ソリューション概要

NETAPP BLUEXP ランサムウェア対策ソリューション

ワークロードのデータ損失を最小限に抑え、すばやく復旧するために必要なインテリジェンスと支援を提供

ランサムウェア攻撃への備えは万全ですか？
ランサムウェア攻撃に備えることもそれに対抗することも、今日では必須事項であり、選択の余地はありません。攻撃はより巧妙になり、自動化が進み、被害はより高額になっています。ゼロデイ脆弱性の悪用やクレデンシャルの盗難を防ぐことは現実的ではないので、攻撃者の侵入に備える必要があります。

攻撃に備えるには、最後の砦であるストレージ レイヤのワークロードデータを保護することが必要です。しかし、バックアップするだけでは不十分です。重要なワークロード データに対するリスクを認識し、すばやく脅威を検出して対応しなければなりませんし、脅迫を受けたときに迅速かつ容易に実施できるリカバリ プランも必要です。とはいえ、こうした対策を講じるための業務負担は重く、ミスを起こしやすい手作業が多すぎるうえ、対応できる人員も少なすぎます。

これらの要件を満たさなければ、ワークロードへの攻撃を検出できず、対応が遅れてしまいます。また、ワークロードのリカバリ作業は複雑であり、平均で7日もかかります[1]。しかもすべてのデータを復旧できるわけではありません。これでは満足のいく結果とは言えませんし、復旧が遅すぎます。

最終防衛ラインを包括的に保護
NetApp® BlueXP™は、NetAppが唯一のストレージ ベンダーとして提供するランサムウェア保護のための単一コントロール プレーンです。ワークロードを主体とする包括的なランサムウェア対策をインテリジェントに調整して実行します。数回クリックするだけで、リスクに瀕している重要なワークロード データを特定し、保護できます。潜在的な攻撃を正確に自動で検出して対応し、その影響を抑えることが可能です。また、ワークロードを数分以内にリカバリできるので、貴重なワークロード データを保護し、システム停止による損害を最小限に抑えることができます。

BlueXPランサムウェア対策ソリューションは、NetApp ONTAP®ソフトウェアの強力な機能とBlueXPデータ サービスを組み合わせて、ワークフローの自動化によるインテリジェントな推奨事項とガイダンスを追加し、以下を実現します。

- **特定**：NetAppストレージ内のワークロード（VM、ファイル共有、一般的なデータベース）とそのデータを自動的に特定し、データをワークロードにマッピングして、ワークロード データの機密性、重要性、リスクを判断します。
- **保護**：ワークロード保護ポリシーを推奨し、ワンクリックで適用します。
- **検出**：AIベースのファイル操作分析とユーザおよびエンティティの行動分析（UEBA）により、ファイルの異常と悪意のあるユーザ行動の両方をリアルタイムで検知し、ワークロード データに対する潜在的な攻撃を検出します。
- **対応**：Snapshotの自動作成や、潜在的な攻撃の疑いがある場合に手動または自動で行うユーザ ブロックにより、ワークロードを保護します。最も一般的なSIEMソリューションと統合できます。
- **復旧**：シンプルなオーケストレーションによるアプリケーション整合性のあるリカバリを通じて、ワークロードと関連データをすばやくリストアします。
- **管理**：ランサムウェア対策戦略とポリシーを導入し、結果を監視します。

ランサムウェアへの備えを支援することで、時間を節約し効果を高める

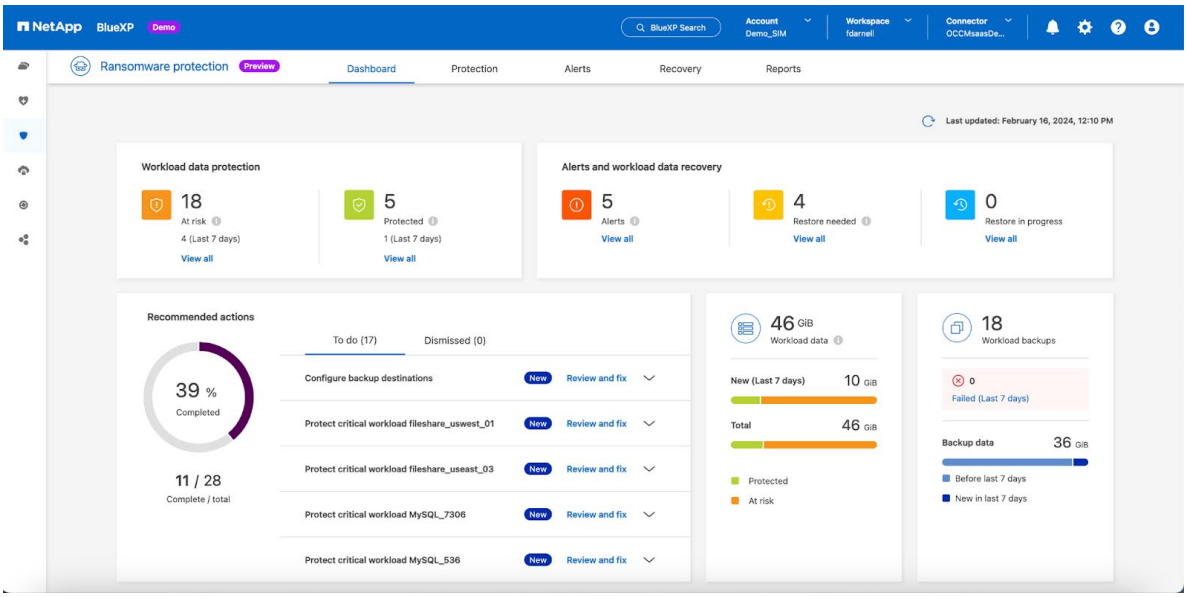
BlueXPランサムウェア対策ソリューションは、NetAppストレージにあるデータの種類を自動的に識別し、そのデータをワークロードにマッピングして、ワークロード データの機密性、重要性を判断し、ワークロードのリスクを分析します。こうした機能があるため、複雑な分析を手作業で行う必要がなく、専門的なスキルや複数のサードパーティ製ツールを備えなくても済みます。

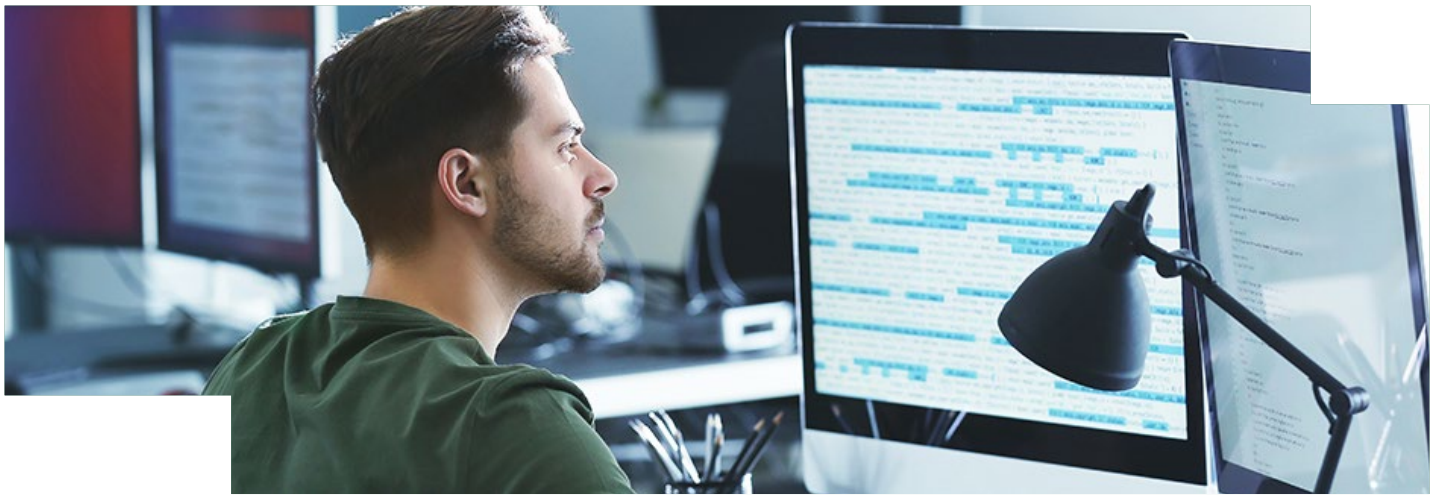
主なメリット

- 最終防衛ラインでの包括的な保護：バックアップに留まらず、米国標準技術研究所（NIST）サイバーセキュリティ フレームワークの6つの分野をすべてカバー
- ワークロード主体でアプリケーションと整合性のあるソリューション
- 優先順位が設定されたインテリジェントな推奨事項
- 自動化されたガイド付きアクション
- 脅威の早期検出
- ワークロード全体の高速リカバリ、（ボリュームまたはファイル単位での）きめ細かなリストアを選択可能

改ざん不能のSnapshotコピー、FPolicyによる悪意のあるファイル拡張子のブロック、自律型ランサムウェア対策の異常検知など、業界をリードするONTAP機能を用いた即座に運用できるインテリジェントな保護ポリシーを提案します。また、最適な投資効果を実現するため、BlueXPランサムウェア対策ソリューションはワークロードの機密性と重要性に合わせた保護を推奨します。

保護ポリシーは、ワンクリックするだけで、ワークロード データにシームレスかつ一貫して適用されます。BlueXPランサムウェア対策ソリューションは、バックグラウンドで動作してONTAPとBlueXPの機能を構成し、関連する各ボリュームにわたって保護ワークフローをオーケストレーションするため、手作業を何度も繰り返す必要がなくなります。





AIによるファイルやユーザ行動の異常検出機能を導入し、脅威をリアルタイムで発見して対応
BlueXPランサムウェア対策ソリューションは不審なファイルやユーザ行動の異常を常時監視し、攻撃による影響拡大を自動的に阻止します。攻撃が疑われる場合は、Snapshotコピーを作成し、ユーザのブロックを有効にして混乱を最小限に抑えます。

このサービスは、プライマリ ストレージでAIベースの高度なランサムウェア検出を行う点でも革新的であり、本番データに対する潜在的な攻撃を迅速に発見し、即座に影響を緩和できます。

さらに、攻撃のフォレンジックをサポートするデータを含むインシデントレポートを提供し、最も一般的なSIEMソリューションとの統合によって、脅威への対応を容易にし、スピード アップします。

ガイドに従ってアプリケーションと整合性のあるリストアを行い、より簡単な方法でワークロードを数分以内にリカバリ
BlueXPランサムウェア対策ソリューションは、ワークロード レベルまたはよりきめ細かく（ボリュームまたはファイル単位で）リストアする機能により、どのSnapshotコピーまたはバックアップが選択されたリカバリ基準に沿った最適な実際の復旧時点（RPA）を提供するかを決定します。ワークロードのオーケストレーションを通じて、すべての関連ワークロードデータをアプリケーションと整合性のある状態でリカバリし、リアルタイムのリカバリ ステータスを可視化することで、迅速なリストアを成功に導きます。

業務の中断が最小限に
BlueXPランサムウェア対策ソリューションは、ランサムウェアに関連するダウンタイムやデータ損失からワークロードを守るうえでの負担と不安を取り除きます。ランサムウェアへの備えを強化し、攻撃に対処し、リカバリに導く包括的なソリューションが実現します。万一攻撃が発生した場合はすぐに警告が表示され、貴重なワークロード データが保護され、より簡単かつ迅速にリカバリが行われるので、ビジネスの中断を最小限に抑えることができます。この安心感が得られるのはNetAppだけです。

▶ **今すぐBlueXPランサムウェア対策を導入しましょう。**

[1]ESG『2023 Ransomware Preparedness: Lighting the Way to Readiness and Mitigation』（2023年11月）

お問い合わせ

NetAppについて

NetAppはインテリジェントなデータインフラ企業として、ユニファイド データ ストレージ、統合データ サービス、CloudOpsソリューションを組み合わせることで、混沌とした世界を変革し、あらゆるお客様にビジネス チャンスをもたらしています。NetAppはデータ サイロのないインフラを構築し、オブザーバビリティとAIを活用して業界最高のデータ管理を実現します。業界大手各社のクラウドにネイティブに組み込まれた唯一のエンタープライズクラスのストレージ サービスとして、NetAppのデータ ストレージはシームレスな柔軟性を提供します。さらに、NetAppのデータ サービスは、優れたサイバー レジリエンス、ガバナンス、アプリケーションの即応性を通じてデータの優位性を生み出し、CloudOpsソリューションは、オブザーバビリティとAIを通じてパフォーマンスと効率を継続的に最適化します。データの種類、ワークロード、環境を問わず、NetAppがデータインフラを変革し、ビジネスの可能性を現実のものにします。詳細については、**www.netapp.com/ja/**をご覧ください。また、**X（旧Twitter）**、**LinkedIn**、**Facebook**、**Instagram**でNetAppをフォローしてください。