ipswitch

Secure. Control. Perform.

IPSWITCH 白皮书

MOVEit 如何满足数据安全和合规性要求

ipswitch

引言

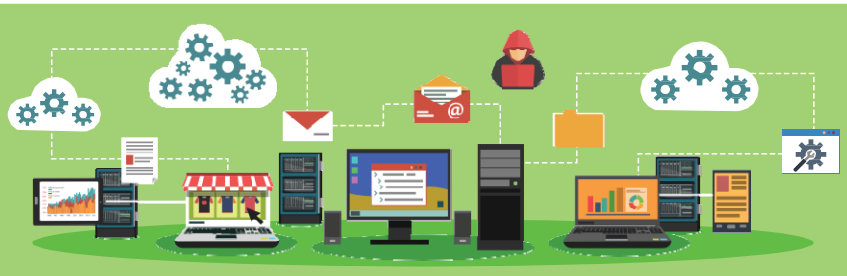
目前没有一个单一而全面的解决方案可以为一个组织解决所有数据保护合规性和保安要求。很多公司都使用不同的系统保护防火墙内的数据。当敏感数据保存在所属组织内时，IT 部门能容易地控制和管理。

那么，当敏感数据要超越防火墙向外传输时，会发生甚么事? 那些敏感数据会变得脆弱、容易操纵、被盗取或在黑市上出售。您的数据可能最终落入非预期的收件人手中，带来数据盗窃和违规的风险。

现在，一个安全可靠的文件传输管理(Managed File Transfer)系统便成为了需要与第三方共享敏感数据的组织的宝贵投资。 一个文件传输管理解决方案可以满足许多安全和合规性要求，同时为 IT 人员提供文件传输活动的控制度、可视性和灵活性。它让 IT 管理层监督涉及把大量数据传输到其他组织、员工、合作伙伴和供货商的日常业务操作。

在这份白皮书里，我们将探讨数据保护法规所要求的七个关键安全控制措施，以及 MOVEit 产品（MOVEit Transfer + MOVEit Automation）的套件如何运作。最后，它将展示 MOVEit 如何超越典型的最低数据保护要求，以确保最敏感数据的安全性、合规性、可视性和控制。

文件传输数据保护



敏感数据一旦处于防火墙外，便会暴露于潜在的盗窃和误用危机当中。

ipswitch

合规性要求

如要确保外部数据交换能安全地完成并符合数据保护的要求，便需要根据以下七个安全要求仔细评估您的文件传输管理解决方案。

安全需求		文件传输控制措施
1. 合规性	→	自动化
2. 通讯安全	→	控制和可视性
3. 信息安全政策	→	信息安全
4. 访问控制	→	验证
5. 密码学	→	密码学
6. 实体和环境安全	→	安全架构
7. 业务连续性安全	→	故障转

现在就让我们深入了解这七项文件传输控制措施，并探讨 MOVEit 解决方案如何全面地满足上述每项安全要求。

自动化

自动化的文件传输操作有许多优点。它既可以减少因未能准时完成 SLA 而导致的收入损失，也可以降低违反数据保护法规要求的风险。

以档案为本的任务和业务工作流程自动化使 IT 人员能够：

- 最大限度地减少维护多个脚本的需要
- 满足服务级别协议（SLA）的要求
- 保持灵活性以适应不断变化的业务情况
- 消除在任何指定时间以人手监视档案位置的需要。

IT 通常依赖脚本处理作为定期传输档案的方式。维护不同员工以不同脚本语言编写的多个脚本是非常复杂的工作，也会降低您处理文件传输工作的能力。如果那位编写文件传输脚本的员工离开了公司，团队能否进行更新或确保效能便成为疑问。更严重的问题是，脚本会变得过时、不能再使用或不安全，并增加数据泄露的风险。

MOVEit Automation 可以助您轻松地安排大部份文件传输工作而无需自定义脚本。简单易用的设置可以让 IT 人员快速创建新任务，然后根据需要随时作出修改。内置的作业调度程序可以在默认的时间间隔内，在档案共享服务器、FTP 服务器或 MOVEit Transfer 内自动传输档案，确保能按需要将档案传送给预定的收件人。

文件传输可以简易地进行设置，定期把作业发送到多个系统，或一次过整批处理文件传输。任何管理员都可以轻松地创建、修改或删除任何已授予访问权限和无需用户脚本功能的档案。即使是复杂的、以逻辑为本的工作流程也可以创建和修改，无需进阶的编程技能。

MOVEit Automation 还可以通过自动转发和错误纠正的功能，为所有传输中的数据提供发送保证。MOVEit 的发送保证会自动重新发出传输失败的档案，直至成功完成传输。数据成功传送后，MOVEit 会向发送者发出通知，确认数据已获授权的收件人接收。

控制和可视性

我们实在没有办法保证组织的敏感数据是百分百受到保护，免受网络攻击。然而，对移动数据的控制和可视性都是有用的工具，可以大大减少黑客非法取得您的数据的机会。对数据流和正在发生的事情了如指掌，您的组织便能实施有效的安全程序，以保护您的数据，并确保您遵守数据保护合规性法规。

中央可视性可以就异常的档案访问活动或文件传输模式向 IT 人员发出警告。MOVEit 提供一组身分验证控制措施，管理用户授权访问敏感数据的时间和长度。这些措施包括用户和群组配置、用户帐户访问、权限、配额以及自定义的档案访问期限。IT 人员也可以设定密码，并可按需要将用户列为黑名单或白名单。任何违反这些政策和控制措施的违规行为都会发出提示，提醒 IT 人员防范未经授权的访问或可能出现的网络攻击，让他们能够快速有效地应对这些安全问题。

对记录和报告的控制能简化审计过程，并确保审计记录完整。系统日志提供了文件传输过程中有价值的数据，包括跟踪文件传输的时间、是否被正确的收件人接收和后来是否被删除。如果这些日志被篡改，整个文件传输过程的完整性都会受到损害。MOVEit 能透过加密防篡改日志避免这种情况发生，确保文件传输日志不能以任何方式篡改。

ipswitch

MOVEit 协助进行审计记录的另一种方法，是使用预设和自定义报告。简单的用户界面方便用户查看和收取报告。在系统中所有 FTP 服务器都是使用相同的报告格式，令审计人员能够轻松审查、比较和对比所有可用的档案活动数据。

信息安全

重要的文件传输合规性要求包括档案完整性检查、数据接收后删除、不可否认和保证送达。这些信息安全保障措施能确保传输中的敏感数据不会被第三方更改或不正确地传递给非预定的收件人。

要把数据传输到您想到的地方看似容易，但您需要在文件传输方法中加入许多后端保护，以保护敏感数据。当有攻击者恶意更改双方之间的直接通讯时，中间人便会发动攻击。MOVEit 的不可否认数据完整性功能可确保发送者和收件人都获授权访问数据。换言之，只有发送者和收件人可访问正在传输的数据。假如第三方以某种方式设法拦截传输，他们也无法读取或更改任何数据。MOVEit 用 SHA1 和 MD5 算法执行档案完整性检查，以确保最初发送的数据是最终传送到预定收件人的相同数据。

MOVEit 能保护敏感的数据，设置控制选择在设定时间（例如 1 小时、1 天、1 周等）自动删除数据的选项，或限制档案在收件人接收后可下载的次数。数据删除和档案下载限制有助确保档案不会无意中让第三方进行未经授权的访问。

MOVEit 的另一个重要功能是让您随时知道档案的去向。保证送达功能可确保您的档案确实发送到您预期的目的地。MOVEit 会自动重新发送传输失败的档案，直至成功传输。当数据送达后，MOVEit 会向发送者发出数据由授权收件者接收的通知。

认证和授权

满足数据安全性和合规性要求的第一道防线可在资料未被访问之前便设置。透过控制对系统和数据的访问，您可以确保只有授权用户才能直接接触您组织最敏感的数据。

MOVEit 使管理员能够利用多个身分验证来源，例如本地用户数据库、通过 LDAP 或 RADIUS 的外部目录和通过 SAML / SSO 的外部 IdP 对用户进行身分验证。

以活动目录（AD）为例，微软的 LDAP 目录服务就是一个数据库，能跟踪您的组织内的所有用户帐户和密码。管理员可以利用 AD 轻易实施企业范围的策略、凭证和安全性。使用 AD 能限制终端用户需要记住的用户名称和登录数，减少 IT 人员需要创建和管理的账户数量，并能增加安全性，因为所有数据都存储在一个受保护的位置。将访问控制与 AD 结合，可确保只有已通过身份验证的 AD 或 LDAP 用户才能访问文件传输系统。由于系统能够跟进员工情况的变化（即新员工或解雇员工）和提供适当的访问，IT 人员便不需要监控这个流程。

多重身分验证是得到 HTTPS 和 FTPS 的 SSL / TLS 证书以及 SFTP 的 SSH 客户端密钥支持。这提供了另一层认证，有助确保试图访问 MOVEit 系统的人士确实具有这样做的权限。

当用户被授予对 MOVEit 服务器的访问权限，内置的授权控制措施便会提供保障，保护敏感数据不会被未授权的一方查看。用户通常会被默认分配最小的访问权限，这意味着在授予权限之前，他们无权访问或阅读数据。换言之，每个用户的档案均受到保护，免于被未授权的人士查看或改动。MOVEit 也提供灵活性，让系统管理员可以根据需要调整授权控制。管理员可以授予用户个人权限或授予群组一组权限。 群组成员的资格可透过 LDAP 或 SAML 与 AD 同步。这样便可以令系统管理员清楚地控制用户登录到 MOVEIT 服务器后可以或不可以访问的内容。

密码学

合规性标准通常要求实施一定级别的数据安全协议，以防止敏感数据落入错误的地方、被盗和在黑市出售。这些合规性法规的原意是好的，但是，加密算法的更新速度通常很快，这些法规很难跟上步伐。加密算法是有保存期限的，您的系统应该不断更新，以确保最新的加密保护可用于传输或静止的数据。

MOVEit 使用 FIPS 140-2 验证算法，例如 AES-256 加密法，以保护静态数据。即使有人入侵您的系统，存储在 MOVEIT Transfer 服务器的任何数据也将会被加密，令入侵者无法读取。他们将无法「破解代码」，无法读取您的敏感档案。

MOVEit 也使用安全文件传输协议 SFTP（SSH）、FTPS（SSL / TLS）和 HTTPS（SSL）保护传输中的数据。这些协议会在 MOVEit 中不断更新，以符合最新的行业标准，确保您的数据永远安全。

安全架构

一个强大和安全的文件传输管理解决方案不仅可以保护静止和传输中的数据安全，还提供具有额外安全层面的系统架构，以区分在内部数据库中的数据和标示为传输中的数据。

MOVEit Transfer 服务器可作为与第三方共享数据的临时存储库。它位于组织的防火墙外，因此存储在内的数据可以被外部人士访问却又不会泄露组织的其余网络。存储在 MOVEit Transfer 上的所有数据都使用 AES-256 加密保护，确保 DMZ 中没有未加密的数据。

ipswitch

Ipswitch Gateway 为您的文件传输解决方案架构增加了另一层保护。它位于 DMZ 内，并可终止认证和数据传输的入站请求。它还扮演了来自公共网络入站连接和组织内部可信任网络之间的代理角色。这个配置使 MOVEit Transfer 部署在防火墙后面，提供额外的安全层，将未经授权的第三方和黑客取得安全网络资源、敏感数据和身分验证服务的风险降至最低。

故障转移

对于必须在防火墙内以及和外部交换敏感数据的组织来说，业务连续性是非常重要的。当您需要保护传输中的数据，并确保它不会在自然灾害、停电或组织内高传输量期间的某个地方「丢失」时，文件传输活动的保密性、完整性和可用性便成为首要任务。

MOVEit 的灵活和可扩展的架构通过提高网络文件传输表现来实现高可用性。高可用性可以透过利用 MOVEit Transfer 组件的分布式网络场来消除单点故障。MOVEit Transfer 的网络场作为单一 MOVEit Transfer 系统运作，可处理所有客户的要求，并把文件传输管理系统负载分发到多个节点。这种分布式结构能为您的系统最有效地分发文件传输工作，并使 IT 能向网络场添加更多应用程序节点，扩展可用性和提升表现。

自动和安全的故障转移功能对确保文件传输工作百分百成功起着重要作用。MOVEit 的故障转移选项能确保档案成功传输，即使在灾难或中断情况下，仍会不断重新发送，直到成功传输。它提供了可靠的全天候文件传输操作，达至零停机及保护数据不会丢失，以确保符合法规和和政策。

结合 MOVEit 的高可用性和故障转移功能，可确保您的文件传输管理系统准备就绪、可用和装备齐全，在需要传输数据时能提供安全和有保证的传输。

Ipswitch MOVEit 数据保护安全和合规性功能摘要

MOVEit 是一个文件传输管理系统，助您管理、查看、保护和控制与外部交换敏感数据，以确保符合数据保护法规。

凭着 MOVEit，您的 IT 团队可以:

- **控制**合作伙伴、人员和系统之间重要数据的转移，以确保数据安全性和合规性
- **简化**自动化工作流程的创建，提高可靠性、安全性和合规性
- **自动化**性能、SLA 和合规性监控

从合规性角度而言，MOVEit 有助解决许多数据安全问题：

- **数据保护保障**：MOVEit 是为实现数据保护保障而设计：静态加密、安全删除、文件传输完整性（不可拒绝）、单一用户 ID 和自动注销
- **访问控制**：MOVEit 允许管理员为访问 ePHI 的内部用户进行配置并自动进行强大的访问控制政策
- **记录和报告**：MOVEit 能编制详细的审核日志帮助用户审核活动，包括登录活动
- **灾难恢复**：MOVEit 的 Ipswitch 故障转移能令实施关键 ePHI 数据应急规划技术更简易

ipswitch

Frost & Sullivan 授予 Ipswitch MOVEit 2016 安全文件传输产品领导奖

在他们的行业最佳实践研究课程中，MOVEit 被视为是解决关键客户和行业对安全性、灵活性和可扩展性需求的最佳软件，同时能提供无与伦比的客户体验和易用性。

下表总结了 MOVEit 文件传输管理解决方案与市场上其他可用的文件传输方法的对比。

保安范畴	FTP 服务器	云端档案共享	电邮服务器	MOVEit MFT 服务器
工作流程自動化	◑	○	◔	●
控制和可视性	◔	◑	◑	●
信息安全	◕	◕	◑	●
认证	◔	◕	◑	●
密码	◑	◕	◑	●
安全架构	◑	◑	◕	●
故障轉移	◑	◕	●	●

有关 Ipswitch

Ipswitch 以简单的解决方案助你解决复杂的信息科技问题。本公司的软件受到全 球数以百万计人士信赖，用于系统、商业伙伴和客户间的文件传输，以及监控网络、应用程序和服务器。Ipswitch 于 1991 年创立，总部位于美国麻省莱辛顿，办事处遍布美国、欧洲和亚洲各地。

详情请浏览 www.ipswitch.com。

ipswitch

下载IpswitchMOVEit 30 天免费试用