

保护您的组织免受勒索软件侵害

据预测，仅在 2023 年，勒索软件攻击便会使组织损失总计 8 万亿美元。¹
具有快速还原选项的数据保护计划对于降低勒索软件和其他形式网络犯罪的影响至关重要。



备份：灾难发生时的最后一道防线

当数据在恶意删除或修改后丢失时，备份使您可以还原任务关键型数据并避免代价高昂的停机时间。利用 Synology 的数据保护解决方案为整个 IT 基础架构设计备份策略。



全面的保护

保护端点和主要备份，为数据创建多个安全屏障。



快速恢复

通过即时恢复选项，尽量缩短灾难发生时的停机时间。



不可变存储

防止对数据和快照进行未经授权的更改。



无需许可证的备份

在存储允许的范围内备份尽可能多的数据，而没有限制或隐藏费用。

集中防范勒索软件

整合来自工作站、服务器、虚拟机和云应用程序群的备份。利用重复数据删除和增量备份技术优化存储消耗并避免带宽瓶颈。 <https://www.synology.cn/dsm/solution/infrastructure>

物理工作负载

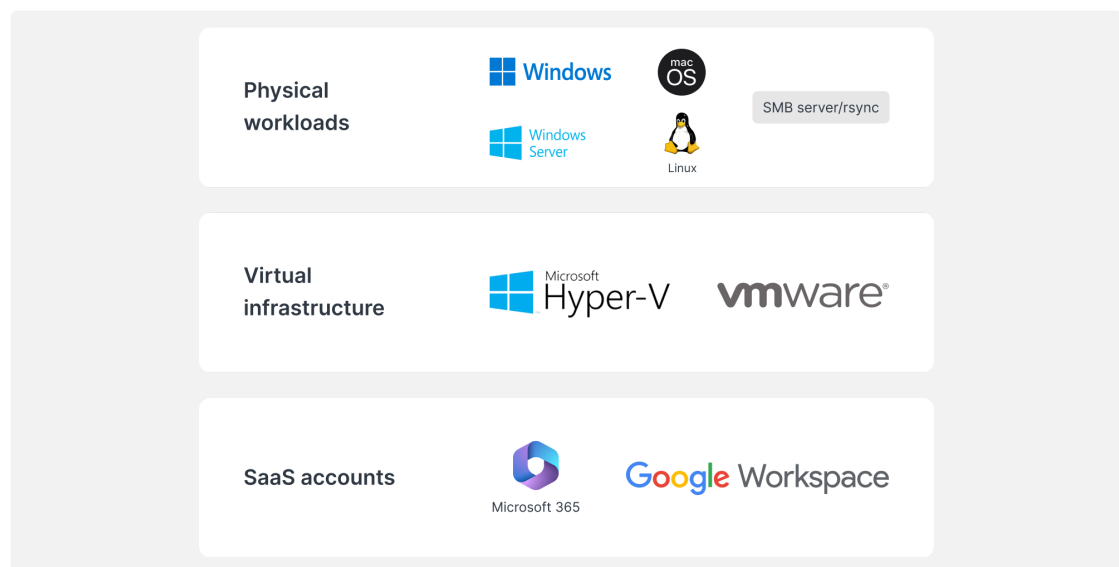
通过全面的裸机备份和灵活的文件级恢复，在发生恶意攻击时保护端点。

虚拟基础架构

使用强大的数据缩减技术备份 VMware® vSphere™、Microsoft® Hyper-V® 虚拟机和 LUN。

SaaS 帐户

通过自动检测新添加的帐户，为存储在云上的数据实现持续保护。



高效恢复

通过从本地或异地 Synology 系统快速还原备份，尽可能减少关键生产系统的停机时间。

RTO 几乎为零

在 VMware®、Hyper-V® 或 Synology Virtual Machine Manager 上装载备份映像以尽快恢复工作。将虚拟机还原到备用 hypervisor 以避免服务中断。

尽可能减少 RPO

根据需要配置备份频率，从而尽可能减少攻击期间可能受影响的数据量。借助增量备份和重复数据删除技术，快速保护系统。

直观的操作

让员工在还原电子邮件、联系人和文件之前，可以从便利的门户浏览和预览这些内容，从而提供对用户更友好的体验并减轻 IT 团队的负担。

额外增添一层保护

遵循 3-2-1 备份策略，具体方法是将第三组数据存储备在异地或云中，保护您的数据免受火灾、自然灾害或盗窃的影响。



到异地服务器

将备份存储到备用位置的 Synology 服务器，抵御物理灾难，并复制不可变快照，以加强勒索软件防护。



到云中

备份到主要云存储提供商，通过客户端 AES-256 加密确保您的数据安全，避免他人未经授权的访问。 <https://c2.synology.com/storage/nas>

在不同行业中深受信赖



“Synology [...] 使我们能够减少服务器硬件支出 [...], 同时使基础架构和工作站备份、系统日志记录和文件管理更加容易。”

https://www.synology.cn/company/case_study/Investortools



“得益于 Active Backup for Business, 我们的所有备份现在都集中存储并且全天候可用, 这有助于我们尽可能减少停机时间并保持遵守 FERPA 法规。”

https://www.synology.cn/company/case_study/University_of_Washington



“[...] “Active Backup for Business 备份速度快、重复数据删除效果好, 在服务器上备份的 58TB 数据, 仅占用了 28TB 的存储空间, 整体表现相当令人满意。”[...]”

https://www.synology.cn/company/case_study/SHISEIDO_Taiwan_ABB



“[...] Active Backup for Business [...] 使我们从单一控制台集中和管理所有备份任务。快速且可靠的恢复还可确保业务连续性。”

https://www.synology.cn/company/case_study/UNESCO

常见问题

什么是勒索软件？

勒索软件是一种加密受害者文件的恶意软件。攻击者随后会索要赎金以还原数据访问，通常威胁说，如果不支付赎金，便会长久销毁数据。勒索软件攻击具有高度破坏性，可能会给个人和组织造成重大财务损失。保护您自己和您的设备免受勒索软件侵害非常重要，例如通过使软件保持新状态和定期备份您的文件。

有哪些类型的勒索软件？

有许多不同类型的勒索软件，并且人们在不断开发新的变种。一些很常见的勒索软件类型包括：

- **加密勒索软件** — 十分常见的勒索软件类型会加密受害者的文件，这样在没有解密密钥的情况下便无法访问这些文件。攻击者随后会要求支付赎金以换取密钥
- **锁定勒索软件** — 一种勒索软件类型会通过更改登录凭据或显示阻止受害者访问其系统的消息，使受害者无法进入其计算机。攻击者随后会要求支付赎金以解锁计算机
- **勒索软件即服务 (RaaS)** — 这是一种业务模型，其中攻击者向要实施攻击的其他个人或群体提供勒索软件。前者通常会提供勒索软件并处理付款，而后者会收到一定比例的赎金
- **恐吓软件** — 旨在恐吓受害者支付赎金的勒索软件。它通常涉及显示虚假的安全警告或消息，声称受害者的计算机感染了病毒。攻击者随后会要求支付赎金以消除假定的感染

勒索软件如何传播？

勒索软件通常通过网络钓鱼电子邮件或利用计算机系统漏洞进行传播。在网络钓鱼攻击中，攻击者会发送看似来自合法来源（例如银行或知名公司）的电子邮件。该电子邮件通常包含链接或附件，单击后会在受害者的计算机上安装勒索软件。利用系统中的漏洞是相似的，不同之处在于攻击者会在受害者不知情的情况下使用系统安全漏洞来安装勒索软件。无论是哪种情况，一旦安装了勒索软件，它都可以快速传播到同一网络上的其他计算机。

勒索软件攻击的典型过程是怎样的？

勒索软件攻击的过程通常遵循以下步骤：

1. 攻击者通过发送网络钓鱼电子邮件或利用系统中的漏洞访问受害者的计算机
2. 一旦攻击者能够访问受害者的计算机，他们便会在系统上安装勒索软件
3. 勒索软件随后会加密受害者的文件，使用户无法访问这些文件
4. 攻击者随后会向受害者索要赎金（通常采用比特币等数字货币的形式），来交换可解锁加密文件的解密密钥
5. 如果受害者支付赎金，攻击者会提供解密密钥，受害者将能够再次访问其文件。但是，不能保证攻击者会实际提供密钥，即使他们提供了密钥，受害者的文件也可能会由于加密过程而遭到破坏或损坏

请务必注意，此过程中存在许多变化，并非所有勒索软件攻击都会完全遵循这些步骤。例如，某些攻击可能根本不涉及加密文件，而其他攻击可能涉及其他形式的强取或勒索邮件。

如何获取勒索软件？

您可以通过多种方式获取勒索软件。十分常见的一种方法是单击网络钓鱼电子邮件中的恶意链接或附件。这种类型的电子邮件看似合法，通常似乎来自知名公司或组织。当您单击链接或附件时，它会在您的计算机上安装勒索软件。获取勒索软件的另一种方式是访问遭到入侵的网站。这些网站已遭到攻击者入侵，攻击者插入了代码，如果您访问该网站，这些代码会自动在您的计算机上安装勒索软件。您还可以从网络下载受感染的文件来获取勒索软件。如果您从可疑网站下载文件，或下载由您不认识的某人共享的文件，则可能会发生这种情况。简而言之，浏览网络时务必谨慎，避免单击链接或从不熟悉的来源下载文件。这有助于保护您免受勒索软件和其他类型的恶意软件攻击。

谁是勒索软件的目标？

勒索软件攻击的目标可能是使用连接到网络的计算机或其他设备的任意用户。然而，一些群体比其他人更有可能成为攻击目标。例如，勒索软件攻击通常以企业为目标，因为企业通常拥有更有价值的信息，并且可能更愿意支付赎金来取回这些数据。医院、学校和其他提供关键服务的组织也是常见的目标，因为勒索软件攻击可能会干扰其运营，甚至危及生命安全。个人也可能成为勒索软件攻击的目标。在这些情况下，攻击者可能试图通过威胁删除受害者的个人文件或发布敏感信息来敲诈受害者的钱财，除非支付赎金。勒索软件攻击的目标通常是根据其信息的价值以及他们是否愿意支付赎金以取回数据来选择的。

向勒索软件付款的风险是什么？

向勒索软件攻击者支付赎金，看似是取回文件的简单方法，但这其实是一个非常危险的决定。支付赎金的风险不少，包括：

- 不能保证攻击者会实际提供解密密钥。在许多情况下，支付赎金的受害者从未收到密钥，仍然无法访问其文件
- 支付赎金可能会鼓励攻击者继续进行攻击。如果攻击者知道受害者愿意支付赎金，他们可能更有可能在未来实施更多攻击
- 支付赎金可能会使您成为未来攻击的目标。如果攻击者知道您愿意支付赎金，您更有可能在未来成为目标
- 支付赎金可能是非法的。在某些情况下，向犯罪组织支付赎金可能被视为一种资助恐怖主义或其他非法活动的形式

虽然支付赎金看似是取回文件的简单方法，但这可能其实是一个非常危险的决定。因此，在进行决策之前，请务必仔细考虑风险。

勒索软件的成本是多少？

勒索软件攻击的成本可能因多种因素而异，例如所使用的勒索软件类型、加密的文件数量以及攻击的有效性。在某些情况下，勒索软件攻击的成本可能相对较低，攻击者要求获得数百美元的赎金。在其他情况下，成本可能会高得多，攻击者要求获得数千美元甚至更多的资金来恢复对受害者文件的访问。除了与支付赎金关联的直接成本外，勒索软件攻击还可能产生大量间接成本。例如，勒索软件攻击可能导致停机时间和生产力损失，从而可能导致收益和收入损失。它还会损害公司的声誉和客户信任，从而对业务产生长期的负面影响。这些间接成本通常比赎金本身高得多。

勒索软件的症状有哪些？

勒索软件攻击的症状可能因所使用的特定勒索软件类型而异。但是，一些常见症状包括：

- 您的文件遭到加密，您无法访问它们
- 您收到来自攻击者的消息，要求支付赎金以换取解密密钥
- 您看到您的计算机上运行不熟悉的程序或进程
- 您的计算机变得缓慢或无响应
- 您的计算机显示异常错误信息或弹出窗口

如果您怀疑计算机感染了勒索软件，则必须迅速采取行动。断开您的计算机与网络的连接，以防止勒索软件传播。

如何预防勒索软件攻击？

这里有几种措施可用来预防勒索软件攻击，包括：

- 使用信誉良好的防病毒或安全软件并使其保持新状态。这有助于保护您的计算机免受勒索软件和其他类型的恶意软件攻击
- 打开电子邮件附件或链接时要谨慎。勒索软件通常通过网络钓鱼电子邮件发送，因此对于您单击的内容请务必小心
- 确保您的操作系统和其他软件保持新状态。软件更新通常包括安全补丁，可帮助保护您的计算机免受勒索软件和其他威胁的侵害
- 定期备份您的文件。如果您的计算机感染了勒索软件，这有助于保护您的数据。确保遵守推荐的备份策略之一，例如 3-2-1 备份策略
- 了解勒索软件的风险，并教育组织中的其他人了解这些威胁。这有助于预防勒索软件攻击，并在发生时更容易检测和响应这些攻击

预防勒索软件攻击的理想方法是保持警惕，并采取措施保护您的计算机和数据。这有助于降低勒索软件攻击的风险，并在发生攻击时更容易从攻击中恢复。

Synology 如何保护我免受勒索软件的攻击？

预防措施对于避免成为勒索软件的受害者至关重要。除了您选择的防病毒软件外，还可使用这些 Synology 解决方案：

- **防止访问** — 可通过设置文件、应用程序和访问权限来减少勒索软件的传播，以及使用 [Secure SignIn](#) 和 [C2 Password](#) 配置安全登录凭据
- **保护设备** — 过时的系统会面临更大的风险。可使用 [Synology Central Management System \(CMS\)](#) 一次性更新所有 NAS，以及使用 [Synology Directory Server](#) 和 [C2 Identity](#) 中的群组策略保护其他设备
- **避免可疑文件** — 包含可疑文件的垃圾邮件和网络钓鱼电子邮件是传播勒索软件的常见方法。[Synology MailPlus](#) 可提供强大的反恶意软件保护和垃圾邮件预防功能
- **检查漏洞** — 可使用 Synology 安全顾问定期扫描恶意软件、漏洞和异常登录活动。实施建议更改以提高 NAS 安全性。 <https://www.synology.com/dsm/overview/security>

保护数据的更多方式

管理设备群

利用广泛的功能集中管理数据访问权限、软件状态、系统运行状况等。

<https://www.synology.cn/dsm/overview/administration>

监控所有系统

识别可疑的登录活动、管理更新并监控设备运行状况，无论您的设备位于何处。

<https://www.synology.cn/dsm/feature/active-insight>

保护数据

遵循 3-2-1 备份规则，保护您的数据免受意外和恶意修改或删除的影响。

https://www.synology.cn/dsm/solution/data_backup

开始使用

联系我们

要了解更多信息，请联系区域销售经理。

<https://www.synology.cn/form/inquiry/sales>

如何购买

查找您所在地区的 Synology 销售经理

<https://www.synology.cn/wheretobuy>

注意事项：

1. eSentire，2022 年官方网络犯罪报告 <https://www.esentire.com/resources/library/2022-official-cybercrime-report>

保护您的组织免受勒索软件侵害

<https://www.synology.cn/zh-cn/dsm/solution/ransomware>

Synology 网站

<https://www.synology.com/>

联系我们

https://www.synology.com/company/contact_us

SYNOLOGY INC.

© 2023, Synology Inc. All rights reserved. Synology, the Synology logo are trademarks or registered trademarks of Synology Inc. Other product and company names mentioned herein may be trademarks of their respective companies. Synology may make changes to specification and product descriptions at anytime, without notice.