NetApp Ransomware Resilience文档

NetApp Ransomware Resilience

NetApp
October 31, 2025

目录

NetApp Ransomware Resilience文档 1
发行说明 2
NetApp Ransomware Resilience的新功能 2
2025年10月6日 2
2025年8月12日 3
2025年7月15日 3
2025年6月9日 3
2025年5月13日 4
2025年4月29日 4
2025年4月14日 5
2025年3月10日 5
2024年12月16日 6
2024年11月7日 6
2024年9月30日 7
2024年9月2日 7
2024年8月5日 8
2024年7月1日 8
2024年6月10日 9
2024年5月14日 9
2024年3月5日 11
2023年10月6日 11
NetApp Ransomware Resilience的已知限制 12
准备演习重置选项问题 12
Amazon FSx for NetApp ONTAP限制 12
开始使用 13
了解NetApp Ransomware Resilience 13
数据层的勒索软件抵御能力 13
勒索软件恢复能力可以做什么 14
使用勒索软件恢复能力的好处 15
成本 15
许可 16
NetApp Console 16
勒索软件抵御能力的工作原理 16
支持的备份目标、系统和工作负载数据源 18
可能有助于您进行勒索软件防护的术语 19
NetApp Ransomware Resilience前提条件 19
在NetApp Console中 19
在ONTAP 9.11.1 及更高版本中 20
数据备份 20

可疑的用户行为 20
更新ONTAP系统中的非管理员用户权限 20
NetApp Ransomware Resilience快速入门 21
设置NetApp Ransomware Resilience 22
准备备份目标 22
设置NetApp Console 23
访问NetApp Ransomware Resilience 23
设置NetApp Ransomware Resilience的许可 24
其他许可证 25
试用 Ransomware Resilience 30 天免费试用版 25
通过 AWS Marketplace 订阅 26
通过 Microsoft Azure Marketplace 订阅 28
通过 Google Cloud Platform Marketplace 订阅 30
自带许可证 (BYOL) 32
控制台许可证到期后请更新 33
结束 PAYGO 订阅 34
发现NetApp Ransomware Resilience中的工作负载 34
选择要发现和保护的工作负载 35
发现先前选定的系统新创建的工作负载 37
发现新系统 37
在NetApp Ransomware Resilience中进行勒索软件攻击准备演练 37
配置勒索软件攻击准备演习 37
开始准备演习 40
响应战备演习警报 40
恢复测试工作负载 42
准备演练后更改警报状态 43
审查准备演习报告 43
在NetApp Ransomware Resilience中配置保护设置 44
直接访问设置页面 44
模拟勒索软件攻击 44
配置工作负载发现 45
可疑的用户活动 45
添加备份目标 45
连接到安全和事件管理系统 (SIEM) 进行威胁分析和检测 52
在NetApp Ransomware Resilience中配置可疑用户活动检测 57
代理商和收藏家 57
启用可疑用户活动检测 57
响应可疑用户活动警报 62
使用勒索软件弹性 63
使用NetApp Ransomware Resilience 63
使用 NetAPp 勒索软件恢复力仪表板监控工作负载健康状况 63

使用仪表板检查工作负载健康状况 63
查看仪表板上的保护建议 65
将保护数据导出到 CSV 文件 66
访问技术文档 67
保护工作负载 67
使用NetApp Ransomware Resilience保护策略保护工作负载 67
使用勒索软件恢复中的NetApp Data Classification扫描个人身份信息 80
使用NetApp Ransomware Resilience处理检测到的勒索软件警报 83
查看警报 84
回复警报电子邮件 85
检测恶意活动和异常用户行为 86
将勒索软件事件标记为准备恢复（事件被消除后） 87
忽略不属于潜在攻击的事件 88
查看受影响文件的列表 90
借助NetApp Ransomware Resilience，在勒索软件攻击发生后恢复 91
查看已准备好恢复的工作负载 92
还原由SnapCenter管理的工作负载 92
还原不受SnapCenter管理的工作负载 93
在NetApp Ransomware Resilience中下载报告 100
知识和支持 102
注册以获得支持 102
支持注册概述 102
注册BlueXP以获得NetApp支持 102
关联 NSS 凭据以获得Cloud Volumes ONTAP支持 104
获取帮助 106
获取云提供商文件服务的支持 106
使用自助选项 106
向NetApp支持创建案例 106
管理您的支持案例（预览） 108
关于NetApp Ransomware Resilience的常见问题解答 111
部署 111
使用权 111
互操作性 111
工作负载 112
保护策略 113
法律声明 114
版权 114
商标 114
专利 114
隐私政策 114
开源 114

NetApp Ransomware Resilience文档

发行说明

NetApp Ransomware Resilience的新功能

了解NetApp Ransomware Resilience的新功能。

2025年10月6日

BlueXP ransomware protection现已升级NetApp Ransomware Resilience

BlueXP ransomware protection服务已更名为NetApp Ransomware Resilience。

BlueXP现在是NetApp Console

NetApp Console提供企业级跨本地和云环境的存储和数据服务的集中管理，提供实时洞察、更快的工作流程和简化的管理。

有关更改的详细信息，请参阅 "NetApp Console发行说明"。

数据泄露检测

勒索软件恢复力包括一种新的检测机制，只需几个步骤即可激活，以检测异常用户读取作为数据泄露的早期指标。勒索软件弹性通过创建历史基线来收集和分析用户读取事件，该基线是根据过去数据得出的预期正常行为的概况。当新用户活动明显偏离既定规范（例如意外的阅读激增与可疑的阅读模式相结合）时，就会生成警报。勒索软件恢复力包括一个用于检测可疑读取模式的 AI 模型。

与存储层的 ARP 加密检测不同，勒索软件弹性 SaaS 服务通过收集 FPolicy 事件来检测用户行为异常。

> 您必须使用新的"勒索软件恢复用户行为管理员和勒索软件恢复用户行为查看器"角色来访问可疑用户行为检测设置。

有关详细信息，请参阅"启用可疑用户活动检测"和"查看异常用户行为"。

其他可疑用户活动检测

除了数据泄露检测之外，勒索软件恢复能力还根据观察到的可疑用户活动检测以下警报类型：

- 数据破坏 - 潜在攻击 - 当文件删除的数量超过历史标准时，会创建具有潜在攻击严重程度的警报。
- 可疑用户行为 - 潜在攻击 - 当观察到类似于勒索软件攻击的读取、重命名和删除操作时，会创建严重程度为潜在攻击的警报
- 可疑用户行为 - 警告 - 当文件活动（读取、删除、重命名等）的总数超过历史标准时，将创建严重程度为警告的警报

用于数据泄露检测的新用户角色

为了管理可疑用户活动警报，Ransomware Resilience 为控制台组织管理员引入了两个新角色，以授予对可疑用户活动检测的访问权限：Ransomware Resilience 用户行为管理员和 Ransomware Resilience 用户行为查看器。

您必须是用户行为管理员才能配置可疑用户行为设置。勒索软件恢复管理员角色不支持配置可疑用户行为设置。

有关更多信息，请参阅"NetApp Ransomware Resilience基于角色的访问" 。

2025年8月12日

该版本包括一般增强功能和改进功能。

2025年7月15日

SAN 工作负载支持

此版本包括对BlueXP ransomware protection中的 SAN 工作负载的支持。现在，除了 NFS 和 CIFS 工作负载之外，您还可以保护 SAN 工作负载。

有关详细信息，请参阅"BlueXP ransomware protection先决条件" 。

改进的工作负载保护

此版本改进了具有其他NetApp工具（如SnapCenter或BlueXP backup and recovery）的快照和备份策略的工作负载的配置过程。在以前的版本中， BlueXP ransomware protection发现了来自其他工具的策略，只允许您更改检测策略。在此版本中，您现在可以用BlueXP ransomware protection策略替换快照和备份策略，或者继续使用其他工具中的策略。

有关详细信息，请参阅"保护工作负载"。

电子邮件通知

如果BlueXP ransomware protection检测到可能的攻击， BlueXP通知中会出现通知，并且会向您配置的电子邮件地址发送电子邮件。

电子邮件包含有关严重性、受影响的工作负载的信息，以及BlueXP ransomware protection*警报* 选项卡中的警报链接。

如果您在BlueXP ransomware protection中配置了安全和事件管理 (SIEM) 系统，该服务会向您的 SIEM 系统发送警报详细信息。

有关详细信息，请参阅"处理检测到的勒索软件警报"。

2025年6月9日

登陆页面更新

此版本包括对BlueXP ransomware protection登陆页面的更新，使开始免费试用和发现变得更加容易。

准备演习更新

以前，您可以通过模拟对新样本工作负载的攻击来运行勒索软件准备演练。利用此功能，您可以调查模拟攻击并恢复工作负载。使用此功能来测试警报通知、响应和恢复。根据需要经常运行和安排这些演习。

在此版本中，您可以使用BlueXP ransomware protection仪表板上的新按钮在测试工作负载上运行勒索软件准备

演练，从而更轻松地模拟勒索软件攻击、调查其影响并有效地恢复工作负载，所有这些都在受控环境中完成。

现在，除了 NFS 工作负载之外，您还可以在 CIFS（SMB）工作负载上运行准备情况演练。

有关详细信息，请参阅 "进行勒索软件攻击准备演习"。

启用**BlueXP classification**更新

在BlueXP ransomware protection服务中使用BlueXP classification之前，您需要启用BlueXP classification来扫描您的数据。对数据进行分类有助于您找到个人身份信息 (PII)，这可能会增加安全风险。

您可以在BlueXP ransomware protection中对文件共享工作负载部署BlueXP classification。在*隐私暴露*栏中，选择*识别暴露*选项。如果您已启用分类服务，此操作将识别曝光。否则，在此版本中，对话框会显示部署BlueXP classification的选项。选择*部署*转到BlueXP classification服务登录页面，您可以在其中部署该服务。W

有关详细信息，请参阅 "在云中部署BlueXP classification"并在BlueXP ransomware protection内使用该服务，请参阅 "使用BlueXP classification扫描个人身份信息"。

2025年5月13日

BlueXP ransomware protection中不支持的工作环境报告

在发现工作流程期间，当您将鼠标悬停在“支持”或“不支持的工作负载”上时， BlueXP ransomware protection会报告更多详细信息。这将帮助您了解为什么您的某些工作负载未被BlueXP ransomware protection服务发现。

服务不支持工作环境的原因有很多，例如，工作环境中的ONTAP版本可能低于所需的版本。当您将鼠标悬停在未受支持的工作环境上时，工具提示会显示原因。

您可以在初始发现期间查看不受支持的工作环境，也可以在其中下载结果。您还可以从“设置”页面中的“工作负载发现”选项查看发现的结果。

有关详细信息，请参阅 "发现BlueXP ransomware protection中的工作负载"。

2025年4月29日

支持**Amazon FSx for NetApp ONTAP**

此版本支持Amazon FSx for NetApp ONTAP 。此功能可帮助您使用BlueXP ransomware protection来保护 FSx for ONTAP工作负载。

FSx for ONTAP是一项完全托管的服务，可在云中提供NetApp ONTAP存储的强大功能。它提供与您在本地使用的相同的功能、性能和管理能力，同时具有原生 AWS 服务的灵活性和可扩展性。

BlueXP ransomware protection工作流程进行了以下更改：

- Discovery 包括 FSx for ONTAP 9.15 工作环境中的工作负载。
- “保护”选项卡显示 FSx for ONTAP环境中的工作负载。在这种环境中，您应该使用 FSx for ONTAP备份服务执行备份操作。您可以使用BlueXP ransomware protection快照恢复这些工作负载。

无法在BlueXP中设置在 FSx for ONTAP上运行的工作负载的备份策略。 Amazon FSx for NetApp ONTAP中设置的任何现有备份策略均保持不变。

- 警报事件展示了新的 FSx for ONTAP工作环境。

有关详细信息，请参阅 "了解BlueXP ransomware protection和工作环境"。

有关受支持选项的信息，请参阅 "BlueXP ransomware protection的局限性"。

需要**BlueXP**访问角色

您现在需要以下访问角色之一来查看、发现或管理BlueXP ransomware protection：组织管理员、文件夹或项目管理员、勒索软件保护管理员或勒索软件保护查看器。

"了解所有服务的BlueXP访问角色" 。

2025年4月14日

准备演习报告

通过此版本，您可以查看勒索软件攻击准备演习报告。准备演练使您能够模拟对新创建的示例工作负载的勒索软件攻击。然后，调查模拟攻击并恢复样本工作负载。此功能可帮助您通过测试警报通知、响应和恢复过程来了解在发生实际勒索软件攻击时您是否已做好准备。

有关详细信息，请参阅 "进行勒索软件攻击准备演习"。

新的基于角色的访问控制角色和权限

以前，您可以根据用户的职责为其分配角色和权限，这有助于您管理用户对BlueXP ransomware protection的访问。在此版本中，有两个特定于BlueXP ransomware protection的新角色具有更新的权限。新角色如下：

- 勒索软件保护管理员
- 勒索软件保护查看器

有关权限的详细信息，请参阅 "BlueXP ransomware protection基于角色的功能访问"。

付款改进

此版本对支付流程进行了多项改进。

有关详细信息，请参阅 "设置许可和付款选项"。

2025年3月10日

模拟攻击并做出响应

通过此版本，模拟勒索软件攻击来测试您对勒索软件警报的响应。此功能可帮助您通过测试警报通知、响应和恢复过程来了解在发生实际勒索软件攻击时您是否已做好准备。

有关详细信息，请参阅 "进行勒索软件攻击准备演习"。

发现过程的增强

此版本包括对选择性发现和重新发现过程的增强：

- 通过此版本，您可以发现添加到先前选择的工作环境中的新创建的工作负载。
- 您还可以在此版本中选择_新_工作环境。此功能可帮助您保护添加到环境中的新工作负载。
- 您可以在最初的发现过程中或在设置选项中执行这些发现过程。

有关详细信息，请参阅 "发现先前选定的工作环境的新创建的工作负载"和 "使用“设置”选项配置功能"。

检测到高度加密时发出警报

在此版本中，即使没有高文件扩展名更改，您也可以在工作负载上检测到高加密时查看警报。此功能使用ONTAP自主勒索软件防护 (ARP) AI，可帮助您识别面临勒索软件攻击风险的工作负载。使用此功能并下载受影响文件的完整列表（无论扩展名是否更改）。

有关详细信息，请参阅 "响应检测到的勒索软件警报"。

2024年12月16日

使用**Data Infrastructure Insights**存储工作负载安全检测异常用户行为

在此版本中，您可以使用Data Infrastructure Insights存储工作负载安全来检测存储工作负载中的异常用户行为。此功能可帮助您识别潜在的安全威胁并阻止潜在的恶意用户以保护您的数据。

有关详细信息，请参阅 "响应检测到的勒索软件警报"。

在使用Data Infrastructure Insights存储工作负载安全检测异常用户行为之前，您需要使用BlueXP ransomware protection*设置* 选项来配置该选项。

参考 "配置BlueXP ransomware protection设置"。

选择要发现和保护的工作负载

在此版本中，您现在可以执行以下操作：

- 在每个连接器中，选择您想要发现工作负载的工作环境。如果您想保护环境中的特定工作负载而不是其他工作负载，您可能会受益于此功能。
- 在工作负载发现期间，您可以启用每个连接器的工作负载自动发现。此功能可让您选择要保护的工作负载。
- 发现先前选择的工作环境的新创建的工作负载。

参考 "发现工作负载"。

2024年11月7日

启用数据分类并扫描个人身份信息 **(PII)**

在此版本中，您可以启用BlueXP classification（ BlueXP系列的核心组件）来扫描和分类文件共享工作负载中的数据。对数据进行分类可以帮助您识别数据是否包含个人信息或私人信息，这可能会增加安全风险。此过程还会影响工作负载的重要性，并帮助您确保使用适当的保护级别来保护工作负载。

部署了BlueXP classification的客户通常可以在BlueXP ransomware protection中扫描 PII 数据。 BlueXP classification作为BlueXP平台的一部分提供，无需额外付费，并且可以在本地或客户云中部署。

参考 "配置BlueXP ransomware protection设置"。

要启动扫描，请在“保护”页面上，单击“隐私暴露”列中的“识别暴露”。

"使用BlueXP classification扫描个人身份敏感数据" 。

SIEM 与 **Microsoft Sentinel** 集成

现在，您可以使用 Microsoft Sentinel 将数据发送到安全和事件管理系统 (SIEM) 以进行威胁分析和检测。以前，您可以选择 AWS Security Hub 或 Splunk Cloud 作为您的 SIEM。

"了解有关配置BlueXP ransomware protection设置的更多信息" 。

立即免费试用 **30** 天

随着此版本的发布， BlueXP ransomware protection的新部署现在有 30 天的免费试用期。此前， BlueXP ransomware protection提供 90 天的免费试用。如果您已享受 90 天免费试用，则该优惠将持续 90 天。

在文件级别恢复 **Podman** 的应用程序工作负载

在文件级别恢复应用程序工作负载之前，您现在可以查看可能受到攻击影响的文件列表并确定要恢复的文件。以前，如果组织（以前是帐户）中的BlueXP连接器正在使用 Podman，则此功能将被禁用。它现在已为 Podman 启用。您可以让BlueXP ransomware protection选择要恢复的文件，您可以上传列出受警报影响的所有文件的 CSV 文件，或者您可以手动识别要恢复的文件。

"了解有关从勒索软件攻击中恢复的更多信息" 。

2024年9月30日

文件共享工作负载的自定义分组

在此版本中，您现在可以将文件共享分组，以便更轻松地保护您的数据资产。该服务可以同时保护组中的所有卷。以前，您需要单独保护每个卷。

"了解有关在勒索软件保护策略中分组文件共享工作负载的更多信息" 。

2024年9月2日

来自**Digital Advisor**的安全风险评估

BlueXP ransomware protection现在从NetApp Digital Advisor收集有关集群的高安全风险和严重安全风险的信息。如果发现任何风险， BlueXP ransomware protection会在仪表板的*推荐操作*窗格中提供建议：“修复集群 <name> 上的已知安全漏洞。”从仪表板上的建议中，单击“查看并修复”建议查看Digital Advisor和常见漏洞和暴露 (CVE) 文章以解决安全风险。如果存在多个安全风险，请查看Digital Advisor中的信息。

参考 "Digital Advisor文档"。

备份到 **Google Cloud Platform**

在此版本中，您可以将备份目标设置为 Google Cloud Platform 存储桶。以前，您只能将备份目标添加到NetApp StorageGRID、Amazon Web Services 和 Microsoft Azure。

"了解有关配置BlueXP ransomware protection设置的更多信息" 。

支持 **Google Cloud Platform**

该服务现在支持适用于 Google Cloud Platform 的Cloud Volumes ONTAP进行存储保护。此前，该服务仅支持适用于 Amazon Web Services 和 Microsoft Azure 的Cloud Volumes ONTAP以及本地 NAS。

"了解BlueXP ransomware protection以及支持的数据源、备份目标和工作环境" 。

基于角色的访问控制

您现在可以使用基于角色的访问控制 (RBAC) 限制对特定活动的访问。 BlueXP ransomware protection使用BlueXP的两个角色： BlueXP帐户管理员和非帐户管理员（查看者）。

有关每个角色可以执行的操作的详细信息，请参阅 "基于角色的访问控制权限"。

2024年8月5日

使用 **Splunk Cloud** 进行威胁检测

您可以自动将数据发送到您的安全和事件管理系统 (SIEM) 进行威胁分析和检测。在以前的版本中，您只能选择 AWS Security Hub 作为您的 SIEM。在此版本中，您可以选择 AWS Security Hub 或 Splunk Cloud 作为您的 SIEM。

"了解有关配置BlueXP ransomware protection设置的更多信息" 。

2024年7月1日

自带许可证 **(BYOL)**

在此版本中，您可以使用 BYOL 许可证，它是您从NetApp销售代表处获得的NetApp许可证文件 (NLF)。

"了解有关设置许可的详细信息" 。

在文件级别恢复应用程序工作负载

在文件级别恢复应用程序工作负载之前，您现在可以查看可能受到攻击影响的文件列表并确定要恢复的文件。您可以让BlueXP ransomware protection选择要恢复的文件，您可以上传列出受警报影响的所有文件的 CSV 文件，或者您可以手动识别要恢复的文件。

> 在此版本中，如果帐户中的所有BlueXP连接器均未使用 Podman，则启用单个文件恢复功能。否则，该帐户将被禁用。

"了解有关从勒索软件攻击中恢复的更多信息" 。

下载受影响文件的列表

在文件级别恢复应用程序工作负载之前，您现在可以访问“警报”页面以 CSV 文件形式下载受影响文件的列表，然后使用“恢复”页面上传该 CSV 文件。

"了解有关在恢复应用程序之前下载受影响文件的更多信息" 。

删除保护计划

通过此版本，您现在可以删除勒索软件保护策略。

"了解有关保护工作负载和管理勒索软件保护策略的更多信息" 。

2024年6月10日

主存储上的快照副本锁定

启用此功能可锁定主存储上的快照副本，以便即使勒索软件攻击进入备份存储目标，它们在一定时间内也无法被修改或删除。

"了解有关在勒索软件保护策略中保护工作负载和启用备份锁定的更多信息" 。

支持适用于 **Microsoft Azure** 的**Cloud Volumes ONTAP**

此版本除了支持适用于 AWS 的Cloud Volumes ONTAP和本地ONTAP NAS 之外，还支持适用于 Microsoft Azure 的Cloud Volumes ONTAP作为系统。

"Azure 中的Cloud Volumes ONTAP快速入门"

"了解BlueXP ransomware protection" 。

Microsoft Azure 添加为备份目标

您现在可以将 Microsoft Azure 与 AWS 和NetApp StorageGRID一起添加为备份目标。

"了解有关如何配置保护设置的更多信息" 。

2024年5月14日

许可更新

您可以注册 90 天免费试用。很快您将能够通过 Amazon Web Services Marketplace 购买即用即付订阅或自带NetApp许可证。

"了解有关设置许可的详细信息" 。

CIFS 协议

该服务现在支持使用 NFS 和 CIFS 协议的 AWS 系统中的本地ONTAP和Cloud Volumes ONTAP 。以前的版本仅支持 NFS 协议。

工作负载详情

此版本现在在保护和其他页面的工作负载信息中提供了更多详细信息，以改进工作负载保护评估。从工作负载详细信息中，您可以查看当前分配的策略并查看配置的备份目标。

"详细了解如何在“保护”页面中查看工作负载详细信息" 。

应用程序一致性和虚拟机一致性保护和恢复

现在，您可以使用NetApp SnapCenter软件执行应用程序一致性保护，并使用SnapCenter Plug-in for VMware vSphere虚拟机一致性保护，从而实现静止和一致的状态，以避免以后需要恢复时可能的数据丢失。如果需要恢复，您可以将应用程序或虚拟机恢复到任何先前可用的状态。

"了解有关保护工作负载的更多信息" 。

勒索软件防护策略

如果工作负载上不存在快照或备份策略，您可以创建勒索软件防护策略，其中可以包含您在此服务中创建的以下策略：

- Snapshot 策略
- 备份策略
- 检测策略

"了解有关保护工作负载的更多信息" 。

威胁检测

现在可以使用第三方安全和事件管理 (SIEM) 系统启用威胁检测。仪表板现在显示“启用威胁检测”的新建议，可以在“设置”页面上进行配置。

"了解有关配置“设置”选项的详细信息" 。

消除误报

从“警报”选项卡中，您现在可以消除误报或决定立即恢复数据。

"详细了解如何响应勒索软件警报" 。

检测状态

新的检测状态出现在“保护”页面上，显示应用于工作负载的勒索软件检测的状态。

"了解有关保护工作负载和查看保护状态的更多信息" 。

下载 **CSV** 文件

您可以从保护、警报和恢复页面下载 CSV 文件*。

"详细了解如何从仪表板和其他页面下载 CSV 文件" 。

文档链接

查看文档链接现在包含在 UI 中。您可以从仪表板垂直*操作*访问此文档  选项。选择“新增功能”查看发行说明中的详细信息，或选择“文档”查看BlueXP ransomware protection文档主页。

BlueXP backup and recovery

BlueXP backup and recovery服务不再需要在系统上启用。看"前提条件" 。 BlueXP ransomware protection服务可帮助通过“设置”选项配置备份目标。看"配置设置" 。

设置选项

您现在可以在BlueXP ransomware protection设置中设置备份目的地。

"了解有关配置“设置”选项的详细信息" 。

2024年3月5日

保护策略管理

除了使用预定义策略之外，您现在还可以创建策略。 "了解有关管理策略的更多信息" 。

二级存储的不变性（**DataLock**）

现在，您可以使用对象存储中的NetApp DataLock 技术使备份在二级存储中不可变。 "了解有关创建保护策略的更多信息" 。

自动备份到**NetApp StorageGRID**

除了使用 AWS，您现在还可以选择StorageGRID作为备份目的地。 "了解有关配置备份目标的更多信息" 。

调查潜在攻击的附加功能

您现在可以查看更多取证详细信息来调查检测到的潜在攻击。 "详细了解如何响应检测到的勒索软件警报" 。

恢复过程

恢复过程得到了加强。现在，您可以按卷或所有卷恢复工作负载。 "了解有关从勒索软件攻击中恢复的更多信息（事件被消除后）" 。

"了解BlueXP ransomware protection" 。

2023年10月6日

BlueXP ransomware protection服务是一种用于保护数据、检测潜在攻击以及从勒索软件攻击中恢复数据的 SaaS 解决方案。

对于预览版，该服务可分别保护BlueXP组织内本地 NAS 存储上的 Oracle、MySQL、VM 数据存储和文件共享以及 AWS 上的Cloud Volumes ONTAP （使用 NFS 协议）的基于应用程序的工作负载，并将数据备份到 Amazon Web Services 云存储。

BlueXP ransomware protection服务充分利用了多种NetApp技术，以便您的数据安全管理员或安全运营工程师能够实现以下目标：

- 一目了然地查看所有工作负载的勒索软件保护情况。
- 深入了解勒索软件防护建议
- 根据BlueXP ransomware protection建议改进防护态势。
- 分配勒索软件保护策略，以保护您的主要工作负载和高风险数据免受勒索软件攻击。
- 监控您的工作负载的健康状况，防范勒索软件攻击并查找数据异常。
- 快速评估勒索软件事件对您的工作量的影响。
- 通过恢复数据并确保不会再次感染存储的数据，智能地从勒索软件事件中恢复。

"了解BlueXP ransomware protection" 。

NetApp Ransomware Resilience的已知限制

已知限制标识了该产品的此版本不支持或不能与其正确互操作的平台、设备或功能。仔细审查这些限制。

准备演习重置选项问题

如果您选择ONTAP 9.11.1 卷进行勒索软件攻击准备演习，勒索软件恢复能力会发送警报。如果您使用“克隆到卷”选项恢复数据并重置钻机，则重置操作将失败。

Amazon FSx for NetApp ONTAP限制

勒索软件恢复能力支持Amazon FSx for NetApp ONTAP系统。该系统有以下限制：

- Fsx for ONTAP不支持备份策略。在这种环境下，您应该使用Amazon FSx执行备份操作。您可以使用勒索软件恢复功能恢复这些工作负载。
- 恢复操作仅从快照执行。

开始使用

了解NetApp Ransomware Resilience

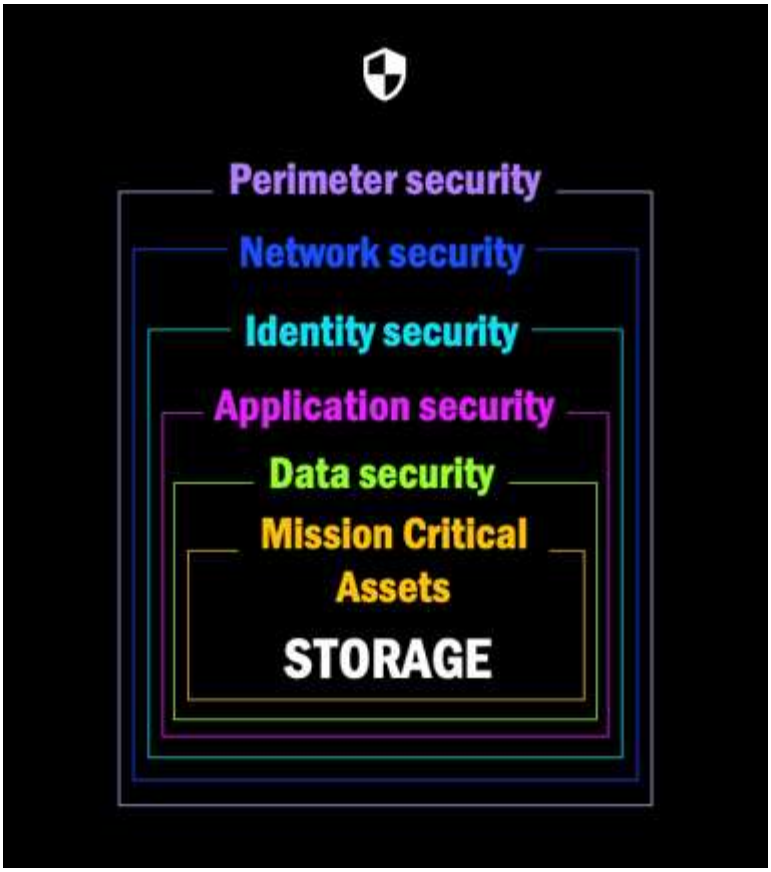
勒索软件攻击可以阻止对您数据的访问，攻击者可以要求赎金以换取数据发布或解密。据 IDC 称，勒索软件受害者遭受多次勒索软件攻击的情况并不少见。攻击可能会中断您对数据的访问，时间从一天到几周不等。

NetApp Ransomware Resilience可保护您的数据免受勒索软件攻击。在勒索软件恢复能力中，可以对基于应用程序的工作负载提供保护，包括本地 NAS 存储（使用 NFS 和 CIFS 协议）和 SAN 存储（FC、iSCSI 和 NVMe ）上的 Oracle、MySQL、VM 数据存储区和文件共享，以及适用于 Amazon Web Services 的Cloud Volumes ONTAP 、适用于 Google Cloud 的Cloud Volumes ONTAP 、适用于 Microsoft Azure 的Cloud Volumes ONTAP 和NetApp Console上的Amazon FSx for NetApp ONTAP 。您可以将数据备份到 Amazon Web Services 、Google Cloud、Microsoft Azure 云存储和NetApp StorageGRID。

数据层的勒索软件抵御能力

您的安全态势通常包含多层防御，以防御一系列网络威胁。

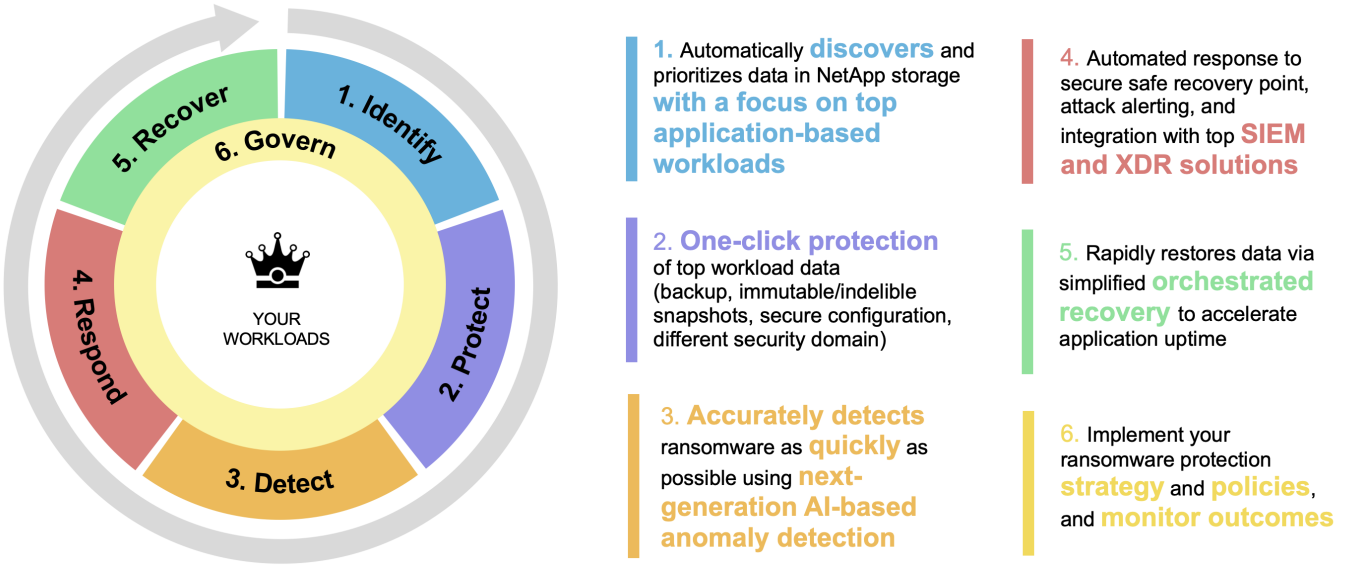
- 最外层：这是使用防火墙、入侵检测系统和虚拟专用网络来保护网络边界的第一道防线。
- 网络安全：这一层建立在网络分段、流量监控和加密的基础上。
- 身份安全：使用身份验证方法、访问控制和身份管理来确保只有授权用户才能访问敏感资源。
- 应用程序安全：使用安全编码实践、安全测试和运行时应用程序自我保护来保护软件应用程序。
- 数据安全：通过数据保护、备份和恢复策略保护您的数据。勒索软件恢复力在此层上运行。



勒索软件恢复能力可以做什么

勒索软件恢复功能充分利用了多种NetApp技术，以便您的存储管理员、数据安全管理员或安全运营工程师可以实现以下目标：

- 识别 NetApp Console、项目和控制台代理中的NetApp内部部署 NAS（NFS 或 CIFS）和 SAN（FC、iSCSI 和 NVMe）系统中所有基于应用程序、文件共享或 VMware 管理的工作负载。勒索软件弹性对数据优先级进行分类，并为您提供勒索软件弹性改进的建议。
- 通过对数据启用备份、快照副本和勒索软件保护策略来*保护*您的工作负载。
- *检测*可能是勒索软件攻击的异常。脚注：[尽管攻击可能未被发现，但我们的研究表明， NetApp技术已对某些基于文件加密的勒索软件攻击实现了高度检测。]
- 通过自动启动锁定的防篡改NetApp ONTAP快照来*应对*潜在的勒索软件攻击，这样副本就不会被意外或恶意删除。您的备份数据将保持不变，并在源头和目标端受到端到端的保护，免受勒索软件攻击。
- 通过协调多种NetApp技术来*恢复*您的工作负载，从而帮助加快工作负载的正常运行时间。您可以选择恢复特定的卷。勒索软件弹性提供有关最佳选项的建议。
- 管理：实施勒索软件保护策略并监控结果。



使用勒索软件恢复能力的好处

勒索软件恢复能力具有以下优势：

- 发现工作负载及其现有的快照和备份计划，并对其相对重要性进行排序。
- 评估您的勒索软件防护态势并将其显示在易于理解的仪表板中。
- 根据发现和保护态势分析提供后续步骤的建议。
- 一键访问即可应用 AI/ML 驱动的数据保护建议。
- 保护顶级基于应用程序的工作负载中的数据，例如 MySQL、Oracle、VMware 数据存储和文件共享。
- 使用人工智能技术实时检测针对主存储数据的勒索软件攻击。
- 通过创建快照副本和启动有关异常活动的警报来启动自动操作以响应检测到的潜在攻击。
- 应用精心策划的恢复以满足 RPO 政策。勒索软件恢复能力通过使用多种NetApp恢复服务（包括NetApp Backup and Recovery（以前称为云备份）和SnapCenter）来协调勒索软件事件的恢复。
- 使用基于角色的访问控制 (RBAC) 来管理对功能和操作的访问。

成本

NetApp不会向您收取使用 Ransomware Resilience 试用版的费用。

> 随着 2024 年 10 月的发布，Ransomware Resilience 的新部署提供了 30 天的免费试用。此前，Ransomware Resilience 提供了 90 天的免费试用。如果您已经注册了 90 天免费试用，则该试用有效期为 90 天。

如果您同时拥有备份和恢复以及勒索软件恢复功能，则受这两种产品保护的任何公共数据仅由勒索软件恢复功能计费。

购买许可证或 PayGo 订阅后，任何启用了勒索软件检测策略（自主勒索软件保护）（由勒索软件恢复力发现或设置）且至少有一个快照或备份策略的工作负载，勒索软件恢复力都会将其归类为“受保护”，并计入购买的容量或 PayGo 订阅。如果发现工作负载没有检测策略，即使它有备份或快照策略，也会被归类为“有风险”，并且不

会计入购买的容量。

90 天试用期结束后，受保护的工作负载将计入购买的容量或订阅。勒索软件恢复按每 GB 为与受保护工作负载相关的数据（在效率之前）收费。

许可

借助 Ransomware Resilience，您可以使用不同的许可计划，包括免费试用、即用即付订阅或自带许可证。

勒索软件恢复需要NetApp ONTAP One 许可证。

勒索软件恢复许可证不包括其他NetApp产品。即使您没有许可证，Ransomware Resilience 也可以使用备份和恢复。

为了检测异常用户行为，Ransomware Resilience 使用NetApp Autonomous Ransomware Protection，这是ONTAP内的一种机器学习 (ML) 模型，可检测恶意文件活动。该模型包含在勒索软件恢复许可证中。

有关详细信息，请参阅"设置许可" 。

NetApp Console

可通过NetApp Console访问勒索软件恢复功能。

NetApp Console提供企业级跨本地和云环境的NetApp存储和数据服务的集中管理。需要控制台才能访问和使用NetApp数据服务。作为管理界面，它使您能够从一个界面管理许多存储资源。控制台管理员可以控制企业内所有系统的存储和服务的访问。

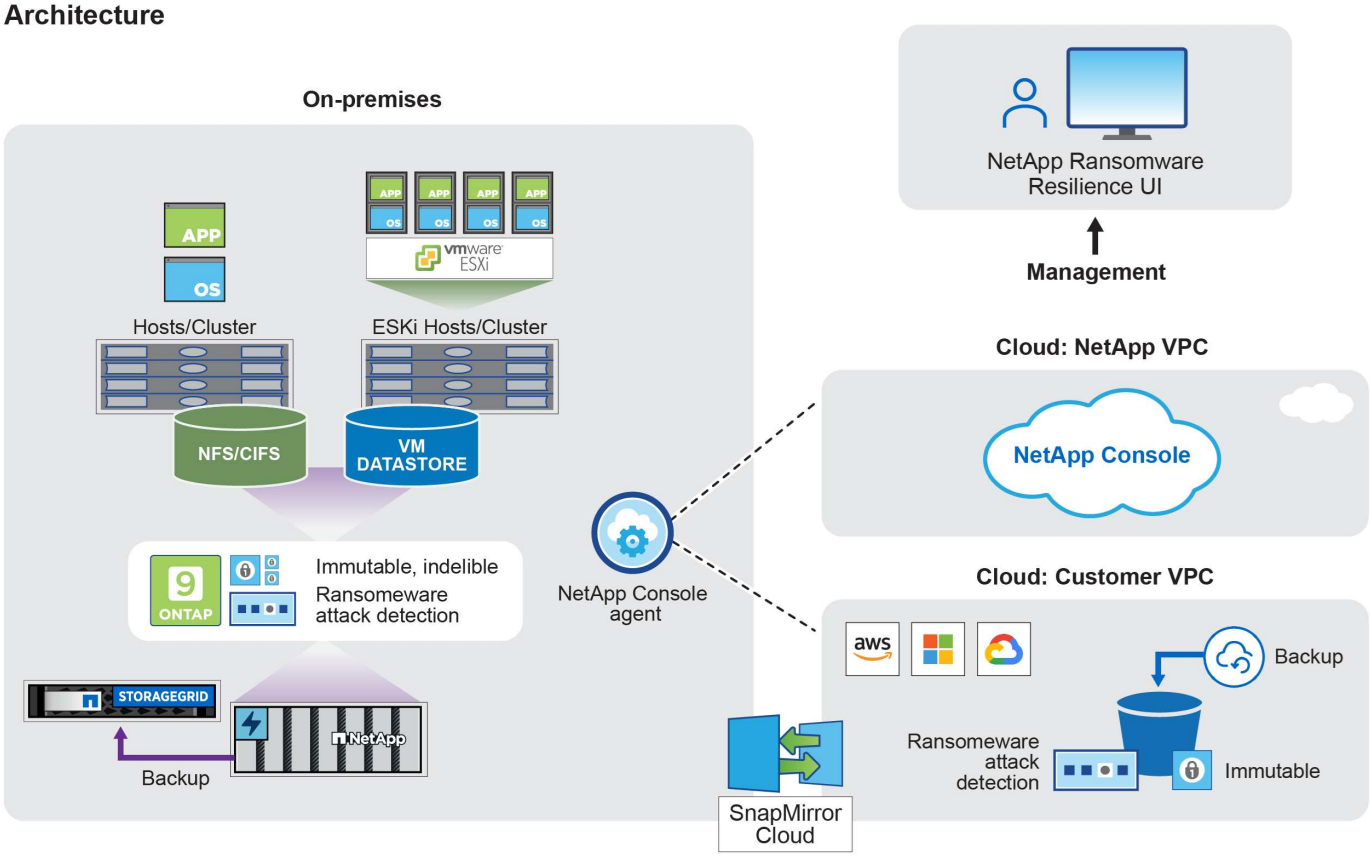
您不需要许可证或订阅即可开始使用NetApp Console，并且只有当您需要在云中部署控制台代理以确保与存储系统或NetApp数据服务的连接时才需要付费。但是，一些可从控制台访问的NetApp数据服务是需要许可或基于订阅的。

详细了解"NetApp Console"。

勒索软件抵御能力的工作原理

Ransomware Resilience 使用NetApp Backup and Recovery来发现和设置文件共享工作负载的快照和备份策略，使用SnapCenter或SnapCenter for VMware 来发现和设置应用程序和虚拟机工作负载的快照和备份策略。此外，Ransomware Resilience 使用备份和恢复以及SnapCenter / SnapCenter for VMware 来执行文件和工作负载一致的恢复。

Architecture



功能	描述
确认	• 查找连接到控制台的所有客户本地 NAS（NFS 和 CIFS 协议）、SAN（FC、iSCSI 和 NVMe）和Cloud Volumes ONTAP数据。 • 从ONTAP和SnapCenter服务 API 中识别客户数据并将其与工作负载关联。详细了解 "ONTAP"和 "SnapCenter软件"。 • 发现每个卷的当前NetApp快照副本和备份策略的保护级别以及任何机上检测功能。然后，勒索软件恢复能力通过使用备份和恢复、 ONTAP服务和NetApp技术（例如自主勒索软件保护（ARP 或 ARP/AI，取决于您的ONTAP版本）、FPolicy、备份策略和快照策略）将此保护态势与工作负载相关联。详细了解 "自主勒索软件防护"， "NetApp Backup and Recovery" ， 和 "ONTAP FPolicy"。 • 根据自动发现的保护级别为每个工作负载分配业务优先级，并根据工作负载的业务优先级推荐保护策略。工作负载优先级基于已应用于与工作负载相关的每个卷的快照频率。
保护	• 通过将策略应用于每个已识别的工作负载，主动监控工作负载并协调备份和恢复、SnapCenter和ONTAP API 的使用。

功能	描述
探测	• 使用集成机器学习 (ML) 模型检测潜在攻击，该模型可检测潜在的异常加密和活动。 • 提供双层检测，首先检测主存储中的潜在勒索软件攻击，然后通过获取额外的自动快照副本来创建最近的数据还原点，以响应异常活动。勒索软件恢复能力能够更深入地挖掘以更精确地识别潜在攻击，而不会影响主要工作负载的性能。 • 使用ONTAP、自主勒索软件防护（ARP 或 ARP/AI，取决于您的ONTAP版本）和 FPolicy 技术确定攻击相关工作负载的特定可疑文件和映射。
回应	• 显示相关数据，例如文件活动、用户活动和熵，以帮助您完成有关攻击的取证审查。 • 使用NetApp技术和产品（例如ONTAP、自主勒索软件防护（ARP 或 ARP/AI，取决于您的ONTAP版本）和 FPolicy）启动快速快照副本。
恢复	• 通过使用备份和恢复、 ONTAP、自主勒索软件防护（ARP 或 ARP/AI，取决于您的ONTAP版本）以及 FPolicy 技术和服务，确定最佳快照或备份并推荐最佳恢复点实际 (RPA)。 • 协调包括虚拟机、文件共享、块存储和数据库在内的工作负载的恢复，并保持应用程序的一致性。
治理	• 分配勒索软件保护策略 • 帮助您监控结果。

支持的备份目标、系统和工作负载数据源

勒索软件恢复支持以下备份目标、系统和数据源：

支持的备份目标

- 亚马逊网络服务（AWS）S3
- Google Cloud Platform
- 微软 Azure Blob
- NetAppStorageGRID

支持的系统

- 本地ONTAP NAS（使用 NFS 和 CIFS 协议），采用ONTAP版本 9.11.1 及更高版本
- 本地ONTAP SAN（使用 FC、iSCSI 和 NVMe 协议），采用ONTAP版本 9.17.1 及更高版本
- 适用于 AWS 的Cloud Volumes ONTAP 9.11.1 或更高版本（使用 NFS 和 CIFS 协议）
- 适用于 Google Cloud Platform 的Cloud Volumes ONTAP 9.11.1 或更高版本（使用 NFS 和 CIFS 协议）
- 适用于 Microsoft Azure 的Cloud Volumes ONTAP 9.12.1 或更高版本（使用 NFS 和 CIFS 协议）
- 适用于 AWS、Google Cloud Platform 和 Microsoft Azure 的Cloud Volumes ONTAP 9.17.1 或更高版本（使用 FC、iSCSI 和 NVMe 协议）
- Amazon FSx for NetApp ONTAP，使用自主勒索软件防护（ARP 而非 ARP/AI）

ARP/AI 需要ONTAP 9.16 或更高版本。

不支持以下内容： FlexGroup卷、早于 9.11.1 的ONTAP版本、挂载点卷、挂载路径卷、离线卷和数据保护 (DP) 卷。

支持的工作负载数据源

勒索软件恢复能力可保护主数据卷上的以下基于应用程序的工作负载：

- NetApp文件共享
- 块存储
- VMware 数据存储区
- 数据库（MySQL 和 Oracle）
- 更多内容即将推出

此外，如果您使用SnapCenter或SnapCenter for VMware，则这些产品支持的所有工作负载也会在 Ransomware Resilience 中得到识别。勒索软件恢复能力可以以工作负载一致的方式保护和恢复这些内容。

可能有助于您进行勒索软件防护的术语

了解一些与勒索软件保护相关的术语可能会对您有所帮助。

- 保护：勒索软件恢复中的保护意味着确保使用保护策略定期在不同的安全域中进行快照和不可变备份。
- 工作负载：勒索软件恢复中的工作负载可以包括 MySQL 或 Oracle 数据库、VMware 数据存储区或文件共享。

NetApp Ransomware Resilience前提条件

通过验证您的操作环境、登录、网络访问和 Web 浏览器的准备情况，开始使用NetApp Ransomware Resilience。

要使用勒索软件恢复能力，您需要满足以下先决条件。

在NetApp Console中

- 具有组织管理员权限的NetApp Console用户帐户，用于发现资源。
- 一个控制台组织，其中至少有一个活动的控制台代理连接到本地ONTAP集群或者 AWS 或 Azure 中的Cloud Volumes ONTAP 。
- 控制台代理必须具有 `cloudmanager-ransomware-protection`容器处于活动状态。
- 至少一个具有NetApp本地ONTAP集群或 AWS 或 Azure 中的Cloud Volumes ONTAP 的控制台系统。勒索软件恢复支持 NAS（NFS 和 SMB）和 SAN（iSCSI、FC 和 NVMe）协议。
  - ONTAP或Cloud Volumes ONTAP集群（ ONTAP版本 9.11.1 或更高版本）支持勒索软件恢复功能。

如果您计划在 SAN 工作负载上使用勒索软件恢复能力，则必须运行ONTAP 9.17.1 或更高版本。

- 如果您的本地ONTAP集群或 AWS 或 Azure 云中的Cloud Volumes ONTAP尚未在控制台中登录，则需要控制台代理。

  参考 "了解如何配置控制台代理"和 "标准控制台要求"。

  如果您在单个控制台组织中拥有多个控制台代理，则勒索软件恢复功能将扫描除控制台 UI 中当前选择的代理之外的所有控制台代理中的ONTAP资源。

在ONTAP 9.11.1 及更高版本中

- 本地ONTAP实例上启用了ONTAP One 许可证。
- NetApp Autonomous Ransomware Protection 许可证（由 Ransomware Resilience 使用）在本地ONTAP实例上启用，具体取决于您使用的ONTAP版本。参考 "自主勒索软件防护概述"。

  与预览版不同，Ransomware Resilience 的正式版包含NetApp Autonomous Ransomware Protection 技术的许可证。参考 "自主勒索软件防护概述"了解详情。

  有关更多许可详细信息，请参阅"了解勒索软件抵御能力"。

- 要应用保护配置（例如启用自主勒索软件保护等），勒索软件恢复能力需要ONTAP集群上的管理员权限。ONTAP集群应该仅使用ONTAP集群管理员用户凭据进行加入。
- 如果已使用非管理员用户凭据在控制台中登录ONTAP集群，则必须通过登录ONTAP集群来更新非管理员用户权限，如本页所述。

数据备份

- NetApp StorageGRID、AWS S3、Azure Blob 或 Google Cloud Platform 中用于备份目标的帐户以及设置的访问权限。

  请参阅 "AWS、Azure 或 S3 权限列表"了解详情。

- 不需要在系统上启用NetApp Backup and Recovery 。

  勒索软件恢复力有助于通过设置选项配置备份目标。看"配置设置" 。

可疑的用户行为

为了使勒索软件恢复能力提供有关可疑用户行为的警报，您必须配置用户活动代理。有关详细信息，请参阅 "在NetApp Ransomware Resilience中配置可疑用户活动检测"。

更新ONTAP系统中的非管理员用户权限

如果您需要更新特定系统的非管理员用户权限，请完成以下步骤。

1. 登录控制台并查找需要更新其ONTAP用户权限的系统。

2. 选择系统以查看详细信息。
3. 选择“查看其他信息”以显示用户名。
4. 使用管理员用户登录ONTAP集群 CLI。
5. 显示该用户的现有角色。进入：

```
security login show -user-or-group-name <username>
```

6. 更改用户的角色。进入：

```
security login modify -user-or-group-name <username> -application
console|http|ontapi|ssh|telnet -authentication-method password -role
admin
```

7. 返回勒索软件恢复 UI 来使用它。

NetApp Ransomware Resilience快速入门

了解设置勒索软件保护功能和保护工作负载所需遵循的高级步骤。

按照每个步骤中的链接获取详细信息。

1 审查先决条件

这些任务需要_Console admin_角色。

- "确保已安装控制台代理"
- "确保您的系统满足要求"
- "审查勒索软件恢复用户角色并为访问勒索软件恢复的用户分配权限"
- "设置许可"

2 开始使用勒索软件抵御能力

这些任务需要“勒索软件恢复管理员”角色。

- "在控制台中发现工作负载"
- "在仪表板上查看工作负载保护健康状况"
- "（可选）进行勒索软件攻击准备演习"

3 在 **Ransomware Resilience** 中配置保护和检测

这些任务需要“勒索软件恢复管理员”角色。配置可疑用户行为活动需要额外的“勒索软件恢复用户行为管理员”角

色。

- "保护工作负载"
  - 可选地，"通过配置可疑用户活动检测来增强保护"
- （可选）配置备份目标：
  - "准备NetApp StorageGRID、Amazon Web Services、Google Cloud Platform 或 Microsoft Azure 作为备份目标"。
  - "配置备份目标"
- "响应检测到的潜在勒索软件攻击"
- "从攻击中恢复（事件消除后）"

4 下一步是什么？

在勒索软件恢复中配置保护后，您可以执行以下操作。

- "启用数据分类来识别治理和安全风险"
- "向 SIEM 发送警报"
- "下载警报、保护、准备演习、恢复或摘要报告"

设置NetApp Ransomware Resilience

您可以轻松部署NetApp Ransomware Resilience。在开始之前，请查看"前提条件"以确保您的环境已准备就绪。

准备备份目标

准备以下备份目标之一：

- NetAppStorageGRID
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure

在备份目标本身中配置选项后，您稍后会将其配置为 Ransomware Resilience 中的备份目标。有关如何在 Ransomware Resilience 中配置备份目标的详细信息，请参阅"配置备份目标"。

准备**StorageGRID**以成为备份目标

如果要使用StorageGRID作为备份目标，请参阅 "StorageGRID文档"有关StorageGRID的详细信息。

准备 **AWS** 成为备份目标

- 在 AWS 中设置一个帐户。
- 配置 "AWS 权限"在 AWS 中。

有关在控制台中管理 AWS 存储的详细信息，请参阅 "管理您的 Amazon S3 存储桶"。

准备 **Azure** 以成为备份目标

- 在 Azure 中设置一个帐户。
- 配置 "Azure 权限"在 Azure 中。

有关在控制台中管理 Azure 存储的详细信息，请参阅 "管理 Azure 存储帐户"。

设置NetApp Console

下一步是设置控制台和勒索软件恢复能力。

审查 "标准模式的控制台要求"。

创建控制台代理

联系您的NetApp销售代表试用或使用此服务。然后，当您使用控制台代理时，它将包含适当的勒索软件恢复功能。

要使用勒索软件恢复功能创建控制台代理，请联系具有创建控制台代理权限的控制台组织管理员，并参考描述 "如何创建控制台代理"。

如果您有多个控制台代理，则勒索软件恢复功能会扫描除控制台中当前显示的代理之外的所有控制台代理的数据。该服务发现与该组织相关的所有项目和所有控制台代理。

访问NetApp Ransomware Resilience

通过NetApp Console登录到NetApp Ransomware Resilience 。

要登录控制台，您可以使用您的NetApp支持站点凭据，也可以使用您的电子邮件和密码注册NetApp云登录。 "了解有关登录的更多信息" 。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员、勒索软件恢复管理员或勒索软件恢复查看器角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

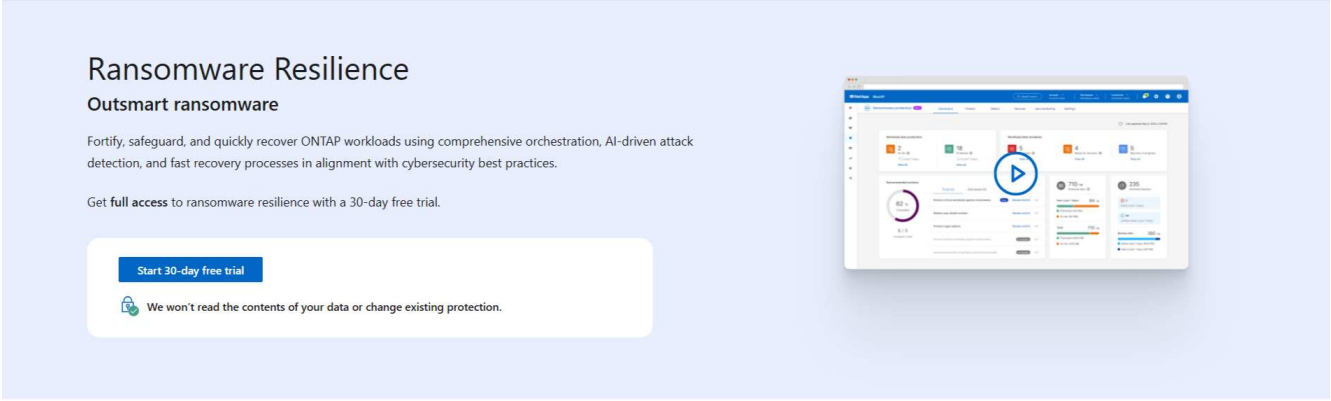
1. 打开网络浏览器并转到"控制台"。

   出现控制台登录页面。

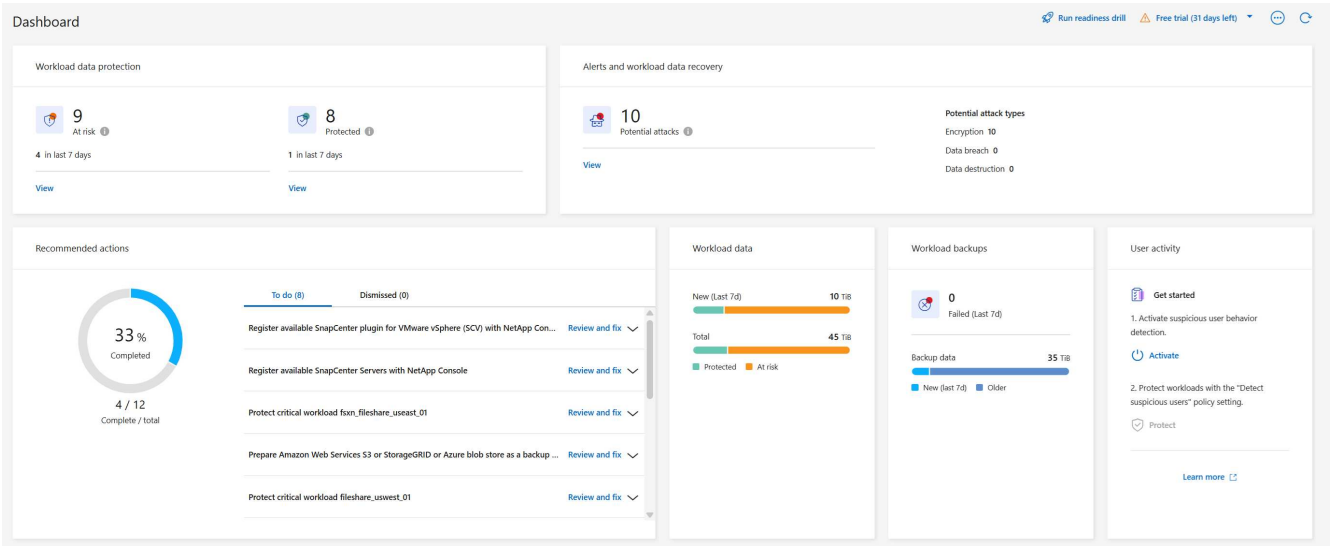
2. 登录控制台。
3. 从控制台左侧导航中，选择*保护*>*勒索软件恢复*。

   如果这是您第一次登录此服务，则会出现登录页面。

   如果您没有控制台代理或者它不是此服务的代理，则需要部署一个。"了解如何设置控制台代理" 。



否则，将出现勒索软件恢复力仪表板。



4. 如果您还没有这样做，请选择“发现工作负载”选项。

   请参阅"发现工作负载" 。

设置NetApp Ransomware Resilience的许可

借助NetApp Ransomware Resilience，您可以使用不同的许可计划。

要执行此任务，您需要组织管理员、文件夹或项目管理员角色。 "了解控制台访问角色" 。

许可证类型 勒索软件恢复能力适用于以下许可证类型：

- 30天免费试用
- 通过 Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace 或 Azure Marketplace 购买即

用即付 (PAYGO) 订阅

- 自带许可证 (BYOL)：您从NetApp销售代表处获得的NetApp许可证文件 (NLF)。您可以使用许可证序列号在控制台中激活 BYOL。

设置 BYOL 或购买 PAYGO 订阅后，您可以在控制台的Licenses and subscriptions部分看到许可证。

免费试用期结束或者许可证或订阅到期后，您仍然可以：

- 查看工作负载和工作负载健康状况
- 删除策略等资源
- 运行在试用期间或许可证下创建的所有计划操作

其他许可证

勒索软件恢复许可证不包括其他NetApp产品。但是，即使您没有单独的备份和恢复许可证，勒索软件恢复能力也可以与NetApp Backup and Recovery集成。

如果您同时拥有备份和恢复以及勒索软件恢复功能，则受这两种产品保护的任何公共数据将仅由勒索软件恢复功能计费。

试用 **Ransomware Resilience 30** 天免费试用版

您可以免费试用 Ransomware Resilience 30 天。您必须是控制台组织管理员才能开始免费试用。

试用期间不强制执行存储容量限制。

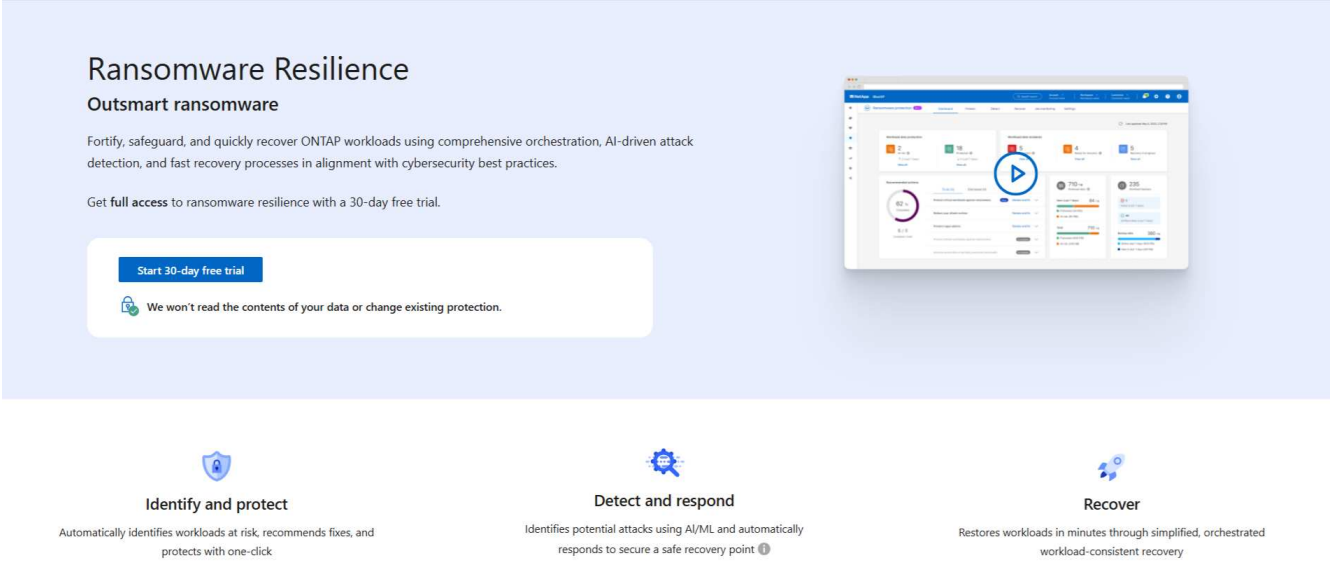
您可以随时获得许可证或订阅，并且在 30 天试用期结束之前不会向您收费。要在 30 天试用期后继续使用，您需要购买 BYOL 许可证或 PAYGO 订阅。

在试用期间，您可以使用全部功能。

步骤

1. 访问 "控制台"。
2. 登录控制台。
3. 从NetApp Console中，选择“保护”>“勒索软件恢复能力”。

   如果这是您第一次登录此服务，则会出现登录页面。



4. 如果您尚未为其他服务添加控制台代理，"添加一个" 。
5. 在勒索软件恢复登陆页面中，选择*从发现工作负载开始*来发现您的工作负载。

   仅当您成功安装了控制台代理后，此选项才可用。

6. 要查看免费试用信息，请选择右上角的下拉选项。

试用结束后，获取订阅或许可

免费试用结束后，您可以通过其中一个市场进行订阅，也可以从NetApp购买许可证。

如果您已经拥有 PAYGO 订阅，则免费试用结束后许可证将自动切换到订阅。

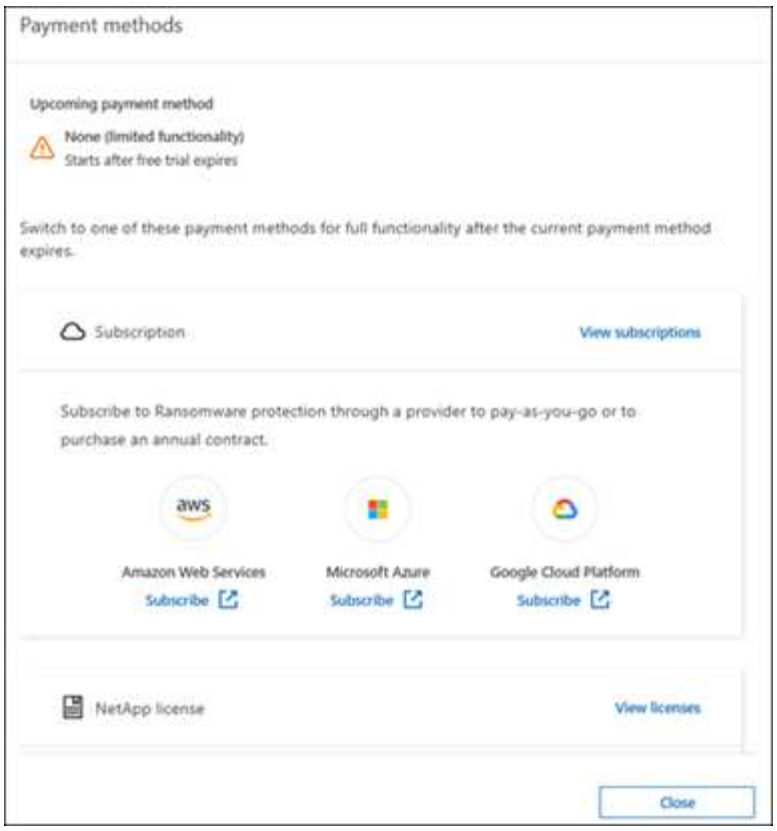
通过 AWS Marketplace 订阅 通过 Microsoft Azure Marketplace 订阅 通过 Google Cloud Platform Marketplace 订阅 自带许可证 (BYOL)

通过 **AWS Marketplace** 订阅

此过程提供了如何在 AWS Marketplace 中直接订阅的高级概述。

步骤

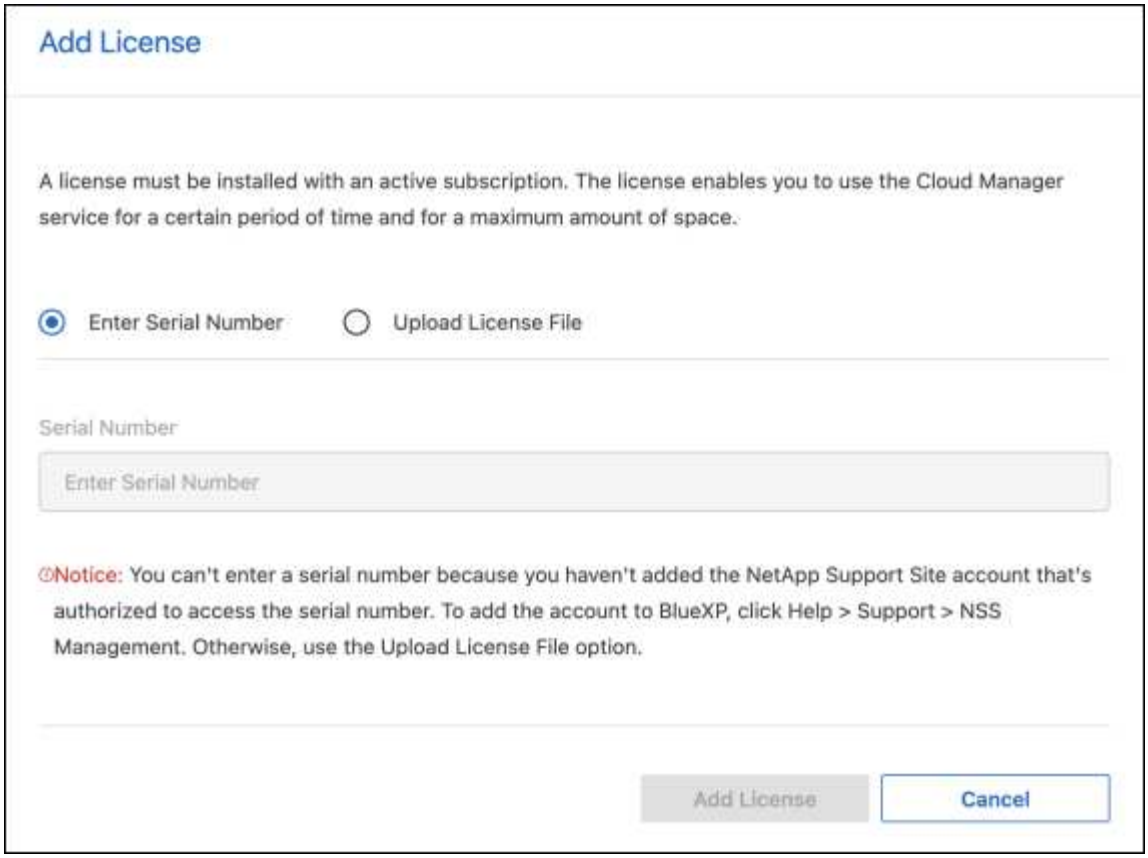
1. 在“勒索软件恢复”中，执行以下操作之一：
   - 如果您收到一条消息表明免费试用即将到期，请选择*查看付款方式*。
   - 如果您尚未开始试用，请选择右上角的*免费试用*通知，然后选择*查看付款方式*。



2. 在付款方式页面中，选择“订阅”**Amazon Web Services**。
3. 在 AWS Marketplace 中，选择 查看购买选项。
4. 使用 AWS Marketplace 订阅 * NetApp Intelligent Services* 和 * 勒索软件恢复能力 *。
5. 当您返回 Ransomware Resilience 时，会出现一条消息表明您已订阅。

> 系统会向您发送一封电子邮件，其中包含 Ransomware Resilience 序列号，并表明您已在 AWS Marketplace 中订阅 Ransomware Resilience。

6. 返回勒索软件恢复付款方式页面。
7. 通过选择“添加许可证”将许可证添加到控制台。



8. 在添加许可证页面中，选择*输入序列号*，输入发送给您的电子邮件中包含的序列号，然后选择*添加许可证*。
9. 要查看许可证详细信息，请从控制台左侧导航中选择“管理”>“**Licenses and subscriptions**”。
   - 要查看订阅信息，请选择*订阅*。
   - 要查看 BYOL 许可证，请选择“数据服务许可证”。
10. 返回勒索软件恢复能力。从控制台左侧导航中，选择*保护*>*勒索软件恢复*。

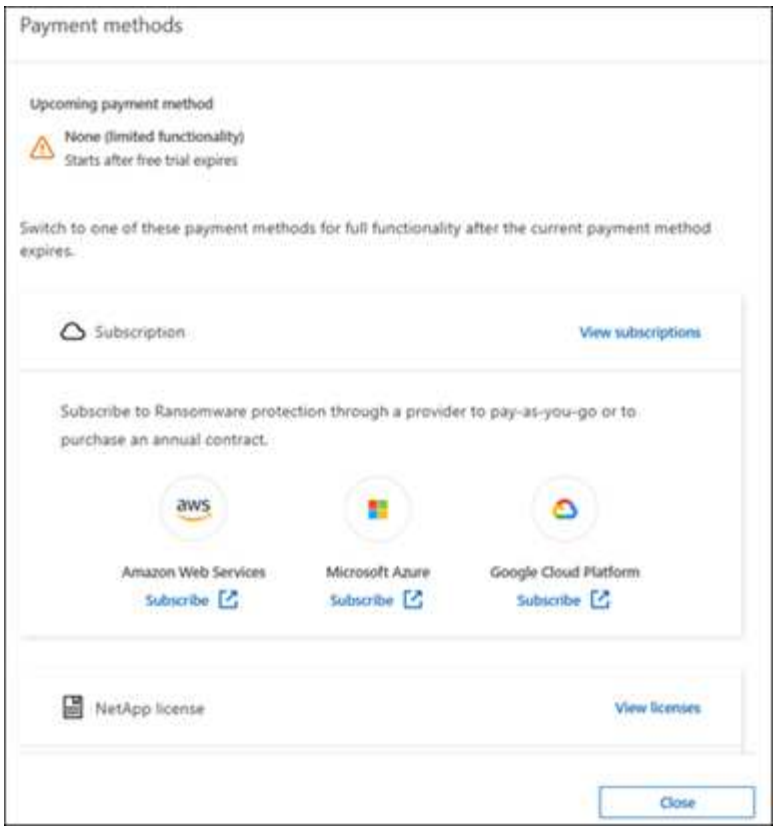
    一条消息确认许可证已添加。

通过 **Microsoft Azure Marketplace** 订阅

此过程提供了如何在 Azure 市场中直接订阅的高级概述。

步骤

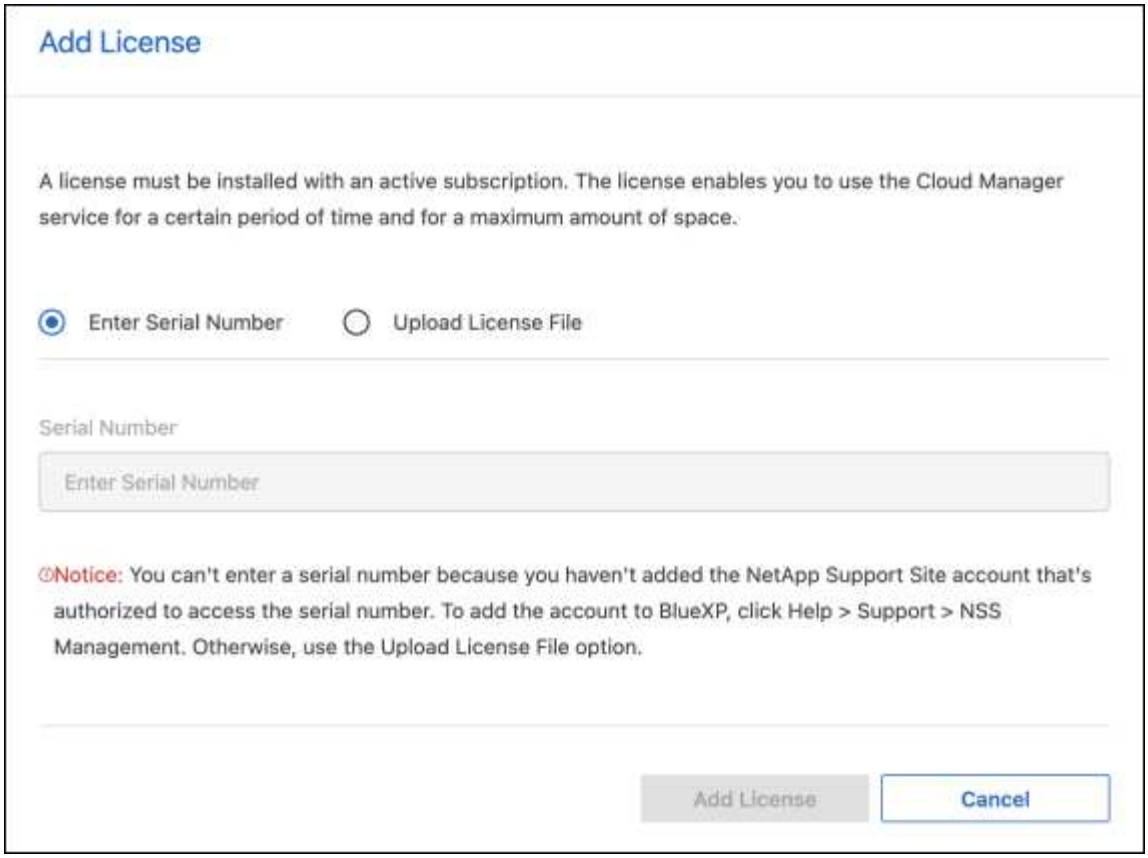
1. 在“勒索软件恢复”中，执行以下操作之一：
   - 如果您收到一条消息表明免费试用即将到期，请选择*查看付款方式*。
   - 如果您尚未开始试用，请选择右上角的*免费试用*通知，然后选择*查看付款方式*。



2. 在付款方式页面中，选择“订阅”**Microsoft Azure Marketplace**。
3. 在 Azure 市场中，选择“查看购买选项”。
4. 使用 Azure Marketplace 订阅 * NetApp Intelligent Services* 和 * 勒索软件恢复能力 *。
5. 当您返回 Ransomware Resilience 时，会出现一条消息表明您已订阅。

> 系统会向您发送一封电子邮件，其中包含 Ransomware Resilience 序列号，并表明已在 Azure 市场中订阅 Ransomware Resilience。

6. 返回勒索软件恢复付款方式页面。
7. 要添加许可证，请选择*添加许可证*。



8. 在添加许可证页面中，选择*输入序列号*，然后输入发送给您的电子邮件中的序列号。选择*添加许可证*。
9. 要查看Licenses and subscriptions中的许可证详细信息，请从控制台左侧导航中选择“治理”>“Licenses and subscriptions”。
   - 要查看订阅信息，请选择*订阅*。
   - 要查看 BYOL 许可证，请选择“数据服务许可证”。
10. 返回勒索软件恢复能力。从控制台左侧导航中，选择*保护*>*勒索软件恢复*。

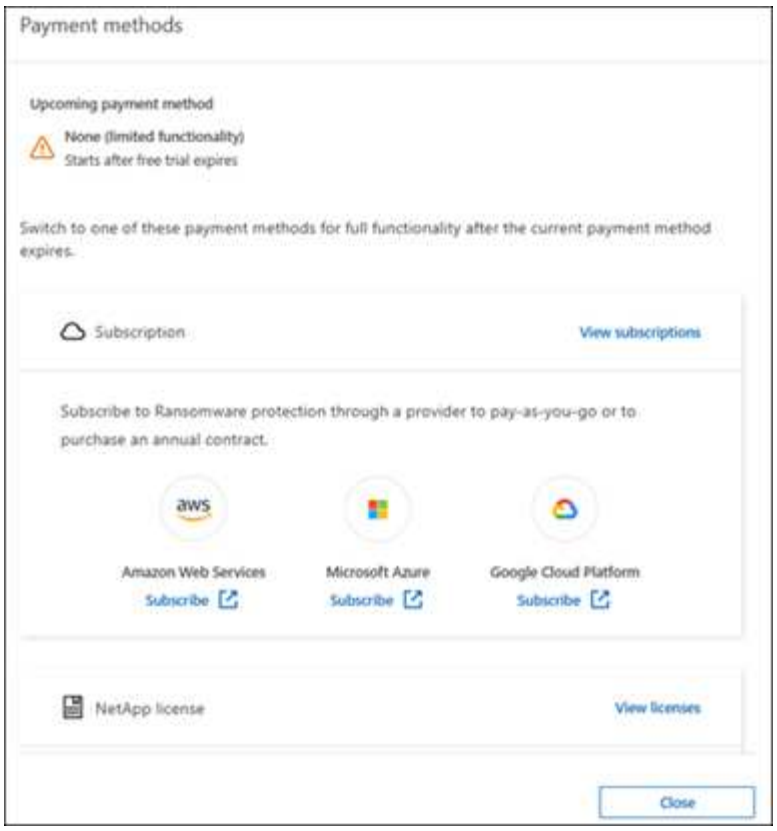
    出现一条消息，表明已添加许可证。

通过 **Google Cloud Platform Marketplace** 订阅

此过程概述了如何在 Google Cloud Platform Marketplace 中直接订阅。

步骤

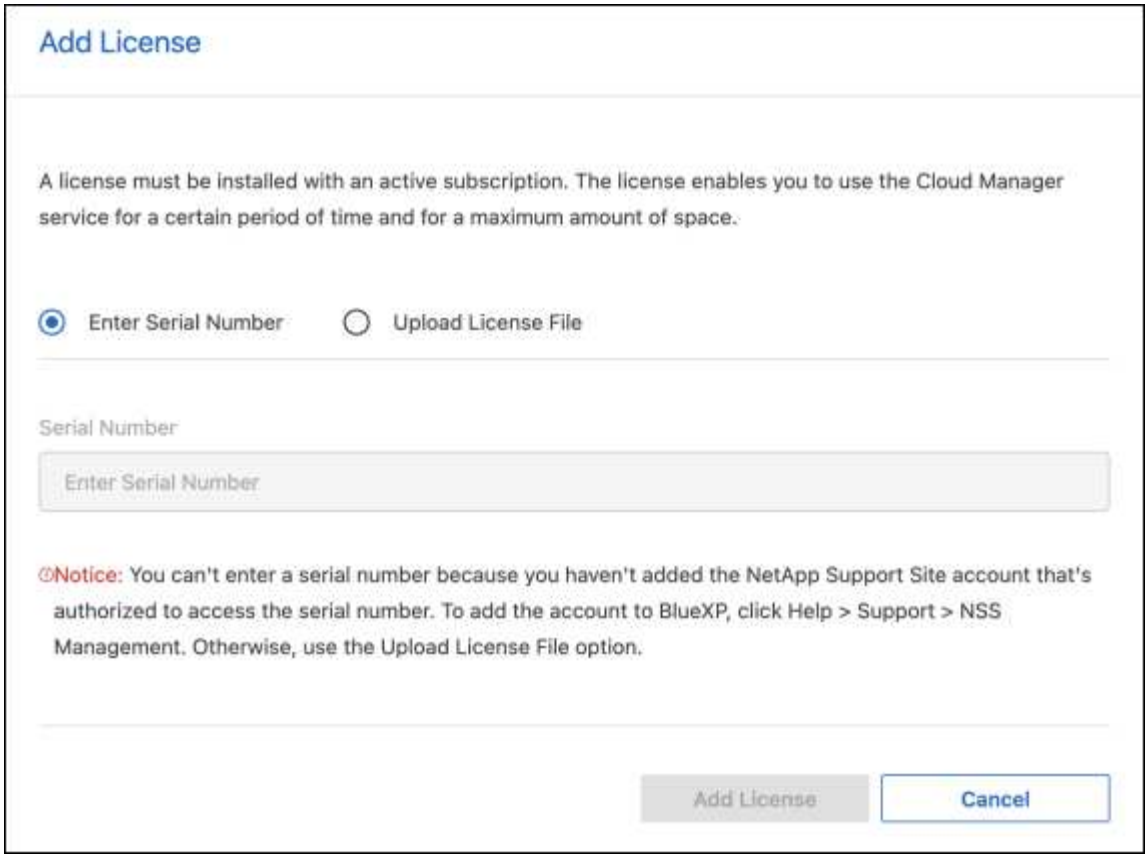
1. 在勒索软件恢复中，执行以下操作之一：
   - 如果您收到一条消息表明免费试用即将到期，请选择*查看付款方式*。
   - 如果您尚未开始试用，请选择右上角的*免费试用*通知，然后选择*查看付款方式*。



2. 在付款方式页面中，选择“订阅”Google Cloud Platform Marketplace*。
3. 在 Google Cloud Platform Marketplace 中，选择 订阅。
4. 使用 Google Cloud Platform Marketplace 订阅 * NetApp Intelligent Services* 和 * Ransomware Resilience *。
5. 当您返回 Ransomware Resilience 时，会出现一条消息表明您已订阅。

> 系统会向您发送一封电子邮件，其中包含 Ransomware Resilience 序列号，并表明您已在 Google Cloud Platform Marketplace 中订阅了 Ransomware Resilience。

6. 返回勒索软件恢复付款方式页面。
7. 要将许可证添加到控制台，请选择“添加许可证”。



8. 在添加许可证页面中，选择*输入序列号*。输入发送给您的电子邮件中的序列号。选择*添加许可证*。
9. 要查看许可证详细信息，请从控制台左侧导航中选择“治理”>“**Licenses and subscriptions**”。
   - 要查看订阅信息，请选择*订阅*。
   - 要查看 BYOL 许可证，请选择“数据服务许可证”。
10. 返回勒索软件恢复能力。从控制台左侧导航中，选择*保护*>*勒索软件恢复*。

    出现一条消息，表明已添加许可证。

自带许可证 (BYOL)

如果您想自带许可证 (BYOL)，则需要购买许可证，获取NetApp许可证文件 (NLF)，然后将许可证添加到控制台。

将您的许可证文件添加到控制台

从NetApp销售代表处购买勒索软件恢复许可证后，您可以通过输入勒索软件恢复序列号和NetApp支持站点 (NSS) 帐户信息来激活许可证。

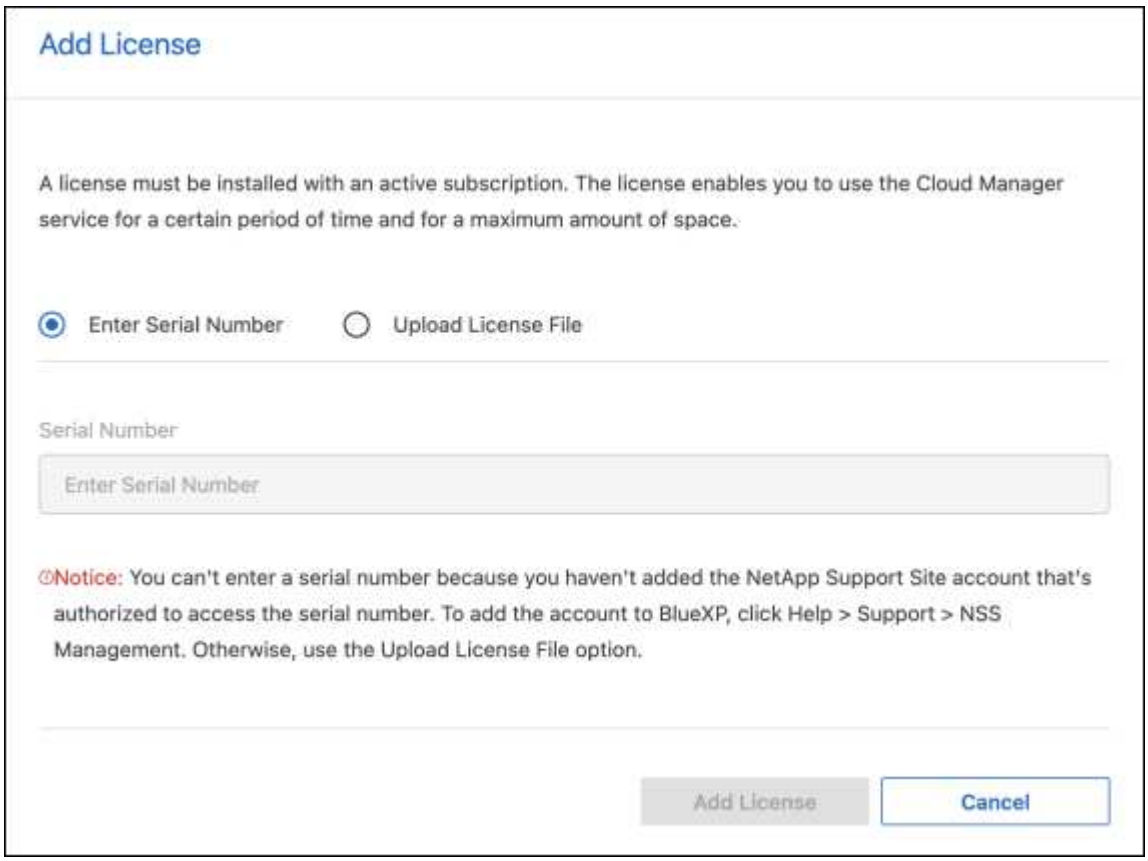
开始之前

您需要 Ransomware Resilience 序列号。从您的销售订单中找到此号码，或联系客户团队获取此信息。

步骤

1. 获得许可证后，返回 Ransomware Resilience。选择右上角的*查看付款方式*选项。或者，在免费试用即将到期的消息中，选择*订阅或购买许可证*。

2. 选择“添加许可证”转到控制台许可证和订阅页面。
3. 从“数据服务许可证”选项卡中，选择“添加许可证”。



4. 在“添加许可证”页面中，输入序列号和NetApp支持站点帐户信息。
   - 如果您有控制台许可证序列号并知道您的 NSS 帐户，请选择 输入序列号 选项并输入该信息。

     如果您的NetApp支持站点帐户未从下拉列表中找到， "将 NSS 帐户添加到控制台" 。
   - 如果您有 zvondolr 许可证文件（在暗站安装时需要），请选择 上传许可证文件 选项并按照提示附加文件。
5. 选择*添加许可证*。

结果

Licenses and subscriptions页面显示 Ransomware Resilience 已获得许可证。

控制台许可证到期后请更新

如果您的许可期限即将到期，或者您的许可容量已达到限制，您将在勒索软件恢复 UI 中收到通知。您可以在勒索软件恢复许可证到期之前进行更新，这样您访问扫描数据的能力就不会受到干扰。

此消息也出现在Licenses and subscriptions以及 "通知设置"。

步骤

1. 您可以发送电子邮件给支持人员以请求更新您的许可证。

在您支付许可证费用并在NetApp支持站点注册后，控制台会自动更新许可证。数据服务许可证页面将在 5 到 10 分钟内反映更改。

2. 如果控制台无法自动更新许可证，则需要手动上传许可证文件。
   a. 您可以从NetApp支持站点获取许可证文件。
   b. 在控制台中，选择管理 > **Licenses and subscriptions**。
   c. 选择“数据服务许可证”选项卡，选择要更新的序列号的“操作...”图标，然后选择“更新许可证”。

结束 **PAYGO** 订阅

如果您想终止 PAYGO 订阅，您可以随时终止。

步骤

1. 在 Ransomware Resilience 中，在右上角选择许可证选项。
2. 选择*查看付款方式*。
3. 在下拉详细信息中，取消选中“当前付款方式过期后使用”框。
4. 选择*保存*。

发现NetApp Ransomware Resilience中的工作负载

在使用NetApp Ransomware Resilience之前，它需要先发现数据。在发现过程中，勒索软件恢复力会分析组织内所有控制台代理和项目系统中的所有卷和文件。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

*勒索软件恢复能力发现了什么？*勒索软件恢复能力评估 MySQL 应用程序、Oracle 应用程序、VMware 数据存储区、文件共享和块存储。

勒索软件恢复能力无法发现使用FlexGroup卷的工作负载。

勒索软件恢复能力在仪表板中发现并显示受支持和不受支持的系统配置。

勒索软件恢复能力会检查您当前的备份保护、快照副本和NetApp自主勒索软件保护选项。然后它会推荐一些改善勒索软件防护的方法。

*如何发现工作负载？*您可以执行以下操作：

- 在每个控制台代理中，选择您想要发现工作负载的系统。如果您想保护环境中的特定工作负载而不是其他工作负载，您可能会受益于此功能。
- 发现先前选择的系统新创建的工作负载。
- 发现新系统。

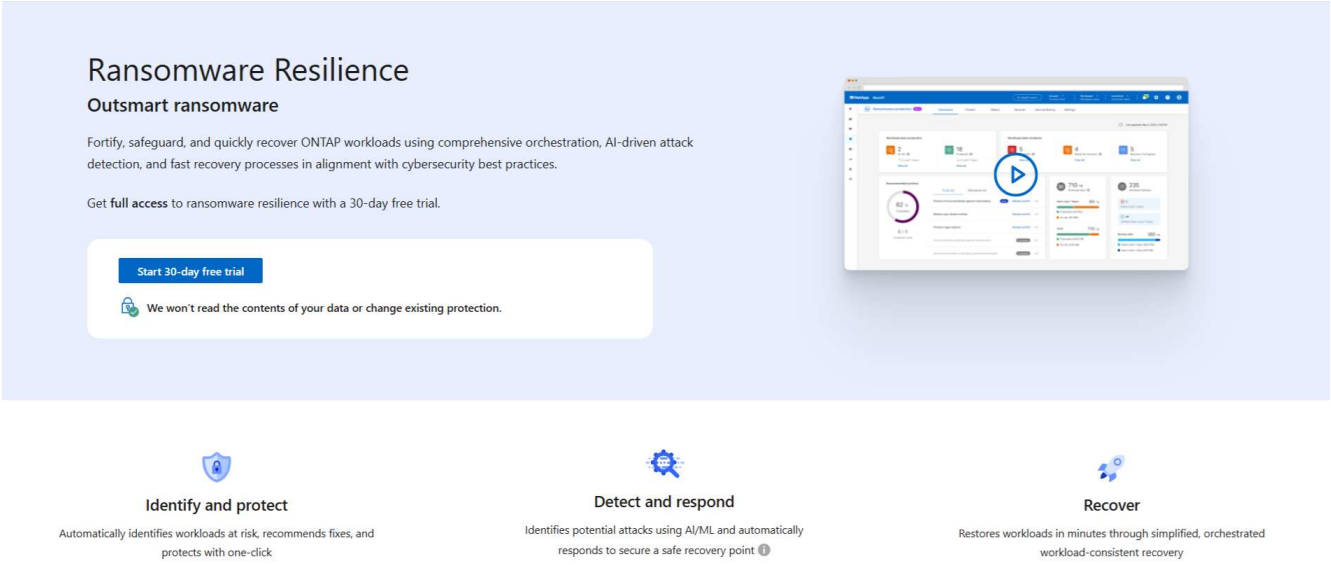
选择要发现和保护的工作负载

在每个控制台代理中，选择您想要发现工作负载的系统。

步骤

1. 从NetApp Console中，选择 保护 > 勒索软件保护。

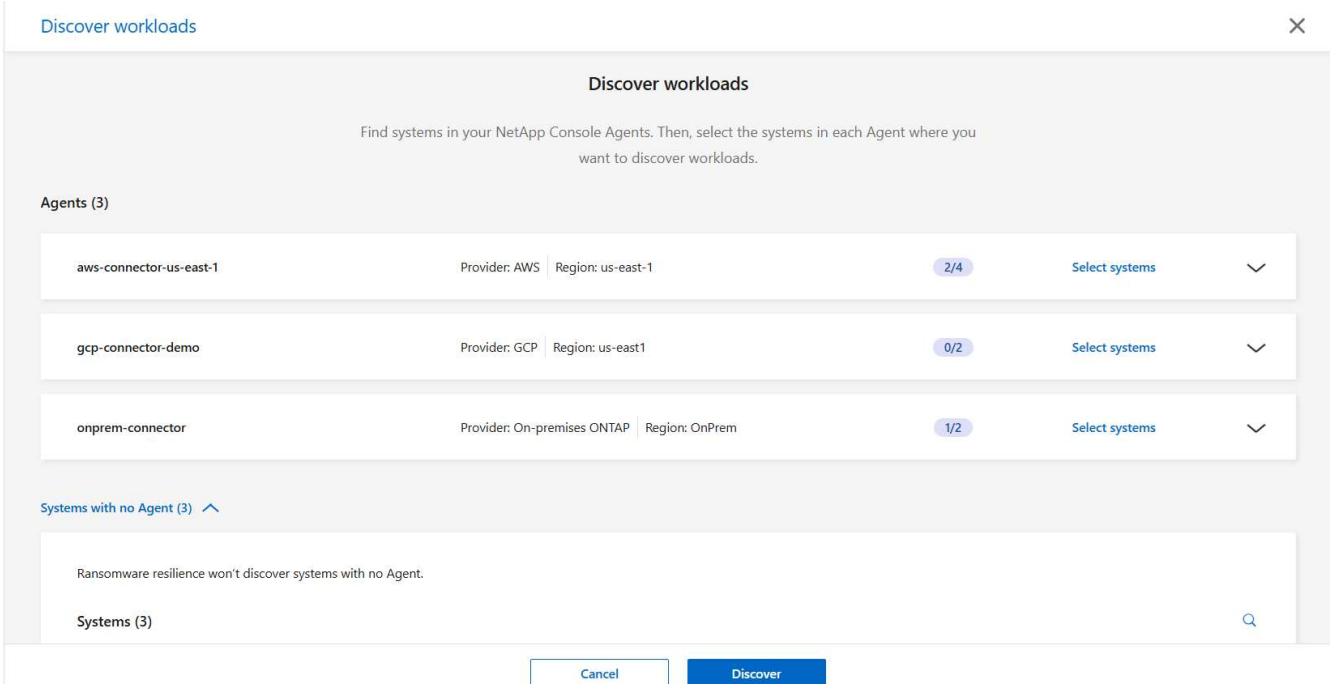
   如果这是您的第一次登录，则会出现登录页面。



   如果您开始免费试用，开始 **30** 天免费试用*按钮标签将更改为*通过发现工作负载开始。

2. 从初始登录页面，选择*从发现工作负载开始*。

   勒索软件恢复力可发现受支持和不受支持的系统。此过程可能需要几分钟。

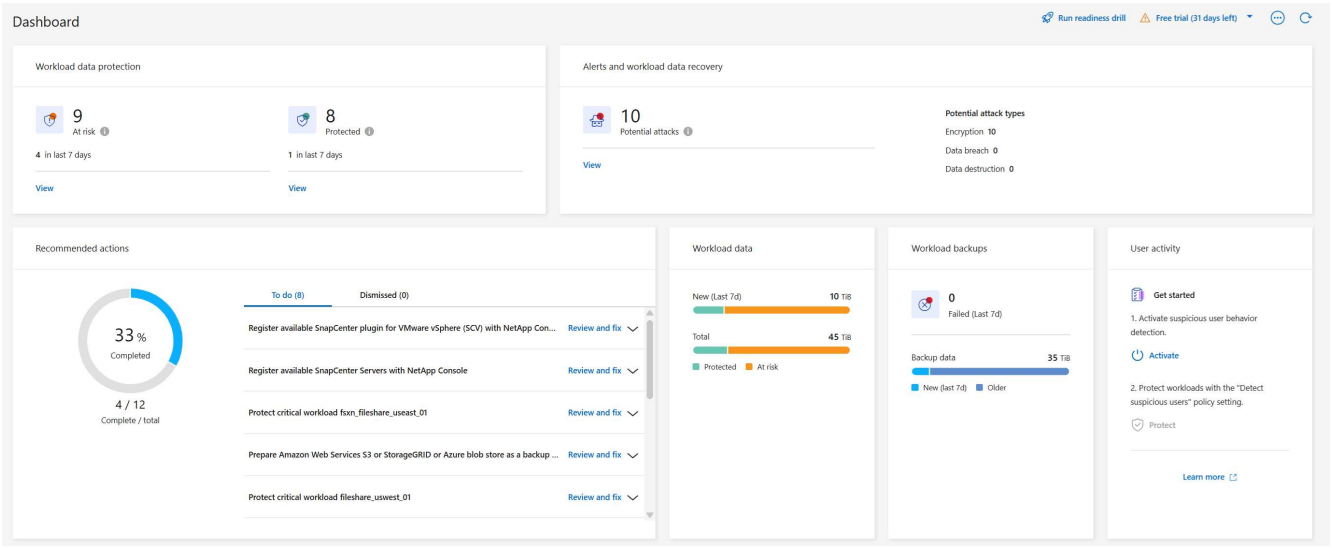


3. 要发现特定控制台代理的工作负载，请选择要发现工作负载的控制台代理旁边的“选择系统”。
4. 选择您想要发现工作负载的系统。
5. 选择*发现*。

   勒索软件恢复力仅发现具有选定系统的控制台代理的工作负载数据。此过程可能需要几分钟。

6. 要下载已发现的工作负载列表，请选择*下载结果*。
7. 要显示勒索软件恢复仪表板，请选择“转到仪表板”。

   仪表板显示数据保护健康状况。随着新工作负载的发现，处于危险中或受保护的工作负载的数量会更新。



"了解仪表板向您显示的内容。"

发现先前选定的系统新创建的工作负载

如果您已经选择了要发现的系统，则可以从仪表板中发现这些环境的新创建的工作负载。

步骤

1. 要确定最后发现的日期，请查看勒索软件恢复力仪表板右上角*刷新*图标旁边的日期和时间戳。
2. 从仪表板中，选择“刷新图标”以查找新的工作负载。

发现新系统

如果您已经发现了系统，您可以找到新的或以前未选择的系统。

步骤

1. 从勒索软件恢复菜单中，选择垂直 …右上角的选项。从下拉菜单中选择*设置*。
2. 在工作负载发现卡中，选择*发现工作负载*。

   此过程可能需要几分钟，加载图标显示进度。

3. 勒索软件恢复力可以发现受支持和不受支持的系统。如果系统的ONTAP版本低于所需版本，则勒索软件恢复能力不支持该系统。当您将鼠标悬停在某个不受支持的系统上时，工具提示会显示原因。选择您想要发现工作负载的系统。
4. 选择*发现*。

在NetApp Ransomware Resilience中进行勒索软件攻击准备演练

通过模拟对新样本工作负载的攻击来运行勒索软件攻击准备演习。调查模拟攻击并恢复工作负载。使用此功能来测试警报通知、响应和恢复。根据需要经常进行演练。

您的实际工作量数据不会受到影响。

您可以对 NFS 和 CIFS (SMB) 工作负载进行准备情况演练。

配置勒索软件攻击准备演习

在运行模拟之前，请在“设置”页面上设置演练。从顶部菜单中的操作选项访问设置页面。

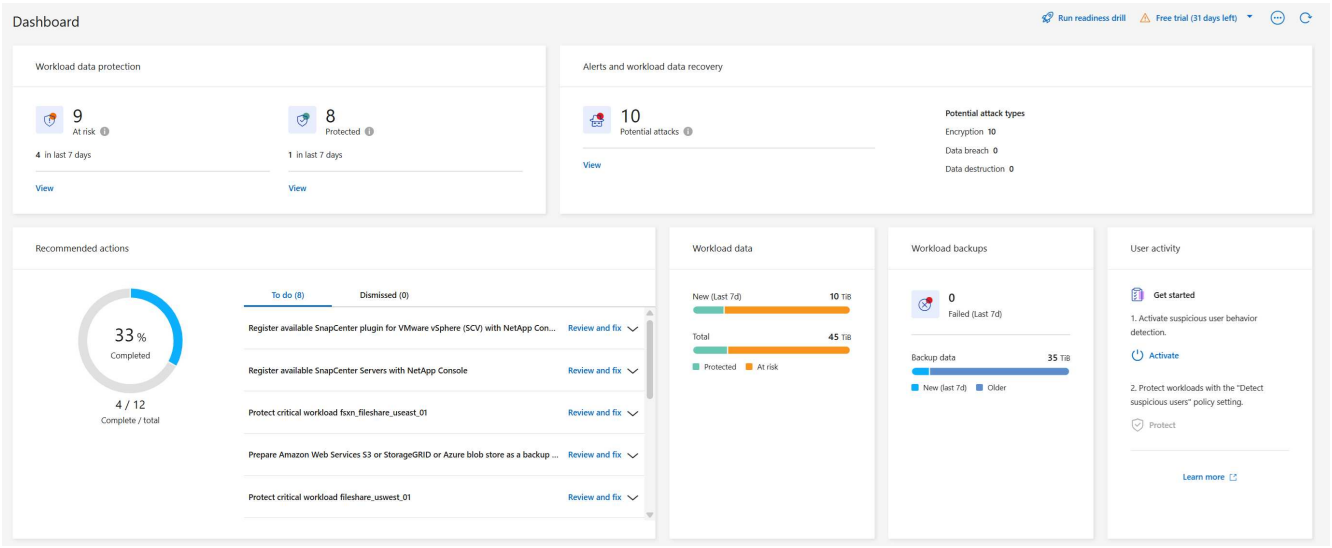
以下情况需要输入用户名和密码：

- 如果先前选择的存储虚拟机的用户名或密码发生更改
- 如果您选择不同的 CIFS (SMB) 存储 VM
- 如果您输入不同的测试工作负载名称

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

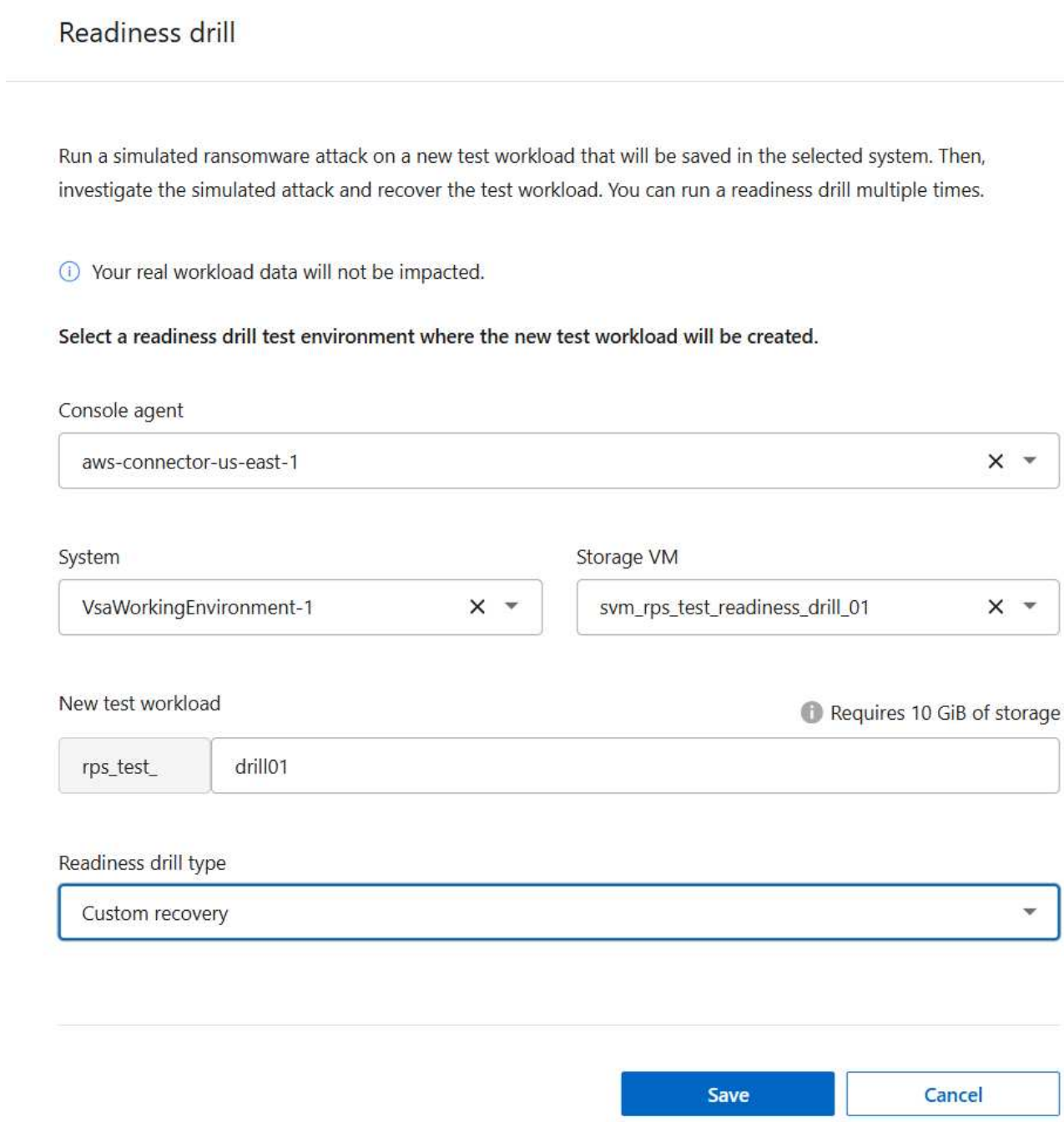
步骤

1. 从NetApp Ransomware Resilience菜单中，选择右上角的 运行准备演练 按钮。



2. 在设置页面的准备情况练习卡中，选择*配置*。

   控制台显示配置准备情况演练页面。



3. 执行以下操作：
   a. 选择您想要用于准备情况演练的控制台代理。
   b. 选择一个测试系统。
   c. 选择测试存储 SVM。
   d. 如果您选择了 CIFS (SMB) 存储虚拟机，则会出现用户名和密码字段。输入存储虚拟机的用户名和密码。
   e. 选择准备演习类型。要从加密数据泄露中手动恢复，请选择自定义恢复。要从可疑用户活动中恢复，请选择数据泄露。
   f. 输入要创建的新测试工作负载的名称。名称中不要包含破折号。

4. 选择*保存*。

您可以稍后使用“设置”页面编辑准备演练配置。

开始准备演习

配置准备情况演练后，即可开始演练。

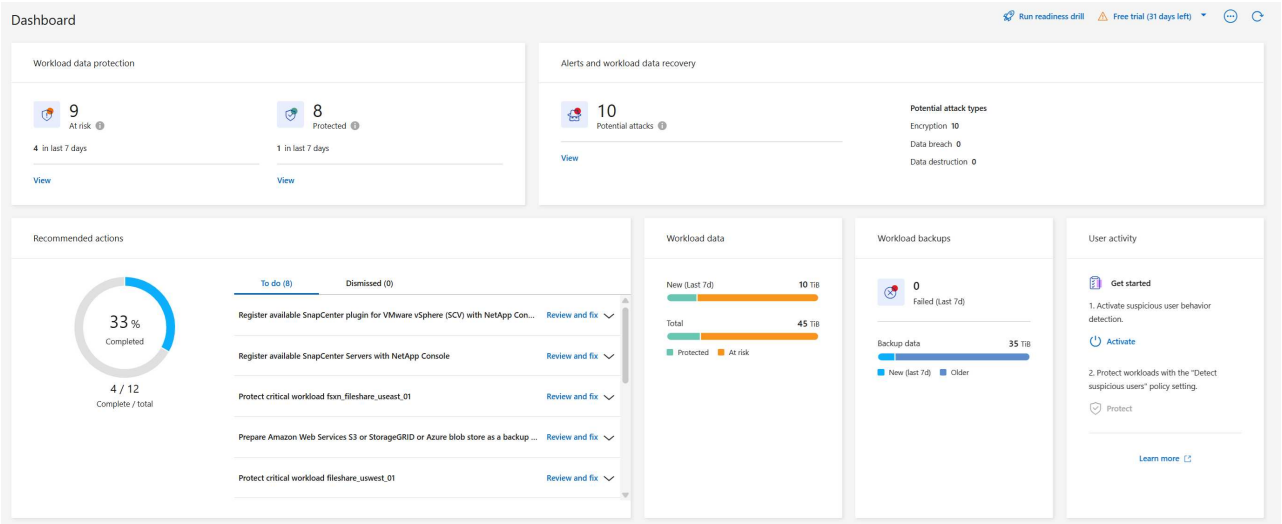
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

当您开始准备演习时，勒索软件恢复力会跳过学习模式并以主动模式开始演习。工作负载的检测状态为“活动”。

当最近分配了检测策略并且勒索软件恢复扫描工作负载时，工作负载可以具有勒索软件检测*学习模式*状态。

步骤

1. 执行以下操作之一：
   - 从勒索软件恢复菜单中，选择右上角的“运行准备演练”按钮。



   - 或者，从“设置”页面的“准备情况练习卡”中选择“开始”。

演练运行时，您无法编辑准备演练配置。您可以重置钻机以停止它并修改配置。

响应战备演习警报

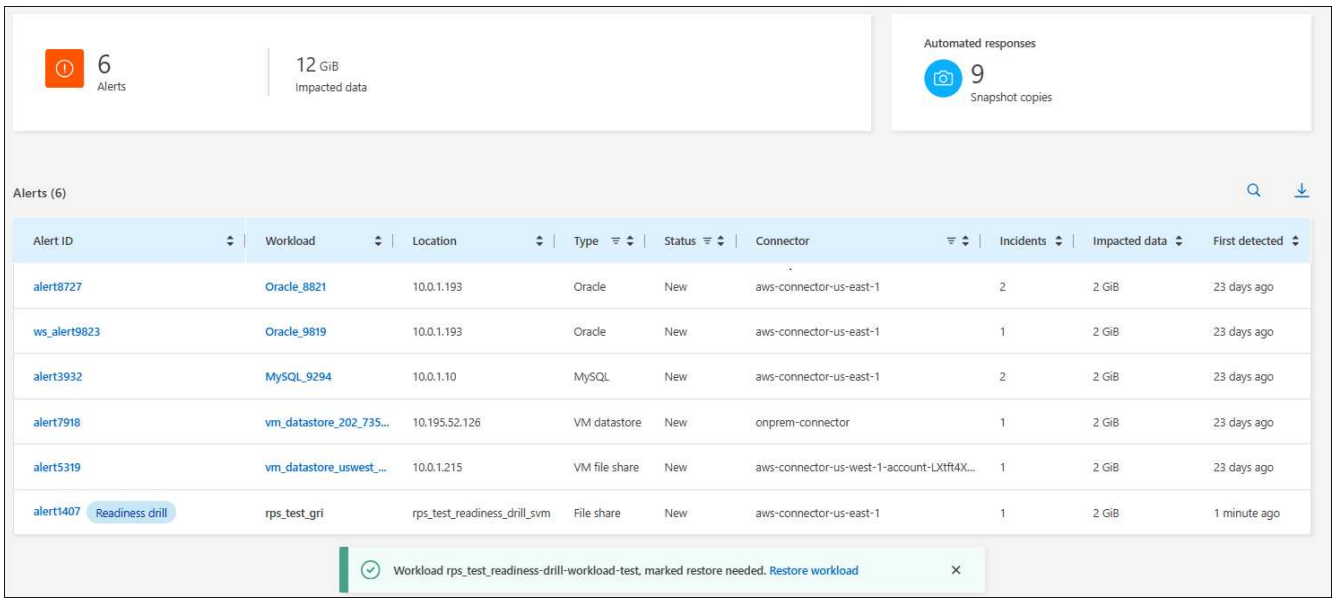
通过响应准备演习警报来测试您的准备情况。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

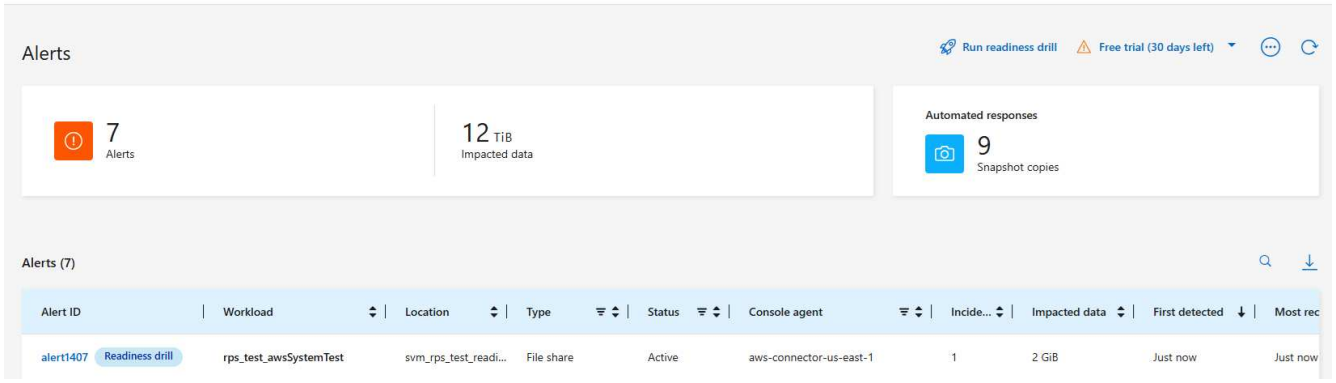
步骤

1. 从勒索软件恢复菜单中，选择*警报*。

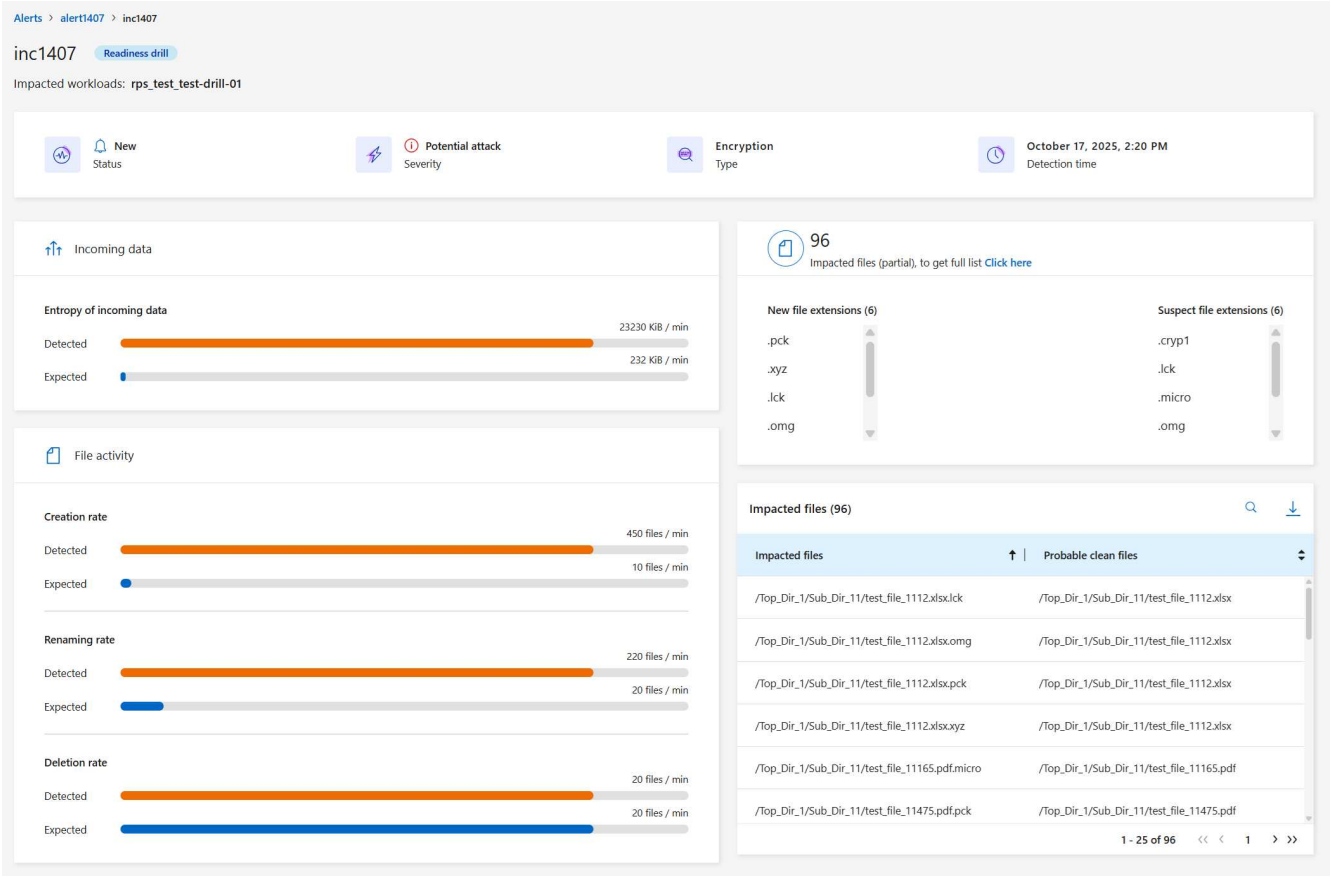
控制台显示警报页面。在警报 ID 列中，您会在 ID 旁边看到“准备情况演练”。



2. 选择带有“准备演习”指示的警报。事件警报列表出现在警报详细信息页面上。



3. 查看警报事件。
4. 选择一个警报事件。



以下是需要注意的一些事项：

- 查看潜在攻击的严重性。

  如果严重性表明用户涉嫌恶意活动，请检查用户名。您还可以"阻止该用户。"

- 查看文件活动和可疑进程：
  - 查看传入的检测数据与预期数据的比较。
  - 查看检测到的文件的创建率与预期率的比较。
  - 查看检测到的文件重命名率与预期率的比较。
  - 查看删除率与预期删除率的对比。
- 查看受影响文件的列表。查看可能导致攻击的扩展。
- 通过查看受影响的文件和目录的数量来确定攻击的影响和广度。

恢复测试工作负载

审查准备情况演习警报后，如有必要，恢复测试工作量。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

1. 返回警报详细信息页面。

2. 如果需要恢复测试工作负载，请执行以下操作：
   - 选择*标记需要恢复*。
   - 查看确认信息，然后在确认框中选择*标记需要恢复*。
     - 从勒索软件恢复菜单中，选择*恢复*。
     - 选择要恢复的标有“准备演练”的测试工作负载。
     - 选择*恢复*。
     - 在“还原”页面中，提供还原的信息：
   - 选择源快照副本。
   - 选择目标卷。
3. 在恢复审核页面中，选择*恢复*。

   控制台在恢复页面上显示准备演练恢复的状态为“进行中”。

   恢复完成后，控制台将工作负载的状态更改为*已恢复*。

4. 查看恢复的工作负载。

有关恢复过程的详细信息，请参阅"从勒索软件攻击中恢复（事件被消除后）"。

准备演练后更改警报状态

审查准备情况演习警报并恢复工作量后，根据需要更改警报状态。

需要控制台角色 组织管理员、文件夹或项目管理员或勒索软件恢复管理员。 "了解所有服务的控制台访问角色"。

步骤

1. 返回警报详细信息页面。
2. 再次选择警报。
3. 通过选择*编辑状态*来指示状态，并将状态更改为以下之一：
   - 已解除：如果您怀疑该活动不是勒索软件攻击，请将状态更改为已解除。

     解除攻击后，您将无法将其改回。如果您解除工作负载，则为应对潜在勒索软件攻击而自动获取的所有快照副本都将被永久删除。如果您解除警报，则准备演习即视为完成。

   - 已解决：事件已得到缓解。

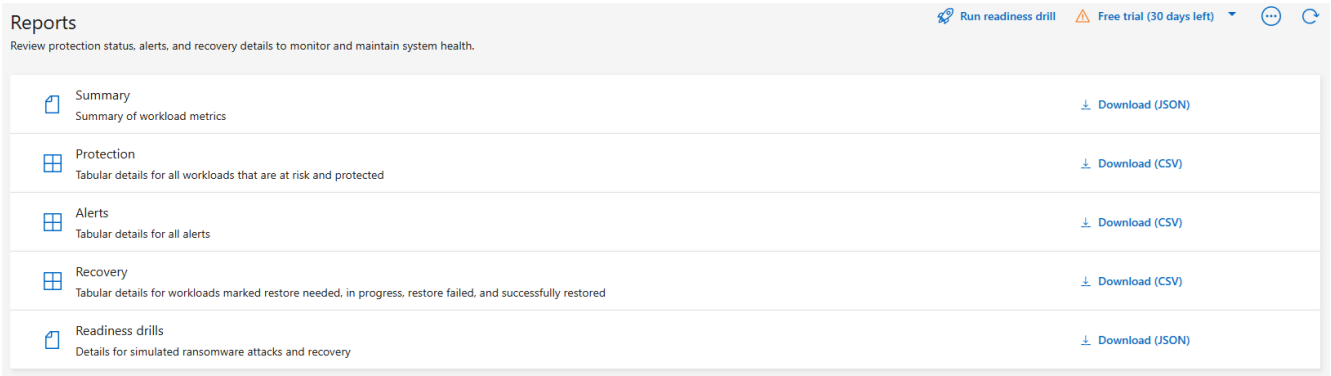
审查准备演习报告

准备演习完成后，您可能需要查看并保存演习报告。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员、勒索软件恢复管理员或勒索软件恢复查看器角色。"了解NetApp Console的勒索软件恢复角色"。

步骤

1. 从勒索软件恢复菜单中，选择*报告*。



2. 选择*准备演习*和*下载*以下载准备演习报告。

在NetApp Ransomware Resilience中配置保护设置

您可以通过访问*设置*选项来配置备份目标、将数据发送到外部安全和事件管理 (SIEM) 系统、进行攻击准备演习、配置工作负载发现或配置可疑用户活动检测。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

*您可以在“设置”页面做什么？*在“设置”页面中，您可以执行以下操作：

- 通过进行准备演习来模拟勒索软件攻击，并对模拟勒索软件警报做出响应。有关详细信息，请参阅"进行勒索软件攻击准备演习" 。
- 配置工作负载发现。
- 配置可疑用户活动报告。
- 添加备份目的地。
- 连接您的安全和事件管理系统 (SIEM) 以进行威胁分析和检测。启用威胁检测会自动将数据发送到您的 SIEM 进行威胁分析。

直接访问设置页面

您可以从顶部菜单附近的“操作”选项轻松访问“设置”页面。

1. 从勒索软件恢复能力中，选择垂直 …右上角的选项。
2. 从下拉菜单中选择*设置*。

模拟勒索软件攻击

通过模拟对新创建的示例工作负载的勒索软件攻击来进行勒索软件准备演习。然后，调查模拟攻击并恢复样本工作负载。此功能可帮助您通过测试警报通知、响应和恢复过程来了解在发生实际勒索软件攻击时您是否已做好准备。您可以多次运行勒索软件准备演习。

有关详细信息，请参阅"进行勒索软件攻击准备演习"。

配置工作负载发现

您可以配置工作负载发现来自动发现环境中的新工作负载。

1. 在“设置”页面中，找到“工作负载发现”图块。
2. 在“工作负载发现”图块中，选择“发现工作负载*”。

   此页面显示之前未选择的系统的控制台代理、新可用的控制台代理和新可用的系统。此页面不显示之前选择的系统。

3. 选择您想要发现工作负载的控制台代理。
4. 查看系统列表。
5. 选中您想要发现工作负载的系统，或选择表格顶部的框以发现所有已发现工作负载环境中的工作负载。
6. 根据需要对其他系统执行此操作。
7. 选择“发现”以使勒索软件恢复功能自动发现所选控制台代理中的新工作负载。

可疑的用户活动

在用户活动卡中，您可以创建和管理检测可疑用户活动所需的用户活动代理。

有关更多信息，请参阅"可疑的用户活动" 。

添加备份目标

勒索软件恢复能力可以识别尚未有任何备份的工作负载以及尚未分配任何备份目标的工作负载。

为了保护这些工作负载，您应该添加备份目标。您可以选择以下备份目标之一：

- NetAppStorageGRID
- 亚马逊网络服务（AWS）
- Google Cloud Platform
- Microsoft Azure

Amazon FSx for NetApp ONTAP中的工作负载没有可用的备份目标。使用 FSx for ONTAP备份服务执行备份操作。

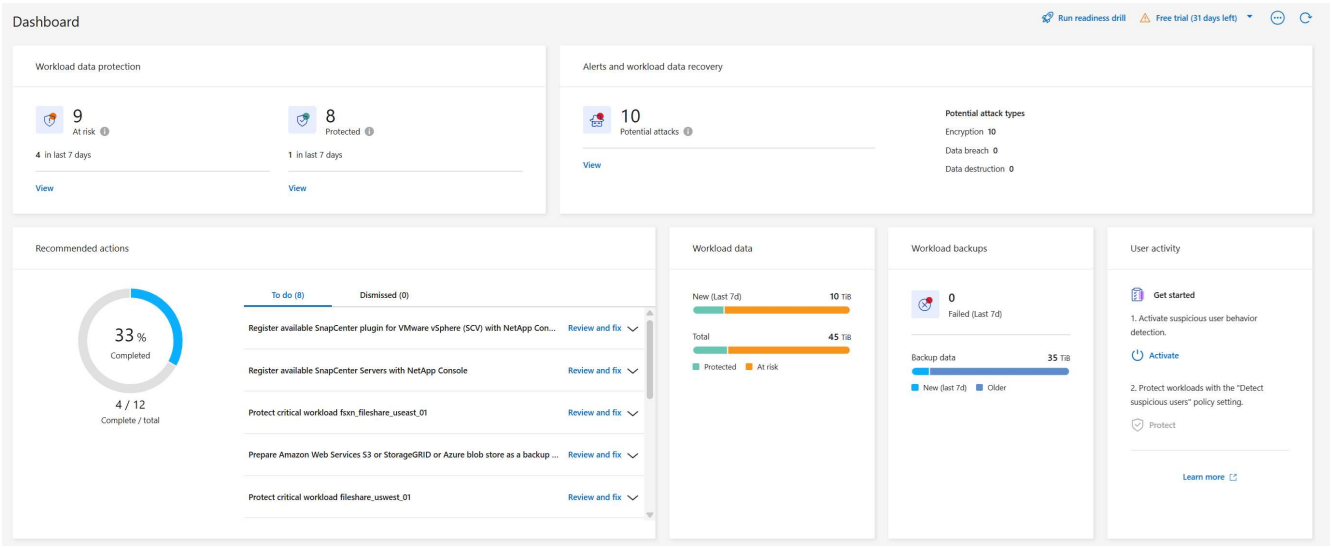
您可以根据仪表板中的推荐操作或访问菜单上的“设置”选项来添加备份目标。

从仪表板的推荐操作访问备份目标选项

仪表板提供了许多建议。一个建议可能是配置备份目标。

步骤

1. 在勒索软件恢复仪表板中，查看“推荐的操作”窗格。



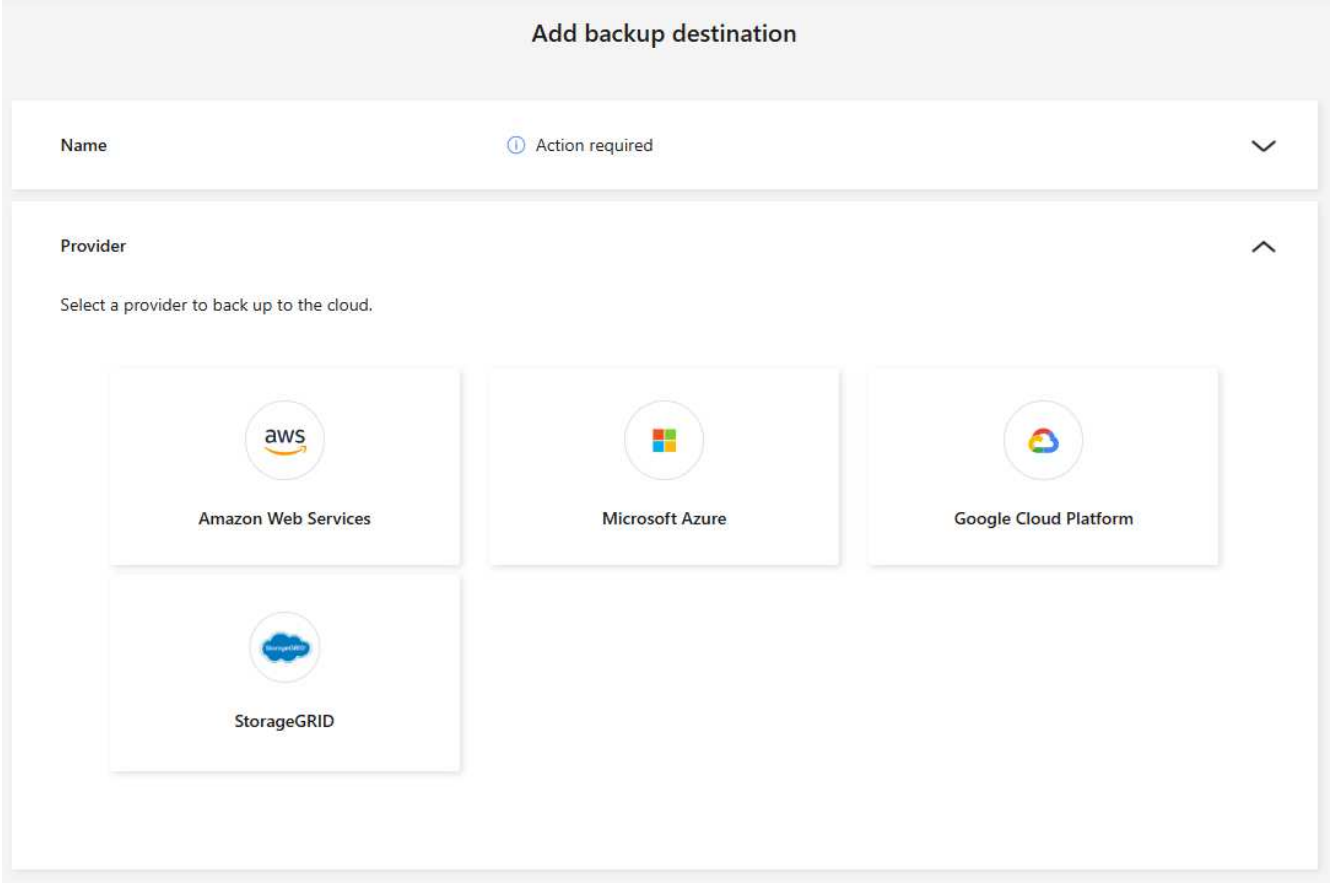
2. 从仪表板中，选择“准备<备份提供商>作为备份目标”的建议的*审查和修复*。
3. 根据备份提供商的指示继续操作。

添加**StorageGRID**作为备份目标

要将NetApp StorageGRID设置为备份目标，请输入以下信息。

步骤

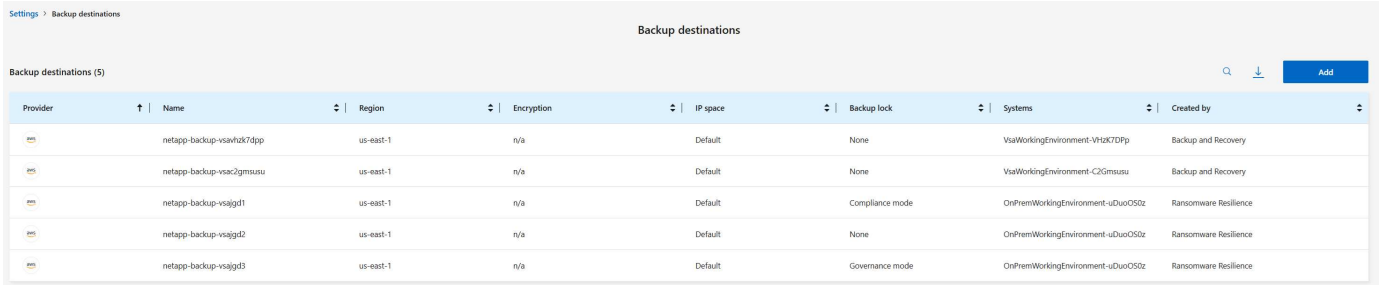
1. 在*设置 > 备份目标*页面中，选择*添加*。
2. 输入备份目标的名称。



3. 选择* StorageGRID*。
4. 选择每个设置旁边的向下箭头并输入或选择值：
   - 提供商设置：
     - 创建一个新的存储桶或自带存储桶来存储备份。
     - StorageGRID网关节点完全限定域名、端口、 StorageGRID访问密钥和密钥凭证。
   - 网络：选择 IP 空间。
     - IP 空间是您要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
5. 选择“添加”。

结果

新的备份目标将添加到备份目标列表中。



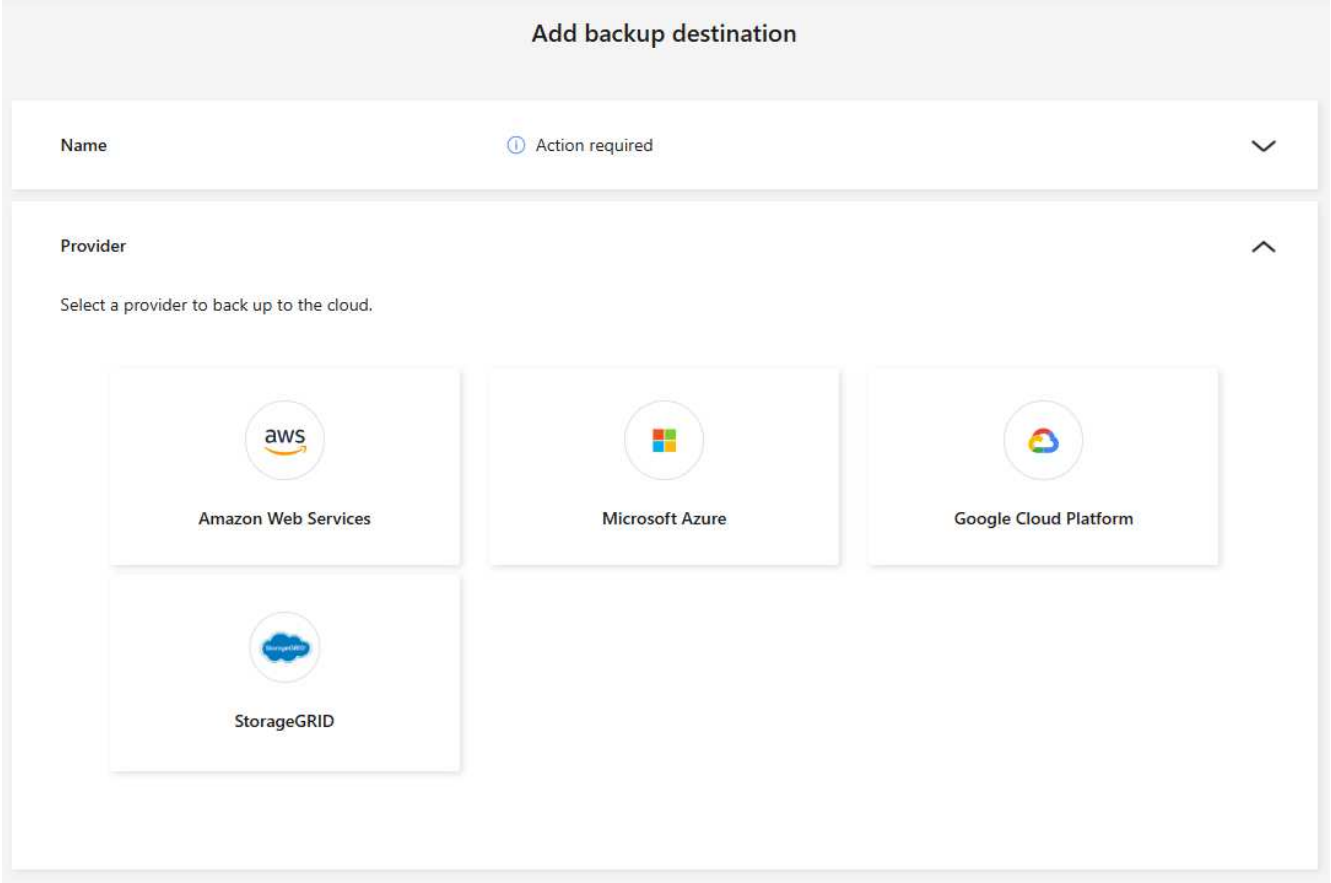
添加 **Amazon Web Services** 作为备份目标

要将 AWS 设置为备份目标，请输入以下信息。

有关在控制台中管理 AWS 存储的详细信息，请参阅 "管理您的 Amazon S3 存储桶"。

步骤

1. 在*设置 > 备份目标*页面中，选择*添加*。
2. 输入备份目标的名称。



3. 选择*Amazon Web Services*。
4. 选择每个设置旁边的向下箭头并输入或选择值：
   - 提供商设置：
     - 创建一个新的存储桶，如果控制台中已经存在存储桶，则选择一个现有存储桶，或者使用您自己的存储桶来存储备份。
     - AWS 账户、区域、AWS 凭证的访问密钥和密钥

       "如果您想要自带存储桶，请参阅添加 S3 存储桶" 。
   - 加密：如果您正在创建新的 S3 存储桶，请输入提供商提供给您的加密密钥信息。如果您选择现有存储桶，则加密信息已经可用。

     默认情况下，存储桶中的数据使用 AWS 管理的密钥加密。您可以继续使用 AWS 管理的密钥，也可以使用您自己的密钥管理数据的加密。

- 网络：选择 IP 空间以及是否使用私有端点。
  - IP 空间是您要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
  - 或者，选择是否使用您之前配置的 AWS 私有终端节点 (PrivateLink)。

    如果您想使用 AWS PrivateLink，请参阅 "适用于 Amazon S3 的 AWS PrivateLink"。
- 备份锁：选择是否希望勒索软件恢复功能保护备份不被修改或删除。此选项使用NetApp DataLock 技术。每个备份将在保留期内锁定，或至少 30 天，再加上最多 14 天的缓冲期。

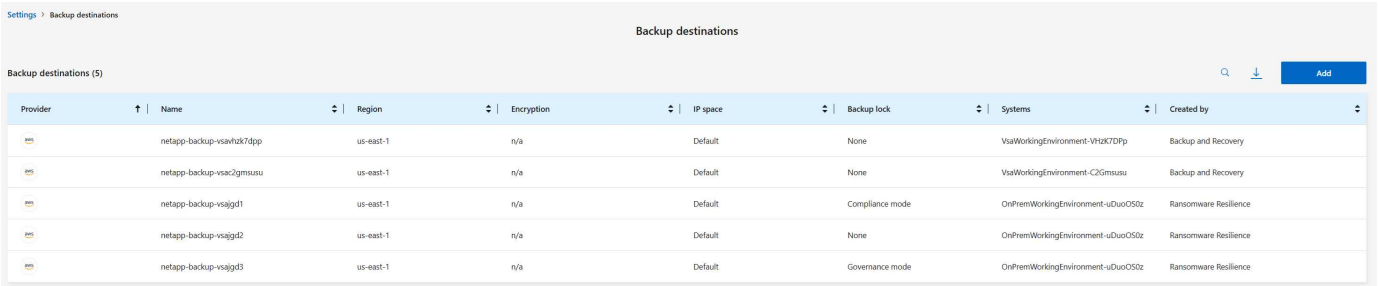
  如果您现在配置备份锁定设置，则在配置备份目标后您将无法更改该设置。

  - 治理模式：特定用户（具有 s3:BypassGovernanceRetention 权限）可以在保留期内覆盖或删除受保护的文件。
  - 合规模式：用户在保留期内无法覆盖或删除受保护的备份文件。

5. 选择“添加”。

结果

新的备份目标将添加到备份目标列表中。



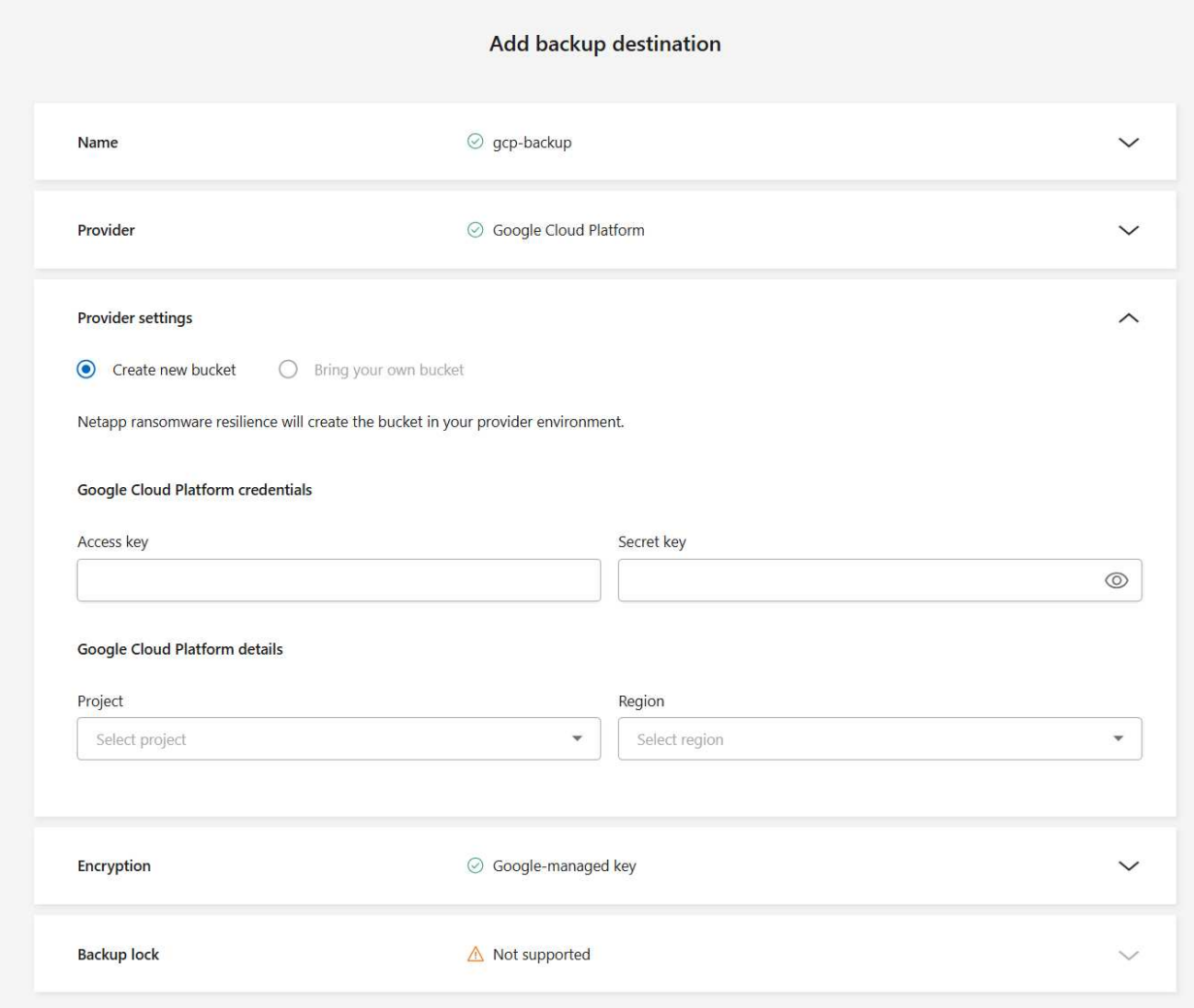
添加 **Google Cloud Platform** 作为备份目标

要将 Google Cloud Platform (GCP) 设置为备份目标，请输入以下信息。

有关在控制台中管理 GCP 存储的详细信息，请参阅 "Google Cloud 中的控制台代理安装选项"。

步骤

1. 在*设置 > 备份目标*页面中，选择*添加*。
2. 输入备份目标的名称。
3. 选择*Google Cloud Platform*。
4. 选择每个设置旁边的向下箭头并输入或选择值：
   - 提供商设置：
     - 创建一个新的存储桶。输入访问密钥和密钥。
     - 输入或选择您的 Google Cloud Platform 项目和区域。



- 加密：如果您正在创建新的存储桶，请输入提供商提供给您的加密密钥信息。如果您选择现有存储桶，则加密信息已经可用。

  默认情况下，存储桶中的数据使用 Google 管理的密钥加密。您可以继续使用 Google 管理的密钥。

- 网络：选择 IP 空间以及是否使用私有端点。
  - IP 空间是您要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
  - 或者，选择是否使用您之前配置的 GCP 专用端点 (PrivateLink)。

5. 选择“添加”。

结果

新的备份目标将添加到备份目标列表中。

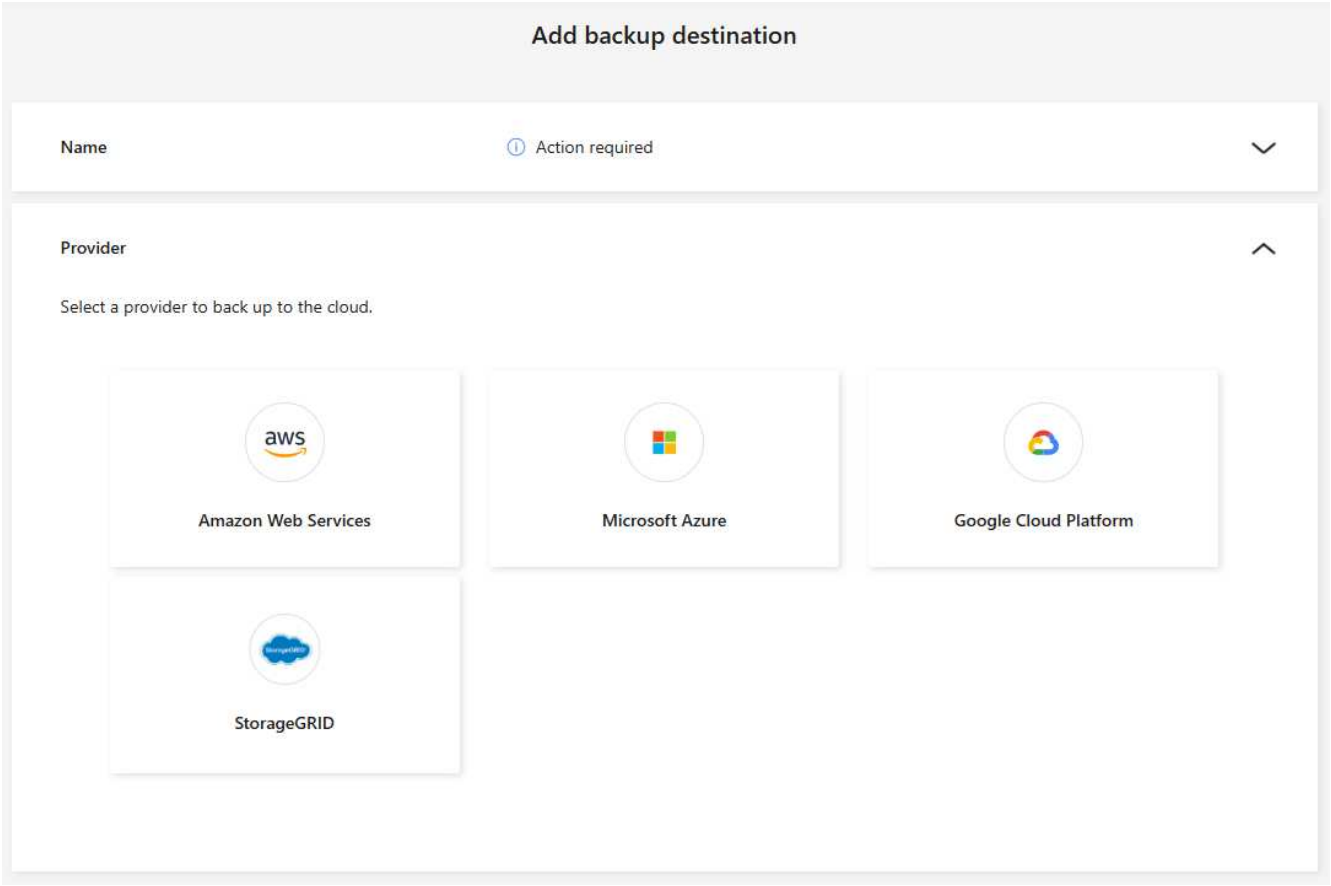
添加 **Microsoft Azure** 作为备份目标

要将 Azure 设置为备份目标，请输入以下信息。

有关在控制台中管理 Azure 凭据和市场订阅的详细信息，请参阅 "管理 Azure 凭据和市场订阅"。

步骤

1. 在*设置 > 备份目标*页面中，选择*添加*。
2. 输入备份目标的名称。



3. 选择“**Azure**”。
4. 选择每个设置旁边的向下箭头并输入或选择值：
   - 提供商设置：
     - 创建一个新的存储帐户，如果控制台中已经存在，则选择一个现有的存储帐户，或者使用您自己的存储帐户来存储备份。
     - Azure 凭据的 Azure 订阅、区域和资源组

       "如果您想自带存储帐户，请参阅添加 Azure Blob 存储帐户" 。
   - 加密：如果您正在创建新的存储帐户，请输入提供商提供给您的加密密钥信息。如果您选择现有帐户，则加密信息已经可用。

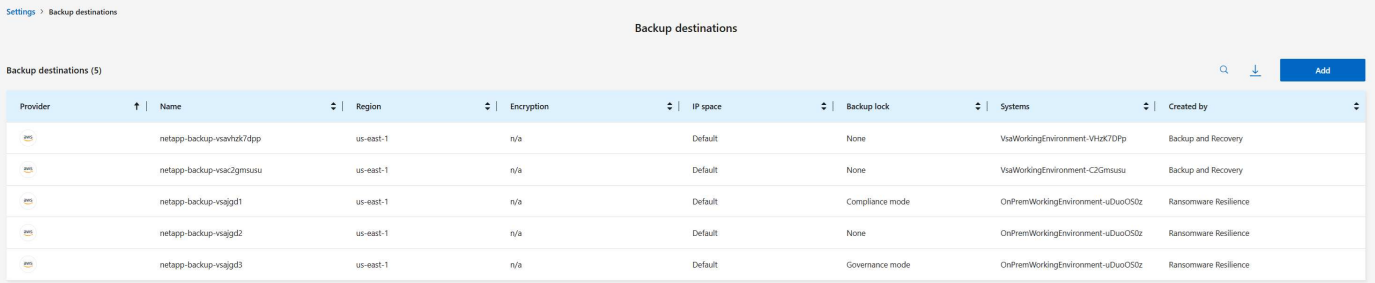
     默认情况下，帐户中的数据使用 Microsoft 管理的密钥加密。您可以继续使用 Microsoft 管理的密钥，也可以使用您自己的密钥管理数据的加密。
   - 网络：选择 IP 空间以及是否使用私有端点。
     - IP 空间是您要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
     - 或者，选择是否使用之前配置的 Azure 专用终结点。

       如果您想使用 Azure PrivateLink，请参阅 "Azure PrivateLink"。

5. 选择“添加”。

结果

新的备份目标将添加到备份目标列表中。



连接到安全和事件管理系统 (SIEM) 进行威胁分析和检测

您可以自动将数据发送到您的安全和事件管理系统 (SIEM) 进行威胁分析和检测。您可以选择 AWS Security Hub、Microsoft Sentinel 或 Splunk Cloud 作为您的 SIEM。

在 Ransomware Resilience 中启用 SIEM 之前，您需要配置您的 SIEM 系统。

关于发送到 **SIEM** 的事件数据

Ransomware Resilience 可以将以下事件数据发送到您的 SIEM 系统：

- 语境：
  - **os**：这是一个具有ONTAP值的常量。
  - **os_version**：系统上运行的ONTAP版本。
  - **connector_id**：管理系统的控制台代理的 ID。
  - **cluster_id**： ONTAP为系统报告的集群 ID。
  - **svm_name**：发现警报的 SVM 的名称。
  - **volume_name**：发现警报的卷的名称。
  - **volume_id**： ONTAP为系统报告的卷的 ID。
- 事件：
  - **incident_id**：勒索软件恢复力针对勒索软件恢复力中受到攻击的卷生成的事件 ID。
  - **alert_id**：勒索软件恢复能力为工作负载生成的 ID。
  - 严重性：以下警报级别之一：“严重”、“高”、“中”、“低”。
  - 描述：有关检测到的警报的详细信息，例如“在工作负载 arp_learning_mode_test_2630 上检测到潜在的勒索软件攻击”

配置 **AWS Security Hub** 进行威胁检测

在 Ransomware Resilience 中启用 AWS Security Hub 之前，您需要在 AWS Security Hub 中执行以下高级步骤：

- 在 AWS Security Hub 中设置权限。

- 在 AWS Security Hub 中设置身份验证访问密钥和密钥。（此处未提供这些步骤。）

在 **AWS Security Hub** 中设置权限的步骤

1. 转到 **AWS IAM** 控制台。
2. 选择*政策*。
3. 使用以下 JSON 格式的代码创建策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

配置 **Microsoft Sentinel** 进行威胁检测

在 Ransomware Resilience 中启用 Microsoft Sentinel 之前，您需要在 Microsoft Sentinel 中执行以下高级步骤：

- 先决条件
  - 启用 Microsoft Sentinel。
  - 在 Microsoft Sentinel 中创建自定义角色。
- 登记
  - 注册 Ransomware Resilience 以接收来自 Microsoft Sentinel 的事件。
  - 为注册创建一个秘密。
- 权限：为应用程序分配权限。
- 身份验证：输入应用程序的身份验证凭据。

启用 **Microsoft Sentinel** 的步骤

1. 转到 Microsoft Sentinel。
2. 创建*Log Analytics 工作区*。

3. 启用 Microsoft Sentinel 以使用您刚刚创建的 Log Analytics 工作区。

在 **Microsoft Sentinel** 中创建自定义角色的步骤

1. 转到 Microsoft Sentinel。
2. 选择*订阅* > 访问控制 **(IAM)**。
3. 输入自定义角色名称。使用名称 **Ransomware Resilience Sentinel Configurator**。
4. 复制以下 JSON 并将其粘贴到 **JSON** 选项卡中。

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes":["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. 检查并保存您的设置。

注册勒索软件恢复能力以接收来自 **Microsoft Sentinel** 的事件的步骤

1. 转到 Microsoft Sentinel。
2. 选择 **Entra ID** > 应用程序 > 应用程序注册。
3. 对于应用程序的*显示名称*，输入“**Ransomware Resilience**”。
4. 在 支持的帐户类型 字段中，选择 仅限此组织目录中的帐户。
5. 选择将推送事件的*默认索引*。
6. 选择*审核*。
7. 选择*注册*来保存您的设置。

   注册后，Microsoft Entra 管理中心将显示应用程序概述窗格。

创建注册密钥的步骤

1. 转到 Microsoft Sentinel。
2. 选择*证书和机密* > 客户端机密 > 新客户端机密。
3. 为您的应用程序机密添加描述。
4. 为秘密选择一个*到期日期*或指定自定义有效期。

   客户端密钥的有效期限制为两年（24 个月）或更短。 Microsoft 建议您设置小于 12 个月的到期值。

5. 选择“添加”来创建您的秘密。
6. 记录身份验证步骤中使用的秘密。离开此页面后，该秘密将不再显示。

为应用程序分配权限的步骤

1. 转到 Microsoft Sentinel。
2. 选择*订阅* > 访问控制 **(IAM)**。
3. 选择*添加* > 添加角色分配。
4. 对于*特权管理员角色*字段，选择*勒索软件弹性哨兵配置器*。

   这是您之前创建的自定义角色。

5. 选择“下一步”。
6. 在*分配访问权限*字段中，选择*用户、组或服务主体*。
7. 选择“选择成员”。然后，选择*Ransomware Resilience Sentinel Configurator*。
8. 选择“下一步”。
9. 在*用户可以做什么*字段中，选择*允许用户分配除特权管理员角色所有者、UAA、RBAC（推荐）之外的所有角色*。
10. 选择“下一步”。
11. 选择*审核并分配*来分配权限。

输入应用程序身份验证凭据的步骤

1. 转到 Microsoft Sentinel。
2. 输入凭证：
   a. 输入租户 ID、客户端应用程序 ID 和客户端应用程序密钥。
   b. 单击“验证”。

      认证成功后，会出现“已认证”的信息。

3. 输入应用程序的 Log Analytics 工作区详细信息。
   a. 选择订阅 ID、资源组和 Log Analytics 工作区。

配置 **Splunk Cloud** 进行威胁检测

在 Ransomware Resilience 中启用 Splunk Cloud 之前，您需要在 Splunk Cloud 中执行以下高级步骤：

- 在 Splunk Cloud 中启用 HTTP 事件收集器以通过 HTTP 或 HTTPS 从控制台接收事件数据。
- 在 Splunk Cloud 中创建事件收集器令牌。

在 **Splunk** 中启用 **HTTP** 事件收集器的步骤

1. 转到 Splunk Cloud。
2. 选择*设置* > 数据输入。
3. 选择 **HTTP** 事件收集器 > 全局设置。
4. 在所有令牌切换上，选择*已启用*。

5. 要让事件收集器通过 HTTPS 而不是 HTTP 进行监听和通信，请选择“启用 SSL”。
6. 在“HTTP 端口号”中输入 HTTP 事件收集器的端口。

在 **Splunk** 中创建事件收集器令牌的步骤

1. 转到 Splunk Cloud。
2. 选择*设置* > 添加数据。
3. 选择*监控* > **HTTP** 事件收集器。
4. 输入令牌的名称并选择*下一步*。
5. 选择将推送事件的*默认索引*，然后选择*审核*。
6. 确认端点的所有设置正确，然后选择*提交*。
7. 复制令牌并将其粘贴到另一个文档中，以准备进行身份验证步骤。

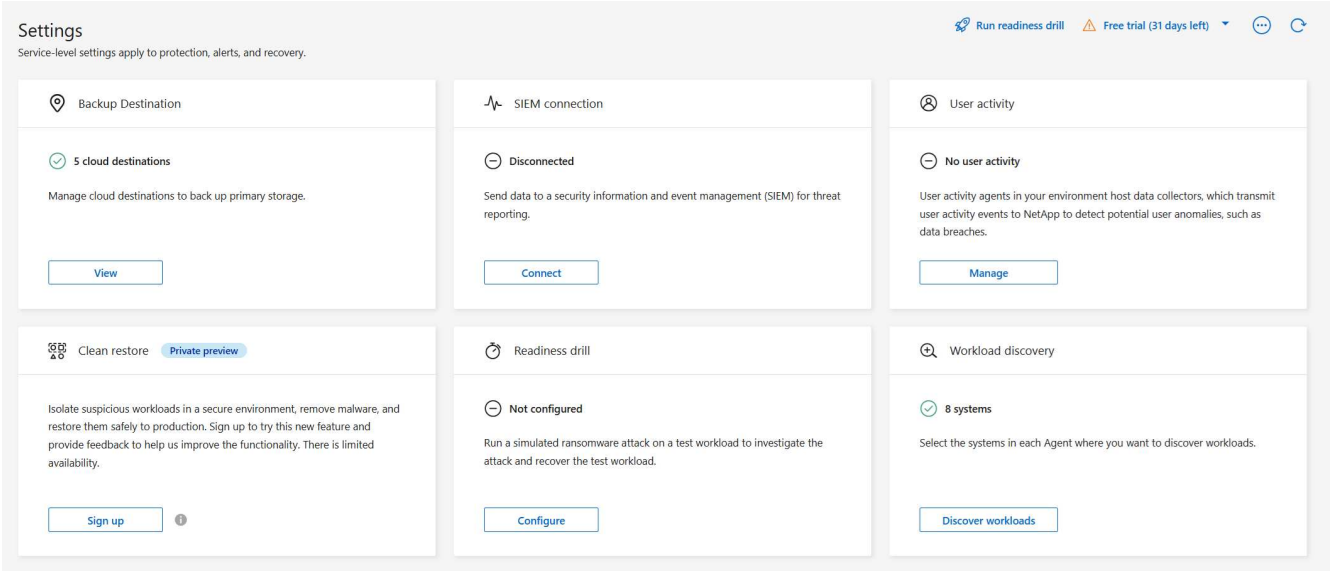
在勒索软件防御中连接 **SIEM**

启用 SIEM 会将勒索软件恢复数据发送到您的 SIEM 服务器以进行威胁分析和报告。

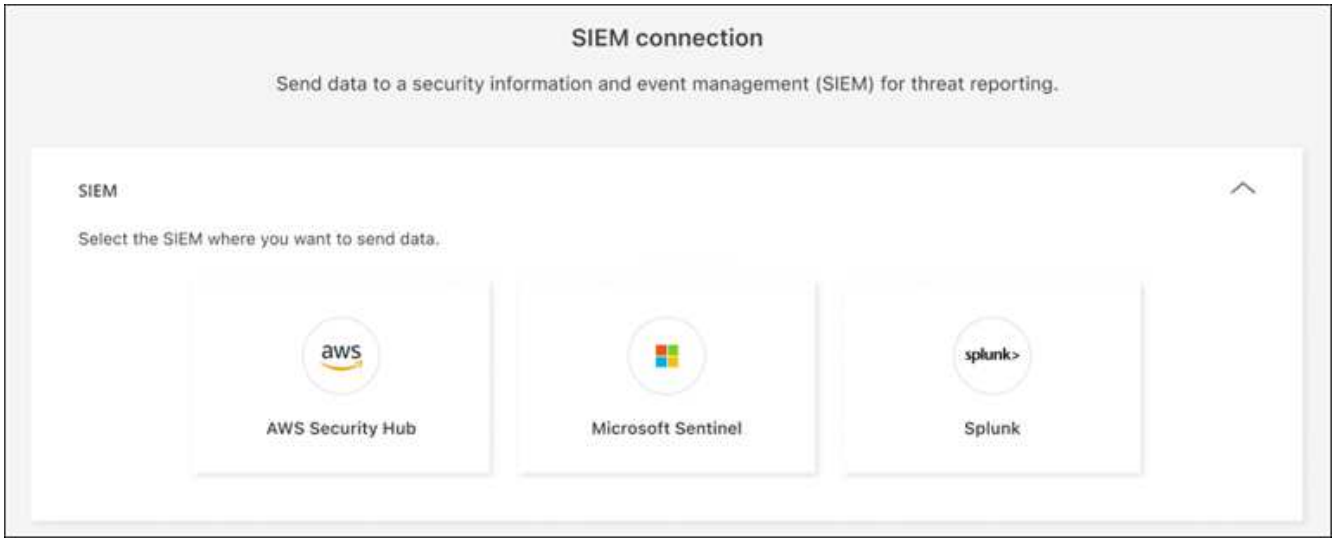
步骤

1. 从控制台菜单中，选择*保护*>*勒索软件恢复*。
2. 从勒索软件恢复菜单中，选择垂直 …右上角的选项。
3. 选择“设置”。

   出现“设置”页面。



4. 在“设置”页面中，选择 SIEM 连接图块中的“连接”。



5. 选择其中一个 SIEM 系统。
6. 输入您在 AWS Security Hub 或 Splunk Cloud 中配置的令牌和身份验证详细信息。

   您输入的信息取决于您选择的 SIEM。

7. 选择*启用*。

   设置页面显示“已连接”。

在NetApp Ransomware Resilience中配置可疑用户活动检测

勒索软件抵御能力支持在检测策略中检测可疑用户行为，使您能够在用户级别解决勒索软件事件。

勒索软件弹性通过分析ONTAP中 FPolicy 生成的用户活动事件来检测可疑的用户活动。要收集用户活动数据，您需要部署一个或多个用户活动代理。该代理是可连接到租户上的设备的 Linux 服务器或 VM。

代理商和收藏家

必须安装至少一个用户活动代理才能激活 Ransomware Resilience 中的可疑用户活动检测。当您从勒索软件恢复仪表板激活可疑用户活动功能时，您需要提供代理主机信息来激活该功能。

一个代理可以托管多个数据收集器。数据收集器将数据发送到 SaaS 位置进行分析。有两种类型的收集器：

- 数据收集器从ONTAP收集用户活动数据。
- 用户目录连接器连接到您的目录以将用户 ID 映射到用户名。

收集器在勒索软件恢复设置中配置。

启用可疑用户活动检测

所需的控制台角色 要激活可疑用户活动检测，您需要组织管理员角色。对于可疑用户活动的后续配置，您需要 Ransomware Resilience 用户行为管理员角色。"了解NetApp Console的勒索软件恢复角色"。

添加用户活动代理

用户活动代理是数据收集器的可执行环境；数据收集器与勒索软件恢复共享用户活动事件。您必须创建至少一个用户活动代理才能启用可疑用户活动检测。

要求

要安装用户活动代理，您需要一个满足以下支持的操作系统和服务器要求的主机或虚拟机。

操作系统要求

操作系统	支持的版本
AlmaLinux	9.4（64 位）至 9.5（64 位）和 10（64 位），包括 SELinux
CentOS	CentOS Stream 9（64 位）
Debian	11（64 位）、12（64 位），包括 SELinux
OpenSUSE 飞跃	15.3（64 位）至 15.6（64 位）
Oracle Linux	8.10（64 位）、9.1（64 位）至 9.6（64 位），包括 SELinux
红帽	8.10（64 位）、9.1（64 位）至 9.6（64 位）和 10（64 位），包括 SELinux
洛基	Rocky 9.4（64 位）至 9.6（64 位），包括 SELinux
SUSE 企业 Linux	15 SP4（64 位）至 15 SP6（64 位），包括 SELinux
Ubuntu	20.04 LTS（64 位）、22.04 LTS（64 位）和 24.04 LTS（64 位）

服务器要求

服务器必须满足以下最低要求：

- **CPU**：4 核
- 内存：16GB 内存
- 磁盘空间：35GB 可用磁盘空间

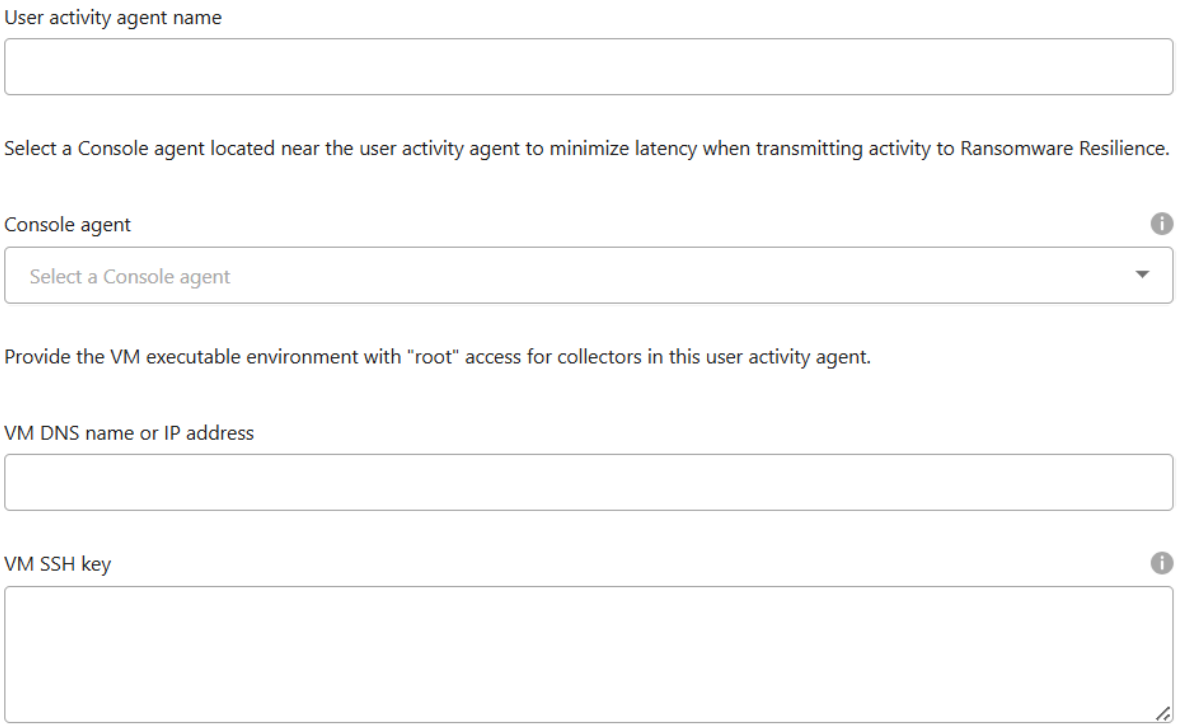
步骤

1. 如果这是您第一次创建用户活动代理，请转到仪表板。在用户活动图块中，选择激活。

   如果您要添加其他用户活动代理，请转到*设置*，找到用户活动图块，然后选择管理。在用户活动屏幕上，选择用户活动代理选项卡，然后选择添加。

2. 选择云提供商，然后选择区域。选择下一步。
3. 提供用户活动代理详细信息：
   - 用户活动代理名称
   - 控制台代理 - 控制台代理应与用户活动代理位于同一网络中，并通过 SSH 连接到用户活动代理 IP 地址。

- **VM DNS** 名称或 **IP** 地址
- 虚拟机 **SSH** 密钥



4. 选择下一步。
5. 检查您的设置。选择*激活*以完成添加用户活动代理。
6. 确认用户活动代理已成功创建。在用户活动图块中，成功部署显示为“正在运行”。

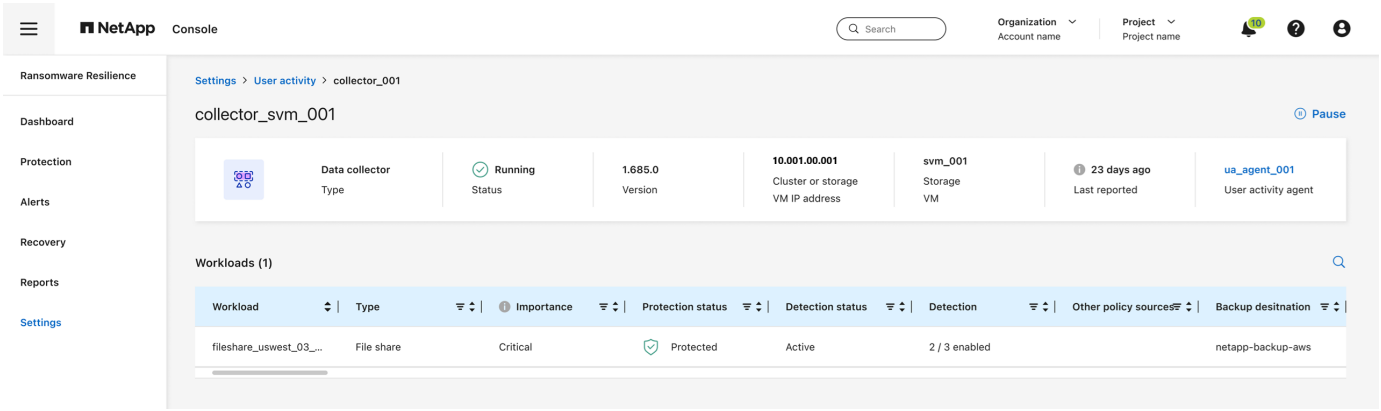
结果

成功创建用户活动代理后，返回设置菜单，然后在用户活动图块中选择管理。选择用户活动代理选项卡，然后选择用户活动代理以查看有关它的详细信息，包括数据收集器和用户目录连接器。

添加数据收集器

当您启用具有可疑用户活动检测功能的勒索软件保护策略时，数据收集器会自动创建。有关详细信息，请参阅添加检测策略。

您可以查看数据收集器的详细信息。从“设置”中，选择“用户活动”图块中的“管理”。选择数据收集器选项卡，然后选择数据收集器以查看其详细信息或暂停它。

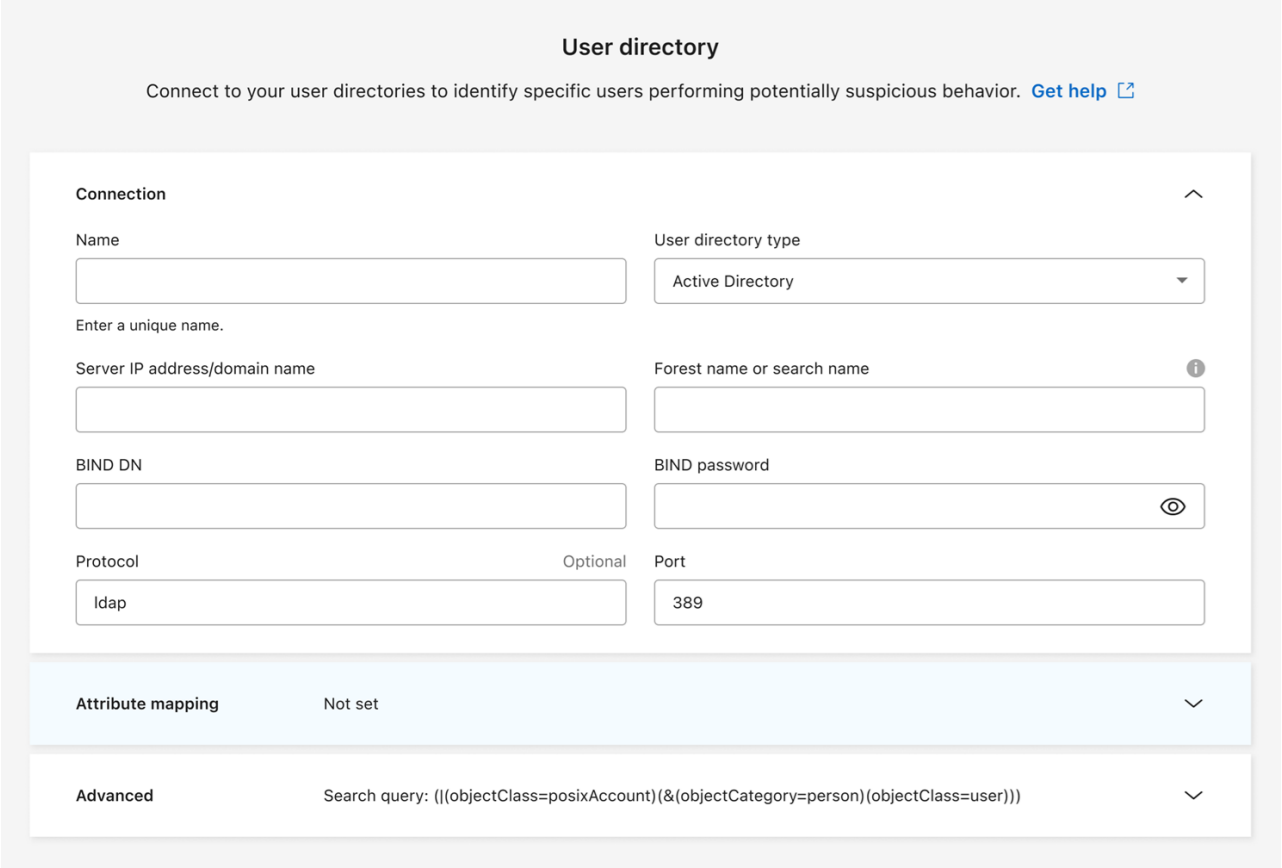


添加用户目录连接器

要将用户 ID 映射到用户名，您必须创建用户目录连接器。

步骤

1. 在勒索软件恢复中，转到*设置*。
2. 在用户活动图块中，选择管理。
3. 选择用户目录连接器选项卡，然后选择添加。
4. 提供连接的详细信息：
    - 姓名
    - 用户目录类型
    - 服务器**IP**地址或域名
    - 森林名称或搜索名称
    - **BIND** 域名
    - 绑定密码
    - 协议（可选）
    - 港口



提供属性映射详细信息：

- 显示名称
- **SID**（如果您使用 LDAP）
- 用户名
- **Unix ID**（如果您使用 NFS）
- 选择*包括可选属性*。您还可以包括电子邮件地址、电话号码、角色、州、国家、部门、照片、经理 DN 或群组。

  选择“高级”以添加可选的搜索查询。

5. 选择添加。
6. 返回用户目录连接器选项卡以检查用户目录连接器的状态。如果创建成功，用户目录连接器的状态显示为*正在运行*。

删除用户目录连接器

1. 在勒索软件恢复中，转到*设置*。
2. 找到用户活动图块，选择管理。
3. 选择用户目录连接器选项卡。
4. 确定要删除的用户目录连接器。在行尾的操作菜单中，选择三个点 `…`然后删除。
5. 在弹出的对话框中，选择删除以确认您的操作。

响应可疑用户活动警报

配置可疑用户活动检测后，您可以在警报页面中监控事件。有关更多信息，请参阅"检测恶意活动和异常用户行为" 。

使用勒索软件弹性

使用NetApp Ransomware Resilience

借助NetApp Ransomware Resilience，您可以查看工作负载的健康状况并保护工作负载。

- "发现勒索软件恢复中的工作负载" 。
- "从仪表板查看保护和工作负载健康状况" 。
  - 审查并采取勒索软件保护建议。
- "保护工作负载"：
  - 为工作负载分配勒索软件保护策略。
  - 加强应用程序保护以防止未来的勒索软件攻击。
  - 创建、更改或删除保护策略。
- "响应检测到的潜在勒索软件攻击" 。
- "从攻击中恢复"（事件消除后）。
- "配置保护设置" 。

使用 NetAPp 勒索软件恢复力仪表板监控工作负载健康状况

NetApp Ransomware Resilience仪表板提供有关工作负载保护健康状况的概览信息。您可以快速确定处于危险之中或受保护的工作负载，识别受事件影响或处于恢复中的工作负载，并通过查看受保护或处于危险中的存储量来衡量保护程度。

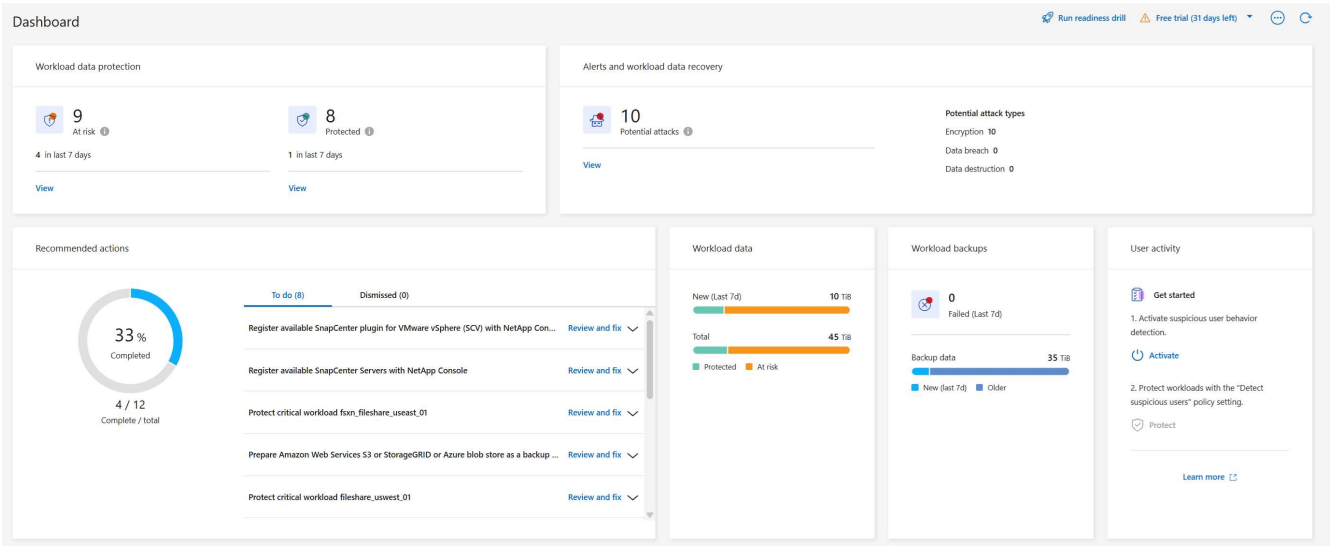
使用仪表板查看保护建议、更改设置、下载报告和查看文档。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员、勒索软件恢复管理员或勒索软件恢复查看器角色。"了解NetApp Console的勒索软件恢复角色" 。

使用仪表板检查工作负载健康状况

步骤

1. 控制台发现您的工作负载后，勒索软件恢复仪表板将显示工作负载数据保护健康状况。



2. 在仪表板中，您可以在每个窗格中执行以下操作：

   - 工作负载数据保护：选择*查看全部*可在保护页面上查看所有处于危险中或受保护的工作负载。当保护级别与保护策略不匹配时，工作负载就会面临风险。请参阅"保护工作负载"。

     选择“i”工具提示即可查看有关此数据的提示。要增加工作量限制，请选择此 i 注释内的 增加工作量限制。选择此选项将带您进入控制台支持页面，您可以在其中创建案例单。

   - 警报和工作负载数据恢复：选择*查看全部*可查看已影响您的工作负载的活动事件、在事件消除后准备恢复的事件或正在恢复的事件。请参阅"响应检测到的警报"。
     - 事件分为以下状态之一：
       - 新增
       - 已取消
       - 解散
       - 已解决
     - 警报可以具有以下状态之一：
       - 新增
       - 非活动
     - 工作负载可以具有以下还原状态之一：
       - 需要恢复
       - 进行中
       - 已恢复
       - 失败
   - 推荐的措施：为了增强保护，请查看每项建议，然后选择*查看并修复*。

     看"查看仪表板上的保护建议"或者"保护工作负载"。

     勒索软件恢复力会显示自您上次访问仪表板以来 24 小时内带有“新”标签的新建议。操作按优先顺序显示

，最重要的操作位于顶部。审查、执行或驳回每项建议。

总操作数不包括您已忽略的操作。

- 工作负载数据：监控过去 7 天内保护覆盖范围的变化。
- 工作负载备份：监控过去 7 天内由勒索软件恢复创建的失败或成功完成的工作负载备份的变化。

查看仪表板上的保护建议

勒索软件恢复能力会评估您工作负载的保护情况，并建议采取措施来改善保护。

您可以查看建议并采取行动，这会将建议状态更改为“完成”。或者，如果您想稍后采取行动，您可以忽略它。忽略某项操作会将建议移至已忽略操作列表中，以便您稍后查看。

以下是 Ransomware Resilience 提供的一些建议。

建议	描述	如何解决
添加勒索软件保护策略。	工作负载目前不受保护。	为工作负载分配策略。请参阅"保护工作负载免受勒索软件攻击" 。
连接到 SIEM 进行威胁报告。	将数据发送到安全和事件管理系统 (SIEM) 进行威胁分析和检测。	输入 SIEM/XDR 服务器详细信息以启用威胁检测。请参阅"配置保护设置" 。
为应用程序或 VMware 启用工作负载一致的保护。	这些工作负载不由SnapCenter软件或SnapCenter Plug-in for VMware vSphere管理。	要让它们由SnapCenter管理，请启用工作负载一致的保护。请参阅"保护工作负载免受勒索软件攻击" 。
改善系统的安全态势	NetApp Digital Advisor已发现至少一个高或严重的安全风险。	审查NetApp Digital Advisor中的所有安全风险。参考 "Digital Advisor文档"。
使政策更加有力。	某些工作负载可能没有足够的保护。通过策略加强对工作负载的保护。	增加保留、添加备份、强制执行不可变备份、阻止可疑文件扩展名、启用二级存储检测等。请参阅"保护工作负载免受勒索软件攻击" 。
准备 <备份提供商> 作为备份目标来备份您的工作负载数据。	工作负载目前没有任何备份目标。	向此工作负载添加备份目标以保护它。请参阅"配置保护设置" 。
保护关键或高度重要的应用程序工作负载免受勒索软件的攻击。	保护页面显示未受保护的关键或高度重要（基于分配的优先级）应用程序工作负载。	为这些工作负载分配策略。请参阅"保护工作负载免受勒索软件攻击" 。
保护关键或高度重要的文件共享工作负载免受勒索软件的侵害。	保护页面显示未受保护的文件共享或数据存储类型的关键或高度重要的工作负载。	为每个工作负载分配一个策略。请参阅"保护工作负载免受勒索软件攻击" 。
使用控制台注册适用于 VMware vSphere (SCV) 的SnapCenter插件	VM 工作负载未受到保护。	通过启用适用于 VMware vSphere 的SnapCenter插件，为 VM 工作负载分配 VM 一致的保护。请参阅"保护工作负载免受勒索软件攻击" 。

建议	描述	如何解决
使用控制台注册可用的SnapCenter服务器	应用程序不受保护。	通过启用SnapCenter Server 为工作负载分配应用程序一致的保护。请参阅"保护工作负载免受勒索软件攻击" 。
查看新警报。	存在新的警报。	查看新警报。请参阅"响应检测到的勒索软件警报" 。

步骤

1. 从勒索软件恢复中的“推荐操作”窗格中，选择一个建议，然后选择“查看并修复”。
2. 要稍后再取消该操作，请选择“取消”。

   该建议将从“待办事项”列表中清除并出现在“已忽略”列表中。

   您稍后可以将已消除的项目更改为待办事项。当您将某项标记为已完成或将已解除的项更改为待办事项时，总操作数会增加 1。

3. 要查看有关如何根据建议采取行动的信息，请选择*信息*图标。

将保护数据导出到 CSV 文件

您可以导出数据并下载显示保护、警报和恢复详细信息的 CSV 文件。

您可以从任何主菜单选项下载 CSV 文件：

- 保护：包含所有工作负载的状态和详细信息，包括勒索软件弹性标记为受保护或处于危险中的工作负载总数。
- 警报：包括所有警报的状态和详细信息，包括警报总数和自动快照。
- 恢复：包括需要恢复的所有工作负载的状态和详细信息，包括勒索软件恢复标记为“需要恢复”、“进行中”、“恢复失败”和“成功恢复”的工作负载总数。

从页面下载的 CSV 文件仅包含该页面的数据。

CSV 文件包含所有控制台系统上所有工作负载的数据。

步骤

1. 从勒索软件恢复力仪表板中，选择*刷新*右上角的选项可刷新文件中显示的数据。
2. 执行以下操作之一：
   - 从页面上选择*下载*选项。
   - 从勒索软件恢复菜单中，选择*报告*。
3. 如果您选择了“报告”选项，请选择一个预配置的命名文件，然后选择“下载（**CSV**）”或“下载（**JSON**）”。

访问技术文档

您可以从以下位置访问勒索软件恢复技术文档"docs.netapp.com"或从勒索软件恢复力内部。

步骤

1. 从勒索软件恢复力仪表板中，选择垂直*操作* 选项。
2. 选择以下选项之一：
   - 新功能 查看发行说明中当前或以前版本的功能信息。
   - 文档 查看勒索软件恢复文档主页和此文档。

保护工作负载

使用NetApp Ransomware Resilience保护策略保护工作负载

您可以通过在NetApp Ransomware Resilience中启用工作负载一致性保护或创建勒索软件保护策略来保护工作负载免受勒索软件攻击。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

了解勒索软件防护策略

勒索软件保护策略包括_检测_和_保护_策略。

- 检测策略 检测勒索软件威胁
- 保护策略包括快照和备份策略。保护策略中需要检测和快照策略。备份策略是可选的。

  如果您使用其他NetApp产品来保护您的工作负载，勒索软件恢复能力会发现这些产品并提供以下选项：

  - 使用勒索软件检测策略并继续使用其他NetApp工具创建的快照和备份策略，或者
  - 使用勒索软件弹性来管理检测、快照和备份。

为了增强对数据资产的管理和保护，您可以创建"群组文件共享"通过一种策略来集体保护卷。

与其他NetApp托管服务结合的保护策略

除了勒索软件恢复能力之外，还可以使用以下服务来管理保护：

- NetApp Backup and Recovery、VM 文件共享
- SnapCenter for VMware 适用于虚拟机数据存储区
- 适用于 Oracle 和 MySQL 的SnapCenter

这些服务的保护信息出现在 Ransomware Resilience 中。您可以使用 Ransomware Resilience 向这些服务添加检测策略。添加具有勒索软件恢复能力的保护策略将取代现有的保护策略。

如果勒索软件检测策略由ONTAP中的自主勒索软件防护（ARP 或 ARP/AI，取决于ONTAP版本）和 FPolicy 管理，则这些工作负载将受到保护并将继续由 ARP 和 FPolicy 管理。

Amazon FSx for NetApp ONTAP中的工作负载没有可用的备份目标。使用 FSx for ONTAP备份服务执行备份操作。您为 AWS 中的 FSx for ONTAP中的工作负载设置备份策略，而不是在 Ransomware Resilience 中设置。备份策略出现在 Ransomware Resilience 中，与 AWS 保持不变。

针对不受**NetApp**应用程序保护的工作负载的保护策略

如果您的工作负载不是由备份和恢复、勒索软件恢复、 SnapCenter或SnapCenter Plug-in for VMware vSphere管理的，则它可能具有作为ONTAP或其他产品的一部分拍摄的快照。如果ONTAP FPolicy 保护已到位，则可以使用ONTAP更改 FPolicy 保护。

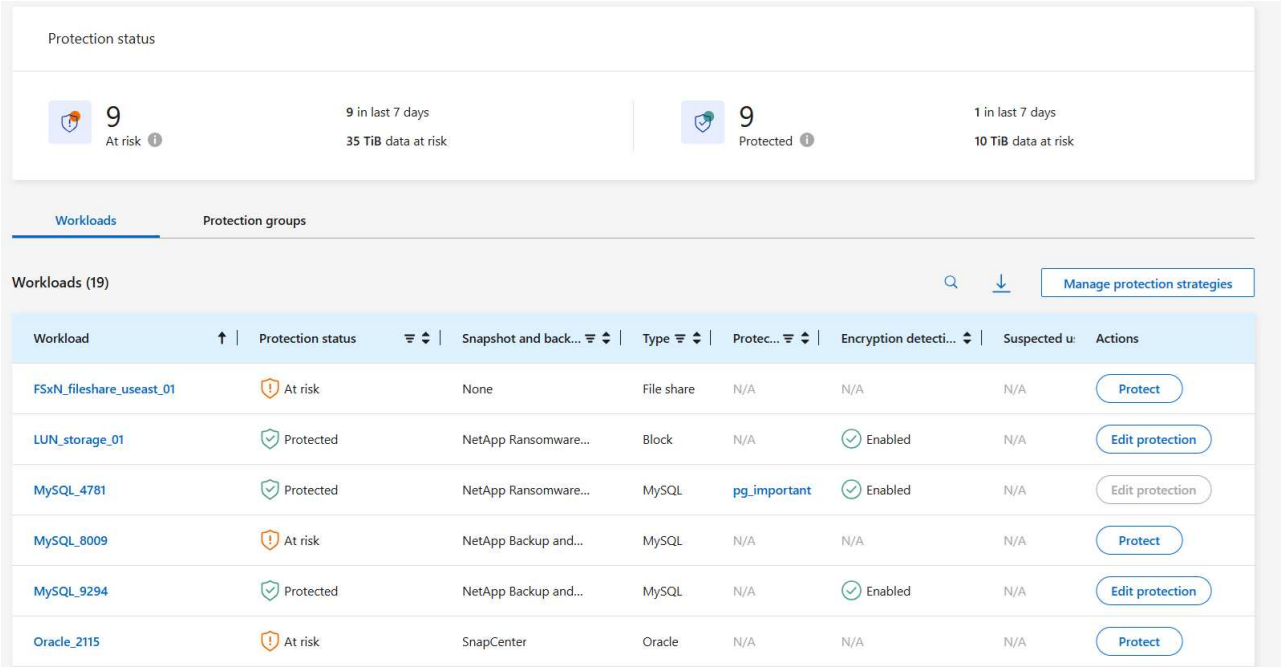
查看工作负载上的勒索软件保护

保护工作负载的第一步是查看当前工作负载及其保护状态。您可以看到以下类型的工作负载：

- 应用程序工作负载
- 阻止工作负载
- 文件共享工作负载
- 虚拟机工作负载

步骤

1. 从控制台左侧导航中，选择*保护*>*勒索软件恢复*。
2. 执行以下操作之一：
   - 从仪表板上的数据保护窗格中，选择“查看全部”。
   - 从菜单中选择*保护*。



3. 在此页面中，您可以查看和更改工作负载的保护详细信息。

看"添加勒索软件防护策略"了解在存在SnapCenter或备份和恢复的现有保护策略的情况下使用勒索软件恢复能力的情况。

了解保护页面

保护页面显示有关工作负载保护的以下信息：

保护状态：工作负载可以显示以下保护状态之一，以指示是否应用了策略：

- 受保护：已应用策略。与工作负载相关的所有卷上均启用了 ARP（或 ARP/AI，取决于ONTAP版本）。
- 存在风险：未应用任何政策。如果工作负载没有启用主要检测策略，那么即使启用了快照和备份策略，它仍然“处于危险之中”。
- 进行中：政策正在应用但尚未完成。
- 失败：策略已应用但不起作用。

检测状态：工作负载可以具有以下勒索软件检测状态之一：

- 学习：最近为工作负载分配了勒索软件检测策略，并且勒索软件恢复正在扫描工作负载。
- 主动：已分配勒索软件检测保护策略。
- 未设置：未分配勒索软件检测保护策略。
- 错误：已分配勒索软件检测策略，但勒索软件恢复遇到错误。

当在勒索软件恢复中启用保护时，勒索软件检测策略状态从学习模式变为主动模式后，警报检测和报告开始。

检测策略：如果已分配勒索软件检测策略，则会显示其名称。如果尚未分配检测策略，则会显示“N/A”。

快照和备份策略：此列显示应用于工作负载的快照和备份策略以及管理这些策略的产品或服务。

- 由SnapCenter管理
- 由适用于SnapCenter Plug-in for VMware vSphere管理
- 由备份和恢复管理
- 管理快照和备份的勒索软件保护策略的名称
- 无

工作量的重要性

勒索软件恢复能力根据对每个工作负载的分析，在发现过程中为每个工作负载分配重要性或优先级。工作负载重要性由以下快照频率决定：

- 严重：每小时拍摄的快照副本超过 1 个（高度激进的保护计划）
- 重要：每小时拍摄的快照副本少于 1 个，但每天拍摄的快照副本多于 1 个
- 标准：每天拍摄的快照副本超过 1 个

预定义检测策略

您可以选择以下勒索软件恢复预定义策略之一，这些策略与工作负载重要性相一致。

加密用户扩展策略是唯一支持可疑用户行为检测的预定义策略。

政策层面	Snapshot	频率	保留时间（天）	快照副本数量	快照副本总数上限
关键工作量政策	每刻钟	每15分钟	3	288	309
	每日	每 1 天	14	14	309
	每周	每 1 周	35	5	309
	每月	每 30 天	60	2	309
重要的工作量政策	每刻钟	每30分钟一班	3	144	165
	每日	每 1 天	14	14	165
	每周	每 1 周	35	5	165
	每月	每 30 天	60	2	165
标准工作量政策	每刻钟	每30分钟	3	72	93
	每日	每 1 天	14	14	93
	每周	每 1 周	35	5	93
	每月	每 30 天	60	2	93
加密用户扩展	每刻钟	每30分钟	3	72	93
	每日	每 1 天	14	14	93
	每周	每 1 周	35	5	93
	每月	每 30 天	60	2	93

使用**SnapCenter**实现应用程序或虚拟机一致的保护

启用应用程序或虚拟机一致性保护可帮助您以一致的方式保护应用程序或虚拟机工作负载，实现静止和一致的状态，以避免以后需要恢复时发生潜在的数据丢失。

此过程启动使用备份和恢复为应用程序注册SnapCenter软件服务器或SnapCenter Plug-in for VMware vSphere。

启用工作负载一致性保护后，您可以在勒索软件恢复中管理保护策略。保护策略包括在其他地方管理的快照和备份策略以及在勒索软件恢复中管理的勒索软件检测策略。

要了解如何使用备份和恢复注册适用于 VMware vSphere 的SnapCenter或SnapCenter Plug-in for VMware vSphere，请参阅以下信息：

- "注册SnapCenter服务器软件"
- "SnapCenter Plug-in for VMware vSphere"

步骤

1. 从勒索软件恢复菜单中，选择*仪表板*。
2. 从“建议”窗格中，找到以下建议之一并选择“审阅并修复”：
   - 使用NetApp Console注册可用的SnapCenter服务器
   - 使用NetApp Console注册适用SnapCenter Plug-in for VMware vSphere（SCV）
3. 按照信息使用备份和恢复为 VMware vSphere 主机注册SnapCenter或SnapCenter Plug-in for VMware vSphere。
4. 返回勒索软件恢复能力。
5. 从勒索软件恢复力导航到仪表板并再次启动发现过程。
6. 从勒索软件恢复中，选择“保护”以查看“保护”页面。
7. 查看“保护”页面上的快照和备份策略列中的详细信息，以了解这些策略是否在其他地方进行管理。

添加勒索软件防护策略

添加勒索软件保护策略有三种方法：

- 如果您没有快照或备份策略，请创建勒索软件保护策略。

  勒索软件防护策略包括：

  - Snapshot 策略
  - 勒索软件检测政策
  - 备份策略
- 用勒索软件恢复管理的保护策略替换**SnapCenter**或备份和恢复保护中的现有快照或备份策略。

  勒索软件防护策略包括：

  - Snapshot 策略
  - 勒索软件检测政策
  - 备份策略
- 使用其他**NetApp**产品或服务中管理的现有快照和备份策略为工作负载创建检测策略。

检测策略不会改变其他产品中管理的策略。

如果已在其他服务中激活了自主勒索软件保护和 FPolicy 保护，则检测策略将启用它们。详细了解"自主勒索软件防护"，"备份和恢复" ， 和"ONTAP FPolicy"。

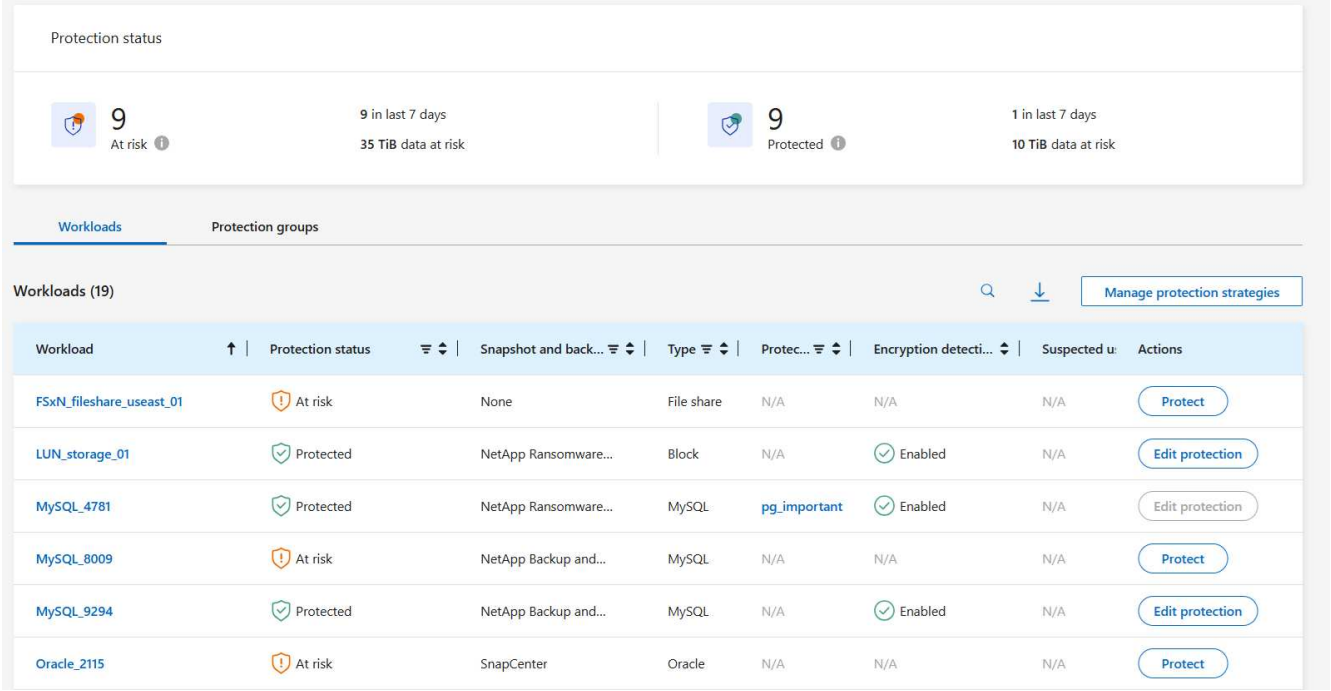
创建勒索软件保护策略（如果您没有快照或备份策略）

如果工作负载上不存在快照或备份策略，您可以创建勒索软件保护策略，其中可以包括您在勒索软件恢复中创建的以下策略：

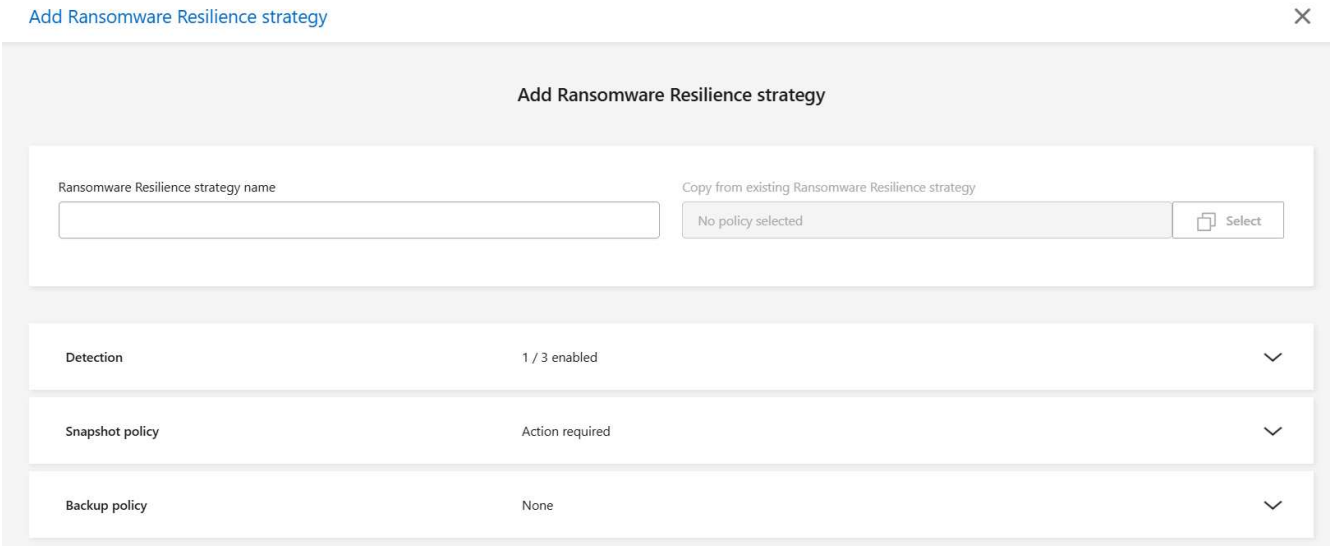
- Snapshot 策略
- 备份策略
- 勒索软件检测政策

创建勒索软件保护策略的步骤

1. 从勒索软件恢复菜单中，选择*保护*。



2. 在“保护”页面中，选择一个工作负载，然后选择“保护”。
3. 在勒索软件防护策略页面中，选择*添加*。



4. 输入新的策略名称，或输入现有名称进行复制。如果您输入的是现有名称，请选择要复制的名称并选择*复制*。

> 如果您选择复制并修改现有策略，Ransomware Resilience 会在原始名称后附加“_copy”。您应该更改名称和至少一个设置以使其唯一。

5. 对于每个项目，选择*向下箭头*。

   - 检测政策：
     - 策略：选择预先设计的检测策略之一。
     - 主要检测：启用勒索软件检测，让勒索软件恢复能力检测潜在的勒索软件攻击。
     - 可疑用户行为检测：启用用户行为检测，将用户活动事件传输到勒索软件恢复能力并检测可疑事件，例如数据泄露。
     - 阻止文件扩展名：启用此功能可让勒索软件恢复功能阻止已知的可疑文件扩展名。当启用主要检测时，勒索软件恢复能力会自动获取快照副本。

       如果您想更改被阻止的文件扩展名，请在系统管理器中编辑它们。
   - 快照策略：
     - 快照策略基础名称：选择一个策略或选择*创建*并输入快照策略的名称。
     - 快照锁定：启用此功能可锁定主存储上的快照副本，以便即使勒索软件攻击进入备份存储目标，它们在一定时间内也无法被修改或删除。这也称为_不可变存储_。这使得恢复时间更快。

       当快照被锁定时，卷的过期时间设置为快照副本的过期时间。

     Snapshot 副本锁定适用于ONTAP 9.12.1 及更高版本。要了解有关SnapLock 的更多信息，请参阅 "ONTAP中的SnapLock"。

     - 快照计划：选择计划选项、要保留的快照副本数量，然后选择启用计划。
   - 备份策略：
     - 备份策略基本名称：输入新名称或选择现有名称。

- 备份计划：选择二级存储的计划选项并启用该计划。

要在辅助存储上启用备份锁定，请使用*设置*选项配置备份目标。有关详细信息，请参阅"配置设置"。

6. 选择“添加”。

将检测策略添加到具有由**SnapCenter**或备份和恢复管理的现有快照和备份策略的工作负载

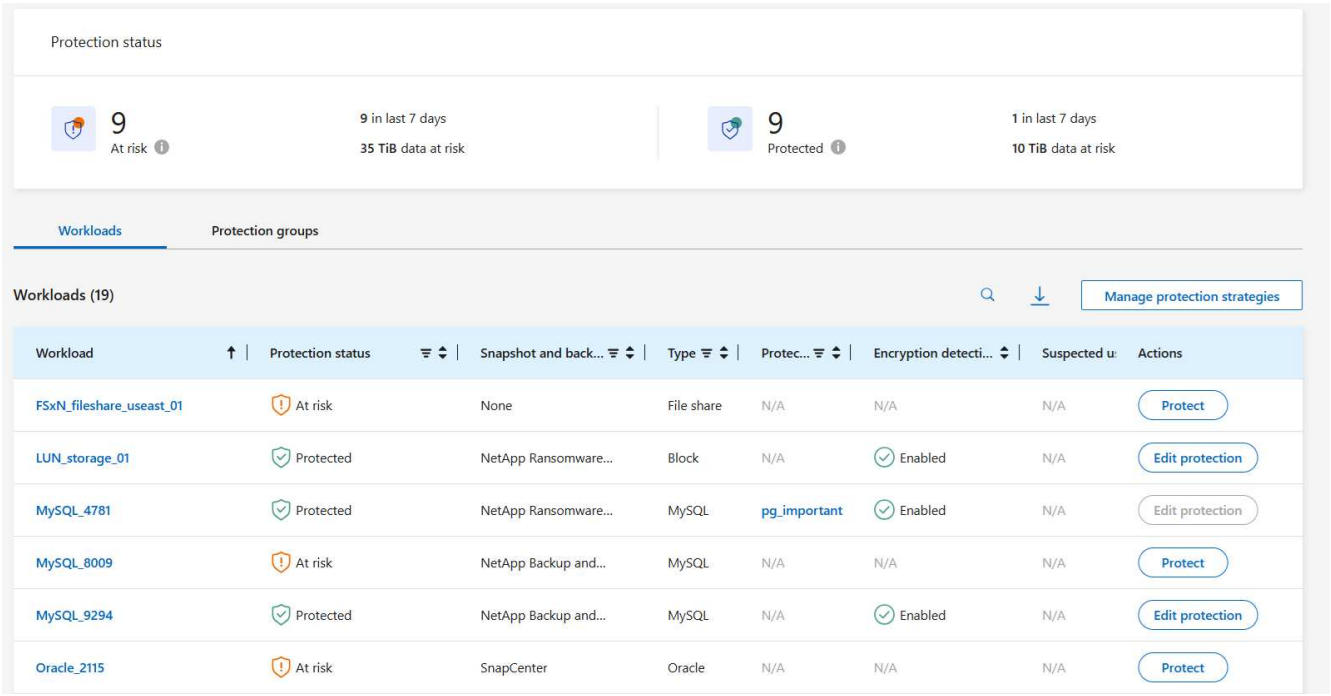
勒索软件恢复能力使您能够为在其他NetApp产品或服务中管理的现有快照和备份保护的工作负载分配检测策略或保护策略。其他服务（例如备份和恢复和SnapCenter）使用管理快照、复制到二级存储或备份到对象存储的策略。

向具有现有备份或快照策略的工作负载添加检测策略

如果您已有带有备份和恢复或SnapCenter 的快照或备份策略，则可以添加策略来检测勒索软件攻击。要使用 Ransomware Resilience 管理保护和检测，请参阅利用勒索软件抵御能力进行保护。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。



2. 在“保护”页面中，选择一个工作负载，然后选择“保护”。
3. 勒索软件恢复能力检测是否存在活动的SnapCenter或备份和恢复策略。
4. 要保留现有的备份和恢复或SnapCenter策略并仅应用_检测_策略，请取消选中替换现有策略框。
5. 要查看SnapCenter策略的详细信息，请选择*向下箭头*。
6. 选择您想要的检测设置：加密检测 可疑用户行为检测 阻止可疑文件扩展名
7. 选择下一步。
8. 如果您选择“可疑用户行为检测”作为检测设置，请选择“用户活动代理”或"或创建一个"。

用户活动代理托管新的数据收集器。Ransomware Resilience 自动创建数据收集器，将用户活动事件传输到 Ransomware Resilience 以检测异常用户行为。

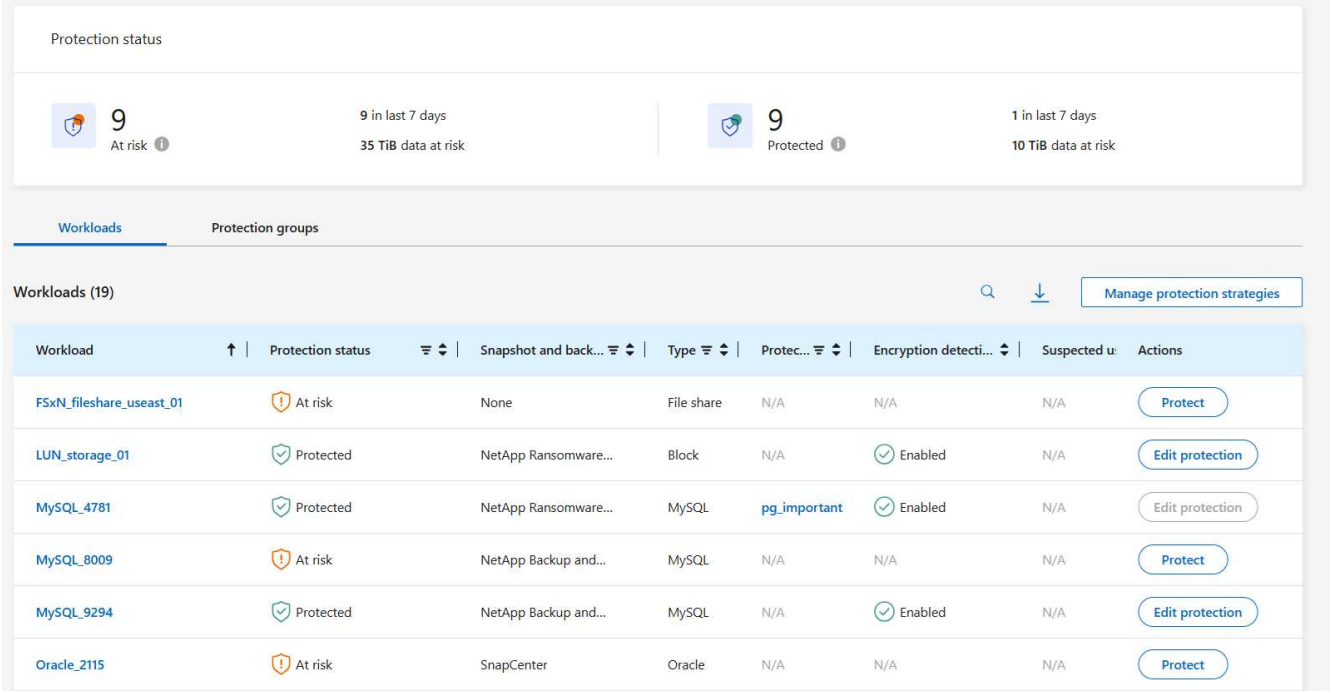
9. 选择下一步。
10. 审查您的选择。选择创建来激活检测。
11. 在“保护”页面上，查看检测状态以确认检测处于活动状态。

用勒索软件保护策略替换现有的备份或快照策略

您可以用勒索软件保护策略替换现有的备份或快照策略。这种方法会删除外部管理的保护，并在勒索软件恢复中配置检测和保护。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。



2. 在“保护”页面中，选择一个工作负载，然后选择“保护”。
3. 勒索软件恢复能力检测是否存在现有的活动备份和恢复或SnapCenter策略。要替换现有的备份和恢复或SnapCenter策略，请选中“替换现有策略”框。当您选中该框时，勒索软件恢复力会用检测策略替换检测策略列表。
4. 选择保护策略。如果不存在保护策略，请选择添加来创建新策略。有关创建策略的信息，请参阅创建保护策略。选择下一步。
5. 选择备份目标或创建一个新的备份目标。选择下一步。
   a. 如果您的保护策略包括用户行为检测，请在您的环境中选择一个用户活动代理来托管新的数据收集器。Ransomware Resilience 自动创建数据收集器，将用户活动事件传输到 Ransomware Resilience 以检测异常用户行为。
6. 查看新的保护策略，然后选择保护来应用它。
7. 在“保护”页面上，查看检测状态以确认检测处于活动状态。

分配不同的策略

您可以用其他策略替换现有策略。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面的工作负载行上，选择“编辑保护”。
3. 如果工作负载具有您想要维护的现有备份和恢复或SnapCenter策略，请取消选中“替换现有策略”。要替换现有策略，请选中替换现有策略。
4. 在“策略”页面中，选择要分配的策略的向下箭头以查看详细信息。
5. 选择您想要分配的策略。
6. 选择*保护*以完成更改。

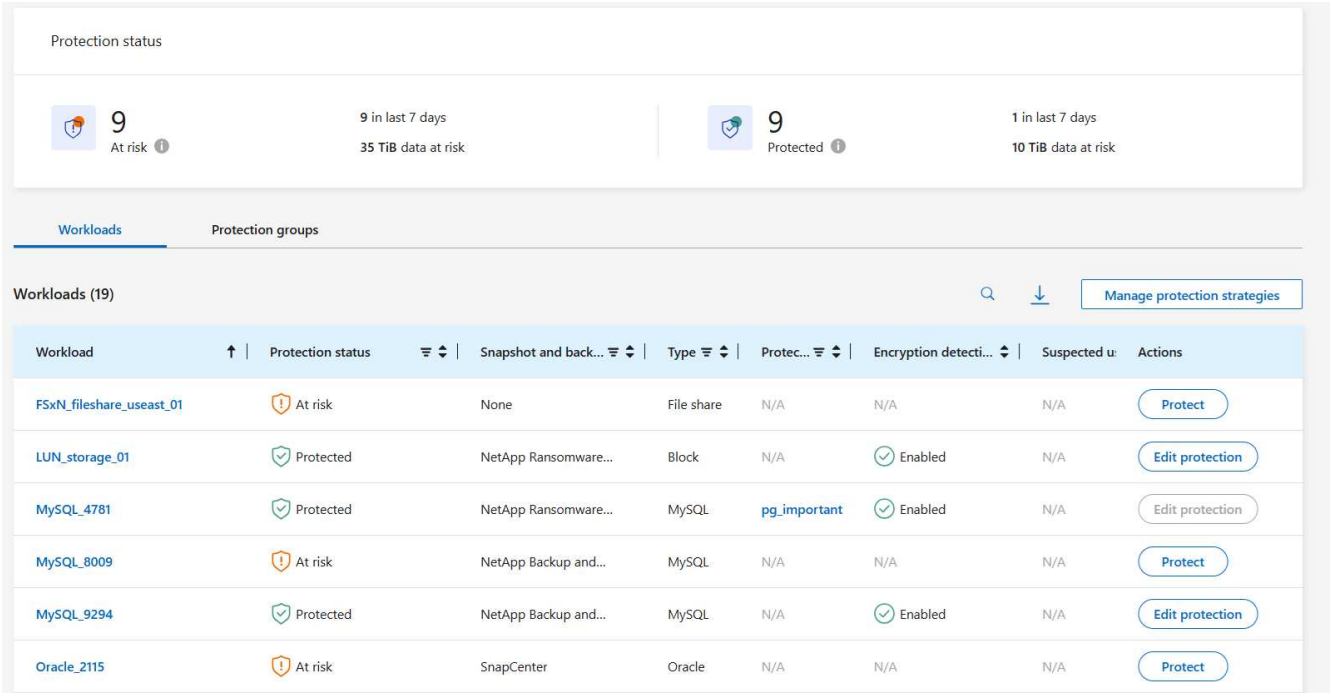
创建保护组

将文件共享分组到保护组中可以更轻松地保护您的数据资产。勒索软件恢复能力可以同时保护组中的所有卷，而不是单独保护每个卷。

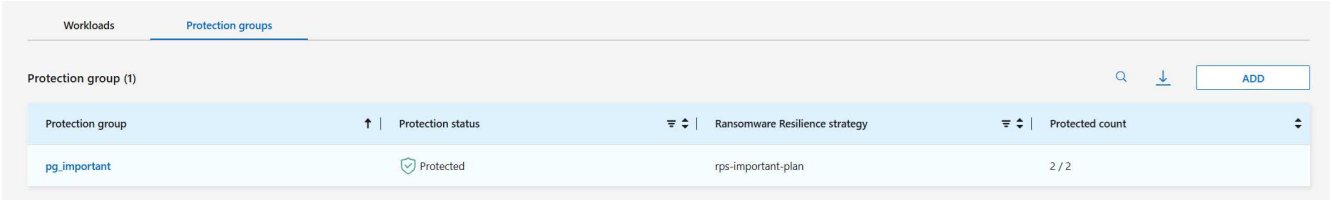
您可以创建组，而不管其保护状态如何（即未受保护的组和受保护的组）。当您将保护策略添加到保护组时，新的保护策略将替换任何现有策略，包括由SnapCenter和NetApp Backup and Recovery管理的策略。

步骤

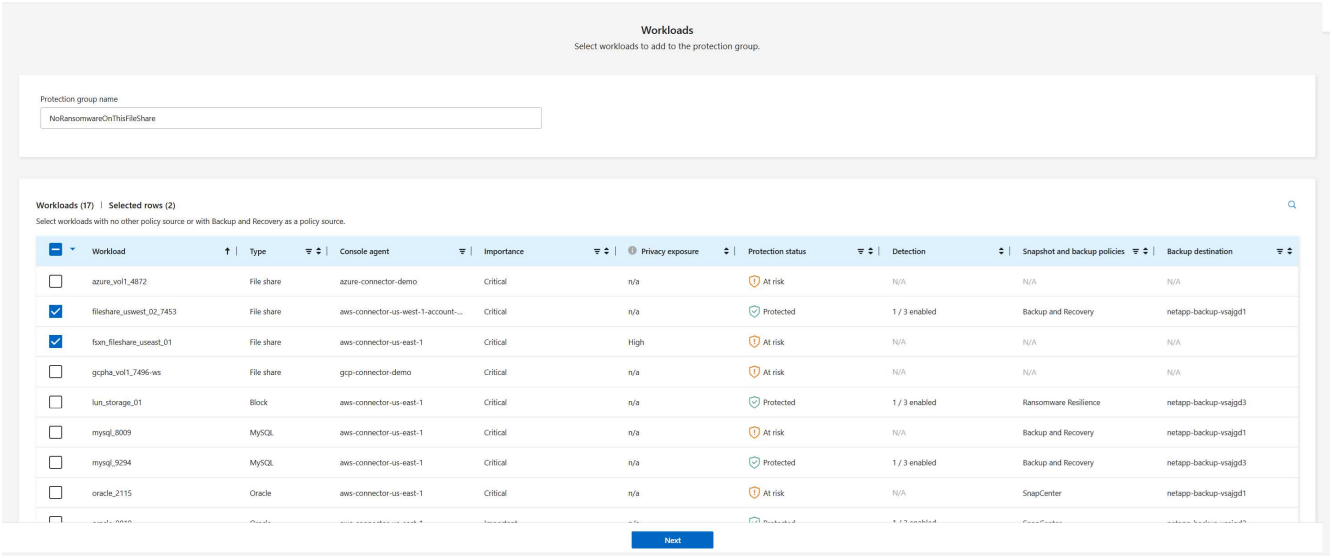
1. 从勒索软件恢复菜单中，选择*保护*。



2. 在“保护”页面中，选择“保护组”选项卡。



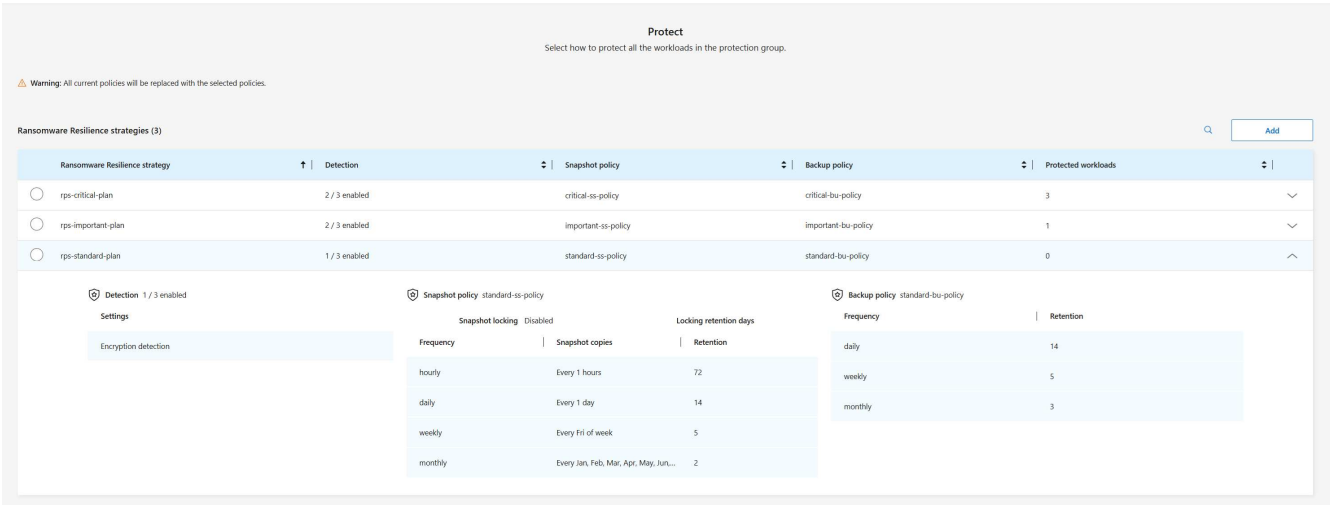
3. 选择“添加”。



4. 输入保护组的名称。
5. 选择要添加到组中的工作负载。

> 要查看有关工作负载的更多详细信息，请滚动到右侧。

6. 选择“下一步”。



7. 选择策略来管理该组的保护。要确认，请选择“下一步”。
   a. 如果需要配置备份策略，请选择一个，然后选择下一步。
   b. 如果您的检测策略包括用户行为检测，请选择您想要使用的数据收集器，然后单击下一步。

8. 检查保护组的选择。
9. 要完成保护组的创建，请选择“添加”。

编辑组保护

您可以更改现有组的检测策略。

步骤

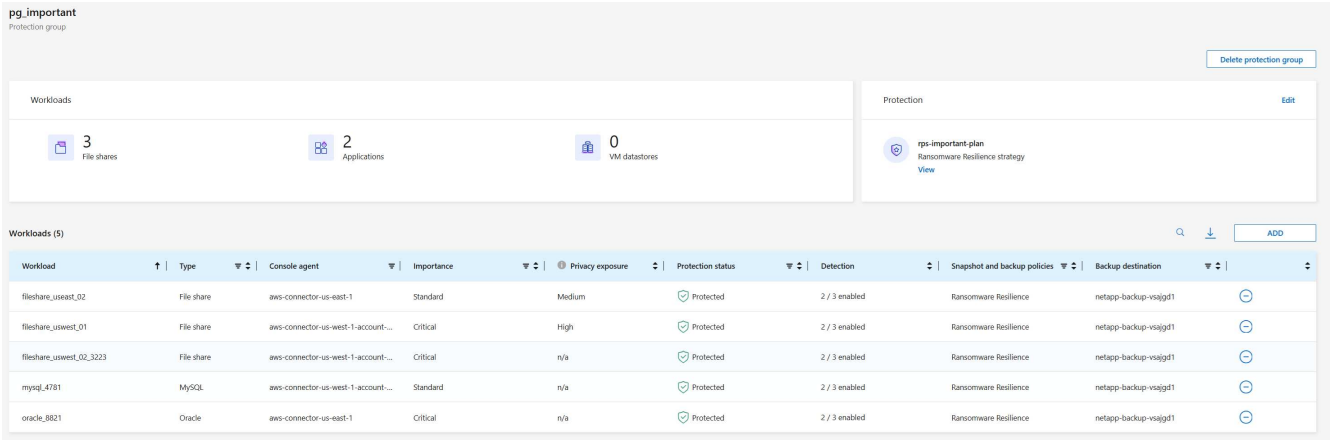
1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，选择“保护组”选项卡，然后选择要修改其策略的组。
3. 从保护组的概览页面中，选择“编辑保护”。
4. 选择要应用的现有保护策略或选择添加以创建新的保护策略。有关添加保护策略的更多信息，请参阅创建保护策略。然后选择保存。
5. 在备份目标概览中，选择现有的备份目标或添加新的备份目标。
6. 选择下一步来查看您的更改。

从组中删除工作负载

您可能稍后需要从现有组中删除工作负载。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，选择“保护组”选项卡。
3. 选择要从中删除一个或多个工作负载的组。



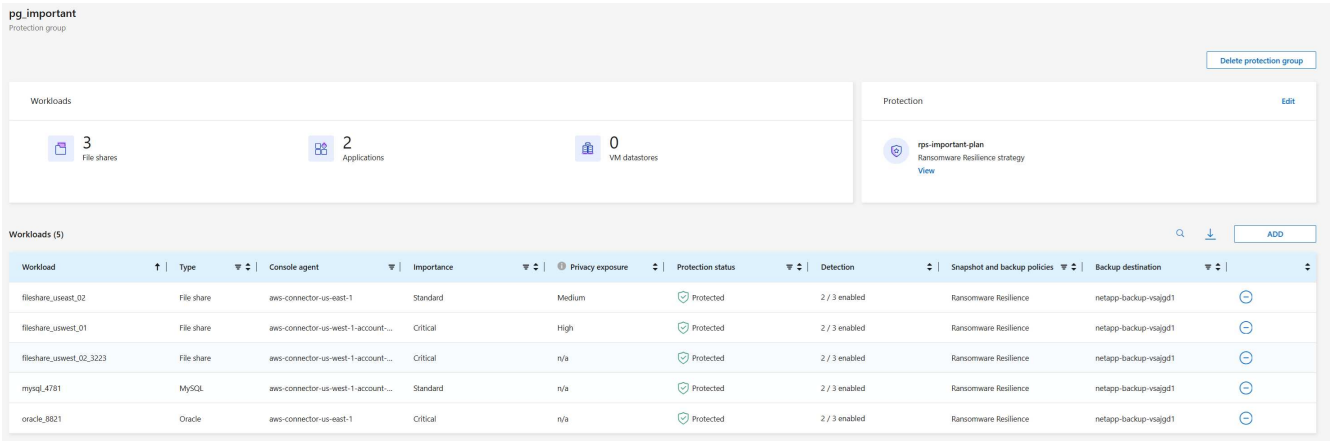
4. 在选定的保护组页面中，选择要从组中删除的工作负载，然后选择“操作”...选项。
5. 从“操作”菜单中，选择“删除工作负载”。
6. 确认您要删除工作负载并选择*删除*。

删除保护组

删除保护组会删除该组及其保护，但不会删除单个工作负载。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，选择“保护组”选项卡。
3. 选择要从中删除一个或多个工作负载的组。



4. 在选定的保护组页面的右上角，选择“删除保护组”。
5. 确认您要删除该组并选择*删除*。

管理勒索软件防护策略

您可以删除勒索软件策略。

查看受勒索软件保护策略保护的工作负载

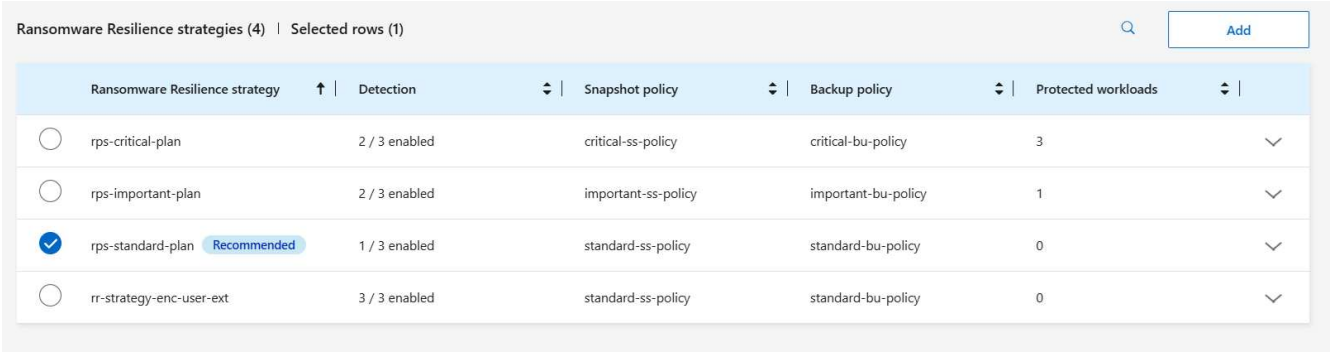
在删除勒索软件保护策略之前，您可能需要查看哪些工作负载受该策略保护。

您可以从策略列表中或在编辑特定策略时查看工作负载。

查看策略的步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，选择“管理保护策略”。

   勒索软件防护策略页面显示策略列表。



3. 在“勒索软件保护策略”页面的“受保护的工作负载”列中，选择行末的向下箭头。

删除勒索软件防护策略

您可以删除当前未与任何工作负载关联的保护策略。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，选择“管理保护策略”。
3. 在“管理策略”页面中，选择“操作”•••您想要删除的策略的选项。
4. 从操作菜单中，选择*删除策略*。

使用勒索软件恢复中的NetApp Data Classification扫描个人身份信息

在NetApp Ransomware Resilience中，您可以使用NetApp Data Classification来扫描和分类文件共享工作负载中的数据。对数据进行分类可以帮助您确定数据集是否包含个人身份信息 (PII)，这可能会增加安全风险。数据分类是NetApp Console的核心组件，无需额外付费即可使用。

"数据分类"利用人工智能驱动的自然语言处理进行上下文数据分析和分类，为您的数据提供可操作的见解，以满足合规性要求、检测安全漏洞、优化成本并加速迁移。

此过程可以影响工作负载的重要性，以帮助确保您获得适当的保护。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

通过数据分类识别隐私暴露

在使用勒索软件恢复功能中的数据分类之前，您需要"启用数据分类来扫描您的数据"。

您可以在勒索软件恢复的保护页面内部署数据分类。按照程序识别隐私泄露。当您选择识别暴露时，如果您尚未部署数据分类，则会出现一个对话框，让您启用数据分类。

有关数据分类的更多信息，请参阅：

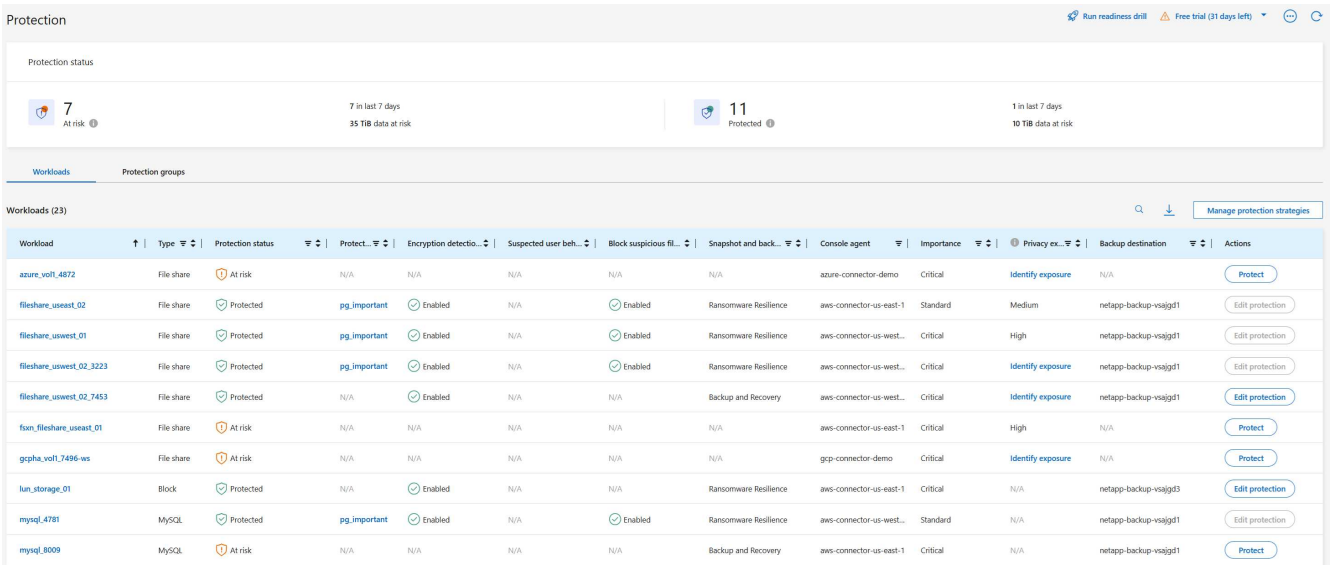
- "了解数据分类"
- "私人数据类别"
- "调查组织中存储的数据"

开始之前

如果您已"部署数据分类"。数据分类作为控制台的一部分提供，无需额外付费，并且可以在本地或客户云中部署。

步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面的“工作负载”列中找到文件共享工作负载。



3. 要启用数据分类来扫描您的数据中的 PII，请在“隐私暴露”列中选择“识别暴露”。

> 如果您尚未部署数据分类，选择“识别暴露”将打开一个对话框来部署数据分类。选择*部署*。部署数据分类后，您可以返回“保护”页面，然后选择“识别暴露”。

结果

扫描可能需要几分钟，具体取决于文件的大小和数量。在扫描过程中，保护页面指示它正在识别文件并提供文件数量。扫描完成后，“隐私暴露”列将暴露级别评定为“低”、“中”或“高”。

审查隐私暴露情况

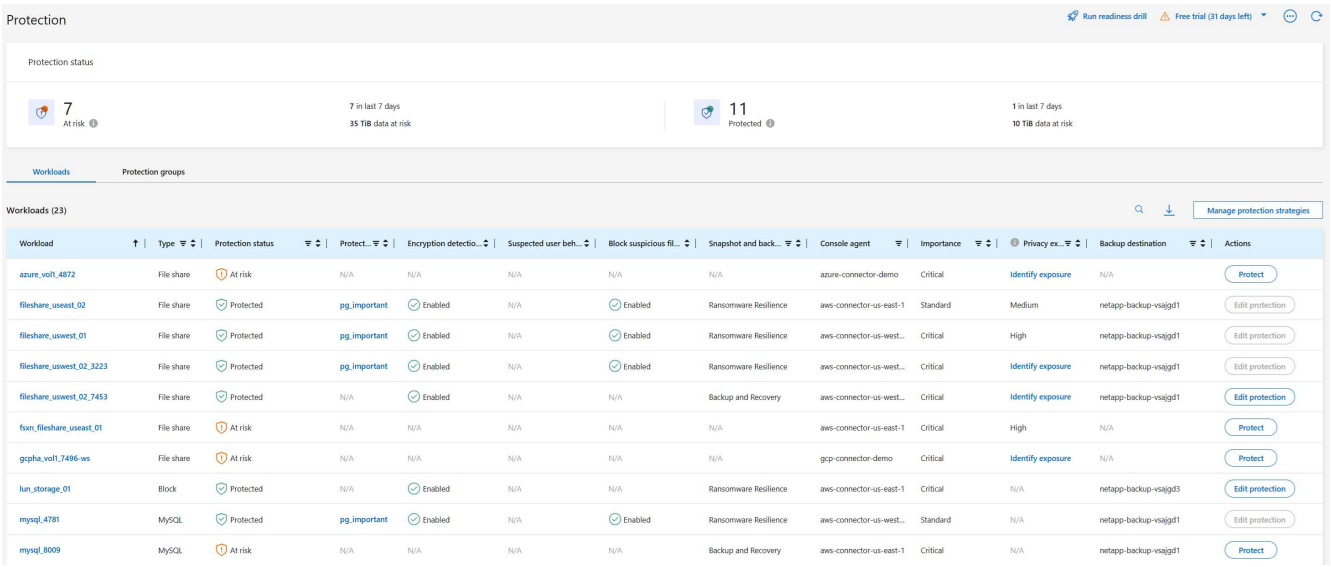
在对 PII 进行数据分类扫描后，评估风险。

PII 数据分为以下三类：

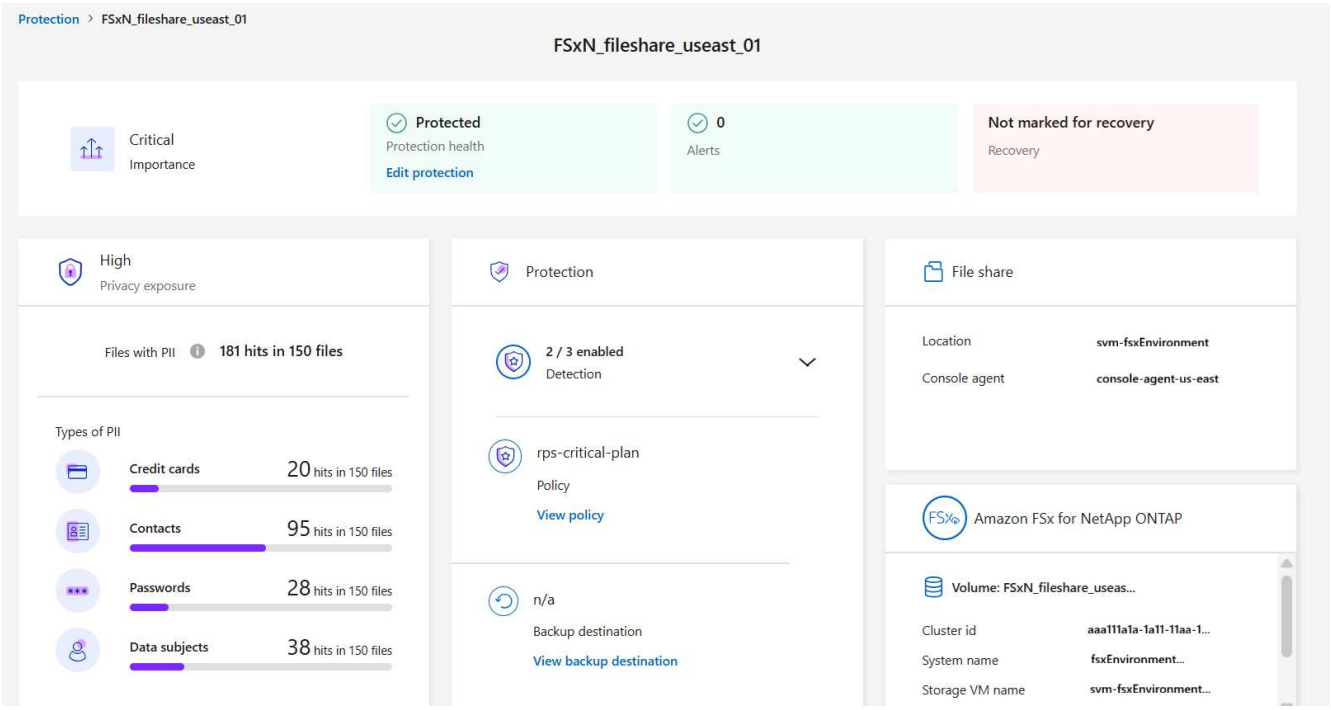
- 高：超过 70% 的文件包含 PII
- 中：超过 30% 且少于 70% 的文件包含 PII
- 低：大于 0% 且小于 30% 的文件包含 PII

步骤

1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，在“工作负载”列中找到显示“隐私暴露”列中状态的文件共享工作负载。



3. 选择“工作负载”列中的工作负载链接即可查看工作负载详情。



4. 在“工作负载详细信息”页面中，查看“隐私暴露”图块中的详细信息。

隐私暴露对工作负载重要性的影响

隐私暴露的变化可能会影响工作负载的重要性。

当隐私暴露时：	从这次隐私曝光来看：	对于此隐私暴露：	那么，工作量重要性会这样做：。
减少	高、中或低	中、低或无	保持不变

当隐私暴露时：	从这次隐私曝光来看：	对于此隐私暴露：	那么，工作量重要性会这样做：。
增加	无	低	保持标准
	低	中	从标准到重要的变化
	低或中	高	从标准或重要变为关键

了解更多信息

有关数据分类的详细信息，请参阅数据分类文档：

- "了解数据分类"
- "私人数据类别"
- "调查组织中存储的数据"

使用NetApp Ransomware Resilience处理检测到的勒索软件警报

当NetApp Ransomware Resilience检测到可能的攻击时，它会在仪表板和通知区域显示警报。勒索软件恢复能力会立即拍摄快照。查看勒索软件恢复能力*警报*选项卡中的潜在风险。

如果勒索软件恢复功能检测到可能的攻击，控制台通知设置中会出现通知，并且电子邮件会发送到配置的地址。电子邮件包含有关严重性、受影响的工作负载的信息，以及勒索软件恢复力*警报*选项卡中警报的链接。

您可以忽略误报或决定立即恢复数据。

如果您关闭警报，勒索软件恢复功能会了解此行为，将其与正常操作关联，并且不会再次对其发出警报。

要开始恢复数据，请将警报标记为准备好恢复，以便存储管理员可以开始恢复过程。

每个警报可能包含不同数量和状态的多个事件。审查所有事件。

勒索软件恢复能力提供了有关导致发出警报的原因的信息（称为“证据”），例如：

- 文件扩展名已创建或更改
- 创建文件并比较检测率与预期率
- 文件删除，并比较检测率与预期率
- 当加密程度较高时，无需更改文件扩展名

警报分为以下类型之一：

- 潜在攻击：当自主勒索软件防护检测到新的扩展并且在过去 24 小时内重复发生 20 次以上时（默认行为），

就会发出警报。

- 警告：基于以下行为会出现警告：
  - 之前没有发现过新的扩展，并且相同行为没有重复足够多次以将其声明为攻击。
  - 观察到高熵。
  - 文件读取、写入、重命名或删除活动比正常水平增加了一倍。

对于 SAN 环境，警告仅基于高熵。

证据基于ONTAP中的自主勒索软件防护信息。有关详细信息，请参阅 "自主勒索软件防护概述"。

警报可以具有以下状态之一：

- 新的
- 不活跃

警报事件可以具有以下状态之一：

- 新：所有事件在首次发现时均标记为“新”。
- 已解除：如果您怀疑该活动不是勒索软件攻击，您可以将状态更改为“已解除”。

在您驳回攻击后，您无法将其改回。如果您解除工作负载，则为应对潜在勒索软件攻击而自动获取的所有快照副本都将被永久删除。

- 正在驳回：该事件正在被驳回。
- 已解决：该事件已修复。
- 自动解决：对于低优先级警报，如果五天内未采取任何措施，则事件将自动解决。

如果您在“设置”页面的“勒索软件恢复”中配置了安全和事件管理系统 (SIEM)，则“勒索软件恢复”会向您的 SIEM 系统发送警报详细信息。

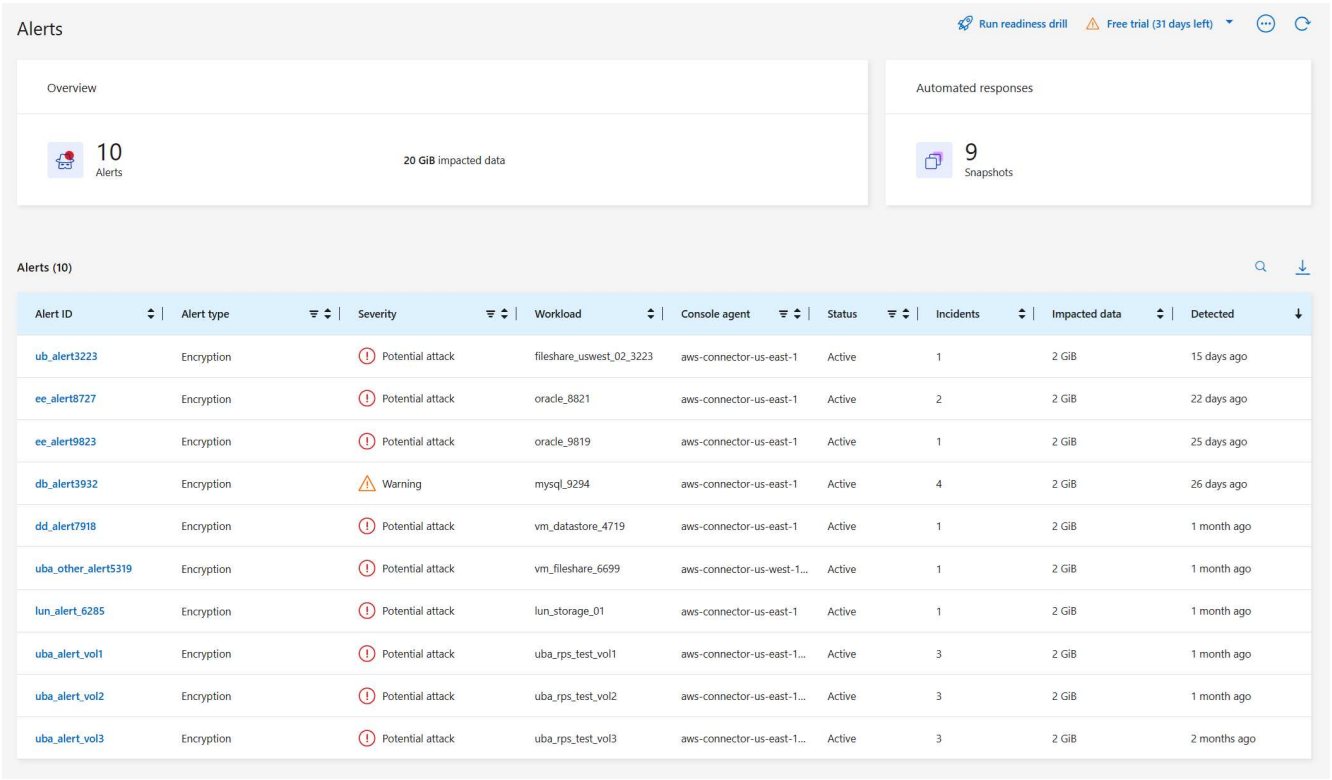
查看警报

您可以从勒索软件恢复仪表板或“警报”选项卡访问警报。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员、勒索软件恢复管理员或勒索软件恢复查看器角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

1. 在勒索软件恢复力仪表板中，查看警报窗格。
2. 选择其中一个状态下的“查看全部”。
3. 选择一个警报来查看每个警报的每个卷上的所有事件。
4. 要查看其他警报，请选择左上角面包屑中的“警报”。
5. 查看警报页面上的警报。



6. 继续执行以下操作之一：
   - [检测恶意活动和异常用户行为] 。
   - [将勒索软件事件标记为准备恢复（事件被消除后）] 。
   - [忽略不属于潜在攻击的事件] 。

回复警报电子邮件

当勒索软件弹性检测到潜在攻击时，它会根据订阅用户的订阅通知偏好向其发送电子邮件通知。电子邮件包含有关警报的信息，包括严重程度和受影响的资源。

您可以接收勒索软件恢复警报的电子邮件通知。此功能可帮助您随时了解警报、警报的严重程度以及受影响的资源。

要订阅电子邮件通知，请参阅 "设置电子邮件通知设置"。

1. 在勒索软件恢复中，转到*设置*页面。
2. 在“通知”下，找到电子邮件通知设置。
3. 输入您想要接收警报的电子邮件地址。
4. 保存更改。

当生成新警报时，您将收到电子邮件通知。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员、勒索软件恢复管理员或勒索软件恢复查看器角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

1. 查看电子邮件。
2. 在电子邮件中，选择“查看警报”并登录“勒索软件恢复”。

   出现“警报”页面。

3. 审查每个卷上每个警报的所有事件。
4. 要查看其他警报，请单击左上角面包屑中的“警报”。
5. 继续执行以下操作之一：
   - [检测恶意活动和异常用户行为] 。
   - [将勒索软件事件标记为准备恢复（事件被消除后）] 。
   - [忽略不属于潜在攻击的事件] 。

检测恶意活动和异常用户行为

查看“警报”选项卡，您可以识别是否存在恶意活动或异常用户行为。

您必须配置用户活动代理并启用具有用户行为检测的保护策略才能查看用户级警报。启用用户行为检测后，*可疑用户*列会出现在警报仪表板中；未启用用户行为检测时则不会显示。要启用可疑用户检测，请参阅"可疑的用户活动"。

> 如果您正在使用NetAppData Infrastructure Insights(DII) 工作负载安全，建议您使用相同的工作负载安全代理来实现勒索软件恢复。您不需要为勒索软件恢复能力部署单独的工作负载安全代理，但是，使用相同的工作负载安全代理需要勒索软件恢复能力控制台组织和 DII 存储工作负载安全租户之间建立配对关系。请联系您的客户代表以启用此配对。

查看恶意活动

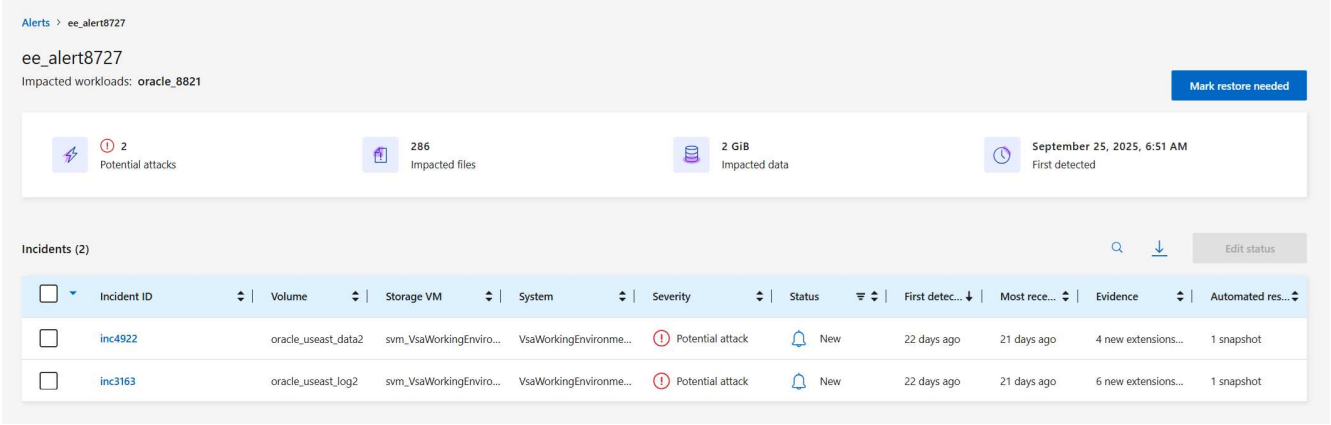
当自主勒索软件防护在勒索软件恢复中触发警报时，您可以查看以下详细信息：

- 输入数据的熵
- 预期的新文件创建率与检测到的速率的比较
- 预期文件删除率与检测率的比较
- 文件的预期重命名率与检测到的重命名率的比较
- 受影响的文件和目录

> 这些详细信息对于 NAS 工作负载是可见的。对于 SAN 环境，只有熵数据可用。

步骤

1. 从勒索软件恢复菜单中，选择*警报*。
2. 选择一个警报。
3. 查看警报中的事件。



4. 选择一个事件来查看该事件的详细信息。

查看异常用户行为

如果您已配置可疑用户检测来查看异常用户行为，则可以查看用户级数据并阻止特定用户。要启用可疑用户设置，请参阅"配置勒索软件抵御能力设置"。

步骤

1. 从勒索软件恢复菜单中，选择*警报*。
2. 选择一个警报。
3. 查看警报中的事件。
4. 要阻止您环境中的可疑用户，请选择该用户名下的“阻止”。

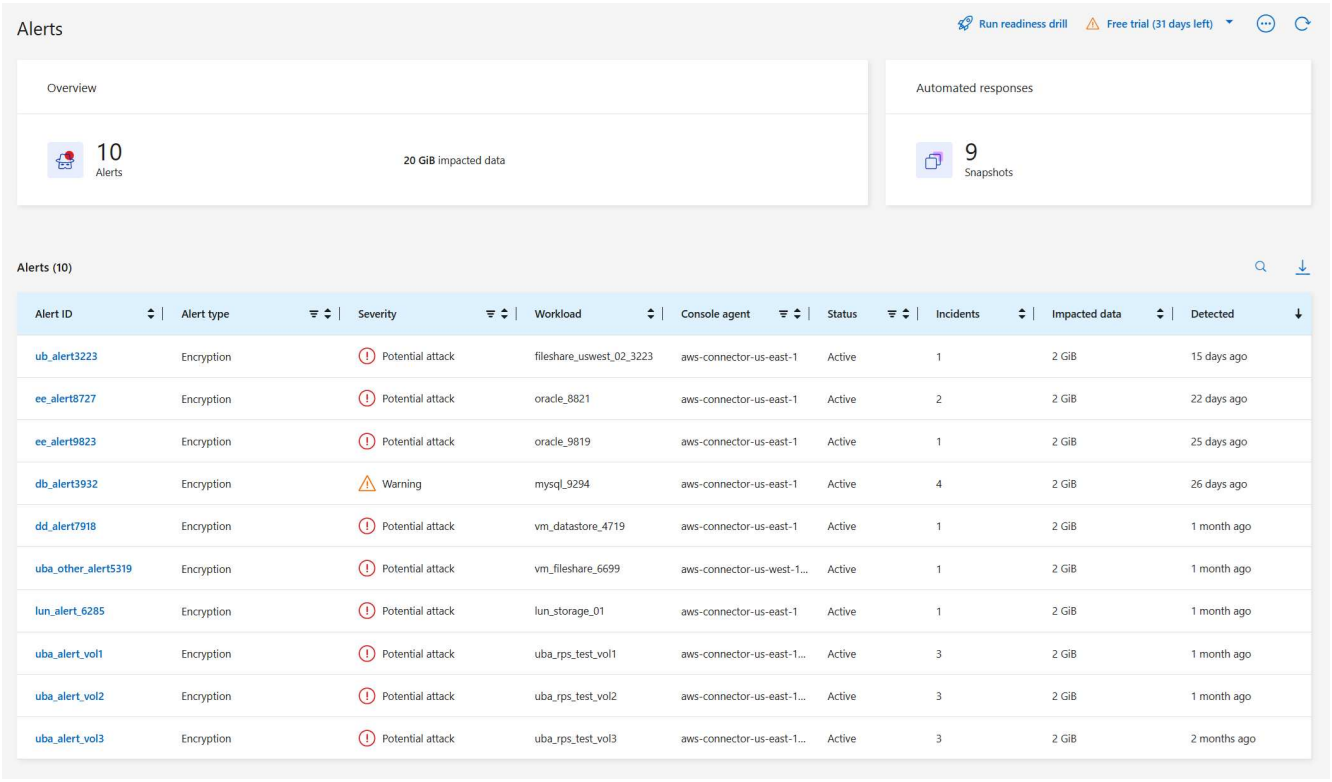
将勒索软件事件标记为准备恢复（事件被消除后）

阻止攻击后，通知存储管理员数据已准备就绪，以便他们可以开始恢复。

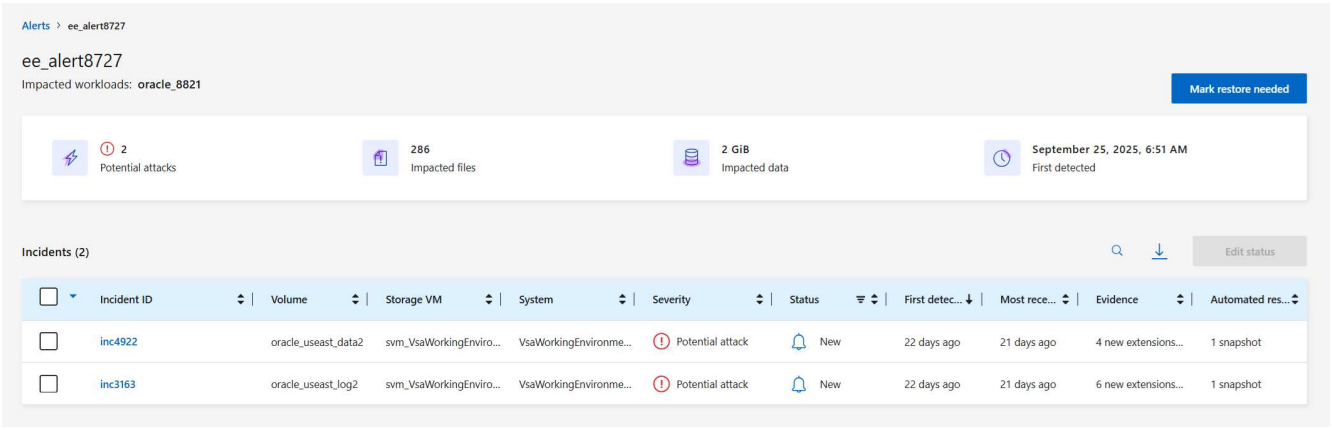
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

1. 从勒索软件恢复菜单中，选择*警报*。



2. 在警报页面中，选择警报。
3. 查看警报中的事件。



4. 如果您确定事件已准备好恢复，请选择*标记需要恢复*。
5. 确认操作并选择*标记需要恢复*。
6. 要启动工作负载恢复，请在消息中选择“恢复*工作负载”或选择“*恢复”选项卡。

结果

将警报标记为恢复后，警报将从“警报”选项卡移至“恢复”选项卡。

忽略不属于潜在攻击的事件

审查事件后，您需要确定该事件是否是潜在的攻击。如果它们不是真正的威胁，则可以将其驳回。

您可以忽略误报或决定立即恢复数据。如果您忽略警报，勒索软件恢复功能会了解此行为，将其与正常操作关联

，并且不会再次针对此类行为发出警报。

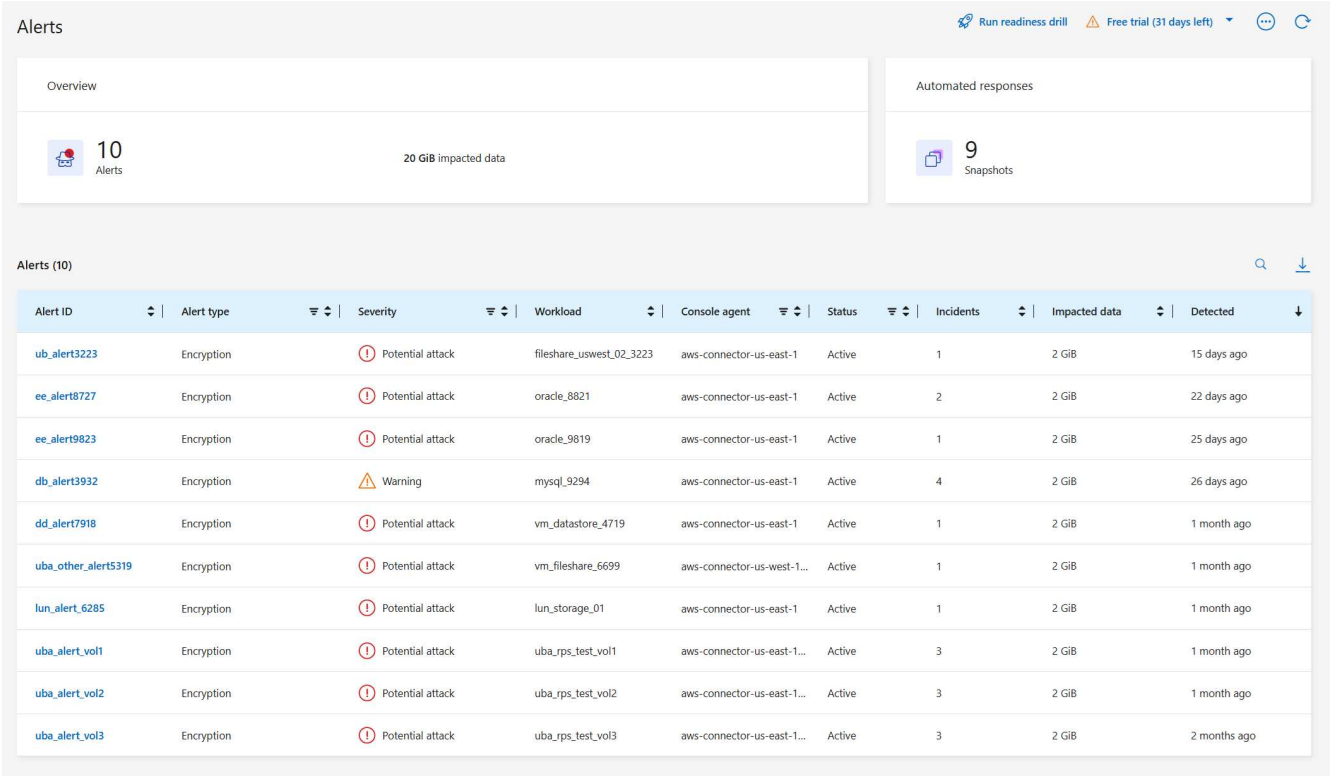
如果您解除工作负载，则为应对潜在勒索软件攻击而自动获取的所有快照副本都将被永久删除。

如果您关闭警报，则无法更改其状态或撤消此更改。

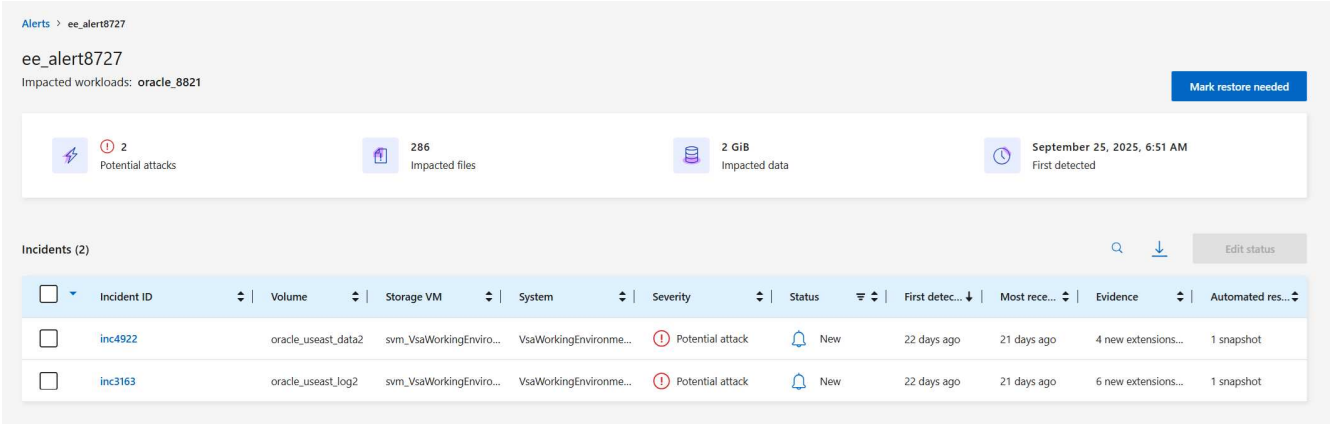
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

1. 从勒索软件恢复菜单中，选择*警报*。

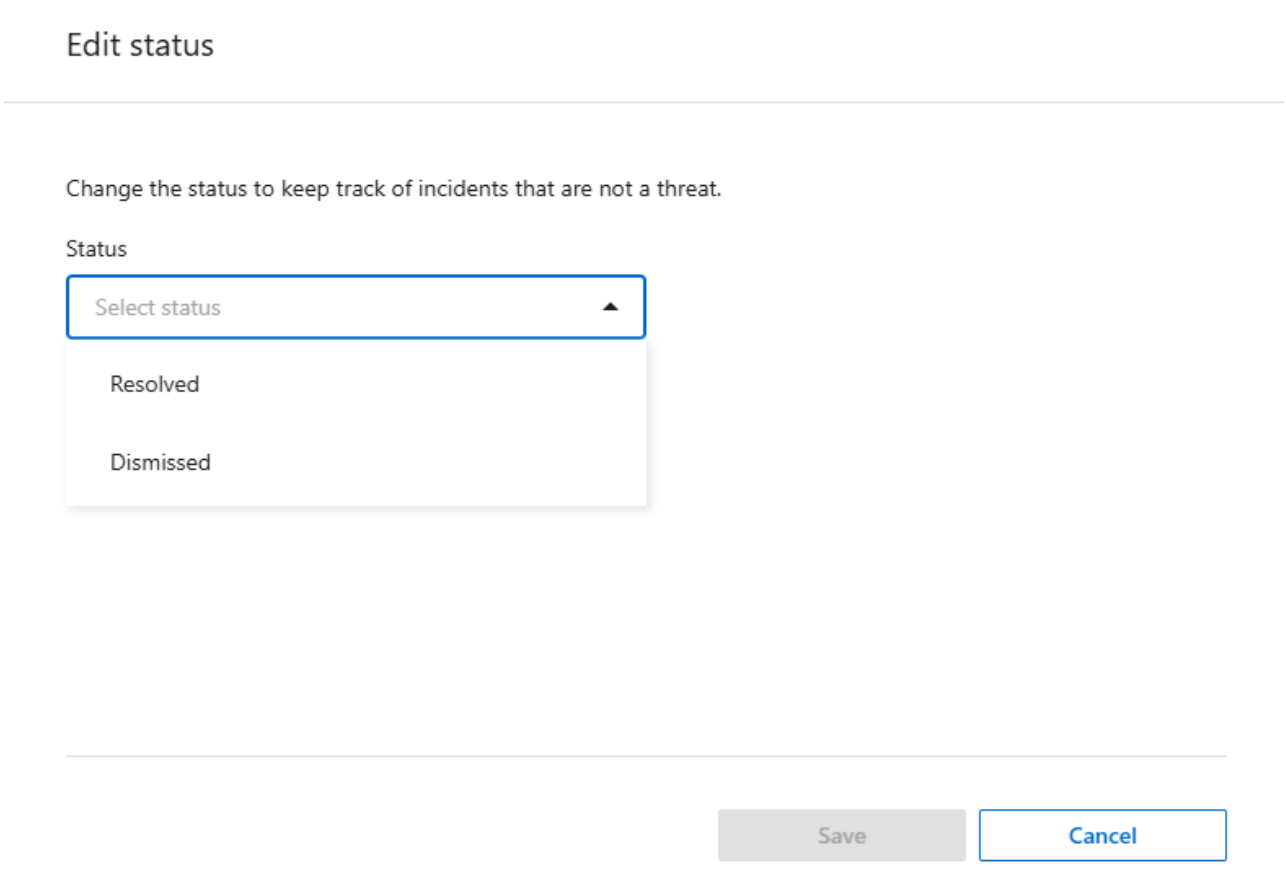


2. 在警报页面中，选择警报。



3. 选择一个或多个事件。或者，通过选择表格左上角的事件 ID 框来选择所有事件。

4. 如果您确定该事件不构成威胁，请将其视为误报：
   - 选择事件。
   - 选择表格上方的*编辑状态*按钮。



5. 从编辑状态框中，选择“已解除”状态。

   将显示有关工作负载和已删除快照副本的其他信息。

6. 选择*保存*。

   一个或多个事件的状态变为“已解除”。

查看受影响文件的列表

在文件级别恢复应用程序工作负载之前，您可以查看受影响文件的列表。您可以访问警报页面下载受影响文件的列表。然后使用恢复页面上传列表并选择要恢复的文件。

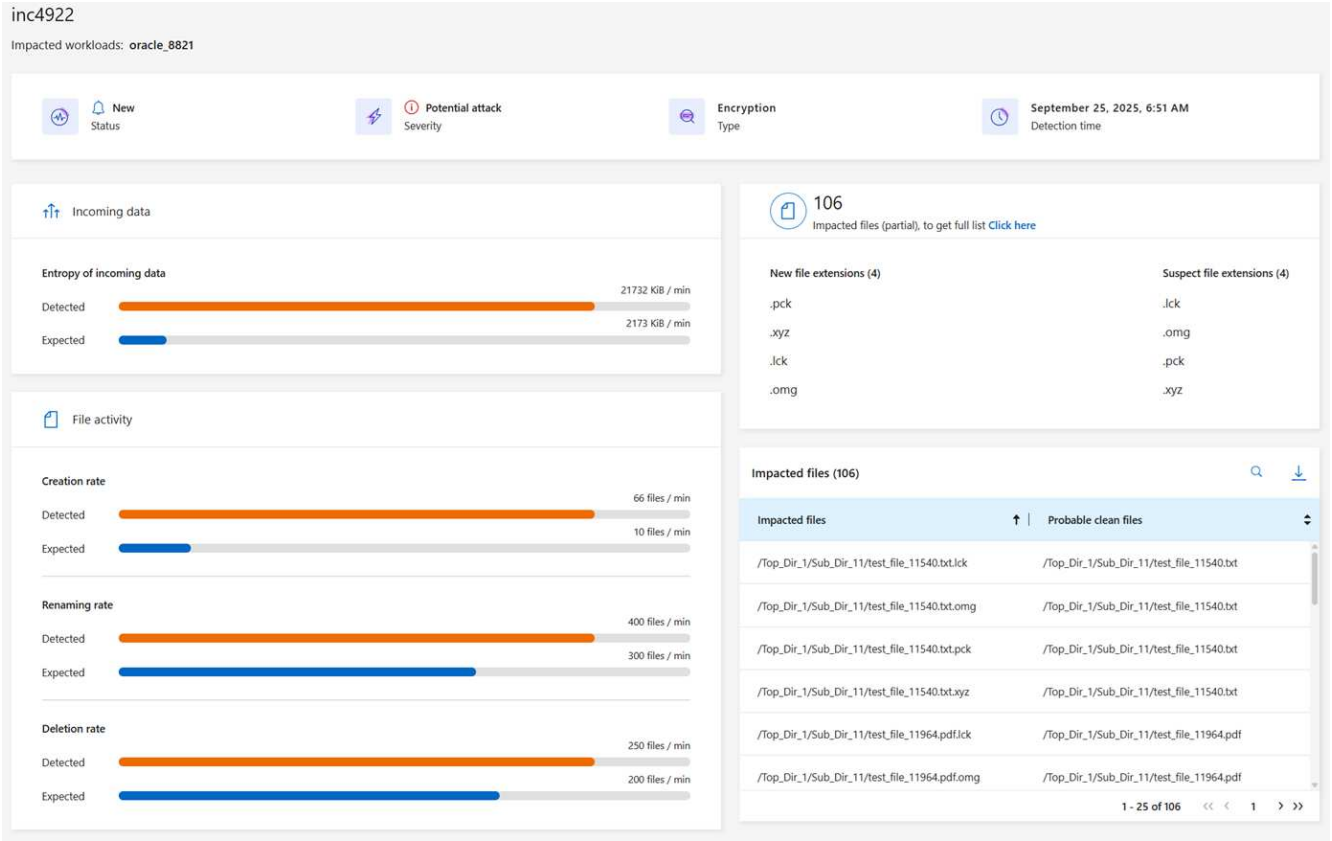
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

使用“警报”页面检索受影响文件的列表。

如果某个卷有多个警报，您可能需要下载每个警报的受影响文件的 CSV 列表。

1. 从勒索软件恢复菜单中，选择*警报*。
2. 在“警报”页面上，按工作负载对结果进行排序，以显示要恢复的应用程序工作负载的警报。
3. 从该工作负载的警报列表中选择一个警报。
4. 对于该警报，选择一个事件。



5. 对于该事件，选择下载图标以 CSV 格式下载受影响文件的列表。

借助NetApp Ransomware Resilience，在勒索软件攻击发生后恢复

在工作负载被标记为“需要恢复”后， NetApp Ransomware Resilience会建议实际恢复点 (RPA) 并协调工作流程以实现抗崩溃恢复。

- 如果应用程序或虚拟机由SnapCenter管理，则勒索软件恢复功能会使用应用程序一致或虚拟机一致的流程将应用程序或虚拟机恢复到其先前的状态和最后的事务。应用程序或 VM 一致性恢复将任何未存储的数据（例如缓存或 I/O 操作中的数据）添加到卷中的数据中。
- 如果应用程序或虚拟机不是由SnapCenter管理，而是由NetApp Backup and Recovery或 Ransomware Resilience 管理，则 Ransomware Resilience 会执行崩溃一致性恢复，其中会恢复同一时间点卷中的所有数据（例如，如果系统崩溃）。

  您可以通过选择所有卷、特定卷或特定文件来恢复工作负载。

工作负载恢复可能会影响正在运行的工作负载。您应该与适当的利益相关者协调恢复过程。

工作负载可以具有以下还原状态之一：

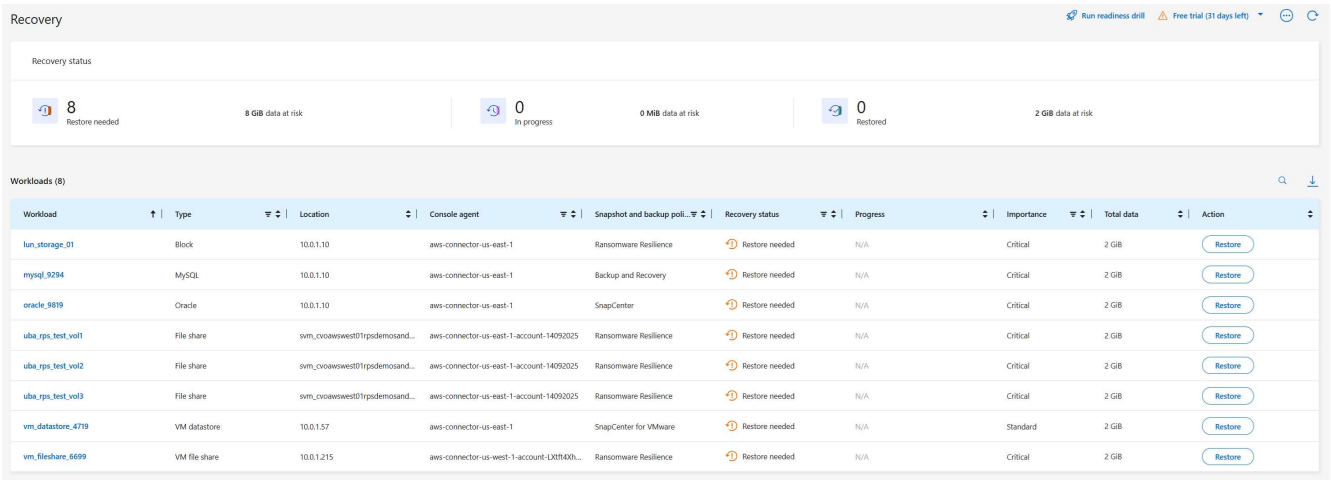
- 需要恢复：需要恢复工作负载。
- 进行中：恢复操作目前正在进行中。
- 已恢复：工作量已恢复。
- 失败：工作负载恢复过程无法完成。

查看已准备好恢复的工作负载

查看处于“需要恢复”恢复状态的工作负载。

步骤

1. 执行以下操作之一：
   - 在仪表板中，查看警报窗格中的“需要恢复”总数，然后选择*查看全部*。
   - 从菜单中选择*恢复*。
2. 查看“恢复”页面中的工作负载信息。



还原由SnapCenter管理的工作负载

使用勒索软件恢复能力，存储管理员可以确定如何从推荐的还原点或首选的还原点最佳地恢复工作负载。

如果需要恢复，应用程序状态将会改变。如果备份中包含控制文件，应用程序将从控制文件恢复到其先前的状态。恢复完成后，应用程序将以读写模式打开。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

1. 从勒索软件恢复中，选择*恢复*。
2. 查看“恢复”页面中的工作负载信息。

3. 选择处于“需要恢复”状态的工作负载。
4. 要恢复，请选择*恢复*。
5. 恢复范围：应用程序一致（或者对于虚拟机的SnapCenter ，恢复范围为“按虚拟机”）
6. 来源：选择来源旁边的向下箭头查看详细信息。选择要用于还原数据的还原点。

勒索软件恢复能力将最佳还原点识别为事件发生前的最新备份，并显示“推荐”指示。

7. 目的地：选择目的地旁边的向下箭头查看详细信息。
   a. 选择原始位置或备用位置。
   b. 选择系统。
   c. 选择存储虚拟机。
8. 如果原始目标没有足够的空间来恢复工作负载，则会出现“临时存储”行。您可以选择临时存储来恢复工作负载数据。恢复的数据将从临时存储复制到原始位置。单击临时存储行中的*向下箭头*并设置目标集群、存储虚拟机和本地层。
9. 选择*保存*。
10. 选择“下一步”。
11. 检查您的选择。
12. 选择*恢复*。
13. 从顶部菜单中，选择“恢复”以查看“恢复”页面上的工作负载，其中操作的状态会在各个状态之间移动。

还原不受SnapCenter管理的工作负载

使用勒索软件恢复能力，存储管理员可以确定如何从推荐的还原点或首选的还原点最佳地恢复工作负载。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

安全存储管理员可以恢复不同级别的数据：

- 恢复所有卷
- 在卷级别或文件和文件夹级别恢复应用程序。
- 在卷级别、目录或文件/文件夹级别恢复文件共享。
- 从虚拟机级别的数据存储中恢复。

该过程根据工作负载类型而有所不同。

步骤

1. 从勒索软件恢复菜单中，选择*恢复*。
2. 查看“恢复”页面中的工作负载信息。
3. 选择处于“需要恢复”状态的工作负载。
4. 要恢复，请选择*恢复*。

5. 恢复范围：选择您想要完成的恢复类型：
   - 所有卷
   - 按体积
   - 按文件：您可以指定要还原的文件夹或单个文件。

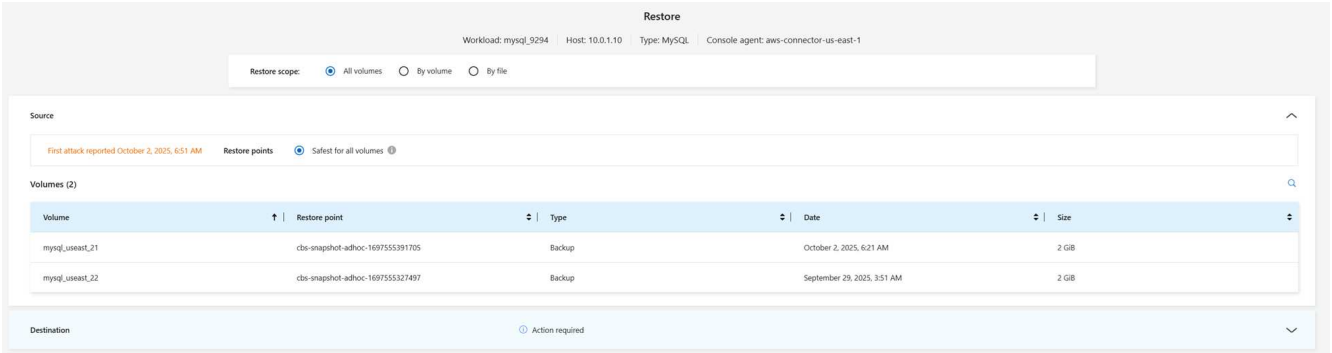
   对于 SAN 工作负载，您只能按工作负载进行恢复。

   您最多可以选择 100 个文件或一个文件夹。

6. 根据您选择的是应用程序、卷还是文件，继续执行以下步骤之一。

恢复所有卷

1. 从勒索软件恢复菜单中，选择*恢复*。
2. 选择处于“需要恢复”状态的工作负载。
3. 要恢复，请选择*恢复*。
4. 在“还原”页面的“还原范围”中，选择“所有卷”。



5. 来源：选择来源旁边的向下箭头查看详细信息。
   a. 选择要用于还原数据的还原点。

   勒索软件恢复能力将最佳还原点识别为事件发生前的最新备份，并显示“对所有卷最安全”的指示。这意味着所有卷都将恢复到检测到的第一个卷受到第一次攻击之前的副本。

6. 目的地：选择目的地旁边的向下箭头查看详细信息。
   a. 选择系统。
   b. 选择存储虚拟机。
   c. 选择聚合。
   d. 更改将添加到所有新卷的卷前缀。

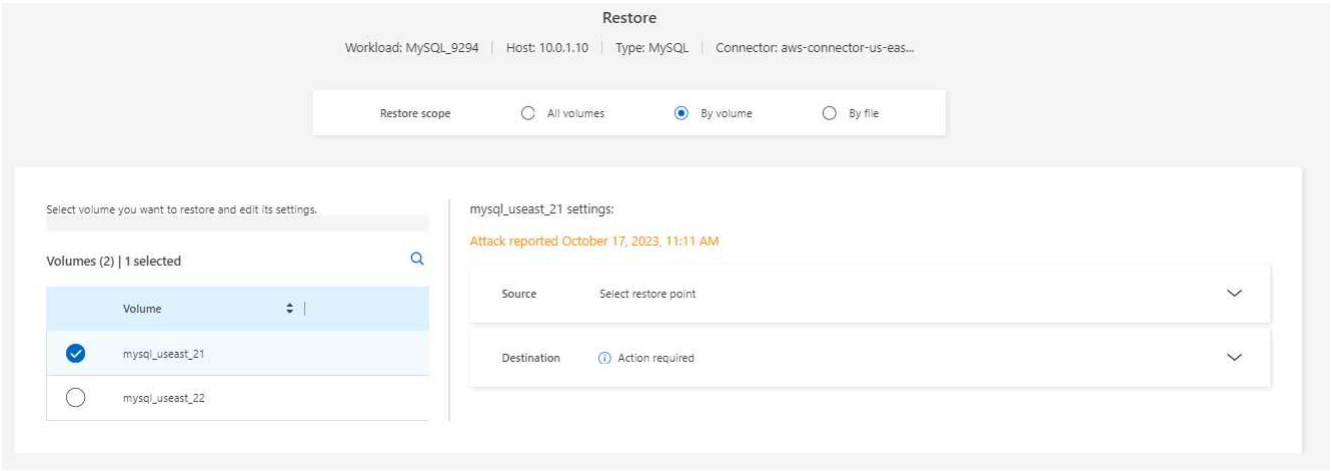
   新卷名称显示为前缀+原始卷名称+备份名称+备份日期。

7. 选择*保存*。

8. 选择“下一步”。
9. 检查您的选择。
10. 选择*恢复*。
11. 从顶部菜单中，选择“恢复”以查看“恢复”页面上的工作负载，其中操作的状态会在各个状态之间移动。

在卷级别恢复应用程序工作负载

1. 从勒索软件恢复菜单中，选择*恢复*。
2. 选择处于“需要恢复”状态的应用程序工作负载。
3. 要恢复，请选择*恢复*。
4. 在“还原”页面的“还原范围”中，选择“按卷”。



5. 在卷列表中，选择要还原的卷。
6. 来源：选择来源旁边的向下箭头查看详细信息。
   a. 选择要用于还原数据的还原点。

   勒索软件恢复能力将最佳还原点识别为事件发生前的最新备份，并显示“推荐”指示。

7. 目的地：选择目的地旁边的向下箭头查看详细信息。
   a. 选择系统。
   b. 选择存储虚拟机。
   c. 选择聚合。
   d. 查看新的卷名称。

   新的卷名称显示为原始卷名称+备份名称+备份日期。

8. 选择*保存*。
9. 选择“下一步”。
10. 检查您的选择。

11. 选择*恢复*。
12. 从顶部菜单中，选择“恢复”以查看“恢复”页面上的工作负载，其中操作的状态会在各个状态之间移动。

在文件级别恢复应用程序工作负载

在文件级别恢复应用程序工作负载之前，您可以查看受影响文件的列表。您可以访问警报页面下载受影响文件的列表。然后使用恢复页面上传列表并选择要恢复的文件。

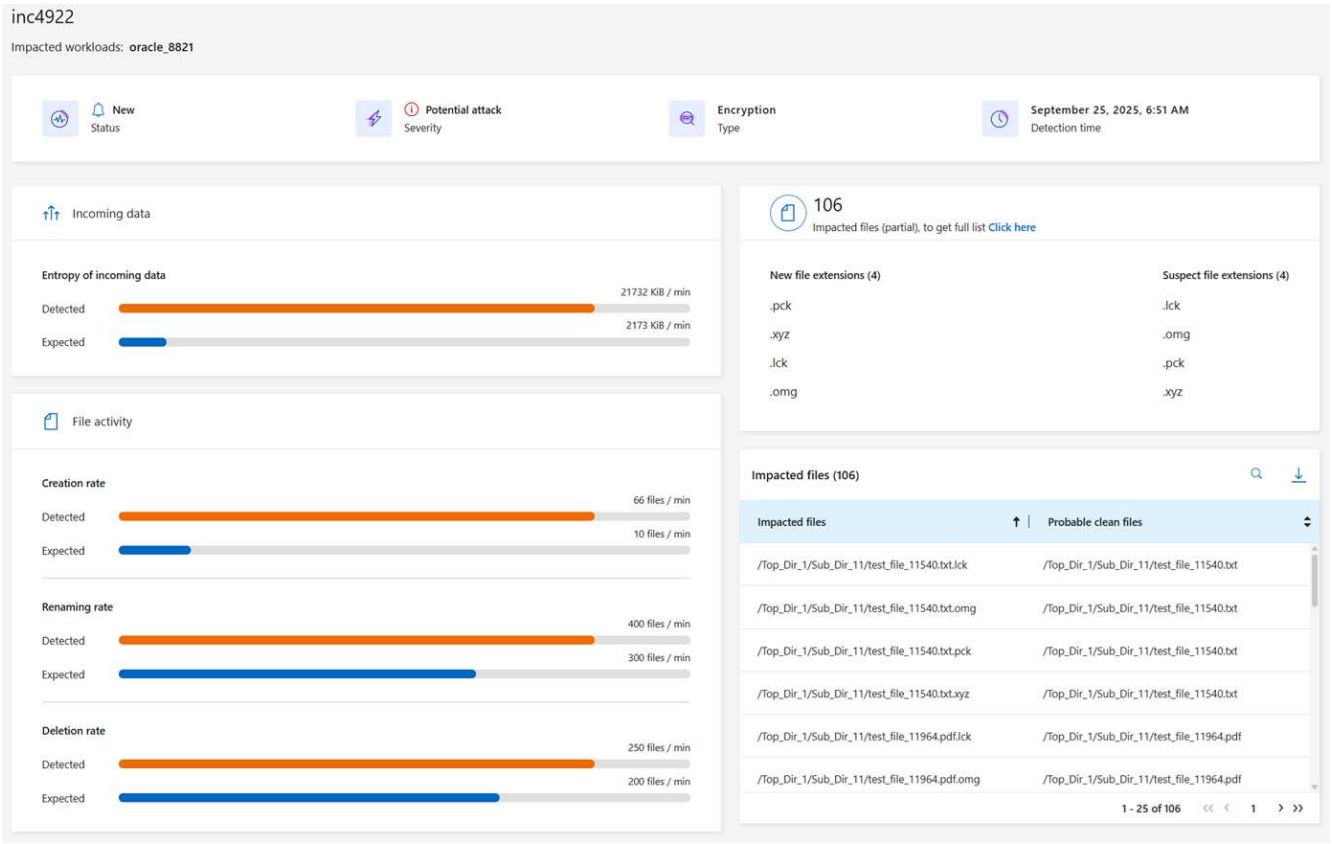
您可以将文件级别的应用程序工作负载还原到相同或不同的系统。

获取受影响文件列表的步骤

使用“警报”页面检索受影响文件的列表。

如果某个卷有多个警报，您将需要下载每个警报的受影响文件的 CSV 列表。

1. 从勒索软件恢复菜单中，选择*警报*。
2. 在“警报”页面上，按工作负载对结果进行排序，以显示要恢复的应用程序工作负载的警报。
3. 从该工作负载的警报列表中选择一个警报。
4. 对于该警报，选择一个事件。



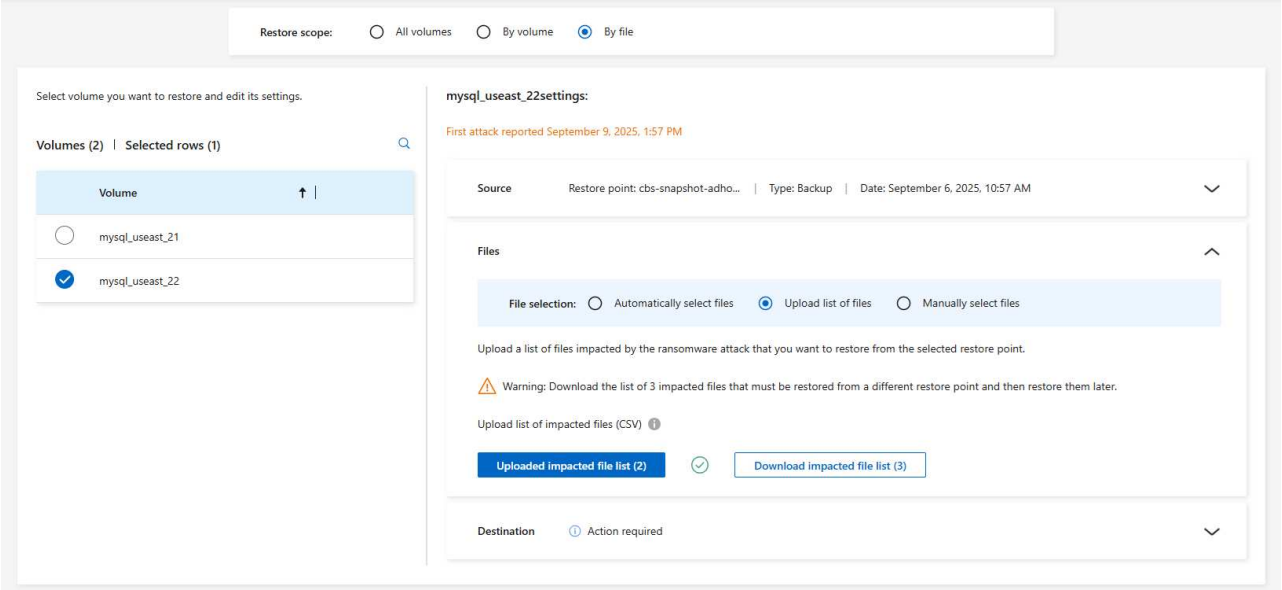
5. 要查看完整的文件列表，请选择“受影响的文件”窗格顶部的“单击此处”。
6. 对于该事件，选择下载图标并以 CSV 格式下载受影响文件的列表。

恢复这些文件的步骤

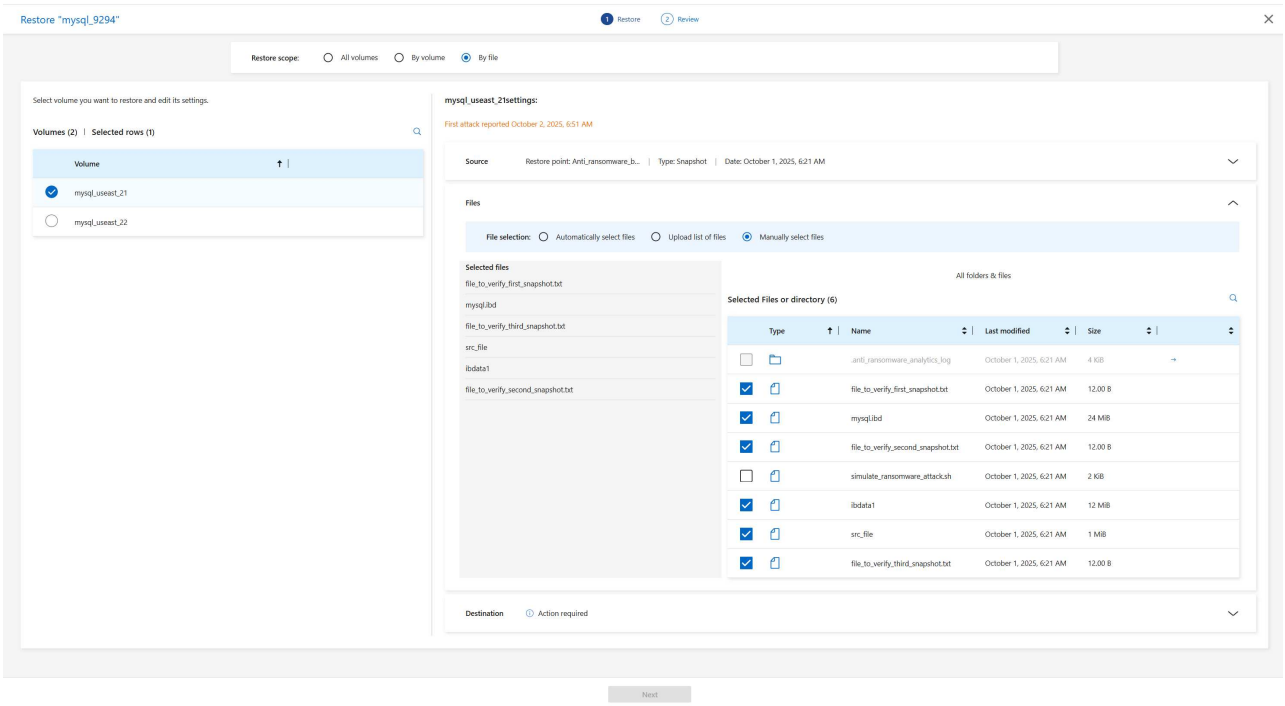
1. 从勒索软件恢复菜单中，选择*恢复*。
2. 选择处于“需要恢复”状态的应用程序工作负载。
3. 要恢复，请选择*恢复*。
4. 在“还原”页面的“还原范围”中，选择“按文件”。
5. 在卷列表中，选择包含要还原的文件的卷。
6. 还原点：选择*还原点*旁边的向下箭头查看详细信息。选择要用于还原数据的还原点。

   还原点窗格中的“原因”列显示快照或备份的原因为“计划”或“对勒索软件事件的自动响应”。

7. 文件：
   - 自动选择文件：让勒索软件恢复功能选择要恢复的文件。
   - 上传文件列表：上传一个 CSV 文件，其中包含您从警报页面获取的或您拥有的受影响文件的列表。您一次最多可以恢复 10,000 个文件。



   - 手动选择文件：选择最多 10,000 个文件或单个文件夹进行恢复。



如果无法使用所选还原点还原任何文件，则会出现一条消息，指示无法还原的文件数量，并允许您通过选择“下载受影响文件的列表”来下载这些文件的列表。

8. 目的地：选择目的地旁边的向下箭头查看详细信息。
   a. 选择恢复数据的位置：原始源位置或您可以指定的备用位置。

      虽然原始文件或目录将被恢复的数据覆盖，但原始文件和文件夹名称将保持不变，除非您指定新名称。

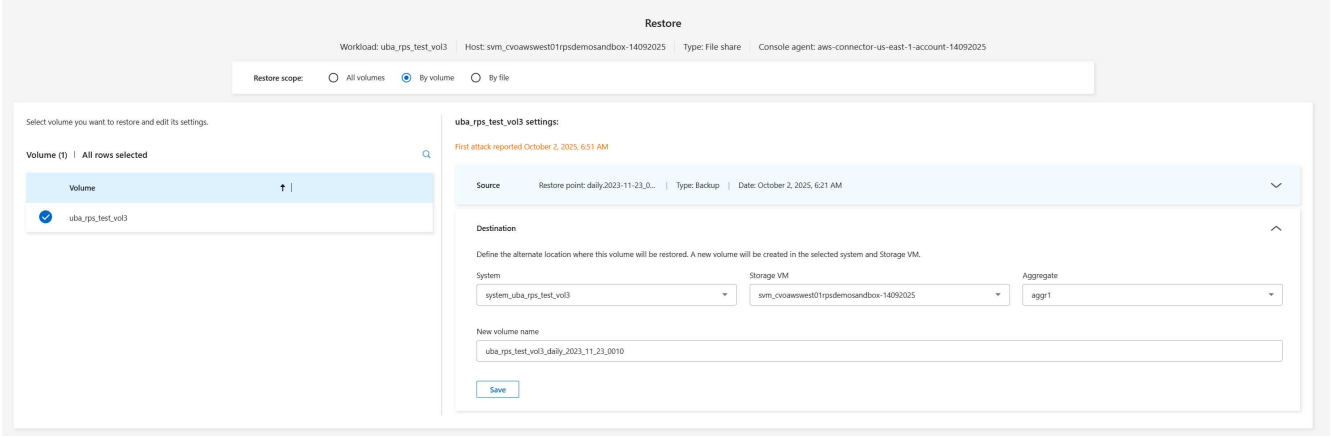
   b. 选择系统。
   c. 选择存储虚拟机。
   d. （可选）输入路径。

      如果您没有指定还原路径，文件将被还原到顶级目录的新卷。

   e. 选择是否希望恢复的文件或目录的名称与当前位置的名称相同或不同。
9. 选择“下一步”。
10. 检查您的选择。
11. 选择*恢复*。
12. 从顶部菜单中，选择“恢复”以查看“恢复”页面上的工作负载，其中操作的状态会在各个状态之间移动。

恢复文件共享或数据存储

1. 选择要还原的文件共享或数据存储后，在“还原”页面的“还原范围”中，选择“按卷”。



2. 在卷列表中，选择要还原的卷。
3. 来源：选择来源旁边的向下箭头查看详细信息。
   a. 选择要用于还原数据的还原点。

   勒索软件恢复能力将最佳还原点识别为事件发生前的最新备份，并显示“推荐”指示。

4. 目的地：选择目的地旁边的向下箭头查看详细信息。
   a. 选择恢复数据的位置：原始源位置或您可以指定的备用位置。

   虽然原始文件或目录将被恢复的数据覆盖，但原始文件和文件夹名称将保持不变，除非您指定新名称。

   b. 选择系统。
   c. 选择存储虚拟机。
   d. （可选）输入路径。

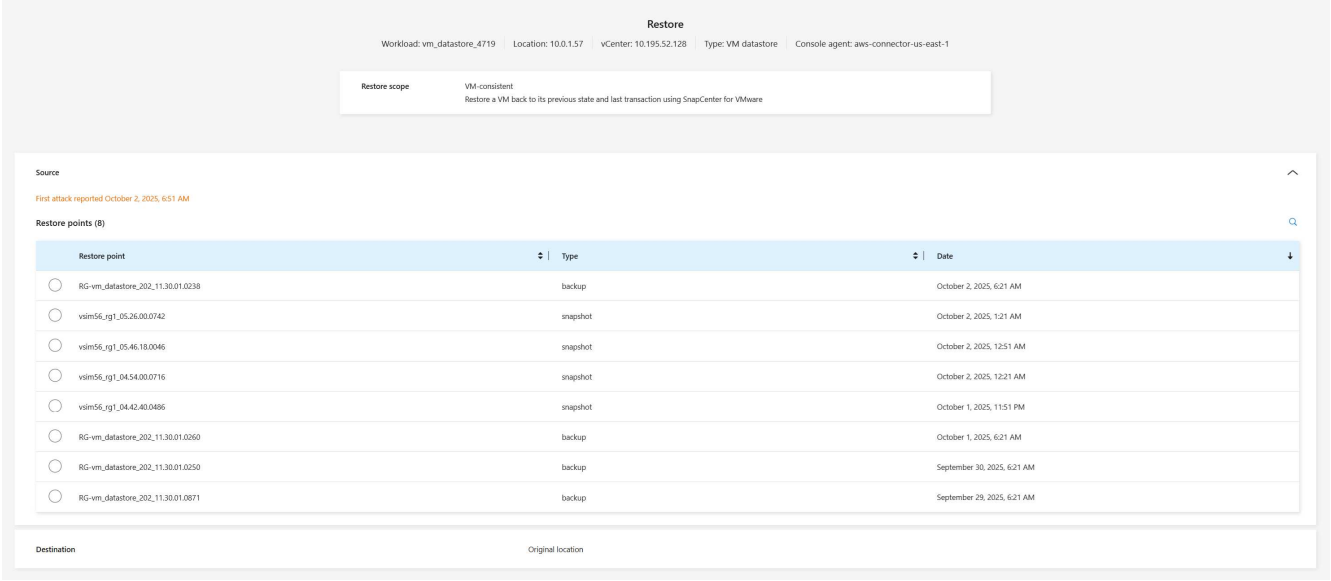
   如果您没有指定还原路径，文件将被还原到顶级目录的新卷。

5. 选择*保存*。
6. 检查您的选择。
7. 选择*恢复*。
8. 从菜单中，选择“恢复”以查看“恢复”页面上的工作负载，其中操作的状态在各个状态之间移动。

在 **VM** 级别还原 **VM** 文件共享

在选择要还原的虚拟机后，在“恢复”页面上继续执行以下步骤。

1. 来源：选择来源旁边的向下箭头查看详细信息。



2. 选择要用于还原数据的还原点。
3. 目的地：返回原始位置。
4. 选择“下一步”。
5. 检查您的选择。
6. 选择*恢复*。
7. 从菜单中，选择“恢复”以查看“恢复”页面上的工作负载，其中操作的状态在各个状态之间移动。

在NetApp Ransomware Resilience中下载报告

您可以导出保护数据并下载显示攻击准备演习、保护、警报和恢复的详细信息的 CSV 或 JSON 文件。

在下载文件之前，您应该刷新数据，这也会刷新文件中出现的数据。

所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员、勒索软件恢复管理员或勒索软件恢复查看器角色。"了解NetApp Console的勒索软件恢复角色" 。

*您可以下载哪些数据？*您可以从任何主菜单选项下载文件：

- 保护：包含所有工作负载的状态和详细信息，包括受保护和处于危险中的工作负载总数。
- 警报：包括所有警报的状态和详细信息，包括警报总数和自动快照。
- 恢复：包括所有需要恢复的工作负载的状态和详细信息，包括标记为“需要恢复”、“进行中”、“恢复失败”和“恢复成功”的工作负载总数。
- 报告：您可以从任何页面导出数据并下载文件。

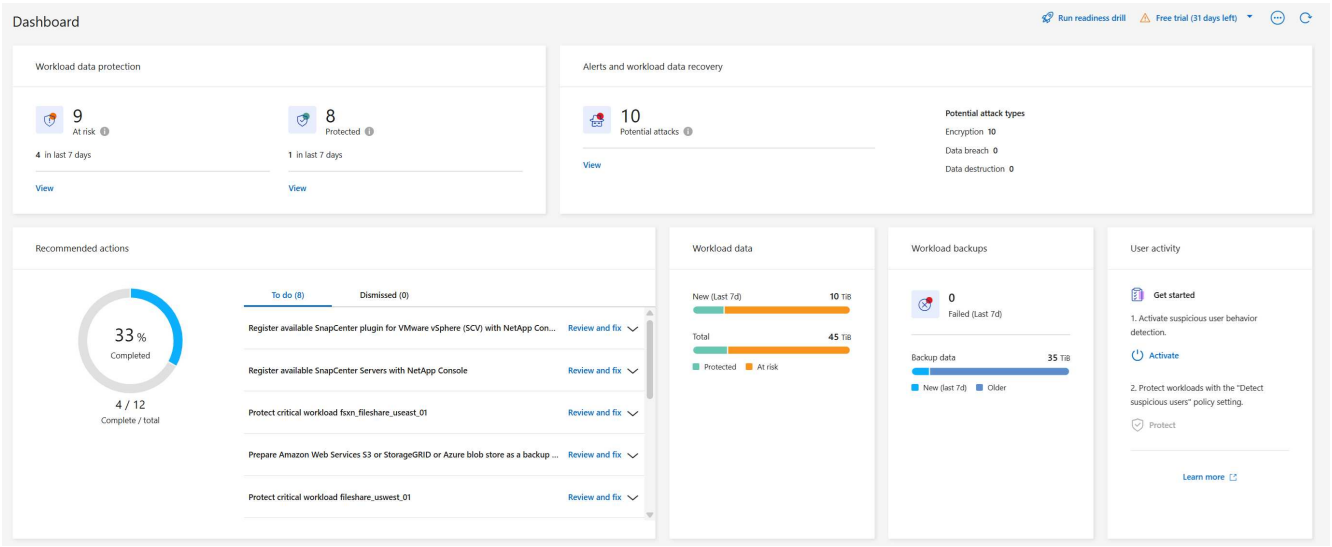
您只能从*报告*页面下载准备情况演习报告。

如果您从保护、警报或恢复页面下载 CSV 或 JSON 文件，则数据仅显示该页面上的数据。

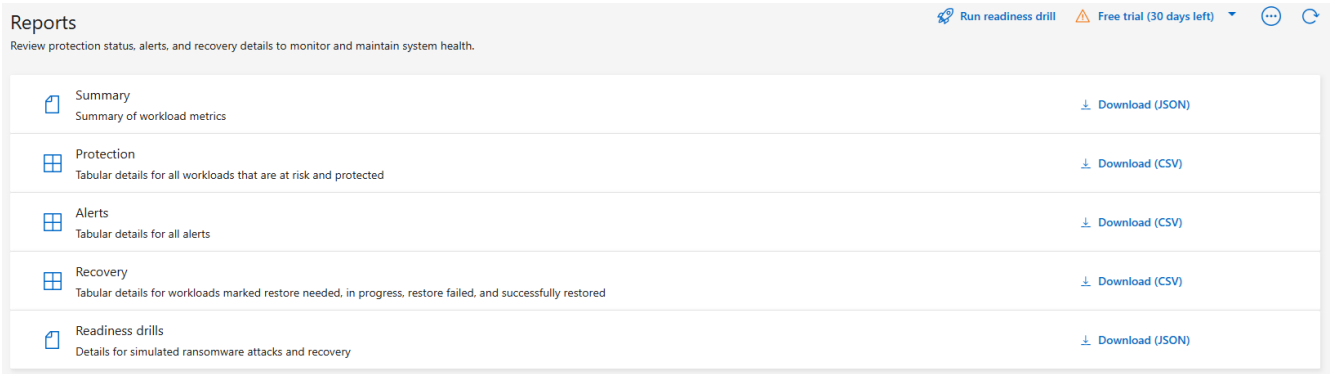
CSV 或 JSON 文件包含所有控制台系统上所有工作负载的数据。

步骤

1. 从控制台左侧导航中，选择*保护*>*勒索软件恢复*。



2. 从仪表板或其他页面，选择*刷新*右上角的选项可刷新报告中显示的数据。
3. 执行以下操作之一：
   - 从页面上选择*下载*选项。
   - 从NetApp Ransomware Resilience菜单中，选择 报告。
4. 如果您选择了“报告”选项，请选择一个预配置的文件名并选择“下载”。



知识和支持

注册以获得支持

需要注册支持才能获得针对BlueXP及其存储解决方案和服务的技术支持。还需要支持注册才能启用Cloud Volumes ONTAP系统的关键工作流程。

注册支持并不能使NetApp获得云提供商文件服务的支持。有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品的BlueXP文档中的“获取帮助”。

- "适用于ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

支持注册概述

激活支持权利的注册方式有两种：

- 注册您的BlueXP帐户序列号（您的 20 位 960xxxxxxxx 序列号位于BlueXP中的支持资源页面上）。

  这是您在BlueXP内任何服务的单一支持订阅 ID。每个BlueXP帐户级支持订阅都必须注册。

- 在您的云提供商市场中注册与订阅相关的Cloud Volumes ONTAP序列号（这些是 20 位 909201xxxxxxxx 序列号）。

  这些序列号通常被称为_PAYGO 序列号_，由BlueXP在Cloud Volumes ONTAP部署时生成。

注册两种类型的序列号可以实现开立支持票和自动生成案例等功能。按照如下所述，通过将NetApp支持站点 (NSS) 帐户添加到BlueXP来完成注册。

注册**BlueXP**以获得**NetApp**支持

要注册支持并激活支持权利，您的BlueXP组织（或帐户）中的一名用户必须将NetApp支持站点帐户与其BlueXP登录名关联。如何注册NetApp支持取决于您是否已经拥有NetApp支持站点 (NSS) 帐户。

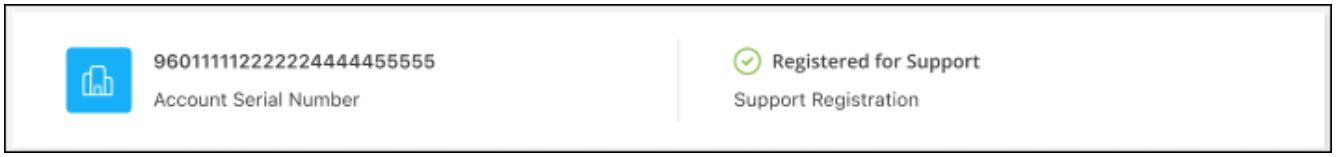
拥有 **NSS** 帐户的现有客户

如果您是拥有 NSS 帐户的NetApp客户，则只需通过BlueXP注册即可获得支持。

步骤

1. 在BlueXP控制台的右上角，选择“设置”图标，然后选择“凭据”。
2. 选择*用户凭证*。
3. 选择*添加 NSS 凭据*并按照NetApp支持站点 (NSS) 身份验证提示进行操作。
4. 要确认注册过程是否成功，请选择“帮助”图标，然后选择“支持”。

   *资源*页面应显示您的BlueXP组织已注册以获得支持。



请注意，如果其他BlueXP用户尚未将NetApp支持站点帐户与其BlueXP登录名关联，他们将看不到相同的支持注册状态。但是，这并不意味着您的BlueXP组织没有注册支持。只要组织中的一名用户遵循了这些步骤，那么您的组织就已注册。

现有客户但没有 **NSS** 账户

如果您是现有的NetApp客户，拥有现有许可证和序列号但没有 NSS 帐户，则需要创建一个 NSS 帐户并将其与您的BlueXP登录关联。

步骤

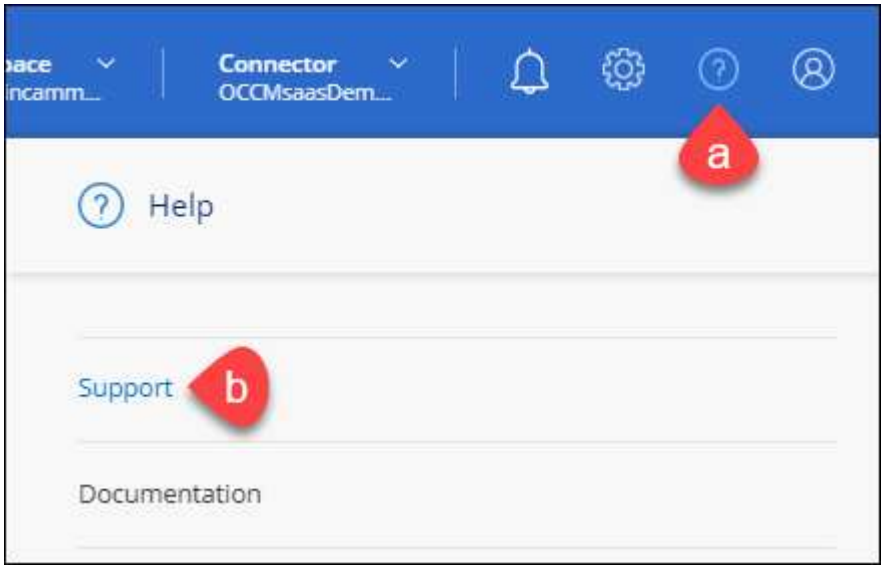
1. 通过完成以下操作创建NetApp支持站点帐户 "NetApp支持站点用户注册表"
   a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的BlueXP帐户序列号 (960xxxx)。这将加快账户处理速度。
2. 完成以下步骤，将您的新 NSS 帐户与您的BlueXP登录名关联拥有 NSS 帐户的现有客户。

NetApp全新产品

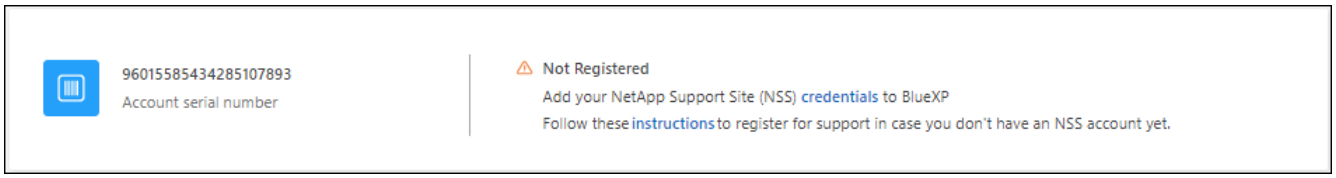
如果您是NetApp新用户并且没有 NSS 帐户，请按照以下步骤操作。

步骤

1. 在BlueXP控制台的右上角，选择“帮助”图标，然后选择“支持”。



2. 从支持注册页面找到您的帐户 ID 序列号。



3. 导航至 "NetApp 的支持注册网站"并选择*我不是注册的NetApp客户*。
4. 填写必填字段（带有红色星号的字段）。
5. 在*产品线*字段中，选择*云管理器*，然后选择适用的计费提供商。
6. 从上面的步骤 2 复制您的帐户序列号，完成安全检查，然后确认您已阅读 NetApp 的全球数据隐私政策。

   一封电子邮件会立即发送到提供的邮箱以完成此安全交易。如果几分钟内没有收到验证电子邮件，请务必检查您的垃圾邮件文件夹。

7. 从电子邮件中确认操作。

   确认向NetApp提交您的请求并建议您创建NetApp支持站点帐户。

8. 通过完成以下操作创建NetApp支持站点帐户 "NetApp支持站点用户注册表"
   a. 请务必选择适当的用户级别，通常为* NetApp客户/最终用户*。
   b. 请务必复制上面用于序列号字段的帐户序列号（960xxxx）。这将加快处理速度。

完成后

NetApp应该在此过程中与您联系。这是针对新用户的一次性入职培训。

拥有NetApp支持站点帐户后，请按照以下步骤将该帐户与您的BlueXP登录关联拥有 NSS 帐户的现有客户。

关联 NSS 凭据以获得Cloud Volumes ONTAP支持

需要将NetApp支持站点凭据与您的BlueXP组织关联才能为Cloud Volumes ONTAP启用以下关键工作流程：

- 注册即用即付Cloud Volumes ONTAP系统以获得支持

  需要提供您的 NSS 帐户才能激活对您的系统的支持并获得对NetApp技术支持资源的访问权限。

- 自带许可证 (BYOL) 时部署Cloud Volumes ONTAP

  需要提供您的 NSS 帐户，以便BlueXP可以上传您的许可证密钥并启用您购买的期限的订阅。这包括期限续订的自动更新。

- 将Cloud Volumes ONTAP软件升级到最新版本

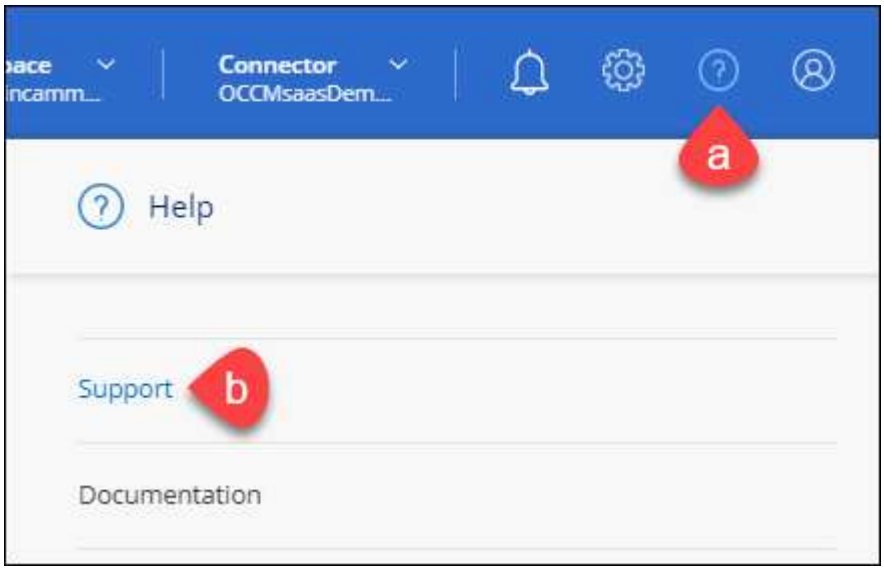
将 NSS 凭证与您的BlueXP组织关联与与BlueXP用户登录关联的 NSS 帐户不同。

这些 NSS 凭证与您的特定BlueXP组织 ID 相关联。属于BlueXP组织的用户可以从 支持 **> NSS** 管理 访问这些凭据。

- 如果您有客户级帐户，则可以添加一个或多个 NSS 帐户。
- 如果您有合作伙伴或经销商帐户，则可以添加一个或多个 NSS 帐户，但不能与客户级帐户一起添加。

步骤

1. 在BlueXP控制台的右上角，选择“帮助”图标，然后选择“支持”。



2. 选择*NSS 管理 > 添加 NSS 帐户*。
3. 当出现提示时，选择“继续”以重定向到 Microsoft 登录页面。

   NetApp使用 Microsoft Entra ID 作为特定于支持和许可的身份验证服务的身份提供者。

4. 在登录页面，提供您的NetApp支持站点注册的电子邮件地址和密码以执行身份验证过程。

   这些操作使BlueXP能够使用您的 NSS 帐户进行许可证下载、软件升级验证和未来支持注册等操作。

   请注意以下事项：

   - NSS 帐户必须是客户级帐户（不是访客或临时帐户）。您可以拥有多个客户级 NSS 帐户。
   - 如果该帐户是合作伙伴级别帐户，则只能有一个 NSS 帐户。如果您尝试添加客户级 NSS 帐户并且合作伙伴级帐户已存在，您将收到以下错误消息：

     “此帐户不允许使用 NSS 客户类型，因为已经存在不同类型的 NSS 用户。”

   如果您已有客户级 NSS 帐户并尝试添加合作伙伴级帐户，情况也是如此。

   - 成功登录后， NetApp将存储 NSS 用户名。

     这是系统生成的映射到您的电子邮件的 ID。在*NSS 管理*页面上，您可以显示来自 ••• 菜单。

   - 如果您需要刷新登录凭证令牌，还有一个*更新凭证*选项 ••• 菜单。

     使用此选项会提示您再次登录。请注意，这些帐户的令牌将在 90 天后过期。我们将发布通知来提醒您此事。

获取帮助

NetApp以多种方式为BlueXP及其云服务提供支持。我们提供全天候 (24/7) 的大量免费自助支持选项，例如知识库 (KB) 文章和社区论坛。您的支持注册包含通过网络工单获取的远程技术支持。

获取云提供商文件服务的支持

有关云提供商文件服务、其基础设施或使用该服务的任何解决方案的技术支持，请参阅该产品的BlueXP文档中的“获取帮助”。

- "适用于ONTAP 的Amazon FSx"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

要获得针对BlueXP及其存储解决方案和服务的技术支持，请使用下面描述的支持选项。

使用自助选项

这些选项每周 7 天、每天 24 小时免费提供：

- 文档

  您当前正在查看的BlueXP文档。

- "知识库"

  搜索BlueXP知识库以查找有助于解决问题的文章。

- "社区"

  加入BlueXP社区以关注正在进行的讨论或创建新的讨论。

向NetApp支持创建案例

除了上述自助支持选项之外，您还可以在激活支持后与NetApp支持专家合作解决任何问题。

开始之前

- 要使用“创建案例”功能，您必须首先将您的NetApp支持站点凭据与您的BlueXP登录名关联。 "了解如何管理与BlueXP登录相关的凭据" 。
- 如果您要为具有序列号的ONTAP系统打开案例，那么您的 NSS 帐户必须与该系统的序列号相关联。

步骤

1. 在BlueXP中，选择 帮助 > 支持。
2. 在“资源”页面上，选择“技术支持”下的可用选项之一：

   a. 如果您想通过电话与某人交谈，请选择“致电我们”。您将被引导至 netapp.com 上的一个页面，其中列出了您可以拨打的电话号码。

b. 选择“创建案例”向NetApp支持专家开具一张票：

- 服务：选择与问题相关的服务。例如， BlueXP专门针对服务中的工作流程或功能的技术支持问题。
- 工作环境：如果适用于存储，请选择* Cloud Volumes ONTAP* 或 **On-Prem**，然后选择相关的工作环境。

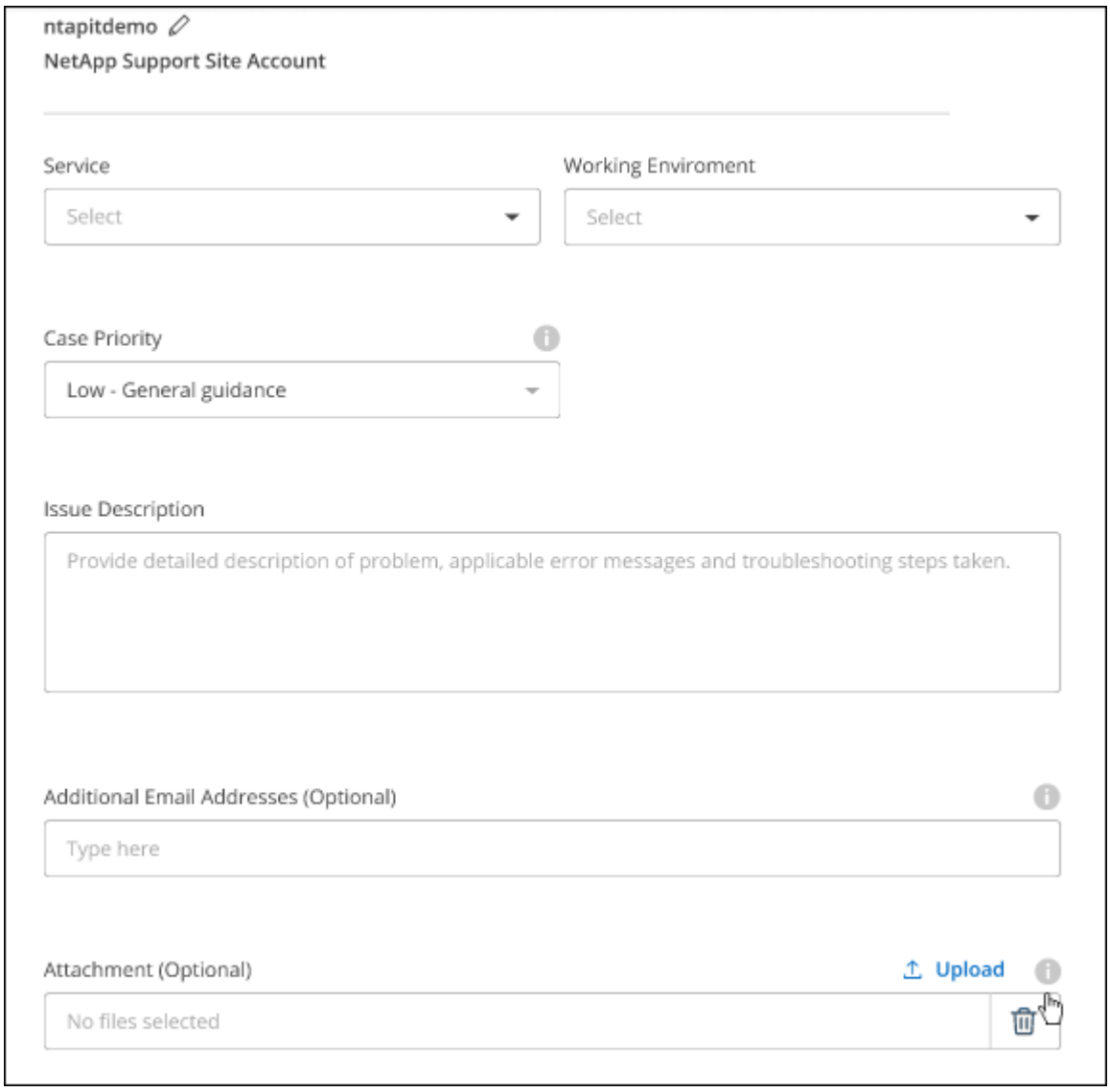
  工作环境列表在您在服务顶部横幅中选择的BlueXP组织（或帐户）、项目（或工作区）和连接器的范围内。

- 案例优先级：选择案例的优先级，可以是低、中、高或严重。

  要了解有关这些优先事项的更多详细信息，请将鼠标悬停在字段名称旁边的信息图标上。

- 问题描述：提供问题的详细描述，包括任何适用的错误消息或您执行的故障排除步骤。
- 其他电子邮件地址：如果您想让其他人知道此问题，请输入其他电子邮件地址。
- 附件（可选）：一次最多上传五个附件。

  每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成后

将会出现一个弹出窗口，其中显示您的支持案例编号。NetApp支持专家将审查您的案例并尽快回复您。

要查看支持案例的历史记录，您可以选择*设置>时间线*并查找名为“创建支持案例”的操作。最右边的按钮可让您展开操作以查看详细信息。

尝试创建案例时，您可能会遇到以下错误消息：

“您无权针对所选服务创建案例”

此错误可能意味着 NSS 帐户及其关联的记录公司与BlueXP帐户序列号的记录公司不是同一家（即。960xxxx）或工作环境序列号。您可以使用以下选项之一寻求帮助：

- 使用产品内聊天
- 提交非技术案例 https://mysupport.netapp.com/site/help

管理您的支持案例（预览）

您可以直接从BlueXP查看和管理活动和已解决的支持案例。您可以管理与您的 NSS 帐户和公司相关的案例。

案例管理目前可作为预览版使用。我们计划在即将发布的版本中完善这种体验并增加增强功能。请使用产品内聊天向我们发送反馈。

请注意以下事项：

- 页面顶部的案例管理仪表板提供两种视图：
  - 左侧视图显示了您提供的用户 NSS 帐户在过去 3 个月内打开的案件总数。
  - 右侧的视图根据您的用户 NSS 帐户显示了过去 3 个月内贵公司级别开设的案件总数。

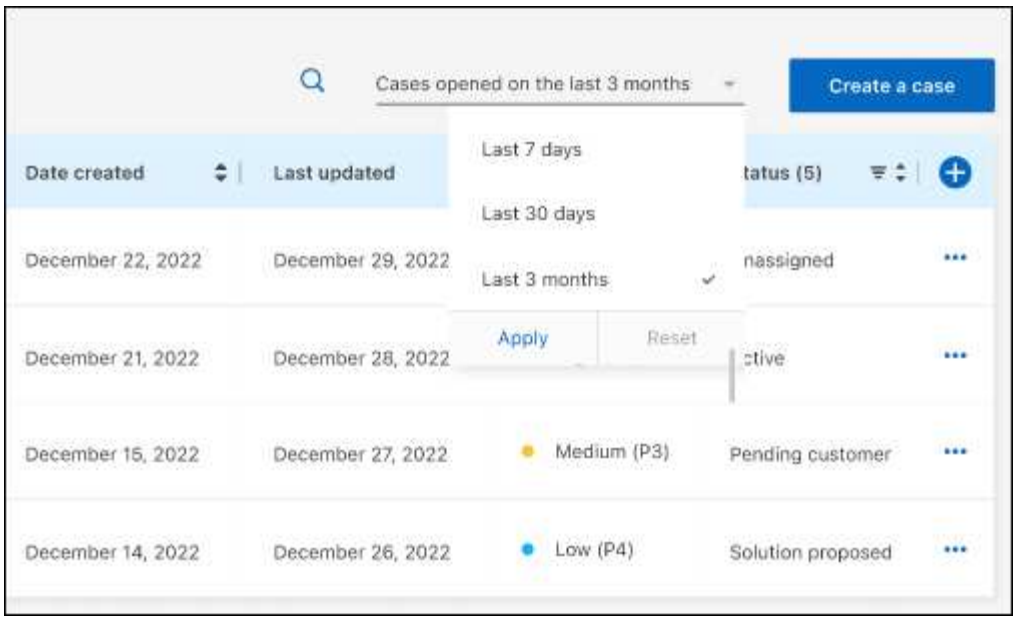
  表中的结果反映了与您选择的视图相关的案例。
- 您可以添加或删除感兴趣的列，并且可以过滤优先级和状态等列的内容。其他列仅提供排序功能。

  请查看以下步骤以了解更多详细信息。
- 在每个案件级别，我们提供更新案件记录或关闭尚未关闭或待关闭状态的案件的功能。

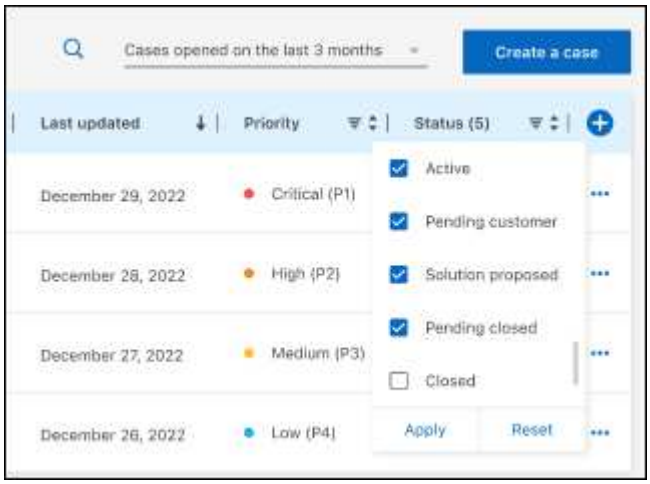
步骤

1. 在BlueXP中，选择 帮助 **>** 支持。
2. 选择*案例管理*，如果出现提示，请将您的 NSS 帐户添加到BlueXP。

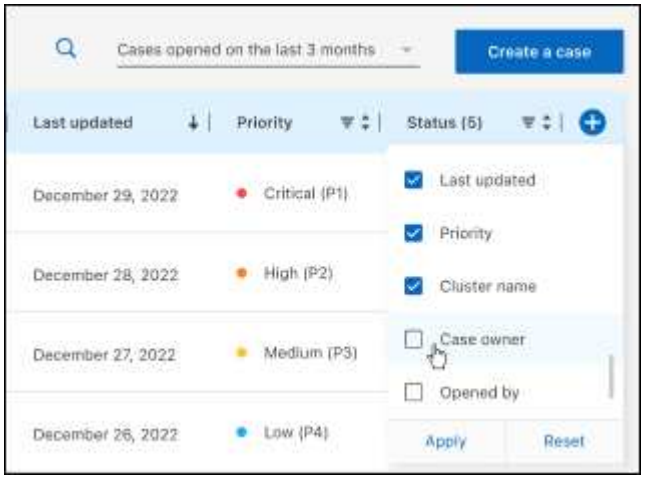
   案例管理*页面显示与您的**BlueXP**用户帐户关联的 **NSS** 帐户相关的未结案例。这与出现在 ***NSS** 管理 页面顶部的 NSS 帐户相同。
3. （可选）修改表中显示的信息：
   - 在“组织的案例”下，选择“查看”以查看与您的公司相关的所有案例。
   - 通过选择精确的日期范围或选择不同的时间范围来修改日期范围。



◦ 过滤列的内容。



◦ 通过选择⊕然后选择您想要显示的列。

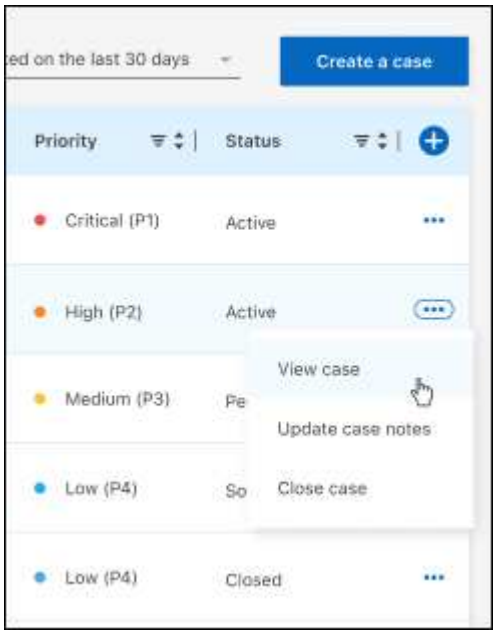


4. 通过选择管理现有案例•••并选择其中一个可用选项：

- 查看案例：查看有关特定案例的完整详细信息。
- 更新案例说明：提供有关您的问题的更多详细信息，或选择*上传文件*以附加最多五个文件。

  每个附件文件大小限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

- 结案：提供有关结案原因的详细信息，然后选择*结案*。



关于NetApp Ransomware Resilience的常见问题解答

如果您只是想快速找到有关NetApp Ransomware Resilience的问题的答案，那么此常见问题解答可以提供帮助。

部署

使用勒索软件恢复功能需要许可证吗?

您可以使用以下许可证类型：

- 注册即可获得 30 天免费试用。
- 通过 Amazon Web Services (AWS) Marketplace、Google Cloud Marketplace 和 Microsoft Azure Marketplace 购买NetApp Intelligent Services和勒索软件恢复的即用即付 (PAYGO) 订阅。
- 自带许可证 (BYOL)，即您从NetApp销售代表处获得的NetApp许可证文件 (NLF)。您可以使用许可证序列号在控制台的“Licenses and subscriptions”部分激活 BYOL。

如何启用勒索软件防御能力?

您可以从NetApp Console访问勒索软件恢复功能。请确保您已 "访问角色" 和 "前提条件"。如果您已成功配置控制台代理，则可以执行以下操作： "发现工作负载"。

有关详细信息，请参阅"访问勒索软件弹性"和"勒索软件抵御能力快速入门指南"。

勒索软件防护是否提供标准模式、受限模式和私有模式?

勒索软件恢复功能目前仅在标准模式下可用。

有关所有NetApp数据服务中这些模式的说明，请参阅 "NetApp Console部署模式"。

使用权

勒索软件恢复能力网址是什么?

在浏览器中输入 "https://console.netapp.com/ransomware-resilience" 访问控制台。

访问权限是如何管理的?

"了解所有服务的控制台访问角色"。勒索软件恢复能力也具备 "专用访问角色"。

哪种设备分辨率最佳?

勒索软件恢复的推荐设备分辨率为 1920x1080 或更高。

我应该使用哪个浏览器?

您可以使用任何现代网络浏览器访问NetApp Console。

互操作性

Ransomware Resilience 是否了解**NetApp ONTAP**中所做的保护设置?

是的，Ransomware Resilience 发现了在ONTAP中设置的快照计划。

勒索软件恢复功能如何与**NetApp Backup and Recovery**和**SnapCenter**交互？

勒索软件恢复功能与备份和恢复功能协同工作，以发现并设置文件共享工作负载的快照和备份策略。

勒索软件恢复能力与SnapCenter或SnapCenter for VMware 配合使用，可以发现并设置应用程序和虚拟机工作负载的快照和备份策略。

勒索软件恢复功能还可以与备份和恢复以及SnapCenter （包括 VMware 版SnapCenter ）配合使用，以执行文件和工作负载一致性恢复。

工作负载

在勒索软件防御的语境下，什么是工作负载？

工作负载是一个应用程序、一个虚拟机或一个文件共享。工作负载包括单个应用程序实例使用的所有卷。

例如，考虑部署在 ora3.host.com 上的 Oracle 数据库。 `vol1` 包含数据和 `vol2` 包含日志。这两个卷构成了该 Oracle 数据库实例的工作负载。

勒索软件恢复能力如何确定工作负载数据的优先级？

工作负载优先级（关键、标准、重要）由已应用于与工作负载关联的每个卷的快照频率和计划备份决定。

"了解工作负载优先级或重要性" 。

勒索软件恢复能力支持哪些工作负载？

勒索软件恢复可以识别以下工作负载：Oracle、MySQL、文件共享、块存储、虚拟机和虚拟机数据存储。

如果您正在使用SnapCenter或SnapCenter for VMware，则这些产品支持的所有工作负载也会在勒索软件恢复功能中得到识别。勒索软件恢复能力可以以与工作负载一致的方式保护和恢复SnapCenter和SnapCenter工作负载。

如何将数据与工作负载关联起来？

勒索软件恢复能力会发现卷和文件扩展名，并将它们与相应的工作负载关联起来。

如果您拥有SnapCenter或SnapCenter for VMware，并且在备份和恢复中配置了工作负载，那么勒索软件恢复功能将发现由SnapCenter和SnapCenter for VMware 管理的工作负载及其关联的卷。

什么是受保护的工作负载？

在勒索软件恢复能力中，当工作负载启用了主要检测策略时，其状态将显示为“受保护”，这意味着 "自主勒索软件防护 (ARP)" 已在与工作负载相关的所有卷上启用。

什么是“高风险”工作量？

如果工作负载未启用主检测策略，即使启用了备份和快照策略，也会被标记为“有风险”。为了防止勒索软件攻击，您应该启用…… "检测策略"。

我添加了一个新卷，但它还没有显示出来。我应该怎么办？

如果您向环境中添加了新卷，请重新启动工作负载发现。在发现体积之后， "采取保护策略以保护新增容量"。

保护策略

勒索软件恢复策略是否可以与其他类型的工作负载策略共存?

目前，备份和恢复（云备份）支持每个卷一个备份策略。如果您使用备份和恢复功能配置备份保护，它将与勒索软件恢复功能共享备份策略。

快照副本不受限制，可以从每个服务单独添加。

勒索软件防护策略需要哪些策略?

一个 "勒索软件防护策略" 需要：

- 勒索软件检测策略，以及
- 快照策略

勒索软件抵御策略中不需要备份策略。

Ransomware Resilience 是否了解**NetApp ONTAP**中所做的保护设置?

是的，Ransomware Resilience 发现了在ONTAP中设置的快照计划。它还会发现已发现的工作负载中的所有卷是否启用了 ARP 和 FPolicy。您在勒索软件恢复仪表板中看到的信息来自其他NetApp解决方案和产品。

勒索软件恢复功能是否了解备份和恢复以及**SnapCenter**中已制定的策略?

是的，如果您在备份和恢复或SnapCenter中管理工作负载，则这些产品管理的策略将被纳入勒索软件恢复能力。

能否修改从**NetApp Backup and Recovery**和/或**SnapCenter**继承的策略?

不可以，您无法从 Ransomware Resilience 修改由备份和恢复或SnapCenter管理的策略。您可以在“备份和恢复”或SnapCenter中管理对这些策略的任何更改。

如果**ONTAP**中存在策略（例如 **ARP**、**FPolicy** 和快照），这些策略是否会在勒索软件恢复功能中更改?

不会。勒索软件恢复不会修改ONTAP中的任何现有检测策略（ARP、FPolicy 设置）。

注册勒索软件恢复功能后，如果在备份和恢复或**SnapCenter**中添加新策略会发生什么情况?

勒索软件恢复能力可以识别备份和恢复或SnapCenter中新创建的策略和策略更改。

能否通过**ONTAP**更改策略?

是的，您可以在 Ransomware Resilience 中从ONTAP更改策略。您还可以在勒索软件恢复中创建新策略并将其应用于工作负载。此操作将用在勒索软件恢复中创建的策略替换现有的ONTAP策略。

可以在**ONTAP**中禁用策略吗?

您可以使用ONTAP中的系统管理器 UI、API 或 CLI 在检测策略中禁用 ARP。

您可以通过应用不包含 FPolicy 和备份策略的其他策略来禁用它们。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 徽标和NetApp商标页面上列出的标志是NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。

"https://www.netapp.com/company/legal/trademarks/"

专利

NetApp拥有的专利的最新列表可以在以下位置找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

通知文件提供有关NetApp软件中使用的第三方版权和许可的信息。

- "NetApp Console通知"