NetApp

NETAPP RANSOMWARE RESILIENCE

实时检测勒索软件攻击，防止数据丢失，快速恢复，并最大限度地减少对业务的影响

您准备好应对勒索软件攻击了吗?
应对勒索软件攻击的一个关键方面是保护存储层（最后一道防线）的工作负载数据。随着攻击变得越来越复杂、自动化且代价高昂，完全阻止勒索软件攻击已不现实。当攻击者入侵时你必须做好准备。

仅靠备份是不够的。您需要能够评估关键工作负载数据的风险，检测威胁并实时响应。您还需要制定可以快速轻松执行的恢复计划。然而，有效抵御勒索软件攻击往往伴随着运维负担，需要完成许多容易出错的手动任务，而且缺乏具备专业能力的员工。

如果没有建立防御机制，针对您的工作负载的攻击将无法被检测到，并且您的响应将会延迟。工作负载恢复将非常复杂 — 平均需要 7 天[1] — 并且您的数据甚至可能无法完全恢复。这无疑是杯水车薪，为时已晚！

在最后一道防线获得全面保护
NetApp® Ransomware Resilience 服务使您能够快速轻松地执行防御计划，覆盖从预防到检测、响应和恢复的全过程。

Ransomware Resilience 通过单一界面来智能地编排以工作负载为中心的勒索软件防御。只需单击几下，您就可以识别并保护处于危险中的关键工作负载数据。该服务还能准确、自动地检测和响应潜在的攻击并限制其影响。您可以不受恶意软件影响，在几分钟内恢复工作负载，保护您宝贵的数据并最大限度地降低对您的业务造成的损害和中断成本。

Ransomware Resilience 将 NetApp ONTAP® 软件的强大功能与 NetApp 数据服务相结合，通过自动化工作流程提供智能建议和指导，帮助：

- **识别。**自动识别 NetApp 存储中的工作负载（虚拟机、文件共享、流行数据库）及其数据，将数据映射到工作负载，并确定数据的敏感度、重要性和风险。
- **保护。**获取工作负载保护策略建议并一键应用。
- **检测。**实时检测可疑文件和用户行为活动，这可能预示着潜在的数据泄露尝试以及文件加密和大规模删除尝试。
- **响应。**当怀疑存在潜在攻击时，通过自动创建 NetApp Snapshot™ 副本并阻止用户来保护工作负载。该服务还与行业领先的安全信息和事件管理 (SIEM) 解决方案相集成。
- **恢复。**通过简单的编排恢复流程快速恢复工作负载及其相关数据。通过使用隔离的恢复环境，确保数据恢复后纯净且无恶意软件。
- **治理。**实施勒索软件防护战略和策略，并监控结果。

准备好防御攻击：节省时间并提高效率

Ransomware Resilience 服务可自动识别 NetApp 存储中的数据类型、将数据映射到特定工作负载、评估数据敏感性和关键性并分析风险。此过程减少了您对复杂的手动分析、额外的第三方工具和专业知识的依赖。

主要优势

在最后一道防线获得全面编排的防御：

- 全面了解您的工作负载保护状况。
- 尽早发现攻击并防止数据丢失。
- 不受恶意软件影响，快速地恢复整个工作负载，以最大限度地减少中断、成本损失、收入下滑和业务损害。
- 获取数据进行取证分析并提出建议以改善您的安全态势。

然后，Ransomware Resilience 服务使用 ONTAP 功能建议智能保护策略，包括具有 AI (ARP/AI) 异常检测的 NetApp 自主勒索软件防护、FPolicy 恶意扩展阻止和防篡改快照副本。Ransomware Resilience 服务还会根据数据资产的敏感度和关键程度定制保护建议。

只需单击一下，保护策略即可无缝且一致地应用于您的工作负载数据。Ransomware Resilience 服务在后台运行，以配置 ONTAP 和 NetApp 数据服务功能并编排每个数据卷的保护工作流程，从而减少重复手动任务的需要。

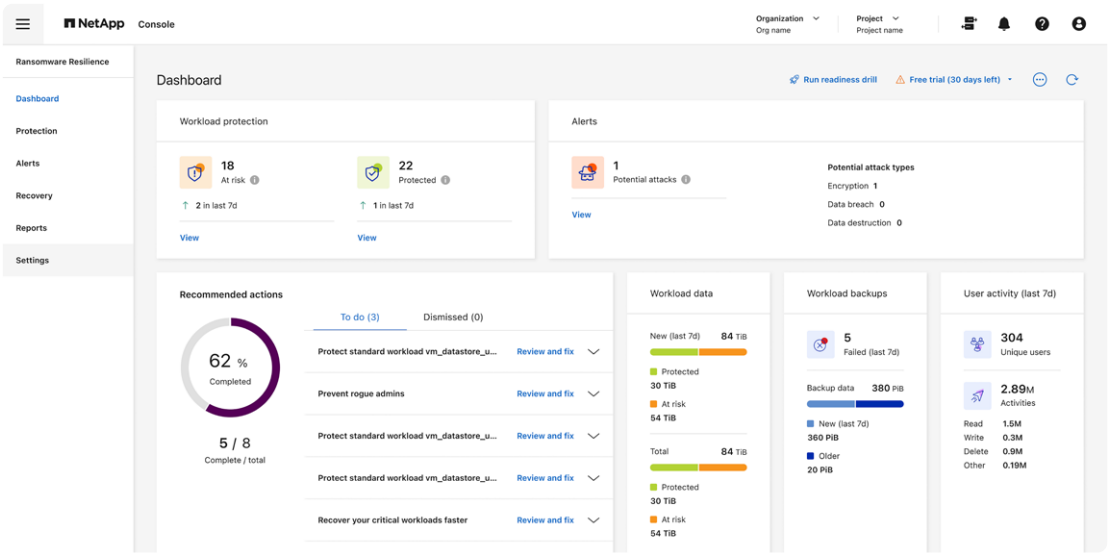
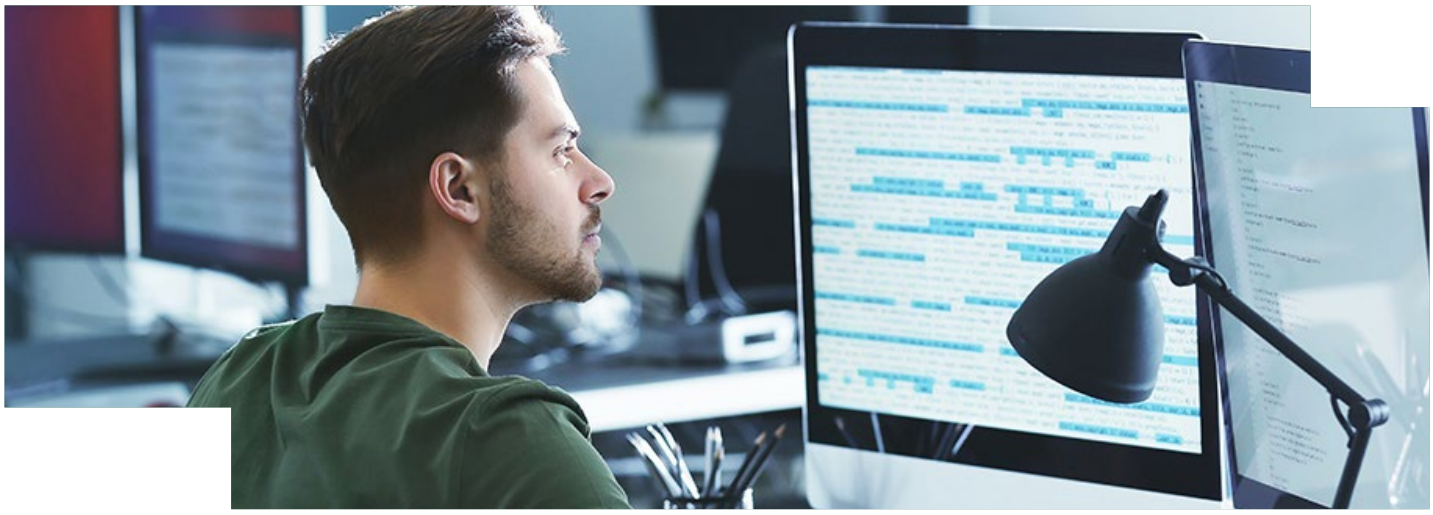


图 1：NetApp Ransomware Resilience 服务通过单一控制平台，提供从检测到恢复的全面编排的以工作负载为中心的勒索软件防御。



实时检测并响应威胁
Ransomware Resilience 服务持续监控可疑文件和用户行为异常。它通过识别早期用户行为来检测数据泄露，这些行为可能预示着潜在的数据泄露尝试以及文件加密和大规模删除尝试。当怀疑发生攻击时，Ransomware Resilience 服务会创建快照副本以防止数据丢失，并可阻止实施攻击的用户，及时制止其行为并防范后续攻击。

该服务在您的主存储上使用创新的、先进的基于 AI 的勒索软件检测。这种方法意味着可以快速发现潜在的攻击并立即采取规避措施。

Ransomware Resilience 服务提供事件报告以支持取证分析，并可与行业领先的 SIEM 解决方案集成。

几分钟内轻松恢复工作负载
Ransomware Resilience 服务可编排所有相关工作负载数据的应用程序一致性恢复工作流程，让您实时了解进度和状态。快照副本可以在工作负载级别还原，也可以更细粒度地在卷或文件级别还原。

作为恢复过程的一部分，Ransomware Resilience 服务提供一个隔离的恢复环境，可以隔离受感染的工作负载、删除恶意软件、推荐恢复点并通过直观界面引导用户完成恢复过程。这种方法可以确保数据恢复后干净且无恶意软件风险，防止数据再次感染。

最大限度地减少业务中断
Ransomware Resilience 服务消除了您对保护工作负载免受勒索软件相关停机和数据丢失的负担和焦虑。它提供全面的服务，可提高您的准备程度、及时响应攻击并指导您完成恢复。只有 NetApp 能让您高枕无忧：当攻击发生时，您会立即收到警报，您宝贵的工作负载数据将受到保护，并且恢复过程快速而简单 — 从而最大限度地减少对您业务的影响。

立即获取 NetApp Ransomware Resilience

[1] 环境、社会和治理 (ESG)，《2023 年勒索软件防御准备：照亮防御准备与缓解之路》2023 年 11 月。

联系我们

关于 NetApp

NetApp 是一家智能数据基础架构公司，通过融合统一数据存储、集成数据、运维和工作负载服务，致力于帮助每一位客户从瞬息万变的全球环境中寻找机遇。NetApp 可以构建无孤岛的基础架构，利用可观察性和 AI 技术，实现业界最佳的数据管理。作为唯一原生嵌入全球最大云平台的企业级存储服务，我们的数据存储解决方案提供无缝的灵活性。此外，我们的数据服务通过卓越的网络弹性、治理能力与应用敏捷性，打造差异化数据优势。我们的运维和工作负载服务通过可观察性和 AI 持续优化基础架构和工作负载的性能和效率。无论数据类型、工作负载或运行环境如何，NetApp 都能助您完成数据基础架构的转型升级，成就商业未来。要了解更多信息，请访问 **www.netapp.com/zh-hans** 或在 **X**、**LinkedIn**、**Facebook** 和 **Instagram** 上关注我们。

NetApp