人员、流程和信息风险问题。

IBM在安全性上的领导地位是其庞大的解决方案组合、大量服务专业人员网络，以及活跃的业务合作伙伴社区的自然产物。IBM是开发和支持开放标准的积极拥护者，而且IBM的安全性解决方案提供了广泛的平台支持。IBM是一位值得信赖的合作伙伴，已帮助各个行业的数千家组织实现了安全的服务，同时减少了风险并改善了整个IT领域的IT安全性与合规性。

IBM让组织可构建一个端到端的安全性基础，帮助保护用户、数据、应用和平台。组织可利用IBM丰富且深厚的经验，帮助它们促进服务质量改进，同时最大限度降低成本并管理风险。IBM Security Framework为解决基础设施不同安全性关注领域的行业解决方案需求提供了基础。IBM在每个关注领域都拥有可独立实现的解决方案，这些解决方案也可与一个专为满足组织特定需求而设计的集成、整体架构相结合。

关于Enterprise Management Associates, Inc.

Enterprise Management Associates (EMA)创办于1996年，是一家著名的行业分析公司，致力于“超越表面”并提供跨所有IT管理技术的深入洞察。EMA分析师利用实践经验、行业最佳实践洞察和当前及计划的供应商解决方案的深入知识独特组合，帮助客户实现其目标。如需进一步了解面向企业IT专业人员和IT供应商的EMA研究、分析和咨询服务，请访问www.enterprisemanagement.com或在Twitter上关注EMA。

企业总部:

5777 Central Avenue, Suite 105

Boulder, CO 80301

电话:+1 303.543.9500

传真:+1 303.543.7687

www.enterprisemanagement.com