NetAppとゼロトラスト

ONTAP Technical Reports

NetApp
January 23, 2026

目次

NetAppとゼロトラスト

NetAppとゼロトラスト

ゼロトラストは、従来、マイクロコアと境界（MCAP）を構築してデータ、サービス、アプリケーション、資産を保護するネットワーク中心のアプローチであり、セグメンテーションゲートウェイと呼ばれる制御機能を備えていました。NetApp ONTAPは、ゼロトラストに対してデータ主体のアプローチを採用しています。このアプローチでは、ストレージ管理システムが、お客様のデータへのアクセスを保護および監視するためのセグメンテーションゲートウェイになります。特に、FPolicyゼロトラストエンジンとFPolicyパートナーエコシステムは、正常なデータアクセスパターンと異常なデータアクセスパターンを詳細に把握し、内部の脅威を特定するためのコントロールセンターとなります。

2024年7月より、以前はPDF形式で公開されていたテクニカルレポート『TR-4829：NetApp and Zero Trust：Enabling a data-centric Zero Trust model_』のコンテンツがdocs.netapp.comで公開されました。

データは組織が所有する最も重要な資産です。2022年の調査によると、内部の脅威はデータ漏えいの18%の原因です "Verizon Data Breach Investigationsレポート"。NetApp ONTAPデータ管理ソフトウェアを使用して、業界をリードするゼロトラストコントロールをデータに導入することで、組織は警戒を強化できます。

ゼロトラストとは

ゼロトラストモデルは、Forrester ResearchのJohn Kindervagによって最初に開発されました。外部からではなく内部からのネットワークセキュリティを想定しています。 Inside-Out Zero Trustアプローチは、マイクロコアと境界（MCAP）を特定します。MCAPは、包括的な制御セットで保護するデータ、サービス、アプリケーション、資産の内部定義です。安全な外部境界の概念は廃止されています。信頼され、境界を介して正常に認証されることが許可されているエンティティは、組織を攻撃に対して脆弱にする可能性があります。内部関係者は、定義上、すでに安全な境界内にいます。従業員、請負業者、およびパートナーは内部関係者であり、組織のインフラストラクチャ内で役割を実行するための適切な制御で運用できるようにする必要があります。

ゼロトラストは、2019年9月に国防総省に約束する技術として言及されました "FY19-23 DoDのデジタル最新化戦略"。Zero Trustは、「データ漏えいを阻止するためにアーキテクチャ全体にセキュリティを組み込むサイバーセキュリティ戦略です。このデータ中心のセキュリティモデルは、信頼できるネットワーク、デバイス、ペルソナ、またはプロセスという概念を排除し、最小特権アクセスの概念の下で認証および承認ポリシーを可能にするマルチ属性ベースの信頼レベルに移行します。ゼロトラストを実装するには、既存のインフラストラクチャを使用して、よりシンプルで効率的な方法でセキュリティを実装する方法を再考する必要があります。

2020年8月、NISTは(ZTA)を発表しまし "Special Pub 800-207ゼロトラストアーキテクチャ" た。ZTAは、ネットワークセグメントではなくリソースの保護に重点を置いています。これは、ネットワークの場所がリソースのセキュリティ体制の主要なコンポーネントではなくなったためです。リソースとはデータとコンピューティングです。ZTA戦略は、エンタープライズネットワークアーキテクト向けです。ZTAでは、元のForresterの概念から新しい用語がいくつか導入されています。ポリシー決定ポイント（PDP）およびポリシー施行ポイント（PEP）と呼ばれる保護メカニズムは、Forresterセグメンテーションゲートウェイに似ています。ZTAでは、次の4つの導入モデルを導入

- デバイスエージェントまたはゲートウェイベースの展開

- Enclaveベースの導入（Forrester MCAPに似ています）
- リソースポータルベースの導入
- デバイスアプリケーションのサンドボックス化

このドキュメントの目的のために、NIST ZTAではなくForrester Researchの概念と用語を使用しています。

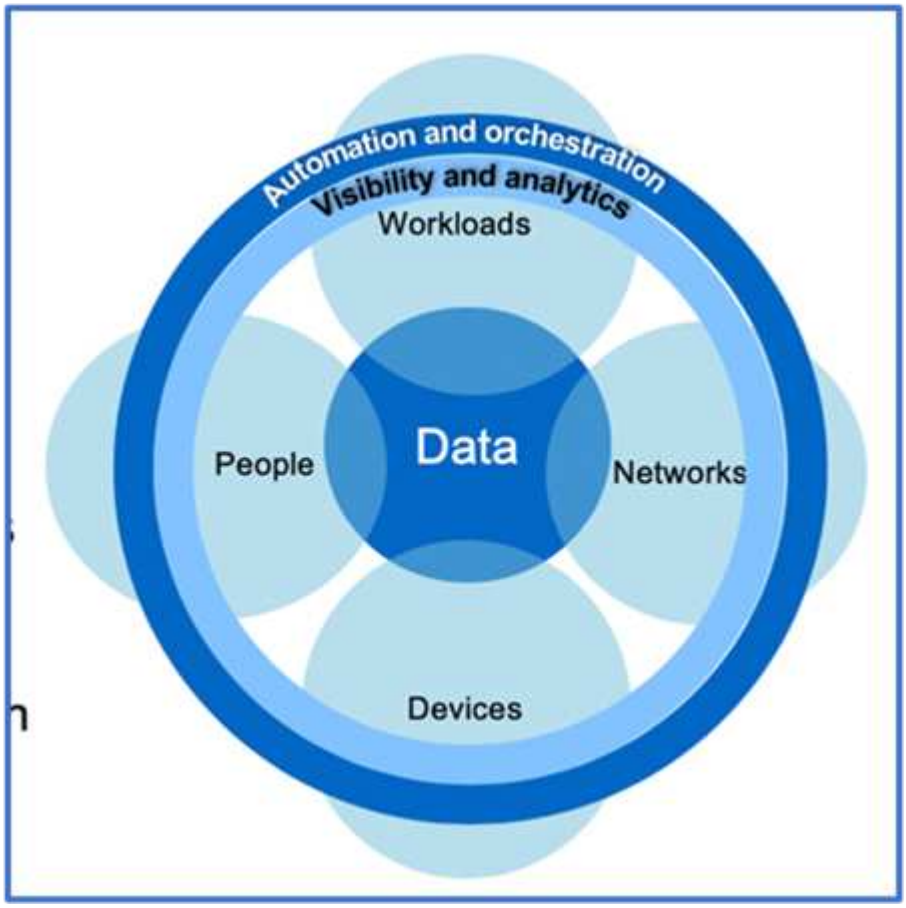
セキュリティリソース

脆弱性とインシデントの報告、NetAppのセキュリティ対応、および顧客の機密性の詳細については、を参照してください "NetAppセキュリティポータル"。

ONTAPでデータ主体のアプローチでゼロトラストを実現

ゼロトラストネットワークは、データ中心のアプローチによって定義され、セキュリティ制御は可能な限りデータに近いものにする必要があります。ONTAPの機能とNetApp FPolicyパートナーエコシステムを組み合わせることで、データ中心のゼロトラストモデルに必要な制御を提供できます。

ONTAPは、NetAppが提供するセキュリティリッチなデータ管理ソフトウェアです。FPolicyゼロトラストエンジンは業界をリードするONTAP機能で、きめ細かなファイルベースのイベント通知インターフェイスを提供します。NetAppのFPolicyパートナーは、このインターフェイスを使用して、ONTAP内のデータアクセスの照度を高めることができます。



ゼロトラストのデータ主体の**MCAP**を設計

データ中心のゼロトラストMCAPを設計するには、次の手順を実行します。

1. すべての組織データの場所を特定します。
2. データを分類
3. 不要になったデータを安全に破棄できます。
4. データ分類へのアクセス権を持つ役割を理解する。
5. 最小権限の原則を適用して、アクセス制御を適用します。
6. 管理アクセスとデータアクセスに多要素認証を使用します。
7. 保存中のデータと転送中のデータに暗号化を使用
8. すべてのアクセスを監視してログに記録します。
9. 不審なアクセスまたは動作を警告します。

すべての組織データの場所を特定する

ONTAPのFPolicy機能とパートナーのNetAppアライアンスパートナーエコシステムを組み合わせることで、組織のデータがどこに存在し、誰がデータにアクセスできるかを特定できます。これには、データアクセスパターンが有効かどうかを特定するユーザ行動分析が使用されます。ユーザーの行動分析の詳細については、「すべてのアクセスを監視してログに記録する」を参照してください。データがどこにあり、誰がデータにアクセスできるかを理解していない場合、ユーザー行動分析は、経験的観察から分類とポリシーを構築するためのベースラインを提供できます。

データを分類

ゼロ トラスト モデルという用語の文脈では、データ分類の過程で高リスク データを特定する必要があります。高リスク データとは、組織外への公開が意図されていない機密データのことを指します。有害なデータの開示は、規制コンプライアンスに違反し、組織の評判を損なう可能性があります。規制遵守の観点から、有害データには、 "クレジットカード業界の データ セキュリティ 標準 (PCI-DSS)" EUの個人データ "一般データ保護規則（GDPR）"、またはヘルスケアデータ "医療保険の携行性と責任に関する法律（HIPAA）"。NetAppを利用できます "NetApp Data Classification"(旧称 Cloud Data Sense) は、AI を活用したツールキットで、データを自動的にスキャン、分析、分類します。

不要になったデータを安全に廃棄

組織のデータを分類した後、一部のデータが不要になったり、組織の機能と関連性がなくなったりすることがあります。不要なデータの保持は責任であり、そのようなデータは削除する必要があります。暗号化によってデータを消去する高度なメカニズムについては、「保存データの暗号化」でのセキュアパージの説明を参照してください。

データ分類へのアクセス権が必要な役割を理解し、アクセス制御を実施するために最小権限の原則を適用する

機密データへのアクセスをマッピングし、最小権限の原則を適用すると、組織内のユーザーに、業務の遂行に必要なデータのみにアクセスできるようになります。このプロセスにはロールベースアクセス制御が含まれ("RBAC"ます）。これは、データアクセスと管理アクセスに適用されます。

ONTAPでは、Storage Virtual Machine（SVM）を使用して、ONTAPクラスタ内のテナントによる組織のデータアクセスを分割できます。RBACは、SVMへのデータアクセスと管理アクセスに適用できます。RBACはク

ラスタ管理レベルでも適用できます。

RBACに加えて、ONTAP（MAV）を使用して、またはなどのコマンドの承認を1人以上の管理者に要求することができます "マルチ管理者認証" `volume delete` `volume snapshot delete`。MAVを有効にすると、MAVを変更または無効にするには、MAV管理者の承認が必要になります。

スナップショットを保護するもう1つの方法は、ONTAP"Snapshotロック"です。Snapshotロックは、ボリュームSnapshotポリシーの保持期間に応じて手動または自動でSnapshotを消去できないようにするSnapLock機能です。スナップショットロックは、改ざん防止スナップショットロックとも呼ばれます。スナップショットロックの目的は、不正な管理者や信頼されていない管理者が、プライマリおよびセカンダリONTAPシステム上のスナップショットを削除するのを防ぐことです。ランサムウェアによって破損したボリュームをリストアするために、プライマリシステム上のロックされたSnapshotの迅速なリカバリを実現できます。

管理アクセスとデータアクセスに多要素認証を使用

クラスタ管理のRBACに加えて、 "多要素認証（MFA）" ONTAP Web管理アクセスおよびSecure Shell（SSH）コマンドラインアクセス用にも導入できます。管理者アクセスのためのMFAは、米国の公共機関またはPCI-DSSに従う必要がある組織の要件です。MFAを使用すると、攻撃者がユーザー名とパスワードのみを使用してアカウントを侵害することが不可能になります。MFAでは、認証に2つ以上の独立した要素が必要です。二要素認証の例としては、秘密鍵などのユーザが所有するものや、パスワードなどのユーザが知っているものがあります。ONTAP System ManagerまたはActiveIQ Unified Managerへの管理Webアクセスは、Security Assertion Markup Language（SAML）2.0で有効になります。SSHコマンドラインアクセスでは、公開鍵とパスワードを使用したチェーン型の2要素認証が使用されます。

ONTAPのIDおよびアクセス管理機能を使用して、APIを使用してユーザおよびマシンのアクセスを制御できます。

- ユーザ：
  - *認証と承認。*SMBとNFSのNASプロトコル機能を介して提供
  - *監査。*アクセスおよびイベントのsyslog。認証ポリシーと許可ポリシーをテストするためのCIFSプロトコルの詳細な監査ログ。詳細なNASアクセスをファイルレベルできめ細かくFPolicyで監査
- デバイス：
  - *認証。*APIアクセス用の証明書ベースの認証。
  - *承認。*デフォルトまたはカスタムのRole-Based Access Control（RBAC；ロールベースアクセス制御）。
  - *監査。*実行されたすべてのアクションのsyslog。

保存中のデータと転送中のデータに暗号化を使用

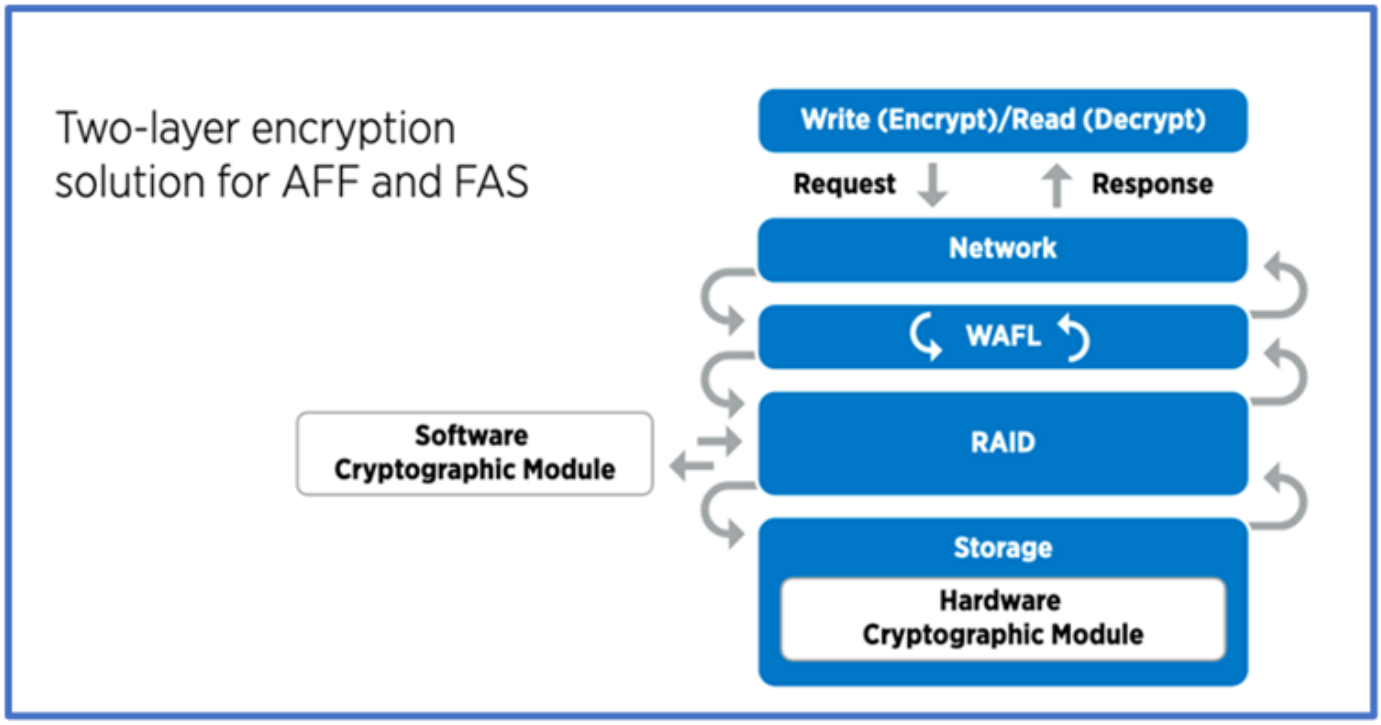
保存データ暗号化

組織がドライブの転用、故障したドライブの返却、大容量ドライブの販売や取り引きを行ってドライブをアップグレードする際に、ストレージシステムのリスクとインフラのギャップを軽減するための新たな要件が日々 発生しています。 ストレージエンジニアには、データの管理者や運用者として、データのライフサイクルを通じて安全にデータを管理、維持することが求められています。 "NetAppストレージ暗号化（NSE）；NetAppボリューム暗号化（NVE）；およびNetAppアグリゲート暗号化" 毒性があるかどうかにかかわらず、日常の運用に影響を与えることなく、保管中のすべてのデータを常に暗号化できます。 "NSE" は、FIPS 140-2レベル2認定自己暗号化ドライブを使用するONTAPハードウェアソリューションです "保存データ" 。 "NVE および NAE" は、を使用するONTAPソフトウェアソリューションです "保存データ" "FIPS 140-2レベル1認定NetApp暗号モジュール"。NVEおよびNAEでは、ハードドライブまたはソリッドステートドライブの

いずれかを使用して保存データを暗号化できます。さらに、NSEドライブを使用して、暗号化の冗長性とセキュリティを強化するネイティブの階層型暗号化ソリューションを提供できます。1つのレイヤに違反しても、2つ目のレイヤでデータが保護されます。これらの機能により、ONTAPはに適しています "Quantum対応の暗号化"。

NVEには、機密ファイルが分類されていないボリュームに書き込まれたときに、暗号化によってデータ流出から有害なデータを削除するという機能もあります。 "セキュアパージ"

ONTAPに組み込まれているキー管理ツールであるを "オンボードキーマネージャ（ OKM ）"使用するか、 "承認済み" またはサードパーティ製品 "カイフキカンリツル" をNSEおよびNVEと併用して、キー情報をセキュアに格納できます。



上の図に示すように、ハードウェアベースとソフトウェアベースの暗号化を組み合わせることができます。この機能により、ではトップシークレットデータの保存が可能になり "分類されたプログラムのためのNSAの商用ソリューションへのONTAPの検証" ました。

転送中データの暗号化

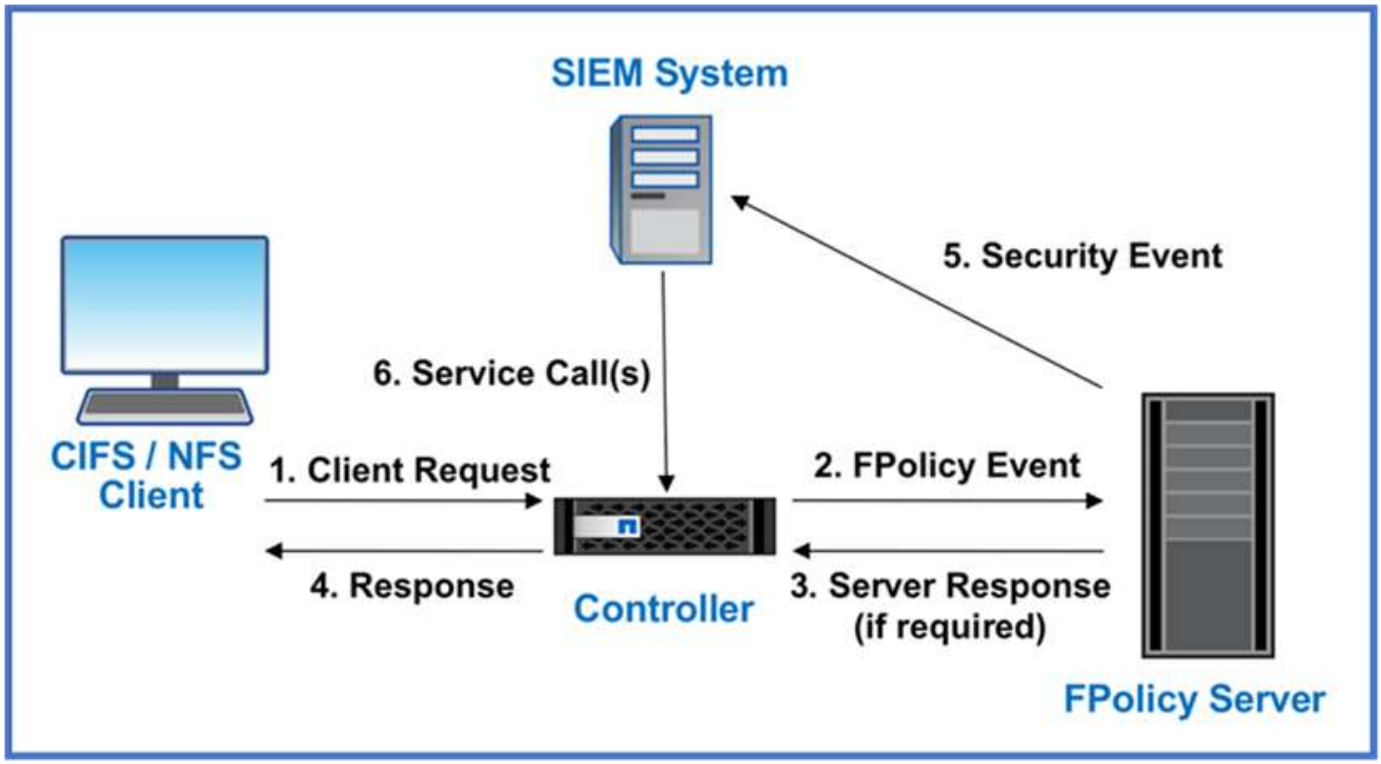
ONTAPの転送中データ暗号化により、ユーザデータアクセスとコントロールプレーンアクセスが保護されます。ユーザデータアクセスは、Microsoft CIFS共有アクセスの場合はSMB 3.0暗号化、NFS Kerberos 5の場合はkrb5pによって暗号化できます。ユーザデータアクセスは、を使用してCIFS、NFS、iSCSIの暗号化することもできます "IPSec" 。コントロールプレーンアクセスは、Transport Layer Security（TLS）で暗号化されます。ONTAPには、コントロールプレーンアクセスのコンプライアンスモードが用意されて"FIPS"います。このモードでは、FIPS承認のアルゴリズムが有効になり、FIPS承認でないアルゴリズムが無効になります。データレプリケーションはで暗号化され "クラスタピア暗号化"ます。これにより、ONTAP SnapVaultテクノロジとSnapMirrorテクノロジが暗号化されます。

すべてのアクセスを監視してログに記録

RBACポリシーを設定したら、アクティブな監視、監査、アラートを導入する必要があります。NetApp ONTAPのFPolicyゼロトラストエンジンとを組み合わせること "NetApp FPolicyパートナーエコシステム"で、データ主体のゼロトラストモデルに必要な制御を実現できます。NetApp ONTAPは、セキュリティが充実した

データ管理ソフトウェアであり "FPolicy" 、きめ細かなファイルベースのイベント通知インターフェイスを提供する、業界をリードするONTAP機能です。NetAppのFPolicyパートナーは、このインターフェイスを使用して、ONTAP内のデータアクセスの照度を高めることができます。ONTAPのFPolicy機能とFPolicyパートナーのNetAppアライアンスパートナーエコシステムを組み合わせることで、組織のデータがどこに存在し、誰がデータにアクセスできるかを特定できます。これには、データアクセスパターンが有効かどうかを特定するユーザ行動分析が使用されます。ユーザの行動分析を使用すると、通常のパターンから外れた不審なデータアクセスや異常なデータアクセスをアラートで通知し、必要に応じてアクセスを拒否するアクションを実行できます。

FPolicyパートナーは、ユーザ行動分析にとどまらず、機械学習（ML）や人工知能（AI）に移行しつつあります。これにより、イベントの忠実度が向上し、誤検出があった場合にはそれを減らすことができます。すべてのイベントは、syslogサーバ、またはMLやAIを使用できるセキュリティ情報イベント管理（SIEM）システムに記録する必要があります。



NetAppの "DII ストレージ ワークロード セキュリティ"クラウドとオンプレミスの両方のONTAPストレージ システムで FPolicy インターフェイスとユーザー行動分析を利用して、悪意のあるユーザー行動に関するリアルタイムのアラートを提供します。また、高度な機械学習と異常検出機能により、悪意のあるユーザやセキュリティ侵害を受けたユーザが組織のデータを不正利用できないよう保護します。ストレージ ワークロード セキュリティは、ランサムウェア攻撃やその他の不正行為を識別し、スナップショットを呼び出して悪意のあるユーザーを隔離できます。また、フォレンジック機能により、ユーザとエンティティのアクティビティを詳細に把握できます。ストレージ ワークロード セキュリティは、 NetApp Data Infrastructure Insightsの一部です。

ONTAPには、ストレージワークロードのセキュリティに加えて、（ARP）と呼ばれるランサムウェア検出機能が搭載され "自律型ランサムウェア対策" ています。ARPは機械学習を使用して、ランサムウェア攻撃が進行中であることを示す異常なファイルアクティビティがないかどうかを判断し、スナップショットを呼び出して管理者にアラートを送信します。Storage Workload Securityは、ONTAPと統合してARPイベントを受信し、追加の分析機能と自動応答レイヤを提供します。

この手順で説明されているコマンドの詳細については、を"ONTAPコマンド リファレンス"参照してください。

ONTAPの外部にあるNetAppセキュリティの自動化とオーケストレーションの制御

自動化を使用すると、最小限の人間の支援でプロセスや手順を実行できます。自動化により、組織はゼロトラスト環境を手動の手順をはるかに超えて拡張し、自動化された不正なアクティビティから保護できます。

Ansibleは、オープンソースのソフトウェアプロビジョニング、構成管理、アプリケーション導入ツールです。多くのUnixライクなシステムで動作し、Microsoft Windowsと同様にUnixライクなシステムの両方を構成することができる。システム構成を記述するための独自の宣言言語が含まれています。AnsibleはMichael DeHaanによって書かれ、2015年にRed Hatに買収された。Ansibleはエージェントレスで、SSHまたはWindowsリモート管理（リモートPowerShell実行可能）を使用して一時的にリモート接続し、タスクを実行します。NetAppはさらに多くの製品を開発し "ONTAPソフトウェア向け150個のAnsibleモジュール" 、Ansible自動化フレームワークとのさらなる統合を可能にしています。NetApp向けのAnsibleモジュールは、必要な状態を定義してターゲットのNetApp環境にリレーする方法に関する一連の指示を提供します。モジュールは、ライセンスのセットアップ、アグリゲートとStorage Virtual Machineの作成、ボリュームの作成、Snapshotのリストアなどのタスクをサポートするように構築されています。Ansibleのロールは "GitHubで公開" 、NetApp DoD Unified Capabilities（UC）Deployment Guideに固有のものです。

利用可能なモジュールのライブラリを使用することで、Ansibleプレイブックを簡単に開発し、独自のアプリケーションやビジネスニーズに合わせてカスタマイズして、日常的なタスクを自動化できます。作成したプレイブックを実行して指定したタスクを実行することで、時間を節約し、生産性を向上させることができます。NetAppでは、サンプルのプレイブックを作成して共有しています。プレイブックは直接使用することも、ニーズに合わせてカスタマイズすることもできます。

Data Infrastructure Insightsは、インフラストラクチャ全体の可視性を提供するインフラストラクチャ監視ツールです。 Data Infrastructure Insightsを使用すると、パブリック クラウド インスタンスやプライベート データ センターを含むすべてのリソースを監視、トラブルシューティング、最適化できます。 Data Infrastructure Insights を使用すると、平均解決時間を 90% 短縮し、クラウドの問題の 80% がエンド ユーザーに影響を与えるのを防ぐことができます。クラウド インフラのコストを平均で33%削減可能なほか、実用的なインテリジェンスによりデータを保護し、内部の脅威に対するリスクも軽減できます。 Data Infrastructure Insightsのストレージ ワークロード セキュリティ機能により、AI と ML を使用したユーザー行動分析が可能になり、内部脅威によって異常なユーザー行動が発生したときに警告を発することができます。ONTAPの場合、Storage Workload SecurityではゼロトラストFPolicyエンジンを使用します。

ゼロトラストとハイブリッドクラウド環境

NetAppは、ハイブリッド クラウドのデータに関するオーソリティです。NetAppは、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud、その他の主要なクラウド プロバイダーを使用して、オンプレミスのデータ管理システムをハイブリッド クラウドに拡張するためのさまざまなオプションを提供しています。NetAppのハイブリッド クラウド ソリューションは、オンプレミスのONTAPシステムおよびONTAP Select Software-Defined Storageで採用されているものと同じゼロ トラスト セキュリティ対策に対応しています。

AWS (FSxN)、Google Cloud (GCNV)、および Microsoft Azure 向けAzure NetApp Files向けのエンタープライズ クラスのクラウドネイティブ ファイル サービスを使用することで、一般的な CAPEX 制約なしにパブリック クラウドの容量を簡単に拡張できます。これらは分析やDevOpsなど、データを大量に使用するワークロードに最適なクラウド データ サービスであり、NetAppの柔軟性のあるオンデマンド ストレージ サービスと、ONTAPデータ管理機能をフルマネージド形式で組み合わせて利用できます。

ONTAP は、 NetApp SnapMirrorデータ レプリケーション ソフトウェアを使用して、オンプレミスのONTAP システムと AWS、Google Cloud、または Azure ストレージ環境間でデータを移動できるようにします。

著作権に関する情報

商標に関する情報