テクニカル レポート

NetAppのランサムウェア対策ソリューション

NetApp
Product Security Team
2023年2月| TR-4572

概要

このガイドでは、ランサムウェアとは何か、どのように進化したのか、NetApp® のランサムウェア対策ソリューションを使用してランサムウェアを特定し、早期に検出し、拡散を防止し、できるだけ迅速にリカバリする方法について説明します。このドキュメントで提供されるガイダンスとソリューションは、情報システムの機密性、整合性、可用性に関する所定のセキュリティ目標を達成しながら、サイバーレジリエントなソリューションを構築できるように設計されています。

目次

図一覧

ランサムウェアの概要

ランサムウェア攻撃は、組織が直面する可能性のある最大のサイバーセキュリティ脅威の1つであることは、誰もが知っています。潜在的な損害は、直接関連する回復コスト(Sophosによると、2019年から2020年の間に241%増加した)だけでなく、会社の評判とブランドへの影響でもあります。

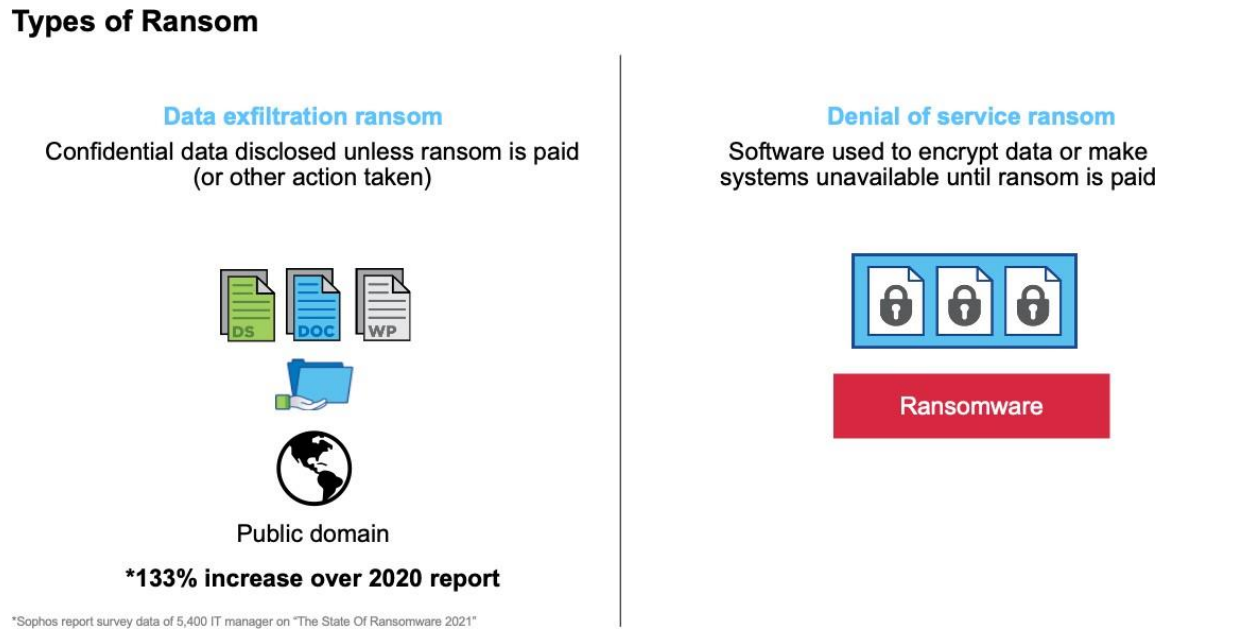
ランサムウェアとは

ランサムウェアを利用する攻撃者の目的は、できるだけ安くお金を稼ぐことです。長年にわたり、攻撃者が使用する戦略は進化してきました。これまで、攻撃者は一般的に分散型サービス拒否攻撃を使用していました。この攻撃では、顧客がアイテムを購入するために使用する企業のWebサイトにアクセスできなくなります。サービス拒否は身代金が支払われるまで続いた。この戦略は今日ではあまり使われていない。もう1つの方法は、データ漏えいと呼ばれます。この戦略により、攻撃者は企業のITシステムにアクセスし、機密データを社外の未知の場所に移動し、身代金が支払われない限り、そのデータを公開すると脅します。Sophosによると、この分野での攻撃は前年比133%増加し、データ漏えいが再び増加しています。

一般的によく知られているランサムウェアのバージョンは、サービス拒否ランサムウェアと呼ばれます。このランサムウェア戦略では、攻撃者が誤って暗号化プログラム（マルウェア）をダウンロードさせます。インストール後、マルウェアはすべてのローカルクライアントファイルと、企業ネットワーク上のNFS共有またはSMB共有上にあるすべてのファイルを暗号化します。ファイルが暗号化されると、元のファイルが削除され、ファイル内のデータにアクセスする方法がなくなります。ファイルはまだネットワーク上にあるため表示できますが、攻撃者によって暗号化されているためアクセスできません。

以前の方法とは対照的に、攻撃者は企業のWebサイトをオフラインにするためにボットの軍隊を呼び出す必要がなく、データを別の場所にコピーする必要がないため、サービス拒否のオーバーヘッドが非常に低くなります。攻撃者は、身代金を払って復号鍵を取得し、データに再びアクセスできるようにするよう要求します。身代金の大きさは、通常、攻撃者が攻撃からかなりの金額の塊を認識するのに十分な大きさですが、組織が支払うことは現実的ではありません。

図1）現在組織に対して使用されている2つの主なタイプのランサムウェア

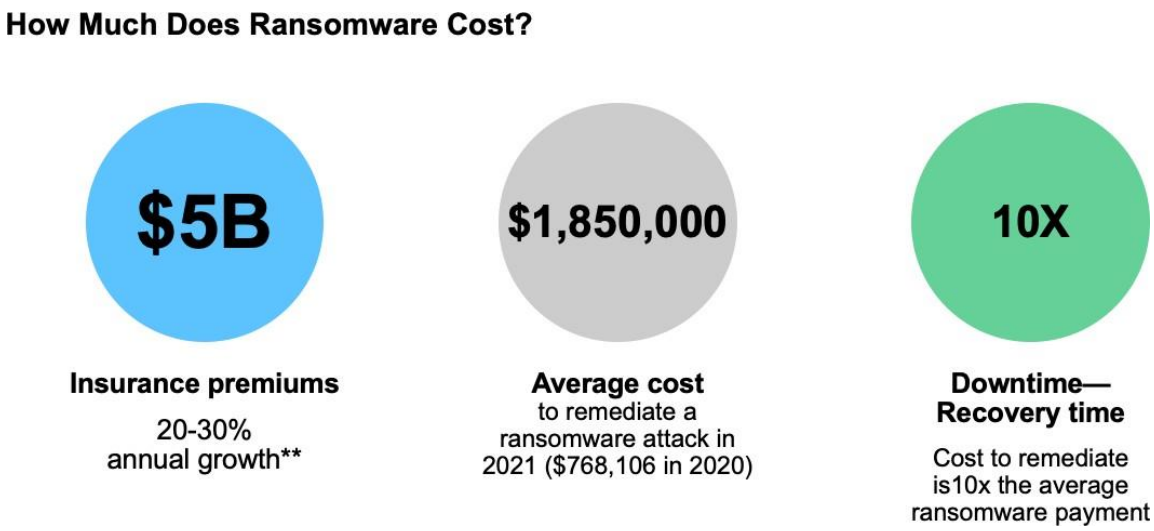


ランサムウェアの真のコスト

身代金の支払い自体がビジネスへの最大の金銭的影響であると考えるかもしれません。しかし、支払いはそれほど重要ではありませんが（平均コストはインシデント1件あたり154,108ドルと考えられています）、ランサムウェアインシデントで発生した実際のコストであるダウンタイムと比較すると、わずかです。

組織がビジネスにとって重要なデータにアクセスできない場合、生産性に深刻な影響を与えます。Cowareの2020年1月の分析によると、ランサムウェアによるダウンタイムの平均は16日以上であり、ダウンタイムコストは通常、実際の身代金の10倍です。米国の平均回復コストは180万ドルでしたダウンタイムによる影響とその結果生じるコストは、ビジネスの種類によって組織ごとに異なります。ITの可用性に大きく依存している組織（Eコマース、株式取引、医療など）は、10倍のコスト要因を検討しています。つまり、実際にダウンタイムが発生した場合、それ以上ではないにしても、1、154、108ドルもの損害が発生する可能性があります。この金額はインシデント1件あたりの金額であることに注意してください。サイバー保険のコストも、被保険企業がランサムウェア攻撃を受ける可能性が非常に高いことから、上昇を続けています。

図2）ランサムウェアの主な被害は、リカバリ中に組織が直面するダウンタイムです。



ランサムウェアの歴史と実際のコストについては、『Fighting Ransomware：Part One−The History and Cost』を参照してください追加情報。

ランサムウェア向けNetAppソリューション

階層型の防御アプローチ

ランサムウェアの検出は、拡散を防ぎ、コストのかかるダウンタイムを回避できるように、できるだけ早く実行することが重要です。しかし、効果的なランサムウェア検出戦略には、複数の保護レイヤを含める必要があります。良い類推とは、衝突時の保護のための車両の安全機能です。シートベルトなどの単一の機能に頼って事故時にあなたを保護することは望ましくありません。エアバッグ、アンチロックブレーキ、さらには前方衝突警告は、はるかに良い結果をもたらすことができる追加の安全機能です。ランサムウェア対策についても同じことが言えます。

たとえば、NetApp® FPolicyとNetApp Cloud Insights®、または当社のパートナーが提供する同様の機能を組み合わせることで、ユーザ行動分析（UBA）を通じてランサムウェアを検出することができます。ランサムウェア攻撃の可能性を、個々のユーザの行動の側面から探します。1つのユーザアカウントをハイジャックすることは、ハッカーがランサムウェア攻撃を開始する際に取る可能性のある1つの手段にすぎません。悪意のある攻撃者は、攻撃手法を絶えず進化させています。

NetApp Active IQ® とNetApp Active IQ Unified Manager® は、ランサムウェアの検出にも追加されています。Active IQは、NetApp ONTAP® システムがNetApp設定のベストプラクティス（NetApp FPolicy®の有効化など）に準拠しているかどうかをチェックします。Active IQ Unified Managerは、NetApp Snapshot™コピーの異常な増加やストレージ効率の低下を示すアラートを生成します。これは、ランサムウェア攻撃の可能性を示している可能性があります。

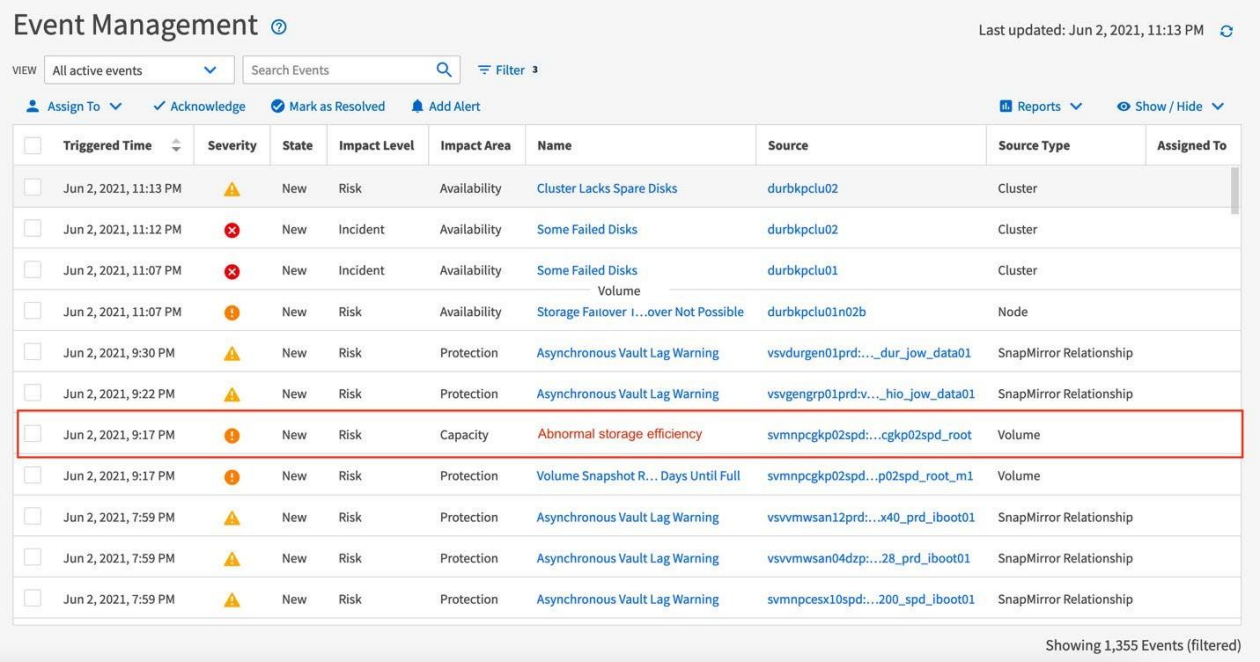
ここで、ONTAP 9.10.1以降のAutonomous Ransomware Protection（ARP）機能が有効になります。ボリュームワークロードのアクティビティとデータエントロピーを確認する組み込みの機械学習（ML）を活用して、ランサムウェアを自動的に検出します。UBAとは異なるアクティビティを監視するため、UBAでは検出できない攻撃を検出できます。たとえば、1つのアカウントだけを使用するのではなく、複数の侵害されたユーザーアカウントの資格情報を使用することで、暗号化が非常に遅くなります。ARPは単一のユーザの行動に焦点を当てていないため、これらのタイプの攻撃を検出することができます。

階層型防御アプローチに関する追加情報については、ブログ「Prevent ransomware spread with ONTAP automatic ransomware protection」をご覧ください。

NetAppネイティブ検出ツール

NetAppには、ランサムウェアの早期検出に役立つネイティブツールまたは組み込みのツールが用意されています。特にONTAPの場合、これらのツールには、異常なSnapshotコピーやボリュームの増加率、ストレージ効率の低下に対するActive IQ Unified Managerアラートが含まれます。

図3）Active IQ Unified Managerから提供される異常なStorage Efficiencyアラート



また、ONTAP System Managerを使用して、Snapshotの変更率やStorage Efficiencyによる削減効果をリアルタイムで確認することもできます。

ONTAPネイティブの検出ツールの詳細については、ブログ「Fighting Ransomware: Part Two-ONTAP Native（別名無料）Tools for Detecting Ransomware」を参照してください。

ネイティブFPolicy

NetApp FPolicyは、NFSまたはSMB / CIFSプロトコル経由のファイルアクセスを監視および管理するためのファイルアクセス通知フレームワークです。10年以上にわたってONTAPの一部であり、ランサムウェアの検出に非常に役立ちます。このゼロトラストエンジンは、Access Control List（ACL;アクセスコントロールリスト）の権限を超える追加のセキュリティ対策を取得できるため、非常に有用です。

ゼロトラストの背後にある概念は、決して信頼せず、常に検証することです。詳細については、NetAppの最新のブログ記事をご覧ください。ただし、重要な点は、ユーザー（または管理者）がファイルまたはフォルダにアクセスする権限を持っているからといって、その場所で必要なコンテンツを変更できるとは限らないということです。

FPolicyの当初の目的は、不要なファイルがエンタープライズクラスのストレージ アプライアンスに保存されるのを防止することでした（たとえば、Spotifyのような音楽ストリーミングサービスが普及する前に、多くのユーザーが.mp3ファイルをホームフォルダに保存しており、ユーザーが個人のデバイスから音楽をストリーミングできるようにしていました）。ただし、FPolicyを使用すると、既知のランサムウェアファイル拡張子をブロックすることもできます。ユーザには引き続きホームフォルダへのフルアクセス権限がありますが、FPolicyでは、.mp3ファイルであるか既知のランサムウェアファイル拡張子であるかに関係なく、管理者がブロックとしてマークしたファイルを保存することはできません。

ネイティブFPolicyの詳細については、ブログ「ランサムウェアとの戦い:パート3−ONTAP FPolicy、もう1つの強力なネイティブ（フリー）ツール」をご覧ください。

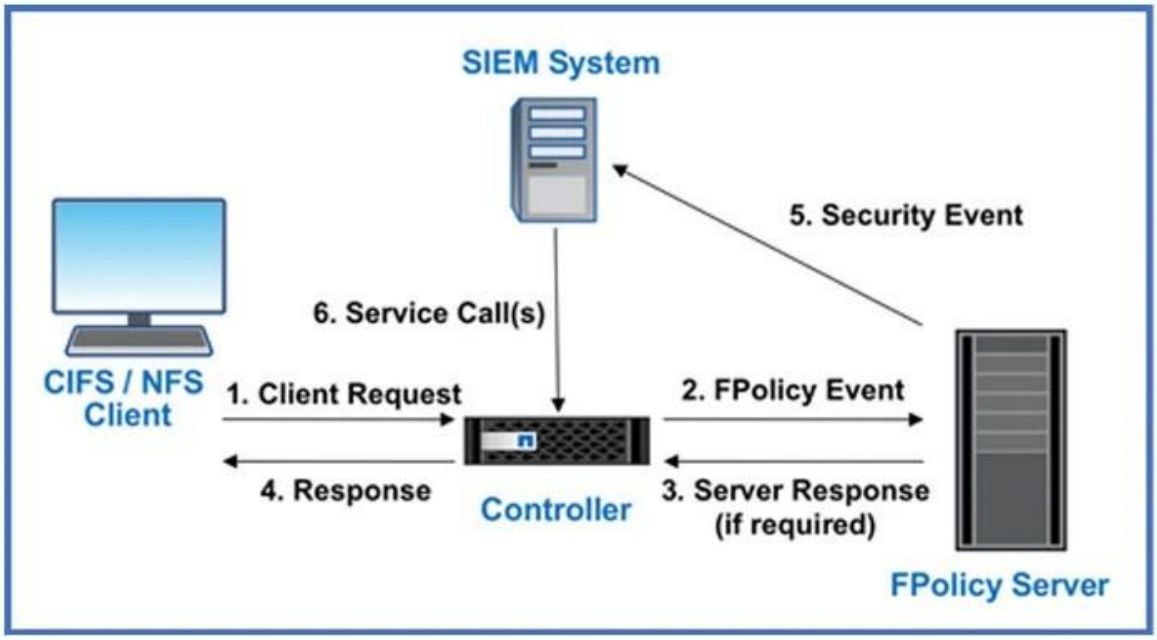
外部のFPolicy

ONTAPのFPolicy外部モードでは、ゼロデイランサムウェア攻撃を阻止するための鍵としてUBA（User and Entity Behavior Analytics、UEBAとも呼ばれる）が使用されます。その方法を理解するには、UBAをしっかりと理解する必要があります。

人間は習慣の生き物である。NetAppの習慣は、データへのアクセス方法やデータの取り扱い方法など、さまざまなことに適用されます。ユーザとグループは、多くの場合、ジョブを実行するために特定のデータセットにアクセスします。UBAはこれらの動作を追跡し、ユーザの一般的なアクセスパターンを特定し、そのユーザの動作がパターンと異なる場合にレポートすることができます。さらに、ユーザーが通常のパターンの外で何かをしている場合、UBAはファイルデータへのアクセスを拒否することもできます。FPolicy外部モードは、UBAを使用する外部サーバと統合されており、ユーザが通常は行わない処理をいつ実行しているかを判断します。

次のセキュリティ情報イベント管理（SIEM）システムの例では、すべてのCIFSまたはNFSクライアント要求がFPolicyサーバに送信され、アクセスが許可されているかどうかが判断されます。

図4）外部モードのFPolicyは、FPolicy固有のAPIを使用して外部サーバと統合される



この追加レベルの分析は、ユーザが操作しようとしているファイルデータに対するファイル権限を持っている場合でも実行されます。権限を常に正しく取得するのは難しいため、FPolicyを使用したUBAを使用すると、ユーザが悪意のあることを実行しようとしているかどうかを判断する際の基準としてはるかに適しています。UBAの詳細については、NetAppテクニカルレポートTR-4829：『NetApp and Zero Trust』を参照してください。

UBAは非常に強力ですが、ゼロデイランサムウェア攻撃との戦いでは終わりではありません。多くのNetAppパートナーやベンダーが、人工知能（AI）とMLを外部FPolicyサーバに組み込み始めています。各ベンダーはONTAPに組み込まれたFPolicy機能に組み込まれているため、AI / MLの強化された機能をすぐに活用できます。

ユーザ行動分析とFPolicy外部モードの詳細については、ブログ「Fighting Ransomware：Part Four−UBA and ONTAP with FPolicy External Mode」を参照してください。

Cloud Insights

前述したように、UBAには外部モードのFPolicyサーバが必要です。NetAppにはこのサービスを提供するパートナーがありますが、Cloud Insights with Cloud Secureという独自の外部モードFPolicyサーバもあります。

Cloud Insightsは、オンプレミス、プライベートクラウド、AWS、Azure、Google Cloudなどのパブリッククラウド環境で動作する、SaaSインフラおよびサービス監視解決策です。Cloud SecureはNetApp Cloud Insightsの機能の1つです。データ アクセスのパターンを分析し、ランサムウェア攻撃のリスクを特定します。

図5）Cloud Secureは3つの主要な方法でランサムウェアからの保護を支援

Cloud Insights with Cloud Secureがランサムウェア攻撃の可能性を検出すると、次のようなアクションを自動的に実行できます（ただし、これらに限定されません）。

- 自動Snapshotコピーの作成
- ファイル暗号化の疑いがあるユーザアカウントのブロック

ONTAPのAutonomous Ransomware ProtectionによるアラートもCloud Secureに表示されるため、ARPとCloud Secureの両方を使用してランサムウェア攻撃から保護する単一のインターフェイスが提供されます。

Cloud Insights with Cloud Secureの詳細については、cloud.netapp.comを参照してください。

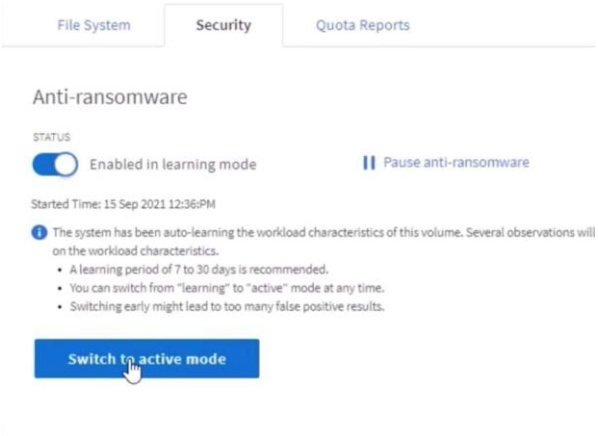
自律型ランサムウェア対策

ONTAP 9.10.1以降では、Autonomous Ransomware Protection（ARP）と呼ばれるランサムウェア対策機能に、まったく新しい形式のランサムウェア検出と防御が導入されています。ARPは、ボリュームワークロードのアクティビティとデータエントロピーを確認する組み込みのMLを活用して、ランサムウェアを自動的に検出します。また、UBAとは異なるアクティビティを監視して、UBAでは検出できない攻撃を検出できます。

ONTAP Autonomous Ransomware Protectionは、マルチテナント暗号化キー管理（MT_EK_MGMT）ライセンスがインストールされている場合に9.10.1で有効になります。9.11.1以降では、ランサムウェア対策ライセンスを使用して有効になります。ARPは、ONTAPの組み込みの管理インターフェイスであるSystem Managerを使用して設定でき、ボリューム単位で有効にできます。

ARP機能はラーニングモードで開始されます。NetAppでは、MLがNASボリューム上の一般的なワークロードを理解できるように、少なくとも30日間を推奨しています。ARPをアクティブモードにすると、ランサムウェアの可能性がある異常なボリュームアクティビティの検出が開始されます。

図6）自律型ランサムウェア対策を学習モードで有効にし、推奨される30日間有効にしてからアクティブモードに設定



異常なアクティビティが検出された場合は、ただちに自動Snapshotコピーが作成され、ファイルの感染にできるだけ近いリストアポイントが確保されます。同時に自動アラートが生成され、管理者は異常なファイルアクティビティを確認して、アクティビティが実際に悪意のあるものかどうかを判断し、適切なアクションを実行できます。または、アクティビティが想定されるワークロードの場合、そのアクティビティを誤検知として簡単にマークできます。ARP MLはワークロードの変化を記録し、攻撃の可能性を示すフラグを立てなくなります。また、この機能によってI/Oが中断されることはありません。代わりに、管理者にネイティブの分析機能、分析情報、データリカバリ機能を提供し、これまでにないランサムウェア検出機能を搭載します。ARP機能を使用すると、ONTAPでNASワークロードのランサムウェアの自動検出をこれまで以上に簡単に実行できます。

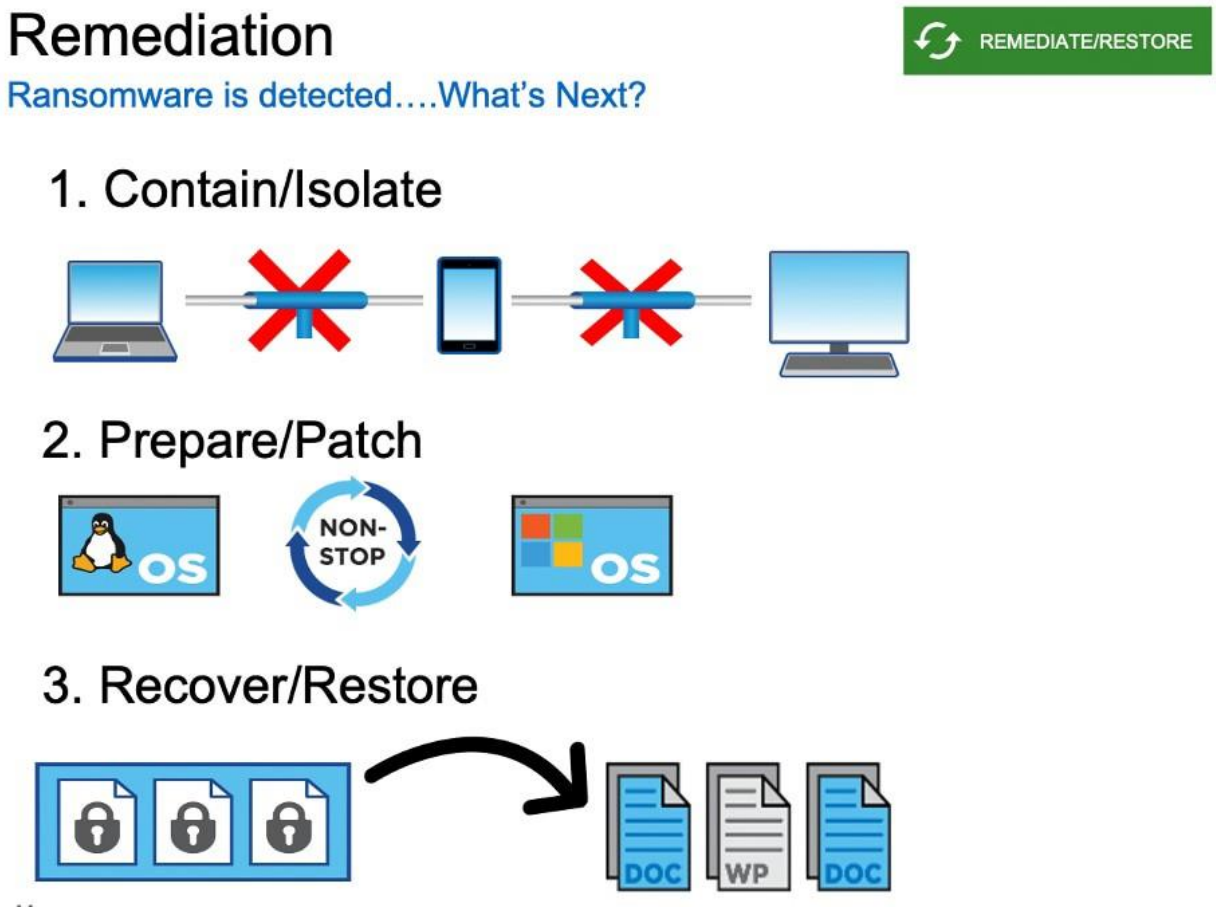
ARP機能の詳細については、Autonomous Ransomware Protection ONTAP 9のドキュメントを参照してください。

ランサムウェア攻撃からのリカバリに関する推奨事項

ランサムウェア攻撃を受けても、最初はデータをすぐにリカバリできると直感的に考えるかもしれません。これは可能ですが、他の手段を講じてランサムウェアが戻ってこないようにしなければ、再感染する可能性が高く、その努力は貴重な時間を無駄にしてしまいます。

ランサムウェアの感染から環境を適切かつ包括的に修復するには、主に3つのステップがあります。これらの手順は次の図に示されており、記載されている順序で実行することを推奨します（必須ではありません）。

図7）攻撃からリカバリするための推奨手順



このアプローチは、データを復元するときに再感染から安全になるようにするための最も効果的な方法です。

ランサムウェアからのリカバリのベストプラクティスの詳細については、ブログ「Fighting Ransomware：Part 5–Smart Recovery to Avoid Reinfection」をご覧ください。

ONTAPリカバリ機能

ランサムウェア攻撃からリカバリする最も簡単な方法は、バックアップからリストアすることであることは誰もが知っています。それは十分に簡単に聞こえますが、実際の復元プロセスは複雑であり、遅くなることは言うまでもありません。

- バックアップデータも暗号化されていますか。
- 必要なバックアップはまだ残っていますか？
- 暗号化されたデータをリストアするのにどれくらいの時間がかかりますか。
- データのリストアは本番環境のワークロードに影響しますか？

リストア中の長時間のダウンタイム（ランサムウェアの真のコスト）を回避するには、これらすべての質問を回答に送信することが重要です。

ONTAPのSnapshotテクノロジは、これらすべての質問に答え、高速リストア（数テラバイト、数秒）を実現し、ランサムウェアによる暗号化からバックアップを保護し、貴重なバックアップデータの削除を防止するための鍵です。ディザスタリカバリ、データアーカイブ、データ階層化など、エコシステム全体でSnapshotコピーの機能を活用できます。

Snapshotコピーを削除から保護し、完全なバックアップの書き換えを防止する方法など、ONTAPリカバリ機能の詳細については、ブログ「ランサムウェアとの戦い：パート6：ONTAP Snapshotコピーでデータを高速にリカバリする」を参照してください。

SnapLockコンプライアンス（論理的なエアギャップ）

攻撃者がバックアップコピーを破棄し、場合によっては暗号化する傾向が高まっています。そのため、サイバーセキュリティ業界の多くが、全体的なサイバーレジリエンス戦略の一環としてエアギャップバックアップを使用することを推奨しています。

問題は、従来のエアギャップ（テープとオフラインメディア）によってリストア時間が大幅に増加し、ダウンタイムと全体的な関連コストが増加することです。エアギャップ解決策へのより現代的なアプローチでさえ、問題が発生する可能性があります。たとえば、新しいバックアップコピーを受信するためにバックアップヴォールトを一時的に開いてから、プライマリデータへのネットワーク接続を切断して閉じ、再び「エアギャップ」状態にすると、攻撃者はこの一時的なオープンを利用する可能性があります。接続がオンラインになっているときに、攻撃者が攻撃してデータを侵害または破壊した場合はどうなりますか。このタイプの設定は、一般に不要な複雑さを追加します。論理的なエアギャップは、バックアップをオンラインに維持しながらセキュリティ保護の原則が同じであるため、従来のエアギャップや最新のエアギャップの代替として最適です。NetAppを使用すると、テープやディスクのエアギャップの複雑さを論理的なエアギャップで解消できます。これは、書き換え不可能なSnapshotコピーとNetApp SnapLock® Complianceによって実現できます。

NetAppは、医療保険の携行性と責任に関する法律（HIPAA）、サーベンスオクスリー法、その他の規制データ規則など、データコンプライアンスの要件に対応するために、10年以上前にSnapLock機能をリリースしました。また、プライマリSnapshotコピーをSnapLockにバックアップしてWORM状態にコミットし、削除を回避することもできます。SnapLockライセンスには、SnapLock ComplianceとSnapLock Enterpriseの2つのバージョンがあります。NetAppでは、ランサムウェア対策として、SnapLockコンプライアンスを推奨しています。これは、ONTAP管理者またはNetAppサポートが、Snapshotコピーをロックして削除できない特定の保持期間を設定できるためです。

SnapLockとその論理的エアギャップ機能の詳細については、ブログ記事「Increase ransomware protection with SnapLock logical AIR gaps and technical report、TR-4526：NetApp SnapLockを使用したWORMストレージ。

Snapshotコピーの改ざん防止

SnapLockコンプライアンスを論理的なエアギャップとして活用することで、攻撃者によるバックアップコピーの削除を防止するための究極の保護が提供されますが、SnapVault経由でSnapLock対応のセカンダリボリュームにSnapshotコピーを移動する必要があります。そのため、多くのお客様がネットワーク経由でセカンダリストレージにこの構成を導入しています。その結果、プライマリボリュームのSnapshotコピーをプライマリストレージにリストアするよりもリストア時間が長くなる可能性があります。改ざんを防止するSnapshotコピーを入力します。

ONTAP 9.12.1以降では、改ざん防止機能を備えたSnapshotコピーを使用して、プライマリストレージとプライマリボリュームにあるSnapshotコピーをSnapLockコンプライアンスレベルに近いレベルで保護できます。SnapVaultを使用してSnapLockedのセカンダリボリュームにSnapshotコピーをバックアップする必要はありません。改ざん防止Snapshotコピーには、SnapLockテクノロジを使用して、ONTAPのフル管理者が同じSnapLock保持期間を使用していてもプライマリSnapshotコピーが削除されないようにします。これにより、リストア時間が短縮され、改ざん防止されたSnapshotコピーを使用してFlexCloneボリュームをバックアップできます。これは、従来のSnapLockコンプライアンスで保存されたSnapshotコピーではできません。

SnapLock SnapLock Complianceと改ざん防止機能を備えたSnapshotコピーの大きな違いは、保存されたSnapshotコピーが有効期限に達していない場合、SnapLock ComplianceではONTAPアレイの初期化と消去を実行できない点です。Snapshotコピーの改ざんを防止するには、SnapLock Complianceライセンスが必要です。

改ざん防止機能を備えたSnapshotコピーと、そのプライマリストレージのSnapshotコピー保護機能の詳細については、ドキュメント「Snapshotコピーをロックしてランサムウェア攻撃から保護」を参照してください。

マルチ管理者認証

SnapLock Complianceまたは改ざん防止機能を備えたSnapshotコピーを使用してSnapshotコピーバックアップを不正削除から保護すると、バックアップを高度に保護できますが、追加のONTAPライセンスが必要です。ライセンスをお持ちでないお客様向けには、バックアップSnapshotコピーの不正削除を保護するための標準の組み込みONTAP 解決策 も用意されています。この解決策は、ONTAP 9.11.1以降で使用できるマルチ管理者検証（MAV）と呼ばれます。

MAVには、ボリュームの削除、管理ユーザの追加作成、Snapshotコピーの削除などの特定の処理を、指定した管理者の承認後にのみ実行できるようにするための堅牢な機能セットが用意されています。これにより、侵害を受けた管理者、悪意のある管理者、または経験の浅い管理者が望ましくない変更やデータの削除を行えないようにすることができます。

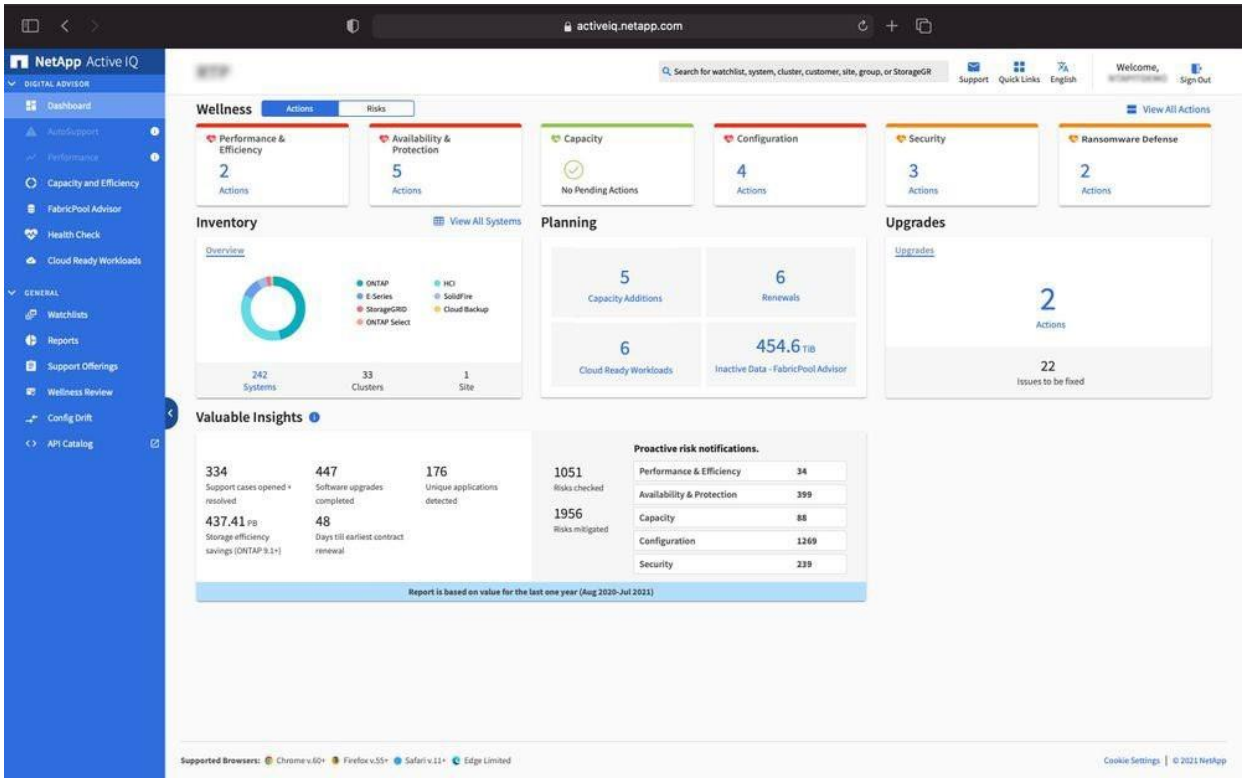
Snapshotコピーを削除する前に、指定した管理者の承認者を必要な数だけ設定できます。MAVは、バックアップSnapshotコピーの不要な早期削除を防止する優れた組み込みの方法を提供します。

MAVとその保護機能の設定方法の詳細については、Multi-admin verification overviewを参照してください。

Active IQ–ランサムウェア対策のベストプラクティス

ランサムウェアからの保護と、NetAppシステムがランサムウェアと戦うためのベストプラクティスに準拠していることの確認に関しては、NetApp Active IQもその役割を果たします。Active IQは、セキュリティの脆弱性の排除に役立つだけでなく、ランサムウェアからの保護に固有の分析情報とガイダンスも提供します。専用の健全性カードに必要な対処方法と対処されたリスクが表示されるため、システムがこれらのベストプラクティスの推奨事項を満たしていることを確認できます。

図8）NetApp Active IQダッシュボードの健全性モニタ



[Ransomware Defense Wellness]ページで追跡されるリスクとアクションには、次のものが含まれます（その他多数）。

- ボリュームのSnapshotコピー数が少ないため、ランサムウェアからの保護の可能性が低下しています。
- NASプロトコル用に設定されたすべてのStorage Virtual Machine（SVM）でFPolicyが有効になっているわけではありません。

Active IQのランサムウェア防御の実際の動作については、NetApp Active IQを参照してください。

まとめ

ランサムウェアは、他の多くのマルウェアの脅威と同様に進化し続けています。防御の方法が改善されるのと同じように、攻撃の方法とベクトルも改善されます。単一の解決策ですべての攻撃を阻止することはできませんが、パートナーシップやサードパーティなどのソリューションポートフォリオを使用することで、多層的な防御を実現できます。

NetApp 解決策 には、可視化、検出、修復のためのさまざまな効果的なツールが用意されており、ランサムウェアの早期発見、拡散の防止、必要に応じた迅速なリカバリを支援して、コストのかかるダウンタイムを回避できます。可視化と検出のためのサードパーティやパートナーソリューションと同様に、従来の階層型防御ソリューションは依然として普及しています。効果的な修復は、あらゆる脅威への対応において依然として重要な部分を占めています。書き換え不能なNetApp Snapshotテクノロジと SnapLockの論理的なエアギャップ解決策を活用する業界独自のアプローチは、業界における差別化要因であり、ランサムウェア修復機能に関する業界のベストプラクティスです。

詳細情報の入手方法

このドキュメントに記載されている情報の詳細については、以下のドキュメントやWebサイトを参照してください。

- NetApp ONTAPドキュメントセンター
  http://docs.netapp.com/ontap-9/index.jsp
- NetAppランサムウェアブログシリーズ
  https://www.netapp.com/blog/prevent-ransomware/
- NetApp Support Siteのリソースページ
  http://mysupport.netapp.com/ontap/resources
- NetApp製品のセキュリティ
  https://security.netapp.com/resources/
- NetApp Snapshotテクノロジ
  www.netapp.com/us/media/ds-2477.pdf
- その他すべてのNetApp製品ドキュメント
  https://docs.netapp.com

本ドキュメントに記載されている製品や機能のバージョンがお客様の環境でサポートされるかどうかについては、NetApp サポート サイトで Interoperability Matrix Tool (IMT)を参照してください。NetApp IMT には、NetApp がサポートする構成を構築するために使用できる製品コンポーネントやバージョンが定義されています。サポートの可否は、お客様の実際のインストール環境が公表されている仕様に従っているかどうかによって異なります。

機械翻訳に関する免責事項

原文は英語で作成されました。英語と日本語訳の間に不一致がある場合には、英語の内容が優先されます。公式な情報については、本資料の英語版を参照してください。翻訳によって生じた矛盾や不一致は、法令の順守や施行に対していかなる拘束力も法的な効力も持ちません。

著作権に関する情報

商標に関する情報

TR-4572-0223-JP

NetApp