jamf

白皮书

Conditional Access：超越基于边界的安全措施

现代化工作模式和新一代安全措施

数十年来，组织机构一直在他们的公司外围构建“防护墙”，利用网络边界作为第一道防线。但是随着工作空间越来越多样化，安全边界也必须发生改变。创建网络并使用防火墙对其进行防护，这样的理念已无法再满足需求。现在，是时候重新考传统的、基于边界的安全模型了。

所有办公室职员早上九点上班、下午五点下班的时代已经一去不返。人们不再像以前那样，需要从周一到周五都在办公室内工作。

他们利用适合自己工作的时间，在家里、咖啡厅、酒店大厅或工作现场开展工作。通过这种方式工作时，他们不仅需要访问公司资源，还需要占用“传统”上班时间以外的时间。

新型的“工作空间”定义非常广泛，现在，人们需要能够跨不同的设备、应用程序和地点来使用工具和数据。

因此，出现了云。

建立在防火墙之外的云服务，是此新型、以员工为核心的灵活工作环境的构建基块。这些服务提供了更加灵活的信息访问方式，方法是允许用户从任何机器登录任何网页或应用程序并访问信息。现代化的云服务让组织机构可以自动开展运营，而所需的成本低于这些服务以往的成本。

此工作模式转变以及对云的依赖比以往任何时候都要显著，正如 Microsoft 高级产品经理 Vladimir Petrosyan 在 Jamf Nation User Conference 2017 上的演讲中所述：

- 85% 的组织机构在云中保存高度机密信息
- 80% 的员工使用未经批准的 SaaS 应用程序来开展工作
- 41% 的员工表示，移动业务应用程序改变了他们的工作方式

随着越来越多的业务希望通过这种不断变化的形势来推动自己的改变（这种改变之前由影子 IT 来推动），安全措施以及安全措施保护用户、设备和应用程序的方式也必须相应地进步。由于很多关键应用程序和服务仍然需要使用本地基础结构和服务器，组织机构中所使用的基于云的工具实际上是由内容和协作平台、云办公套件和使用能够在设备之外存储数据的移动设备来推动的。实际上，不仅员工在防火墙之外工作，而且他们所访问的大部分应用程序和数据也在云中。更不用说很多人都尝试通过自己的个人设备访问组织资源。此外，还有越来越多的公司开始将自己的基础结构移动到云中，这也需要强大的安全措施来确保安全访问企业服务。因此，很多公司都在寻找新的、更好的方式来保持合规性和安全性。

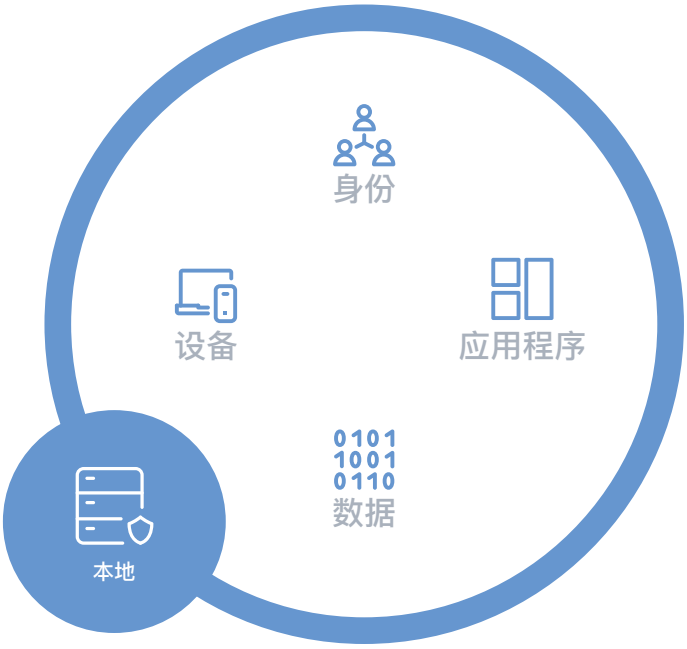
这种尝试的关键在于，在支持员工达到最佳工作效率的同时，让宝贵的公司数据得到保护。

当今企业中的安全措施转变

安全边界已经发生了变化。创建网络并使用防火墙对其进行保护，这样的理念已无法再满足要求，因为设备和数据已不在本地进行托管。人们现在可以使用世界范围内的设备，可以随时随地直接访问云服务、电子邮件应用程序和其他可能高度机密的企业资源。

以上是传统安全模型用来在防火墙内部保护边界的措施示例。

然而，这仅仅是我们的同事及其设备所访问内容中的一小部分。在防火墙之外跨多种设备的云存储、生产力应用程序将成为新趋势。虽然我们目前所依赖的安全措施具有普遍适用性，但如果组织机构继续使用这种基于边界的安全措施模



传统的安全模型

型，将很容易受到攻击。

组织机构不再使用传统的本地身份管理方式来提供服务访问权限，因为大多数的设备和资源用户都需要转为使用云。为了减少潜在的安全漏洞并保证用户的生产力（无论他们身在何处），都需要重新考　传统的、基于边界的安全模式，其中的身份需要像我们访问的云服务那样可以在全球访问并且具有充分的灵活性。

现代的安全模型

设备和访问权限：安全措施层

安全措施和身份验证有三种常用的方式，每种方式都有其自己的缺陷:

- 基于设备的安全措施
- 基于用户的安全措施
- 多因素身份验证

基于设备的安全措施

这种安全措施方法可以应用到托管的企业设备或不符合组织机构安全策略要求的托管设备。当能够通过钓鱼软件或“幸运的”猜测来获取这些凭证时，这种安全措施模式则难以保护设备。此外，如果设备未托管 (很多设备都是这样) ，那么设备将不再安全，也不符合组织结构的标准。

基于用户的安全措施

这种安全措施层可以应用到通过用户的用户名和密码进行访问的设备。但是，如果可以访问企业服务和资源的未托管设备或计算机丢失或被盗，或者用户的凭证被恶意获取，则整个网络都处于风险之中。

多因素身份验证

多因素身份验证，此安全措施层仅在用户成功提供多条单独的验证信息之后才能为其授予设备和公司资源的访问权限。个人可识别的凭证示例包括：

- 您知道的信息 (密码)
- 您具有的信息 (安全令牌)
- 您的特征 (指纹)

虽然要求提供用户名或密码以及辅助的物理身份验证方法 (例如 RSA 令牌) 的措施看起来是十分安全的用户验证方法，但组织机构仍然缺少工具来支持用户获取环境设备可以提供的丰富内容，并且没有适当的方法来保护众多的用户案例、用户、地点以及随之产生相关事项。

以上论述旨在说明，安全的用户或物理身份验证仍然不足。组织机构必须要求同时提供这两项内容和其他信息，同时又必须保证不损害最终用户体验。

身份是全新的边界

有很多供应商已经转而帮助管理服务的身份和访问权限，包括 Centrify、Duo Security、Microsoft、Ping Identity、Okta、Sailpoint 和 Salesforce。其中的很多工具可以与现有身份验证基础结构 (例如 Active Directory) 配合使用，并利用各种协议 (例如 Oauth、SAML 和 OpenID) 将这些身份扩展到云服务。

身份在所有用户的设备上具有普遍适用性，其可靠程度超越了基于用户、设备或令牌的简单安全措施。将身份管理融入到安全管理流程是在移动的云计算界创建安全环境的关键。

根据 Microsoft 企业副总裁 Brad Anderson 的说法，“安全性破坏和攻击已经达到了一种非常精细的水平，并且扩展速度非常之快，仅仅依靠人类思维和人类的双手已经无法阻挡。”

组织机构需要一套完整的功能来帮助他们了解身份风险、设备风险和应用程序风险，从而最终达到这样的目标：只有受信任的用户才能在受信任的设备上使用受信任的应用程序访问数据。

通过基于身份的安全措施，Microsoft 在用户访问 Microsoft Office 365 时，根据 Azure Active Directory (AD) 对用户凭证进行身份验证。如 Anderson 所述，这种身份验证每天需要执行 150 亿次。

全世界超过 90% 的用户都使用 Active Directory 作为企业身份的本地授权来源。对于很多用户来说，Azure AD 就是云端的企业身份授权来源。所有基于 Microsoft 技术构建的程序，同时也是构建在 Microsoft 云中的 Azure AD 之上的。

Microsoft Enterprise Mobility + Security: https://www.microsoft.com/en-us/cloud-platform/enterprise-mobility-security

安全措施漏洞的解决方案

在 2017 年的 Jamf Nation User Conference 上，Anderson 为现代安全措施中的漏洞提供了新的解决方案。

“Jamf Pro 在 Azure Active Directory 中使用 Microsoft Workplace Join（工作模式接入）功能，将注册了 Jamf 的 Mac 电脑接入到企业中其余属于企业或个人所有的全部设备。工作模式接入完成后，Intune 即可在其上进行报告，方式与在已经注册到 Intune 的设备中进行报告的方式相同。”他继续说道，“这意味着企业在为企业资源提供访问权限时，不仅基于用户的凭证，还基于 Mac 电脑的合规性。这就是我们所说的 conditional access。

Jamf Pro 是 Apple 设备管理的标准，可以在设备上强制执行各种策略，以便它们可以利用 EMS conditional access 来访问 Office 365。托管到 Jamf 的 Mac 电脑只要满足了 Intune 设备的合规性要求，即可将工作模式接入到 Microsoft 云，这些合规性要求可以根据每个组织机构的需求进行定制。计算机的数据进入云之后，Microsoft Intune 和 Enterprise Mobility + Security (EMS) 即可与 Jamf 进行全面集成来管理这些设备。

如果未托管的 Mac 请求访问电子邮件或其他云服务，IT 可以从 Jamf Pro 启用由用户发起的注册流程，以确保在授予访问权限之前对不安全的或未托管的设备进行管理。

可以通过 Intune 来定义 Mac 策略（例如密码要求），从而让 IT 在整个系统中应用这些策略。Jamf 和 Microsoft 的协作是独一无二的，在访问本地工具方面，其功能已经超越了 Apple 的移动设备管理工作框架的范围。例如，管理员可以创建配置文件来实施和验证密码的强度。这种能力弥补了 Mac 的传统 MDM 选项所提供的现有功能和组织策略之间的差距。

在 Microsoft 验证用户凭证时以及 Jamf 验证设备凭证时，将会运行用户风险分析、设备风险分析（设备是否符合组织的策略要求）以及应用程序风险分析（将使用什么样的应用程序），以确定是授予云资源的访问权限还是拦截访问。

在多因素身份验证无法重点关注用户本身的情况下，这种新型的方法可以进一步验证用户与信息的交互方式，从而使受信任的身份与合规设备中通过了身份验证的用户保持一致。

现在，组织机构可以通过经验证的合规性来获得多因素身份验证的扩展功能：1) 用户名和密码，2) 代码和令牌，以及 3) 设备合规性；现在，组织机构必须提供基于用户、设备和使用场景环境的正确访问权限，这样才能提供当今多设备、多地点工作人员所需的、具有强大适应性和灵活性的边界。

免代理的 CONDITIONAL ACCESS

EMS Conditional Access 是实现这种安全措施水平的关键所在，同时也是能够自动验证与身份、设备和应用程序有关的任何风险的关键所在。

这让 IT 可以控制用户在什么样的条件下可以访问资源。

很多企业移动化管理 (EMM) 提供商都拥有通过代理服务器提供 Conditional Access 的解决方案，以检验　程设备是否有资格通过身份验证来访问保存在组织机构网络边界内部的资源。代理服务器，此服务器可在用户从其他服务器请求访问资源时用作中间桥梁。可用于管理进入网络或离开网络的流量。对于独特的 Jamf 和 Microsoft 协作，则不需要代理。通过这种合作方式，所有要素都与 Azure Active Directory 直接集成，从而成为单一的事实来源，并且设备的合规性也被考　在内，可以用作获取各种服务访问权限的前提条件。这意味着将不存在需要网络配置来确定访问权限的任何中间措施（例如代理服务器），也不存在需要进行维护的附加网络基础结构。这样，可提供能够直接在 Azure Active Directory 中构建的、更加丰富的身份验证体验，同时还减少一个可能发生故障的部位。

企业组织已经接受并认可快速采用 Mac。这也是为什么他们需要一个解决方案来超越基于边界的安全措施，正如他们针对其他设备采取的措施一样。在 layman 的条件中，在信任一个用户之前，必须首先批准发起用户身份验证的设备。

Microsoft 和 Jamf 协作创建了一个专用的解决方案，该解决方案与其基础性 Azure Active Directory 和 Intune 技术堆栈完全集成，让用户的本机体验更加完善，并利用 Jamf 和 Intune 的优势为客户构建了一个完全超越单个组织机构所实现功能的解决方案。

MICROSOFT 和 JAMF 的合作契约

Jamf 和 Microsoft EMS 合作契约提供的自动化合规性管理解决方案，适用于访问应用程序通过 Azure AD 身份验证进行设置的 Mac 电脑。此协作方式利用 Conditional Access 来确保仅受信任的用户使用经批准的应用程序通过符合规定的设备才能访问公司数据。

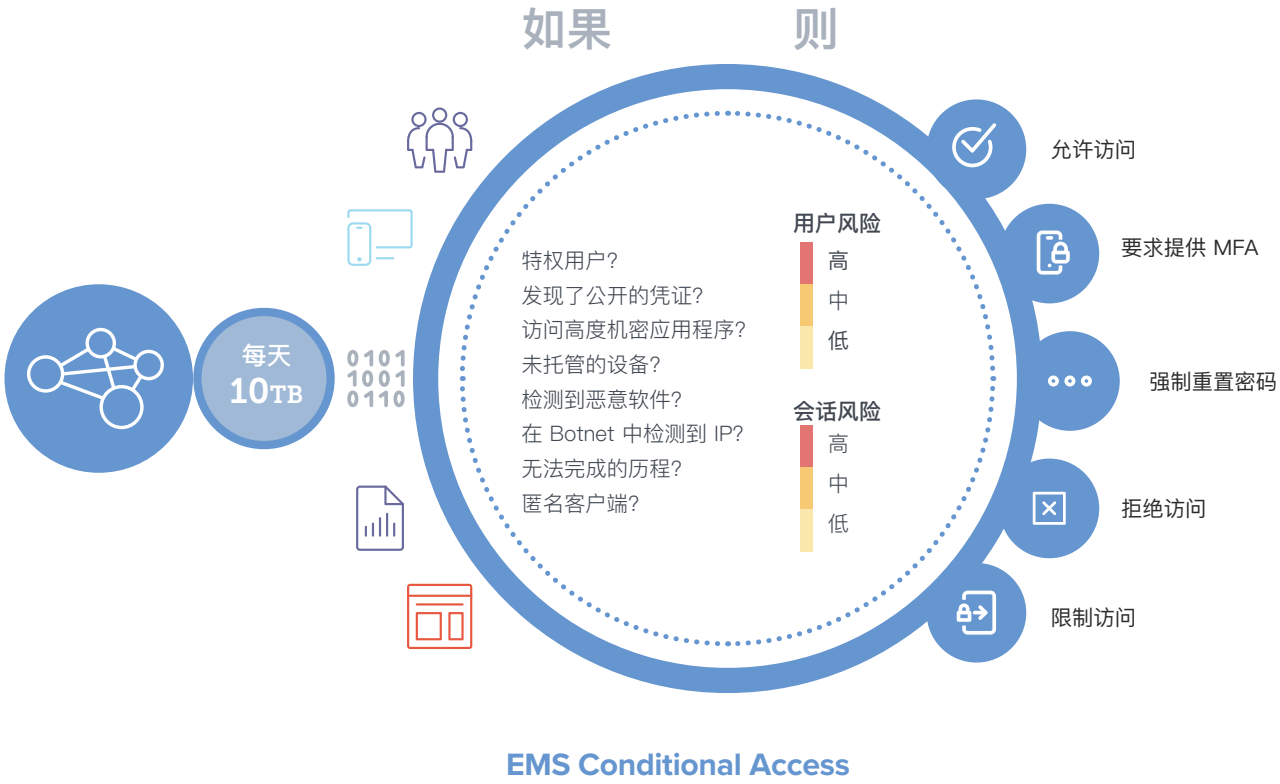
Jamf 和 EMS 共同阻止未获得授权的用户使用设备来访问组织机构提供的指定资源。这些设备可以是个人设备、未托管的设备，或因不符合安全措施策略而在尝试访问企业数据是易受攻击的已托管企业设备。通过要求用户注册用于访问 Microsoft Office 365 以及经 Azure AD 验证的其他应用程序的设备，可以实现这一目标。

该流程之所以不同于其他宣称具备 Conditional Access 能力的供应商，是因为设备不再需要通过代理进行访问。由于不必使用代理，组织机构可以简化设备保护方法。

那么，最终用户体验如何呢？信息量大而简单易用。如果设备不合规但用户尝试进行身份验证和获取访问权限，则其设备上会显示一条消息，提示其不符合某些要求。用户随后可以单击该消息并完成所提供的步骤来解决合规性问题。

该消息可使用户了解到所发生的问题以及设备不合规的原因。如果是密码问题，用户只需要单击“解决问题”然后更新密码使其合规，然后即可获得访问权限。

Jamf 向 Microsoft 提供的信息让安全措施更加　固并且更加智能，而由此产生的管理解决方案也可以带来更加简单的最终用户体验。



EMS Conditional Access

正如 ANDERSON 所说，“用户喜欢，企业信赖”

为了提供现代化、经授权且安全可靠的体验，管理工作流必须与人们的工作方式、工作地点以及所使用工具相匹配。IT 需要以一种自然的方式来集成其保护协议并设置指南，以使得在用户不合规的情况下能够提供一种可使其重新合规的无缝方式，而不会威胁公司数据。

Jamf 和 Microsoft 共同协作，让 IT 通过基于身份的安全措施实现了这一目标。这使得用户不需要经过代理即可访问信息。

数十年来，组织机构一直在其公司外围构建“防护墙”，利用网络边界作为第一道防线，这会使得内部安全措施显得有些落后。数据已经转移到其他位置，世界也已发生变化，而这些现代化解决方案正在处理所发生的变化。

发现安全实践的演变方式，从而让 IT 获得其所需的工具，让用户在其选择的设备保持安全且高效。

更好的安全措施从此处开始

jamf

www.jamf.com

要了解有关 Jamf Pro 如何影响 Mac 和 iOS 管理的详细信息，请访问 jamf.com/zh。