



ゼロトラストモデルを実現 ONTAP 9

NetApp
July 12, 2024

目次

ゼロトラストモデルを実現	1
NetAppとゼロトラスト	1
ONTAPでデータ主体のアプローチでゼロトラストを実現	2
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	7
ゼロトラストとハイブリッドクラウド環境	7
ONTAPゼロトラストコンテンツの詳細	8

ゼロトラストモデルを実現

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、以前にPDFとして公開されていたテクニカルレポート『TR-4015：NetApp and Zero Trust：Enabling a data-centric Zero Trust model』のコンテンツが、ONTAPのその他の製品ドキュメントに統合されました。

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によって最初に開発され "[John Kindervag氏](#)" 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、パートナーは内部関係者であるため、組織のインフラ内で役割を果たすために適切な管理を行って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どのように活用して、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かを再考する必要があります。

2020年8月、NISTは(ZTA)を発表し "[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。

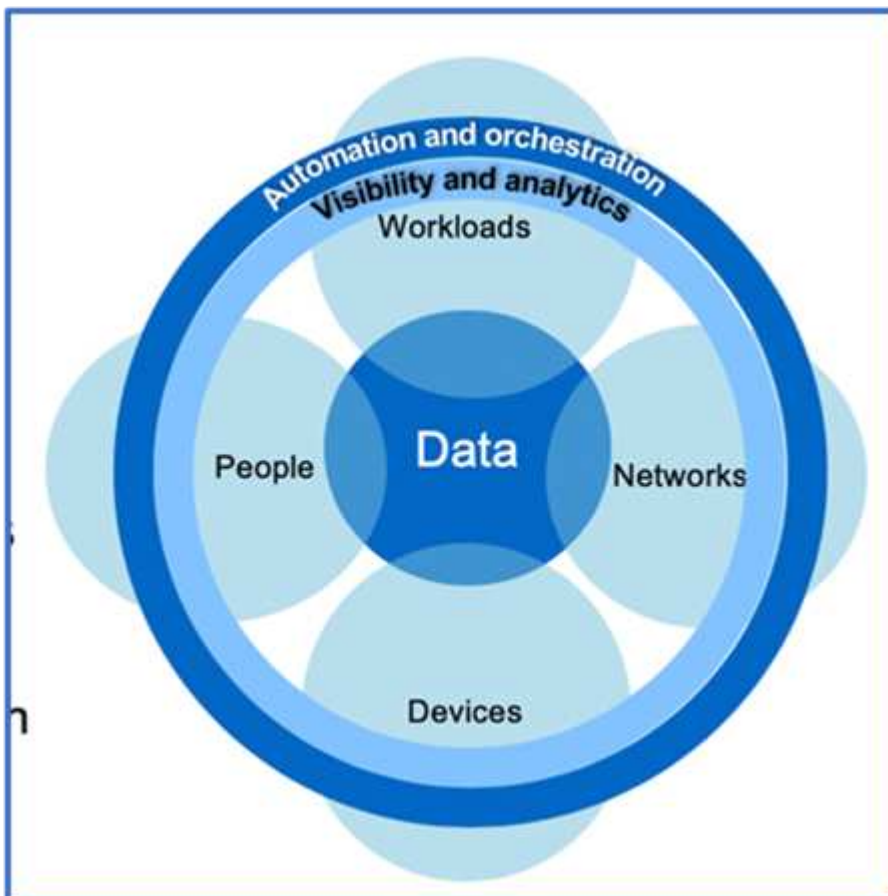
セキュリティリソース

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の用語では、データの分類には毒性データの識別が含まれます。有害データとは、組織の外部に公開することを意図していない機密データです。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。規制コンプライアンスの観点から、有害データには、のカード所有者データ、EUの個人データ、またはの医療データが含まれます ["クレジットカード業界のデータセキュリティ標準 \(PCI-DSS\)"](#) ["一般データ保護規則 \(GDPR\)"](#) ["医療保険の携行性と責任に関する法律 \(HIPAA\)"](#)。AIベースのツールキットであるNetApp (旧称Cloud Data Sense) を使用すると、データを自動的にスキャン、分析、分類でき ["BlueXPの分類"](#) 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」でのセキュアペ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。

Snapshotコピーを保護するもう1つの方法として、ONTAPがあり **"Snapshotコピーロック"**ます。Snapshotコピーロックは、ボリュームSnapshotコピーポリシーの保持期間に応じて手動または自動でSnapshotコピーを消去できないようにするSnapLock機能です。Snapshotコピーロックは、改ざん防止Snapshotコピーロックとも呼ばれます。Snapshotコピーロックの目的は、悪意のある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Snapshotコピーを削除しないようにすることです。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コピーを迅速にリカバリできます。

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

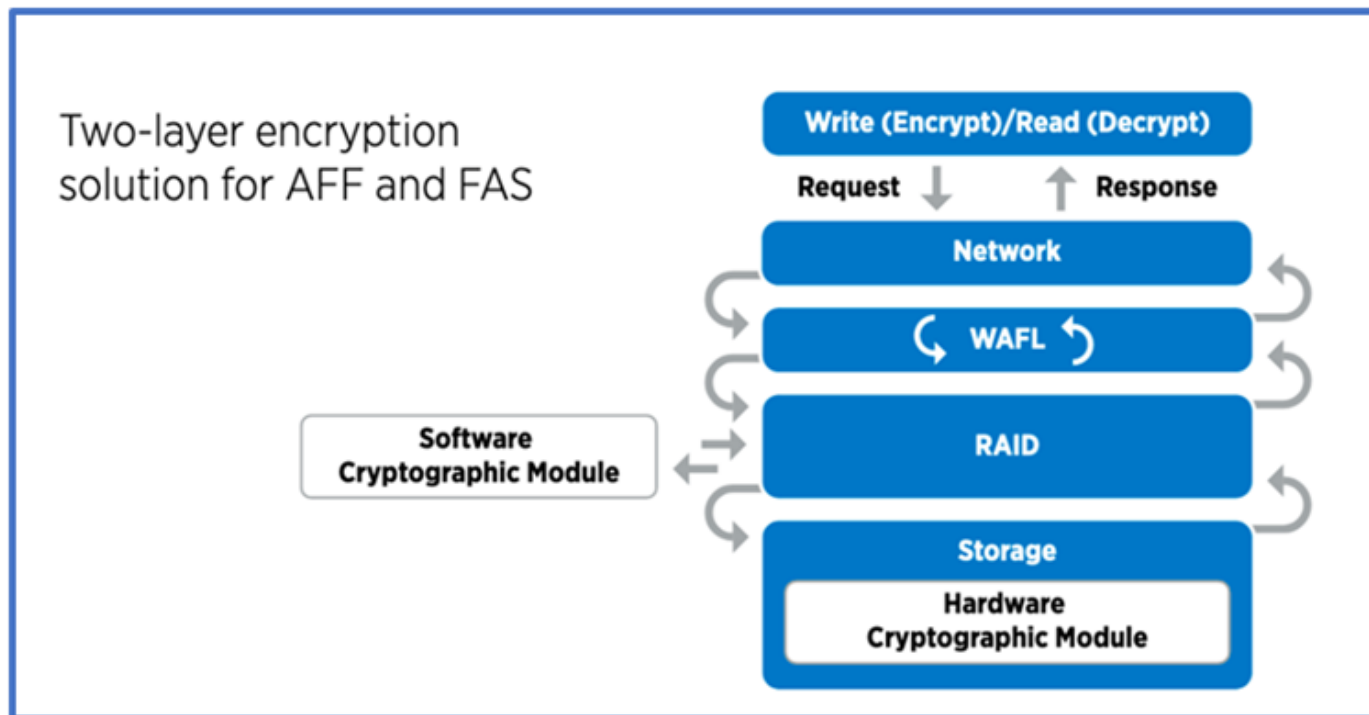
保存データ暗号化

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のハードウェア保管データソリューションです。 **"NVEおよびNAE"** は、を使用するONTAPソフトウェアの保存データデータソリューションです **"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。 ["セキュアパーズ"](#)

ONTAPに組み込みのキー管理ツールである ["オンボードキーマネージャ \(OKM\)"](#) 使用するか、 ["承認済み"](#) サードパーティ製 ["カイフキカンリツル"](#) をNSEおよびNVEとともに使用して、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"](#) しました。

転送中データの暗号化

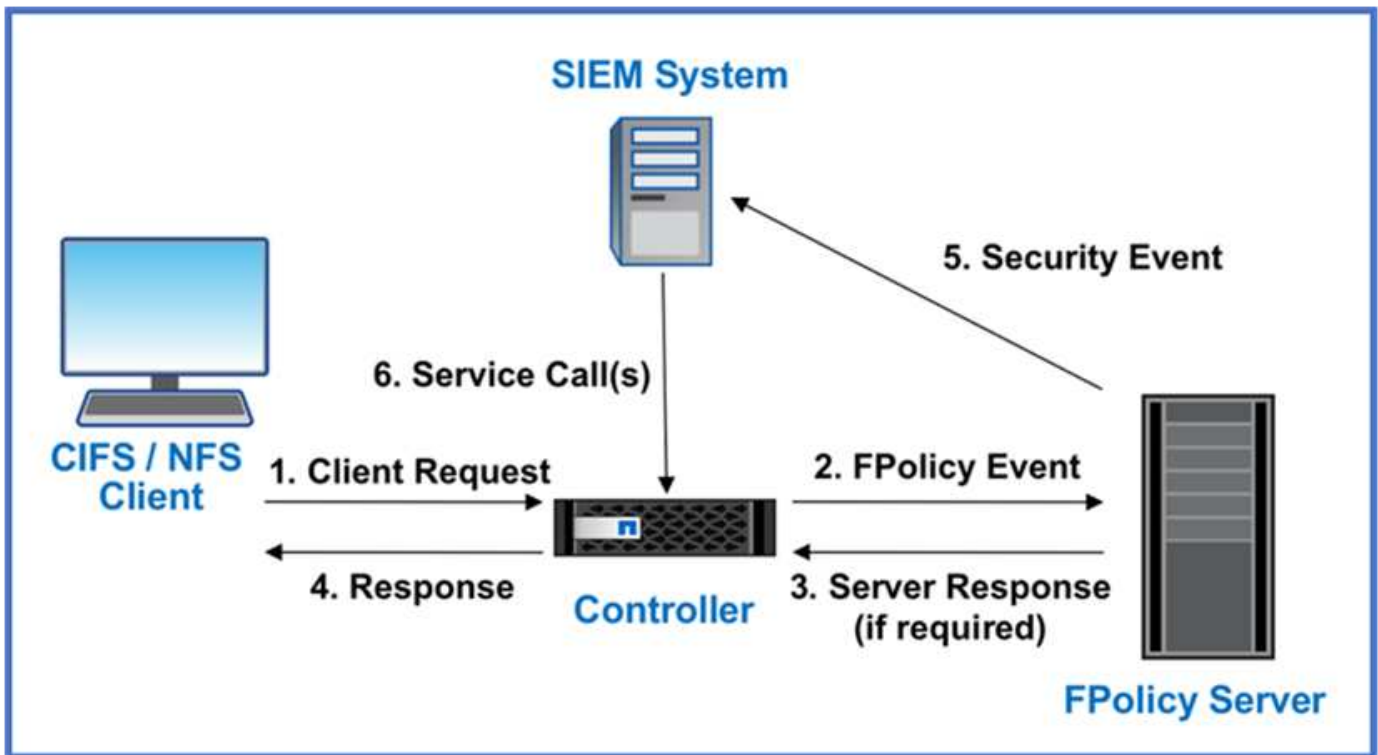
ONTAPの転送中データ暗号化により、ユーザデータアクセスとコントロールプレーンアクセスが保護されます。ユーザデータアクセスは、Microsoft CIFS共有アクセスの場合はSMB 3.0暗号化、NFS Kerberos 5の場合はkrb5pによって暗号化できます。ユーザデータアクセスは、を使用してCIFS、NFS、iSCSIの暗号化することもできます ["IPSec"](#)。コントロールプレーンアクセスは、Transport Layer Security (TLS) で暗号化されません。ONTAPには、コントロールプレーンアクセスのコンプライアンスモードが用意されて ["FIPS"](#) 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 の"**、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。



ネットアップのストレージワークロードセキュリティ (旧称: **"Cloud Secure"**) は、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行動分析を使用して、悪意のあるユーザの行動に関するリアルタイムのアラートを提供します。Storage Workload Securityは、高度な機械学習と異常検出機能を通じて、悪意のあるユーザや不正ユーザによる不正使用を防ぎます。Storage Workload Securityは、ランサムウェア攻撃やその他の不正な動作を特定し、Snapshotコピーを起動して、悪意のあるユーザを隔離します。Storage Workload Securityには、ユーザとエンティティのアクティビティの詳細を表示するフォレンジック機能もあります。ストレージワークロードセキュリティはNetApp Cloud 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 **"自律的なランサムウェア防御"** 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、Snapshotコピー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。

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、

利用可能なモジュールのライブラリを使用すると、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。

Cloud Insightsは、インフラ全体を可視化できるインフラ監視ツールです。Cloud 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、すべてのリソースの監視、トラブルシューティング、最適化を実行できます。Cloud Insightsを使用すると、平均問題解決時間を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及ぼすのを防止できます。また、実用的な情報に基づいてデータを保護することで、クラウドインフラのコストを平均33%削減し、内部の脅威によるリスクを軽減できます。Cloud Insightsのストレージワークロードセキュリティ機能を使用すると、内部の脅威が原因でユーザの異常な行動が発生した場合に、AIやMLを使用したユーザ行動分析でアラートを生成できます。ONTAPの場合、ストレージワークロードセキュリティはゼロトラスト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

ネットアップは、ハイブリッドクラウド環境におけるデータ管理のオーソリティです。NetAppは、Amazon Web Services (AWS)、Microsoft Azure、Google Cloud Platform (GCP) などの主要なクラウドプロバイダを利用して、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システムとONTAP SelectのSoftware-Defined Storageと同じゼロトラストセキュリティ管理をサポートします。

業界初のエンタープライズクラスのAWS / GCP向けクラウドネイティブファイルサービスであるNetApp Cloud Volumes Serviceと、Azure NetApp Files for Microsoft Azureを使用すれば、一般的なCAPEX（設備投資）の制約を受けることなくパブリッククラウドの容量を簡単に拡張できます。分析やDevOpsなど、大量のデータを処理するワークロードに最適なこのクラウドデータサービスは、NetAppの柔軟なオンデマンドストレージサービスとONTAPデータ管理機能を組み合わせたフルマネージドサービスです。

AWS EBSやS3、Azureストレージなど、クラウドブロックサービスやオブジェクトストレージサービス向けの高度なデータサービスをお探しの場合は、Cloud Volumes ONTAPを使用すれば、オンプレミス環境とパブリッククラウド間のデータ管理を単一の共通ビューで管理できます。AWSまたはAzureでオンデマンドインスタンスとして実行されるCloud Volumes ONTAPは、ONTAPソフトウェアのStorage Efficiency、可用性、拡張性を提供します。ONTAPでは、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またはAzureのストレージ環境の間でデータを移動できます。

ONTAPゼロトラストコンテンツの詳細

ONTAPゼロトラストのコンテンツに記載されている情報の詳細については、次のドキュメントやWebサイトを参照してください。

- ["Verizon Data Breach Investigationsレポート"](#)
- ["国防総省のデジタル最新化戦略"](#)
- ["NIST SP 800-207ゼロトラストアーキテクチャ"](#)
- ["NetApp Partner Connect：セキュリティアライアンスパートナー"](#)
- ["SVMでのFPolicyによるファイルの監視と管理"](#)
- ["PCI-DSS 3.2 ONTAP 9"](#)
- ["一般データ保護規則（GDPR）"](#)
- ["HIPPAプライバシー規則の概要"](#)
- ["NetApp BlueXPの分類"](#)
- ["管理者による検証が複数必要です"](#)
- ["タンパープルーフスナップショットコピーロック"](#)
- ["ONTAP 9での多要素認証"](#)
- ["NetApp ストレージ暗号化、 NVMe 自己暗号化ドライブ、 NetApp Volume Encryption 、 NetApp Aggregate Encryption"](#)
- ["NetApp Storage Encryption の略"](#)
- ["NetApp Volume Encryption および NetApp Aggregate Encryption の略"](#)
- ["NetApp暗号モジュールFIPS-140-2証明書"](#)
- ["NetAppによるQuantum対応の保管データ暗号化"](#)
- ["セキュリティでイノベーション：NetAppとOntrackがフラッシュメモリサミットアワードを受賞"](#)
- ["オンボード キー管理の有効化"](#)
- ["NetApp Interoperability Matrix Tool で確認できます"](#)
- ["外部キー管理の設定"](#)
- ["分類された企業向けソリューション"](#)
- ["ONTAP IPsec"](#)
- ["security config modifyを使用してFIPSモードを有効にする"](#)
- ["既存のピア関係でのクラスタ ピ어링暗号化の有効化"](#)

- "ストレージワークロードのセキュリティ (Cloud Secure) "
- "NetAppとAnsibleで開発ワークフローを自動化する方法をご紹介します"
- "NetApp DoD Unified Capabilities (UC) 導入ガイドに固有のAnsibleモジュール"
- "管理者認証とRBAC"
- "ONTAP保存データの暗号化"
- "TR-4569 『Security Hardening Guide for NetApp ONTAP 9』 "

著作権に関する情報

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および/または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。