发行说明

BlueXP ransomware protection

NetApp
December 20, 2024

目录

发行说明

BlueXP 勒索软件防护中的新增功能

了解BlueXP勒索软件保护的新增功能。

2024年12月16日

使用**Data Infrastructure Insight**存储工作负载安全性检测异常用户行为

在此版本中、您可以使用Data Infrastructure Insight存储工作负载安全性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来保护您的数据。

有关详细信息，请参见 "响应检测到的勒索软件警报"。

在使用数据基础架构洞察存储工作负载安全性检测异常用户行为之前、您需要使用BlueXP 勒索软件保护*设置*选项来配置此选项。

请参阅 "配置BlueXP勒索软件保护设置"。

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Connector中、选择要发现工作负载的工作环境。如果您希望保护环境中的特定工作负载、而不是其他工作负载、则可以从该功能中受益。
- 在发现工作负载期间、您可以为每个连接器启用工作负载自动发现。通过此功能、您可以选择要保护的工作负载。
- 发现先前选定工作环境中新创建的工作负载。

请参阅 "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(个人身份信息、个人身份信息)

在此版本中、您可以启用BlueXP 分类(BlueXP 系列的核心组件)来扫描文件共享工作负载中的数据并对其进行分类。对数据进行分类有助于确定您的数据包含个人信息还是私人信息、这会增加安全风险。此过程还会影响工作负载的重要性、并帮助您确保以适当的保护级别保护工作负载。

部署BlueXP 分类的客户通常可以在BlueXP 勒索软件保护中扫描数据。BlueXP 分类可作为BlueXP 平台的一部分免费提供、并且可以部署在内部环境或客户云中。

请参阅 "配置BlueXP勒索软件保护设置"。

要启动扫描，请在“保护”页面上，单击“隐私暴露”列中的*识别曝光*。

"使用BlueXP 分类扫描个人身份敏感数据"(英文)

与**Microsoft Sentinel**的暹粒集成

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安全中心或Splunk Cloud作为您的SIEM。

"了解有关配置BlueXP 勒索软件保护设置的更多信息"(英文)

现在**30**天免费试用

在此版本中、全新部署的BlueXP 勒索软件保护现在有30天的免费试用时间。以前、BlueXP 勒索软件防护提供90天免费试用。如果您已获得90天免费试用、此优惠将持续90天。

在文件级别恢复**Podman**的应用程序工作负载

现在、在文件级别还原应用程序工作负载之前、您可以查看可能受攻击影响的文件列表、并确定要还原的文件。以前、如果组织(以前称为帐户)中的BlueXP 连接器使用的是Podman、则此功能已禁用。现在已为Podman启用此功能。您可以让BlueXP勒索软件保护选择要还原的文件、也可以上传CSV文件以列出受警报影响的所有文件、或者手动确定要还原的文件。

"详细了解如何从勒索软件攻击中恢复"(英文)

2024年9月30日

自定义文件共享工作负载分组

在此版本中、您现在可以将文件共享分组到多个组中、以便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。以前、您需要单独保护每个卷。

"详细了解如何在勒索软件保护策略中对文件共享工作负载进行分组"(英文)

2024年9月2日

Digital Advisor的安全风险评估

BlueXP 勒索软件防护现在可从NetApp数字顾问收集与集群相关的高安全风险和严重安全风险的信息。如果发现任何风险、BlueXP 勒索软件保护会在信息板的*建议操作*窗格中提供建议："修复集群<name>上的已知安全漏洞。"根据信息板上的建议，单击"*查看并修复"，建议查看Digital Advisor和"常见漏洞与披露"(Common漏洞与披露，CVA)文章以解决安全风险。如果存在多个安全风险、请查看Digital Advisor中的信息。

请参阅 "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存储分段。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 勒索软件保护设置的更多信息"(英文)

支持**Google Cloud Platform**

该服务现在支持Cloud Volumes ONTAP for Google Cloud Platform以实现存储保护。以前、该服务仅支持适用于Amazon Web Services和Microsoft Azure的Cloud Volumes ONTAP以及内部NAS。

"了解BlueXP 勒索软件保护以及支持的数据源、备份目标和工作环境"(英文)

基于角色的访问控制

现在、您可以使用基于角色的访问控制(Role-Based Access Control、RBAC)限制对特定活动的访问。BlueXP 勒索软件保护使用BlueXP 中的两个角色：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，请参见 "基于角色的访问控制Privileges"。

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安全和事件管理系统(SIEM)、以进行威胁分析和检测。对于先前版本、您只能选择AWS安全中心作为您的SIEM。在此版本中、您可以选择AWS安全中心或Splunk Cloud作为您的SIEM。

"了解有关配置BlueXP 勒索软件保护设置的更多信息"(英文)

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、这是一个可从NetApp销售代表处获取的NetApp许可证文件(NLL)

"了解有关设置许可的更多信息"。

在文件级别还原应用程序工作负载

现在、在文件级别还原应用程序工作负载之前、您可以查看可能受攻击影响的文件列表、并确定要还原的文件。您可以让BlueXP勒索软件保护选择要还原的文件、也可以上传CSV文件以列出受警报影响的所有文件、或者手动确定要还原的文件。

在此版本中、如果帐户中的所有BlueXP连接器均未使用Podman、则会启用单个文件还原功能。否则、该帐户将被禁用。

"详细了解如何从勒索软件攻击中恢复"(英文)

下载受影响文件的列表

现在、在文件级还原应用程序工作负载之前、您可以访问警报页面以下载CSV文件中受影响文件的列表、然后使用恢复页面上传CSV文件。

"了解有关在还原应用程序之前下载受影响文件的更多信息"(英文)

删除保护计划

在此版本中、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"(英文)

2024年6月10日

主存储上的**Snapshot**副本锁定

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。

"详细了解如何在勒索软件保护策略中保护工作负载和启用备份锁定"。

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和内部ONTAP NAS之外、还支持将适用于Microsoft Azure的Cloud Volumes ONTAP用作工作环境。

"在 Azure 中快速启动 Cloud Volumes ONTAP"

"了解BlueXP勒索软件保护"。

已将**Microsoft Azure**添加为备份目标

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

"详细了解如何配置保护设置"。

2024年5月14日

许可更新

您可以注册90天免费试用。很快、您将能够通过亚马逊网络服务商城购买按需购买订阅或自带NetApp许可证。

"了解有关设置许可的更多信息"。

CIFS协议

现在、该服务支持在使用NFS和CIFS协议的AWS工作环境中使用内部ONTAP和Cloud Volumes ONTAP。先前版本仅支持NFS协议。

工作负载详细信息

现在、此版本可在"Protection (保护)"和"Other (其他)"页面中的工作负载信息中提供更多详细信息、以改进工作负载保护评估。您可以通过工作负载详细信息查看当前分配的策略以及配置的备份目标。

"有关查看工作负载详细信息的更多信息、请参见保护页面"。

应用程序一致和**VM**一致的保护和恢复

现在、您可以使用NetApp SnapCenter软件执行应用程序一致的保护、并使用适用于VMware vSphere的SnapCenter插件执行VM一致的保护、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。如果需要恢复、您可以将应用程序或VM还原回先前可用的任何状态。

"了解有关保护工作负载的更多信息"。

勒索软件保护策略

如果工作负载上不存在Snapshot或备份策略、您可以创建勒索软件保护策略、其中可包括在此服务中创建的以下策略：

- 快照策略
- 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、可使用第三方安全和事件管理(SIEM)系统进行威胁检测。现在、信息板会显示一个新的"启用威胁检测"建议、您可以在"设置"页面上配置该建议。

"了解有关配置设置选项的更多信息"。

消除误报警报

现在、您可以从"Alerts"(警报)选项卡中消除误报或决定立即恢复数据。

"了解有关响应勒索软件警报的更多信息"(英文)

检测状态

新的检测状态将显示在"保护"页面上、其中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*。

"了解有关从信息板和其他页面下载CSV文件的更多信息"。

文档链接

查看文档链接现在包含在用户界面中。您可以从信息板垂直*操作*选项访问此文档  。选择*新增功能*以查看发行说明中的详细信息、或者选择*文档*以查看BlueXP勒索软件保护文档主页。

BlueXP备份和恢复

工作环境中不再需要启用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

现在、您可以在BlueXP 勒索软件保护设置中设置备份目标。

"了解有关配置设置选项的更多信息"。

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"(英文)。

二级存储上的不可破坏性**(DataLock)**

现在、您可以在对象存储中使用NetApp DataLock技术使备份在二级存储中不可更改。 "了解有关创建保护策略的更多信息"(英文)。

自动备份到**NetApp StorageGRID**

除了使用AWS之外、您现在还可以选择StorageGRID作为备份目标。 "了解有关配置备份目标的更多信息"(英文)。

用于调查潜在攻击的其他功能

现在、您可以查看更多取证详细信息、以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"(英文)。

恢复过程

恢复过程得到了改进。现在、您可以逐个卷或为一个工作负载恢复所有卷。 "详细了解如何从勒索软件攻击中恢复(在消除意外事件后)"(英文)。

"了解BlueXP勒索软件保护"。

2023年10月6日

BlueXP勒索软件保护服务是一种SaaS解决方案、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。

对于预览版、该服务可保护内部NAS存储以及AWS上的Cloud Volumes ONTAP (使用NFS协议)上基于应用程序的Oracle、MySQL、VM数据存储库和文件共享的各个BlueXP 组织工作负载、并将数据备份到Amazon Web Services云存储。

BlueXP勒索软件保护服务可充分利用多种NetApp技术、以便您的数据安全管理员或安全运营工程师可以实现以下目标：

- 一目了然地查看所有工作负载上的勒索软件保护。
- 深入了解勒索软件保护建议
- 根据BlueXP勒索软件保护建议改善保护状况。
- 分配勒索软件保护策略、以保护您的首要工作负载和高风险数据免受勒索软件攻击。
- 监控工作负载的运行状况、防止勒索软件攻击发现数据异常。
- 快速评估勒索软件事件对工作负载的影响。

- 通过还原数据并确保存储的数据不会再次感染、从勒索软件事件中智能恢复。

"了解BlueXP勒索软件保护"。