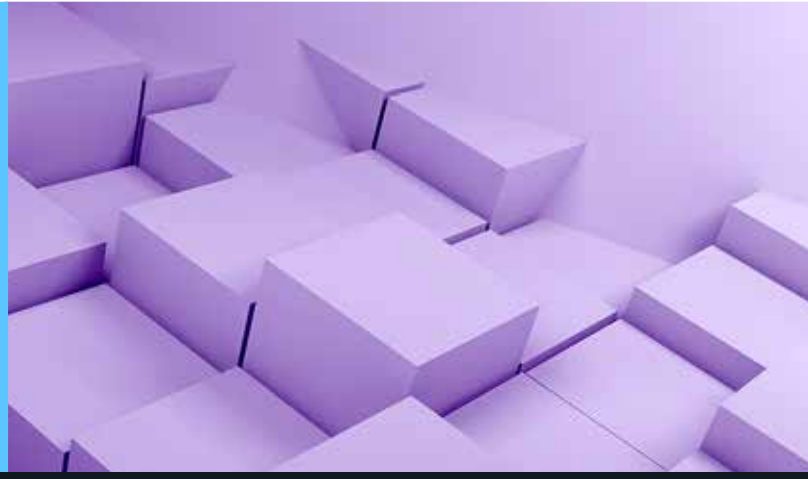
10の理由：

ネットアップはランサムウェア対策に最適



01 論理的なエア ギャップ

ファイルやオブジェクトを安全にロックするための論理的なエア ギャップを作成します。NetApp® SnapLock® ComplianceとNetApp StorageGRID® S3 Object Lockは、WORM（Write Once, Read Many）機能を標準装備しており、たとえ管理者アカウントが漏えいしても、保持期間中にデータが削除されることはありません。

02 迅速なリカバリ

ランサムウェア攻撃を受けた場合、最もコストがかかるのはダウンタイムです。書き換え不能なネットアップのSnapshotコピーを使用すれば、データを迅速にオンラインに戻すことができ、数時間ではなく数秒という速さでテラバイト規模のデータをリストアできることがおわかりいただけます。

03 自律型ランサムウェア対策

機械学習技術を活用して、サイバー脅威を迅速に発見し、修正します。NetApp ONTAP®ソフトウェアに組み込まれたこの技術は、ファイルシステムの異常を監視します。動きの遅いマルウェアの存在はファイルシステムの異常に現れる場合があるからです。また、組み込みのマルウェア対策用ファイル拡張子ブロック機能により、既知のマルウェアを検出し、拡散を未然に防ぎます。

04 ユーザ操作の異常検出

NetApp Cloud InsightsのCloud Secure機能により、リアルタイムに異常を検知し、ユーザ アカウントの漏えいや不正な行動の可能性を特定できます。ONTAPのNetApp FPolicyコンポーネントと組み合わせることで、データ リカバリ ポイントを自動で作成し、さらにアカウントへのアクセスをブロックして、データの盗難や大量削除を防ぐこともできます。

05 ゼロ トラストの互換性

多要素認証、ロールベースのアクセス、包括的なロギング、監査などのコントロールによるゼロ トラストのセキュリティ アプローチを採用し、副次的な攻撃からも保護します。

06 悪意のある管理者からの保護

ONTAPに標準搭載された複数管理者認証機能により、管理者アカウントの漏えいによる被害を防ぎます。この機能では、ボリュームやSnapshotコピーの削除などのクリティカルなストレージ操作を複数の管理者が承認する必要があります。

07 高度なコピー管理

バックアップとディザスタ リカバリの機能が強化されます。NetApp SnapMirror®とNetApp Cloud Backup Serviceを使用することで、Snapshotコピーを別のONTAPシステムや任意のオブジェクト ストレージ（オンプレミスまたはクラウド）に効率的にレプリケートできます。

08 リスクの軽減

NetApp Cloud Data Senseを使用して、データのセキュリティ体制を可視化し、機密データとその格納場所を特定することができます。フォルダのアクセス権を追跡し、データ漏えいなどの潜在的なリスクを軽減するためのオプションを提供します。

09 一元的な監視

シンプルなUIでハイブリッド クラウド インフラを監視します。NetApp Cloud Managerのランサムウェア対策ダッシュボードを利用して脅威を特定し、是正に取り掛かることができます。

10 フォレンジック分析

ネットアップの実績あるソリューションを利用して、ランサムウェア攻撃のイベント前後に対してフォレンジックを実行できます。攻撃を受けた経路を理解し、管理し、閉鎖するために必要なインサイトが提供されます。

NetApp

NA-838-0522