NetAppランサムウェア対策について

ONTAP 9

NetApp
August 31, 2024

目次

NetAppランサムウェア対策について

ランサムウェアとNetAppの保護ポートフォリオ

ランサムウェアは、2024年に組織のビジネス中断を引き起こす最も重大な脅威の1つです。の "Sophosランサムウェアの現状2024"調査によると、ランサムウェア攻撃は調査対象者の72%に影響を及ぼしています。ランサムウェア攻撃はより高度で標的型に進化しており、脅威アクターは人工知能などの高度な手法を採用して影響と利益を最大化しています。

組織は、境界、ネットワーク、ID、アプリケーション、データの保存場所など、セキュリティ体制全体をストレージレベルで把握し、これらのレイヤを保護する必要があります。今日の脅威の状況では、ストレージレイヤでサイバー保護にデータ主体のアプローチを採用することが不可欠です。単一のソリューション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。

にはNetApp製品ポートフォリオ、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の論理的エアギャップソリューションを活用する業界独自のアプローチは、ランサムウェア対策機能における業界の差別化要因であり、業界のベストプラクティスでもあります。

> 2024年7月以降、以前はPDFとして公開されていたテクニカルレポート_TR-4572：『NetApp Ransomware Protection_』の内容が、ONTAPの他の製品ドキュメントに統合されました。

データが主なターゲット

サイバー犯罪者は、データの価値を認識し、データを直接ターゲットにすることが増えています。境界、ネットワーク、およびアプリケーションのセキュリティは重要ですが、バイパスすることができます。ソースであるストレージレイヤでのデータ保護に重点を置き、重要な最終防衛線を提供します。ランサムウェア攻撃の目的は、本番環境のデータにアクセスして暗号化したりアクセス不能にしたりすることです。そのためには、攻撃者は境界からアプリケーションのセキュリティまで、今日組織によって導入されている既存の防御をすでに貫通している必要があります。

[境界からデータセキュリティまでのセキュリティレイヤ]

残念ながら、多くの組織はデータレイヤのセキュリティ機能を利用していません。そこで登場するのが、NetAppランサムウェア対策ポートフォリオであり、最前線でお客様を保護します。

ランサムウェアの真のコスト

身代金の支払い自体は、ビジネスへの最大の金銭的影響ではありません。支払い額はわずかではありませんが、ランサムウェアインシデントの被害によるダウンタイムコストと比べると、わずかです。

身代金の支払いは、ランサムウェア攻撃に対処する際のリカバリコストの要素の1つにすぎません。支払われた身代金を除くと、2024年の組織の報告によると、ランサムウェア攻撃からの復旧に要する平均コストは2730万ドルであり、2023年に報告された1820万ドルから100万ドル近く増加して "2024 Sophosランサムウ

ェアの現状"います。Eコマース、株式取引、医療など、ITの可用性に大きく依存している組織の場合、コストは10倍以上になる可能性があります。

また、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、サイバー保険のコストも上昇し続けています。

データレイヤでのランサムウェア対策

NetAppは、境界からストレージレイヤでのデータの配置場所まで、組織全体にわたってセキュリティ体制が広く深く浸透していることを認識しています。セキュリティスタックは複雑であり、テクノロジスタックのあらゆるレベルでセキュリティを提供する必要があります。

データレイヤでのリアルタイムの保護は、さらに重要であり、独自の要件があります。効果的に機能するには、この層のソリューションが次の重要な属性を提供する必要があります。

- *設計によるセキュリティ*により、攻撃が成功する可能性を最小限に抑える
- *リアルタイムの検出と対応*により、攻撃が成功した場合の影響を最小限に抑えます。
- *エアギャップによるWORM保護*重要なデータのバックアップを分離
- *単一のコントロールプレーン*による包括的なランサムウェア防御

NetAppはこれらすべてを実現し、さらに多くの機能を提供します。

[NetAppランサムウェア対策ポートフォリオ（説明されている重要な属性を含む）]

NetAppのランサムウェア対策ポートフォリオ

NetAppは、"組み込みのランサムウェア対策"重要なデータに対してリアルタイムで堅牢かつ多面的な防御を提供します。その中核である、AIを活用した高度な検出アルゴリズムは、データパターンを継続的に監視し、99%の精度で潜在的なランサムウェアの脅威を迅速に特定します。攻撃に迅速に対応することで、ネットアップのストレージはデータのスナップショットを迅速に作成し、コピーを保護して迅速なリカバリを実現します。

データをさらに強化するために、NetAppの"サイバーヴォールティング"機能は論理的なエアギャップでデータを分離します。重要なデータを保護することで、迅速なビジネス継続性を確保します。

NetAppは"BlueXPのランサムウェア対策"、単一のコントロールプレーンで運用上の負担を軽減し、ワークロード中心のエンドツーエンドのランサムウェア防御をインテリジェントに調整して実行します。そのため、リスクにさらされている重要なワークロードデータをワンクリックで特定して保護し、潜在的な攻撃の影響を正確かつ自動的に検出して対応し、数日ではなく数分でワークロードをリカバリし、貴重なワークロードデータを保護し、コストの中断を最小限に抑えます。

データへの不正アクセスを保護するための標準の組み込みONTAPソリューションとして、"マルチ管理者認証（MAV）"堅牢な一連の機能を備えています。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処理は、少なくとも2人目の指定管理者から承認を得た場合にのみ実行できます。これにより、侵害された管理者や悪意のある管理者、経験の浅い管理者が望ましくない変更やデータ削除を行うのを防ぐことができます。Snapshotコピーを削除する前に、指定された管理者承認者を必要な数だけ設定できます。

NetApp ONTAPは、Webベースの "多要素認証（MFA）"System ManagerおよびSSH CLI認証の要件に対応しています。

NetAppのランサムウェア対策は、進化し続ける脅威の状況にも安心して対応します。その包括的なアプローチは、現在のランサムウェア攻撃から防御するだけでなく、新たな脅威にも適応し、データインフラに長期的なセキュリティを提供します。

その他の保護オプションについて

- "Active IQランサムウェア対策"
- "Cloud Insightsストレージワークロードセキュリティ（CISWS）"
- "FPolicy の"
- "SnapLockと改ざん防止機能を備えたSnapshotコピー"

ランサムウェアからのリカバリ保証

NetAppは、ランサムウェア攻撃が発生した場合にSnapshotデータをリストアすることを保証します。当社の保証：スナップショットデータのリストアをサポートできない場合は、適切に対応します。この保証は、AFF Aシリーズ、AFF Cシリーズ、ASA、FASシステムの新規購入時に利用できます。

詳細はこちら。

- "リカバリ保証サービスの説明"
- "ランサムウェア対策保証ブログ"です。

関連情報

- NetAppサポートサイトのリソースページ http://mysupport.netapp.com/ontap/resources
- NetApp製品のセキュリティ https://security.netapp.com/resources/

SnapLockと改ざん防止Snapshotコピーによるランサムウェア対策

NetAppのスナップ兵器の重要な武器は、ランサムウェアの脅威からの保護に非常に効果的であることが証明されているSnapLockです。不正なデータ削除を防止することで、SnapLockは追加のセキュリティレイヤを提供し、悪意のある攻撃が発生した場合でも重要なデータに影響を与えずにアクセスできるようにします。

SnapLock コンプライアンス

SnapLock Compliance（SLC）は、データを消去できない方法で保護します。SLCでは、管理者がアレイを再初期化しようとした場合でも、データの削除が禁止されています。他の競合製品とは異なり、SnapLock Complianceはそれらの製品のサポートチームを通じてソーシャルエンジニアリングのハッキングに対して脆弱ではありません。SnapLock Complianceボリュームで保護されているデータは、そのデータが有効期限に達するまでリカバリできます。

SnapLockを有効にするには"ONTAP One"、ライセンスが必要です。

詳細はこちら。

- "SnapLockのドキュメント"

改ざん防止**Snapshot**コピー

改ざん防止Snapshot（TPS）コピーを使用すると、悪意のある行為からデータを簡単かつ迅速に保護できます。SnapLock Complianceとは異なり、TPSは通常、ユーザが決められた時間データを保護し、高速リカバリのためにローカルに残しておくことができるプライマリシステムや、プライマリシステムからデータをレプリケートする必要がないプライマリシステムで使用されます。TPSでは、SnapLockテクノロジを使用して、同じSnapLock保持期限を使用しているONTAP管理者でもプライマリSnapshotコピーが削除されないようにします。Snapshotコピーは、ボリュームでSnapLockが有効になっていない場合でも削除できません。ただし、SnapshotにはSnapLock Complianceと同じ消去不能な性質はありません。

Snapshotコピーの改ざんを防止するには"ONTAP One"、ライセンスが必要です。

詳細はこちら。

- "Snapshotコピーをロックしてランサムウェア攻撃から保護"です。

FPolicyファイルブロッキング

FPolicyは、エンタープライズクラスのストレージアプライアンスへの不要なファイルの保存をブロックします。FPolicyは、既知のランサムウェアファイル拡張子をブロックする方法も提供します。ユーザには引き続きホームフォルダに対するフルアクセス権限がありますが、FPolicyでは管理者がブロック済みとしてマークしたファイルを格納することはできません。これらのファイルが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は関係ありません。

FPolicyネイティブモードで悪意のあるファイルをブロック

NetApp FPolicyのネイティブモード（ファイルポリシーという名前を発展させたもの）は、不要なファイル拡張子が環境に侵入するのをブロックできるファイル拡張子ブロックフレームワークです。10年以上にわたってONTAPの一部として提供されており、ランサムウェアからの保護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）権限以外にもセキュリティ対策を追加できるため、価値があります。

ONTAP System ManagerおよびBlueXP では、3000を超えるファイル拡張子のリストを参照できます。

> 一部の拡張機能はご使用の環境では正当なものであり、ブロックすると予期しない問題が発生する可能性があります。ネイティブFPolicyを設定する前に、環境に適した独自のリストを作成してください。

ONTAPのネイティブモードはすべてのライセンスに含まれています。

詳細はこちら。

- "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（別名フリー）ツール"

FPolicy外部モードを使用したユーザとエンティティの動作分析（**UEBA**）の有効化

FPolicy外部モードは、ファイルアクティビティとユーザアクティビティを可視化するための、ファイルアクティビティの通知および制御フレームワークです。これらの通知は、外部ソリューションでAIベースの分析を実行して悪意のある動作を検出するために使用できます。

FPolicy外部モードは、特定のアクティビティを許可する前にFPolicyサーバからの承認を待機するように設定することもできます。このような複数のポリシーを1つのクラスタに設定できるため、柔軟性に優れています。

承認を提供するように設定されている場合、FPolicyサーバはFPolicy要求に応答する必要があります。そうしないと、ストレージシステムのパフォーマンスが低下する可能性があります。

FPolicy外部モードはに含まれてい"スヘテノONTAPライセンス"ます。

詳細はこちら。

- "ブログ：Fighting Ransomware: Part Four—UBA and ONTAP with FPolicy external mode"

Cloud Insightsストレージワークロードセキュリティ（CISWS）

Storage Workload Security（SWS；ストレージワークロードセキュリティ）は、ONTAP環境のセキュリティ体制、リカバリ性、説明責任を大幅に強化するNetApp Cloud Insightsの機能です。SWSはユーザー中心のアプローチを採用し、環境内のすべての認証済みユーザーからのすべてのファイルアクティビティを追跡します。高度な分析を使用して、すべてのユーザーの通常のアクセスパターンと季節的なアクセスパターンを確立します。これらのパターンは、ランサムウェアシグネチャを使用せずに疑わしい動作を迅速に特定するために使用されます。

SWSは、ランサムウェア、データ削除、窃盗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。

- 該当するボリュームのSnapshotを作成します。
- 悪意のあるアクティビティの疑いがあるユーザアカウントとIPアドレスをブロックします。
- 管理者にアラートを送信します。

SWSは、内部の脅威を迅速に阻止し、すべてのファイルアクティビティを追跡する自動化されたアクションを実行できるため、ランサムウェアイベントからのリカバリをはるかに簡単かつ迅速に実行できます。高度な監査ツールとフォレンジックツールが組み込まれているため、攻撃の影響を受けたボリュームやファイル、攻撃元のユーザアカウント、実行された悪意のあるアクションをすぐに確認できます。Snapshotの自動作成により、被害を軽減し、ファイルのリストアを高速化します。

[Cloud Insightsストレージワークロードセキュリティ攻撃の結果]

ONTAPのAutonomous Ransomware Protection（ARP;自律型ランサムウェア対策）によるアラートもSWSに表示されるため、ARPとSWS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。

詳細はこちら。

- "NetApp Cloud Insights の略"

NetApp ONTAPに搭載されたAIベースの検出と応答機能

ランサムウェアの脅威がますます巧妙になるにつれ、防御メカニズムも進化していきます。NetAppの自律型ランサムウェア対策（ARP）は、ONTAPに組み込まれたインテリジェントな異常検出機能を備えたAIを基盤としています。オンにすると、サイバーレジリエンスに新たな防御レイヤを追加できます。

ARPとARP / AIは、ONTAPの組み込みの管理インターフェイスと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。

自律型ランサムウェア防御（ARP）

ONTAP 9.10.1以降のもう1つのネイティブ組み込みONTAPソリューションである自律型ランサムウェア対策（ARP）では、NASストレージボリュームのワークロードのファイルアクティビティとデータエントロピーを調べて、潜在的なランサムウェアを自動的に検出します。ARPは、管理者にリアルタイムの検出、分析情報、データリカバリポイントを提供し、これまでにないオンボックスの潜在的なランサムウェア検出を可能にします。

ARPをサポートするONTAP 9 .15.1以前のバージョンでは、ARPは学習モードで開始され、一般的なワークロードのデータアクティビティを学習します。ほとんどの環境では、この処理に7日かかることがあります。ラーニングモードが完了すると、ARPは自動的にアクティブモードに切り替わり、ランサムウェアの可能性がある異常なワークロードアクティビティを探し始めます。

異常なアクティビティが検出されると、ただちにSnapshotコピーが自動作成されます。これにより、感染データを最小限に抑えながら、可能な限り攻撃時点に近いリストアポイントを作成できます。同時に、管理者が異常なファイルアクティビティを確認できる自動アラート（設定可能）が生成され、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て適切なアクションを実行できるようになります。

アクティビティが想定されるワークロードである場合、管理者は簡単に誤検出としてマークできます。ARPはこの変更を通常のワークロードアクティビティとして学習し、今後の潜在的な攻撃としてフラグを立てなくなります。

ARPをイネーブルにするには"ONTAP One"、ライセンスが必要です。

詳細はこちら。

- "自律的なランサムウェア防御"

自律型ランサムウェア対策/ AI（ARP / AI）

ONTAP 9のテクニカルプレビューとして紹介されました。15.1に搭載されたARP / AIにより、NASストレージシステムのリアルタイム検出が次のレベルに引き上げられます。AIを活用した新しい検出テクノロジは、100万件を超えるファイルやさまざまな既知のランサムウェア攻撃についてトレーニングされています。ARPで使用される信号に加えて、ARP/AIはヘッダー暗号化も検出します。AIパワーと追加信号により、ARP/AIは99%以上の検出精度を実現します。これは、ARP/AIに最高のAAA評価を与えた独立したテストラボであるSE Labsによって検証されています。

モデルのトレーニングはクラウドで継続的に行われるため、ARP / AIはラーニングモードを必要としません。オンになった瞬間にアクティブになります。継続的なトレーニングとは、ARP / AIが発生したときに常に新しいタイプのランサムウェア攻撃に対して検証されることも意味します。ARP/AIには、自動更新機能も搭載されており、ランサムウェアの検出を最新の状態に保つために、すべてのお客様に新しいパラメータを提供します。ARPの他のすべての検出、インサイト、およびデータ復旧ポイント機能は、ARP/AI用に維持されます。

ARP/AIを有効にするには"ONTAP One"、ライセンスが必要です。

詳細はこちら。

- "ブログ：NetAppのAI-based real-time ransomware detection solution achieves AAA rating"

エアギャップによるWORM保護とサイバーヴォールティング

NetAppのサイバーボールトへのアプローチは、論理的にエアギャップを埋めるサイバーボールトのために構築されたリファレンスアーキテクチャです。このアプローチでは、SnapLockなどのセキュリティ強化テクノロジやコンプライアンステクノロジを活用して、変更や消去が不可能なSnapshotを作成できます。

SnapLock Complianceと論理的なエアギャップによるサイバーヴォールティング

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。エアギャップソリューションに対する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間に、攻撃者がデータを侵害または破壊する可能性があります。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では、変更不可のSnapshotコピーとNetApp SnapLock Complianceを使用して、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。

[NetApp Cyber Vaultとの論理的なエアギャップ]

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ボリューム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のためにSnapLock Complianceを推奨しています。Snapshotコピーがロックされて削除できない特定の保持期間を設定できるため、ONTAP管理者やNetAppサポートはこの期間を指定できます。

詳細はこちら。

- "ブログ：Layered ransomware protection with NetApp's Cyber Vault solution"

Snapshotコピーの改ざん防止

SnapLock Compliance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できますが、SnapVaultを使用してSnapshotコピーをセカンダリSnapLock対応ボリュームに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。

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コピーをほぼSnapLock Compliance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。Snapshotコピーの改ざんを防止するには、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 Complianceで保存されたSnapshotコピーではできません。

SnapLock Compliance SnapLock Complianceと改ざん防止機能を備えたSnapshotコピーの主な違いは、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。

詳細はこちら。

- "Snapshotコピーをロックしてランサムウェア攻撃から保護"

Active IQランサムウェア対策

NetApp Active IQは、NetAppストレージのプロアクティブなサポートと最適化を簡易化し、実用的な情報に基づいて最適なデータ管理を実現するデジタルアドバイザです。多種多様なインストールベースから収集された計測データを基に、AIとMLの高度な手法を活用して、リスクを軽減し、ストレージ環境のパフォーマンスと効率を向上させる機会を明らかにします。

だけで "NetApp Active IQ" "セキュリティの脆弱性を排除"なく、ランサムウェアからの保護に特化した分析情報や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。

[NetApp Active IQダッシュボードの健全性監視]

[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ランサムウェア対策の実際の動作については、を参照してください"NetApp Active IQ"。

BlueXP ランサムウェア対策による包括的な耐障害性

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、できるだけ早く実施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。NetAppのランサムウェア対策は、BlueXP を使用してデータサービスに拡張するリアルタイムのオンボックス機能と、サイバーヴォールティング用の分離された階層型ソリューションを含む包括的なアプローチを採用しています。

BlueXPのランサムウェア対策

BlueXP は、ワークロード中心の包括的なランサムウェア防御をインテリジェントにオーケストレーションするための単一のコントロールプレーンです。BlueXP のランサムウェア対策には、ARP、FPolicy、改ざん防止スナップショットなどのONTAPの強力なサイバーレジリエンス機能と、BlueXP のバックアップとリカバリなどのBlueXP データサービスが統合されています。また、自動化されたワークフローによる推奨事項やガイダンスも追加され、単一のUIでエンドツーエンドの防御を実現します。ワークロードレベルで動作し、ビジネスを実行するアプリケーションを保護し、攻撃が発生した場合に可能な限り迅速にリカバリできるようにします。

[BlueXP ランサムウェア対策は、ワークロードのデータ損失を最小限に抑え、迅速に回復するために必要なAIベースのインテリジェンスと支援です。この図は、BlueXP UIを示しています。]

お客様にもたらされるメリット：

- ランサムウェアへの備えを支援することで、運用上のオーバーヘッドを軽減し、効果を向上
- AI / MLを活用した異常検出により、高い精度と迅速な対応でリスクを抑制
- アプリケーションと整合性のあるガイド付きリストアにより、ワークロードを数分で簡単にリカバリできます。

"BlueXPのランサムウェア対策"これらのNIST機能を簡単に実現できます。

- アプリケーションベースの最上位のワークロードに重点を置いて、NetAppストレージ*内のデータを自動的に*検出*し、優先順位を付けます*。
- トップワークロードのデータバックアップ、不変で安全な構成、悪意のあるファイルブロッキング、さまざまなセキュリティドメインのワンクリック保護。
- 次世代の**AI**ベースの異常検出*を使用して、*ランサムウェアを*可能な限り*迅速に*正確に検出*します。
- 自動化された応答とワークフロー、およびトップ* SIEMおよびXDRソリューションとの統合*。
- シンプルな*オーケストレーションされたリカバリ*を使用してデータを迅速にリストアし、アプリケーションのアップタイムを短縮します。
- ランサムウェア対策*戦略と*ポリシー*を導入し、*成果を監視*します。

著作権に関する情報

商標に関する情報