ipswitch

Secure. Control. Perform.

Ipswitch 电子书

什么是 FTP?

安全文件传输指南

使用者彼此之间、使用者与客户及合作伙伴之间，是透过什么样的方式分享及传输信息呢？大家会合并运用电子邮件、快闪磁盘驱动器和/或 Dropbox 之类的企业档案同步与共享 (Enterprise File Sync and Share，EFSS) 产品吗？如果会，您就该拿回控制权。请提供单一、简易、安全又能实际派上用场的技术给使用者。

电子邮件和快闪磁盘驱动器都不安全

问问从事 IT 业的人，对方会告诉您，电子邮件的安全性十分薄弱。想想用户贪图方便而使用私人电子邮件帐户传送档案所须承担的风险。举例来说，电子邮件本身并没有加密，因此，若透过电子邮件传送数据，遭第三方拦截的可能性会更高。

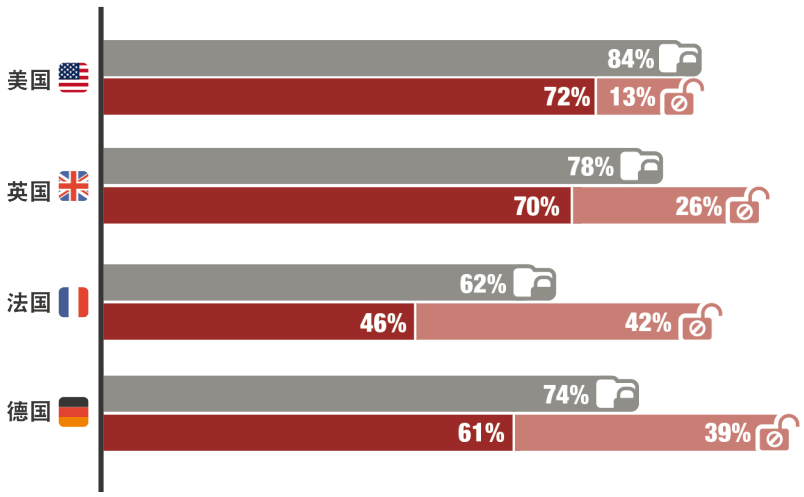
管理电子邮件也是个棘手的问题。您有没有遇过这种情形：使用者传送大型档案，导致 Exchange 服务器流量壅塞，因此您必须想尽办法恢复正常流量。

如果您认为电子邮件令人头痛，请再想想快闪磁盘驱动器。现在还有人使用这类一点也不安全的玩意传输数据和档案吗？Ipswitch 不久前透过社群媒体进行了一项民调，共有 595 人回复，其中有 **15%** 的人目前仍然使用快闪磁盘驱动器搬移数据。即使您所从事的产业并不需要如此严格的管制，您也不会希望数据安全毫无保障。快闪磁盘驱动器也是网络攻击者侵入公司网络的管道。

EFSS 对 IT 不友善

既然对电子邮件心存疑虑，您或许会实行防护机制，避免人们使用电子邮件传输大型档案和/或敏感档案。这么做的问题在于，大多数的一般使用者会设法投机取巧，干脆改用自己私人的 Dropbox 或 Google Drive。

根据 Ipswitch 近期所做的 *2016 年安全与法遵现况*调查，**84%** 的受访者认为对内对外都能在安全的前提下传输及共享档案非常重要，但是，有 **46%** 的受访者表示自己会使用不安全的云端档案共享服务。



认为**安全传输和共享档案**非常重要的受访者所占百分比

目前**明文规定**禁止使用特定文件传输解决方案的受访者所占百分比

打算明文规定禁止使用特定文件传输解决方案的受访者所占百分比

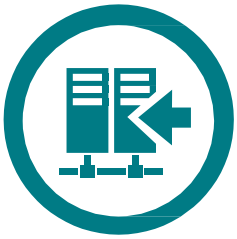
需要将大型档案传送到其他位置时，Dropbox 和 Google Drive 这类 EFSS 服务是非常方便的工具。但是，这类服务的主机不在您自己的网络中，也不是由您管理，因此，使用上难以避免固有问题。IT 无法控制可能存在云端中的敏感数据，也无法控制这类数据最后的去处。这类资料的终点不计其数。

想想十几个人共享一份 Google 文件的情况。假设其中三分之一的人在去年离职。由于您无法关闭他们曾经共享的 Google 文件，因此，这些人很有可能依然拥有这些文件的访问权限。

更糟糕的是，使用者可以同时使用多台装置登入同一个 EFSS 服务，这种情况更让危险因子倍增。遑论 EFSS 系统本身也是遭黑客锁定的大型目标。Dropbox 和 Apple Cloud 都曾经在过去几年内遭骇，相关事件十分引人注目。

IT 想要什么？数据能够存在安全的代管环境里，而且能够控制访问权限。

ipswitch



FTP 服务器安全吗?

您是否曾经考虑过在组织内部或与合作伙伴及客户之间使用 FTP 客户端及服务器，希望能透过安全的方式传输档案？FTP 服务器的管道可以加密。FTP 服务器一点也不麻烦。FTP 服务器很灵活。此外，FTP 服务器不贵，这或许是最棒的一点。

我们懂。IT 预算十分拮据。不是每一个 IT 团队都能负担得起管理式文件传输 (MFT) 解决方案，也不是每一个 IT 团队所任职的公司都像医疗保健业一样要求严格管制。若考虑合理的时间和心力，能按照需求自定义的简易型 FTP 服务器可说安全性和可靠性兼具。

不同类型的 FTP

FTP 分为几种常见的形式，其中最大的差异在于所采用的加密类型。最常见的 FTP 类型包括：

- FTP
- 含 TLS 功能的 FTP (FTPS)
- SSH 文件传输协议 (SFTP)
- 超文本安全传输通讯协议 (HTTPS)

如前所述，除了要求输入密码以外，FTP 本身并不提供额外的安全防护机制。若您需要传送的数据不属于敏感数据，且/或只能在您的网络内部传送档案，那么，FTP 不失为最理想的选择。许多公司单纯使用具基本密码防护功能的 FTP 传送只能在网络内部传送或 IT 禁止透过电子邮件传送的大型档案。若要将敏感数据传输到公司网络之外，请勿使用这类简易型 FTP。

FTPS 就是利用传输套接字层安全机制 (又称 TLS) 防护透过 FTP 传输之档案的方法。TLS 也称为安全套接字层 (SSL)，因为 TLS 正是紧接在 SSL 之后发展出来的。TLS 加密方法是在会话 (大多是网页会话) 一开始便进行交握，因为 TLS 是大部分知名网站所采用的数据加密技术。

SFTP 又称安全文件传输协议，可在两地之间进行可靠的数据存取与传输。这种技术额外增加了几项功能，可以在档案中断传输后继续传输，也能透过远程移除档案。

从名称就看得出来，HTTPS 是安全版的 HTTP。HTTPS 运用 TLS 向对应的网页服务器验证网页，方法与 FTPS 运用 TLS 加密技术传输档案的原理大同小异。安全传输层是避免窃听的必要机制，近年来，Google 也规定要采用这项技术才能在 Google 搜寻结果中保持良好的排名。HTTPS 的存在已经很久了，但原本的用途是网络付款。后来，资料隐私权的重要性越来越高，许多属于几项产业的网站也开始部署这项技术。

要采用哪一种文件传输标准，单纯取决于您所要传输的内容，以及您需要的加密类型。某些加密标准比较繁复，但却是遵守法令规定不可或缺的。其他加密标准部署起来较容易，也有助于加快数据传输速度。

不同的加密类型

应采用的加密类型取决于您的需求。有些加密标准易于管理、速度又快，有些则较繁复，但数据安全层级较高。例如，若遵守 HIPAA 之类的法规对您而言非常重要，那么您就会选择采用符合 HIPAA 规定并通过认证的加密标准。

以下列举几项最常用的加密通讯协议：

- 传输层安全 (Transport Layer Security，TLS)
- 安全套接字层 (Secure Socket Layer，SSL)
- 安全壳层 (Secure Shell，SSH)

TLS 是最常见的加密通讯协议，但并不是 FTP 最常用的加密技术。多数网站、VPN、电子邮件和网络电话 (VoIP) 之类的其他通讯，以及 Twitter 之类的社群媒体，全都采用 TLS 加密技术。TLS 1.2 是接受度最高的通讯协议版本，而目前正在编写的版本则是 TLS 1.3。

另有一点也值得注意，相较于 SSH (稍后会深入讨论 SSH)，TLS 采用的是 X.509 数字证书。您或许会问，什么是 X.509？简而言之，X.509 是一种公钥加密标准。以数据传输而言，X.509 会验证数据交换传送者和接收者双方的身分。

SSL 就是 TLS 的前一代技术。最新的版本是 SSL 3.0，人们曾经认为这是比 TLS 1.0 和 1.1 还要强大的安全技术。目前仍然有人采用 SSL，但 SSL 已经是旧式的加密标准了。近年来，SSL 屡屡遭黑客成功破解，因此，人们不再认为这是一项安全的加密技术。若您从事于必须受管制的产业，强烈建议您选择 TLS 1.2 加密。

ipswitch

如前所述，SSH 和 TLS 之间最大的差别就在于使用 X.509 之类的数字证书。SFTP 运用 SSH 保障数据安全，与 FTP 不同之处就在于 SFTP 不会以纯文本传送验证讯息和数据。SSH 是采用壳层技术的解决方案，因此名称是安全壳层。网络服务和应用程序鲜少采用 SSH。不过，IT 和开发团队最常采用 SSH，尤其是用于文件传输。

一套工具包办全部

进一步了解了 FTP 和其他加密文件传输协议后，或许您会开始思考该如何部署安全文件传输解决方案。不妨利用以下的快速自我评估要点找出最符合需求的标准：

1. 您是否希望您所传输的数据遵循 HIPAA、GDPR 或 SOX 等特定的法令规定？
2. 可靠性是否比成本更重要？
3. 系统存取与数据控制对您而言有多重要？
4. 您是否需要保留数据传输记录，供高层主管和稽查人员查看？
5. 您的数据太重要了，所以您需要故障转移功能？

只要掌握不可或缺的功能后，您就可以决定使用 FTP 究竟是否符合您的需求。如果是，接下来就要决定您打算采用的数据传输代管环境。Ipswitch 的 WS_FTP 是一种简单易用、功能丰富的客户端与服务器组合。

以下举例说明某公司依据其文件传输需求采用 WS_FTP 的情形。

ipswitch

安全防护

Rocksteady Studios 运用 WS_FTP 服务器的 256 位 AES 加密技术保护传输到公司以外的创意资产。

Rocksteady Studios 运用文件传输技术提升游戏水平

Rocksteady Studios 总部设于英国北伦敦，是一家电玩游戏开发商，因得过奖项的蝙蝠侠：阿卡汉 (Batman: Arkham) 系列而闻名。该公司需要与合作代理商传输创意资产，因此需要依赖可靠的安全文件传输系统准时开发游戏。

安全完整地传输大量创意资产

Rocksteady 每天都需要和合作伙伴分享大量档案，档案内容包括音效、音乐、美术图案、屏幕绘图以及道具画面图。Rocksteady 就像许多其他同类型的公司一样，因为保密方面的需求而必须采用安全的创意资产传输方式。此外，必须按照预定规划将档案完整无缺地准时送达，这一点也同样重要。

Rocksteady 之前一直使用 Microsoft Internet Information Services (IIS) 内建的 FTP 传输档案。但是，该公司的 SDSL 连接速度太慢，因此这种系统根本不敷使用。以这种方式传输数据时，必须将庞大的数据分解成 RAR 封包，因此会出现遗漏封包和可靠性方面的问题。

Rocksteady Studios 共同创始人 Sefton Hill 解释他一开始遇到的难题：「联机不稳定就无法保证能将所有封包顺利传送到目的地。代理商不断寄电子邮件和打电话向我抱怨根本没有收到资产档案。我需要更稳定而且值得信赖的传输机制。」

安全文件传输能降低 IT 的复杂度

最后，Hill 的团队选择了 Ipswitch 的 WS_FTP 服务器。Hill 特别提到：「这项产品非常稳定，而且提供进阶加密功能，选择安全文件传输产品当然要挑这个。」

Rocksteady Studios 运用 WS_FTP 服务器的 256 位 AES 加密技术保护传输到公司以外的创意资产。而在公司外部的合作代理商则使用会定期自动过期的强密码验证身分并存取档案。

对游戏开发商而言，一旦失去任何数字资产，很有可能会在法律和经济方面引发严重的究责问题。WS_FTP 服务器让 Rocksteady Studios 确信它能够遵循发行者要求该公司遵守的严格法律规定，更让该公司的合作代理商认为 Rocksteady Studios 是有能力的公司，值得继续合作。

此外，该公司能够控制使用者的存取情形，也能实时掌握文件传输活动。系统工程师 Benjamin Nias 表示，安装 WS_FTP 让他省了不少时间和心力。他还提到：「在我们这一行，时间最重要，只要能透过任何方法加速流程，就能得到最大的优势。每天将资产数据分解成可以管理的封包，再利用半夜的时间透过 IIS 进行传输，这种方式真的很花时间。有了 WS_FTP 服务器之后，我只花 30 秒就搞定了。」

ipswitch

保障所有数据传输作业的安全

多数 IT 团队最重视的就是数据安全，但采用电子邮件或 EFSS 解决方案传输数据顶多只能利用密码保护传输中的数据。密码保护已经不够安全了，因此这种方式也无法令人放心。您会发现一般使用者喜欢用好记又方便共享的弱式密码，但要破解这类密码几乎不费吹灰之力。

或许，您和您的团队应该开始考虑逐步采用既能让使用者觉得好用又能在数据安全方面发挥最高防护作用的 FTP 客户端和服务器组合。

ipswitch
WS_FTP

运用 WS_FTP 保护传输中的资料

下载 30 天免费试用版 ▶

关于 Ipswitch

Ipswitch 专注于设计与研发能够跨云端、虚拟及内部环境轻松发挥24 小时全天候效能与安全性的业内顶尖软体，使用者人数超过100 万，分属116 个国家的42,000 间不同的公司，负责管理超过150,000 个网路。全球 IT 团队均依靠Ipswitch 25 年的优良创新经验，利用Ipswitch MOVEit® 安全档案传输、Ipswitch WhatsUp® Gold 网路监控及Ipswitch WS_FTP®，在各自的岗位上发挥商业交易、应用程式与基础架构的最大效能，并提供出色的安全保障。 Ipswitch 的产品组合丰富广泛，可以直接运用，也可透过与一流IT 厂商建立的策略联盟及Ipswitch 不断扩大的全球合作伙伴生态系统取得，这些产品组合能够提升应用程式与网路的效能、监控各种IT环境，并确保在遵循PCI、HIPAA、GDPR 和其他产业及政府资料安全与法令规范的前提下保障资料交换的安全。

本公司在美国、欧洲、亚洲及拉丁美洲均设有办事处。如需详细资讯，请造访 http://ipswitchcn.com 或透过 LinkedIn 与 Twitter 保持联络。若要了解 Ipswitch 的策略联盟或全球合作伙伴服务网，请造访 https://tw.ipswitch.com/partners 。

ipswitch

下载 Ipswitch WS_FTP
30 天免费试用版 ›