使用勒索软件弹性
NetApp Ransomware Resilience

NetApp
February 27, 2026

目录

使用勒索软件弹性

访问NetApp Ransomware Resilience

要访问 NetApp Ransomware Resilience，您必须通过 NetApp Console 登录。

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

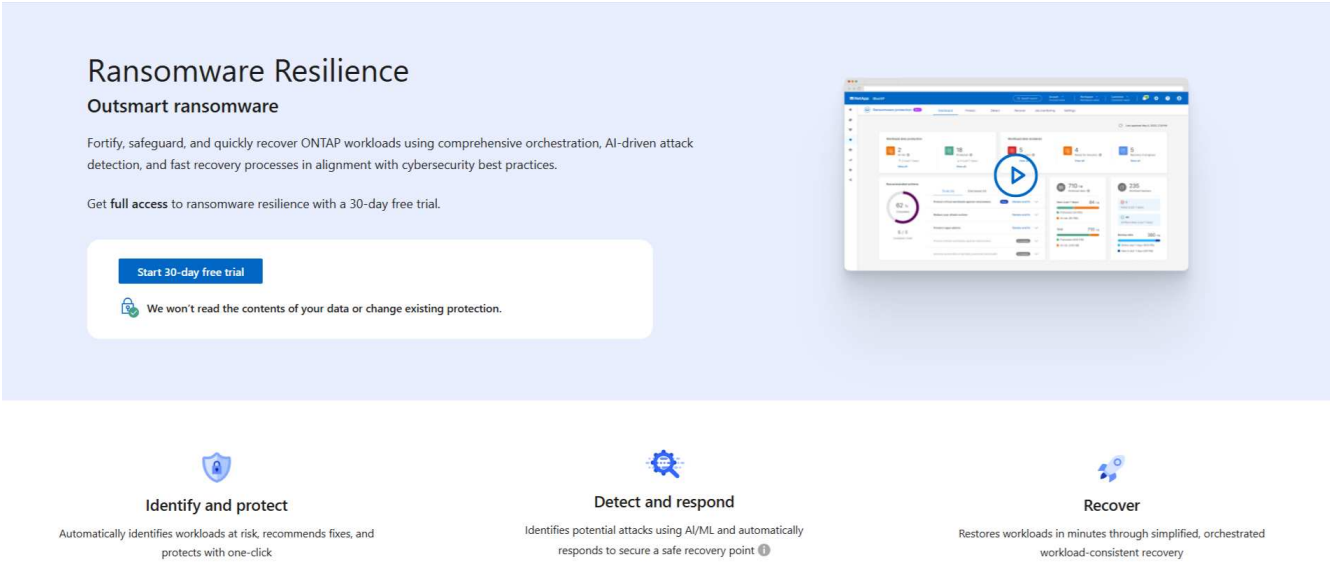
1. 打开网络浏览器并转到"控制台"。

   出现控制台登录页面。

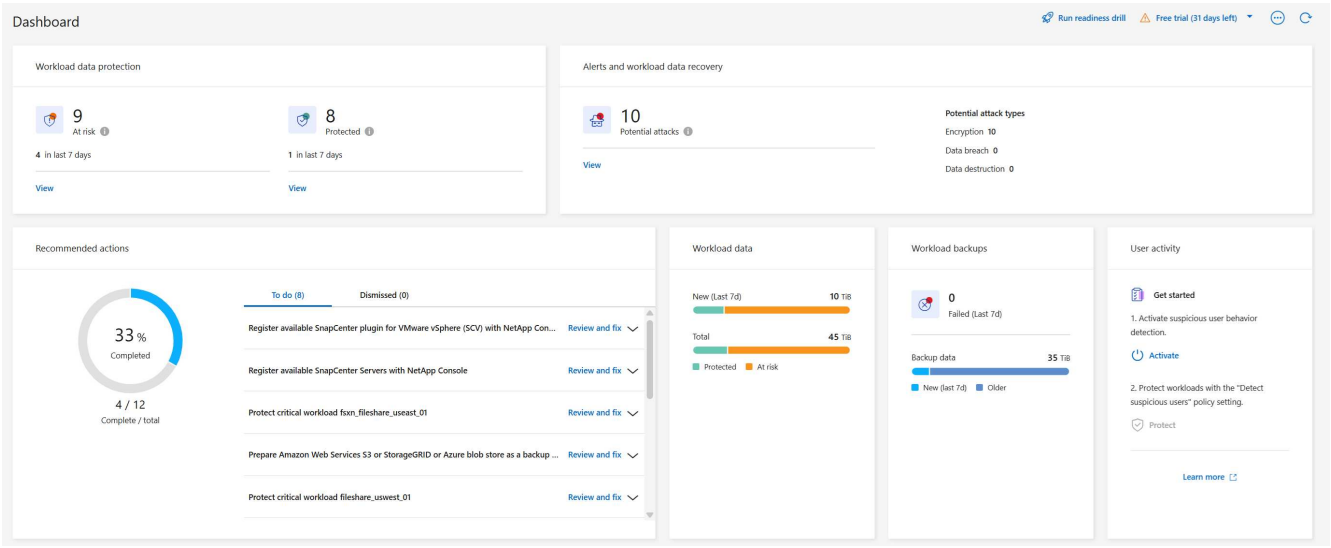
2. 登录控制台。
3. 从控制台左侧导航中，选择*保护*>*勒索软件恢复*。

   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" 。

在 NetApp Ransomware Resilience 中监控工作负载运行状况

NetApp Ransomware Resilience 仪表板可一目了然地显示您的工作负载保护健康状况。您可以快速确定处于风险或受保护状态的工作负载，识别受事件影响或正在恢复的工作负载，并通过查看受保护或处于风险状态的存储量来评估保护范围。

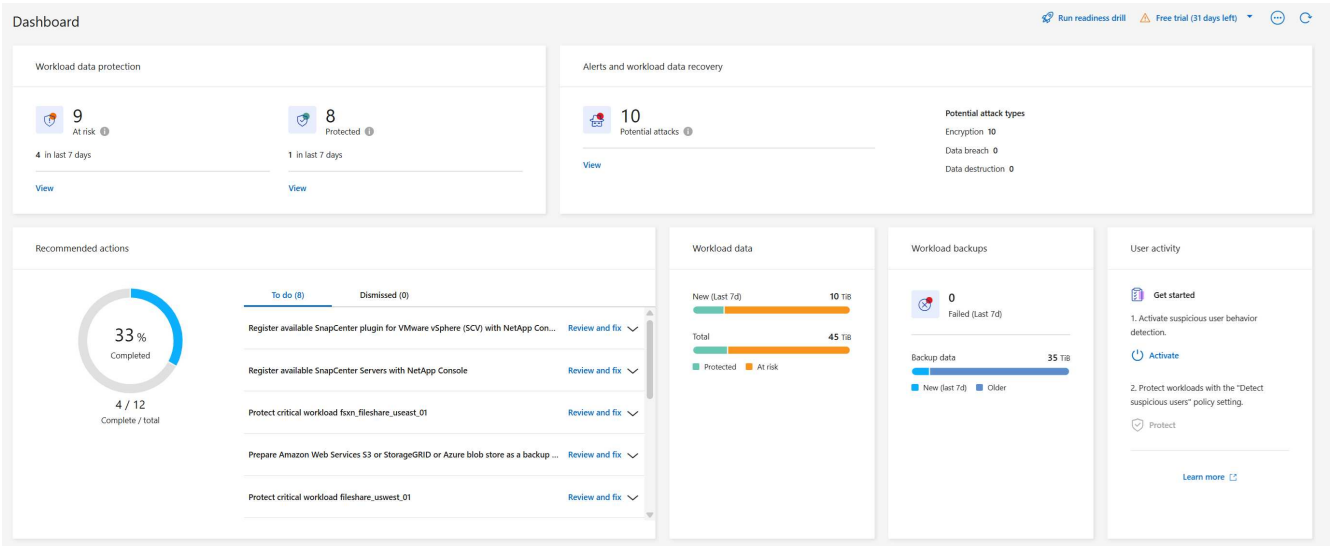
使用仪表板查看保护建议、更改设置和下载报告。

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" 。

使用控制面板查看工作负载运行状况

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. 在控制面板中，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*。

     请参见 "在控制面板上查看保护建议" 或 "保护工作负载"。

     Ransomware Resilience 使用"New"标签显示自您上次访问仪表板以来 24 小时内的新推荐。操作按优先

级顺序显示，最重要的显示在顶部。审查、采取行动或驳回每项建议。

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。

在控制面板上查看防护建议

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"连接到 SIEM"。
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。	将备份目标添加到此工作负载以对其进行保护。请参阅 "添加备份目标"。
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"。请参阅 "保护工作负载免受勒索软件攻击"。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。

从网页下载的 CSV 文件仅包含该网页中的数据。

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. 在勒索软件恢复能力控制面板中，选择“刷新”。 右上角有刷新文件中显示的数据的选项。
2. 执行以下操作之一：
   - 从页面上选择“下载”按钮。 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。

保护和检测

在 NetApp Ransomware Resilience 中查看防护状态

NetApp Ransomware Resilience 的保护仪表板概述了工作负载的保护状态和准备情况。使用保护仪表板，深入了解受保护的内容、需要保护的内容以及保护范围。

一旦您了解了当前保护的范围，"您可以创建勒索软件保护策略并将其应用于您的工作负载"。

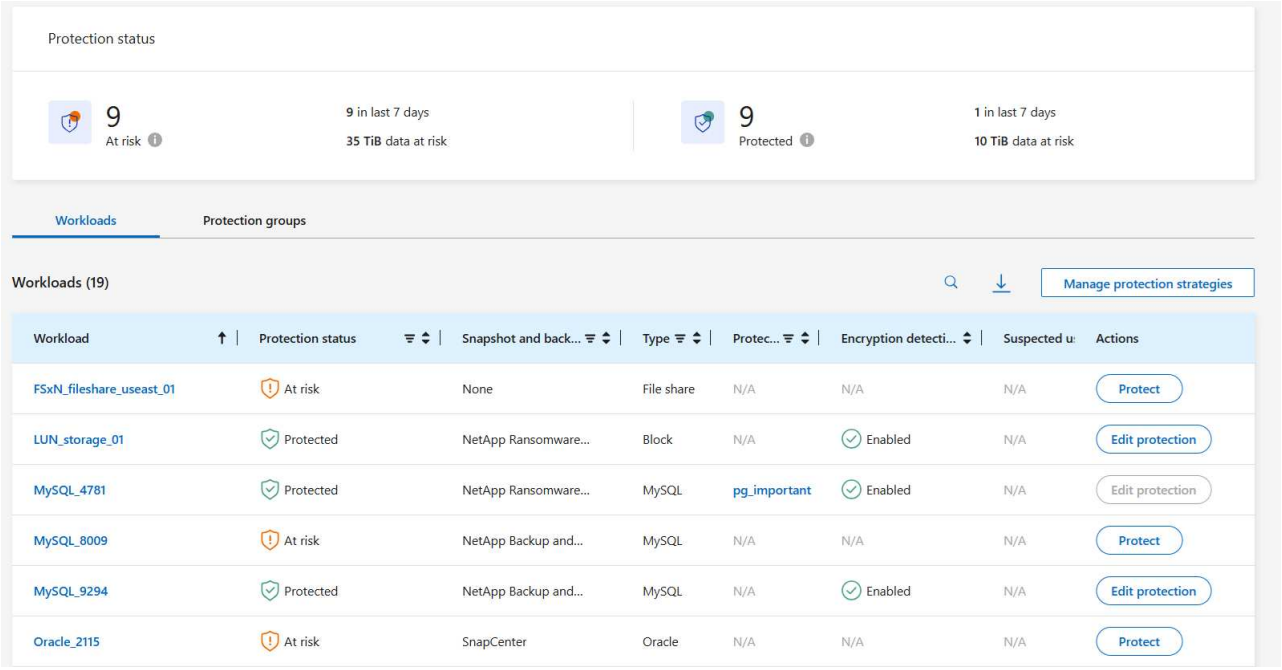
查看工作负载的保护

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. 从控制台左侧导航栏中选择“保护”>“勒索软件恢复”。
2. 执行以下操作之一：
   - 在控制面板的 Data Protection 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。

请参阅 "添加勒索软件防护策略" 了解当存在具有 Backup and Recovery 的现有保护策略时如何使用 Ransomware Resilience。

了解保护信息板

Ransomware Resilience 中的保护仪表板显示有关工作负载的详细信息（例如，工作负载名称和类型、Console 代理、系统和存储 VM）以及有关保护状态的见解。使用保护仪表板查看和管理针对工作负载的勒索软件准备情况。以下列尤其有助于了解您的保护姿势：

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：

+ Ransomware Resilience 可深入了解您在工作负载上配置的勒索软件检测策略的范围。使用以下字段查看检测范围。

- 加密检测状态
- 可疑用户行为检测状态
- 阻止可疑文件扩展名

快照、复制和备份策略：此列显示管理策略的产品或服务。如果没有策略，该字段将显示 N/A。

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：

- 关键：每小时会创建多个快照副本（高度激进的保护计划）
- 重要提示：快照副本的创建频率低于每小时一次，但高于每天一次。
- 标准：每天拍摄多次快照副本

Privacy exposure：选择此选项以"使用 NetApp Data Classification 扫描个人身份信息"。

复制目标：如果已配置快照复制，则会列出目标存储 VM 和系统的名称。如果没有复制，此字段显示 "N/A"。

备份目标：如果您已使用备份配置了勒索软件保护策略，此处将列出备份目标系统的名称。

后续步骤

- "使用勒索软件保护策略保护工作负载"
- "管理保护组"
- "扫描个人身份信息"

在 **NetApp Ransomware Resilience** 中添加备份目标

当 NetApp Ransomware Resilience 发现工作负载时，如果配置了备份，则 Ransomware Resilience 会识别备份目标。如果您计划将备份用作 "勒索软件防护策略" 的一部分，但尚未在工作负载上配置备份目标，则必须在 NetApp Ransomware Resilience 中添加备份目标，以提高网络弹性。

您可以从以下备份目标中选择一个：

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

Amazon FSx for NetApp ONTAP 和 Azure NetApp Files 中的工作负载无法使用备份目标。使用本机备份解决方案执行备份操作：FSx for ONTAP 备份服务或 Azure NetApp Files 备份。

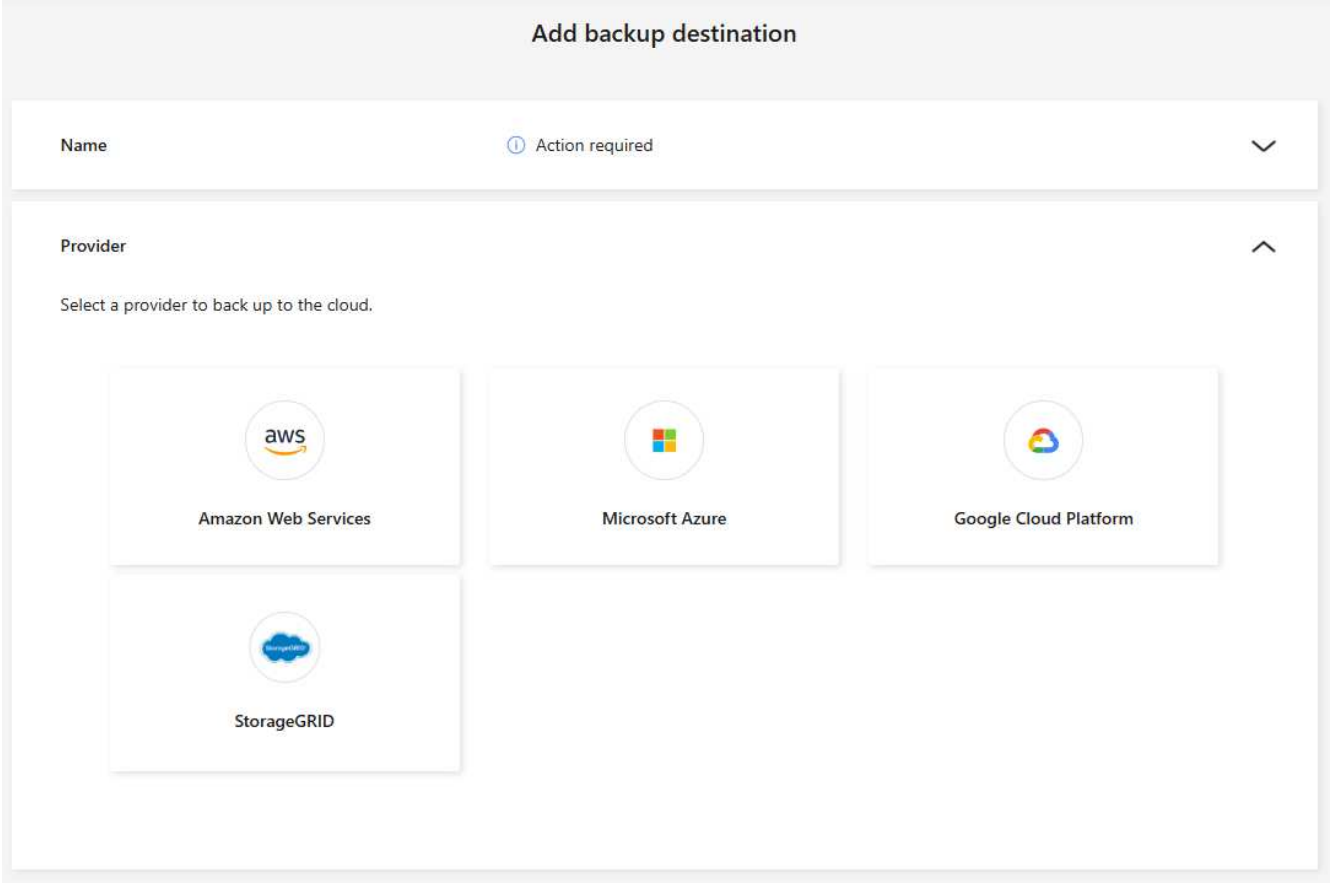
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

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. 在勒索软件恢复功能中，选择设置。
2. 在备份目的地图块中，选择查看。
3. 选择添加。
4. 输入备份目标的名称。

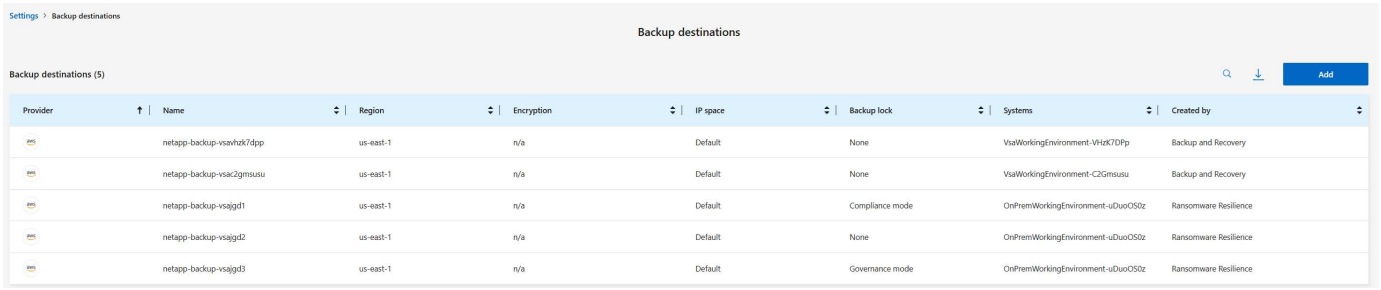


5. 选择* StorageGRID*。
6. 选择每个设置旁边的向下箭头以查看必填字段：
   - 提供商设置：
     - 选择创建新存储桶或自带存储桶。
     - 提供网关节点完全限定域名 **(FQDN)** 和端口。
     - 提供 StorageGRID 凭据：**Access key** 和 **Secret key**。
   - 网络：选择 IP 空间。
     - IP 空间是您要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
   - 备份锁定

     选择是否要配置备份锁定。使用备份锁定，副本受到保护，不会被修改或删除，并会扫描勒索软件威胁。配置备份目标后，您无法修改此设置。 如果您不想要备份锁定，请选择 None。 选择 **Governance mode** 以允许具有特定权限的用户在保留期间覆盖或删除受保护的备份文件。 选择 Compliance mode** 以防止用户在保留期间覆盖或删除受保护的备份文件。
7. 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，请参见 "管理您的 Amazon S3 存储桶"。

步骤

1. 在勒索软件恢复功能中，选择设置。
2. 在备份目的地图块中，选择查看。
3. 选择添加。
4. 选择*Amazon Web Services*。
5. 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。

     如果现在配置备份锁定设置，则无法在配置备份目标后更改该设置。

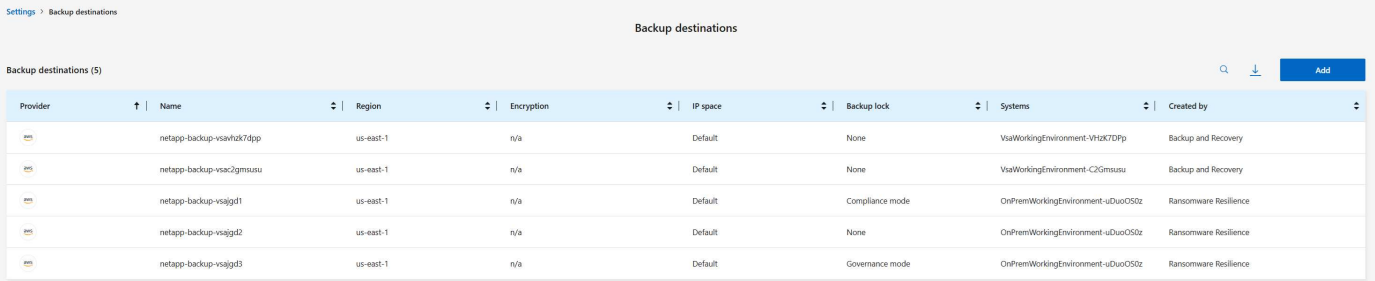
     - 治理模式：特定用户（具有 s3:BypassGovernanceRetention 权限）可以在保留期内覆盖或删除受保护的文件。

- 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。

6. 选择“添加”。

结果

新的备份目标将添加到备份目标列表中。



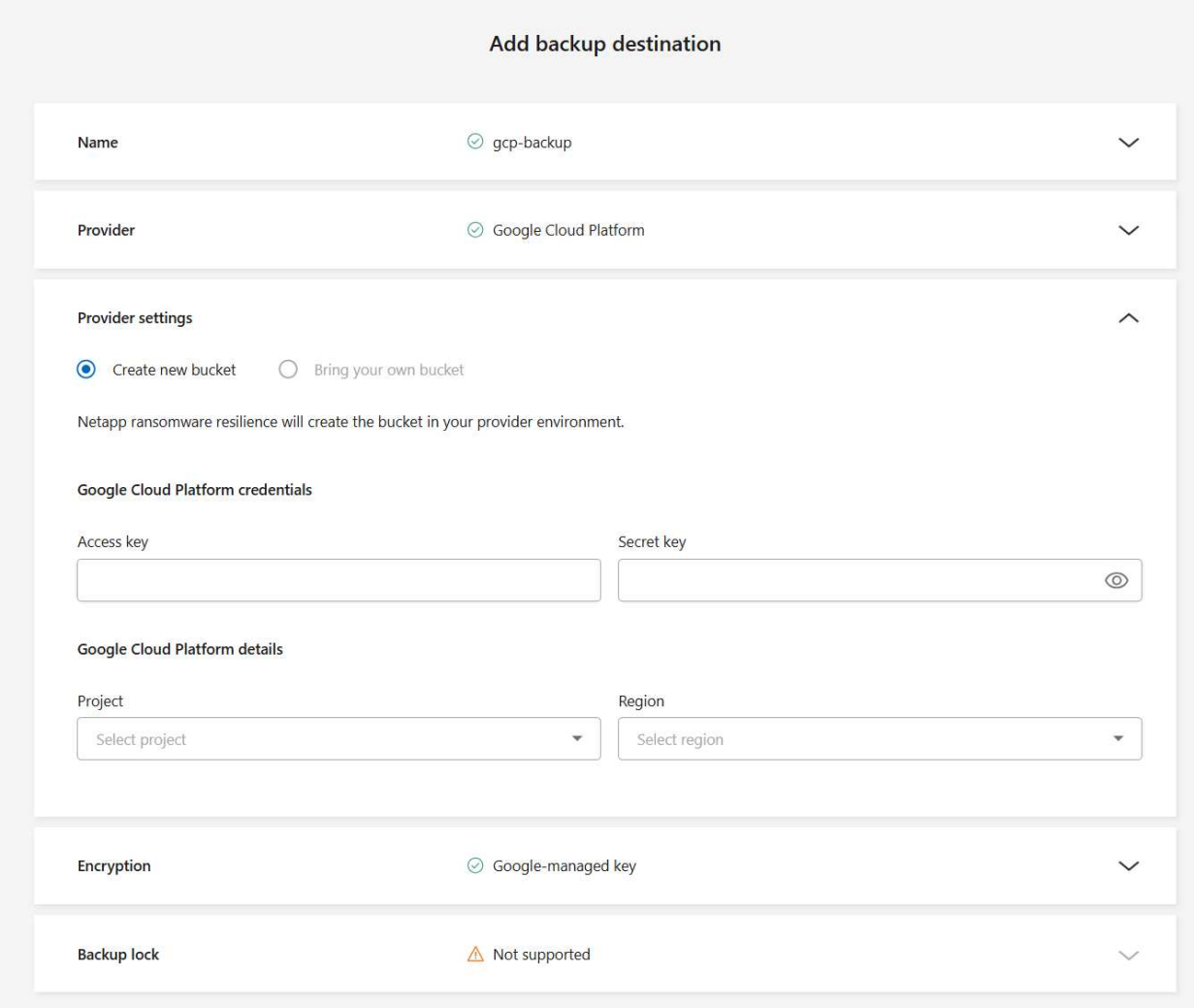
添加 **Google Cloud Platform** 作为备份目标

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

有关在 Console 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. 在勒索软件恢复功能中，选择设置。
2. 在备份目的地图块中，选择查看。
3. 选择添加。
4. 输入备份目标的名称。
5. 选择*Google Cloud Platform*。
6. 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：
     - 选择创建新存储桶或自带存储桶。
     - 提供 Google Cloud Platform 凭据：**Access key** 和 **Secret key**。
     - 选择您的 **Project** 及其所在的 **Region**。



- 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 管理的密钥进行加密。您可以通过选择 **Google** 管理的密钥或使用客户管理的密钥继续使用默认设置。

7. 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. 在勒索软件恢复功能中，选择设置。
2. 在备份目的地图块中，选择查看。

3. 选择添加。
4. 选择“**Azure**”。
5. 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。
     - 请提供应用程序（客户端）ID、客户端密码和目录（租户）ID。选择 身份验证。
     - 为您的 Azure 订阅选择 Azure 订阅、区域和资源组。

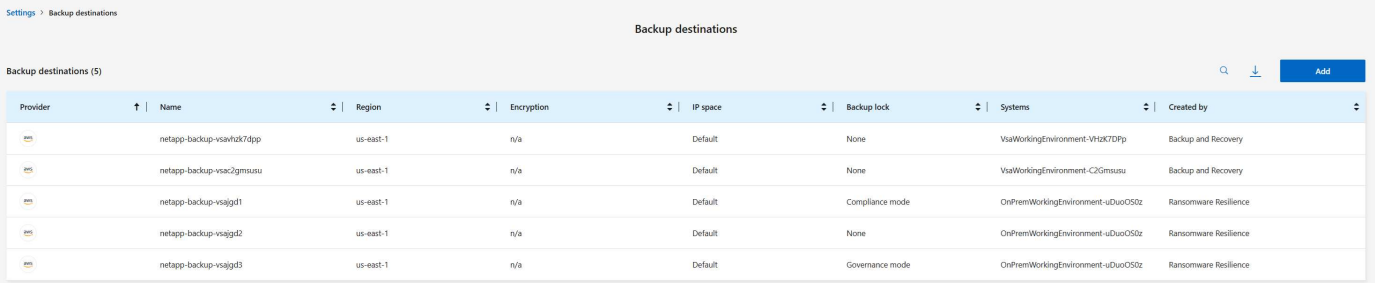
       "如果您想自带存储帐户，请参阅添加 Azure Blob 存储帐户" 。
   - 加密：默认情况下，数据使用 Microsoft 托管的密钥加密。选择 **Microsoft-managed key** 以保留此选项；或者，选择 **Customer managed key** 以使用您自己的密钥进行加密。
   - 网络：选择 IP 空间以及是否使用私有端点。
     - IP 空间是您要备份的卷所在的集群。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
     - 或者，选择是否使用之前配置的 Azure 专用终结点。

       如果您想使用 Azure PrivateLink，请参阅 "Azure PrivateLink"。
   - 备份锁定

     选择是否要配置备份锁定。使用备份锁定，副本受到保护，不会被修改或删除，并会扫描勒索软件威胁。配置备份目标后，您无法修改此设置。 如果您不想要备份锁定，请选择 None。 选择 **Governance mode** 以允许具有特定权限的用户在保留期间覆盖或删除受保护的备份文件。 选择 Compliance mode** 以防止用户在保留期间覆盖或删除受保护的备份文件。
6. 选择“添加”。

结果

新的备份目标将添加到备份目标列表中。



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

勒索软件防护策略是 NetApp Ransomware Resilience 的一个关键特征：它们支持检测、保护和复制。保护策略是网络安全态势的重要组成部分。

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

勒索软件防护策略包括_检测_、_保护_和_复制_策略。

- 检测策略 识别勒索软件威胁
- 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。
- 复制策略 使您能够将勒索软件恢复功能的快照复制到辅助站点。复制计划可以设置为每小时、每天、每周或每月一次的频率。

  目前，您只能将快照复制到本地ONTAP存储。

如果要为 Amazon FSxN for ONTAP 和 Azure NetApp Files 配置保护策略，请参阅 "每项服务的限制"。

为了增强对数据资产的管理和保护，您可以创建"组工作负载"来在一个策略下共同保护卷。

与其他**NetApp**托管服务结合的保护策略

除了 Ransomware Resilience 之外，您还可以使用 NetApp Backup and Recovery 来管理文件共享、VM 文件共享的保护。

来自 Backup & Recovery 服务的保护信息显示在 Ransomware Resilience 中。您可以使用 Ransomware Resilience 向这些服务添加检测策略。使用 Ransomware Resilience 添加保护策略将取代现有的保护策略。

Ransomware Resilience 还从 SnapCenter for VMware 为 VM 数据存储库和 SnapCenter for Oracle 发现保护策略。您无法使用这些服务通过 Ransomware Resilience 进行还原。

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 或 Azure NetApp Files 中的工作负载无法使用备份目标。使用 FSx for ONTAP 备份服务执行备份操作。您可以在 AWS 中为 FSx for ONTAP 中的工作负载设置备份策略，而不是在 Ransomware Resilience 中。备份策略显示在 Ransomware Resilience 中，并且与 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 Backup and Recovery 或 Ransomware Resilience 管理，则可能有作为 ONTAP 或其他产品的一部分拍摄的快照。如果 ONTAP FPolicy 保护到位，则可以使用 ONTAP 更改 FPolicy 保护。

预定义的检测策略

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。

+ 关键复制策略 是唯一支持将快照复制到ONTAP 的预定义策略。

政策层面	Snapshot	频率	保留时间（天）	快照副本数量	快照副本的最大数量
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

政策层面	Snapshot	频率	保留时间（天）	快照副本数量	快照副本的最大数量
关键复制策略	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

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
- 将 **Backup and Recovery** 保护中的现有快照或备份策略替换为由 **Ransomware Resilience** 管理的保护策略。

  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
- 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）

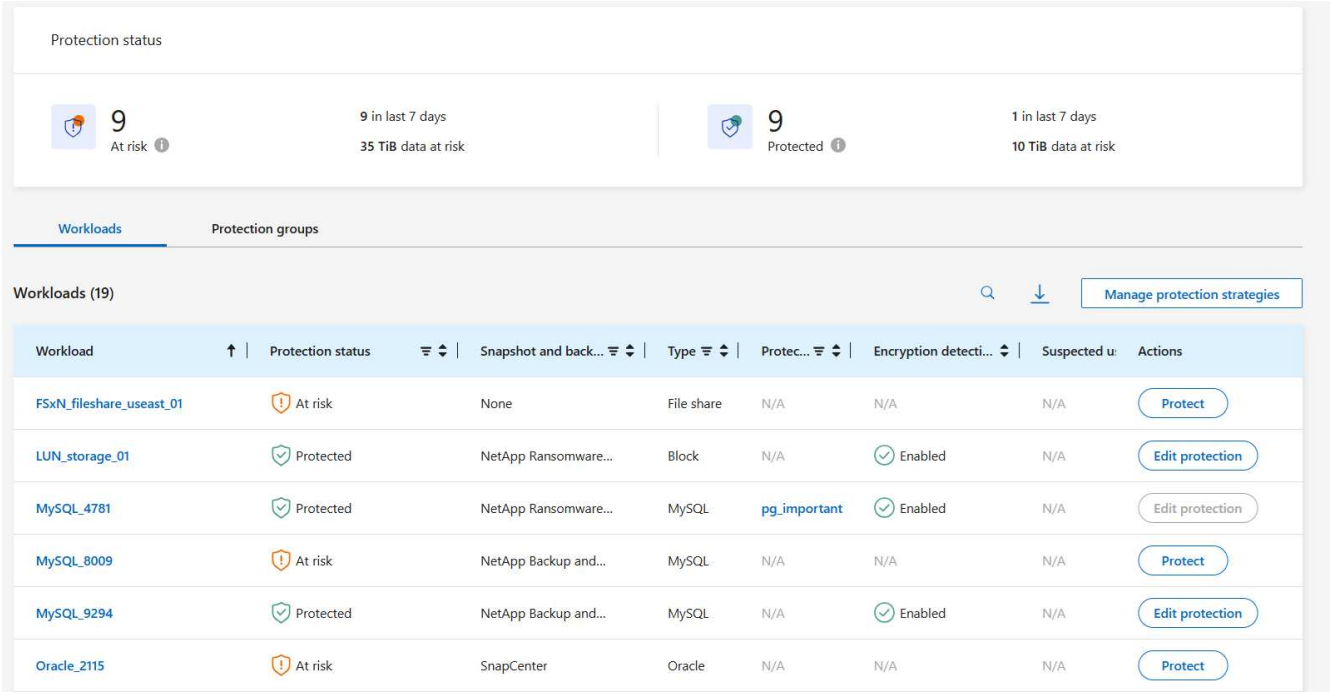
如果工作负载上不存在快照或备份策略，您可以创建勒索软件保护策略，其中可以包括您在勒索软件恢复中创建的以下策略：

- Snapshot 策略
- 备份策略
- 勒索软件检测政策

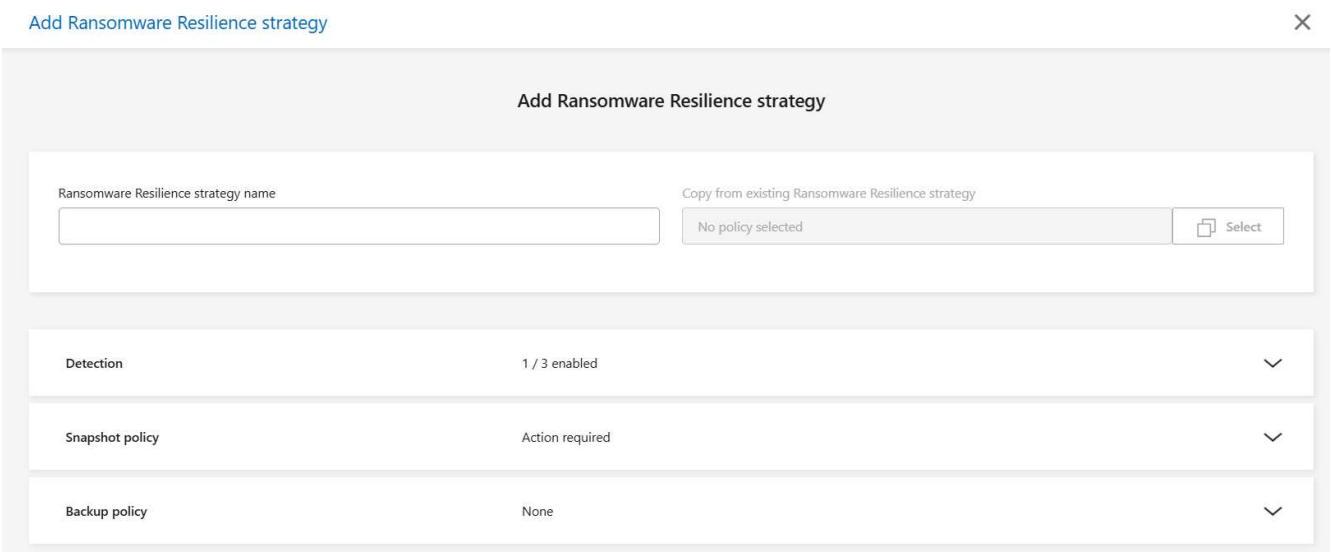
- 二次复制到ONTAP

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：启用勒索软件恢复功能，以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：启用勒索软件恢复功能，以阻止已知的可疑文件扩展名。启用主检测功能后，勒索软件恢复功能会自动创建快照副本。

       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。
     - 复制策略：
   - 复制策略基本名称：输入新名称或选择现有名称。基本名称是附加到所有快照的前缀。
   - 复制计划：切换要启用的频率（每小时、每天、每周或每月），并为每个启用的计划设置保留值（要保留的复制快照的数量）。
     - 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。

   要启用辅助存储上的备份锁定，请使用 **Settings** 选项配置备份目标。有关详细信息，请参见 "配置设置"。

6. 选择“添加”。

将检测策略添加到具有由 **Backup and Recovery** 管理的现有快照和备份策略的工作负载

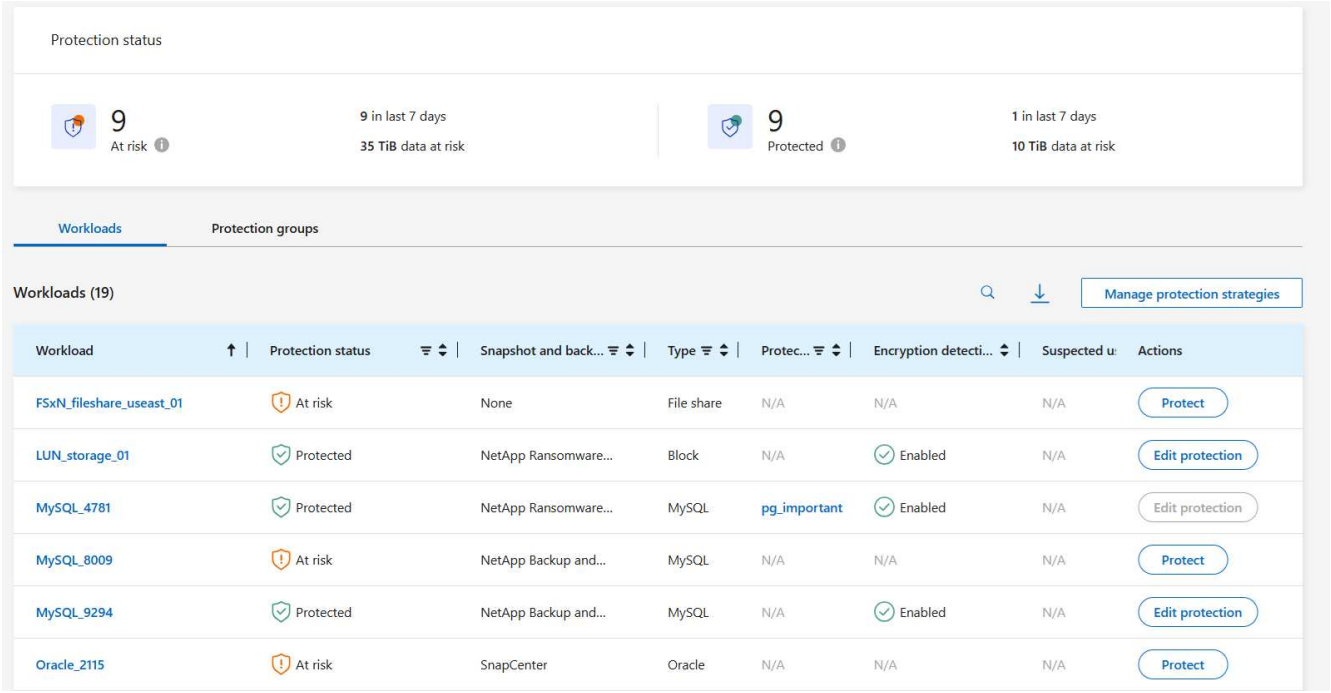
Ransomware Resilience 使您能够为工作负载分配检测策略或保护策略，并使用其他 NetApp 产品或服务管理的现有快照和备份保护。Backup and Recovery 使用管理快照、复制到辅助存储或备份到对象存储的策略。

向具有现有备份或快照策略的工作负载添加检测策略

如果您有具有 Backup and Recovery 功能的现有快照或备份策略，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. Ransomware Resilience 检测是否存在现有的活动 Backup and Recovery 策略。
4. 要保留现有的 Backup and Recovery 并仅应用_检测_策略，请不要选中替换现有策略框。
5. 选择所需的检测设置：
   - 加密检测
   - 可疑用户行为检测
   - 阻止可疑文件扩展名
6. 选择下一步。
7. 如果您选择 **Suspicious user behavior detection** 作为检测设置，请选择 User activity agent 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。

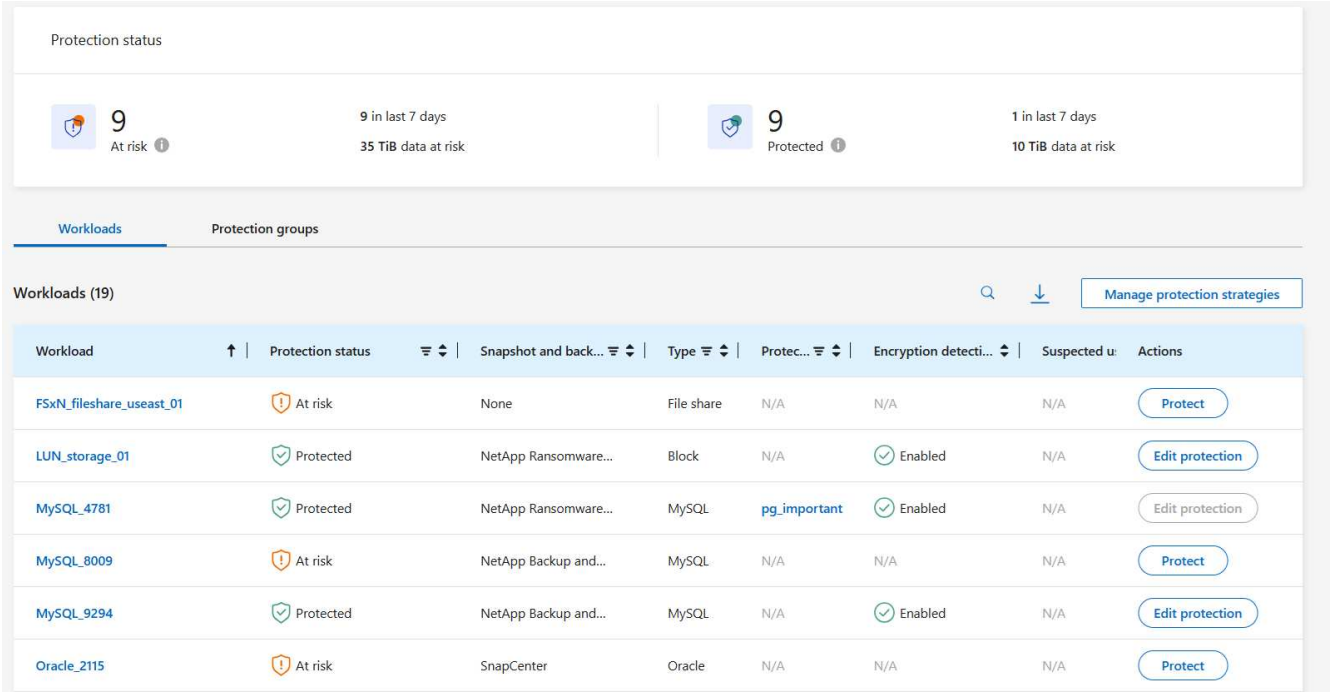
8. 选择下一步。
9. 审查您的选择。选择创建来激活检测。
10. 在“保护”页面上，查看检测状态以确认检测处于活动状态。

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. Ransomware Resilience 检测是否存在现有的活动 Backup and Recovery 策略。要替换现有策略，请选择替换现有策略框。选中此框后，Ransomware Resilience 将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. 如果您的策略包含复制，请选择目标系统和目标存储虚拟机。选择下一步。
6. 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。
7. 查看新的保护策略，然后选择保护来应用它。
8. 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. 如果工作负载具有要维护的现有 Backup and Recovery 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。

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

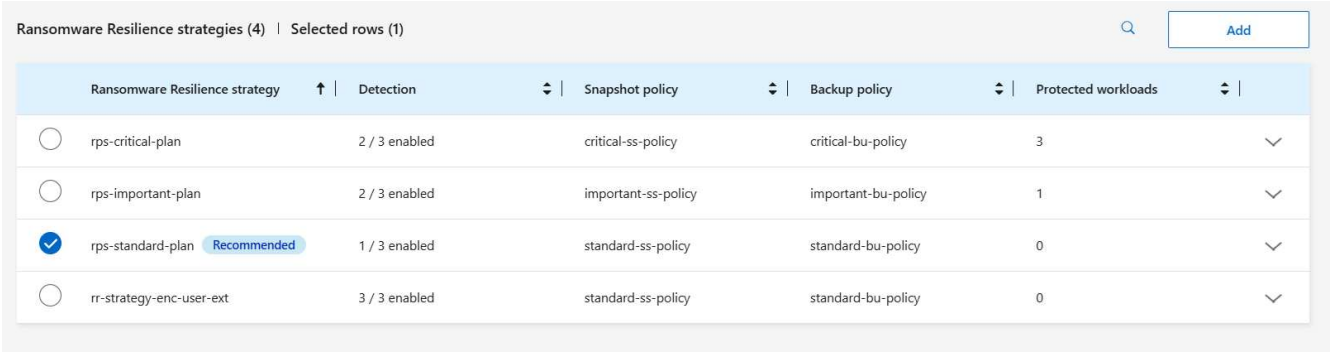
在删除勒索软件保护策略之前，您可能需要查看哪些工作负载受该策略保护。

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*。

配置用户活动检测

了解 **NetApp Ransomware Resilience** 中的用户活动检测

借助用户活动检测，NetApp Ransomware Resilience 使您能够在用户级别解决勒索软件事件，从而阻止数据泄露和大规模删除等事件。

NetApp Ransomware Resilience 通过监控可疑的用户活动，提供人工智能驱动的数据泄露检测。读取活动和读

取活动访问模式的急剧增加用于确定恶意意图。检测到后，Ransomware Resilience 会在 NetApp Console、电子邮件和任何已配置的安全生态系统（例如 SIEM）中自动生成警报。

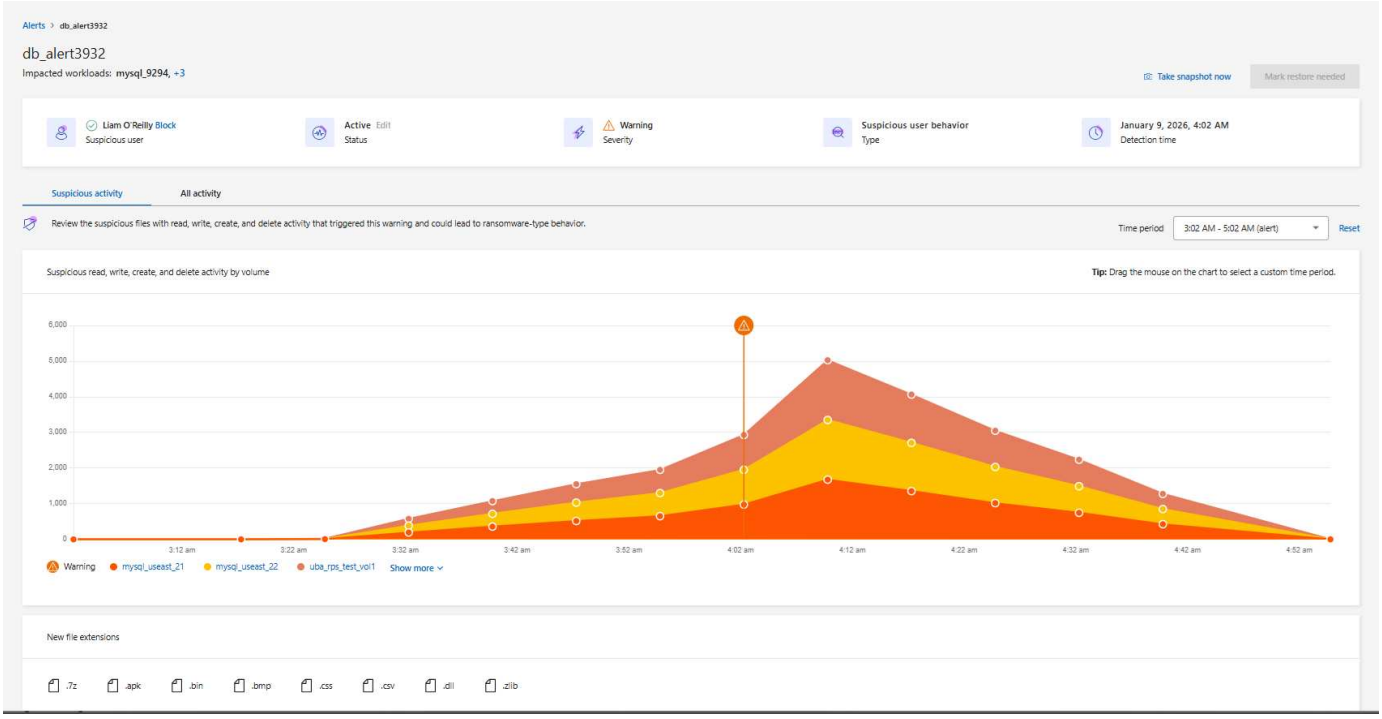
通过可疑的用户行为检测和警报，Ransomware Resilience 会提醒您数据泄露和销毁企图以及看似可疑的模式。在每个警报中，Ransomware Resilience 都会识别您可以阻止的用户。

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。

SAN 工作负载当前不支持用户活动检测。您可以在 Amazon FSxN for ONTAP、Cloud Volumes ONTAP 和 ONTAP 中对 NAS 工作负载使用用户活动检测。

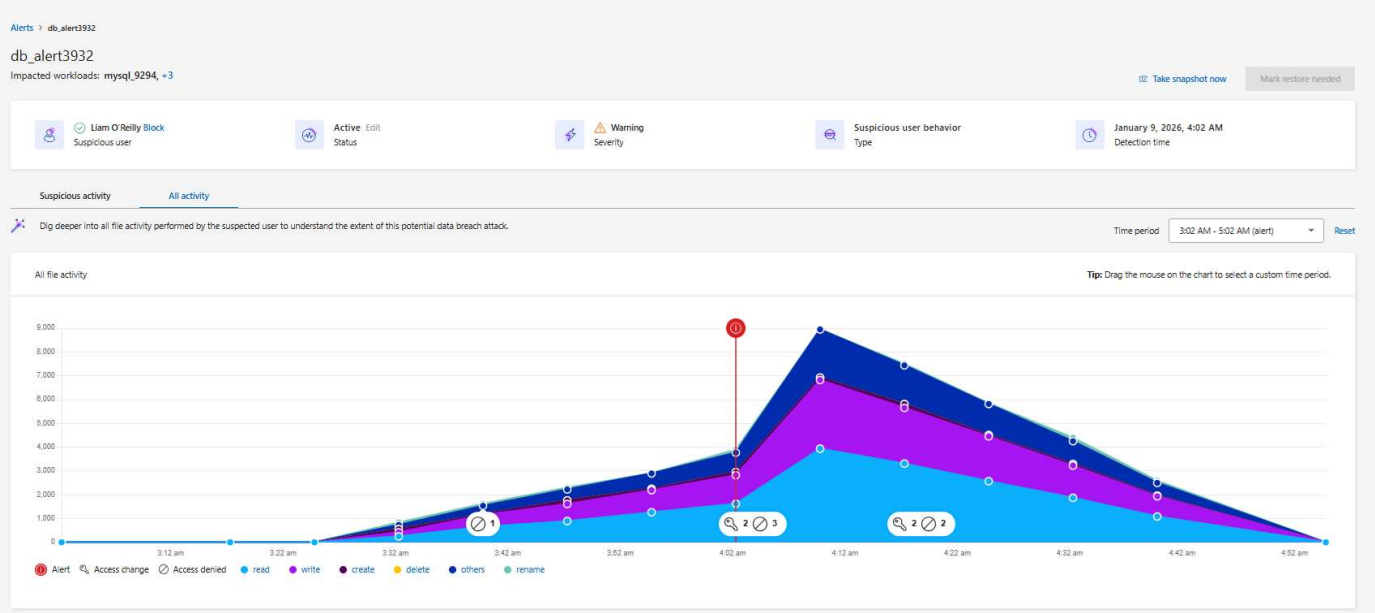
可疑用户活动取证

Ransomware Resilience 为用户行为提供取证：显示何时发生可疑活动以及何时发出通知的列表和图形。这些详细说明了文件、目录、卷和工作负载上可疑活动随时间变化的频率，以帮助绘制事件图表。您还可以观察新文件扩展名的出现。



o

您可以将可疑活动与所有活动的视图进行比较。在所有活动视图中，除了访问更改和访问被拒绝的事件外，您还可以观察读取、写入、重命名、移动、创建和删除事件。



o

组件

Ransomware Resilience 可疑用户行为活动检测有三个关键组成部分。

- 用户活动代理是数据收集器的可执行环境。您必须配置用户活动代理。
- 数据收集器与 Ransomware Resilience 共享用户活动事件。当您"启用带有可疑用户活动检测的勒索软件保护策略"时，会自动创建数据收集器。
- 用户目录连接器启用用户名和用户 ID 之间的映射，从而在响应可疑用户行为时提高清晰度。您必须配置用户目录连接器。

Ransomware Resilience 和 Data Infrastructure Insights

Ransomware Resilience 的可疑用户行为检测是与 Data Infrastructure Insights (DII) Workload Security 的集成，并使用 "DII 端点"。您无需任何 DII 配置即可在 Ransomware Resilience 中启用用户行为检测。要启用用户行为检测，"创建所需的代理和收集器，并启用适当的勒索软件保护策略"。

如果您已经在使用 NetApp Data Infrastructure Insights (DII) Workload Security，建议您使用相同的 Workload Security 代理来实现 Ransomware Resilience。您不需要为 Ransomware Resilience 部署单独的 Workload Security 代理，但是，使用相同的 Workload Security 代理需要在 Ransomware Resilience Console 组织和 DII Storage Workload Security 租户之间建立配对关系。请联系您的账号代表以启用此配对。

后续步骤

- "用户行为活动检测要求"
- "配置用户行为活动代理和检测器"

NetApp Ransomware Resilience 中用户行为检测的要求

NetApp Ransomware Resilience 用户行为检测使您能够对用户级别的勒索软件事件做出响应。您必须创建一组代理才能启用用户行为检测。在启用检测之前，您必须确保满足概述的操作系统、服务器和网络要求，以便 Ransomware Resilience 能够正确检测和报告事

件。

云提供商支持

可疑用户活动数据可以存储在 AWS 和 Azure 的以下区域中：

云提供商	地区
AWS	• 亚太地区（悉尼）（ap-southeast-2） • 欧洲（法兰克福）(eu-central-1) • 美国东部（弗吉尼亚北部）（us-east-1）
Azure	美国东部

操作系统要求

以下操作系统支持可疑用户行为检测：

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
Red Hat	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）

用于用户活动代理的计算机不应运行其他应用程序级软件。建议使用专用服务器。

这 `unzip` 安装需要该命令。这 `sudo su -` 该命令用于安装、运行脚本和卸载。

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：36 GB 可用磁盘空间

服务器建议

- 分配额外的磁盘空间以用于创建文件系统。请确保文件系统中至少有 35 GB 的可用空间。+ 如果 `/opt` 这是从 NAS 存储设备挂载的文件夹，本地用户必须有权限访问此文件夹。如果本地用户没有必要的权限，则用户活动代理创建可能会失败。
- 建议您在与 Ransomware Resilience 环境分开的系统中安装用户活动代理。如果您将它们安装在同一台计算机上，则应允许 50 到 55 GB 的磁盘空间。对于 Linux，分配 25-30 GB 的空间到 `/opt/netapp`，分配 25 GB 的空间到 `var/log/netapp`。
- 建议您使用网络时间协议 (NTP) 或简单网络时间协议 (SNTP) 同步ONTAP系统和用户活动代理计算机上的时间。

云网络访问规则

查看您所在地区（亚太地区、欧洲或美国）的云网络访问规则。

在初始安装期间，将 `<site_name>`替换为通配符 (*`）权限。激活代理并完全运行后，您可以将权限替换为站点名称。有关站点名称，请联系您的 NetApp 代表。

用户活动代理使用 NetApp Data Infrastructure Insights 技术，因此使用 `cloudinsights`端点。有关详细信息，请参见

基于 **APAC** 的用户活动代理部署

协议	端口	源	目标	描述
HTTPS（TCP）	443	用户活动代理	• <site_name>.cs01-ap-1.cloudinsights.netapp.com/cn • <site_name>.c01-ap-1.cloudinsights.netapp.com/cn • <site_name>.c02-ap-1.cloudinsights.netapp.com/cn • gentlogin.cs01-ap-1.cloudinsights.netapp.com/cn	获得勒索软件恢复能力

基于欧洲的用户活动代理部署

协议	端口	源	目标	描述
HTTPS（TCP）	443	用户活动代理	• <site_name>.cs01-eu-1.cloudinsights.netapp.com/cn • <site_name>.c01-eu-1.cloudinsights.netapp.com/cn • <site_name>.c02-eu-1.cloudinsights.netapp.com/cn • agentlogin.cs01-eu-1.cloudinsights.netapp.com/cn	获得勒索软件恢复能力

基于美国的用户活动代理部署

协议	端口	源	目标	描述
HTTPS（TCP）	443	用户活动代理	• <site_name>.cs01.cloudinsights.netapp.com/cn • <site_name>.c01.cloudinsights.netapp.com/cn • <site_name>.c02.cloudinsights.netapp.com/cn • agentlogin.cs01.cloudinsights.netapp.com	获得勒索软件恢复能力

网络内规则

协议	端口	源	目标	描述
TCP	389（LDAP） 636（LDAP/启动-tls）	用户活动代理	LDAP Server URL	连接到 LDAP
HTTPS（TCP）	443	用户活动代理	集群或SVM管理IP地址（取决于SVM收集器配置）	API 与ONTAP进行通信
TCP	35000 - 55000	SVM 数据 LIF IP 地址	用户活动代理	ONTAP与用户活动代理之间关于Fpolicy 事件的通信。为了让ONTAP能够向用户活动代理发送事件，必须向其开放这些端口，包括用户活动代理本身上的任何防火墙（如果存在）。+ 注意：您不需要预留*所有*这些端口，但您为此预留的端口必须在此范围内。建议您先预留 100 个端口，如有必要再增加。

协议	端口	源	目标	描述
TCP	35000-55000	集群管理 IP	用户活动代理	ONTAP集群管理 IP 与用户活动代理之间关于 **EMS** 事件 的通信。为了让ONTAP能够向用户活动代理发送 EMS 事件，必须向用户活动代理开放这些端口，包括用户活动代理本身上的任何防火墙。+ 注意：您不需要预留*所有*这些端口，但您为此预留的端口必须在此范围内。建议您先预留 100 个端口，如有必要再增加。
SSH	22	用户活动代理	集群管理	需要 CIFS/SMB 用户阻止。

下一步

- "配置用户活动代理和收集器"

在 **NetApp Ransomware Resilience** 中为用户活动检测配置代理和收集器

NetApp Ransomware Resilience 用户活动检测可帮助您防止用户级别的勒索软件事件。要在 Ransomware Resilience 中启用可疑用户行为检测，必须至少安装一个用户活动代理，该代理将创建一个数据收集环境，以监控用户行为中类似于勒索软件事件的异常模式。

用户活动代理托管数据收集器和用户目录连接器，它们都将数据发送到 SaaS 位置进行分析。

- 数据收集器从 ONTAP 收集用户活动数据。当您创建具有用户行为检测的保护策略时，将自动创建数据收集器。
- 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。您必须配置用户目录连接器。

用户活动代理、数据收集器和用户目录连接器都可以从 Ransomware Resilience 设置信息板进行管理。

如果您已经在使用 NetApp Data Infrastructure Insights (DII) Workload Security，建议您使用相同的 Workload Security 代理来实现 Ransomware Resilience。您不需要为 Ransomware Resilience 部署单独的 Workload Security 代理，但是，使用相同的 Workload Security 代理需要在 Ransomware Resilience Console 组织和 DII Storage Workload Security 租户之间建立配对关系。请联系您的账号代表以启用此配对。

+ 如果您_不_使用 DII，请继续执行此处的配置说明。

开始之前

- 请确保满足 "操作系统、服务器和网络要求"。

需要控制台角色 要激活可疑用户活动检测，您需要组织管理员角色。对于后续的可疑用户活动配置，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"。

确保每个角色都应用于组织级别。

创建用户活动代理

用户活动代理是 "数据收集器" 的可执行环境；数据收集器与 Ransomware Resilience 共享用户活动事件。您必须至少创建一个用户活动代理才能启用可疑用户活动检测。

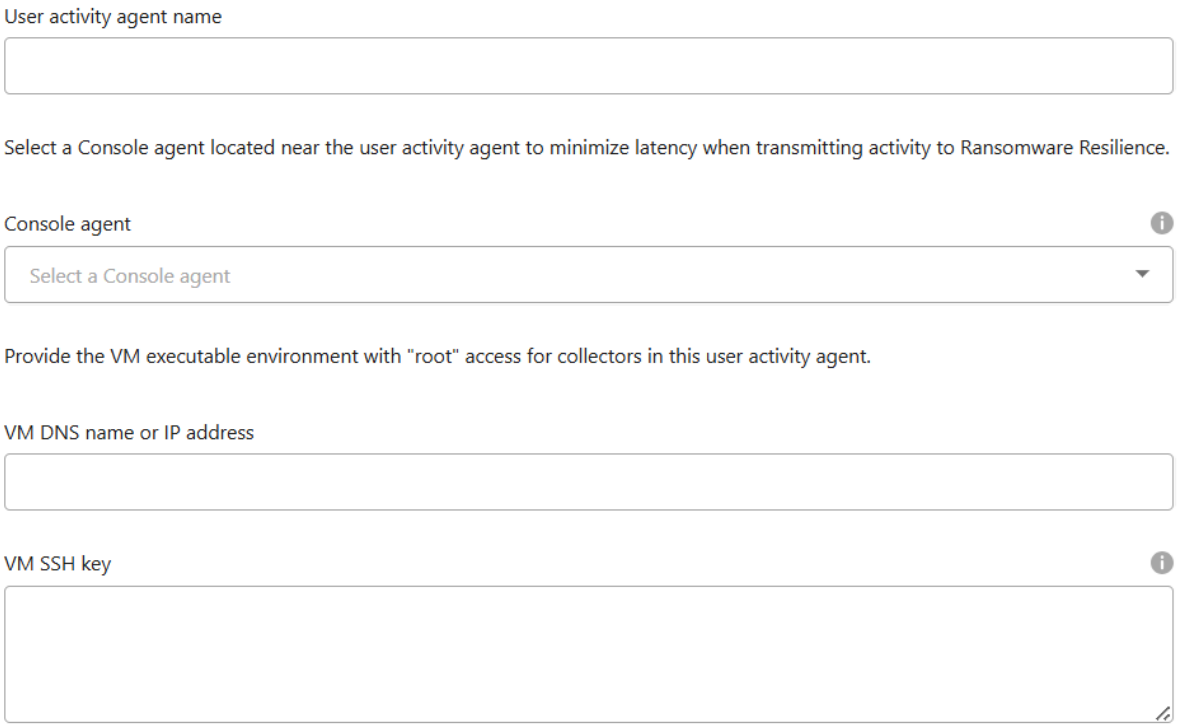
步骤

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，并可通过 SSH 连接到用户活动代理的 IP 地址。
   - **VM DNS** 名称或 **IP** 地址
   - **VM SSH Key** - 使用以下格式输入 SSH 密钥：

     ```
     -----BEGIN OPENSSH PRIVATE KEY-----
     private-key-contents
     -----END OPENSSH PRIVATE KEY-----
     ```



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. 确认已成功创建用户活动代理。在用户活动图块中，成功的部署显示为 **Running**。

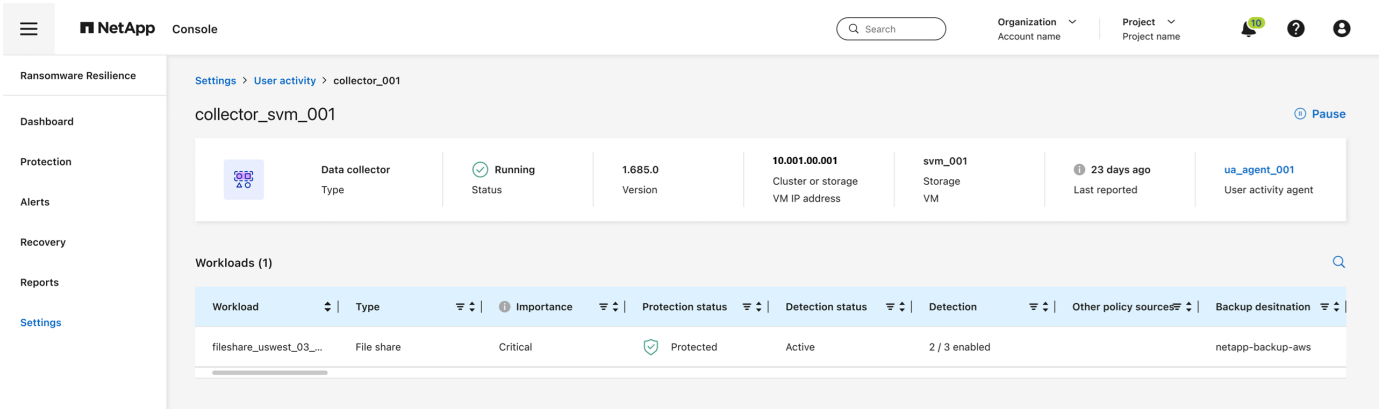
结果

成功创建用户活动代理后，返回 **Settings** 菜单，然后在 User activity 图块中选择 **Manage**。选择 **User activity agents** 选项卡，然后选择用户活动代理以查看其详细信息，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的勒索软件保护策略时，会自动创建数据收集器。有关详细信息，请参见 "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。



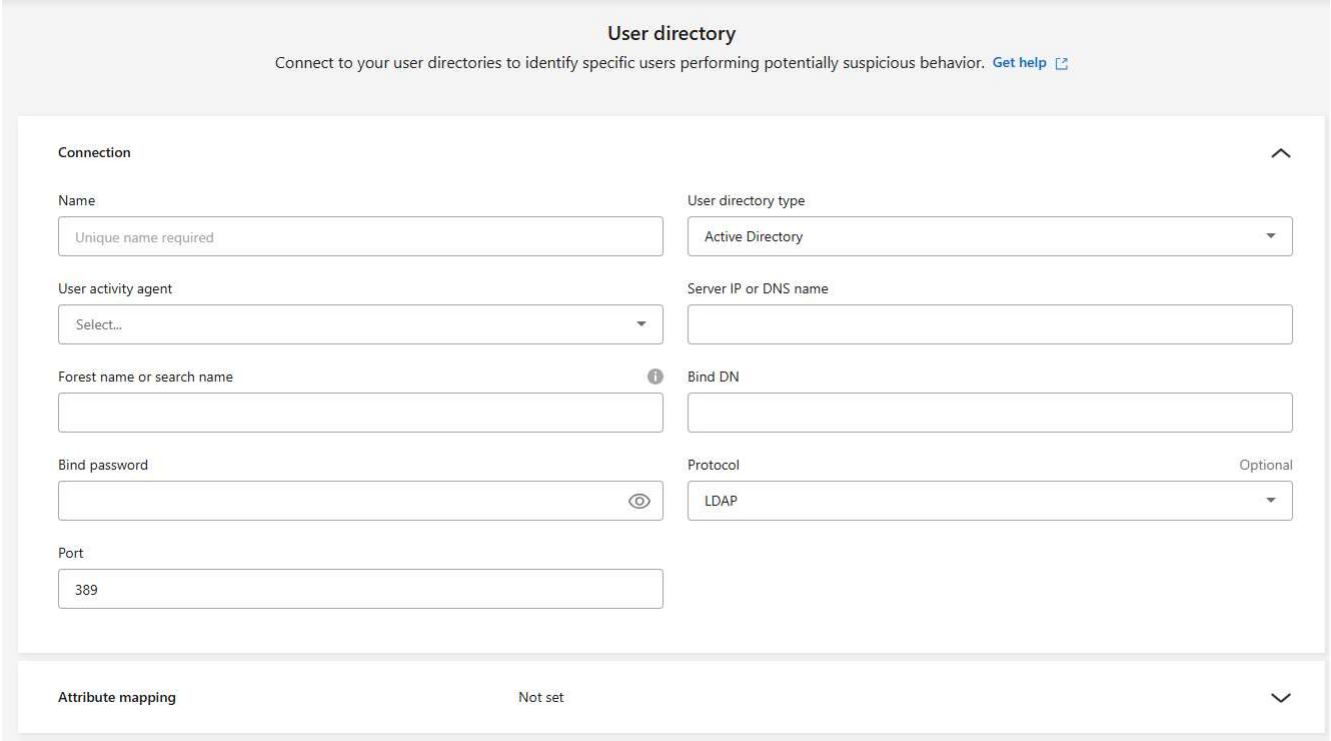
创建用户目录连接器

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. 配置连接。请在每个字段中填写所需信息。

字段	描述
姓名	请为用户目录连接器输入一个唯一的名称
用户目录类型	目录类型
服务器IP地址或域名	连接所在服务器的 IP 地址或完全限定域名 (FQDN)
森林名称或搜索名称	您可以将目录结构的林级别指定为直接域名（例如）。 `unit.company.com`）或一组相对专有名称（例如： `DC=unit,DC=company,DC=com`）。你也可以输入一个 `OU` 按组织单元或 `CN` 仅限特定用户（例如：`CN=user,OU=engineering,DC=unit,DC=company,DC=com`）。
绑定DN	BIND DN 是被允许搜索目录的用户帐户，例如 user@domain.com。用户需要域只读权限。
绑定密码	BIND DN 中提供的用户密码
协议	协议字段为可选字段。您可以使用 LDAP、LDAPS 或基于 StartTLS 的 LDAP。
港口	请输入您选择的端口号



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）
- 如果您选择“包含可选属性”，您还可以添加电子邮件地址、电话号码、角色、州/省、国家/地区、部门、照片、经理 DN 或组。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

步骤

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. 在弹出对话框中，选择 删除 进行确认。

从警报中排除用户

如果存在某些受信任的用户，其行为可能会触发用户行为警报，则可以将其从警报中排除。

步骤

1. 在勒索软件恢复功能中，选择设置。
2. 在设置仪表板中，找到用户活动卡，然后选择 管理。
3. 选择 排除用户 选项卡。
4. 要在 UI 中查看单个用户，请选择手动选择。要上传排除用户的列表，请选择上传。
   a. 如果选择了手动选择，请选中要排除的特定用户名旁边的复选框。
   b. 如果您选择 **Upload**，则必须先下载包含所有用户列表的 CSV 文件。选择 **Download** 以访问列表。

      查看 CSV 文件。删除要为其维护检测的所有用户的名称。当列表仅包含要从检测中排除的用户的名称时，请将其保存。选择 **Upload** 以查找文件，然后选择它。
5. 选择 **Add** 以完成将用户添加到排除列表。
6. 在排除的用户选项卡中，从用户行为检测警报中删除的用户名称现在显示在仪表板中。

您还可以直接从警报中排除用户。有关详细信息，请参见 "响应勒索软件警报"。

从排除的用户列表中删除用户

您可以在之后将用户添加回检测。

步骤

1. 在设置仪表板中，找到用户活动卡，然后选择 管理。
2. 选择 排除用户 选项卡。
3. 从排除的用户选择中找到要删除的用户的名称。选择具有用户名的行上的操作菜单 (...) ，然后选择 删除。
4. 在对话框中，选择 **Remove** 以确认要删除选定用户。

响应可疑用户活动警报

配置可疑用户活动检测后，可以在警报页面中监控事件。有关详细信息，请参见 "检测恶意活动和可疑用户行为"。

在 NetApp Ransomware Resilience 中管理保护组

NetApp Ransomware Resilience 提供保护组，以便更轻松地管理您的数据资产。保护组是工作负载的逻辑分组。Ransomware Resilience 可以使用单一保护策略同时保护保护组中的所有卷，使您无需对每个工作负载应用策略。

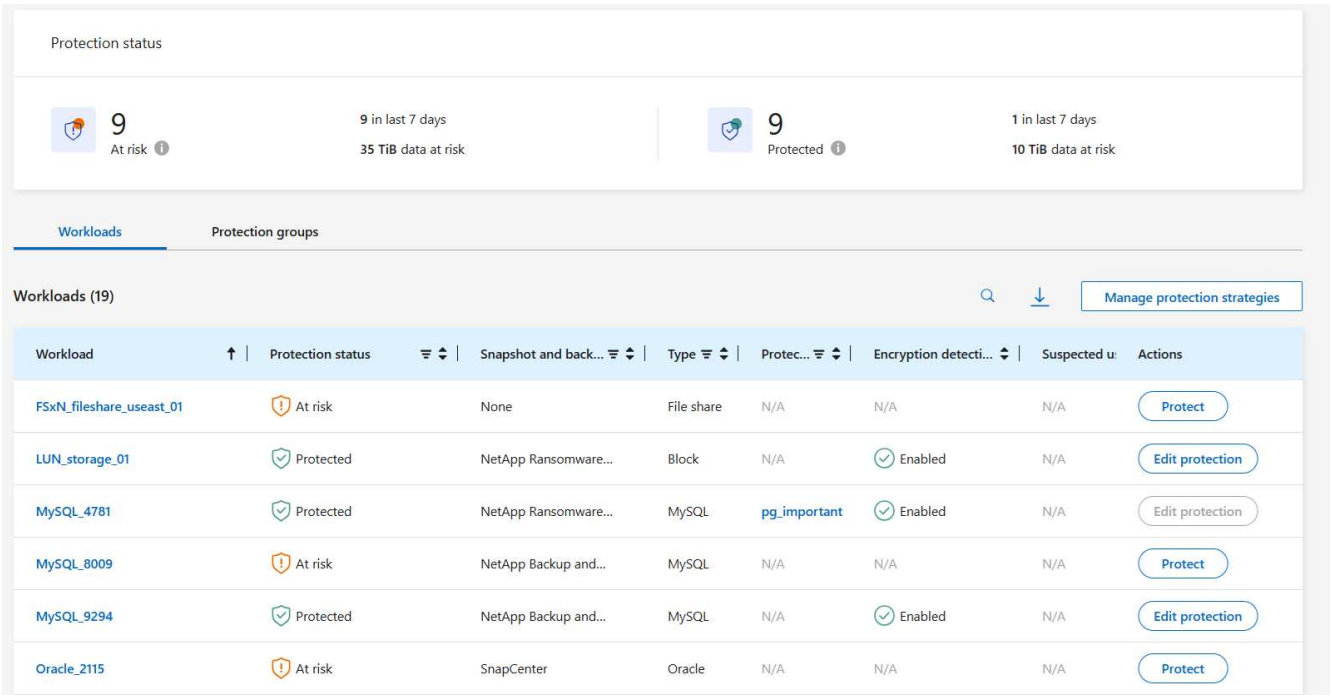
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

创建保护组

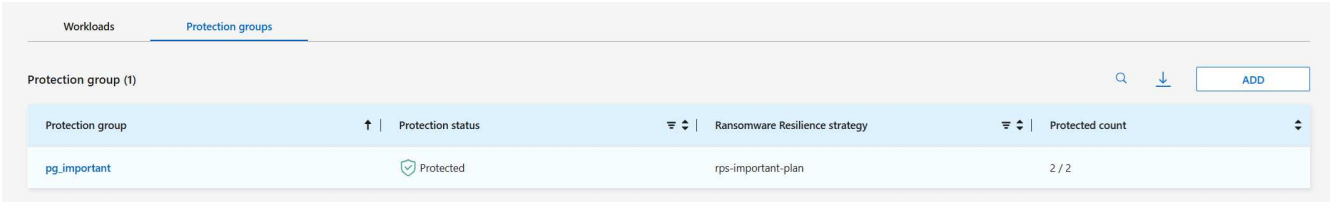
无论其保护状态如何，您都可以创建组（即未受保护的组和受保护的组）。向保护组添加保护策略时，新保护策略将替换任何现有策略，包括由 NetApp Backup and Recovery 管理的策略。

步骤

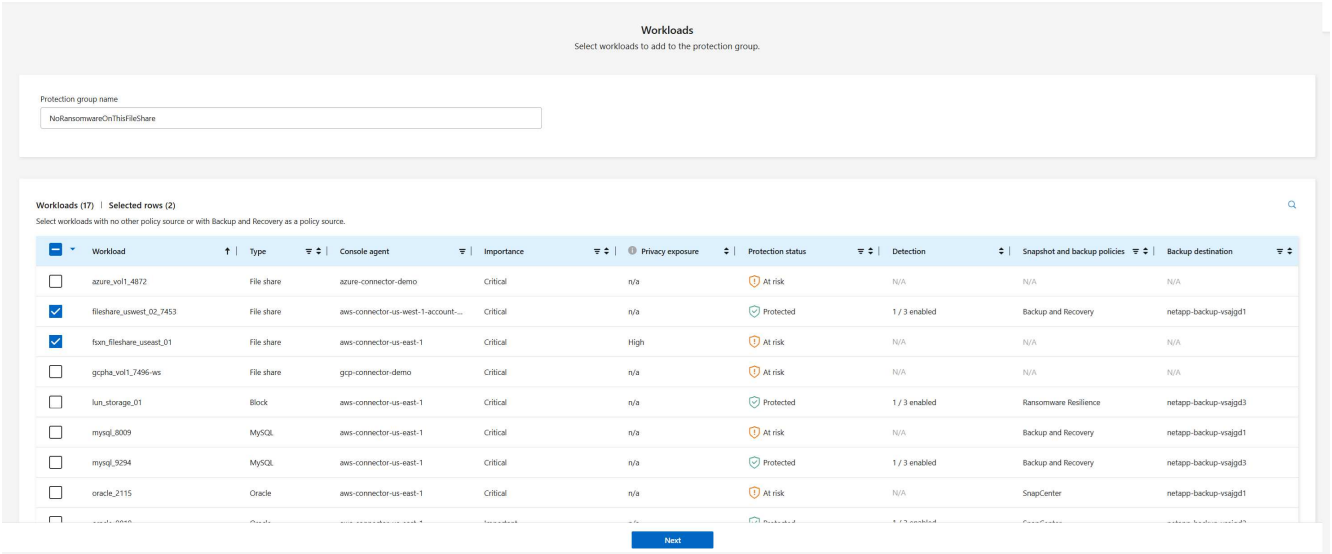
1. 从勒索软件恢复菜单中，选择*保护*。



2. 从 Protection 仪表板中，选择 **Protection groups** 选项卡。



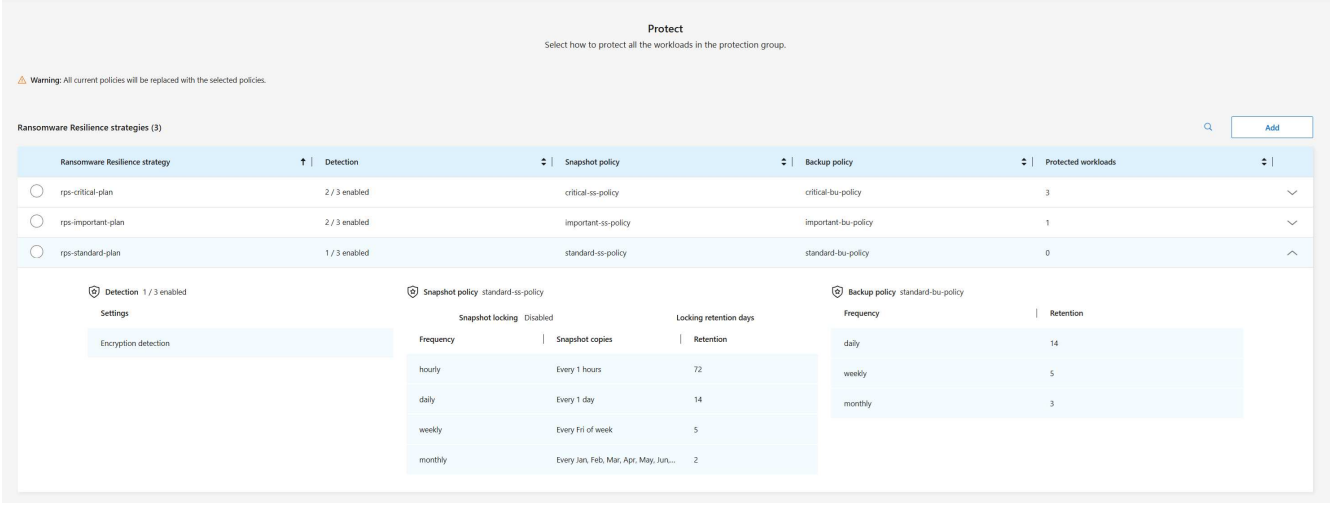
3. 选择“添加”。



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. 为组选择保护策略。
8. 如果保护策略包含复制功能，请检查复制设置。
   a. 要将所有快照复制到同一目标位置，请选中“每个工作负载使用同一目标位置”。在控制台代理部分，为工作负载选择*目标系统*和*目标存储虚拟机*。+ 要使用不同的目的地，请取消选中该框。检查每个控制台代理下的每个工作负载，并为每个工作负载分配一个*目标系统*和*目标存储虚拟机*。选择下一步。
9. 要配置备份策略，请选择一个，然后选择下一步。
10. 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。
11. 检查保护组的选择。
12. 要最终确定保护组，请选择 **Add** 。

在 Ransomware Resilience 中查看保护仪表板时，您可以按保护组对工作负载进行排序。

编辑组保护

您可以更改现有组的检测策略。

步骤

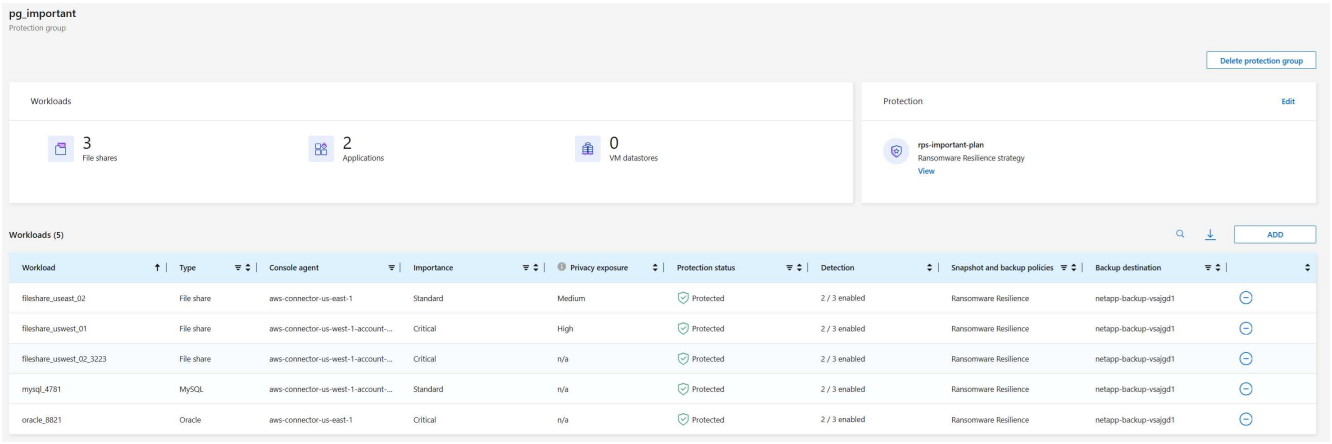
1. 从勒索软件恢复菜单中，选择*保护*。
2. 在“保护”页面中，选择“保护组”选项卡，然后选择要修改其策略的组。
3. 从保护组的概览页面中，选择“编辑保护”。
4. 选择要应用的现有保护策略，或选择 添加 以创建新的保护策略。有关添加保护策略的详细信息，请参见 "创建保护策略"。然后选择 保存。
5. 在备份目标概览中，选择现有的备份目标或添加新的备份目标。
6. 选择下一步来查看您的更改。

从保护组中删除工作负载

稍后可能需要从现有保护组中删除工作负载。

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。



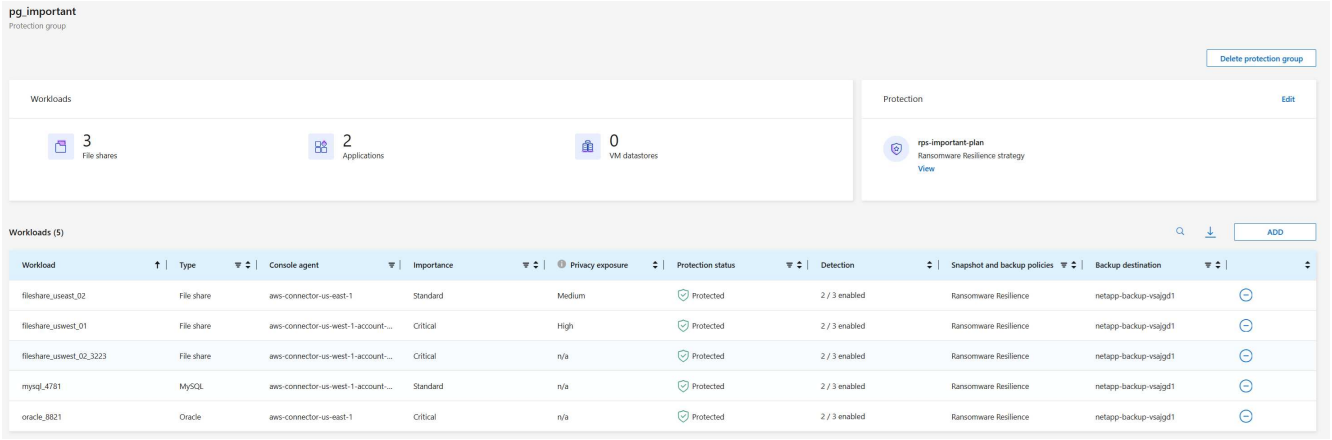
4. 从保护组页面中，选择要从组中删除的工作负载，然后选择 **Actions** ••• 选项。
5. 从“操作”菜单中，选择“删除工作负载”。
6. 确认您要删除工作负载并选择*删除*。

删除保护组

删除保护组时，Ransomware Resilience 会删除工作负载上的组和保护策略。它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*。

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：

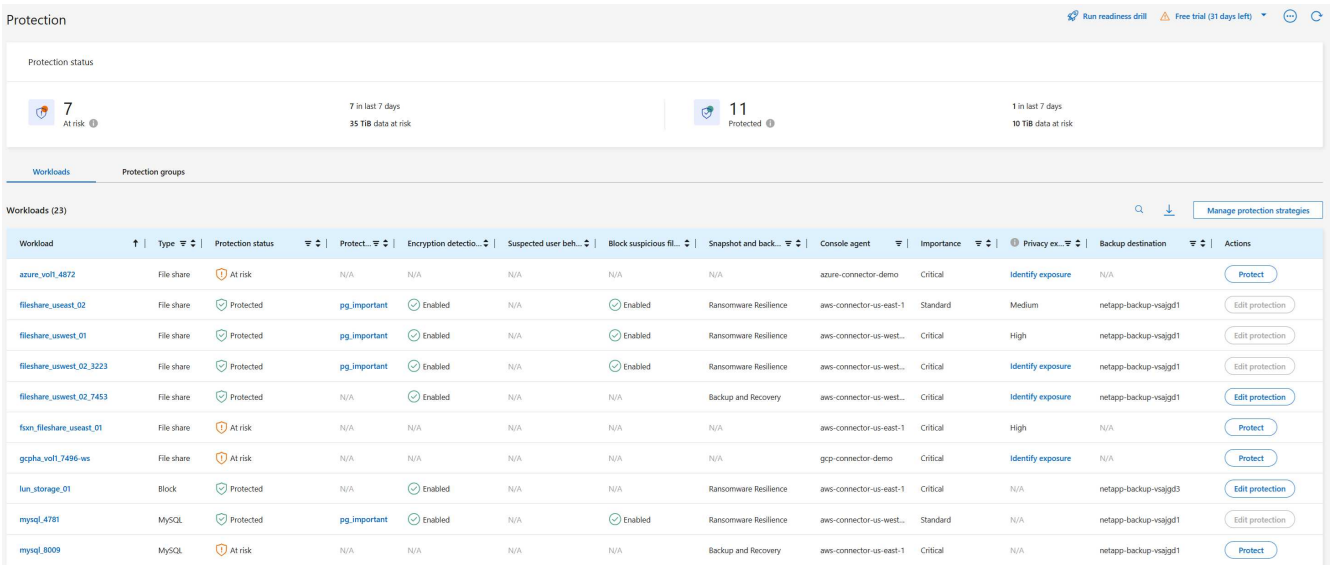
- "了解数据分类"
- "私人数据类别"
- "调查组织中存储的数据"

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

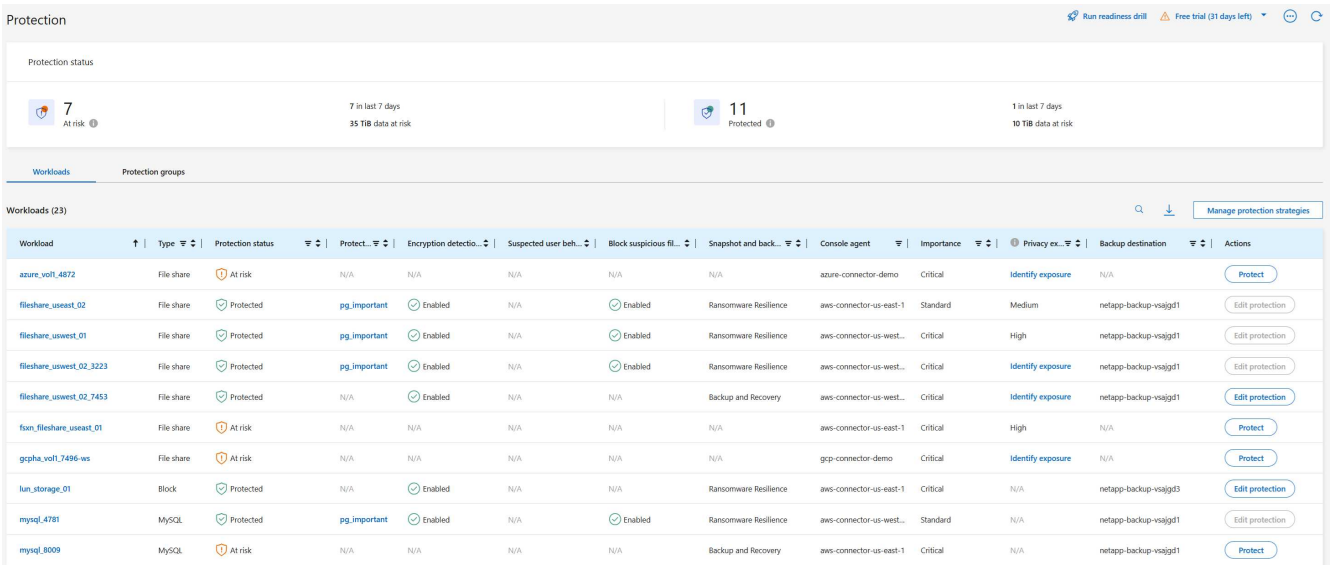
在对 PII 进行数据分类扫描后，评估风险。

PII 数据分为以下三类：

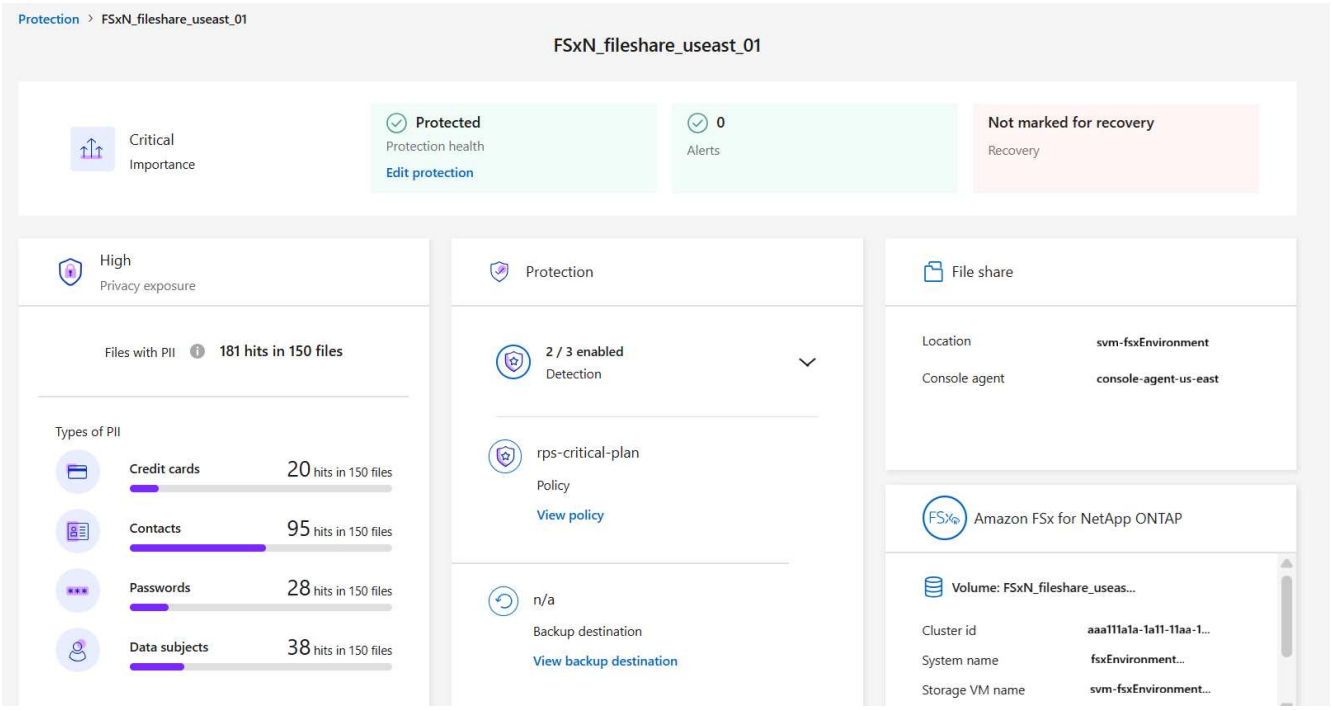
- 高：超过 70% 的文件包含 PII
- 中：超过 30% 且少于 70% 的文件包含 PII
- 低：大于 0% 且小于 30% 的文件包含 PII

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"

响应和恢复

在NetApp Ransomware Resilience中管理警报

当 NetApp Ransomware Resilience 检测到可能的攻击时，它会在仪表板和"通知"菜单中显示警报。Ransomware Resilience 立即拍摄快照。收到警报时，请查看 Ransomware Resilience *警报*选项卡中的潜在风险，以评估对数据的影响并防止潜在的勒索软件攻击。

如果 Ransomware Resilience 检测到可能的攻击，则会在 Console Notification 设置中显示通知，并向配置的地址发送电子邮件。电子邮件包括有关严重程度、受影响工作负载的信息，以及 Ransomware Resilience **Alerts** 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。

如何生成警报

Ransomware Resilience 依赖于有关数据熵模式、文件扩展名类型和加密的证据来生成警报。警报基于以下事件：

- 数据泄露
- 数据销毁

- 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
- 可疑的用户行为
- 当加密程度较高时，无需更改文件扩展名

对于数据泄露、数据销毁和可疑用户行为警报，必须配置 "用户活动检测"。

警报类型和状态

提醒具有两种状态之一：新建 或 未激活。

警报分为以下几种类型：

- 潜在攻击：警报在以下情况下被归类为潜在攻击：
  - Autonomous Ransomware Protection 检测到新的扩展，并且在过去 24 小时内重复发生超过 20 次（默认行为）。
  - 检测到数据泄露。
  - 检测到数据销毁。
- 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，警告仅基于高熵值。

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"。

警报状态

警报事件可以具有以下几种状态：

状态	描述
新的	所有事件在首次识别时都标记为"新"。
审核中	您可以在评估警报事件时将其手动标记为"审核中"。
已关闭	如果您怀疑该活动不是勒索软件攻击，则可以将状态更改为"已解除"。+ 注意：解除攻击后，无法恢复其状态。如果解除工作负载，则为响应潜在的勒索软件攻击而自动创建的所有快照副本都将被永久删除。
已解决	此事件已修复。
自动解决	对于低优先级警报，如果在五天内未采取任何行动，则会自动解决事件。

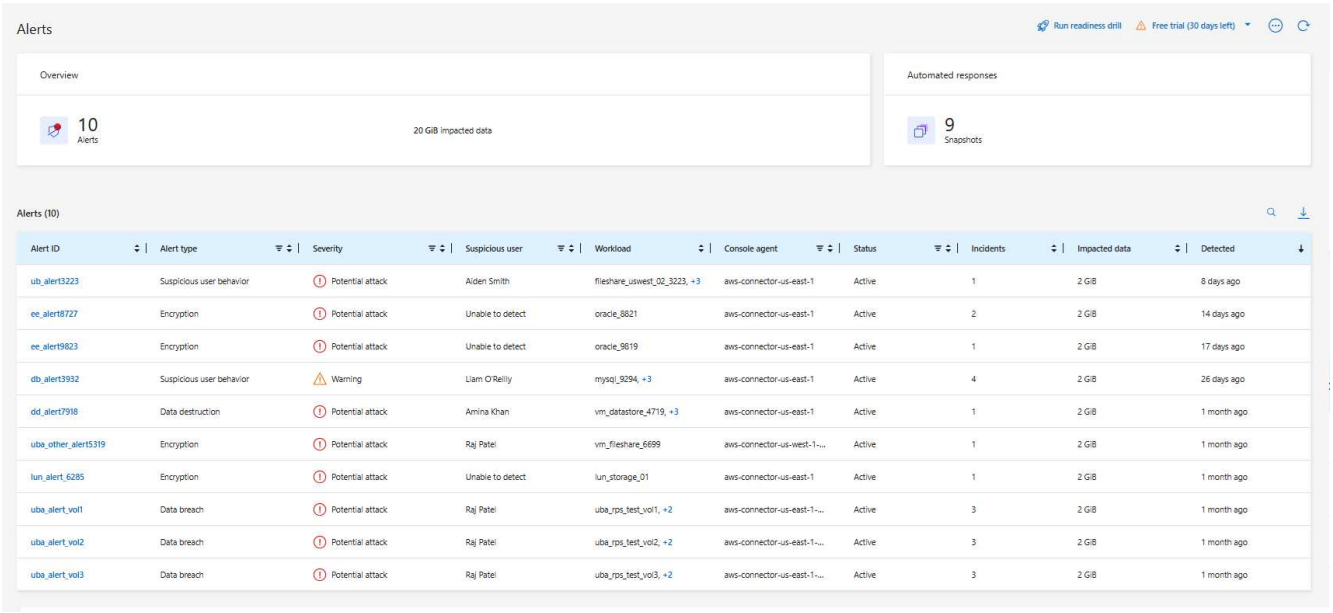
查看警报

您可以从 Ransomware Resilience 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 Ransomware Resilience 控制面板中，查看 Alerts 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 Ransomware Resilience 检测到潜在的攻击时，它会根据在 NetApp Console 设置中配置的订阅通知首选项向订阅用户发送电子邮件通知。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。

要在 Console 中设置电子邮件通知，请参见 "设置电子邮件通知设置"。

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 **View alert** 并登录到 Ransomware Resilience。

   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，请选择左上角面包屑中的“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。

必须已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。仅当启用了用户行为检测时，*可疑用户*列才会显示在警报仪表板中。要启用可疑用户检测，请参阅 "可疑的用户活动"。

查看恶意活动

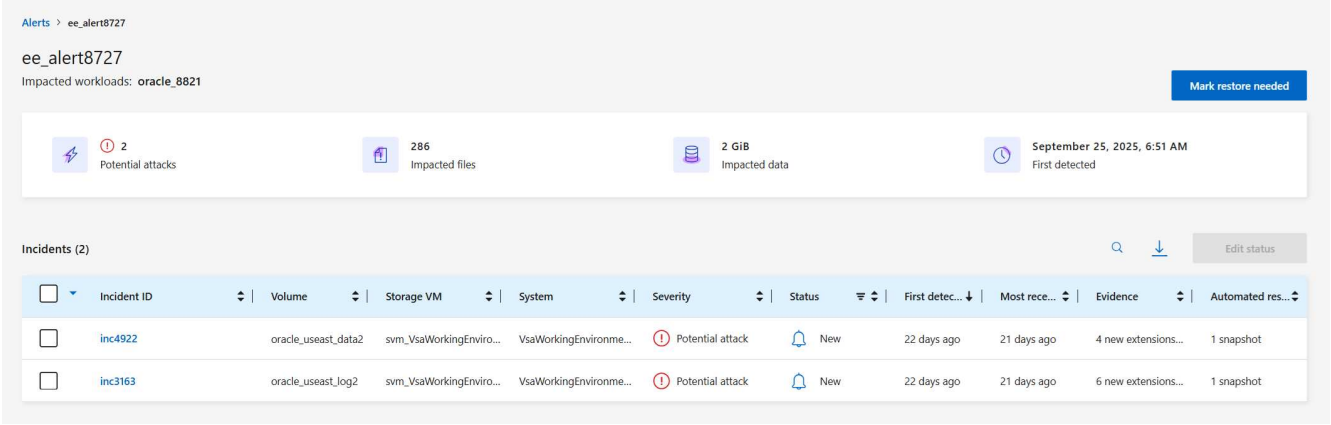
当 Autonomous Ransomware Protection 在 Ransomware Resilience 中触发警报时，您可以查看以下详细信息：

- 触发警报时
- 当访问权限被更改或拒绝时
- 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
- 受影响的工作负载、卷、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

如果您已将可疑用户检测配置为查看异常用户行为，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"为用户活动检测配置代理和收集器"。

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。
   a. 要阻止环境中的可疑用户，请选择用户名称旁边的 **Block**。
   b. 要禁用给定用户的警报，该用户是您知道是错误的警报的主题，请选择三个点 (...) ，然后将此用户排除在监控之外。查看对话框，然后选择排除进行确认。

要为用户重新启用警报，请返回警报。选择三个点，然后选择将此用户包含在监控中。您也可以"排除用户"监控。

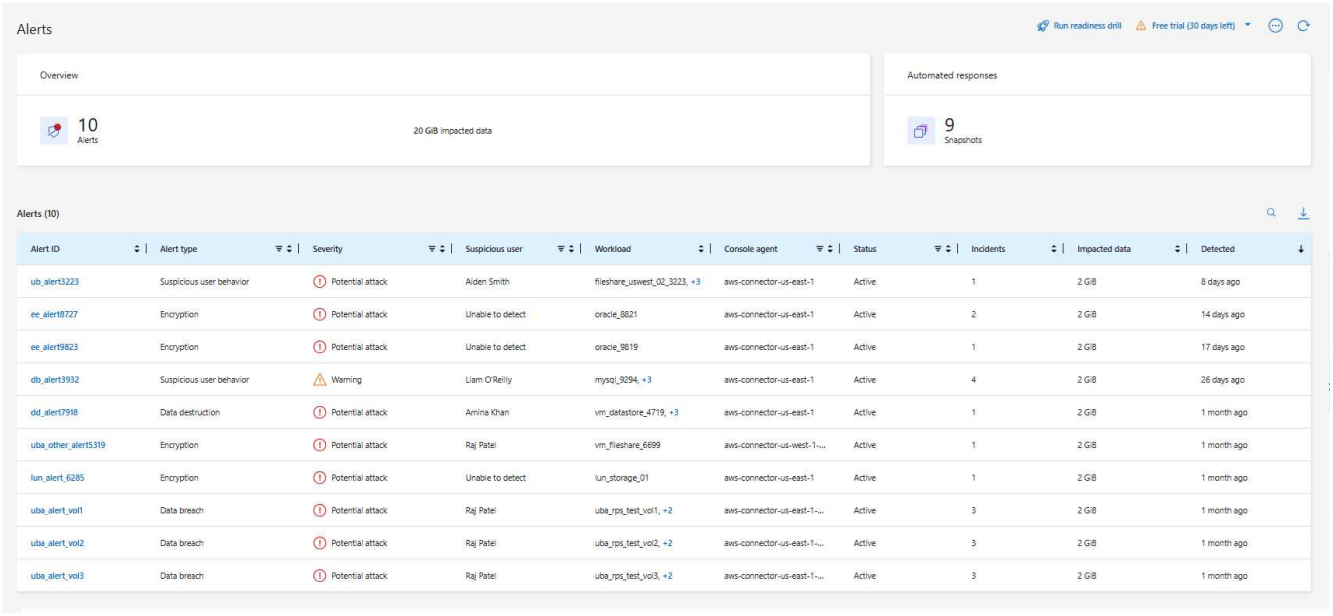
将勒索软件事件标记为准备恢复（事件被消除后）

停止攻击后，通知您的存储管理员数据已准备就绪，以便他们可以启动恢复过程。

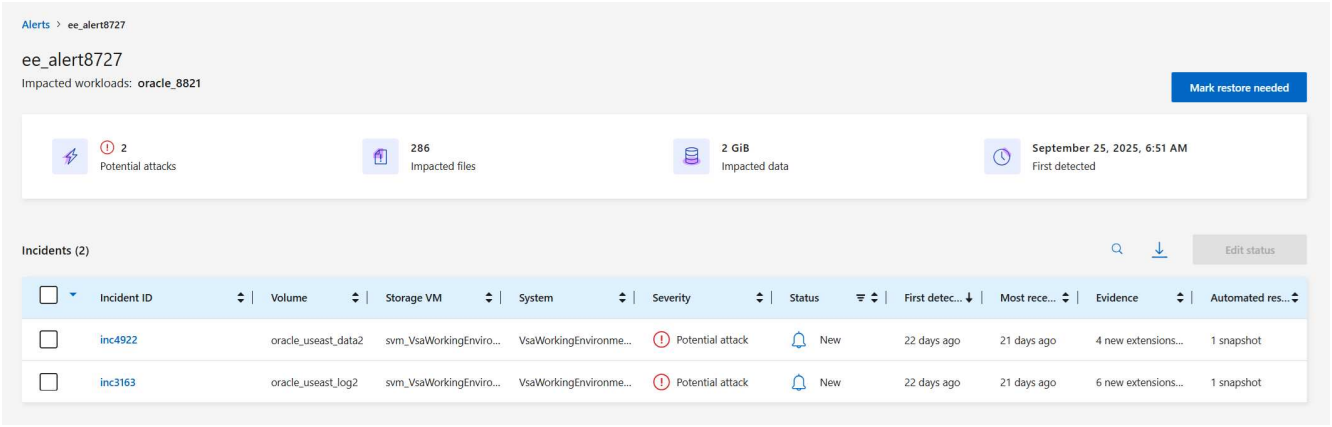
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

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。如果它们不构成实际威胁，就可以忽略不计。

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学习此行为并将其与正常操作关联起来，并且不会再次针对此类行为发出警报。

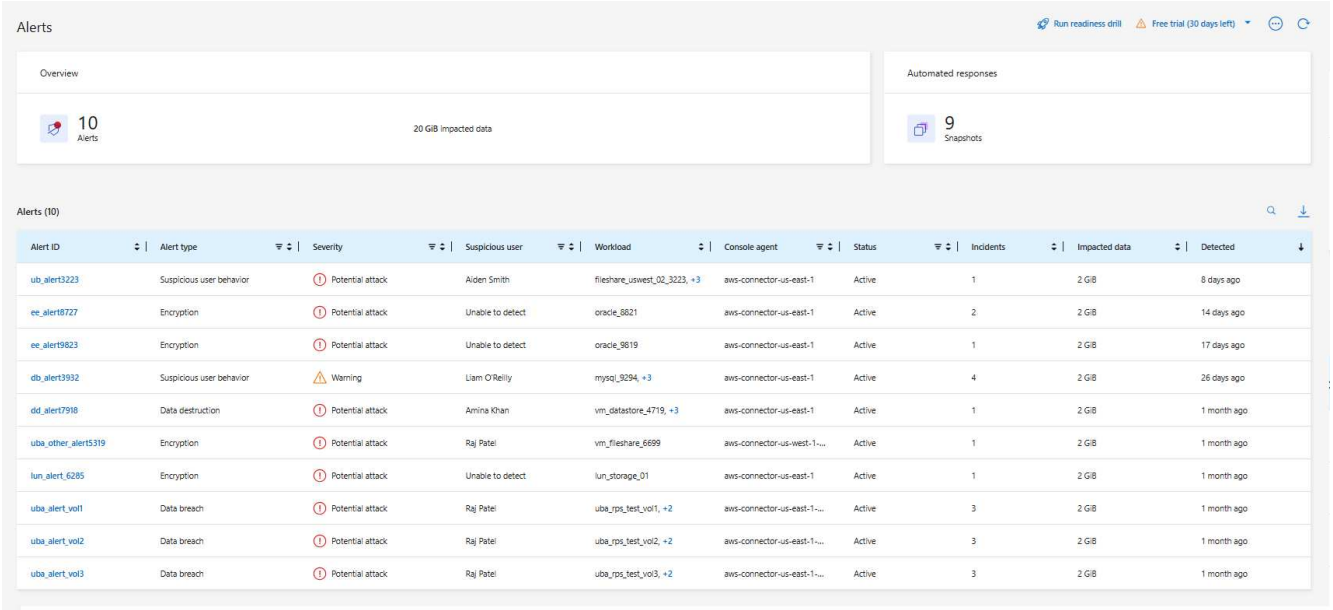
如果您解除工作负载，则为应对潜在勒索软件攻击而自动获取的所有快照副本都将被永久删除。

如果您关闭警报，则无法更改其状态或撤消此更改。

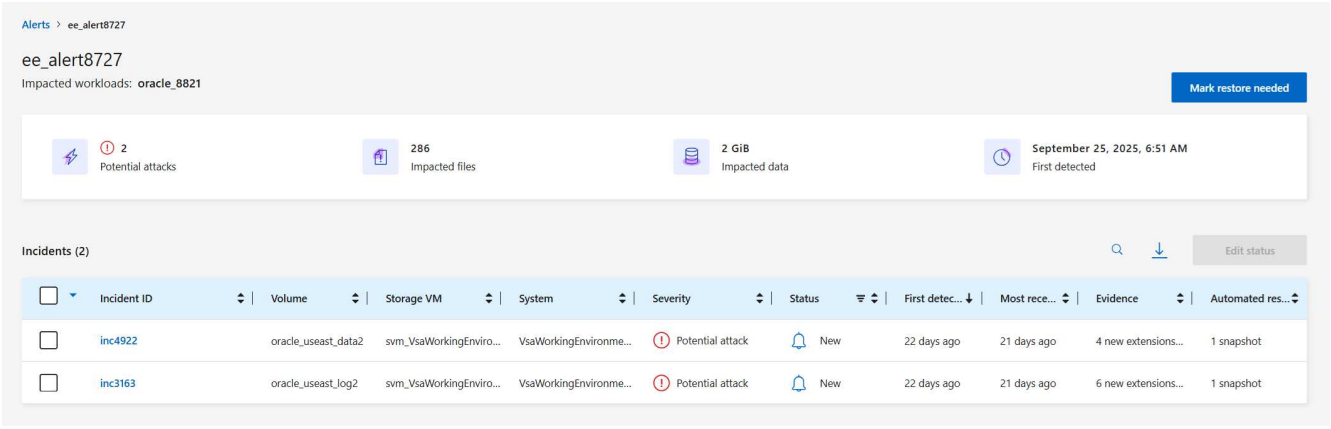
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

步骤

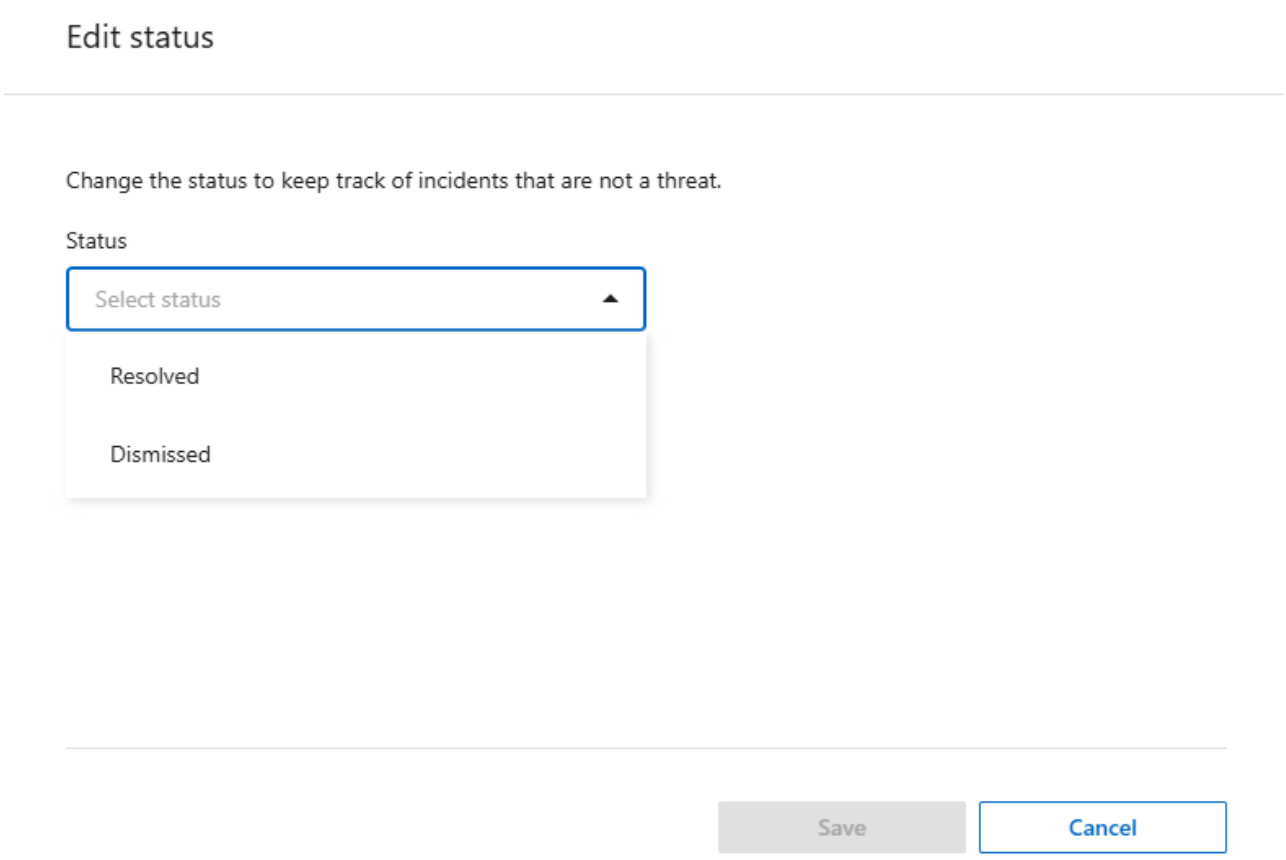
1. 从勒索软件恢复菜单中，选择*警报*。



2. 在警报页面中，选择警报。



3. 选择一个或多个事件。或者，选择表格左上角的“事件 ID”框，即可选择所有事件。
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. 在“编辑状态”框中，选择“已解雇”状态。

   显示了有关工作负载和快照副本被删除的更多信息。

6. 选择*保存*。

   事件状态更改为“已驳回”。

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" 。

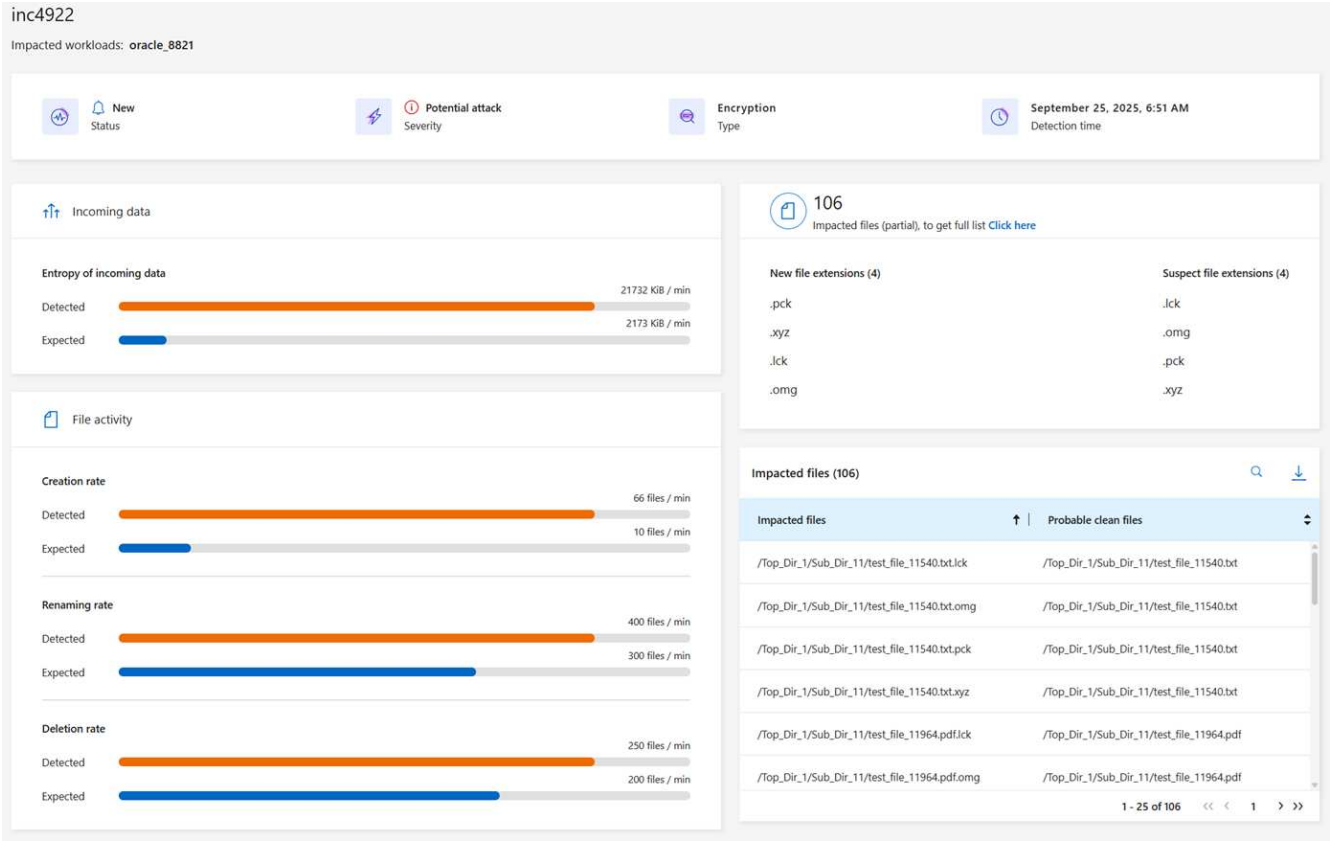
步骤

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 NetApp Backup and Recovery 或 Ransomware Resilience 管理，则 Ransomware Resilience 执行崩溃一致性恢复，例如，如果系统崩溃，则在同一时间点还原卷中的所有数据。

  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：

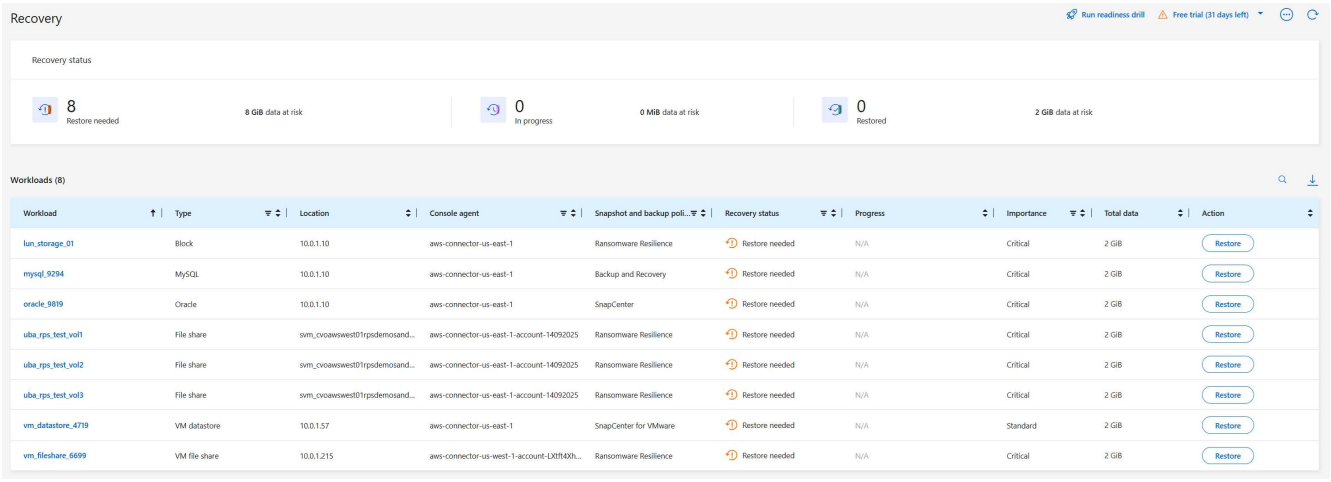
- 需要恢复：需要恢复工作负载。
- 进行中：恢复操作目前正在进行中。
- 已恢复：工作量已恢复。
- 失败：工作负载恢复过程无法完成。

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：
   - 在控制面板中，查看"提醒"窗格中的"恢复所需"总计，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。

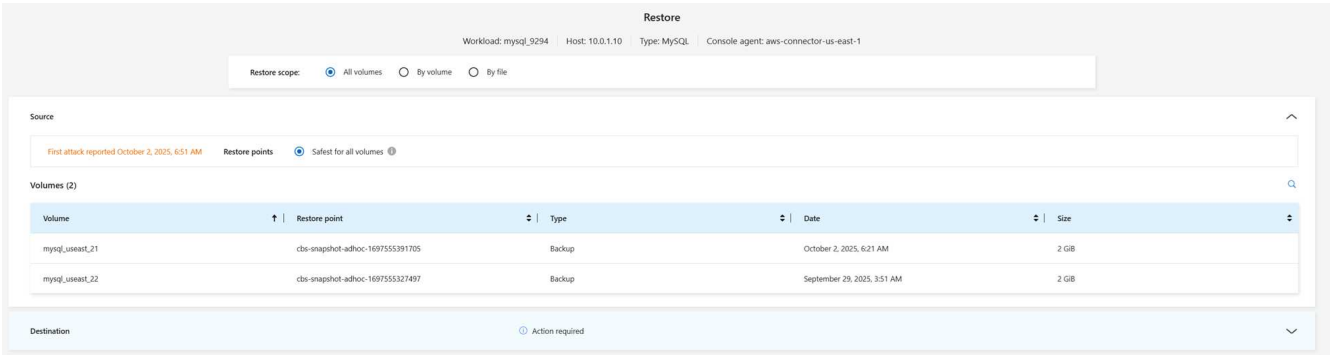
对于 SAN 工作负载，您只能按工作负载进行恢复。

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。

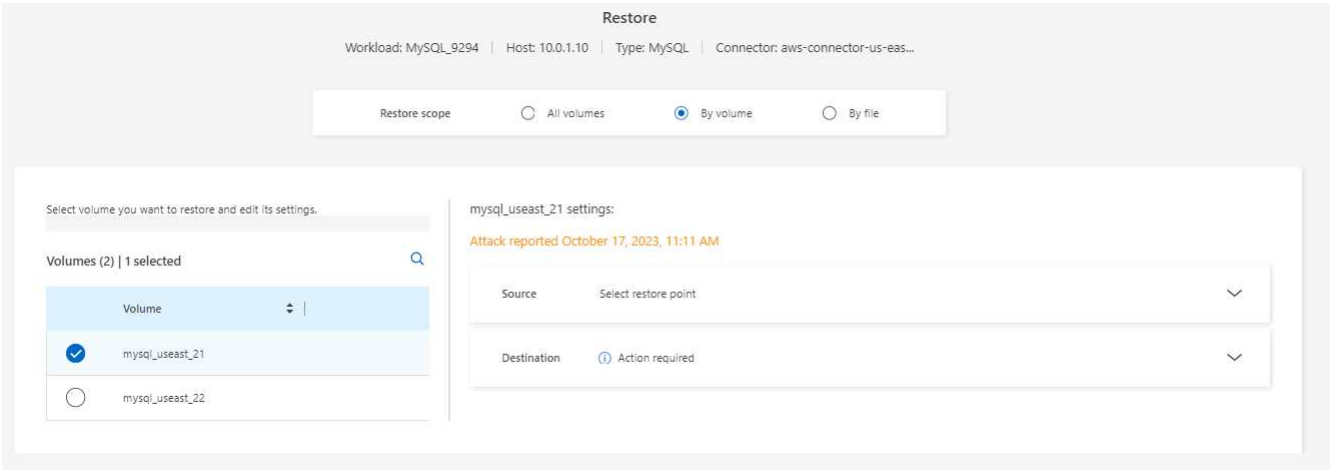
新卷名称显示为前缀+原始卷名称+备份名称+备份日期。

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。

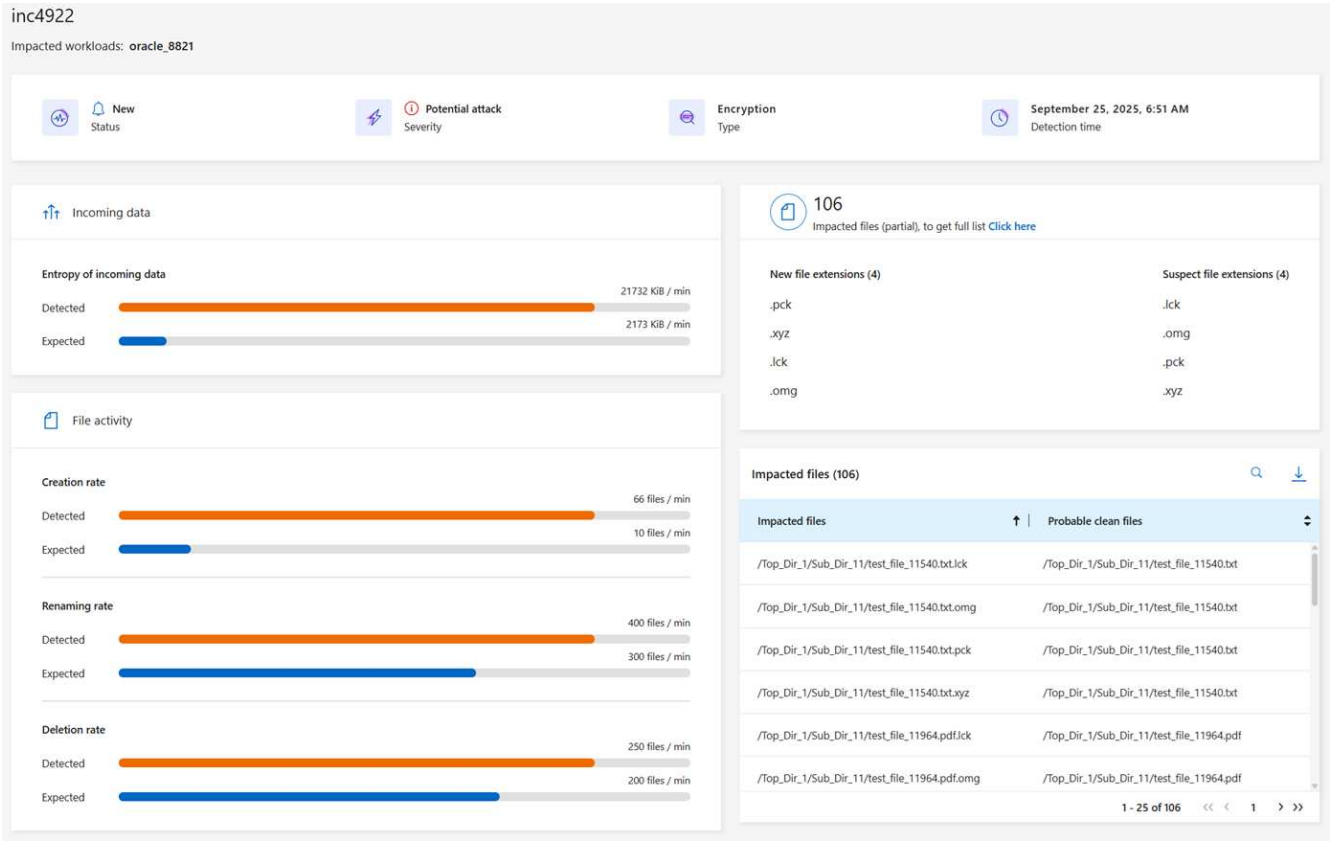
您可以将文件级别的应用程序工作负载还原到相同或不同的系统。

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。

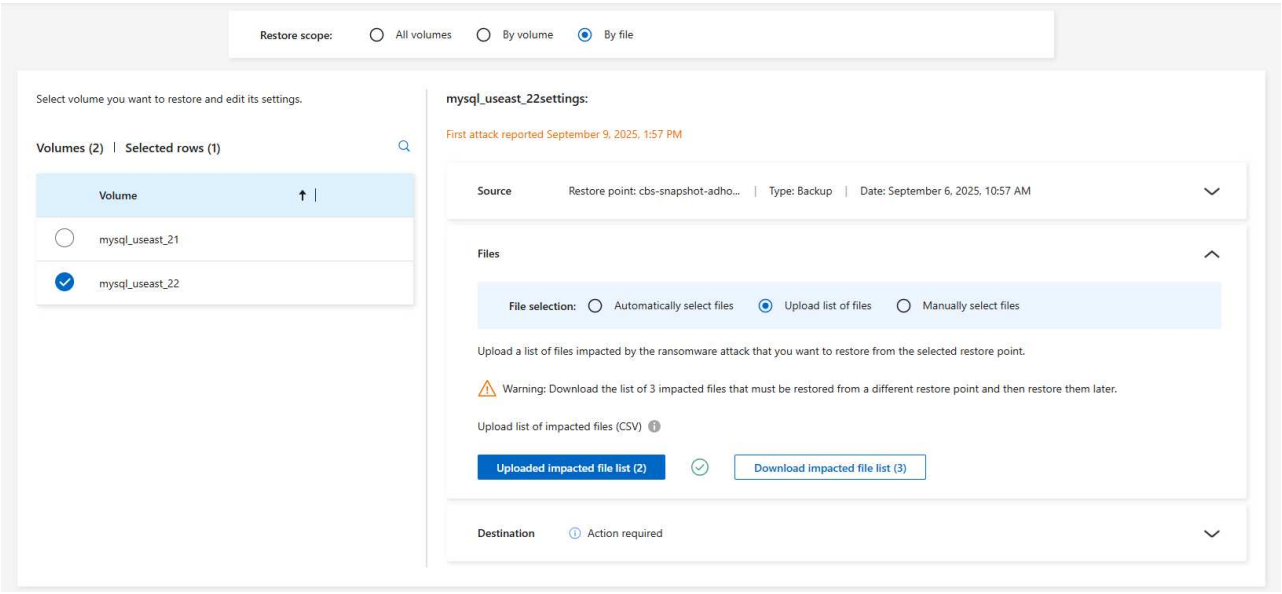
恢复这些文件的步骤

1. 从勒索软件恢复菜单中，选择*恢复*。

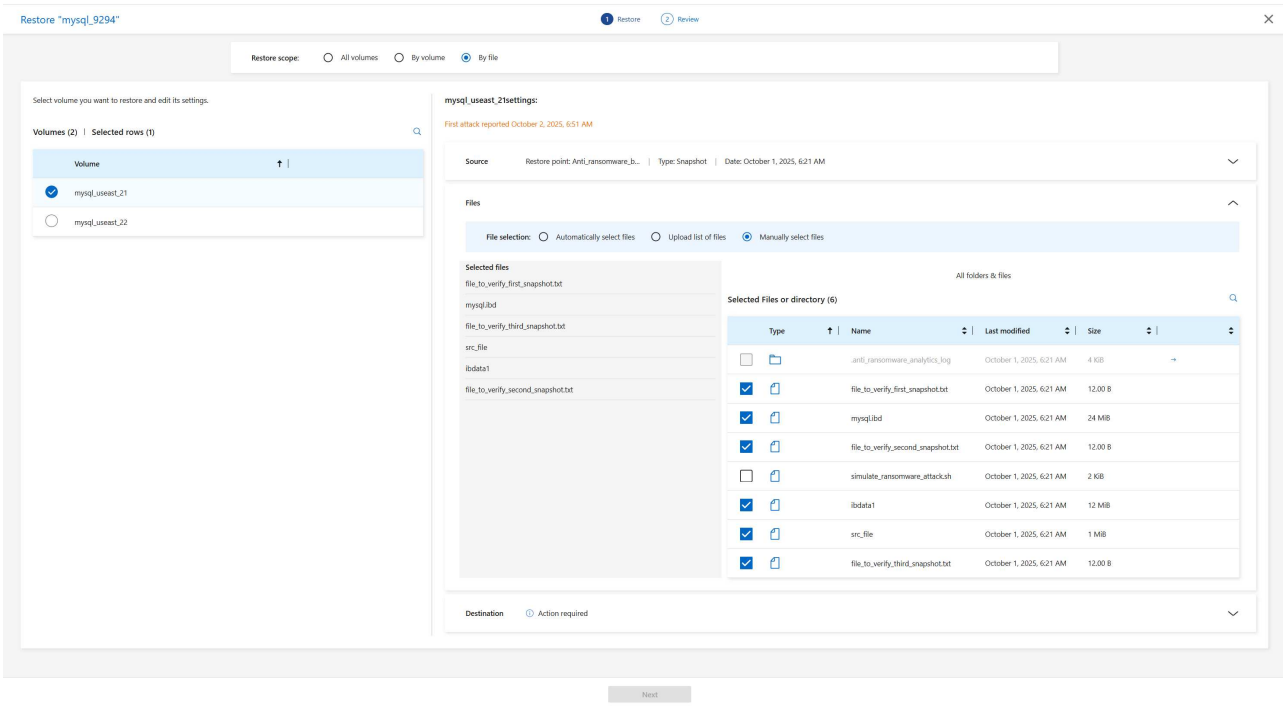
2. 选择处于“需要恢复”状态的应用程序工作负载。
3. 要恢复，请选择*恢复*。
4. 在“还原”页面的“还原范围”中，选择“按文件”。
5. 在卷列表中，选择包含要还原的文件的卷。
6. 还原点：选择*还原点*旁边的向下箭头查看详细信息。选择要用于还原数据的还原点。

   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。

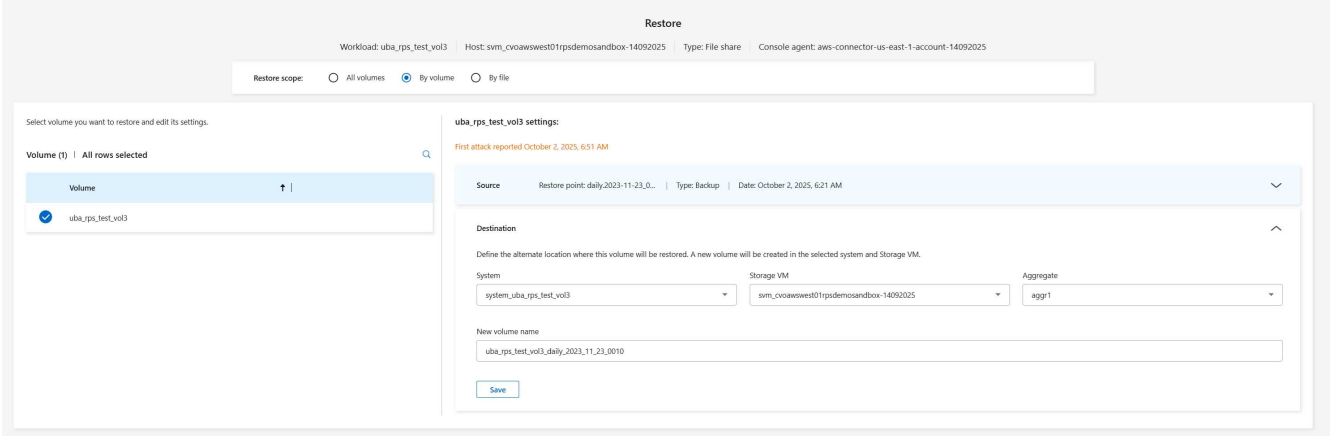
   b. 选择系统。
   c. 选择存储虚拟机。
   d. （可选）输入路径。

      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。

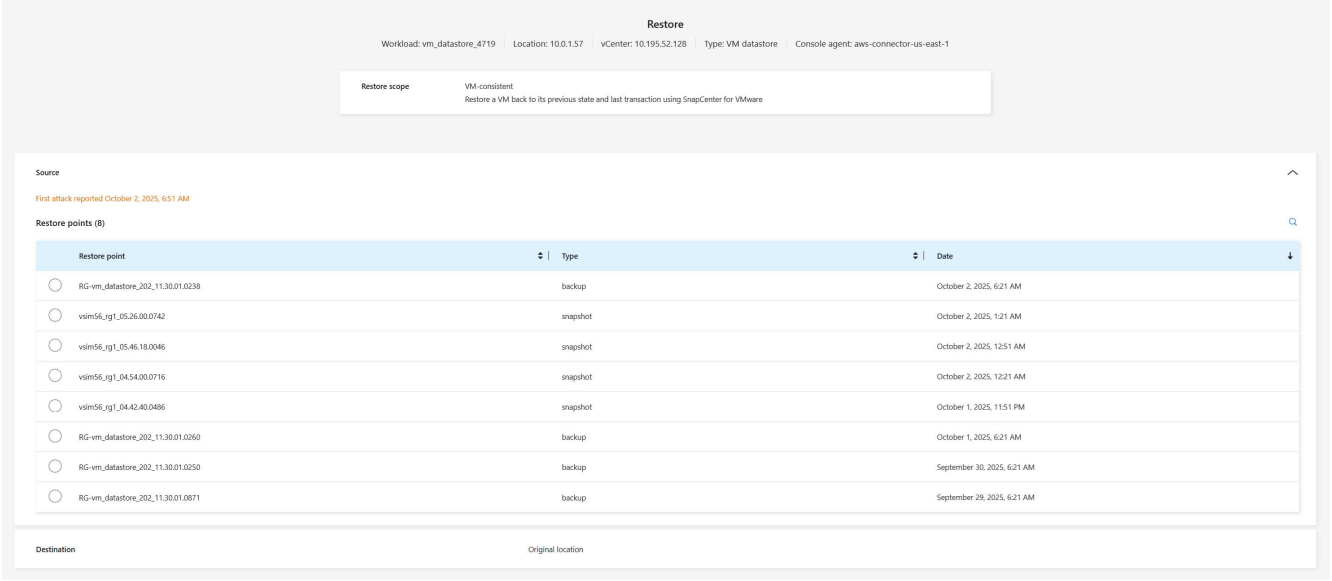
   如果您没有指定还原路径，文件将被还原到顶级目录的新卷。

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。

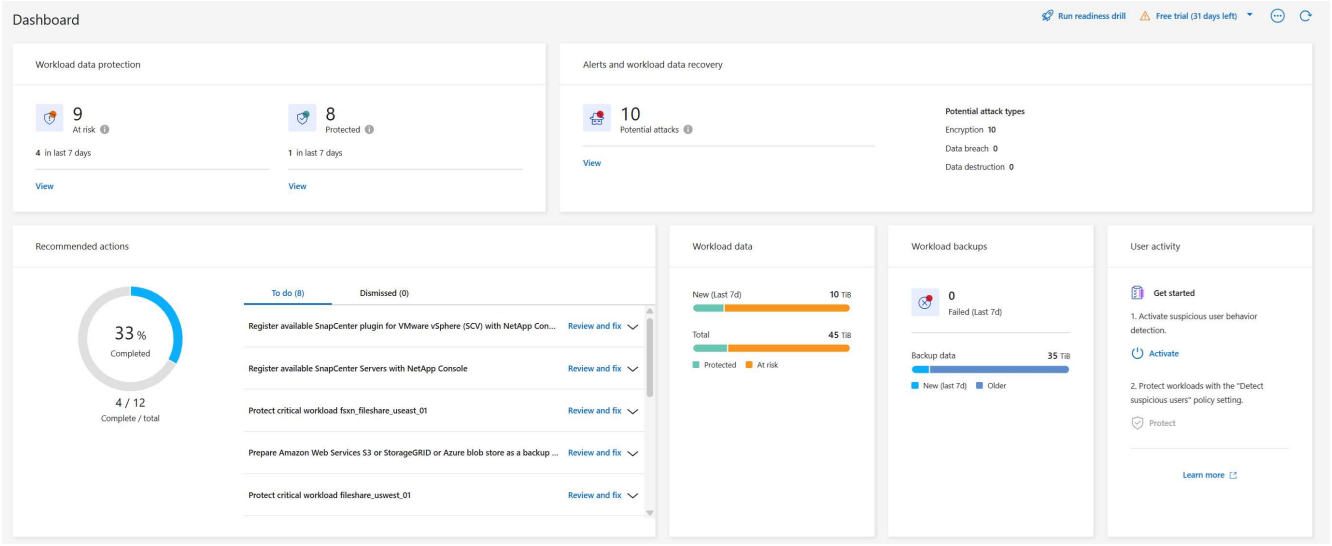
以下情况需要输入用户名和密码：

- 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" 。

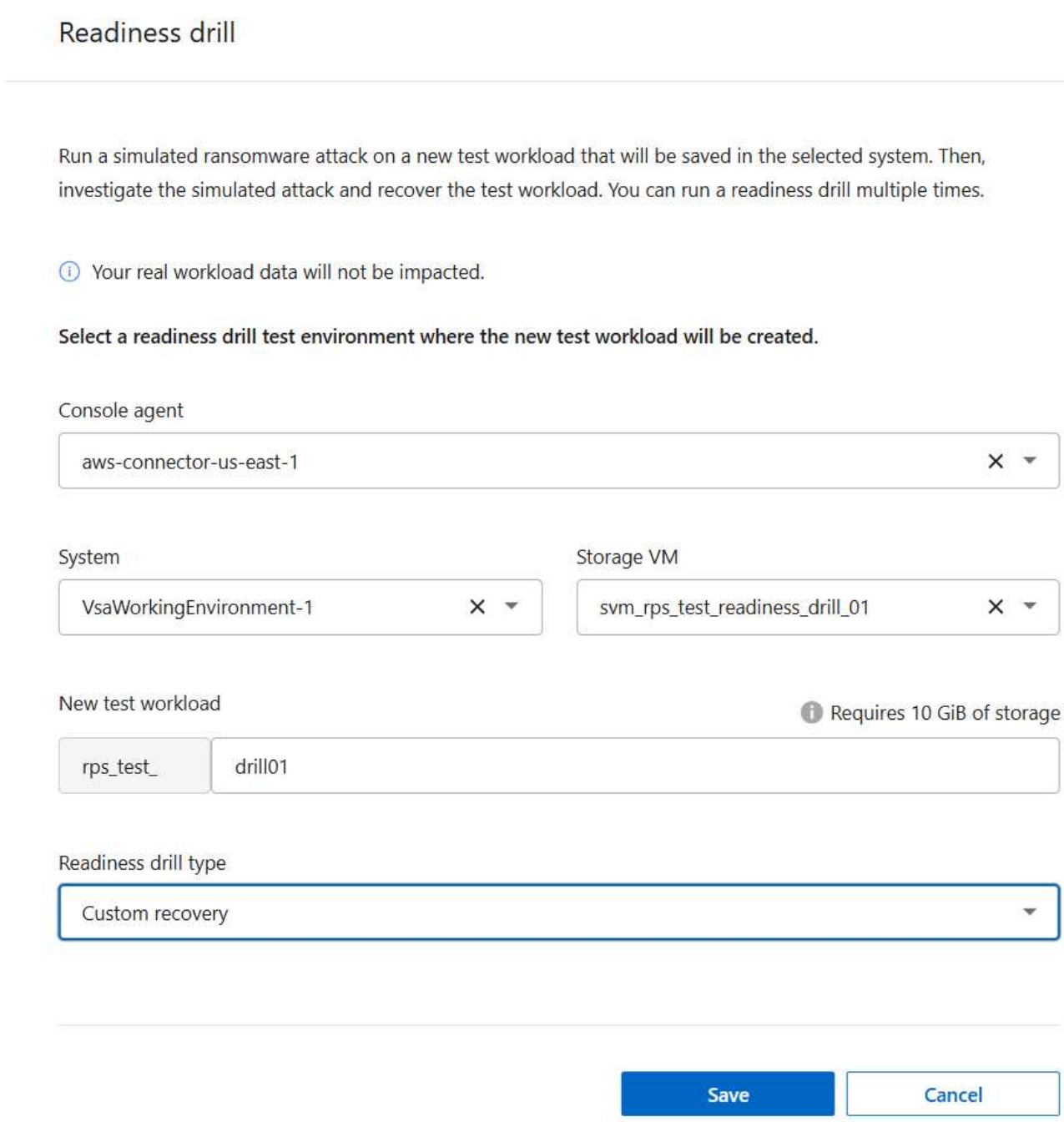
步骤

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。

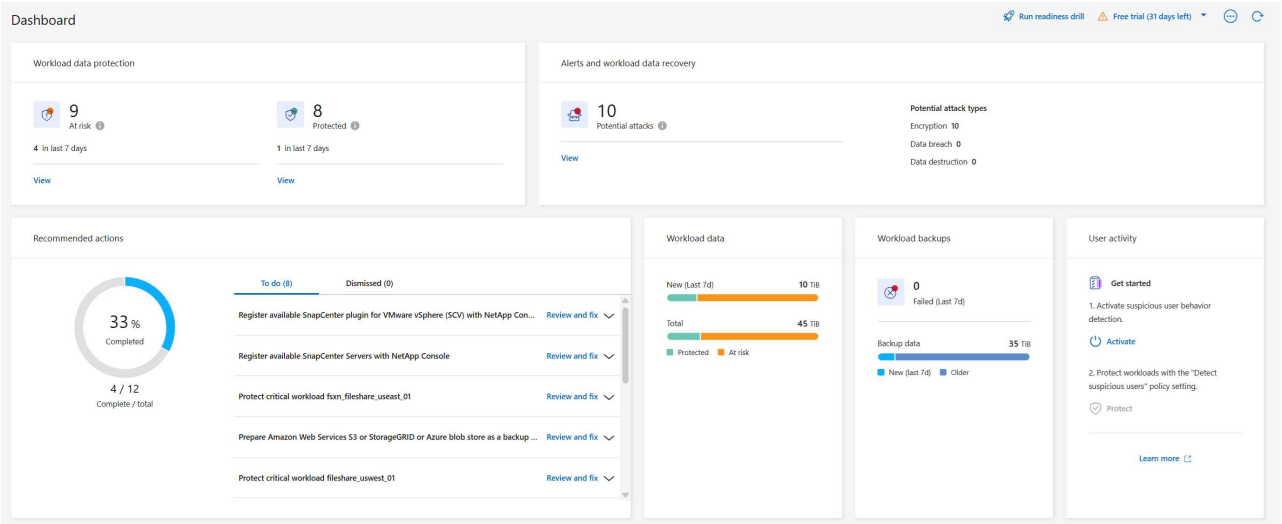
所需的控制台角色 要执行此任务，您需要组织管理员、文件夹或项目管理员或勒索软件恢复管理员角色。"了解NetApp Console的勒索软件恢复角色" 。

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

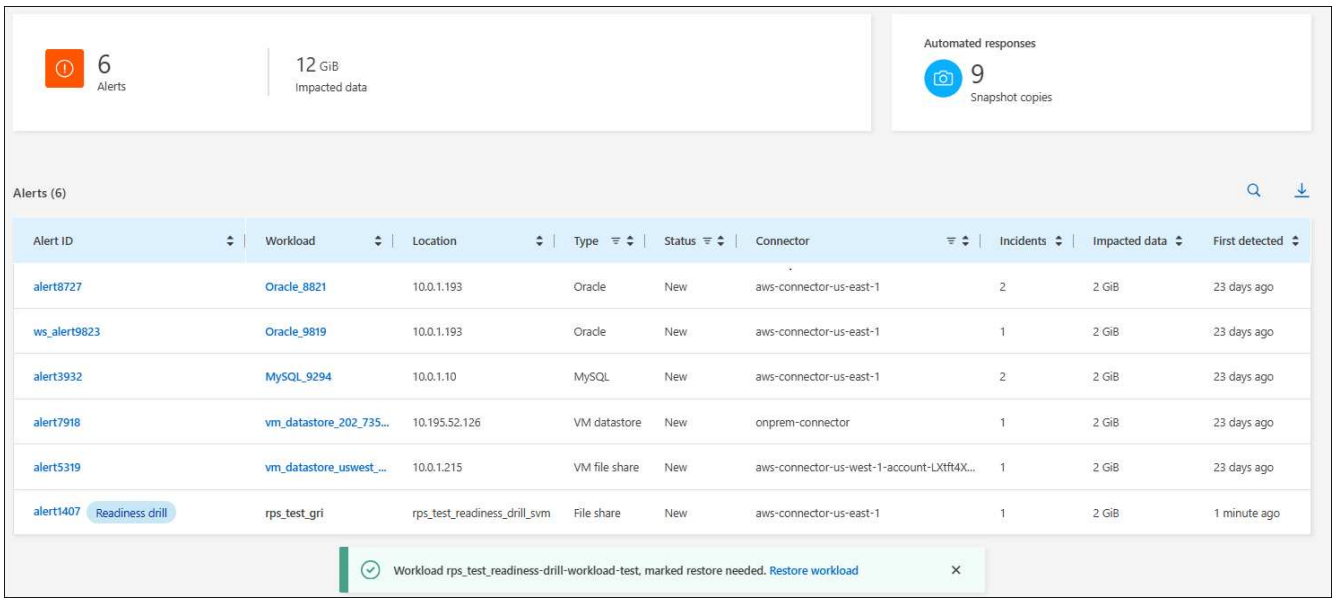
通过响应准备演习警报来测试您的准备情况。

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" 。

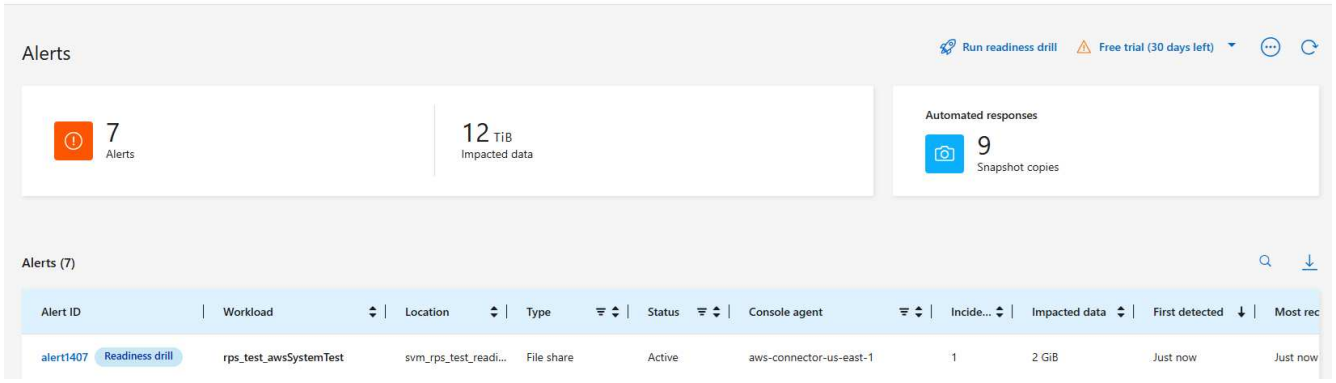
步骤

1. 从勒索软件恢复菜单中，选择*警报*。

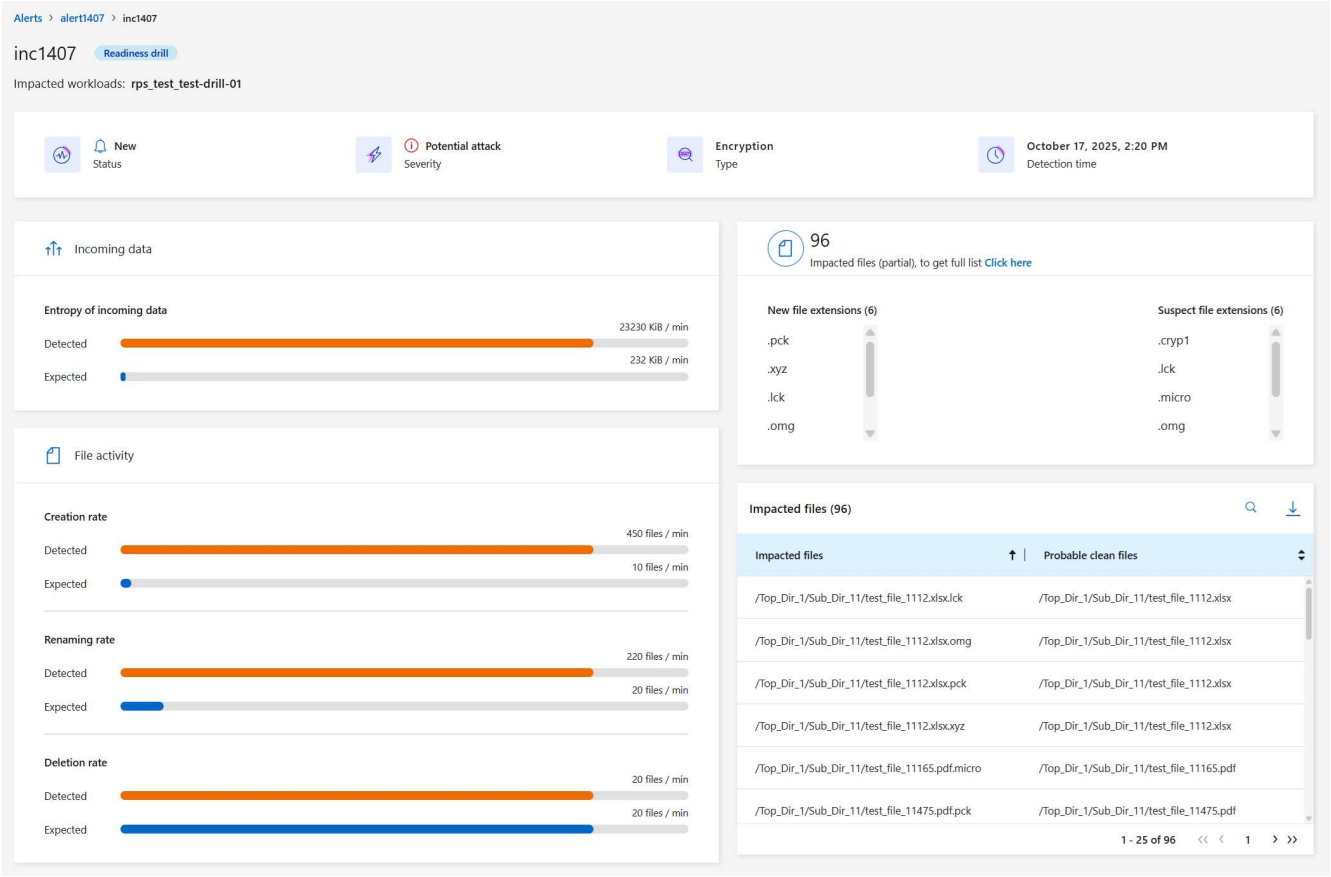
控制台显示警报页面。在警报 ID 列中，您会在 ID 旁边看到“准备情况演练”。



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。

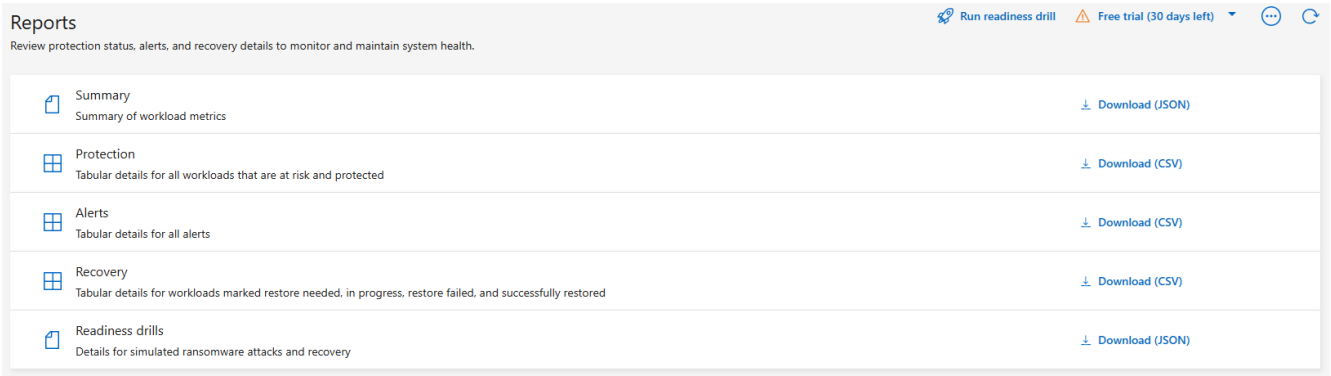
审查准备演习报告

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。

将 NetApp Ransomware Resilience 连接到安全和事件管理系统 (SIEM)，以进行威胁分析和检测

安全和事件管理系统 (SIEM) 集中日志和事件数据，以提供有关安全事件和合规性的见解。NetApp Ransomware Resilience 支持自动将数据发送到您的 SIEM，以简化威胁分析和检测。

Ransomware Resilience 支持以下 SIEM：

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

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

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，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，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. 选择 **Authenticate**。

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。

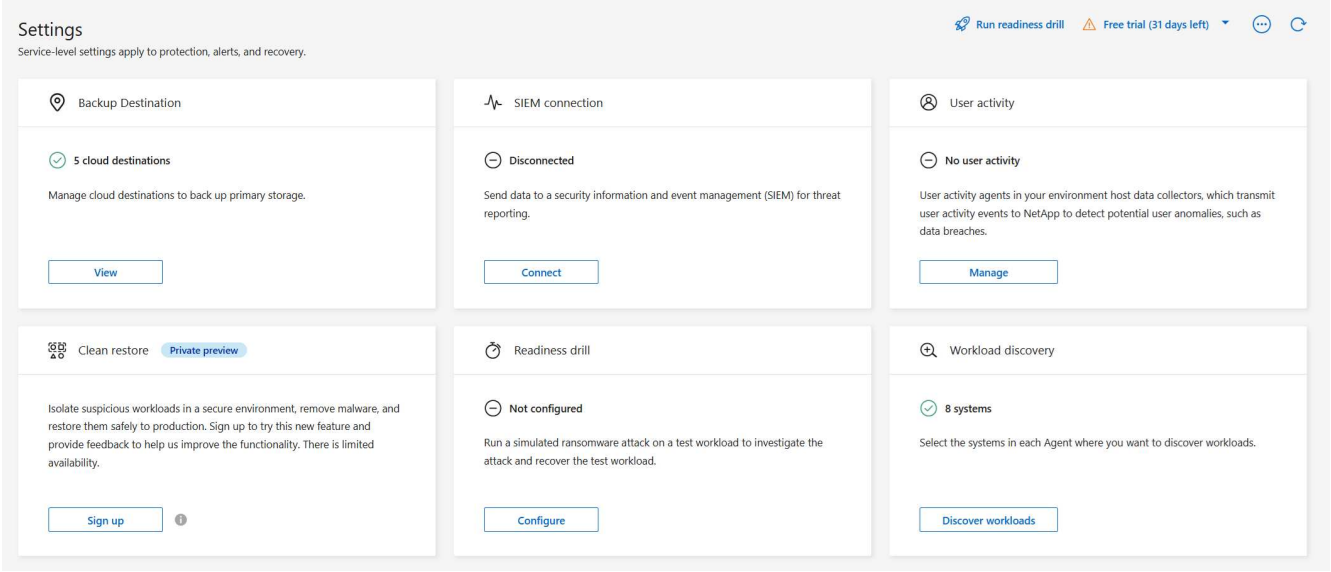
在勒索软件防御中连接 **SIEM**

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中下载报告

NetApp Ransomware Resilience 以 CSV 和 JSON 格式提供报告，显示受支持和不受支持卷的详细信息、攻击准备演练、保护、警报和恢复。使用报告，您可以保存和查看有关演练、保护状态、警报和恢复事件的离线报告。

下载文件之前，请刷新仪表盘以获取报告中的最新数据。

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：

- 摘要：包括受支持和不受支持的工作负载列表、改善网络弹性态势的建议措施，以及勒索软件弹性仪表板中捕获的信息。
- 保护：包括所有工作负载的状态和详细信息，包括受保护的工作负载总数和面临风险的工作负载总数。
- 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。

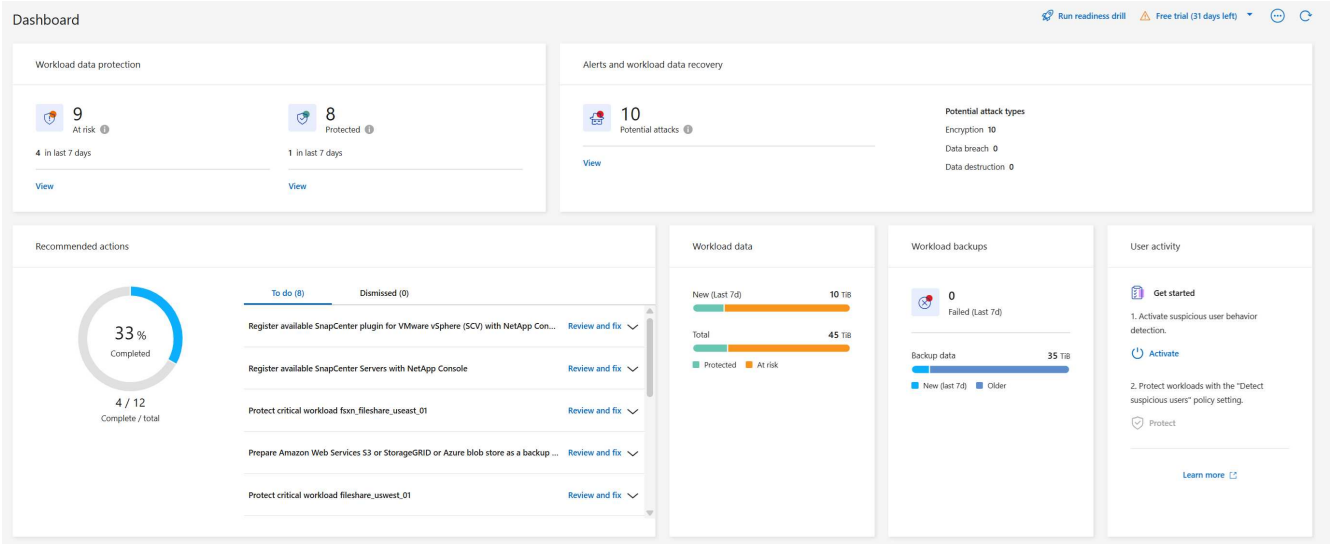
您只能从*报告*页面下载准备情况演习报告。

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. 在控制面板或其他页面中，选择右上角的 刷新 选项以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”。