保护工作负载

BlueXP ransomware protection

NetApp
October 07, 2024

目录

保护工作负载

利用勒索软件策略保护工作负载

您可以通过使用BlueXP勒索软件保护完成以下操作来保护工作负载免受勒索软件攻击。

- 启用工作负载一致的保护、此功能可与适用于VMware vSphere的SnapCenter软件或SnapCenter插件结合使用。
- 创建或管理勒索软件保护策略、其中包括您为快照、备份和勒索软件保护创建的策略(称为_detection policies_)。
- 导入策略并进行调整。
- 对文件共享进行分组、使您可以更轻松地保护工作负载、而不是逐个进行保护。
- 删除勒索软件保护策略。

*哪些服务用于保护？*以下服务可用于管理保护策略。来自这些服务的保护信息显示在BlueXP 勒索软件保护中：

- 为文件共享、VM文件共享提供BlueXP 备份和恢复
- 适用于VMware的VM数据存储库SnapCenter
- 适用于Oracle和MySQL的SnapCenter

保护策略

您可能会发现、查看有关可以更改的保护策略以及保护策略中的策略类型的信息会很有帮助。

您可以更改哪些保护策略?

您可以根据所拥有的工作负载保护更改保护策略：

- 不受**NetApp**应用程序保护的工作负载：这些工作负载不受SnapCenter、适用于VMware vSphere的SnapCenter插件或BlueXP 备份和恢复管理。这些工作负载可能会在ONTAP或其他产品中创建快照。如果已启用ONTAP FPolicy保护、则可以使用ONTAP更改FPolicy保护。
- 受**NetApp**应用程序保护的工作负载：这些工作负载的备份或快照策略由SnapCenter、适用于VMware vSphere的SnapCenter或BlueXP 备份和恢复管理。
  - 如果快照或备份策略由SnapCenter、SnapCenter for VMware或BlueXP 备份和恢复管理、则这些策略将继续由这些应用程序管理。通过使用BlueXP 勒索软件保护、您还可以对这些工作负载应用勒索软件检测策略。
  - 如果ONTAP中的勒索软件检测策略由自动勒索软件保护(ARP)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。

勒索软件保护策略需要哪些策略?

勒索软件保护策略需要以下策略：

- 勒索软件检测策略

- 快照策略

BlueXP 勒索软件保护策略不需要备份策略。

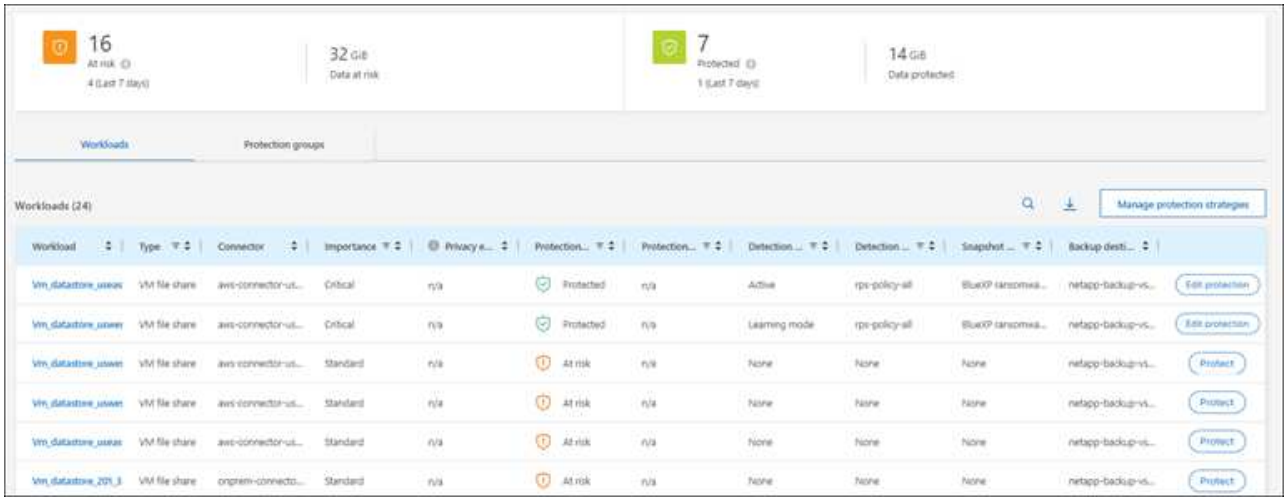
查看工作负载上的勒索软件保护

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
- VM工作负载
- 文件共享工作负载

步骤

1. 从BlueXP左侧导航栏中、选择*保护*>*防软件保护*。
2. 执行以下操作之一：
   - 从信息板上的"Data Protection (数据保护)"窗格中、选择*查看全部*。
   - 从菜单中，选择*Protection。



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。

> 对于已使用SnapCenter或BlueXP备份和恢复服务制定保护策略的工作负载、您无法编辑此保护。对于这些工作负载、如果已在其他服务中激活、则BlueXP勒索软件可启用自动勒索软件保护和/或FPolicy保护。了解有关、和的更多信息 "自主勒索软件保护" "BlueXP备份和恢复" "ONTAP FPolicy"。

保护页面上的保护详细信息

"Protection (保护)"页面显示了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、以指示是否已应用策略：

- 受保护：应用策略。已在与工作负载相关的所有卷上启用ARP。
- 存在风险：未应用任何策略。如果工作负载未启用主检测策略、则即使启用了快照和备份策略、它也会处于"

风险"状态。

- 进行中：正在应用策略、但尚未完成。
- *failed *：已应用策略，但策略不起作用。

检测状态：工作负载可以具有以下勒索软件检测状态之一：

- 正在学习：最近为工作负载分配了勒索软件检测策略、服务正在扫描工作负载。
- **Active**：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，但服务遇到错误。

在BlueXP 勒索软件保护中启用保护后、在勒索软件检测策略状态从"学习"模式更改为"活动"模式后、将开始进行警报检测和报告。

检测策略：如果已分配勒索软件检测策略、则会显示该策略的名称。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以及管理这些策略的产品或服务的快照和备份策略。

- 由SnapCenter管理
- 由适用于VMware vSphere的SnapCenter插件管理
- 由BlueXP备份和恢复管理
- 用于管理快照和备份的勒索软件保护策略的名称
- 无

工作负载重要性

在发现期间、BlueXP勒索软件保护会根据对每个工作负载的分析为每个工作负载分配一个重要性或优先级。工作负载的重要性取决于以下快照频率：

- 严重：每小时创建1个以上的Snapshot副本(主动保护计划)
- 重要：每小时创建的Snapshot副本少于1个、但每天创建的Snapshot副本多于1个
- 标准：每天创建1个以上的Snapshot副本

预定义检测策略

您可以根据工作负载的重要性选择以下BlueXP 勒索软件保护预定义策略之一：

策略级别	Snapshot	Frequency	保留(天)	Snapshot副本数	Snapshot副本的最大总数
关键工作负载策略	每季度	每15分钟	3.	288	309
	每天	每1天	14	14	309
	每周	每1周	35	5.	309
	每月	每30天	60	2.	309
重要的工作负载策略	每季度	每30分钟	3.	144.	165
	每天	每1天	14	14	165
	每周	每1周	35	5.	165
	每月	每30天	60	2.	165
标准工作负载策略	每季度	每30分钟	3.	72.	93
	每天	每1天	14	14	93
	每周	每1周	35	5.	93
	每月	每30天	60	2.	93

利用SnapCenter实现应用程序或VM一致的保护

启用应用程序或VM一致的保护有助于您以一致的方式保护应用程序或VM工作负载、从而实现稳定一致的状态、以避免日后需要恢复时可能丢失数据。

此过程将开始使用BlueXP备份和恢复为应用程序注册SnapCenter软件服务器或为VM注册适用于VMware vSphere的SnapCenter插件。

启用工作负载一致的保护后、您可以在BlueXP勒索软件保护中管理保护策略。保护策略包括在其他位置管理的快照和备份策略、以及在BlueXP 勒索软件保护中管理的勒索软件检测策略。

要了解有关使用BlueXP备份和恢复注册适用于VMware vSphere的SnapCenter或SnapCenter插件的信息、请参阅以下信息：

- "注册SnapCenter服务器软件"
- "注册适用于VMware vSphere的SnapCenter 插件"

步骤

1. 从BlueXP勒索软件保护菜单中、选择*信息板*。

2. 从“建议”窗格中，找到以下建议之一，然后选择*复查并修复*：
   - 向BlueXP注册可用的SnapCenter服务器
   - 向BlueXP注册适用于VMware vSphere的SnapCenter插件(SCV)
3. 按照信息使用BlueXP备份和恢复注册适用于VMware vSphere的SnapCenter或SnapCenter插件主机。
4. 返回到BlueXP勒索软件保护。
5. 从BlueXP勒索软件保护中、转到信息板并重新启动发现过程。
6. 从BlueXP勒索软件保护中选择*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、以查看这些策略是否在其他位置进行管理。

添加勒索软件保护策略

您可以为工作负载添加勒索软件保护策略。执行此操作的方式取决于Snapshot和备份策略是否已存在：

- 如果没有快照或备份策略，请创建勒索软件保护策略。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保护策略、其中可包括在BlueXP 勒索软件保护中创建的以下策略：
  - 快照策略
  - 备份策略
  - 勒索软件检测策略
- *为已经具有快照和备份策略*的工作负载创建检测策略，这些工作负载在其他NetApp产品或服务中进行管理。检测策略不会更改在其他产品中管理的策略。

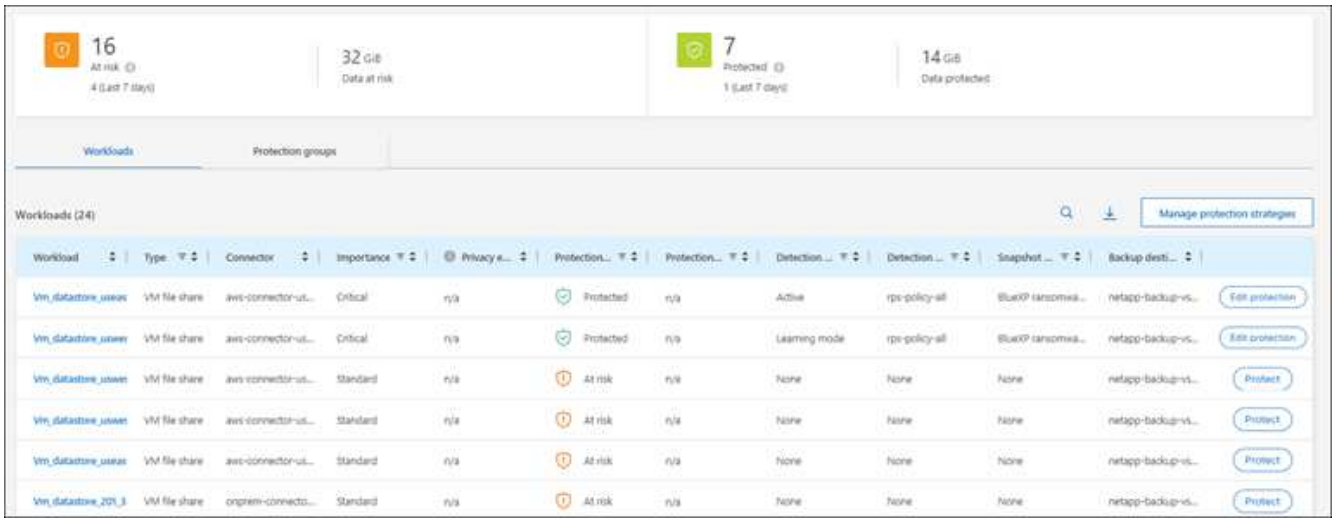
制定勒索软件保护策略(如果您没有快照或备份策略)

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、其中可包括在BlueXP 勒索软件保护中创建的以下策略：

- 快照策略
- 备份策略
- 勒索软件检测策略

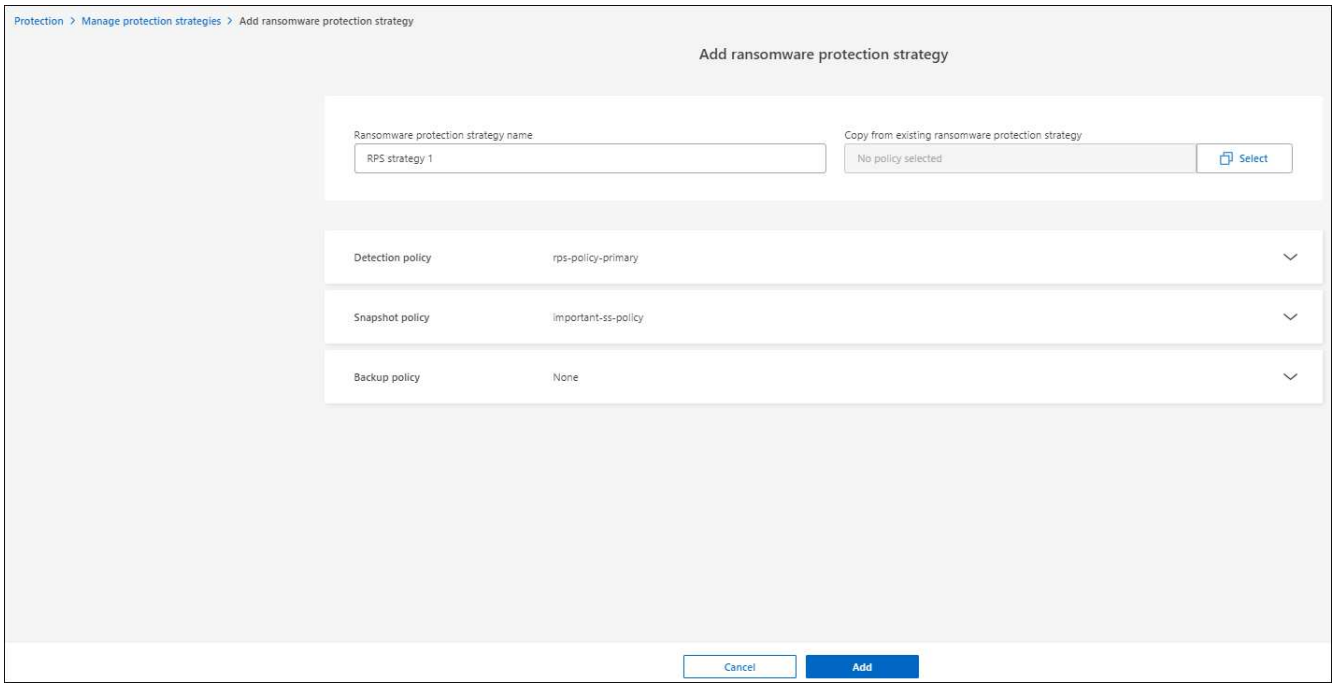
制定勒索软件保护策略的步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。



2. 在保护页面中，选择*管理保护策略*。

3. 从"RansU要 软件保护策略"页面中、选择*添加*。



4. 输入新的策略名称、或者输入现有名称进行复制。如果输入现有名称，请选择要复制的名称，然后选择*Copy*。

如果选择复制和修改现有策略、则该服务会在原始名称后附加"_copy"。您应更改此名称以及至少一个设置、以使其唯一。

5. 对于每个项目，选择*向下箭头*。
   - 检测策略：
     - 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、使服务检测潜在的勒索软件攻击。
     - 阻止文件扩展名：启用此选项可使服务阻止已知的可疑文件扩展名。启用主检测后、该服务会自动创建Snapshot副本。

       如果要更改阻止的文件扩展名、请在System Manager中编辑它们。
   - **Snapshot**策略:
     - **Snapshot policy base ame**：选择一个策略或选择*Create*并输入快照策略的名称。
     - **Snapshot**锁定：启用此选项可锁定主存储上的Snapshot副本、以便在一段时间内无法修改或删除这些副本、即使勒索软件攻击设法到达备份存储目标也是如此。这也称为_immutable storage_。这样可以缩短恢复时间。

       锁定快照后、卷到期时间将设置为快照副本的到期时间。

     ONTAP 9.12.1及更高版本提供了Snapshot副本锁定功能。要了解有关SnapLock的更多信息、请参见"ONTAP中的SnapLock"。

     - **Snapshot**计划：选择计划选项、要保留的Snapshot副本数、然后选择以启用计划。
   - 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：为二级存储选择计划选项并启用计划。

要在二级存储上启用备份锁定，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 * 。

向已具有**Snapshot**和备份策略的工作负载添加检测策略

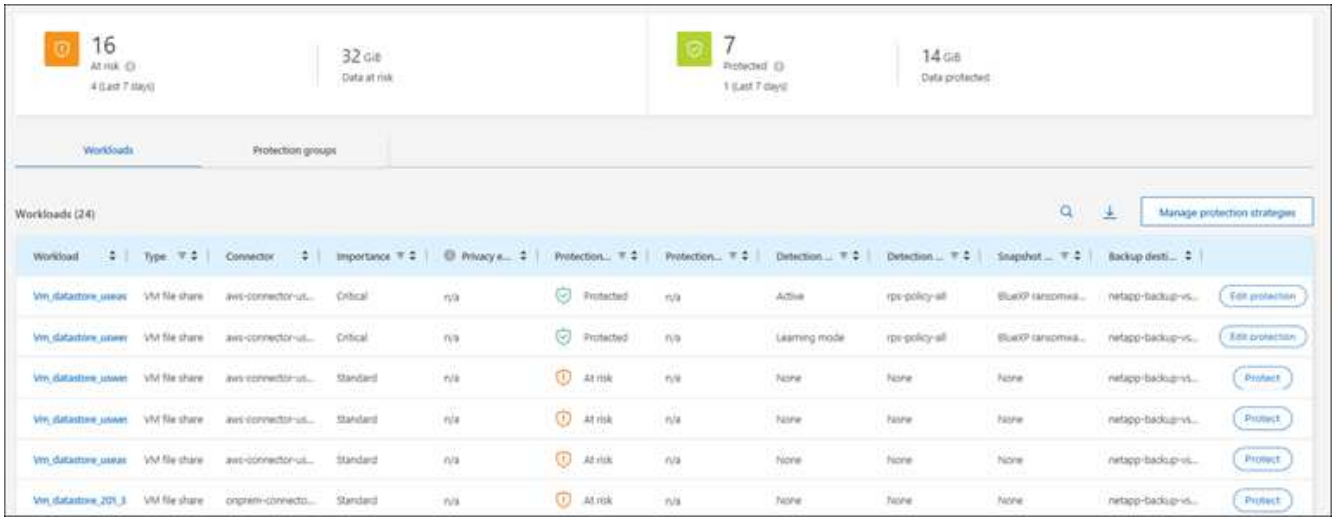
借助BlueXP 勒索软件保护、您可以将勒索软件检测策略分配给已具有Snapshot和备份策略的工作负载、这些策略将在其他NetApp产品或服务中进行管理。检测策略不会更改在其他产品中管理的策略。

BlueXP备份和恢复以及SnapCenter等其他服务使用以下类型的策略来管理工作负载：

- 用于管理快照的策略
- 用于控制复制到二级存储的策略
- 用于管理对象存储备份的策略

步骤

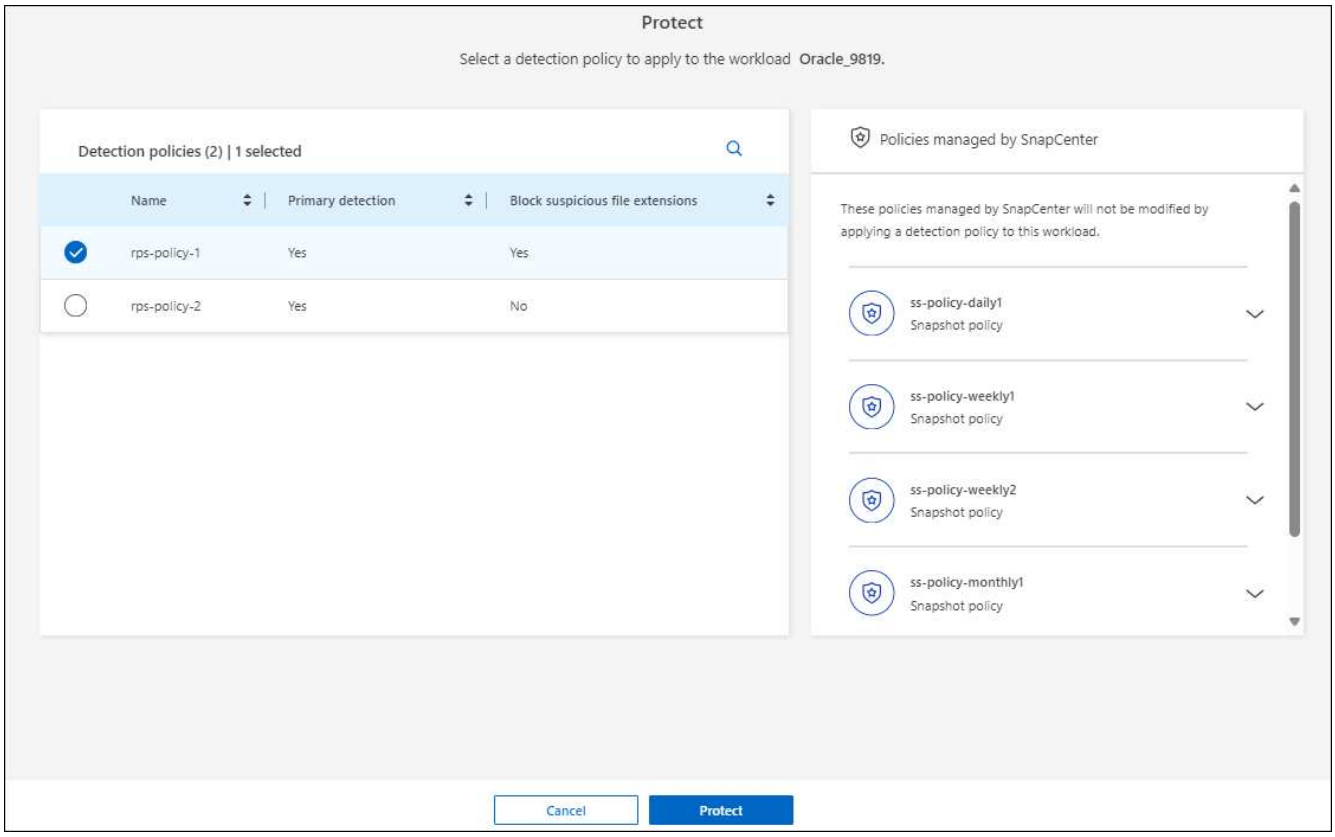
1. 从BlueXP勒索软件保护菜单中、选择*保护*。



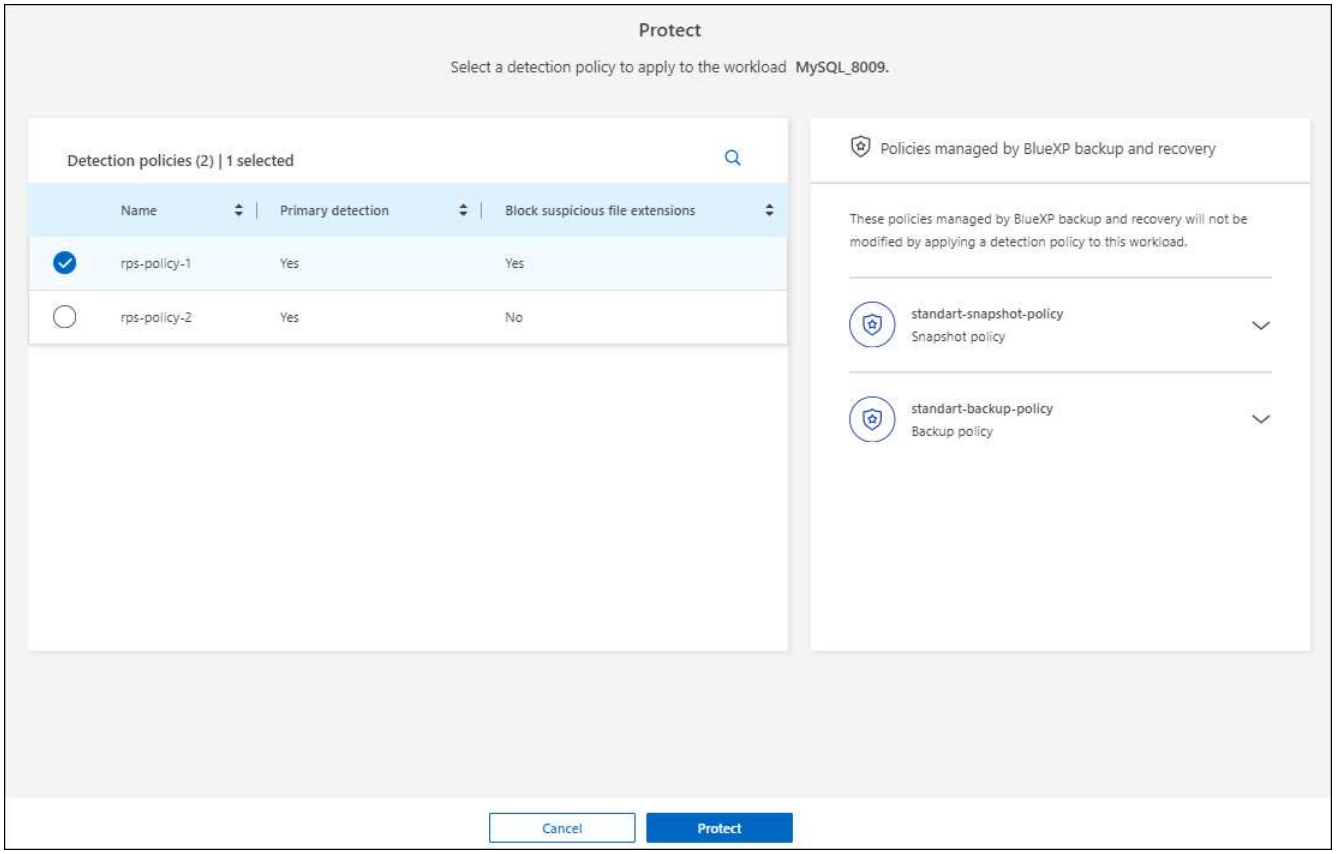
2. 从保护页面中、选择一个工作负载、然后选择*保护*。

保护页面显示了由SnapCenter软件、适用于VMware vSphere的SnapCenter以及BlueXP备份和恢复管理的策略。

以下示例显示了由SnapCenter管理的策略：



以下示例显示了由BlueXP备份和恢复管理的策略：



3. 要查看在其他位置管理的策略的详细信息，请单击*向下箭头*。
4. 要应用检测策略以及在其他位置管理的快照和备份策略、请选择检测策略。
5. 选择*保护*。
6. 在保护页面上、查看检测策略列以查看分配的检测策略。此外、快照和备份策略列会显示管理策略的产品或服务的名称。

分配其他策略

您可以分配不同的保护策略来替换当前保护策略。

步骤

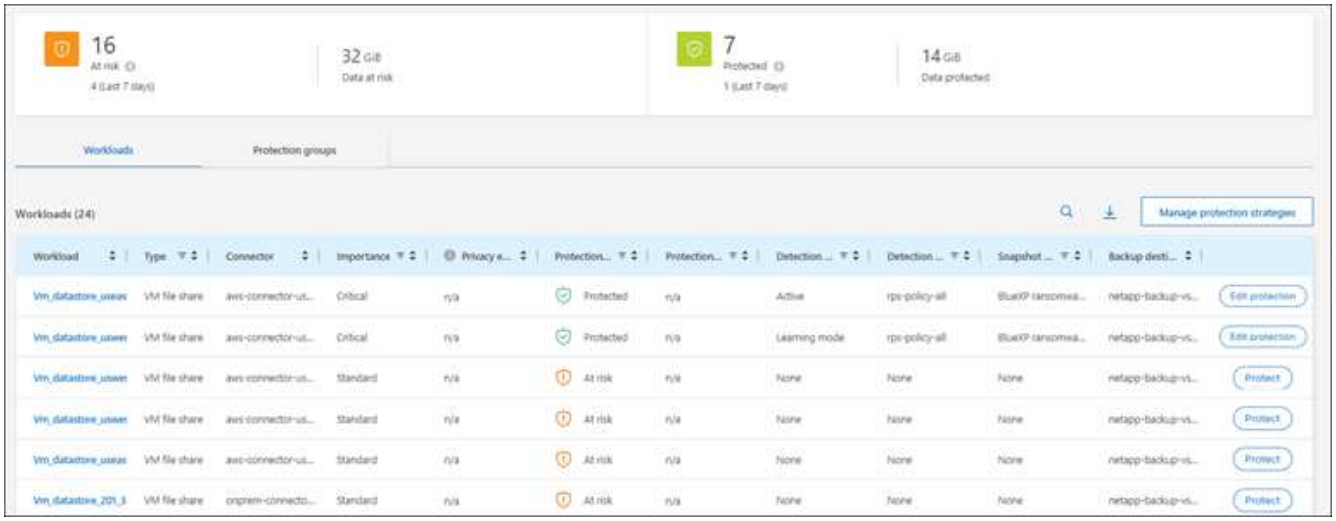
1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 从"Protection (保护)"页面的"Workload (工作负载)"行中、选择*编辑保护*。
3. 在策略页面中、单击要分配的策略对应的向下箭头以查看详细信息。
4. 选择要分配的策略。
5. 选择*保护*以完成更改。

对文件共享进行分组、以简化保护

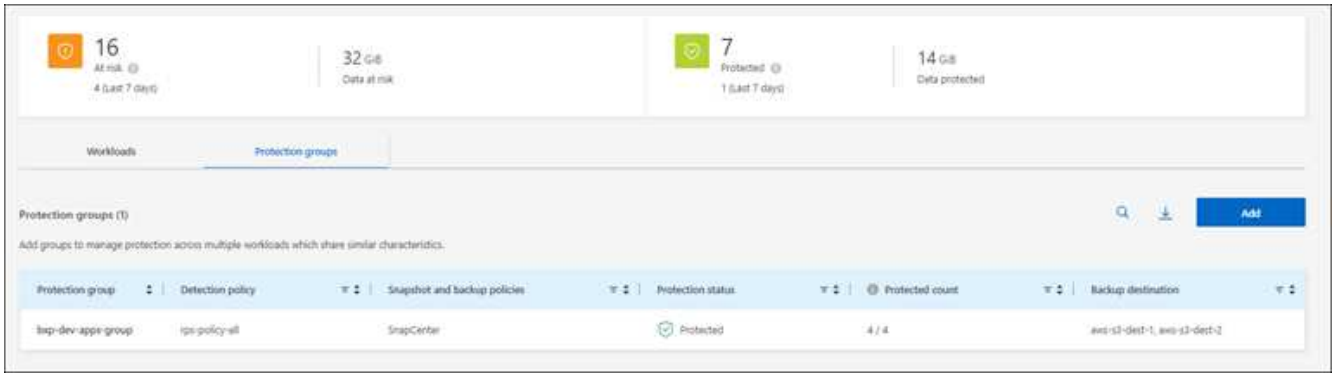
通过对文件共享进行分组、可以更轻松地保护数据资产。该服务可以同时保护组中的所有卷、而不是单独保护每个卷。

步骤

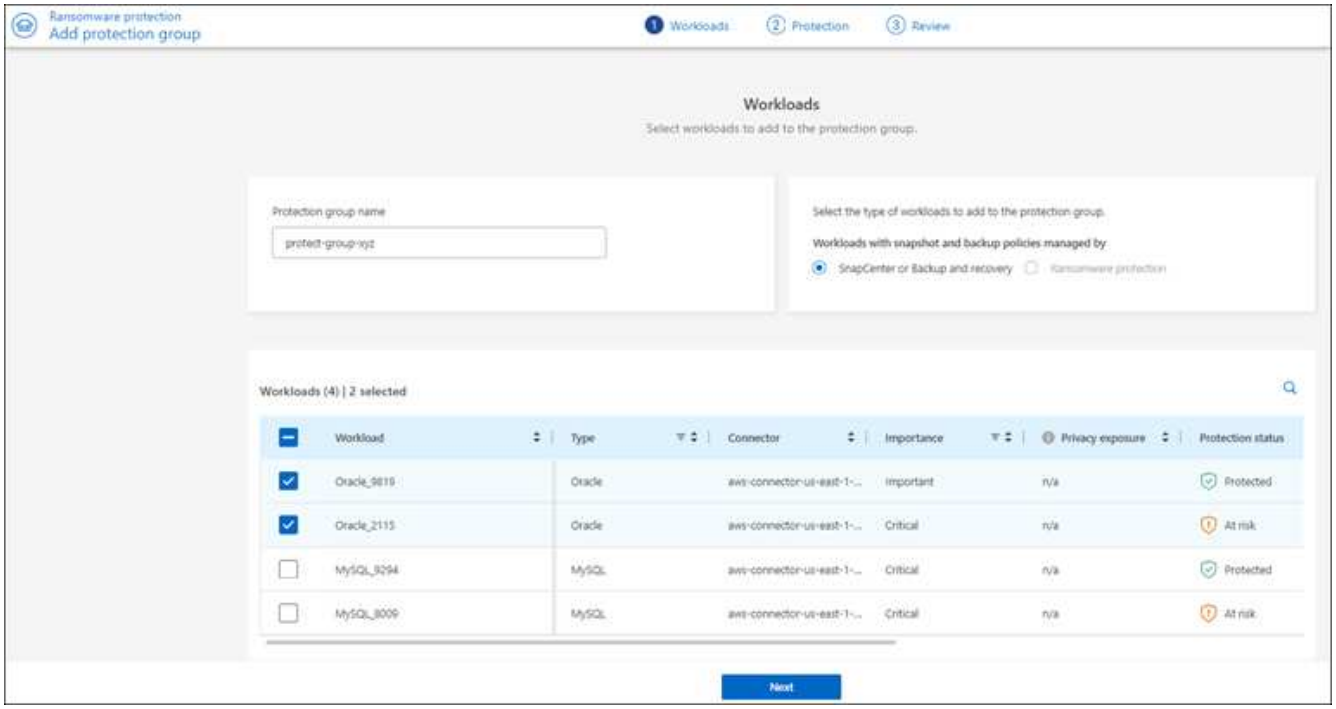
1. 从BlueXP勒索软件保护菜单中、选择*保护*。



2. 从保护页面中，选择*保护组*选项卡。



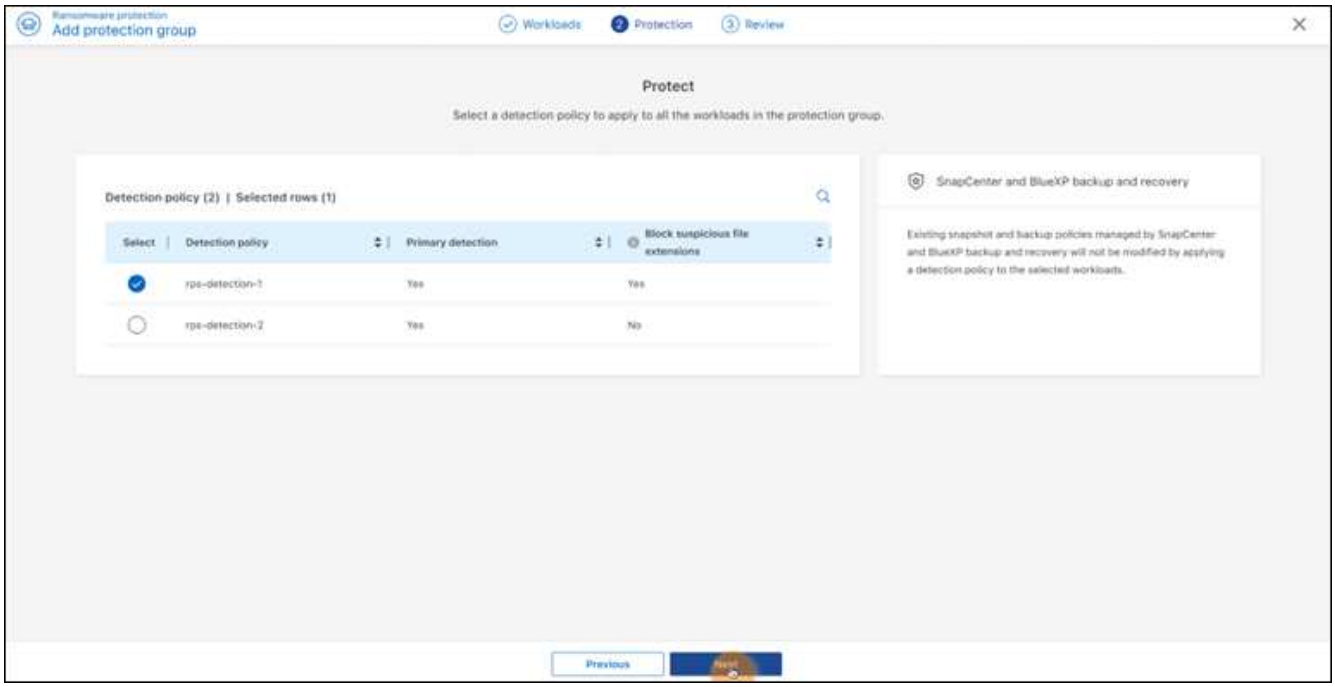
3. 选择 * 添加 * 。



4. 输入保护组的名称。
5. 完成以下步骤之一：
   a. 如果您已制定保护策略、请选择是否要根据工作负载是否受以下策略之一管理对其进行分组：
      - BlueXP勒索软件保护
      - SnapCenter或BlueXP 备份和恢复
   b. 如果您尚未制定保护策略、此页面将显示预配置的勒索软件保护策略。
      i. 选择一个以保护您的组，然后选择*下一步*。
      ii. 如果您选择的工作负载的卷位于多个工作环境中、请为多个工作环境选择备份目标、以便将其备份到云。
6. 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。

7. 选择 * 下一步 * 。



8. 选择要管理此组的保护的策略。
9. 选择 * 下一步 * 。
10. 查看为保护组选择的内容。
11. 选择 * 添加 * 。

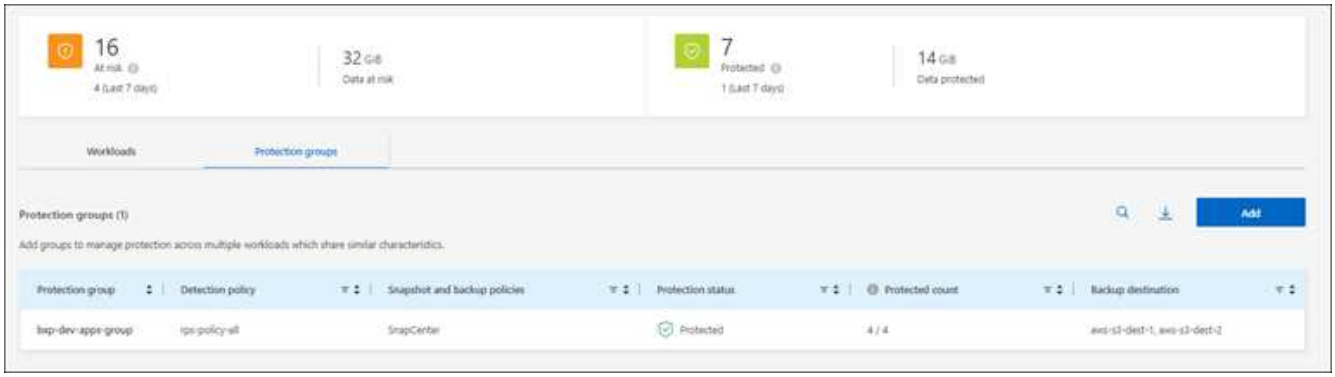
向组添加更多工作负载

您稍后可能需要向现有组添加更多工作负载。

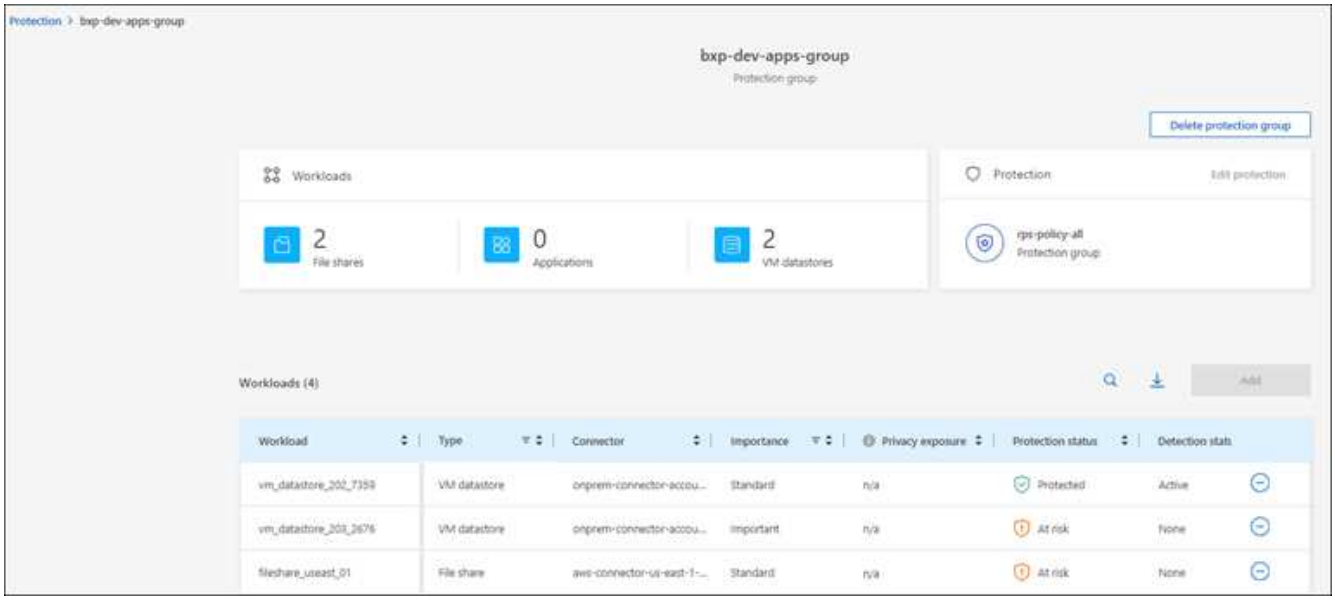
如果该组中的工作负载仅由BlueXP 勒索软件保护管理(而不是由SnapCenter或BlueXP 备份和恢复管理)、则应对仅由BlueXP 勒索软件保护管理的工作负载使用单独的组、而对由其他服务管理的工作负载使用另一组。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 从保护页面中，选择*保护组*选项卡。



3. 选择要添加更多工作负载的组。



4. 从"Selected protection group"(选定保护组)页面中、选择*Add*。

   BlueXP 勒索软件保护仅会显示组中尚未使用与组相同的快照和备份策略的工作负载。

   页面顶部显示了维护快照、备份和检测策略的服务。

5. 选择应添加到组中的其他工作负载。
6. 选择 * 保存 * 。

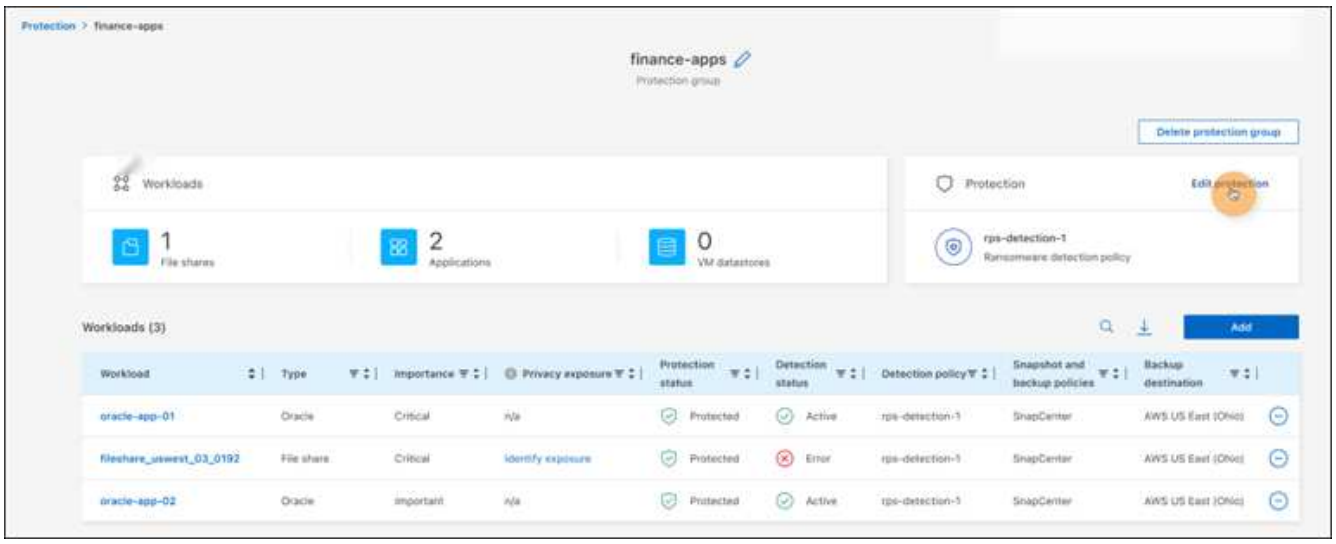
编辑组保护

您可以更改现有组上的检测策略。如果检测策略尚未添加到此组、则可以立即添加它。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。

2. 从保护页面中，选择*保护组*选项卡。



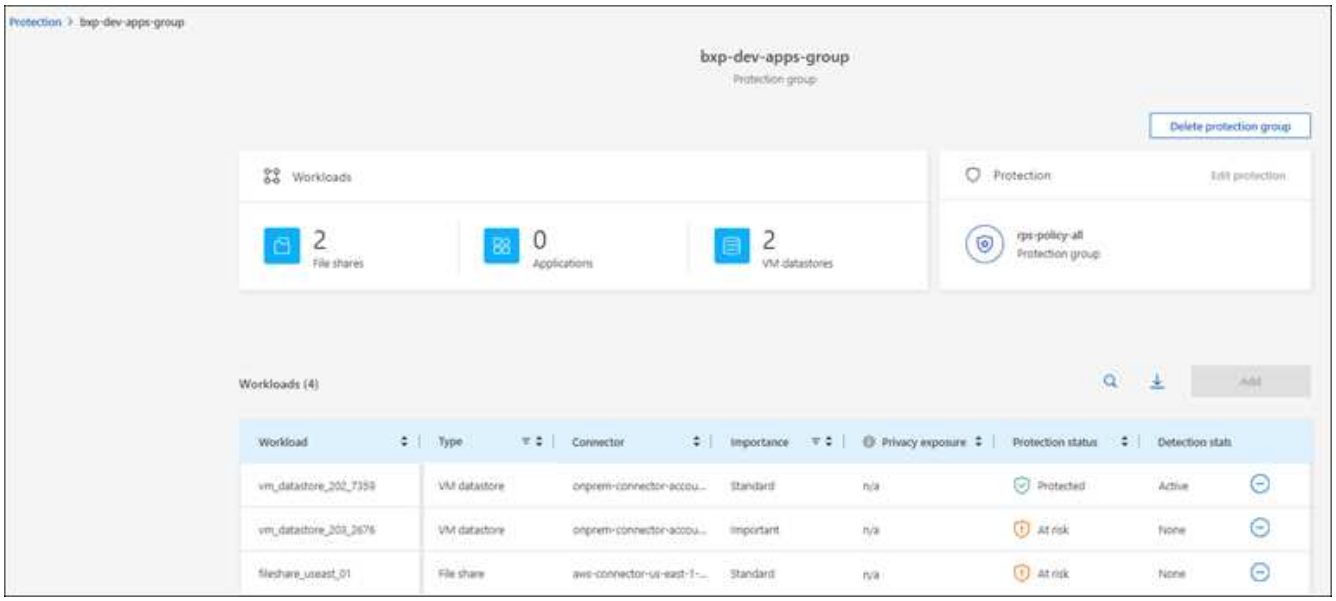
3. 从保护窗格中，选择*编辑保护*。
4. 选择检测策略或将其添加到此组。

从组中删除工作负载

您稍后可能需要从现有组中删除工作负载。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 从保护页面中，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"Selected protection group"(选定保护组)页面中、选择要从组中删除的工作负载、然后选择*操作*•••选项。

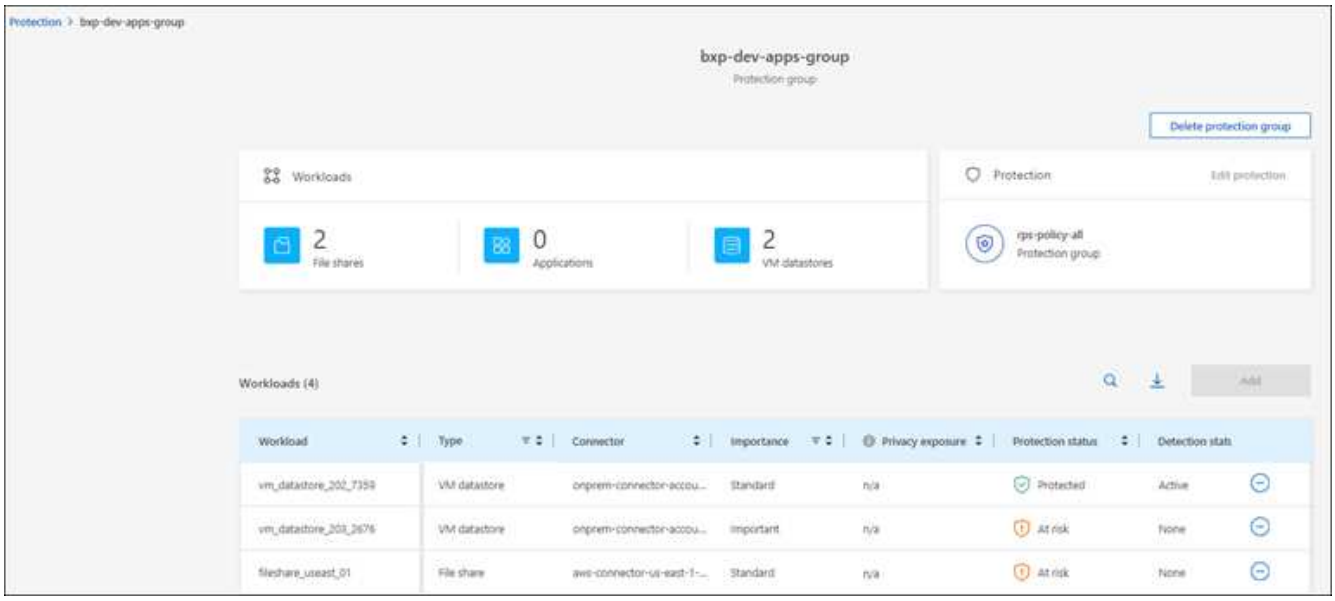
5. 从操作菜单中，选择*Remove Workload*。
6. 确认要删除此工作负载，然后选择*Remove*。

删除此保护组

删除保护组将删除该组及其保护、但不会删除各个工作负载。

步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 从保护页面中，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. 从选定保护组页面的右上角选择*删除保护组*。
5. 确认要删除该组，然后选择*Delete*。

管理勒索软件保护策略

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查看工作负载、也可以在编辑特定策略时查看这些工作负载。

查看策略列表的步骤

1. 从BlueXP勒索软件保护菜单中、选择*保护*。
2. 在保护页面中，选择*管理保护策略*。

   "Rans要 程序保护策略"页面将显示策略列表。

3. 在"反向器保护策略"页面上的"受保护的工作负载"列中、单击行尾的向下箭头。

删除勒索软件保护策略

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BlueXP勒索软件保护菜单中、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，为要删除的策略选择*Actions* ••• 选项。
4. 从操作菜单中，选择*Delete policy*。