リリース ノート

NetApp Ransomware Resilience

NetApp
March 05, 2026

目次

リリース ノート

NetApp Ransomware Resilienceの新機能

NetApp Ransomware Resilienceの新機能についてご確認ください。

2026年2月16日

Azure NetApp Files サポート

Ransomware Resilienceは、Azure NetApp Filesシステムをサポートするようになり、Azure NetApp Filesでランサムウェアの脅威を効率的に検出して対応できるようになりました。ワークロードを検出すると、Ransomware ResilienceはAzure NetApp Filesを表示し、保護ダッシュボードに表示します。Azure NetApp FilesのRansomware Resilienceサポートには、スナップショットのみを使用した検出および保護戦略が含まれます。Azure NetApp Filesのサポートは現在プレビュー段階です。

詳細については、"ランサムウェア耐性について学ぶ"を参照してください。

ユーザー行動アラートからユーザーを除外する

NetApp Ransomware Resilienceにより、ユーザー行動アラートから特定のユーザーを除外できるようになりました。信頼できるユーザーを除外すると、誤検知や不要なアラートを防ぐことができます。

詳細については、"アラートからユーザーを除外する"を参照してください。

ユーザー行動アクティビティの保護グループサポート

Ransomware Resilience保護グループは、疑わしいユーザーの行動を検出するための検出ポリシーをサポートするようになりました。保護グループにランサムウェア保護戦略を適用すると、ワークロード全体にポリシーが適用され、サイバーセキュリティ体制の管理が効率化されます。

詳細については、"保護グループを作成する"を参照してください。

2026年1月19日

サポートされていないボリューム

Ransomware Resilienceレポートでは、概要レポートでサポートされているボリュームとサポートされていないボリュームに関する情報が取得されるようになりました。この情報を使用して、システム内のボリュームがランサムウェア保護の対象外となる理由を診断します。

詳細については、 "ランサムウェア耐性レポートをダウンロード"。

2026年1月12日

スナップショットを**ONTAP**に複製する

ランサムウェア耐性は、スナップショットのレプリケーションをセカンダリONTAPサイトに追加できるようになりました。レプリケーションポリシーを使用する保護グループを使用すると、ワークロードごとに同じ宛

先または異なる宛先にレプリケートできます。レプリケーションを含むランサムウェア保護戦略を作成することも、定義済みの戦略を使用することもできます。

詳細については、 "ランサムウェア耐性でワークロードを保護する"。

ランサムウェア耐性からワークロードを除外する

ランサムウェア耐性では、システム内の特定のワークロードを保護およびランサムウェア耐性ダッシュボードから除外することがサポートされるようになりました。検出後にワークロードを除外し、ランサムウェア保護を追加する場合は再度含めることができます。除外されたワークロードについては課金されません。

詳細については、 "ワークロードを除外する"。

アラートをレビュー中としてマークする

Ransomware Resilience では、アラートを「レビュー中」としてマークできるようになりました。「レビュー中」ラベルを使用すると、アクティブなランサムウェアの脅威をトリアージおよび管理する際に、チーム全体の明確性が向上します。

詳細については、 "ランサムウェア耐性のアラートを管理する"。

2025年12月8日

拡張機能のブロックはワークロードレベルで有効になります

拡張機能のブロックを有効にすると、ストレージ VM レベルではなくワークロード レベルで有効になります。

ユーザー行動アラートステータスの編集

Ransomware Resilience では、ユーザー行動アラートのステータスを編集できるようになりました。アラートを手動で解除したり解決したりできます。

詳細については、 "ランサムウェア耐性のアラートを管理する"。

複数のコンソールエージェントのサポート

Ransomware Resilience では、複数のコンソール エージェントを使用して同じシステムを管理することがサポートされるようになりました。

コンソールエージェントの詳細については、以下を参照してください。"コンソールエージェントを作成する"。

2025年11月10日

このリリースには、全般的な機能強化と改善が含まれています。

2025年10月6日

BlueXP ransomware protectionはNetApp Ransomware Resilienceました

BlueXP ransomware protectionサービスの名前がNetApp Ransomware Resilienceに変更されました。

BlueXPはNetApp Consoleになりました

NetApp Consoleは、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのストレージとデータ サービスの集中管理を提供し、リアルタイムの分析情報、ワークフローの高速化、管理の簡素化を実現します。

変更内容の詳細については、 "NetApp Consoleのリリースノート" 。

データ侵害検出

Ransomware Resilience には、数ステップでアクティブ化できる新しい検出メカニズムが含まれており、データ侵害の早期指標として異常なユーザー読み取りを検出します。ランサムウェア耐性は、過去のデータから予想される通常の動作のプロファイルである履歴ベースラインを作成することにより、ユーザーの読み取りイベントを収集および分析します。新しいユーザーのアクティビティがこの確立された標準から大幅に逸脱すると(予期しない読み取りの急増と疑わしい読み取りパターンの組み合わせなど)、アラートが生成されます。Ransomware Resilience には、疑わしい読み取りパターンを検出する AI モデルが含まれています。

ストレージ層での ARP による暗号化検出とは異なり、ユーザー動作の異常の検出は、Ransomware Resilience SaaS サービスで FPolicy イベントを収集することによって行われます。

新しい"ランサムウェア耐性ユーザー行動管理者およびランサムウェア耐性ユーザー行動閲覧者"疑わしいユーザー行動の検出設定にアクセスするロール。

詳細については、"不審なユーザーアクティビティの検出を有効にする"そして"異常なユーザー行動を表示する"。

追加の不審なユーザーアクティビティの検出

データ侵害の検出に加えて、Ransomware Resilience は、観察された疑わしいユーザー アクティビティに基づいて次の種類のアラートも検出します。

- データ破壊 - 潜在的な攻撃 - ファイルの削除数が過去の標準を超えると、潜在的な攻撃の重大度を示すアラートが作成されます。
- 疑わしいユーザー行動 - 潜在的な攻撃 - ランサムウェア攻撃に類似したシーケンスでの読み取り、名前変更、削除操作が観察された場合、潜在的な攻撃の重大度を持つアラートが作成されます。
- 疑わしいユーザー行動 - 警告 - ファイルアクティビティ（読み取り、削除、名前変更など）の合計数が過去の標準を超えると、警告の重大度を持つアラートが作成されます。

データ侵害検出のための新しいユーザーロール

疑わしいユーザー アクティビティのアラートを管理するために、Ransomware Resilience では、コンソール組織管理者が疑わしいユーザー アクティビティの検出へのアクセスを許可するための 2 つの新しいロール(Ransomware Resilience ユーザー ビヘイビア管理者と Ransomware Resilience ユーザー ビヘイビア閲覧者)を導入しました。

疑わしいユーザーの行動設定を構成するには、ユーザー行動管理者である必要があります。ランサムウェア耐性管理者ロールは、疑わしいユーザーの行動設定の構成ではサポートされていません。

詳細については、以下を参照してください。 "NetApp Ransomware Resilienceロールベースアクセス" 。

2025年8月12日

このリリースには、全般的な機能強化と改善が含まれています。

2025年7月15日

SANワークロードのサポート

このリリースには、BlueXP ransomware protectionにおける SAN ワークロードのサポートが含まれています。NFS および CIFS ワークロードに加えて、SAN ワークロードも保護できるようになりました。

詳細については、 "BlueXP ransomware protectionの前提条件" 。

ワークロード保護の改善

このリリースでは、NetAppの他のツール（BlueXPバックアップとリカバリなど）のスナップショットポリシーやバックアップポリシーを使用したワークロードの設定プロセスが改善されました。以前のリリースでは、BlueXPランサムウェア対策は他のツールからのポリシーを検出し、検出ポリシーの変更のみを許可していました。このリリースでは、スナップショットポリシーとバックアップポリシーをBlueXPランサムウェア対策ポリシーに置き換えるか、他のツールのポリシーを引き続き使用できるようになりました。

詳細については、"ワークロードを保護する" 。

メール通知

BlueXP ransomware protectionが攻撃の可能性を検出すると、 BlueXP通知に通知が表示され、設定した電子メール アドレスに電子メールが送信されます。

電子メールには、重大度、影響を受けるワークロード、 BlueXP ransomware protectionの アラート タブのアラートへのリンクに関する情報が含まれています。

BlueXP ransomware protectionでセキュリティおよびイベント管理 (SIEM) システムを構成した場合、サービスはアラートの詳細を SIEM システムに送信します。

詳細については、"検出されたランサムウェアアラートを処理する" 。

2025年6月9日

ランディングページの更新

このリリースには、BlueXP ransomware protectionのランディング ページの更新が含まれており、無料トライアルの開始と検出が容易になります。

準備訓練の最新情報

以前は、新しいサンプル ワークロードに対する攻撃をシミュレートすることで、ランサムウェア対策訓練を実行できました。この機能を使用すると、シミュレートされた攻撃を調査し、ワークロードを回復できます。この機能を使用して、アラート通知、応答、および回復をテストします。必要に応じてこれらのドリルを実行し、スケジュールを設定します。

このリリースでは、 BlueXP ransomware protectionダッシュボードの新しいボタンを使用して、テスト ワークロードでランサムウェア準備ドリルを実行できるようになりました。これにより、制御された環境内でランサムウェア攻撃のシミュレート、その影響の調査、ワークロードの効率的な回復が容易になります。

NFS ワークロードに加えて、CIFS (SMB) ワークロードでも準備ドリルを実行できるようになりました。

詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。

BlueXP classificationの更新を有効にする

BlueXP ransomware protectionサービス内でBlueXP classificationを使用する前に、 BlueXP classificationを有効にしてデータをスキャンする必要があります。データを分類すると、セキュリティ リスクを増大させる可能性のある個人を特定できる情報 (PII) を見つけるのに役立ちます。

BlueXP ransomware protection内から、ファイル共有ワークロードにBlueXP classificationを展開できます。プライバシー露出*列で、*露出の特定*オプションを選択します。分類サービスを有効にしている場合、このアクションによって露出が識別されます。それ以外の場合、このリリースでは、ダイアログ ボックスに**BlueXP classification**を展開するオプションが表示されます。 *デプロイ を選択すると、 BlueXP classificationサービスのランディング ページに移動し、そのサービスをデプロイできます。W

詳細については、 "クラウドでBlueXP classificationを展開"を参照してください。BlueXP ransomware protection内でサービスを使用する方法については、 "BlueXP classificationで個人を特定できる情報をスキャン"を参照してください。

2025年5月13日

BlueXP ransomware protectionにおけるサポートされていない作業環境の報告

検出ワークフロー中に、サポートされているワークロードまたはサポートされていないワークロードにマウスを移動すると、 BlueXP ransomware protectionによって詳細が報告されます。これにより、一部のワークロードがBlueXP ransomware protectionサービスによって検出されない理由を理解するのに役立ちます。

サービスが作業環境をサポートしない理由は多数あります。たとえば、作業環境のONTAPバージョンが必要なバージョンよりも低い可能性があります。サポートされていない作業環境にマウスを移動すると、ツールヒントに理由が表示されます。

初期検出中にサポートされていない作業環境を表示でき、結果をダウンロードすることもできます。設定ページの ワークロード検出 オプションから検出結果を表示することもできます。

詳細については、 "BlueXP ransomware protectionでワークロードを発見" 。

2025年4月29日

Amazon FSx for NetApp ONTAPのサポート

このリリースでは、Amazon FSx for NetApp ONTAPがサポートされます。この機能は、BlueXP ransomware protectionを使用して FSx for ONTAPワークロードを保護するのに役立ちます。

FSx for ONTAP は、クラウドでNetApp ONTAPストレージのパワーを提供する、完全に管理されたサービスです。ネイティブ AWS サービスの俊敏性と拡張性を備え、オンプレミスで使用するのと同じ機能、パフォーマンス、管理機能を提供します。

BlueXP ransomware protectionワークフローに次の変更が加えられました。

- 検出には、FSx for ONTAP 9.15 作業環境のワークロードが含まれます。
- [保護] タブには、FSx for ONTAP環境のワークロードが表示されます。この環境では、FSx for ONTAPバックアップ サービスを使用してバックアップ操作を実行する必要があります。 BlueXP ransomware protectionスナップショットを使用してこれらのワークロードを復元できます。

FSx for ONTAPで実行されているワークロードのバックアップ ポリシーは、 BlueXPでは設定できません。 Amazon FSx for NetApp ONTAPに設定されている既存のバックアップポリシーは変更されません。

- アラート インシデントには、新しい FSx for ONTAP作業環境が表示されます。

詳細については、 "BlueXP ransomware protectionと動作環境について学ぶ" 。

サポートされているオプションの詳細については、 "BlueXP ransomware protectionの制限" 。

BlueXPアクセスロールが必要

BlueXP ransomware protectionを表示、検出、または管理するには、組織管理者、フォルダーまたはプロジェクト管理者、ランサムウェア保護管理者、またはランサムウェア保護閲覧者のいずれかのアクセス ロールが必要です。

"すべてのサービスに対するBlueXPのアクセスロールについて学ぶ" 。

2025年4月14日

即応訓練報告書

このリリースでは、ランサムウェア攻撃の準備訓練レポートを確認できるようになりました。準備ドリルを使用すると、新しく作成されたサンプル ワークロードに対するランサムウェア攻撃をシミュレートできます。次に、シミュレートされた攻撃を調査し、サンプルのワークロードを回復します。この機能は、アラート通知、対応、および回復プロセスをテストすることで、実際のランサムウェア攻撃が発生した場合に備えて準備ができていることを確認するのに役立ちます。

詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。

新しいロールベースのアクセス制御のロールと権限

以前は、ユーザーの責任に基づいて役割と権限を割り当てることができました。これにより、 BlueXP ransomware protectionへのユーザー アクセスを管理するのに役立ちました。このリリースでは、権限が更新されたBlueXP ransomware protectionに固有の 2 つの新しいロールが追加されました。新しい役割は次のとおりです。

- ランサムウェア保護管理者
- ランサムウェア保護ビューア

権限の詳細については、 "BlueXP ransomware protection機能へのロールベースのアクセス" 。

支払いの改善

このリリースには、支払いプロセスに対するいくつかの改善が含まれています。

詳細については、 "ライセンスと支払いオプションを設定する" 。

2025年3月10日

攻撃をシミュレートして対応する

このリリースでは、ランサムウェア攻撃をシミュレートして、ランサムウェアアラートへの対応をテストします。この機能は、アラート通知、対応、および回復プロセスをテストすることで、実際のランサムウェア攻撃が発生した場合に備えて準備ができていることを確認するのに役立ちます。

詳細については、 "ランサムウェア攻撃への備えの訓練を実施する" 。

発見プロセスの強化

このリリースには、選択的検出および再検出プロセスの機能強化が含まれています。

- このリリースでは、以前に選択した作業環境に追加された新しく作成されたワークロードを検出できます。
- このリリースでは、新しい作業環境を選択することもできます。この機能は、環境に追加された新しいワークロードを保護するのに役立ちます。
- これらの検出プロセスは、検出プロセス中に最初に実行することも、設定オプション内で実行することもできます。

詳細については、 "以前に選択した作業環境に対して新しく作成されたワークロードを検出する"そして "設定オプションで機能を設定する"。

高度な暗号化が検出されるとアラートが発せられます

このリリースでは、ファイル拡張子を大幅に変更しなくても、ワークロードで高度な暗号化が検出された場合にアラートを表示できます。この機能は、 ONTAP Autonomous Ransomware Protection (ARP) AI を使用し、ランサムウェア攻撃のリスクがあるワークロードを特定するのに役立ちます。この機能を使用して、拡張子の変更の有無にかかわらず、影響を受けるファイルのリスト全体をダウンロードします。

詳細については、 "検出されたランサムウェアアラートに応答する" 。

2024年12月16日

Data Infrastructure Insightsストレージワークロードセキュリティを使用して異常なユーザー行動を検出する

このリリースでは、 Data Infrastructure Insights Storage Workload Security を使用して、ストレージ ワークロード内の異常なユーザー動作を検出できます。この機能は、潜在的なセキュリティ脅威を特定し、悪意のある可能性のあるユーザーをブロックしてデータを保護するのに役立ちます。

詳細については、 "検出されたランサムウェアアラートに応答する" 。

Data Infrastructure Insights Storage Workload Security を使用して異常なユーザー動作を検出する前に、BlueXP ransomware protectionの*設定* オプションを使用してオプションを構成する必要があります。

参照 "BlueXP ransomware protection設定を構成する"。

検出して保護するワークロードを選択する

このリリースでは、次のことが可能になります。

- 各コネクタ内で、ワークロードを検出する作業環境を選択します。環境内の特定のワークロードを保護し、他のワークロードは保護しない場合は、この機能が役立つ可能性があります。
- ワークロードの検出中に、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。この機能を使用すると、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に対して新しく作成されたワークロードを検出します。

参照 "ワークロードを発見する"。

2024年11月7日

データ分類を有効にし、個人を特定できる情報 **(PII)** をスキャンします

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 classificationを有効にして、ファイル共有ワークロード内のデータをスキャンおよび分類できます。データを分類すると、データに個人情報やプライベートな情報が含まれているかどうかを識別するのに役立ち、セキュリティ リスクが増大する可能性があります。このプロセスはワークロードの重要性にも影響を及ぼし、適切なレベルの保護でワークロードを保護していることを確認するのに役立ちます。

BlueXP ransomware protectionにおける PII データのスキャンは、 BlueXP classificationを導入したお客様には一般にご利用いただけます。 BlueXP classification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顧客のクラウドに展開できます。

スキャンを開始するには、Protectionページで、ProtectionダッシュボードのPrivacy exposure列にある*Identify exposure*を選択します。詳細については、 "BlueXP classificationで個人を特定できる機密データをスキャンする"を参照してください。

Microsoft Sentinel との **SIEM** 統合

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

"BlueXP ransomware protection設定の構成について詳しくは、こちらをご覧ください。"。

今すぐ**30**日間無料トライアル

このリリースでは、 BlueXP ransomware protectionの新規導入に 30 日間の無料トライアルが提供されます。以前は、 BlueXP ransomware protectionは90 日間の無料トライアルを提供していました。すでに 90 日間の無料トライアル中の場合は、そのオファーは 90 日間継続されます。

Podman のファイルレベルでアプリケーション ワークロードを復元する

アプリケーション ワークロードをファイル レベルで復元する前に、攻撃の影響を受けた可能性のあるファイルの一覧を表示し、復元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 (以前のアカウント) 内の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。 Podman で有効にな

りました。 BlueXP ransomware protectionで復元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リストした CSV ファイルをアップロードしたり、復元するファイルを手動で特定したりすることができます。

"ランサムウェア攻撃からの回復について詳しくはこちら" 。

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まとめることができるため、データ資産をより簡単に保護できるようになりました。このサービスでは、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について詳しくは、こちらをご覧ください。" 。

2024年9月2日

Digital Advisorによるセキュリティリスク評価

BlueXP ransomware protectionは、NetApp Digital Advisorからクラスタに関連する高および重大なセキュリティリスクに関する情報を収集するようになりました。リスクが見つかった場合、BlueXP ransomware protectionはダッシュボードの*推奨アクション*ペインに推奨事項を表示します：「クラスタ上の既知のセキュリティ脆弱性を修正する<name>。」ダッシュボードの推奨事項から*レビューして修正*を選択すると、セキュリティリスクを解決するためにDigital AdvisorとCommon Vulnerability & Exposure（CVE）記事を確認することが提案されます。複数のセキュリティリスクがある場合は、Digital Advisorで情報を確認してください。

参照 "Digital Advisorのドキュメント"。

Google Cloud Platform へのバックアップ

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 ransomware protection設定の構成について詳しくは、こちらをご覧ください。"。

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、Google Cloud Platform 用のCloud Volumes ONTAP をサポートするようになりました。以前は、このサービスはオンプレミスの NAS に加えて、Amazon Web Services および Microsoft Azure 向けのCloud Volumes ONTAPのみをサポートしていました。

"BlueXP ransomware protectionとサポートされているデータソース、バックアップ先、作業環境について学びます" 。

ロールベース アクセス制御

ロールベースのアクセス制御 (RBAC) を使用して、特定のアクティビティへのアクセスを制限できるようになりました。 BlueXP ransomware protection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 (閲覧者)) を使用します。

各ロールが実行できるアクションの詳細については、 "ロールベースのアクセス制御権限" 。

2024年8月5日

Splunk Cloudによる脅威検出

脅威の分析と検出のために、データをセキュリティおよびイベント管理システム (SIEM) に自動的に送信できます。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、SIEM として AWS Security Hub または Splunk Cloud を選択できるようになりました。

"BlueXP ransomware protection設定の構成について詳しくは、こちらをご覧ください。"。

2024年7月1日

ライセンス持ち込み（BYOL）

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

"ライセンスの設定について詳しくはこちら" 。

ファイルレベルでアプリケーションのワークロードを復元する

アプリケーション ワークロードをファイル レベルで復元する前に、攻撃の影響を受けた可能性のあるファイルの一覧を表示し、復元するファイルを特定できるようになりました。 BlueXP ransomware protectionで復元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リストした CSV ファイルをアップロードしたり、復元するファイルを手動で特定したりすることができます。

> 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でも、単一ファイルの復元機能が有効になります。それ以外の場合、そのアカウントは無効になります。

"ランサムウェア攻撃からの回復について詳しくはこちら" 。

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 レベルで復元する前に、[アラート] ページにアクセスして影響を受けるファイルのリストを CSV ファイルでダウンロードし、[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復元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について詳しくは、こちらをご覧ください。" 。

保護プランを削除する

このリリースでは、ランサムウェア保護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保護戦略の管理について詳しく学ぶ" 。

2024年6月10日

プライマリストレージ上のスナップショットコピーのロック

これを有効にすると、プライマリ ストレージ上のスナップショット コピーがロックされ、ランサムウェア攻撃がバックアップ ストレージの保存先にまで到達した場合でも、一定期間スナップショット コピーを変更または削除できなくなります。

"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について詳しくは、こちらをご覧ください。" 。

Microsoft Azure 向け**Cloud Volumes ONTAP**のサポート

このリリースでは、Cloud Volumes ONTAP for AWS およびオンプレミスのONTAP NAS に加えて、 Cloud Volumes ONTAP for Microsoft Azure をシステムとしてサポートします。

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

"BlueXP ransomware protectionについて学ぶ" 。

バックアップ先として **Microsoft Azure** が追加されました

AWS およびNetApp StorageGRIDに加えて、Microsoft Azure をバックアップ先として追加できるようになりました。

"保護設定を構成する方法について詳しくは、こちらをご覧ください。"。

2024年5月14日

ライセンスの更新

90 日間の無料トライアルにご登録いただけます。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したり、独自の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ついて詳しくはこちら" 。

CIFSプロトコル

このサービスでは、NFS プロトコルと CIFS プロトコルの両方を使用して、AWS システム内のオンプレミスのONTAPとCloud Volumes ONTAP をサポートす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、保護ページやその他のページのワークロード情報にさらに詳しい情報が提供され、ワークロード保護の評価が改善されました。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を確認し、構成されているバックアップ先を確認できます。

"保護ページでワークロードの詳細を表示する方法の詳細" 。

ランサムウェア対策戦略

ワークロードにスナップショットまたはバックアップ ポリシーが存在しない場合は、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るランサムウェア保護戦略を作成できます。

- 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ついて詳しく見る" 。

脅威検出

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、脅威検出を有効にできるようになりました。ダッシュボードには、「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構成できます。

"設定オプションの構成について詳しくは"。

誤検知アラートを無視する

[アラート] タブから、誤検知を無視したり、データをすぐに回復したりできるようになりました。

"ランサムウェアアラートへの対応について詳しくはこちら" 。

検出ステータス

新しい検出ステータスが [保護] ページに表示されます。これには、ワークロードに適用されたランサムウェア検出の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ついて詳しくは、こちらをご覧ください。" 。

CSVファイルをダウンロード

保護、アラート、回復のページから CSV ファイル* をダウンロードできます。

"ダッシュボードやその他のページからCSVファイルをダウンロードする方法について詳しくは、こちらをご覧ください。" 。

ドキュメントリンク

ドキュメントの表示リンクが UI に含まれるようになりました。このドキュメントにはダッシュボードの「アクション」からアクセスできます。 オプション。リリース ノートの詳細を表示するには 新機能 を選択し、 BlueXP ransomware protectionドキュメントのホーム ページを表示するには ドキュメント を選択してください。

BlueXP backup and recovery

BlueXPバックアップおよびリカバリサービスをシステム上で有効にしておく必要がなくなりました。"前提条件"を参照してください。BlueXPランサムウェア保護サービスは、設定オプションを通じてバックアップ先を

構成するのに役立ちます。"設定を構成する"を参照してください。

設定オプション

BlueXP ransomware protection設定でバックアップ先を設定できるようになりました。

"設定オプションの構成について詳しくは"。

2024年3月5日

保護ポリシー管理

定義済みのポリシーを使用するだけでなく、ポリシーを作成できるようになりました。 "ポリシー管理の詳細"。

二次ストレージの不変性（**DataLock**）

オブジェクト ストア内のNetApp DataLock テクノロジーを使用して、セカンダリ ストレージ内のバックアップを不変にできるようになりました。 "保護ポリシーの作成について詳しくは" 。

NetApp StorageGRIDへの自動バックアップ

AWSの使用に加えて、StorageGRIDをバックアップ先として選択できるようになりました "バックアップ先の設定について詳しくは"。

潜在的な攻撃を調査するための追加機能

検出された潜在的な攻撃を調査するために、より詳細なフォレンジック情報を表示できるようになりました。 "検出されたランサムウェアアラートへの対応について詳しくは、こちらをご覧ください。" 。

回復プロセス

回復プロセスが強化されました。これで、ワークロードのボリュームごとに、またはすべてのボリュームを回復できるようになりました。 "ランサムウェア攻撃からの復旧（インシデントが中和された後）について詳しくは、こちらをご覧ください。" 。

"BlueXP ransomware protectionについて学ぶ" 。

2023年10月6日

BlueXP ransomware protectionサービスは、データを保護し、潜在的な攻撃を検出し、ランサムウェア攻撃からデータを回復するための SaaS ソリューションです。

プレビュー バージョンでは、このサービスは、Oracle、VM データストア、オンプレミスの NAS ストレージ上のファイル共有、およびBlueXP組織全体の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個別に保護し、データを Amazon Web Services クラウド ストレージにバックアップします。

BlueXP ransomware protectionサービスは、 NetAppの複数のテクノロジをフル活用して、データ セキュリティ管理者またはセキュリティ運用エンジニアが次の目標を達成できるようにします。

- すべてのワークロードにおけるランサムウェア保護を一目で確認できます。
- ランサムウェア対策の推奨事項を理解する
- BlueXP ransomware protectionの推奨事項に基づいて保護体制を改善します。
- ランサムウェア保護ポリシーを割り当てて、主要なワークロードと高リスクのデータをランサムウェア攻撃から保護します。
- データの異常を探しながら、ランサムウェア攻撃に対するワークロードの健全性を監視します。
- ランサムウェア 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。
- データを復元し、保存されたデータからの再感染が発生しないようにすることで、ランサムウェア インシデントからインテリジェントに回復します。

"BlueXP ransomware protectionについて学ぶ" 。

NetApp Ransomware Resilienceの既知の制限

今回のリリースでサポートされていない、または今回のリリースでは正常に機能しないプラットフォーム、デバイス、機能が記載されています。これらの制限事項をよく確認してください。

準備訓練のリセットオプションの問題

ランサムウェア攻撃対策ドリル用にONTAP 9.11.1 ボリュームを選択すると、Ransomware Resilience によってアラートが送信されます。 「ボリュームへのクローン」オプションを使用してデータを回復し、ドリルをリセットすると、リセット操作は失敗します。

Amazon FSx for NetApp ONTAP の制限

Amazon FSx for NetApp ONTAPシステムは、Ransomware Resilience でサポートされています。Amazon FSx for ONTAPには次の制限が適用されます。

- Amazon FSx for ONTAP ではバックアップポリシーはサポートされていません。この環境では、Amazon FSx for ONTAP のバックアップ機能を使用してバックアップ操作を実行する必要があります。NetApp Ransomware Resilience を使用してこれらのワークロードを復元できます。
- 復元操作はスナップショットからのみ実行されます。

Azure NetApp Files の制限事項

Azure NetApp Files は、NetApp Ransomware Resilience でサポートされています。Azure NetApp Files には以下の制限事項が適用されます：

- バックアップポリシーを使用したランサムウェア保護戦略は、Azure NetApp Files ではサポートされていません。代わりに、Azure NetApp Files バックアップを使用できます。
- レプリケーションを使用したランサムウェア保護戦略は Azure NetApp Files ではサポートされていません。
- 保護戦略を選択するときは、スナップショットスケジュールがAzure NetApp Filesと互換性があることを確認してください。Azure NetApp Filesで利用できる最も頻繁なスナップショットスケジュールは1時間ごとです。