发行说明

NetApp Ransomware Resilience

NetApp
February 27, 2026

目录

发行说明

NetApp Ransomware Resilience的新功能

了解NetApp Ransomware Resilience的新功能。

2026 年 2 月 16 日

Azure NetApp Files 支持

Ransomware Resilience 现在支持 Azure NetApp Files 系统，使您能够有效检测和响应 Azure NetApp Files 中的勒索软件威胁。当您发现工作负载时，Ransomware Resilience 现在会显示 Azure NetApp Files 并将其显示在保护仪表板中。Ransomware Resilience 对 Azure NetApp Files 的支持仅包括快照检测和保护策略。对 Azure NetApp Files 的支持当前处于预览状态。

有关详细信息，请参见 "了解勒索软件抵御能力"。

从用户行为警报中排除用户

Ransomware Resilience 现在允许您从用户行为警报中排除特定用户。排除受信任的用户可以防止误报和不必要的警报。

有关详细信息，请参见 "从警报中排除用户"。

用户行为活动的保护组支持

Ransomware Resilience 保护组现在支持可疑用户行为检测的检测策略。当您将勒索软件保护策略应用于保护组时，它会跨工作负载应用策略，从而简化对网络安全态势的管理。

有关详细信息，请参见 "创建保护组"。

2026年1月19日

不支持的卷

Ransomware Resilience 报告现在可以在摘要报告中捕获有关受支持和不受支持卷的信息。使用此信息可诊断系统中的卷可能不符合勒索软件保护条件的原因。

有关详细信息，请参阅 "下载勒索软件恢复力报告"。

2026年1月12日

将快照复制到**ONTAP**

Ransomware Resilience 现在支持将快照复制添加到辅助 ONTAP 站点。使用复制策略的保护组，您可以为每个工作负载复制到相同的目标或不同的目标。您可以创建包括复制的勒索软件保护策略或使用预定义策略。

有关详细信息，请参阅 "在勒索软件恢复中保护工作负载"。

将工作负载排除在勒索软件恢复能力之外

勒索软件恢复功能现在支持将系统中的特定工作负载从保护范围和勒索软件恢复仪表板中排除。发现工作负载后，您可以将其排除在外；如果想要添加勒索软件防护，则可以重新将其包含在内。排除在外的工作负载无需付费。

有关详细信息，请参阅 "排除工作负载"。

标记提醒，如正在审核中

勒索软件恢复功能现在允许您将警报标记为“审核中”。使用“审核中”标签可以提高团队在对活跃的勒索软件威胁进行分类和管理时的清晰度。

有关详细信息，请参阅 "管理勒索软件恢复能力中的警报"。

2025年12月8日

扩展程序阻止功能已在工作负载级别启用。

启用扩展阻止功能后，现在是在工作负载级别而不是存储虚拟机级别启用该功能。

编辑用户行为警报状态

勒索软件恢复功能现在允许您编辑用户行为警报的状态。您可以手动关闭和解决警报。

有关详细信息，请参阅 "管理勒索软件恢复能力中的警报"。

支持多个控制台代理

勒索软件恢复功能现在支持使用多个控制台代理来管理同一系统。

有关控制台代理的更多信息，请参阅"创建控制台代理"。

2025年11月10日

该版本包括一般增强功能和改进功能。

2025年10月6日

BlueXP ransomware protection现已升级NetApp Ransomware Resilience

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

BlueXP现在是NetApp Console

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

有关更改的详细信息，请参阅 "NetApp Console发行说明"。

数据泄露检测

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

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

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

有关详细信息，请参阅"启用可疑用户活动检测"和"查看异常用户行为"。

其他可疑用户活动检测

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

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

用于数据泄露检测的新用户角色

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

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

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

2025年8月12日

该版本包括一般增强功能和改进功能。

2025年7月15日

SAN 工作负载支持

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

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

改进的工作负载保护

此版本改进了具有其他NetApp工具（如SnapCenter或BlueXP backup and recovery）的快照和备份策略的工作负载的配置过程。在以前的版本中， BlueXP ransomware protection发现了来自其他工具的策略，只允许您更改

检测策略。在此版本中，您现在可以用BlueXP ransomware protection策略替换快照和备份策略，或者继续使用其他工具中的策略。

有关详细信息，请参阅"保护工作负载"。

电子邮件通知

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

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

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

有关详细信息，请参阅"处理检测到的勒索软件警报"。

2025年6月9日

登陆页面更新

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

准备演习更新

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

在此版本中，您可以使用BlueXP ransomware protection仪表板上的新按钮在测试工作负载上运行勒索软件准备演练，从而更轻松地模拟勒索软件攻击、调查其影响并有效地恢复工作负载，所有这些都在受控环境中完成。

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

有关详细信息，请参阅 "进行勒索软件攻击准备演习"。

启用**BlueXP classification**更新

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

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

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

2025年5月13日

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

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

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

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

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

2025年4月29日

支持Amazon FSx for NetApp ONTAP

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

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

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

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

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

- 警报事件展示了新的 FSx for ONTAP工作环境。

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

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

需要BlueXP访问角色

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

"了解所有服务的BlueXP访问角色" 。

2025年4月14日

准备演习报告

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

在发生实际勒索软件攻击时您是否已做好准备。

有关详细信息，请参阅 "进行勒索软件攻击准备演习"。

新的基于角色的访问控制角色和权限

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

- 勒索软件保护管理员
- 勒索软件保护查看器

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

付款改进

此版本对支付流程进行了多项改进。

有关详细信息，请参阅 "设置许可和付款选项"。

2025年3月10日

模拟攻击并做出响应

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

有关详细信息，请参阅 "进行勒索软件攻击准备演习"。

发现过程的增强

此版本包括对选择性发现和重新发现过程的增强：

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

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

检测到高度加密时发出警报

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

有关详细信息，请参阅 "响应检测到的勒索软件警报"。

2024年12月16日

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

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

有关详细信息，请参阅 "响应检测到的勒索软件警报"。

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

参考 "配置BlueXP ransomware protection设置"。

选择要发现和保护的工作负载

在此版本中，您现在可以执行以下操作：

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

参考 "发现工作负载"。

2024年11月7日

启用数据分类并扫描个人身份信息 **(PII)**

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

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

要启动扫描，请在 Protection 页面上，在 Protection 仪表板的 Privacy exposure 列中选择 **Identify exposure**。有关详细信息，请参见 "使用 BlueXP classification 扫描个人可识别的敏感数据"。

SIEM 与 **Microsoft Sentinel** 集成

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

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

立即免费试用 **30** 天

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

在文件级别恢复 **Podman** 的应用程序工作负载

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

"了解有关从勒索软件攻击中恢复的更多信息" 。

2024年9月30日

文件共享工作负载的自定义分组

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

"了解有关在勒索软件保护策略中分组文件共享工作负载的更多信息" 。

2024年9月2日

来自**Digital Advisor**的安全风险评估

BlueXP ransomware protection 现在从 NetApp Digital Advisor 收集有关集群的高风险和严重安全风险的信息。如果发现任何风险，BlueXP ransomware protection 会在仪表板的*推荐操作*窗格中提供建议："修复集群上的已知安全漏洞<name>。"从仪表板上的建议中，选择*查看和修复*建议查看 Digital Advisor 和常见漏洞和暴露 (CVE) 文章，以解决安全风险。如果存在多重安全风险，请在 Digital Advisor 中查看信息。

参考 "Digital Advisor文档"。

备份到 **Google Cloud Platform**

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

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

支持 **Google Cloud Platform**

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

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

基于角色的访问控制

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

有关每个角色可以执行的操作的详细信息，请参阅 "基于角色的访问控制权限"。

2024年8月5日

使用 **Splunk Cloud** 进行威胁检测

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

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

2024年7月1日

自带许可证 **(BYOL)**

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

"了解有关设置许可的详细信息" 。

在文件级别恢复应用程序工作负载

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

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

"了解有关从勒索软件攻击中恢复的更多信息" 。

下载受影响文件的列表

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

"了解有关在恢复应用程序之前下载受影响文件的更多信息" 。

删除保护计划

通过此版本，您现在可以删除勒索软件保护策略。

"了解有关保护工作负载和管理勒索软件保护策略的更多信息" 。

2024年6月10日

主存储上的快照副本锁定

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

"了解有关在勒索软件保护策略中保护工作负载和启用备份锁定的更多信息" 。

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

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

"Azure 中的Cloud Volumes ONTAP快速入门"

"了解BlueXP ransomware protection" 。

Microsoft Azure 添加为备份目标

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

"了解有关如何配置保护设置的更多信息"。

2024年5月14日

许可更新

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

"了解有关设置许可的详细信息" 。

CIFS 协议

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

工作负载详情

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

"详细了解如何在“保护”页面中查看工作负载详细信息" 。

应用程序一致性和虚拟机一致性保护和恢复

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

"了解有关保护工作负载的更多信息" 。

勒索软件防护策略

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

- Snapshot 策略
- 备份策略

- 检测策略

"了解有关保护工作负载的更多信息" 。

威胁检测

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

"了解有关配置“设置”选项的详细信息"。

消除误报

从“警报”选项卡中，您现在可以消除误报或决定立即恢复数据。

"详细了解如何响应勒索软件警报" 。

检测状态

新的检测状态出现在“保护”页面上，显示应用于工作负载的勒索软件检测的状态。

"了解有关保护工作负载和查看保护状态的更多信息" 。

下载 **CSV** 文件

您可以从保护、警报和恢复页面下载 CSV 文件*。

"详细了解如何从仪表板和其他页面下载 CSV 文件" 。

文档链接

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

BlueXP backup and recovery

系统上不再需要预先启用 BlueXP 备份和恢复服务。请参阅 "前提条件"。BlueXP 勒索软件保护服务有助于通过"设置"选项配置备份目标。请参阅 "配置设置"。

设置选项

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

"了解有关配置“设置”选项的详细信息"。

2024年3月5日

保护策略管理

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

二级存储的不变性（**DataLock**）

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

自动备份到**NetApp StorageGRID**

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

调查潜在攻击的附加功能

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

恢复过程

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

"了解BlueXP ransomware protection" 。

2023年10月6日

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

预览版服务可保护BlueXP组织内各个组织中 Oracle、VM 数据存储和本地 NAS 存储上的文件共享以及 AWS 上的Cloud Volumes ONTAP （使用 NFS 协议）上的应用程序工作负载，并将数据备份到 Amazon Web Services 云存储。

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

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

"了解BlueXP ransomware protection" 。

NetApp Ransomware Resilience的已知限制

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

准备演习重置选项问题

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

Amazon FSx for NetApp ONTAP限制

勒索软件恢复能力支持Amazon FSx for NetApp ONTAP系统。以下限制适用于Amazon FSx for ONTAP：

- Amazon FSx for ONTAP 不支持备份策略。在此环境中，您应使用 Amazon FSx 执行备份操作。您可以使用 Ransomware Resilience 恢复这些工作负载。
- 恢复操作仅从快照执行。

Azure NetApp Files 限制

Ransomware Resilience 支持 Azure NetApp Files。以下限制适用于 Azure NetApp Files：

- Azure NetApp Files 不支持带有备份策略的勒索软件保护策略。您可以使用 Azure NetApp Files 备份。
- Azure NetApp Files 不支持带有复制的勒索软件保护策略。
- 选择保护策略时，请确保其快照计划与 Azure NetApp Files 兼容。Azure NetApp Files 中最常用的快照计划是每小时一次。