リリースノート
BlueXP ransomware protection

NetApp
December 20, 2024

目次

リリースノート

BlueXP ランサムウェア対策の新機能

BlueXPランサムウェア対策の新機能をご紹介します。

2024年12月16日

Data Infrastructure Insights Storage Workload Securityを使用してユーザの異常な行動を検出

このリリースでは、Data Infrastructure Insights Storage Workload Securityを使用して、ストレージワークロードの異常なユーザ行動を検出できます。この機能を使用すると、潜在的なセキュリティ脅威を特定し、悪意のあるユーザをブロックしてデータを保護できます。

詳細については、を参照してください "検出されたランサムウェアに関するアラートに対応"。

Data Infrastructure Insights Storage Workload Securityを使用して異常なユーザ行動を検出するには、事前にBlueXP ransomware protection * Settings *オプションを使用してオプションを設定する必要があります。

を参照してください "BlueXPのランサムウェア対策の設定"。

検出して保護するワークロードを選択

このリリースでは、次の操作を実行できます。

- 各コネクタで、ワークロードを検出する作業環境を選択します。この機能は、環境内の特定のワークロードを保護し、他のワークロードを保護する必要がない場合に役立ちます。
- ワークロードの検出時に、コネクタごとにワークロードの自動検出を有効にすることができます。保護するワークロードを選択できます。
- 以前に選択した作業環境用に新しく作成されたワークロードを検出します。

を参照してください "ワークロードを検出"。

2024年11月7日

データの分類を有効にし、個人識別情報（**PII**）をスキャンする

このリリースでは、BlueXP ファミリーのコアコンポーネントであるBlueXP 分類を有効にして、ファイル共有ワークロードのデータをスキャンして分類することができます。データを分類することで、データに個人情報が含まれているかどうかを特定し、セキュリティリスクを高めることができます。このプロセスは、ワークロードの重要性にも影響し、適切なレベルの保護でワークロードを保護するのに役立ちます。

BlueXP ランサムウェア対策でのPIIデータのスキャンは、BlueXP 分類を導入したお客様が一般に利用できます。BlueXP の分類は、BlueXP プラットフォームの一部として追加料金なしで利用でき、オンプレミスまたはお客様のクラウドに導入できます。

を参照してください "BlueXPのランサムウェア対策の設定"。

スキャンを開始するには、[Protection]ページで、[Privacy exposure]列の*[Identify exposure]*をクリックしま

す。

"BlueXP 分類を使用して、個人を特定できる機密データをスキャン"です。

SIEMと**Microsoft Sentinel**の統合

Microsoft Sentinelを使用して脅威の分析と検出のために、セキュリティおよびイベント管理システム(SIEM)にデータを送信できるようになりました。以前は、AWS Security HubまたはSplunk CloudをSIEMとして選択できました。

"BlueXP ランサムウェア対策の設定の詳細"です。

30日間の無償トライアル

このリリースでは、BlueXP ランサムウェア対策の新規導入に30日間の無償トライアルが提供されるようになりました。以前は、BlueXP ランサムウェア対策は90日間の無償トライアルを提供していました。すでに90日間の無償トライアルを利用している場合は、90日間継続されます。

Podmanのアプリケーションワークロードをファイルレベルでリストア

アプリケーションワークロードをファイルレベルでリストアする前に、攻撃の影響を受けた可能性があるファイルのリストを表示し、リストアするファイルを特定できるようになりました。以前は、組織（以前はアカウント）のBlueXP コネクタがPodmanを使用していた場合、この機能は無効になっていました。これでPodmanで有効になりました。BlueXPランサムウェア対策でリストアするファイルを選択したり、アラートの影響を受けたすべてのファイルを記載したCSVファイルをアップロードしたり、リストアするファイルを手動で特定したりできます。

"ランサムウェア攻撃からのリカバリの詳細"です。

2024年9月30日

ファイル共有ワークロードのカスタムグループ化

このリリースでは、ファイル共有をグループにグループ化して、データ資産を簡単に保護できるようになりました。グループ内のすべてのボリュームを同時に保護できます。以前は、各ボリュームを個別に保護する必要がありました。

"ランサムウェア対策戦略におけるファイル共有ワークロードのグループ化の詳細"です。

2024年9月2日

Digital Advisorによるセキュリティリスク評価

BlueXP ランサムウェア対策では、クラスタに関連する高リスクと重大なセキュリティリスクに関する情報がNetAppデジタルアドバイザから収集されるようになりました。リスクが検出された場合、BlueXP ランサムウェア対策により、ダッシュボードの[推奨される操作]ペインに「クラスタ<name>の既知のセキュリティの脆弱性を修正する」という推奨事項が表示されます。ダッシュボードの推奨事項で、*[確認と修正]*をクリックすると、Digital AdvisorとCommon Vulnerability & Exposure（CVE）の記事を確認してセキュリティリスクを解決するよう提案されます。複数のセキュリティリスクがある場合は、Digital Advisorで情報を確認します。

を参照してください "Digital Advisorのドキュメント"。

Google Cloud Platformにバックアップ

このリリースでは、バックアップ先をGoogle Cloud Platformバケットに設定できます。以前は、バックアップ先を追加できるのはNetApp StorageGRID、Amazon Web Services、Microsoft Azureのみでした。

"BlueXP ランサムウェア対策の設定の詳細"です。

Google Cloud Platformのサポート

このサービスでは、ストレージ保護のためにCloud Volumes ONTAP for Google Cloud Platformがサポートされるようになりました。以前は、Amazon Web ServicesとMicrosoft AzureのCloud Volumes ONTAPとオンプレミスのNASのみがサポートされていました。

"BlueXP ランサムウェア対策、サポート対象のデータソース、バックアップ先、作業環境について説明します。"です。

ロールベースアクセス制御

Role-Based Access Control（RBAC；ロールベースアクセス制御）を使用して、特定のアクティビティにアクセスを制限できるようになりました。BlueXP ランサムウェア対策では、BlueXP の2つのロール、BlueXP アカウント管理者と非アカウント管理者（ビューア）を使用します。

各ロールで実行できるアクションの詳細については、を参照してください "ロールベースアクセス制御Privileges"。

2024 年 8 月 5 日

Splunk Cloudによる脅威の検出

セキュリティおよびイベント管理システム（SIEM）にデータを自動的に送信して、脅威の分析と検出を行うことができます。以前のリリースでは、SIEMとしてAWS Security Hubのみを選択できました。このリリースでは、AWS Security HubまたはSplunk CloudをSIEMとして選択できます。

"BlueXP ランサムウェア対策の設定の詳細"です。

2024年7月1日

お客様所有のライセンスを使用（**BYOL**）

このリリースでは、BYOLライセンスを使用できます。BYOLライセンスは、NetApp営業担当から取得したNetAppライセンスファイル（NLF）です。

"ライセンスの設定に関する詳細情報"。

アプリケーションワークロードをファイルレベルでリストア

アプリケーションワークロードをファイルレベルでリストアする前に、攻撃の影響を受けた可能性があるファイルのリストを表示し、リストアするファイルを特定できるようになりました。BlueXPランサムウェア対策でリストアするファイルを選択したり、アラートの影響を受けたすべてのファイルを記載したCSVファイルをアップロードしたり、リストアするファイルを手動で特定したりできます。

このリリースでは、アカウント内のすべてのBlueXPコネクタがPodmanを使用していない場合、単一ファイルのリストア機能が有効になります。それ以外の場合、そのアカウントでは無効になります。

"ランサムウェア攻撃からのリカバリの詳細"です。

影響を受けるファイルのリストをダウンロードする

アプリケーションワークロードをファイルレベルでリストアする前に、[アラート]ページにアクセスして影響を受けたファイルのリストをCSVファイルにダウンロードし、[リカバリ]ページを使用してCSVファイルをアップロードできるようになりました。

"アプリケーションをリストアする前に影響を受けるファイルをダウンロードする方法の詳細"です。

保護プランの削除

このリリースでは、ランサムウェア対策戦略を削除できるようになりました。

"ワークロードの保護とランサムウェア対策戦略の管理の詳細"です。

2024年6月10日

プライマリストレージでの**Snapshot**コピーロック

これを有効にすると、プライマリストレージ上のSnapshotコピーがロックされ、ランサムウェア攻撃を受けてバックアップ先にたどり着いた場合でも、一定期間変更や削除ができないようになります。

"ランサムウェア対策戦略におけるワークロードの保護とバックアップロックの有効化の詳細"。

Cloud Volumes ONTAP for Microsoft Azureのサポート

このリリースでは、Cloud Volumes ONTAP for AWSとオンプレミスのONTAP NASに加え、作業環境としてCloud Volumes ONTAP for Microsoft Azureがサポートされます。

"Azure での Cloud Volumes ONTAP のクイックスタート"

"BlueXPランサムウェア対策の詳細をご確認ください"。

バックアップ先として**Microsoft Azure**を追加

AWSおよびNetApp StorageGRIDとともに、バックアップ先としてMicrosoft Azureを追加できるようになりました。

"保護設定の構成方法の詳細"。

2024年5月14日

ライセンスの更新

90日間の無償トライアルにサインアップできます。まもなく、Amazon Web Services Marketplaceで従量課金制サブスクリプションを購入するか、お客様所有のNetAppライセンスを使用できるようになります。

"ライセンスの設定に関する詳細情報"。

CIFSプロトコル

AWSの作業環境で、NFSプロトコルとCIFSプロトコルの両方を使用したオンプレミスのONTAPとCloud Volumes ONTAPがサポートされるようになりました。以前のリリースでは、NFSプロトコルのみがサポートされていました。

ワークロードの詳細

このリリースでは、ワークロード保護の評価を改善するために、[保護]ページと[その他]ページのワークロード情報に詳細が表示されるようになりました。ワークロードの詳細から、現在割り当てられているポリシーと設定されているバックアップ先を確認できます。

"[保護ページでのワークロードの詳細の表示に関する詳細を確認する"]。

アプリケーションと整合性のある保護とリカバリ、VMと整合性のある保護とリカバリ

NetApp SnapCenterソフトウェアを使用したアプリケーションと整合性のある保護と、SnapCenter Plug-in for VMware vSphereを使用したVMと整合性のある保護を実行できるようになりました。休止状態と整合性のある状態を実現して、リカバリが必要になった場合のデータ損失を回避できます。リカバリが必要な場合は、アプリケーションまたはVMを以前の状態にリストアできます。

"ワークロードの保護に関する詳細情報"。

ランサムウェア対策戦略

ワークロードにSnapshotポリシーまたはバックアップポリシーがない場合は、ランサムウェア対策戦略を作成できます。この戦略には、このサービスで作成する次のポリシーを含めることができます。

- スナップショットポリシー
- バックアップポリシー
- 検出ポリシー

"ワークロードの保護に関する詳細情報"。

脅威の検出

サードパーティのセキュリティおよびイベント管理（SIEM）システムを使用して、脅威検出を有効にすることができるようになりました。ダッシュボードに「脅威検出を有効にする」という新しい推奨事項が表示されるようになりました。これは、[設定]ページで設定できます。

"設定オプションの設定の詳細"。

誤検出アラートを却下する

[Alerts]タブで、誤検出を却下したり、データをすぐにリカバリしたりできるようになりました。

"ランサムウェアのアラートへの対応の詳細"です。

検出ステータス

[Protection]ページに、ワークロードに適用されたランサムウェアの検出ステータスを示す新しい検出ステータスが表示されます。

"ワークロードの保護と保護ステータスの表示に関する詳細情報"。

CSVファイルのダウンロード

CSVファイル*は、[保護]、[アラート]、[リカバリ]の各ページからダウンロードできます。

"ダッシュボードおよびその他のページからのCSVファイルのダウンロードに関する詳細情報"。

ドキュメントへのリンク

UIに[View Documentation]リンクが追加されました。このドキュメントには、[ダッシュボード][アクション]*

オプションからアクセスできます  オプション"] 。「**What's new**」*を選択して詳細をリリースノートに表示するか、「Documentation」*を選択してBlueXPランサムウェア対策ドキュメントのホームページを表示します。

BlueXPのバックアップとリカバリ

作業環境でBlueXPのバックアップとリカバリサービスを有効にしておく必要はなくなりました。を参照して "前提条件"BlueXPランサムウェア対策サービスは、[Settings]オプションを使用してバックアップ先を設定するのに役立ちます。を参照して "セツテイノセツテイ"

設定オプション

BlueXP ランサムウェア対策設定でバックアップ先を設定できるようになりました。

"設定オプションの設定の詳細"。

2024年3月5日

保護ポリシーの管理

事前定義されたポリシーの使用に加えて、ポリシーを作成できるようになりました。 "ポリシーの管理の詳細"です。

セカンダリストレージの変更不可（**DataLock**）

オブジェクトストアでNetApp DataLockテクノロジを使用して、セカンダリストレージ内のバックアップを変更不可にできるようになりました。 "保護ポリシーの作成に関する詳細情報"です。

NetApp StorageGRIDへの自動バックアップ

AWSを使用するだけでなく、バックアップ先としてStorageGRIDを選択できるようになりました。 "バックアップ先の設定に関する詳細情報"です。

攻撃の可能性を調査するための追加機能

さらにフォレンジックの詳細を表示して、検出された攻撃の可能性を調査できるようになりました。 "ランサムウェアのアラートが検出された場合の対応の詳細"です。

リカバリプロセス

回復プロセスが強化されました。ワークロードのボリューム単位またはすべてのボリュームをリカバリできるようになりました。 "ランサムウェア攻撃からのリカバリの詳細（インシデントの中和後）"です。

"BlueXPランサムウェア対策の詳細をご確認ください"。

2023年10月6日

BlueXPランサムウェア対策サービスは、データの保護、潜在的な攻撃の検出、ランサムウェア攻撃からのデータのリカバリを行うSaaS解決策です。

プレビュー版では、オンプレミスのNASストレージ上のOracle、MySQL、VMデータストア、ファイル共有、およびCloud Volumes ONTAP on AWS（NFSプロトコルを使用）のアプリケーションベースのワークロードをBlueXP 組織全体で個別に保護し、Amazon Web Servicesクラウドストレージにデータをバックアップします。

BlueXPのランサムウェア対策サービスでは、複数のNetAppテクノロジをフルに活用できるため、データセキュリティ管理者やセキュリティ運用エンジニアは次の目標を達成できます。

- すべてのワークロードに対するランサムウェア対策を一目で確認できます。
- ランサムウェア対策に関する推奨事項を分析
- BlueXPのランサムウェア対策に関する推奨事項に基づいて、保護態勢を強化
- ランサムウェア対策ポリシーを割り当てて、主要なワークロードとハイリスクデータをランサムウェア攻撃から保護します。
- ワークロードの健全性を監視してランサムウェア攻撃からデータの異常を検出
- ランサムウェアのインシデントがワークロードに与える影響を迅速に評価します。
- データをリストアし、保存されたデータからの再感染を防ぐことで、ランサムウェアのインシデントからインテリジェントにリカバリします。

"BlueXPランサムウェア対策の詳細をご確認ください"。

著作権に関する情報

商標に関する情報