IBM Systems

网络弹性

存储的一项重要新角色

目录

要点

- 通过实施 IBM 存储系统，构建强大的网络弹性解决方案
- 部署为贵企业量身打造的网络安全解决方案
- 充分利用广泛的 IBM 存储产品组合
- 在闪存、磁盘、磁带、软件定义和云对象存储解决方案之间做出选择

IBM Storage 部门提供一系列广泛的网络弹性解决方案

随着信息技术（IT）日渐渗透至我们的日常生活，以及企业、政府部门和个人收集的数据越来越多，网络安全逐渐变成了一项重要的社会需求。每周都有知名企业或政府部门内的安全故障被曝光，并且这些安全故障会波及无数人。

在 IBM Security 的赞助下，Ponemon Institute 在 2018 年 7 月展开了一项调研。该调研报告显示，过去 12 个月全球数据泄露的平均成本为 386 万美元，其中最大的数据泄露事故成本高达 3.5 亿美元。数据泄露的根源包括人工失误 (27%)、系统故障 (25%)，以及恶意或犯罪攻击 (48%)。在调研中，近一半的事故是因恶意攻击所致，这类攻击的单条记录成本比其他攻击的单条记录成本高 20%。[1]

全球企业面临的重大风险

根据攻击意图的不同，对 IT 基础架构的虚拟攻击有多种形式。在某些情况下，攻击者会攻击安装的软件，以访问机密数据，比如信用卡或银行账户。勒索软件就是一种形式的恶意软件，它会加密文件，要求用户付款之后才为用户提供密钥用于解锁数据。2017 年报告的 WannaCry 病毒攻击可能感染了 200000 台电脑，其中包括英国国民医疗服务体系的系统，导致受到影响的医院不得不拒接患者。[2] 有些攻击的目标是停止系统运转、禁用支付功能，或者只是简单地破坏数据，这意味着，这种攻击的目的就是为了破坏企业或政府机构。

除了上面提到的外部恶意软件的威胁外，我们还面临内部攻击的威胁。不诚实或心怀不满的员工可能会滥用数据或中断企业运营，其中一些有极大权力的员工甚至会损害 IT 运营。

考虑到现代社会高度依赖 IT 和数据，《世界经济论坛 2019 年全球风险报告》将网络攻击列为最有可能危害人类福利的重大风险之一。[3] 显然，因为网络攻击的成本和出现的几率非常高，所以 IT 部门需要采用系统化的安全方法。

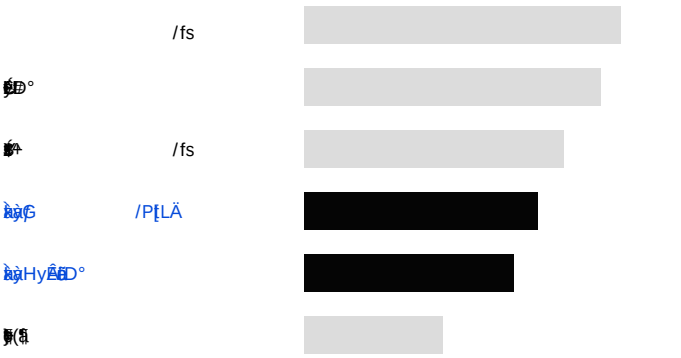


图 1：世界经济论坛评出的危害人类福利的主要风险

网络安全和网络弹性

不论数据泄露是因为意外事故还是恶意攻击所致，对 IT 运营及维持 IT 运营的数据的保护都至关重要。随着企业不断普及技术并且使用的资产越来越多，包括移动设备、物联网 (IoT) 和多供应商供应链，再加上攻击变得越来越复杂，企业的 IT 安全部门也需要应势而动。目前，市场上已经有很多方法致力于帮助企业避免业务中断并将成本降至最低。Ponemon 调研介绍了实施这些安全战略的价值。对于企业来说，最有益的安全战略包括组建事件响应团队、广泛使用加密、采用业务连续性管理，以及改进员工培训。这些战略能帮助企业将数据泄露成本降低 1/3。

为了实现和维持强大的网络安全和相关的网络弹性，企业需要采用程序化方法，了解您拥有哪些数据和系统资产及其价值所在，以及这些资产面临哪些风险。假如没有预算或人员限制，您会希望能够始终将安全性提升至最高。但是现实情况并非如此。因此，您需要贯彻风险管理原则，考虑各种可能的实施层级，并利用工具描绘出贵企业当前以及期望的安全状态。

NIST 框架

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）发布了一个*关键基础架构网络安全改进框架*，作为帮助企业和政府部门改进关键基础架构的建议。该文件引用“USA Patriot Act of 2001”对关键基础架构进行了定义：“对于美国来说，无论是物理或是虚拟的系统和资产都是至关重要的，如果出现失能或遭到破坏就会对安全、国家经济安全、国家公共卫生/安全，或任意上述组合产生相当不利的影响。”企业可以将引用的“美国”或“国家公共卫生”替换成“企业生存”，这样，该框架就能作为任意行业、任意规模 IT 部门的指导。

该框架从风险管理流程入手，旨在识别、评估和管理企业 IT 部门面临的风险。该框架由三个部分组成：框架核心、框架实施和框架概况。

框架核心包括五个网络安全功能，旨在帮助企业：

- *识别*：帮助企业了解现状，以管理危及系统、人员、资产、数据和功能的网络安全风险。
- *保护*：制定和实施适当的保障措施，确保交付关键服务。
- *检测*：创建并实施适当的活动，识别出现的网络安全活动。
- *响应*：创建并实施适当的活动，针对检测出的网络安全事件采取行动。
- *恢复*：创建并实施适当的活动，以便持续执行弹性规划，并恢复因网络安全事件受损的任意功能或服务。

综合来看，这些功能针对企业的网络安全风险管理生命周期，提供了一个高级别的战略性视图。

框架实施层描述了四个成熟度级别的网络安全功能，并解析了流程、管理计划的实施，以及外部关系考量因素，比如局部、风险指引、可重复和响应性。这些实施层体现了从非正式的被动响应逐渐过渡至敏捷的风险指引方法的过程。

框架概况体现了基于业务需求的网络安全结果。您可以利用这些概况，比较当前概况（即，初始状态）与“目标”概况（即，完成状态），发现改进企业网络安全态势的机会。

该框架从风险管理流程入手，旨在识别、评估和管理企业 IT 部门面临的风险。

规划网络弹性

通过使用 NIST 框架，业务主管能够确定当前的安全态势并规划未来的改进。IBM 等供应商利用 NIST 框架，识别最佳实践和前沿技术，并解析产品功能如何集成到总体安全状态。

总体网络安全原则中有一组网络弹性实践子集，后者是一个相对更新的理念。*Bjorck* 及其团队提供了一个定义：“网络弹性指的是不论发生什么不良网络事件都能持续交付预期结果的能力。”[4] 该理念承认事件或攻击可能入侵安全保护体系，但是成熟的 IT 部门将采取适当的方法，限制损害并提供快速恢复措施，为这些事件做好准备。在提供涉及重大公共利益的服务或者简单地实施企业的日常运营时，IT 基础架构必须足够强大，即使系统被成功入侵，IT 基础架构依然能够正常运转。

比如，在数据盗窃事件中，恶意软件会尽量不被察觉，尽可能不干扰正常运营，这样，企业可能几百天都不会发现这种入侵。勒索软件和擦除攻击这类新型攻击的目标不是盗取数据，而是干扰正常的企业运营。逻辑数据损坏 (LDC) 这一术语用于描述这类恶意软件试图实施的损害。在上述两种情况下，攻击的目标都是业务应用所用的数据。为了确保业务弹性，IT 基础架构必须保存最新的活动数据副本，这些数据副本将在攻击事件中充当可行的恢复点。

存储基础架构的角色

存储在企业运营中长期扮演“数据管理员”的角色。除了在数据未存储到主存储器时提供容器来存储数据之外，该系统存储层还一直提供保护功能，帮助企业从异常事件中恢复过来。随着时间的推移，这些功能集也有所增加：

- *备份*。从 20 世纪 60 年代起，存储就能支持应用用户在独立的介质中保存数据版本，避免被意外地删除、损坏或引起主要设备故障。
- *高可用性*。从 20 世纪 90 年代起，存储就一直提供设计方式，以构建多路径访问、多服务器访问并在机房内复制在线数据副本。
- *灾难恢复*。从 20 世纪 90 年代末起，存储就一直提供设计方式，以便远程构建复制的活动数据副本，避免被停电或地震、洪水或火灾等地区性灾难影响。
- *快速在线数据恢复*。自 21 世纪 10 年代起，存储开始提供数据副本快照，以便在数据意外删除或损坏的情况下快速恢复数据。

在每种情况下，存储系统、管理软件和运营流程都引入了新功能，来解决特定的风险案例。

为了应对网络攻击，尤其是勒索软件或擦除攻击带来的 LDC 威胁，企业需要考虑一系列新的保护因素。为了提供所需级别的弹性，解决方案提供商可以使用一些现有的存储工具，用于备份和灾难恢复，但是他们也需要新的存储功能来解决新的威胁。

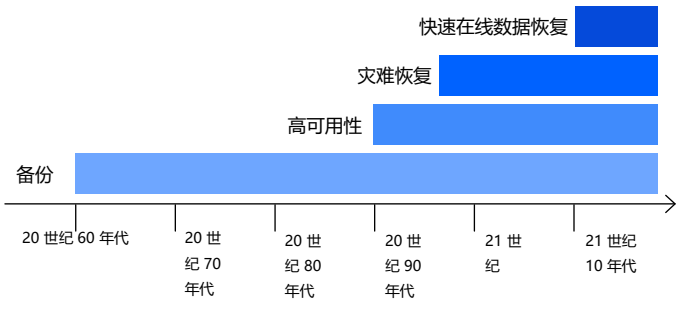


图 2：存储保护功能随着时间的推移的发展

比如，一旦出现成功的 LDC 攻击时，存储层必须保护数据，抵御伪装成日常操作的攻击。现在，写入文件、块或对象可能都是恶意软件的操作，旨在加密或毁坏重要数据，其方式可能是通过创建新的备份快速让良好备份过期，并将这些备份替换为受损数据的备份。您需要采用一种结合了存储功能和运营流程的机制，保存最新的数据恢复副本，即使面临复杂的恶意软件攻击。一旦检测出攻击并启动了响应，您可以使用这些保存的副本，重启应用，恢复正常的服务。IBM Redpaper *DS8000 Safeguarded Copy* 确定了创建留存副本所需的三个新功能：[5]

- *粒度*：企业必须能够创建多个保护副本，在损坏事件发生时将数据丢失降至最低。
- *隔离*：保护副本必须与活动的生产数据隔离开来，避免受损的主机系统损坏保护副本（该功能也被称为“气隙”）。
- *不变性*：数据副本不能被未经授权的操作所影响。

在“*Five Key Technologies for Enabling a Cyber-Resilience Framework*”报告中，IDC 的 Phil Goodwin 和 Sean Pike 在最佳实践列表中添加了两个新的考量因素，这两个因素并不仅仅适用于 LDC 攻击弹性：[6]

- 面向平台和应用恢复的自动化与统筹安排
- 监管报告和保证

您需要采用一种结合了存储功能和运营流程的机制，保存最新的数据恢复副本，即使面临复杂的恶意软件攻击。一旦检测出攻击并启动了响应，您可以使用这些保存的副本，重启应用，恢复正常的服务。

利用 NIST 框架，设计数据弹性解决方案

实现 LDC 弹性所用的特定技术在性能、响应时间、总体恢复时间和成本上大有不同。在 DR 领域的术语中，实施有不同的恢复点目标 (RPO) 和恢复时间目标 (RTO)。NIST 框架和风险评估方法能够有效地指导您设计总体网络安全态势。您在制定总体计划时可能包括以下步骤：

- *识别*：使用风险管理方法，列出关键应用和数据资产，确定适用于每项资产的保护策略。哪些资产是任务关键型资产？哪些资产的数据变化频率高？哪些资产可以从外部数据源重构？对恢复时间 (RTO) 和允许的数据丢失率 (RPO) 有何要求？您可以投入多少成本用于保护每项数据资产？
- *保护*：在生产环境中评估其他安全保护措施，比如对特权访问的限制。构建流程，以预期 RPO 要求的速度创建数据备份副本。为副本选择适当的存储位置，包括利用网络隔离保护副本，存储不可变副本，避免软件或管理员操作删除数据。提供自动化功能用于创建备份，不再依赖人工干预。制定响应计划，包括响应团队和流程步骤或运行手册，从而恢复特定的应用或服务器，或者整个基础架构。
- 检测：利用适当的机制，识别出现的恶意软件、黑客或恶意特权用户，并暂停受损的服务器或应用，将损失降至最低。
- *响应*：启用响应团队（包括高技能人才），采取行动保护备份，识别受影响的资产，并规划恢复行动。识别攻击源并调整保护措施，以避免攻击再次发生。
- *恢复*：在高技能人才就位并自动创建备份后，即可启动流程，创建恢复环境。备份应作为二级副本源使用，而非直接传输至可能仍会损坏的应用。如果系统依然在运转，那么通过取证分析，您可以确定哪些领域受到了影响，并指导恢复行动。根据损坏程度的不同，恢复的范围也大有不同。局部恢复可以用于解决特定文件或应用的损坏；而当损坏范围相当广时，您需要采用灾难性恢复，恢复整个系统。

每个企业都必须有独属于自己的企业弹性计划，他们应该通过执行风险评估流程，识别自身的具体需求。该计划将生成当前状态或概况的视图，并基于“目标”概况，发现改进或投资领域。随着您变更基础架构，构建新的业务流程，或者发现新类型的威胁，您应该相应地更新弹性计划。在大多数情况下，您需要结合利用网络弹性与产品和流程，实施更多传统的备份和 DR 实践。

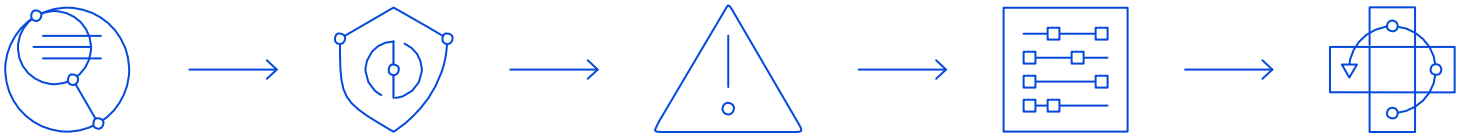
IBM Storage 系统提供一系列广泛的功能，让您能够实现弹性的 IT 运营，应对 LDC 攻击或意外中断。

IBM 的存储基础架构解决方案

IBM Storage 系统提供一系列广泛的功能，让您能够实现弹性的 IT 运营，应对 LDC 攻击或意外中断。综合型 IBM 解决方案整合了存储功能、网络配置、管理控制和物理安全功能。下面，我们介绍 IBM Storage 提供的一些重要的网络弹性解决方案和技术。

基于快照的传统备份和恢复

在满足传统备份要求时，快照（比如 IBM FlashCopy® 功能）已经成为了表现最佳、成本效益最高的方法之一。IBM DS8000® 数据系统、IBM Storwize® 系列阵列、IBM SAN Volume Controller、IBM FlashSystem® 9100、利用 IBM Spectrum® Virtualize 的 FlashSystem A9000 和 FlashSystem A9000R 软件定义存储实施、IBM Spectrum Scale、IBM Spectrum Accelerate 和 IBM Spectrum NAS 都支持 FlashCopy 功能。空间高效的只读数据副本提供经济高效的恢复点，用于快速复原以前的数据版本。利用快照从意外删除或损坏中恢复过来已经得到了广泛普及。IBM Redbooks® and Redpapers 中记录了不同的 FlashCopy 解决方案。[7, 8, 9] 数据备份能够针对部分 LDC 恶意软件攻击提供恢复点，但是不考虑额外的风险敞口，您依然会面临高级攻击。



借助 IBM Storwize 和 IBM FlashSystem 解决方案，保护快照

从 Storwize 或 FlashSystem 阵列现有的快照功能入手，您可以部署软件设施，在存储阵列中自动定期触发快照，从而配置更多弹性 LDC 保护解决方案。快照的频率决定了受保护数据的 RPO，同时利用更多存储资源降低 RPO。所保存备份的数量决定了找到完好无损的数据版本所需的回溯时长。您应该利用风险评估流程，识别适用于特定应用的策略。适用于该目的的软件解决方案包括 IBM Copy Storage Management、IBM Spectrum Copy Data Management 和 IBM Spectrum Protect Snapshot。

除了快照自动化外，您还面临如何保护快照的问题。其中一种方法是将存储卷从生产系统复制到同类型的次级存储系统。然后，您可以利用周期快照作为次级阵列上的恢复副本。软件应该提供自动化的复制和快照功能。非生产存储系统不能直接连接任意应用服务器，唯一一个活动的存储数据连接应该是备份副本传入的端口。管理员应该使用不同的密码登录，管理员登录由另一个人而非生产系统负责管理。非生产系统的管理员应该是网络弹性响应团队的成员。

系统之间的物理隔离与实施设计有关；距离更近，即使是在同一个数据中心里，您就能获得更高的性能和更低的网络成本；远程设施中也可以使用非生产存储解决方案进行灾难恢复。

在发生 LDC 恶意软件攻击或者测试恢复行动时，您应该将非生产系统上存储的数据副本当作恢复副本源使用，这些副本可以回传至生产存储系统。通过使用非生产存储系统，您可以在生产副本和受保护副本之间提供一个逻辑空气跳空。系统之间的物理隔离与实施设计有关；距离更近，即使是在同一个数据中心里，您就能获得更高的性能和更低的网络成本；远程设施中也可以使用非生产存储解决方案进行灾难恢复。

借助 IBM Spectrum Scale 保护快照

文件系统数据往往也是任务关键型运营的一部分，它们必须纳入网络弹性计划内。左边描述的方法使用了受保护的活动数据快照，可用于实施 IBM Spectrum Scale。

IBM Spectrum Scale 支持 DR 配置，并提供一个主生产站点和次级恢复站点。在真实的 DR 场景中，应按照基于灾难风险类型而确定的距离对这些系统进行隔离，此类风险类型包括当地水灾、停电或地震等风险。在实现网络弹性时，物理隔离不是必需的，但是网络弹性解决方案可与 DR 解决方案结合使用。IBM Spectrum Scale 在两个站点之间维护文件数据副本；基础技术是站点之间的数据复制技术，如 IBM Redbook *Spectrum Scale（前身为 GPFS）*中所述。[10]

然后，您可以在次级站点中获取代表备份的快照，用于在出现恶意软件攻击时恢复数据。如上所示，次级系统应该没有主机连接，并且其管理员登录与主站点的管理员登录不同。次级管理员应该是网络响应团队的成员。

除了生成快照外，IBM Spectrum Scale 还能够将数据复制到单写多读 (WORM) 磁带作为额外的保障措施。正如 "IBM Redbook *Active Archive Implementation Guide with IBM Spectrum Scale Object and IBM Spectrum Archive*" 报告所述，IBM Spectrum Scale 支持多个映射至独立物理存储的存储池。[11] 磁带就是其中一个支持的存储类型，它将作为 Linear Tape File System (LTFS) 安装到 IBM Spectrum Scale 存储池中。Linear Tape Open (LTO) 磁带可以部署为 WORM 介质，创建额外的不可变副本，免受恶意软件操作的影响。一旦攻击影响主系统操作，响应团队能够确定应该使用哪个副本在次级站点恢复数据。

DS8800 Safeguarded Copy

为了提供更高级别的自动化、更有力的保护和更深入的备份记录，IBM DS8880 存储阵列系列于 2018 年 9 月引入了 Safeguarded Copy 功能。Safeguarded Copy 是一个特殊版本的 FlashCopy；它会创建空间高效的只读副本，这些副本不能安装到外部服务器中，管理员也不能删除这些副本。您最高可以为每个 DS8880 卷创建 500 个副本，这样，用户就能针对受保护的数据创建大量记录。管理员至少需要两个界面，用于创建、启用和管理 Safeguarded Copy（DS8880 DS CLI 或 DS GUI），以配置备份容量和 IBM Copy Services Manager 来执行和管理 Safeguarded Copy 任务。副本可以保存在同一个生产存储系统中，或者复制到远程 DS8880 阵列中，这个阵列也是同步或异步复制的目标。

正如前面讨论的，您应该隔离次级 DS8880 存储系统，最小化它的攻击面。次级 DS8880 存储系统不能直接连接应用服务器，唯一一个活动的存储数据连接应该是备份副本传入的端口。管理员应该使用不同的密码登录，管理员登录由另一个人而非生产系统负责管理。非生产系统的管理员应该是网络弹性响应团队的成员。

如需详细了解 DS8880 Safeguarded Copy 解决方案的设计、规划和运营，请参阅 IBM Safeguarded Copy Redpaper。[12]

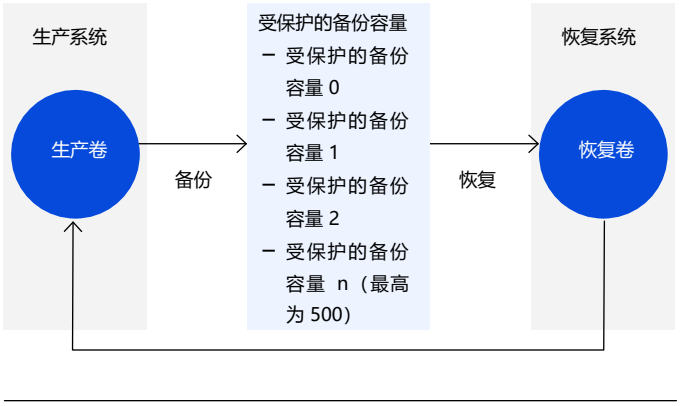


图 3：DS8800 Safeguard Copy 流程

网络弹性管理解决方案

IBM 针对网络弹性提供特定的管理解决方案，包括总体复制拓扑的认知和管理，以及服务器集成。这些解决方案包括面向 IBM Z® 服务器的 IBM GDPS® 逻辑损坏保护功能和 IBM i PowerHA® 工具集。

利用 WORM 介质，保护备份

IBM Spectrum Protect 提供功能强大的备份和归档软件系统。它能将所有数据副本移动到托管存储空间，并利用渐进式设计，存储变更的数据，维护备份版本。IBM Spectrum Protect 能够管理一系列存储池，包括闪存、磁盘、对象存储，或物理和虚拟磁带。

WORM 介质非常适合用于保护恢复副本。IBM TS1100 和 LTO 系列磁带机可为完全分离的介质提供额外的保护，除了通过库函数控制执行的访问外，不支持编程访问。盒式磁带可标记为 WORM，并用于写入恢复副本以避免其被磁带机覆写。一旦被标记为 WORM 盒带，应用或管理服务器中的任何恶意软件都不能毁坏备份副本。当然，您也必须考虑物理保护措施。TS7700 Virtual Tape 系统提供由存储控制器执行的逻辑 WORM 功能。

与空间高效的快照不同，您需要花费一定的时间才能移动写入磁带的所有副本中的数据，数据复原速度比快照中的复原速度更慢。您需要根据企业的具体需求采用自定义设计方式，但是您最好是采用全面防护，并利用备份，将数据保存在离线介质中，增强基于快照的恢复功能。如需了解更多详情，请查阅 IBM Spectrum Protect 产品文档。[13]

在 IBM Virtual Tape 上保护数据

IBM TS7700 Virtual Tape 系统提供 Logical WORM (LWORM) 功能，进而在物理磁带上提供 WORM 的软件版本。这有助于避免 LWORM 卷上面的数据被覆写，一旦创建了卷，您只能增补卷或让卷过期，不能修改卷。

您可以结合使用 LWORM 和 TS77OO 存储留存功能，及时将过期的磁带卷复原到前一个恢复点。借助存储留存功能，直到指定的时间到期之前，卷不会被重复使用。此外，在与磁带系统（如 IBM TS4500 和 TS7700）相集成后，它能在数据和在线黑客之间提供空气跳空功能，抵御网络攻击。

强大的磁带空气跳空保护

网络的设计目的在于在组织内流畅地传播信息。它能够精准地高效传输数据，这也让恶意软件能够快速地进入网络并在网络中传播，由此，组织就会面临内部暴露问题，以及潜在的外部暴露风险，具体取决于感染的系统。

如前所述，“空气跳空”一词指的是系统或网络的物理或虚拟隔离，以避免因恶意软件被感染、系统故障或人工失误而导致数据广泛损坏。空气跳空的基本理念是定期让次级存储系统上线，融合最新的变更，然后再让次级存储系统下线。这种解决方案方法利用快照功能创建副本，您可以快速安装这些副本，恢复受损的应用。但是复制数据的全面保护也有一些限制；在每种情况下，副本库都有某种类型的网络连接。

您可以使用磁带库，实施最全面的保护方法，即不允许任何网络或软件访问受保护的副本。IBM TS4500、TS4300 和 TS2900 磁带库仅在盒式磁带安装到磁带机时才允许访问该磁带。磁带“离线设计”的特性提供了一个真正的物理空气跳空和最安全的保护机制之一，用于抵御网络犯罪。如需详细了解如何利用磁带保护数据，包括使用空气跳空技术、WORM 和其他安全功能，请参阅 *“IBM Tape solutions provide modern and powerful data protection* solution brief”。[14]

网络的设计目的在于在组织内流畅地传播信息。它能够精准地高效传输数据，这也让恶意软件能够快速地进入网络并在网络中传播，由此，组织就会面临内部暴露问题，以及潜在的外部暴露风险，具体取决于感染的系统。

借助 IBM Cloud Object Storage，保护数据

IBM Cloud™ Object Storage 提供持久、安全且成本高效的云存储，用于归档和保护数据。IBM Cloud Object Storage 以 WORM 方式维持完整性，避免数据被删除或修改。借助策略定义，您可以灵活指定默认、最短和最长的留存期，帮助您满足数据留存要求。您还可以在对象层面利用依法留存功能，避免在指定审计活动完成之前删除数据。在将数据输入 IBM Cloud Object Storage 时，您可以对单一对象或多个对象使用留存期和依法留存功能。在留存期到期及所有依法留存数据被移除之前，对象均不会被删除。

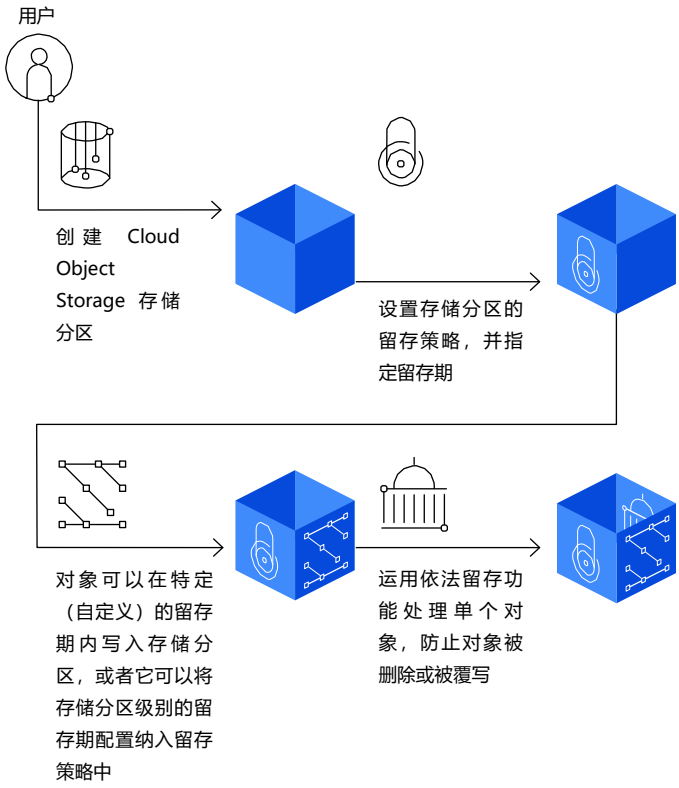


图 4：借助 IBM Cloud Object Storage，保护数据安全

借助 IBM Spectrum Protect 检测恶意软件

IBM 在 IBM Spectrum Protect 备份软件中增加了一个功能，以检测特定类型的恶意软件的操作，包括与 LDC 攻击有关的操作。当恶意软件用加密或损坏的版本覆写文件时，这些变更将被视为更新，IBM Spectrum Protect 备份软件将收集新数据。该解决方案将保存正常操作记录，恶意软件的活动与正常访问模式存在重大差异。2018 年 3 月，IBM Spectrum Protect Operations Center V8.1.5 发布了新的警报功能。[15] 在每个客户端备份会话结束后，它会分析统计数据，发现感染恶意软件的迹象。如果出现迹象，操作中心将显示警报消息。您可以通过新的安全通知页面，查看每个安全通知的详细信息。这些信息能帮助您确定客户端是否感染了恶意软件，或者警报通知是不是误报。

面向 21 世纪的网络弹性

在可预见的将来，意图拒绝访问或破坏数据的网络攻击可能依然是企业的主要风险。您必须利用技术和运营流程抵御网络攻击，并采取措施从成功的攻击中恢复过来，这也是设计周密的安全态势的重要组成部分。通过利用经过验证的技术和方法，比如 NIST 框架和风险管理理念，IBM Storage 产品可用于创建和实施网络弹性解决方案，帮助 21 世纪企业在新世纪蓬勃发展。

参考资料

1 “2018 Cost of a Data Breach Study: Global Overview”. *Ponemon Institute*. 2018 年 7 月.

2 “Investigation: WannaCry Cyber Attack and the NHS”. *Report by the Comptroller and Auditor General, National Audit Office*. 2018 年 4 月.

3 “Global Risks Report 2019, 14th Edition”. *World Economic Forum*, Geneva Switzerland, 2019 年.

4 Björck F.、Henkel M.、Stirna J.、Zdravkovic J. (2015) Cyber Resilience—Fundamentals for a Definition.In:Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies.Advances in Intelligent Systems and Computing, vol 353.Springer, Cham

5 Alexander Warmuth, Robert Tondini, Michael Frankenberg, Nick Clayton, and Bert Dufrasne, “DS8000 Safeguarded Copy”. *IBM Corp*. 2018 年 11 月

6 Phil Goodwin and Sean Pike. “Five key technologies for enabling a cyber resistant framework”. *IDC*. 2018 年 7 月.

7 Bert Dufrasne、Francesco Anderloni、Roger Eriksson 和 Lisa Martinez. “IBM FlashSystem A9000 and A9000R Business Continuity Solutions, A draft IBM Redpaper publication”. *IBM Corp*. 2018 年 11 月

8 Jon Tate、Rafael Viela Dias、Ivaylo Dikanarov、Jim Kelly 和 Peter Mescher. “IBM System Storage SAN Volume Controller and Storwize V7000 Replication Family Services”, *IBM Corp*. 2013 年 3 月.

9 Dino Quintero. “IBM Spectrum Scale (formerly GPFS)”. *IBM Corp*. 2015 年 5 月

10 Dino Quintero、Luis Bolinches、Puneet Chaudhary、Willard Davis、Steve Duersch、Carlos Henrique Fachim、Andrei Socoliuc 和 Olaf Weiser. “IBM Spectrum Scale (Formerly GPFS)”. *IBM Corp*. 2015 年.

11 Larry Coyne、Joe Dain、Khanh Ngo 和 Aaron Palazzolo. “Active Archive Implementation Guide with IBM Spectrum Scale Object and IBM Spectrum Archive”. *IBM Corp*. 2016 年.

12 Warmuth 等. Op.Cit.

13 “IBM Spectrum Protect Version 8.1.3 Tape Solution Guide”. *IBM Corp*. 2017 年.

14 “解决方案简述 - IBM 磁带解决方案可提供强大的现代化数据保护功能”. IBM Corp. *2019 年*. https://www.ibm.com/downloads/cas/Z5RV1AKP

15 “IBM Spectrum Protect V8.1.5 和 IBM Spectrum Protect Plus V10.1.1 可交付增强的性能及其他诸多功能”. 产品发布通告. *IBM Corp.*, March 2018.

IBM Corporation
New Orchard Road
Armonk, NY 10504

美国印刷
2019 年 6 月

29025229-CNZH-02 | 思想领导力白皮书