AKAMAI チェックリスト

ゼロトラスト・プラットフォームの機能

効果的なゼロトラスト・プラットフォームは、ゼロトラスト・ネットワーク・アクセス（ZTNA）、マイクロセグメンテーション、DNS ファイアウォール、脅威ハンティングなど、かつては個別だったポイントソリューションを、単一コンソールのプラットフォームに統合します。ゼロトラストの迅速かつ効果的な展開は、ランサムウェアを阻止し、厳しいコンプライアンス要件に対応し、各地に分散した従業員とハイブリッド・クラウド・インフラのセキュリティを確保することを意味します。このチェックリストは、ベンダーの機能の評価に加え、単一のプラットフォームを備えたゼロトラストを実装するうえで、要件を確認するリストとしても使用いただけます。

カテゴリー 1：プラットフォーム要件

ゼロトラスト・プラットフォーム・ソリューションは、柔軟でスケーラブル、かつ容易に管理できるものである必要があります。

- [ ] パフォーマンスを損なわずに、トラフィック需要に応じて常に保護を提供できるスケーラビリティ
- [ ] SIEM、SOAR、EDR、CMDB など、お客様が現在使用している既存のセキュリティツールと統合可能
- [ ] ハイブリッド環境、マルチクラウド環境、レガシーシステム、エンドユーザーデバイス、Kubernetes クラスター、仮想マシン、IoT ／ OT 環境など、異種混在のデータセンターに対応
- [ ] クラウド、仮想、オンプレミスなど、多様なハイブリッドアーキテクチャをサポートする柔軟な展開モデル
- [ ] エージェントベースとエージェントレスの両方の展開に対応可能（IoT ／ OT、PaaS）
- [ ] Windows、Linux、macOS、およびレガシー・オペレーティング・システムをサポート
- [ ] すべてのアクションを確実に記録するための監査ログ機能

カテゴリー 2：可視性の要件

環境を把握し、疑わしい接続を特定し、脅威に迅速かつ正確に対応するためには、詳細な可視性が不可欠です。

- [ ] 単一のコンソールで、コンテナ、サーバーレス、IaaS、PaaS などのあらゆる環境におけるユーザーからアプリケーションへのアクセスだけでなく、すべてのアプリケーションとワークロードフローをマップ形式で視覚化
- [ ] 調査およびフォレンジックのための履歴およびリアルタイムフロー
- [ ] サードパーティのファイアウォールやハードウェア（スイッチデバイスなど）との相互運用性
- [ ] CMDB、EDR、クラウド API などのさまざまなサードパーティソースからデータを収集して、コンテキストラベルやルールに利用可能
- [ ] ラベリングを支援（なるべく AI を活用して、スピードと正確さを確保）

カテゴリー 3：ポリシーの要件

ランサムウェア防御、テレワーカー保護、ゼロデイ対応、コンプライアンスなどのさまざまなユースケースで使用できる属性に基づいて、水平方向（マイクロセグメンテーション）と垂直方向（ZTNA）の両方のポリシーが一箇所から適用されます。

- [ ] チョークポイントを生み出す物理的な内部ファイアウォールを必要とせずに、エンタープライズ全体でソフトウェア定義および分散されるポリシー
- [ ] IP とポートだけでなく、さまざまなワークロード属性に基づいて作成されるルール
- [ ] アプリケーション中心のきめ細かいポリシーを適用して、ワークロードをポート、プロセス、さらにはサービスレベルまで保護
- [ ] 事前定義済みのカスタムテンプレートを備えたポリシー推奨エンジン（なるべく AI を活用し、ポリシー作成を迅速化）
- [ ] エージェントの有無にかかわらずポリシーを適用
- [ ] 包括的なフローマッピングに基づくポリシー制御
- [ ] 業界のベストプラクティスに基づいて、事前に設定されたグローバルなリスク軽減ポリシー
- [ ] 仮想環境、IaaS 環境、PaaS 環境全体にわたるハイブリッドクラウドのポリシー
- [ ] ワークロードに関連付けられたポリシーで、ワークロードの移動、移行、変更を追跡可能
- [ ] オフィス内のユーザーやテレワーク中のユーザーのアクセスポリシー

カテゴリー 4：ゼロトラスト・コンポーネントの要件

統一されたゼロトラスト・プラットフォームに統合されたさまざまな機能のうち、ゼロトラスト・ネットワーク・アクセス（ZTNA）とマイクロセグメンテーションが基本の柱として際立っています。これらのテクノロジーにより、組織は従業員や事業継続性に悪影響を与えることなく、ゼロトラスト制御を展開できます。

- ☐ 統一されたアクセスおよびネットワーク・ポリシー・エンジン（水平方向と垂直方向の制御を統合）
- ☐ FIDO2 多要素認証（MFA）による強力なアイデンティティの適用
- ☐ DNS トラフィックを監視およびフィルタリングすることにより、幅広い脅威から IT 環境とユーザーを保護することが可能
- ☐ 検知から逃れようとする脅威の継続的な検知とセキュリティ体制の監視
- ☐ プラットフォームツール間での信号共有により、攻撃者がアクセスメカニズムを通り抜けても確実に阻止
- ☐ 攻撃者を追跡および隔離できる動的なディセプションシステムを採用
- ☐ クエリーによってエンドポイントまたはサーバーに脆弱性が存在するかどうかを確認し、迅速にランサムウェアを検知し緩和することが可能

カテゴリー 5：統合 AI の要件

ゼロトラストを効果的に実行する際の多くの側面は、AI を使用して合理化できます。これにより、ポリシーの作成、コンプライアンス、インシデント対応、脆弱性評価が迅速化され、シンプル化されます。

- ☐ 自然言語を使用したネットワークログとの通信により、インシデント対応やコンプライアンスのスコーピングなどに要する時間を短縮
- ☐ 独自のトラフィックパターンに基づいてラベルとポリシーを提案する AI を使用して、ポリシープロセス全体を合理化
- ☐ 自然言語を構文に変換することで、IOC の調査やカスタムクエリーの作成を行わずに、ネットワークの脆弱性を迅速に探索
- ☐ 従来のツールでは見逃されていた異常や悪性のアクティビティを見つけるための、高度な検知方法を提供する AI 脅威ハンティングメカニズム

詳しくは、Akamai ゼロトラスト・セキュリティの Web ページをご覧ください。

| 公開日 2024 年 4 月