ゼロトラストの導入: 安全かつ機敏なビジネス変革戦略のための戦略

AWS 規範ガイダンス

AWS 規範ガイダンス: ゼロトラストの導入: 安全かつ機敏なビジネス変革戦略のための戦略

Table of Contents

序章 1
意思決定プロセス 1
ターゲットを絞ったビジネス成果 3
セキュリティ態勢の強化 3
シームレスなクラウドの採用 3
コンプライアンスと規制の調整 3
データ保護の強化 4
効率的なインシデント対応 4
従業員の生産性向上 5
デジタルトランスフォーメーションの活用 5
セクション概要 5
ゼロトラストの原則 6
検証と認証 6
最小特権アクセス 6
マイクロセグメンテーション 6
継続的なモニタリングと分析 7
自動化とオーケストレーション 7
Authorization 7
セクション概要 8
ZTA の主要コンポーネント 9
ID とアクセス管理 9
セキュアアクセスサービスエッジ 9
データ損失防止 9
Security Information and Event Management 10
エンタープライズリソース所有権カタログ 10
統合エンドポイント管理 10
ポリシーベースの適用ポイント 10
セクション概要 11
組織の準備状況 12
リーダーシップの連携とコミュニケーション 12
スキル開発とトレーニング 12
組織構造と役割 13
IT インフラストラクチャとアーキテクチャ 14
リスク管理、ガバナンス、変更管理 14

モニタリングと評価 14
セクション概要 15
ゼロトラストの考え方 16
ゼロトラストの教育とトレーニング 16
協力とコミュニケーション 16
継続的な学習と改善 16
メトリクスと説明責任 16
セクション概要 16
段階的アプローチ 18
フェーズ 1: 評価と計画 18
フェーズ 2: 試験運用と実装 19
フェーズ 3: モニタリングと継続的改善 19
セクション概要 20
ベストプラクティス 21
重要なポイント 24
次のステップ 26
よくある質問 27
ゼロトラストとは? 27
ゼロトラストアーキテクチャの実装 AWS のサービス に役立つものは何ですか? 27
でデータセキュリティを確保するにはどうすればよいですか AWS? 27
ゼロトラスト環境でコンプライアンス要件 AWS に対応できますか? 27
ゼロトラスト環境でセキュリティを自動化するための AWS ツールやサービスはありますか? 28
を使用してゼロトラストクラウド環境で継続的なモニタリングとインシデント対応を確保する方法 AWS 28
リソース 29
リファレンス 29
ツール 29
ドキュメント履歴 31
..... xxxii

ゼロトラストの導入: 安全かつ機敏なビジネス変革戦略のための戦略

Greg Gooden (Amazon Web Services (AWS))

2023 年 12 月 (ドキュメント履歴)

今日、組織はこれまで以上にセキュリティを重要な優先事項として重視しています。これにより、顧客の信頼の維持から、従業員のモビリティの向上、新しいデジタルビジネス機会の開拓まで、幅広いメリットが得られます。その際、「システムとデータに適切なレベルのセキュリティと可用性を確保するための最適なパターンは何か？」という古くからの質問が次から次へと出てきます。ゼロトラストが、この質問に対する答えを表すのに使われる最新の用語になってきています。

ゼロトラストアーキテクチャ (ZTA) は、従来のネットワーク制御やネットワーク境界だけに依存しない、またはそれに根本的に依存しない、デジタル資産に関するセキュリティ制御を提供することに焦点を当てた概念モデルおよび、関連する一連のメカニズムです。代わりに、ID、デバイス、動作、その他の豊富なコンテキストやシグナルをネットワーク制御に追加して、よりきめ細かく、インテリジェントで、適応性が高く、継続的なアクセスに関する意思決定を行います。ZTA モデルを実装することで、サイバーセキュリティ、特に多層防御の概念が継続的に成熟する中で、次の段階において有意義な成果を上げることができます。

意思決定プロセス

ZTA 戦略を実施するには、慎重な計画と意思決定が必要です。これには、さまざまな要素を評価し、組織の目標と整合させることが含まれます。ZTA の取り組みに着手するための主な意思決定プロセスには以下が含まれます。

1. 利害関係者の関与 — 他の経営幹部、バイスプレジデント、上級管理職と連携して、組織のセキュリティ態勢に関する優先事項、懸案事項、ビジョンを理解してもらうことが重要です。主要な利害関係者を最初から関与させることで、ZTA の導入を全体的な戦略的目標に合わせることができ、必要なサポートやリソースを獲得できます。
2. リスク評価 — 包括的なリスク評価を実施することで、問題、過剰な露出、重要な資産を特定できます。これによりセキュリティ制御と投資について情報に基づいた決定を下すことができます。業界や運用環境に固有のリスク状況に基づいて、組織の既存のセキュリティ態勢を評価し、潜在的な弱点を特定し、改善すべき分野に優先順位を付けます。

3. 技術評価 — 組織の既存の技術状況を評価し、ギャップを特定することは、ZTA の原則に沿った適切なツールやソリューションを選択するのに役立ちます。この評価には、以下の項目を綿密に分析する必要があります。
   - ネットワークアーキテクチャ
   - アイデンティティとアクセス管理システム
   - 認証と認可のメカニズム
   - 統合エンドポイント管理
   - リソース所有ツールとプロセス
   - 暗号化技術
   - モニタリングとログ記録の機能
   - 堅牢な ZTA モデルを構築するには、適切なテクノロジースタックを選択することが欠かせません。
4. 変更管理 — ZTA モデルを採用することによる文化的および組織的な影響を認識することは不可欠です。変更管理のプラクティスを導入することで、組織全体での移行と承認が円滑になります。これには、ZTA の原則と利点に関する従業員の教育、新しいセキュリティ慣行に関するトレーニングの提供、アカウンタビリティと継続的な学習を奨励するセキュリティ意識の文化の促進が含まれます。

この規範的なガイダンスは、経営幹部、バイスプレジデント、上級管理職に ZTA を導入するための包括的な戦略を提供することを目的としています。以下を含む ZTA の主要な側面について掘り下げて説明します。

- 組織の準備状況
- 段階的導入アプローチ
- 利害関係者の協力
- 安全かつ機敏なビジネス変革を実現するためのベストプラクティス

このガイダンスに従うことで、組織は ZTA ランドスケープをナビゲートし、Amazon Web Services (AWS) クラウドのセキュリティジャーニーを成功させることができます。 AWS は、 AWS Verified Access、 AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway、Amazon GuardDuty など、ZTA の実装に使用できるさまざまなサービスを提供します。これらのサービスは、不正アクセスから AWS リソースを保護するのに役立ちます。

ターゲットを絞ったビジネス成果

このセクションでは、組織全体でのゼロトラストアーキテクチャの定義と実装に関連して期待される成果について説明します。

セキュリティ態勢の強化

ゼロトラストの原則を採用することで、組織はセキュリティ体制を強化し、セキュリティリスクを軽減し、クラウドインフラストラクチャとデータを保護することができます。知る必要性に応じてアクセス権を付与するというゼロトラストの基本原則は、厳格な管理と相まって、露出を大幅に削減し、セキュリティイベントの潜在的な影響を制限します。このプロアクティブなアプローチにより、組織は新たなセキュリティリスクに先んじて、資産の機密性、整合性、可用性を達成することができます。

シームレスなクラウドの採用

明確に定義されたゼロトラストアーキテクチャ (ZTA) 導入計画を策定することで、クラウド環境への移行を円滑に成功させることができます。ZTA の原則は、組織がクラウドコンピューティングのメリットを安全に享受するための強固な基盤を提供するという点で、クラウドセキュリティのベストプラクティスと密接に一致しています。ZTA の原則を最初から組み込むことで、組織はセキュリティを中核要素とするクラウドアーキテクチャを設計しやすくなります。

コンプライアンスと規制の調整

ZTA プラクティスを導入することで、組織は業界や規制の要件や基準を満たすことができます。ZTA は本質的に最小特権の原則を推進し、厳格なアクセス制御を実施しています。アクセス制御は、多くの場合、次のような規制によって義務付けられています。

- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)。

ゼロトラストを採用することで、組織は罰則や風評被害を受ける可能性を最小限に抑えながら、データ保護、プライバシー、規制順守への取り組みを実証することができます。

データ保護の強化

組織は、データ暗号化、アクセス制御、定期的なセキュリティ評価を実施することで、クラウド導入プロセス全体を通じて機密データを保護できます。組織では次のような具体的な対策を講じることができます。

- データ暗号化 — データ暗号化 — データ暗号化は、クリアテキストデータを暗号文に暗号化するプロセスで、データを復号化して元のクリアテキスト形式に戻すには鍵が必要です。これにより、たとえ権限のない個人がデータのコピーを入手できたとしても、機密データにアクセスすることがはるかに困難になります。
- アクセス制御 — アクセス制御は、機密データにアクセスできるユーザーと、そのデータを使ってできることを制限します。これは、ユーザーの役割とアクセス許可を割り当て、多要素認証やその他の方法を使用してユーザー ID を確認することで実現できます。
- 定期的なセキュリティ評価 — 定期的なセキュリティ評価により、組織はセキュリティ問題を特定して対処し、事前に修正することができます。これらの評価は、社内のセキュリティチームまたは外部のセキュリティ会社によって実施されます。

ゼロトラストアーキテクチャは、さまざまなセキュリティ対策を実施することにより、データ保護に包括的なアプローチを取ります。これらの対策には、強力な認証、データ暗号化、きめ細かなアクセス制御が含まれます。このアプローチは、データ関連のセキュリティイベントのリスクを最小限に抑え、機密情報を不正アクセスから保護します。

効率的なインシデント対応

組織は、クラウド環境で監視とインシデント対応のフレームワークを確立することで、セキュリティイベントをより迅速かつ効果的に検出して対応できます。ゼロトラストアーキテクチャは、継続的な監視、脅威インテリジェンスの統合、ユーザーアクティビティ、ネットワークトラフィック、システム動作のリアルタイムの可視化に重点を置いています。そうすると、セキュリティチームはセキュリティイベントを事前に特定して軽減できます。このアプローチは、潜在的な問題の検出と対応にかかる時間を短縮し、事業運営への影響を最小限に抑えます。主な特徴は次のとおりです。

- テスト — 組織が採用しているインシデント対応のフレームワークや方法論にかかわらず、インシデント対応計画を定期的にテストする必要があります。テーブルトップ演習、シミュレーション、レッドチーム編成によって、現実的な設定でインシデント対応を実践し、ツールや能力のギャップを明らかにし、インシデント対応担当者の経験と自信を高めることができます。

- 監視 — クラウド環境に異常なアクティビティの兆候がないか継続的に監視します。これには、ログ分析、ネットワーク監視、脆弱性スキャンなど、さまざまなツールや手法を利用します。
- 脅威インテリジェンスの統合 — 脅威インテリジェンスを、監視およびインシデント対応のフレームワークに統合します。これにより、組織は脅威をより迅速かつ効果的に特定して対応できるようになります。
- リアルタイムの可視性 — セキュリティインシデントを迅速に特定して対応するには、ユーザーのアクティビティ、ネットワークトラフィック、システム動作をリアルタイムで可視化する必要があります。
- 事前の特定と軽減 — セキュリティイベントを事前に特定して軽減することで、潜在的な脅威の検出と対応にかかる時間を短縮し、事業運営への影響を最小限に抑えることができます。

従業員の生産性向上

現代の従業員には、ますます多様化する場所、デバイス、時間帯から仕事をこなせる柔軟性が求められます。ZTA を導入することで、組織のセキュリティ態勢を維持または改善しながら、これらの要件に対応し、従業員のモビリティ、生産性、満足度を向上させることができます。

デジタルトランスフォーメーションの活用

組織にとって、デジタルトランスフォーメーションの一環として、従来のネットワーク境界の外にあるデバイス、マシン、施設、インフラストラクチャ、プロセスの相互接続の必要性が増しています。モノのインターネット (IoT) やオペレーショナルテクノロジー (OT、産業用モノのインターネット (IIoT) とも呼ばれる) デバイスは、遠隔測定情報や予知保全情報をクラウドに直接送信することがよくあります。ワークロードを保護するには、従来の境界アプローチを超えるセキュリティ制御を適用する必要があります。

セクション概要

こうしたターゲットを絞ったビジネス成果に焦点を当てることで、組織は ZTA の可能性を最大限に引き出し、クラウドにおけるセキュリティ態勢を強化することができます。これらの成果を特定の組織の目標と整合させ、独自のビジネス要件に合わせて調整し、その有効性を定期的に評価して継続的な改善を推進することが重要です。

ゼロトラストの原則を理解する

ゼロトラストアーキテクチャ (ZTA) は、セキュリティモデルの基礎となる一連の中核となる原則に基づいています。これらの原則を理解することは、ZTA 戦略を効果的に採用しようとしている組織にとって不可欠です。このセクションでは、ZTA の中核的原則について説明します。

検証と認証

検証と認証の原則は、ユーザー、マシン、デバイスを含むあらゆるタイプのプリンシパルの強力な識別と認証の重要性を強調しています。ZTA では、セッション中、ID と認証ステータスを継続的に検証する必要があります。理想的には、リクエストごとに行われることが期待されます。それは、従来のネットワークの位置や制御だけに頼るものではありません。これには、最新の強力な多要素認証 (MFA) の実装や、認証プロセス中の追加の環境信号やコンテキスト信号の評価が含まれます。この原則を採用することで、組織はリソース承認の決定に可能な限り最高の ID インプットが反映されるようにすることができます。

最小特権アクセス

最小特権の原則では、プリンシパルにタスクの実行に必要な最低限のアクセスを付与します。最小特権アクセスの原則を採用することで、組織はきめ細かなアクセス制御を実施し、プリンシパルがそれぞれの役割と責任を果たすために必要なリソースにのみアクセスできるようにすることができます。これには、ジャストインタイムのアクセスプロビジョニング、ロールベースのアクセス制御 (RBAC)、定期的なアクセスレビューを実施して、露出と不正アクセスのリスクを最小限に抑えることが含まれます。

マイクロセグメンテーション

マイクロセグメンテーションは、特定のトラフィックフローを許可するために、ネットワークをより小さな独立したセグメントに分割するネットワークセキュリティ戦略です。ワークロードの境界を作り、異なるセグメント間で厳格なアクセス制御を実施することで、マイクロセグメンテーションを実現できます。

マイクロセグメンテーションは、ネットワーク仮想化、Software-Defined Networking (SDN)、ホストベースのファイアウォール、ネットワークアクセスコントロールリスト (NACLs)、および Amazon Elastic Compute Cloud (Amazon EC2) セキュリティグループや などの AWS 特定の機能を

通じて実装できます AWS PrivateLink。セグメンテーションゲートウェイは、セグメント間のトラフィックを制御してアクセスを明示的に許可します。マイクロセグメンテーションとセグメンテーションゲートウェイは、組織がネットワークを経由する不要な経路、特に重要なシステムやデータにつながる経路を制限するのに役立ちます。

継続的なモニタリングと分析

継続的なモニタリングと分析には、組織の環境全体にわたるセキュリティ関連のイベントとデータの収集、分析、相関関係が含まれます。堅牢なモニタリングツールと分析ツールを導入することで、組織はセキュリティデータとテレメトリを一元的に評価できます。

この原則は、異常や潜在的なセキュリティイベントを特定するために、ユーザーの行動、ネットワークトラフィック、システムアクティビティを可視化することの重要性を強調しています。セキュリティ情報およびイベント管理 (SIEM)、ユーザーおよびエンティティ行動分析 (UEBA)、脅威インテリジェンスプラットフォームなどの高度なテクノロジーは、継続的なモニタリグと予防的な脅威検出を実現する上で重要な役割を果たします。

自動化とオーケストレーション

自動化とオーケストレーションは、組織がセキュリティプロセスを合理化し、手作業による介入を減らし、応答時間を短縮するのに役立ちます。日常的なセキュリティタスクを自動化し、オーケストレーション機能を使用することで、組織は一貫したセキュリティポリシーを実施し、セキュリティイベントに迅速に対応できます。この原則には、ユーザー権限を適時かつ正確に管理できるように、アクセスのプロビジョニングとプロビジョニング解除のプロセスを自動化することも含まれます。自動化とオーケストレーションを取り入れることで、組織は業務効率を高め、人的ミスを減らし、より戦略的なセキュリティイニシアチブにリソースを集中させることができます。

Authorization

ZTA では、リソースへのアクセスを求める各リクエストは、ゲーティング適用ポイントによって明示的に承認される必要があります。認証された ID に加えて、認可ポリシーでは、デバイスの状態と態勢、動作パターン、リソース分類、ネットワーク要因などの追加のコンテキストを考慮する必要があります。承認プロセスでは、この集中型コンテキストを、アクセスされているリソースに関連する対応するアクセスポリシーと照らし合わせて評価する必要があります。機械学習モデルで宣言型ポリシーを動的に補完できることが望ましいです。これらのモデルを使用する場合は、追加の制限のみに重点を置いてください。明示的に指定されていないアクセス権を付与すべきではありません。

セクション概要

ZTA のこれらの中核的原則を順守することで、組織は現代の企業環境の多様性に対応する強固なセキュリティモデルを確立できます。これらの原則を実装するには、テクノロジー、プロセス、人材を組み合わせた包括的なアプローチでゼロトラストの考え方を実現し、レジリエントなセキュリティ態勢を構築する必要があります。

ゼロトラストアーキテクチャの主要コンポーネント

ゼロトラストアーキテクチャ (ZTA) 戦略を効果的に実装するには、組織が ZTA を構成する主要なコンポーネントを理解する必要があります。これらのコンポーネントは連携して、ゼロトラストの原則に沿った包括的なセキュリティモデルを確立します。このセクションでは、ZTA の主要コンポーネントについて説明します。

ID とアクセス管理

アイデンティティとアクセス管理は、強固なユーザー認証と大まかなアクセス制御メカニズムを提供することで ZTA の基盤を形成します。これには、シングルサインオン (SSO)、多要素認証 (MFA)、および ID ガバナンスと管理ソリューションなどのテクノロジーが含まれます。アイデンティティとアクセス管理は、ゼロトラストの認可決定を行うために不可欠な、高いレベルの認証保証と重要なコンテキストを提供します。同時に、ZTA は、ユーザーごと、デバイスごと、セッションごとにアプリケーションやリソースへのアクセスが許可されるセキュリティモデルでもあります。これにより、ユーザーの認証情報が漏えいした場合でも、組織を不正アクセスから守ることができます。

セキュアアクセスサービスエッジ

セキュアアクセスサービスエッジ (SASE) は、ネットワークとセキュリティの機能を仮想化、結合、分散して、単一のクラウドベースのサービスにする、ネットワークセキュリティへの新しいアプローチです。SASE は、ユーザーの場所に関係なく、アプリケーションやリソースへの安全なアクセスを提供します。

SASE には、セキュアウェブゲートウェイ、サービスとしてのファイアウォール、ゼロトラストネットワークアクセス (ZTNA) など、さまざまなセキュリティ機能が含まれています。これらの機能が連携して、マルウェア、フィッシング、ランサムウェアなどのさまざまな脅威から組織を保護します。

データ損失防止

データ損失防止 (DLP) テクノロジーは、組織が機密データを不正開示から保護するのに役立ちます。DLP ソリューションは、移動中および保管中のデータをモニタリングおよび制御します。これにより、組織はデータ関連のセキュリティイベントを防止するポリシーを定義して適用できるようになり、機密情報をネットワーク全体で確実に保護できるようになります。

Security Information and Event Management

Security Information and Event Management (SIEM) ソリューションは、組織のインフラストラクチャ全体のさまざまなソースからセキュリティイベントログを収集、集約、分析します。このデータを使用して、セキュリティインシデントの検出、インシデント対応の促進、潜在的な脅威や脆弱性に関するインサイトの提供を行うことができます。

特に ZTA にとって、さまざまなセキュリティシステムからの関連するテレメトリを相互に関連付けて理解する SIEM ソリューションの機能は、異常パターンの検出と対応を向上するために重要です。

エンタープライズリソース所有権カタログ

エンタープライズリソースへのアクセスを適切に許可するには、組織はこれらのリソースおよび、重要なこととしては、その所有者をカタログ化する信頼できるシステムを必要とします。この信頼できる情報源は、アクセス要求、関連する承認決定、およびそれらの定期的な証明を容易にするワークフローを備えている必要があります。やがて、この信頼できる情報源には、組織内において「誰が何にアクセスできるのか」という答えが含まれることになります。その回答を、承認と監査、コンプライアンスの両方に使用できます。

統合エンドポイント管理

ZTA は、ユーザーを強力に認証するだけでなく、ユーザーのデバイスのヘルス、態勢、状態も考慮して、企業データとリソースへのアクセスが安全かどうかを評価する必要があります。統合エンドポイント管理 (UEM) プラットフォームには以下の機能があります。

- デバイスプロビジョニング
- 継続的な構成とパッチ管理
- セキュリティのベースライン
- テレメトリレポート
- デバイスのクレンジングと使用終了

ポリシーベースの適用ポイント

ZTA では、各リソースへのアクセスは、ゲーティングポリシーベースの適用ポイントによって明示的に許可される必要があります。最初は、これらの適用ポイントを、既存のネットワークや ID システム内の既存の適用ポイントに基づいて設定してもかまいません。ZTA が提供する幅広いコンテキ

ストとシグナルを考慮することで、適用ポイントの機能を段階的に高めることができます。長期的には、統合コンテキストに基づいて運用され、シグナルプロバイダーを一貫して統合し、包括的なポリシーセットを維持し、テレメトリを組み合わせて収集した情報で強化される、ZTA 固有の適用ポイントを組織に導入する必要があります。

セクション概要

これらの主要要素を理解することは、ZTA の採用を計画している組織にとって不可欠です。これらのコンポーネントを実装し、まとまりのあるセキュリティモデルに統合することで、組織はゼロトラストの原則に基づいた強力なセキュリティ態勢を確立できます。以下のセクションでは、組織内での ZTA の導入を成功させるのに役立つ、組織の準備状況、段階的導入アプローチ、ベストプラクティスについて説明します。

ゼロトラスト導入に向けた組織の準備状況の評価

新しいアーキテクチャ戦略を採用することは、慎重な計画と組織の要因の検討を必要とする重要な作業です。このセクションでは、全社でゼロトラストを採用するための組織の準備状況に関する重要な考慮事項に焦点を当てます。これらの考慮事項に取り組むことで、組織はより強力で効果的なセキュリティ対策への道を開くことができます。

リーダーシップの連携とコミュニケーション

ゼロトラストをうまく実施するには、リーダーシップの連携とコミュニケーションが不可欠です。リーダーは、ゼロトラストの利点と必要なリソースを理解する必要があります。また、リーダーは組織の文化やプロセスを積極的に変えていかなければなりません。信頼を築き、賛同してもらうには、従業員とのコミュニケーションが不可欠です。従業員は、なぜ組織がゼロトラストを導入しているのか、それが彼らにとって何を意味するのか、どのように協力できるのかを理解する必要があります。コミュニケーションはオープンで、透明性があり、継続的である必要があります。

リーダーシップの支援と賛同

ゼロトラストアーキテクチャ (ZTA) の導入を成功させるには、アーキテクチャの目標、メリット、成功の尺度について、主要な利害関係者と経営陣の足並みを揃えることが重要です。従来の境界ベースのセキュリティから、よりきめ細かなユーザー中心のアプローチに移行することで、セキュリティを強化し、ビジネスの俊敏性を実現する上で、ゼロトラスト原則の重要性を共有します。このアプローチに切り替えることで、組織は変化や脅威により迅速に適応できます。経営陣が連携することで、組織の雰囲気を整え、変化に対する潜在的な抵抗を克服することができます。

透明性の高いコミュニケーション

ゼロトラストの導入プロセス全体を通じて、従業員とのオープンで透明なコミュニケーションを維持します。導入の根拠、利点、期待される結果を説明し、懸念事項に迅速に対処します。実施の進捗状況を定期的に更新します。これにより、賛同が増え、抵抗が減り、信頼が築かれます。

スキル開発とトレーニング

リーダーが足並みを揃え、コミュニケーションがオープンになったら、ゼロトラストを導入する従業員がスキルと知識を身に付けることが重要です。これには、ゼロトラストの原則の理解、業務への実装方法、セキュリティイベントへの対応方法などが含まれます。従業員がこれらのスキルを習得できるように、トレーニングと能力開発の機会を提供してください。

クラウドに関する知識とスキル

クラウドテクノロジーとゼロトラストの原則に関する組織のスキルと知識のギャップを評価します。従業員のスキルを向上させ、クラウド中心のゼロトラスト環境で効果的に働くために必要な専門知識を身に付けるためのトレーニングと能力開発プログラムを提供します。進化するテクノロジーやセキュリティ慣行に遅れずについていくために、継続的な学習の文化を育んでください。

セキュリティ文化と意識

組織のセキュリティ文化を評価します。従業員のセキュリティ意識のレベル、セキュリティのベストプラクティスに対する理解、ポリシーと手順の順守状況を評価します。セキュリティに関する知識のギャップを特定します。ゼロトラストの重要性と安全な環境を維持する上での役割について従業員を教育するために、セキュリティ意識向上トレーニングプログラムの実施を検討してください。

組織構造と役割

ゼロトラストの実装を成功させるために、効果的な組織構造と役割を確立します。これには、Cloud Center of Excellence (CCoE) の設立、セキュリティ運用のレビューと変更、脆弱性管理、インシデント対応、セキュリティモニタリングの役割と責任の割り当てが含まれます。

Cloud Center of Excellence

CCoE を確立して、クラウド運用のガイダンス、ベストプラクティス、監督を行います。CCoE は、クラウド関連のベストプラクティス、ガイドライン、ガバナンスポリシーの作成と実施を担当するチームまたは個人のグループです。CCoE にさまざまな事業部門や IT チームの代表者が参加して、コラボレーションと連携を確保します。CCoE は、クラウドホスト型のワークロードへのゼロトラストの原則の導入を促進する上で重要な役割を果たします。組織全体での知識共有を促進するのも、CCoE の役割です。

セキュリティオペレーション

ゼロトラスト環境のニーズを満たすには、現在のセキュリティ運用組織を見直し、修正します。モニタリング、インシデント対応、脅威インテリジェンス機能を向上させるには、セキュリティオペレーションセンター (SOC) またはマネージドセキュリティサービスプロバイダー (MSSP) の導入を検討してください。脆弱性管理、インシデント対応、セキュリティモニタリングの役割と責任を確立してください。軽微なセキュリティイベントを迅速に検出して修正し、一連のイベントを中断させるには、インシデント対応プロセスを適切に機能させることが不可欠です。これにより、軽微なイベントがより影響の大きいイベントに発展するのを防ぐことができます。

IT インフラストラクチャとアーキテクチャ

自社の IT アーキテクチャとインフラストラクチャを調べて、ゼロトラストアプローチの導入に影響する可能性のある制約や依存関係がないか調べます。現在のアプリケーションやシステムが、必要なゼロトラストアーキテクチャコンポーネントと互換性があるかどうかを判断します。ゼロトラスト原則の導入を成功させるためには、インフラストラクチャの改善や調整が必要かどうかを分析します。アプリケーションまたはシステムごとに、ゼロトラストを現場で実装するのが最適なのか、それとも大規模なモダナイズ努力によって実装するのが最善なのかを検討してください。

リスク管理、ガバナンス、変更管理

ゼロトラストの実装を成功させるために、効果的なリスク管理、ガバナンス、変更管理のプロセスを確立します。これには、リスク管理とゼロトラスト原則との連携、インシデント対応計画の策定、法務部門やコンプライアンス部門との協力、変更管理プロセスの確立などが含まれます。

リスク管理

自社で実施されているリスク管理戦略を調べ、それがゼロトラストの原則にどの程度準拠しているかを判断してください。現在のインシデント対応システム、セキュリティ対策、リスク評価手順の効率性を分析します。ゼロトラスト戦略に準拠するために改善が必要な分野を特定します。解決までの時間を短縮するために、自動インシデント対応システムまたは継続的なモニタリングと分析のフレームワークの開発に取りかかってください。

変更管理プロセス

クラウド関連のすべての変更がセキュリティとコンプライアンスの要件を満たすようにするために、効果的な変更管理方法を確立します。セキュリティ構成分析、リスク評価、承認、文書化を含む体系的な変更管理手順を確立します。ゼロトラストアーキテクチャの完全性を維持するために、更新を頻繁に確認して監査してください。

モニタリングと評価

ゼロトラストの実装を成功させるには、組織はセキュリティ体制を継続的にモニタリングし、評価する必要があります。これには、重要業績評価指標 (KPI) の確立、KPI のモニタリングと評価、継続的改善の文化の促進が含まれます。これらのステップに従うことで、組織はゼロトラストの実施を成功させ、常にセキュリティの向上に取り組んでいることを確認できます。

重要業績評価指標

適切な重要業績評価指標 (KPI) を確立して、ゼロトラスト導入の成功と有効性を評価します。これらの KPI により、ユーザー満足度、設備と展開の進捗状況、コスト削減、コンプライアンス順守、セキュリティ手段の発生回数を測定する場合があります。全体的な開発状況を把握し、改善の機会を見つけるために、これらの KPI を定期的にモニタリングして評価します。

継続的な改善

ステークホルダーから意見やインサイトを引き出すシステムを確立することで、継続的な改善の文化を育むことができます。クラウド環境のセキュリティ、有効性、ユーザーエクスペリエンスを改善するための考えや提案を共有するよう、スタッフに促します。この意見を手順の効率化、セキュリティ対策の改善、イノベーションの促進に役立ててください。

セクション概要

このような組織的および文化的な考慮事項に対処することで、組織はゼロトラストのセキュリティモデルのクラウド導入を支援する環境を促進できます。次のセクションでは、段階的な導入アプローチを検討し、ゼロトラストの原則を実用的かつ管理しやすい方法で徐々に実装する方法についてのガイダンスを提供します。

ゼロトラストの考え方を育む

ゼロトラストの実装は、技術的な実装にとどまりません。これには、組織内の文化的な変化が必要です。ゼロトラストの考え方を育むには、以下の重要な側面を強調する必要があります。

ゼロトラストの教育とトレーニング

ゼロトラストアーキテクチャ (ZTA) の価値と利点について従業員を教育します。トレーニングセッション、ワークショップ、その他のリソースを通じて、ZTA の概念とアプローチの技術的および非技術的な説明を行います。スタッフがゼロトラストセキュリティパラダイムの確立と維持における自らの責任を認識するよう促します。

協力とコミュニケーション

ZTA の実装にかかわるすべてのチームや部門で、協力と透明性を促進します。全員が計画を十分に理解できるように、部門横断的なコミュニケーション、知識共有、情報交換を推進します。ビジネス全体のセキュリティに対する自らの貢献の重要性を全員が認識する、責任共有の文化を育成します。

継続的な学習と改善

ゼロトラストの取り組みにおいて、継続的な学習と改善を優先します。従業員が最新のセキュリティ動向、テクノロジー、ベストプラクティスを常に把握し続けるよう促します。イノベーションと実践の文化を育み、従業員が組織のセキュリティ体制を強化するための新しいソリューションとアプローチを探求できるようにします。

メトリクスと説明責任

ゼロトラスト戦略の有効性を測定するための明確なメトリクスと説明責任のメカニズムを確立します。組織のセキュリティ目標に沿った主要業績評価指標 (KPI) を定義し、定期的に進捗状況を追跡します。ゼロトラストの原則を実装および維持する上での貢献に対して、個人とチームが責任を持つようにします。

セクション概要

これらの側面に対処し、ゼロトラストの考え方を育むことで、組織はゼロトラストの導入と実装を成功させるための強固な基盤を構築できます。この文化的変化は、組織内のすべての人がゼロトラストの重要性を理解し、その成功に積極的に貢献するために不可欠です。

次のセクションでは、段階的な導入アプローチを検討し、ゼロトラストの原則を実用的かつ管理しやすい方法で徐々に実装する方法についてのガイダンスを提供します。

ゼロトラストへの段階的アプローチ

ゼロトラストアーキテクチャ (ZTA) を採用するには、慎重な計画と実装が必要です。移行を円滑に進め、事業運営の中断を最小限に抑えるために、段階的な導入アプローチをお勧めします。このセクションでは、ZTA の採用に関わる主な段階に関するガイダンスを提供します。

フェーズ 1: 評価と計画

ゼロトラスト導入の最初のフェーズは、評価と計画です。このフェーズは、組織の現在のセキュリティ体制におけるギャップを特定して対処する必要があるため、導入全体を成功させるために不可欠です。時間をかけて現在の状態を評価し、セキュリティ目標を定義することで、ゼロトラスト導入を成功させるための基礎を築くことができます。

同時に、完全で正確な評価が現実的ではない場合もあります。分析が停滞して次のフェーズに進めなくなることがないように、区分化の準備をするか、ある程度の不完全さを受け入れてください。

1. 現在の状態の評価 — 既存のセキュリティインフラストラクチャ、ポリシー、統制を評価してください。潜在的な脆弱性、セキュリティ上のギャップ、ゼロトラスト原則の導入によって改善が見込める分野を特定します。
2. セキュリティ目標の定義 — 現在の状況の評価結果に基づいて、ゼロトラストの原則に沿ったセキュリティ目標を定義します。これらのセキュリティ目標は、組織の全体的なセキュリティ戦略と一致するものであり、特定された脆弱性やギャップに対処できるものである必要もあります。
3. アーキテクチャの設計 — 組織のセキュリティ目標をサポートする ZTA を開発します。このアーキテクチャには、ID およびアクセス管理ソリューション、ネットワークセグメンテーションメカニズム、継続的監視システムなど、必要なコンポーネントが含まれている必要があります。また、アーキテクチャはスケーラブルで適応性があり、将来の成長や技術の進歩に対応できるものでなければなりません。このアーキテクチャは、単なる文書や図としてではなく、AWS CloudFormation テンプレートなど、実装を担当するチームが使いやすい形式で表現されることが望ましいです。
4. 利害関係者の関与 — 事業部門、IT チーム、セキュリティチームを含むすべての利害関係者を関与させ、洞察を得て、目標を ZTA 実装計画と一致させます。ゼロトラストアプローチの利点と要件について共通の理解を確立するために、コラボレーションとコミュニケーションを奨励します。

フェーズ 2: 試験運用と実装

ゼロトラスト導入の第 2 フェーズは、試験運用と実装です。このフェーズでは、小規模で制御された環境で ZTA をテストし、組織全体に繰り返し展開します。新しいセキュリティ対策と、ゼロトラスト環境を維持する上での各自の役割について、従業員を教育することが重要です。

1. 導入の試験運用 — 小規模で制御された環境で ZTA をテストします。アーキテクチャ設計段階で定義した必要なコンポーネントとセキュリティ制御を実装します。パイロット展開を注意深く監視し、フィードバックを収集し、必要な調整を行います。ゼロトラストが架空の演習から実際の体験を構築する演習に移行する段階で、プロセスの早い段階で柔軟に対応できるように準備してください。
2. 反復的な導入 — パイロット展開から学んだ教訓に基づいて、ゼロトラストの組織全体への反復的な導入を開始してください。フライホイール効果で勢いをつけましょう。大規模なキャンペーンを行わなくても、クリティカルな大規模展開を実現できます。リーダーシップの委任やエスカレーションは、ロールアウトの長期化によって必要になる可能性がある場合に取っておきます。
3. ユーザートレーニングの提供と意識向上 — 新しいセキュリティ対策と、ゼロトラスト環境を維持する上での各自の役割について従業員を教育します。強固なパスワード、多要素認証、定期的なセキュリティアップデートなど、セキュリティ対策の重要性を強調してください。
4. 変更管理 — ゼロトラストの導入に伴う組織的および文化的な変化に対応するための包括的な変更管理計画を作成します。導入の背景にある利点と理論的根拠を従業員に伝え、懸念事項や抵抗があれば対処します。円滑な移行を促進するため、継続的なサポートとガイダンスを提供してください。

フェーズ 3: モニタリングと継続的改善

ゼロトラスト導入の最終となる第 3 フェーズは、モニタリングと継続的改善です。このフェーズでは、包括的な監視および分析プログラムの確立、包括的なインシデント対応計画の作成、ステークホルダーやユーザーからの定期的なフィードバックの募集を行います。

1. 継続的な監視 — セキュリティ状況を継続的に評価し、潜在的な異常を検出するための包括的な監視および分析プログラムを確立します。高度なセキュリティツールとテクノロジーを使用して、ユーザーの行動、ネットワークトラフィック、システムアクティビティを監視します。
2. インシデント対応と修復の計画 — ゼロトラストの原則に沿った包括的なインシデント対応計画を作成します。明確なエスカレーションパスを確立し、役割と責任を定義し、可能な場合は自動インシデント対応メカニズムを実装します。インシデント対応計画への定期的なテストと更新を行います。

3. フィードバックと評価の取得 — 利害関係者やユーザーから定期的にフィードバックを募り、ゼロトラストアーキテクチャ (ZTA) の有効性に関する洞察を集めます。定期的な評価を実施して、セキュリティ体制、運用効率、ユーザーエクスペリエンスへの影響を測定します。フィードバックと評価結果を利用して、改善すべき分野を特定します。ZTA は時間の経過とともに変化することを想定し、開発チームが最小限の労力や中断でこれらの更新を実装する方法を検討してください。

セクション概要

この段階的な導入アプローチに従うことで、組織はリスクと混乱を最小限に抑えながら、ZTA に効果的に移行できます。次のセクションでは、ゼロトラストの導入を成功させるためのベストプラクティスについて、経営幹部、バイスプレジデント、上級管理職向けの重要な考慮事項と推奨事項について説明します。

ゼロトラストで成功を収めるためのベストプラクティス

ゼロトラストアーキテクチャ (ZTA) の導入を成功させるには、戦略的アプローチとベストプラクティスの順守が必要です。このセクションでは、経営幹部、バイスプレジデント、上級管理職がゼロトラストの導入を成功に導くための一連のベストプラクティスを紹介します。以下の推奨事項に従うことで、組織は強固なセキュリティ基盤を確立し、ゼロトラストアプローチのメリットを実感できます。

- 明確な目標とビジネス成果の定義 — クラウド運用の目標と期待されるビジネス成果を明確に定義します。これらの目標をゼロトラストの原則と一致させて、強固なセキュリティ基盤を構築すると同時に、ビジネスの成長と革新を可能にします。
- 包括的な評価の実施 — 現在の IT インフラストラクチャ、アプリケーション、データ資産を総合的に評価します。依存関係、技術的負債、潜在的な互換性問題を特定します。この評価は導入計画に反映され、重要度、複雑さ、ビジネスへの影響に基づいてワークロードに優先順位を付けるのに役立ちます。
- 導入計画の策定 — ワークロード、アプリケーション、データをクラウドに移行するための段階的なアプローチを概説した詳細な導入計画を組み込みます。導入フェーズ、スケジュール、依存関係を定義します。主要な利害関係者を関与させ、それに応じてリソースを割り当てます。
- 早期に構築を始める — ゼロトラストが組織内でどのようなものになるかを真に表す能力は、(分析して話し合うよりも) ゼロトラストの構築と展開を開始した後に大幅に向上します。
- 経営幹部の後援を得る — ゼロトラストの導入に向けて、経営幹部の後援とサポートを確保しましょう。他の経営幹部の協力を得てイニシアチブを支持し、必要なリソースを割り当てます。実施を成功させるために必要な文化や組織の変革を推進するには、リーダーシップのコミットメントが不可欠です。
- ガバナンスフレームワークの実装 — ゼロトラスト導入の役割、責任、意思決定プロセスを定義するガバナンスのフレームワークを作成します。セキュリティコントロール、リスク管理、コンプライアンスに関する説明責任と所有権を明確に定義します。変化するセキュリティ要件に適応できるよう、ガバナンスのフレームワークを定期的に見直し、更新します。
- 部門間のコラボレーションのサポート — 異なる事業部門、IT チーム、セキュリティチーム間のコラボレーションとコミュニケーションを促進します。ゼロトラストの実装全体を通じて連携と調整を促進するために、責任を共有する文化を作ります。頻繁なやり取り、知識の共有、共同での問題解決を奨励します。
- データとアプリケーションの保護 — ゼロトラストとは、エンドユーザーがリソースやアプリケーションにアクセスすることだけではありません。ゼロトラストの原則は、ワークロード内および

ワークロード間にも実装する必要があります。同じ技術原則 (強固なアイデンティティ、マイクロセグメンテーション、認可) をデータセンター内でも利用できるすべてのコンテキストを活用して適用します。

- 多層防御の提供 — 複数層のセキュリティ制御を使用して、多層防御戦略を実装します。多要素認証 (MFA)、ネットワークセグメンテーション、暗号化、異常検出などのさまざまなセキュリティテクノロジーを組み合わせて、包括的な保護を提供します。各レイヤーが他のレイヤーを補完して、強力な防御システムを構築するようにしてください。
- 強力な認証を要求 — すべてのリソースにアクセスするすべてのユーザーに、MFA などの強力な認証メカニズムを適用します。理想的には、ゼロトラストに高レベルの認証を保証し、幅広いセキュリティ上の利点 (フィッシングからの保護など) をもたらす FIDO2 ハードウェアベースのセキュリティキーなどの最新の MFA を検討してください。
- 認可の一元化と改善 — すべてのアクセス試行を個別に認可します。プロトコルの仕様によっては、接続ごとまたはリクエストごとに行う必要があります。リクエストごとが理想的です。ID、デバイス、動作、ネットワーク情報など、利用可能なすべてのコンテキストを使用して、より詳細で適応性の高い高度な承認決定を行います。
- 最小特権の原則を使用 — 最小特権の原則を実装して、職務遂行に必要な最低限のアクセス権をユーザーに付与します。職務上の役割、責任、ビジネスニーズに基づいて、アクセス許可を定期的に見直し、更新します。ジャストインタイムのアクセスプロビジョニングを実装します。
- 特権アクセス管理の使用 — 特権アクセス管理 (PAM) ソリューションを実装して、特権アカウントを保護し、重要なシステムへの不正アクセスのリスクを軽減します。PAM ソリューションには、特権アクセス制御、セッション記録、監査機能が備わっているため、組織が最も機密性の高いデータやシステムを保護しやすくなります。
- マイクロセグメンテーションの使用 — ネットワークをより小さく、より分離されたセグメントに分割します。マイクロセグメンテーションを使用して、ユーザーの役割、アプリケーション、またはデータの機密性に基づいて、セグメント間の厳格なアクセス制御を適用します。不要なネットワーク経路、特にデータにつながる経路をすべて排除するよう努めてください。
- セキュリティアラートのモニタリングと対応 — 包括的なセキュリティモニタリングとインシデント対応プログラムをクラウド環境に実装します。クラウドネイティブなセキュリティツールとサービスを使用して、脅威をリアルタイムで検出し、ログを分析し、インシデント対応を自動化します。明確なインシデント対応手順を確立し、定期的なセキュリティ評価を実施し、異常や疑わしいアクティビティを継続的にモニタリングします。
- 継続的なモニタリングの利用 — セキュリティインシデントを迅速かつ効果的に検出して対応するために、継続的なモニタンリングを実施します。高度なセキュリティ分析ツールを使用して、ユーザーの行動、ネットワークトラフィック、システムアクティビティをモニタリングします。アラートと通知を自動化して、インシデントにタイムリーに対応できるようにします。

- セキュリティとコンプライアンスの文化の促進 — セキュリティとコンプライアンスの文化を組織全体に浸透させます。セキュリティのベストプラクティス、ゼロトラストの原則を順守することの重要性、安全なクラウド環境を維持する上での従業員の役割について、従業員を教育します。定期的にセキュリティ意識向上トレーニングを実施して、従業員がソーシャルエンジニアリングに警戒し、データ保護とプライバシーに関する責任を理解するようにします。
- ソーシャルエンジニアリングシミュレーションの使用 — ソーシャルエンジニアリングシミュレーションを実施して、ソーシャルエンジニアリング攻撃に対するユーザーの感受性を評価します。シミュレーションの結果を使用して、トレーニングプログラムをユーザーの意識を高め、潜在的な脅威への対応を向上させるように調整します。
- 継続的な教育の促進 — 継続的なセキュリティトレーニングとリソースを提供することで、継続的な教育と学習の文化を確立します。進化し続けるセキュリティのベストプラクティスの情報をユーザーに提供し続けましょう。常に警戒を怠らず、疑わしいアクティビティがあれば速やかに報告するようユーザーに促してください。
- 継続的な評価と最適化 — クラウド環境の改善点を定期的に評価します。クラウドネイティブのツールを使用してリソースの使用状況とパフォーマンスをモニタリングし、脆弱性評価とペネトレーションテストを実施して弱点を特定して対処します。
- ガバナンスとコンプライアンスのフレームワークの確立 — 組織が業界標準や規制要件に準拠していることを確認するのに役立つガバナンスとコンプライアンスのフレームワークを策定します。このフレームワークでは、データやシステムを不正なアクセス、使用、開示、中断、変更、破壊から保護するためのポリシー、手順、統制を定義します。コンプライアンス指標の追跡と報告、定期的な監査の実施、コンプライアンス違反の問題への迅速な対処のためのメカニズムを実装します。
- コラボレーションと知識共有の奨励 — ZTA の採用に関わるチーム間のコラボレーションと知識共有を奨励します。これは、IT 部門、セキュリティ部門、事業部門の部門間のコミュニケーションとコラボレーションを促進することで実現できます。また、組織はフォーラム、ワークショップ、知識共有セッションを開設して、理解を促進し、課題に取り組み、導入プロセスを通じて学んだ教訓を共有することもできます。

重要なポイント

このガイドでは、ゼロトラストアーキテクチャ (ZTA) 戦略を成功させるための重要な側面について説明しました。このセクションでは、提示された規範的ガイダンスから得られた重要なポイントをまとめています。

- ゼロトラストの原則を理解する — ゼロトラストは、従来のネットワーク制御やネットワーク境界だけに依存しない、またはそれに根本的に依存しない、デジタル資産に関するセキュリティ制御を提供することに焦点を当てた概念モデルおよび、関連する一連のメカニズムです。代わりに、ID、デバイス、動作、その他の豊富なコンテキストやシグナルをネットワーク制御に追加して、よりきめ細かく、インテリジェントで、適応性が高く、継続的なアクセスに関する意思決定を行います。最小特権、マイクロセグメンテーション、継続的認証、適応型認可など、ゼロトラストの基本原則をよく理解しておいてください。
- 明確な目標の定義 — ZTA 導入の目標と期待されるビジネス成果を明確に定義します。これらの目標をゼロトラストの原則と一致させて、強固なセキュリティ基盤を確保すると同時に、ビジネスの成長と革新を可能にします。
- 包括的な評価の実施 — 既存の IT インフラストラクチャ、アプリケーション、データ資産を徹底的に評価します。依存関係、技術的負債、互換性の問題を特定して、導入戦略の参考にしてください。
- ZTA 導入計画の作成 — ワークロード、アプリケーション、データをクラウドに移行するための段階的なアプローチの概要を示す詳細な計画を作成します。コンプライアンス要件やアプリケーションのモダナイズなどの要素を検討してください。
- 強固な ZTA の実装 — きめ細かなアクセス制御、強力な認証メカニズム、継続的なモニタリングを実施する ZTA を設計して実装します。ZTA をより効率的に導入するには、AWS Verified Access や Amazon VPC Lattice などのクラウドネイティブなゼロトラストサービスを使用します。
- データとアプリケーションのセキュリティを優先する — ゼロトラストの原則 (強固なアイデンティティ、マイクロセグメンテーション、認可) を適用して、利用可能なすべてのコンテキストを提供します。このコンテキストは、システムやリソースにアクセスするユーザーや、バックエンドコンポーネント内およびバックエンドコンポーネント間の通信とデータの流れに使用してください。
- モニタリングとインシデント対応のフレームワークの確立 — 強固なセキュリティモニタリングとインシデント対応機能をクラウド環境に実装します。Amazon Inspector、AWS Security Hub CSPM、Amazon GuardDuty などのクラウドネイティブなセキュリティツールを使用して、リアルタイムの脅威検出、ログ分析、インシデント対応の自動化を行います。

- セキュリティとコンプライアンスの文化を育む — セキュリティ意識とコンプライアンスの文化を組織全体に浸透させます。セキュリティのベストプラクティスおよび、安全なクラウド環境を維持する上での従業員の役割について従業員を教育します。
- 継続的な評価と最適化 — クラウド環境、セキュリティコントロール、運用プロセスを定期的に評価します。インサイトを収集し、リソースの使用状況、コスト管理、パフォーマンスを最適化するには、Amazon CloudWatch や AWS Security Hub CSPM などのクラウドネイティブな分析およびモニタリングツールを使用してください。
- ガバナンスとコンプライアンスのフレームワークの確立 — 組織が業界標準や規制要件に準拠した、ガバナンスとコンプライアンスのフレームワークを策定します。ポリシー、手順、統制を定義して、セキュリティ、プライバシー、コンプライアンス基準を確実に順守できるようにします。

次のステップ

ゼロトラストアーキテクチャ (ZTA) の導入は、組織の態勢を改善しリスクを軽減する最も安全な方法の 1 つです。この規範的なガイダンスは、原則の理解から準備状況の評価、必要なコンポーネントの実装に至るまで、ゼロトラストを導入するための包括的なロードマップを提供しています。

このワークストリームまたはドメインにおける次のステップでは、次のことを扱います。

- 採用計画実施
- ZTA の実装
- 定期的なセキュリティ評価の実施
- クラウド環境とセキュリティ制御の継続的な最適化

ZTA は継続的なプロセスであり、強固なセキュリティ基盤を確保するための継続的なモニタリング、評価、導入を必要とします。このガイダンスに記載されているベストプラクティスに従うことで、組織はセキュリティ体制を強化し、規制を確実に順守し、機密データを保護することができます。

よくある質問

このセクションでは、ゼロトラストアーキテクチャ (ZTA) の設計と実装に関するよくある質問に対して回答します。

ゼロトラストとは?

ゼロトラストは、従来のネットワーク制御やネットワーク境界だけに依存しない、またはそれに根本的に依存しない、デジタル資産に関するセキュリティ制御を提供することに焦点を当てた概念モデルおよび、関連する一連のメカニズムです。代わりに、ID、デバイス、動作、その他の豊富なコンテキストやシグナルをネットワーク制御に追加して、よりきめ細かく、インテリジェントで、適応性が高く、継続的なアクセスに関する意思決定を行います。

ゼロトラストアーキテクチャの実装 AWS のサービス に役立つものは何ですか?

AWS には AWS Verified Access、 AWS Identity and Access Management (IAM)、Amazon Virtual Private Cloud (Amazon VPC)、Amazon VPC Lattice、Amazon Verified Permissions、Amazon API Gateway、Amazon GuardDuty など、ゼロトラストの実装に役立つサービスがいくつか用意されています。

でデータセキュリティを確保するにはどうすればよいですか AWS?

AWS は、保管中および転送中のデータ暗号化用の AWS Key Management Service (AWS KMS)、ネットワーク分離用の Amazon Virtual Private Cloud (Amazon VPC)、認証情報の安全な保存と取得 AWS Secrets Manager 用の などのサービスを提供します。

ゼロトラスト環境でコンプライアンス要件 AWS に対応できますか?

はい。 AWS には、さまざまな規制要件を満たすのに役立つコンプライアンスプログラムとサービスがあります。 は AWS 、コンプライアンスレポートへのアクセス AWS Artifact を提供し、 AWS Config コンプライアンスの継続的なモニタリングと評価をサポートします。

ゼロトラスト環境でセキュリティを自動化するための AWS ツールやサービスはありますか?

AWS は AWS Security Hub CSPM、セキュリティ検出結果を一元化および自動化する などのサービスや、セキュリティポリシーを定義および適用するための AWS Config ルールを提供します。

を使用してゼロトラストクラウド環境で継続的なモニタリングとインシデント対応を確保する方法 AWS

AWS は、Amazon CloudWatch などのサービスをリアルタイムモニタリングや口グ記録、分析 AWS CloudTrail のために提供しています。インシデント対応のベストプラクティスについては、「 AWS セキュリティインシデントレスポンスガイド」をご利用ください。

リソース

リファレンス

- Cloud Center of Excellence とは何か、なぜ組織は Cloud Center of Excellence を作成すべきなのか？ — このブログ記事では、CCoE の概要、効果的な CCoE を構築するためのベストプラクティスなどについて説明しています。
- ゼロトラストオン AWS – このページでは、 AWS 環境におけるゼロトラストのセキュリティ原則とベストプラクティスの概要を説明します。
- ゼロトラストアーキテクチャ: AWS 視点 – このブログ記事では、ゼロトラストの実装方法の定義と指針について説明します AWS。
- AWS Identity and Access Management (IAM) ユーザーガイド – このガイドでは、ゼロトラストアーキテクチャの重要なコンポーネントである IAM でのユーザーアクセスとアクセス許可の管理に関する包括的なドキュメントを提供します。
- AWS Security Hub CSPM – Security Hub CSPM について説明します。これは、 全体のセキュリティアラートとコンプライアンスステータスを包括的に把握できるサービスです AWS アカウント。
- AWS Well-Architected フレームワーク – AWS上の安全性、高パフォーマンス、耐障害性、効率性に優れたアーキテクチャの構築に関するガイダンスとなる、Well-Architected フレームワークについて掘り下げます。
- AWS セキュリティインシデント対応ガイド – このガイドでは、組織の AWS クラウド 環境内のセキュリティインシデントへの対応の基本について説明します。クラウドセキュリティとインシデント対応の概念の概要を示し、セキュリティ問題に対応する顧客が利用できるクラウドの機能、サービス、メカニズムを特定します。

ツール

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch
- AWS Config
- Amazon GuardDuty

- AWS Identity and Access Management
- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub CSPM
- AWS Verified Access

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
追加された更新内容	「ゼロトラストアーキテクチャの主要コンポーネント」セクションへの情報の追加、「ゼロトラスト導入に向けた組織の準備状況の評価」セクションの変更、「ベストプラクティス」セクションへの情報の追加、FAQ の変更を行いました。	2023 年 12 月 4 日
初版発行	—	2023 年 6 月 19 日

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。