



保护工作负载 NetApp Ransomware Resilience

NetApp
February 19, 2026

目录

保护工作负载	1
在 NetApp Ransomware Resilience 中查看防护状态	1
查看工作负载的保护	1
了解保护信息板	2
后续步骤	2
使用 NetApp Ransomware Resilience 保护策略保护工作负载	3
了解勒索软件防护策略	3
添加勒索软件防护策略	5
管理勒索软件防护策略	10
在 NetApp Ransomware Resilience 中管理保护组	11
创建保护组	11
从保护组中删除工作负载	13
删除保护组	14
使用勒索软件恢复中的 NetApp Data Classification 扫描个人信息	15
通过数据分类识别隐私暴露	15
审查隐私暴露情况	16
隐私暴露对工作负载重要性的影响	17
了解更多信息	18

保护工作负载

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：
 - 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*。

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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"](#)

- ["扫描个人信息"](#)

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、文件夹或项目经理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

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
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
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*。

The screenshot displays the 'Protection status' dashboard. It shows two summary cards: one for 'At risk' with 9 items and 35 TiB data at risk, and another for 'Protected' with 9 items and 10 TiB data at risk. Below this is a table of workloads with 19 items. The table has columns for Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u, and Actions.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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*。

Add Ransomware Resilience strategy

Ransomware Resilience strategy name

Copy from existing Ransomware Resilience strategy

No policy selected
Select

Detection	1 / 3 enabled	▼
Snapshot policy	Action required	▼
Backup policy	None	▼

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 **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*。

The screenshot shows a dashboard with a 'Protection status' section at the top. It displays two metrics: 'At risk' (9 items, 35 TiB data at risk) and 'Protected' (9 items, 10 TiB data at risk). Below this is a table of workloads with columns for Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u..., and Actions.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u...	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. 在“保护”页面中，选择一工作负载，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*。

The screenshot shows a dashboard for Protection status. At the top, there are two summary cards: 'At risk' with 9 items and 'Protected' with 9 items. Below this is a 'Workloads' section with a table of 19 workloads. The table has columns for Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u, and Actions. The workloads listed are FSxN_fileshare_useast_01 (At risk), LUN_storage_01 (Protected), MySQL_4781 (Protected), MySQL_8009 (At risk), MySQL_9294 (Protected), and Oracle_2115 (At risk).

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. 在“保护”页面中，选择个工作负载，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。

Ransomware Resilience strategies (4) | Selected rows (1) Add

Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
<input checked="" type="radio"/> rps-standard-plan Recommended	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0
<input type="radio"/> rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0

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*。

在 NetApp Ransomware Resilience 中管理保护组

NetApp Ransomware Resilience 提供保护组，以便更轻松的管理您的数据资产。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*。

Protection status

9 At risk 9 in last 7 days 35 TiB data at risk

9 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransoware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransoware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

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

Workloads Protection groups

Protection group (1)

Protection group	Protection status	Ransomware Resilience strategy	Protected count
pg_important	Protected	rps-important-plan	2 / 2

3. 选择“添加”。

Workloads

Select workloads to add to the protection group.

Protection group name

NetRansomwareOnThisFileShare

Workloads (17) | Selected rows (2)

Select workloads with no other policy source or with Backup and Recovery as a policy source.

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
azure_vol1_4872	File share	azure-connector-demo	Critical	n/a	At risk	N/A	N/A	N/A
fileshare_uswest_02_7453	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsajgd1
fsan_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	N/A	N/A	N/A
gcpsha_vol1_7496-ws	File share	gcp-connector-demo	Critical	n/a	At risk	N/A	N/A	N/A
lun_storage_01	Block	aws-connector-us-east-1	Critical	n/a	Protected	1 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd3
mysql_8009	MySQL	aws-connector-us-east-1	Critical	n/a	At risk	N/A	Backup and Recovery	netapp-backup-vsajgd1
mysql_9294	MySQL	aws-connector-us-east-1	Critical	n/a	Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsajgd3
oracle_2115	Oracle	aws-connector-us-east-1	Critical	n/a	At risk	N/A	SnapCenter	netapp-backup-vsajgd1

Next

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”。

Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
<input type="radio"/> rps-standard-plan	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0

Frequency	Snapshot copies	Retention
hourly	Every 1 hours	72
daily	Every 1 day	14
weekly	Every Fri of week	5
monthly	Every Jan, Feb, Mar, Apr, May, Jun...	2

Frequency	Retention
daily	14
weekly	5
monthly	3

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。

- 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

- 从勒索软件恢复菜单中，选择*保护*。
- 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。
- 从保护组的概览页面中，选择“编辑保护”。
- 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](#)。
- 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。
- 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。

pg_important
Protection group

Workloads

3 File shares, 2 Applications, 0 VM datastores

Protection: rps-important-plan Ransomware Resilience strategy

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_uswest_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_01	File share	aws-connector-us-west-1-account...	Critical	High	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_02_3223	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
mysql_4781	MySQL	aws-connector-us-west-1-account...	Standard	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1

4. 从保护组页面中，选择要从中删除的工作负载，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。

pg_important
Protection group

Workloads

3 File shares, 2 Applications, 0 VM datastores

Protection: rps-important-plan Ransomware Resilience strategy

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_uswest_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_01	File share	aws-connector-us-west-1-account...	Critical	High	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
fileshare_uswest_02_3223	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
mysql_4781	MySQL	aws-connector-us-west-1-account...	Standard	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsajgd1

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、文件夹或项目经理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。

Protection

Protection status

7 At risk 7 in last 7 days 35 TiB data at risk 11 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (23)

Workload	Type	Protection status	Protect...	Encryption detecto...	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_vofl_4872	File share	At risk	N/A	N/A	N/A	N/A	N/A	azure-connector-demo	Critical	Identify exposure	N/A	Protect
fileshare_useest_02	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_01	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_3223	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fsxn_fileshare_useast_01	File share	At risk	N/A	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	Protect
gcpa_vofl_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	Protect
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd3	Edit protection
mysql_4781	MySQL	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsajgd1	Edit protection
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd1	Protect

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。

Protection

Protection status

7 At risk 7 in last 7 days 35 TiB data at risk 11 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (23)

Workload	Type	Protection status	Protect...	Encryption detecto...	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_voil_4872	File share	At risk	N/A	N/A	N/A	N/A	N/A	azure-connector-demo	Critical	Identify exposure	N/A	Protect
fileshare_useast_02	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_01	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_3223	File share	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fsxn_fileshare_useast_01	File share	At risk	N/A	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	Protect
gcpa_voil_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	Protect
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd3	Edit protection
mysql_4781	MySQL	Protected	pg_important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsajgd1	Edit protection
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd1	Protect

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。

Protection > FSxN_fileshare_useast_01

FSxN_fileshare_useast_01

Critical Importance

Protected Protection health Edit protection

0 Alerts

Not marked for recovery Recovery

High Privacy exposure

Files with PII 181 hits in 150 files

Types of PII

- Credit cards 20 hits in 150 files
- Contacts 95 hits in 150 files
- Passwords 28 hits in 150 files
- Data subjects 38 hits in 150 files

Protection

2 / 3 enabled Detection

rps-critical-plan Policy View policy

n/a Backup destination View backup destination

File share

Location svm-fsxEnvironment

Console agent console-agent-us-east

Amazon FSx for NetApp ONTAP

Volume: FSxN_fileshare_useas...

Cluster id aaa111a1a-1a11-11aa-1...

System name fsxEnvironment...

Storage VM name svm-fsxEnvironment...

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"](#)

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 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。