Red Hat
Enterprise Linux

Linux 環境でゼロトラストの基盤を構築する

ゼロトラスト・アーキテクチャによって、IT 環境と組織の保護を強化することができます。

Red Hat では、ゼロトラスト・アーキテクチャの実装を導く重要な原則を使用します。

- 当事者を暗黙に信頼せず、常に確認する。
- 最小特権アクセスを適用する。
- ネットワークとネットワークトラフィックはそもそも危険にさらされていると仮定する。

先進的な IT 環境にはセキュリティに対する新しいアプローチが必要

従来の境界に基づくセキュリティアプローチでは、広く分散したクラウドベースの新しい環境を効果的に保護することはできません。また、セキュリティの脅威とセキュリティ侵害による影響は拡大し続けています。悪意のある攻撃者は脆弱性を悪用しますが、この脆弱性の原因は多くの場合、単一要素認証、暗黙の信頼、境界ベースのアーキテクチャ、ユーザーやイベントに対する不十分な行動追跡など、時代遅れのセキュリティパラダイムです。

ゼロトラスト・アーキテクチャの実装は、IT 環境と組織を保護するための助けとなります。この概要では、Linux® 環境でゼロトラスト・アーキテクチャを確立する場合の検討事項について説明します。

ゼロトラストとは何か？その仕組みとは？

ゼロトラストは、ネットワーク境界でセキュリティを排他的に管理したり、一元化されたセキュリティ管理ソリューションを介して管理したりするのではなく、各アセットにセキュリティを適用するアーキテクチャパターンです。ゼロトラストモデルの基本原則は、セキュリティ境界の内外で動作する当事者、システム、ネットワーク、またはサービスを暗黙に信頼しないことです。あるリソースが別のリソースに接続するには、そのセッションが認証および認可され、明示的な信頼を確立する必要があります。

ID とアクセス管理はゼロトラスト・アーキテクチャの中核をなすものです。ゼロトラスト・アーキテクチャは、デフォルトでアセットへのアクセスを拒否します。アセットとのやり取りを希望するすべてのサブジェクトは、その特定のやり取りに対する明示的なアクセスを要求しなければならず、アクセスを許可する前に、そのやり取りのリスクが評価される必要があります。この評価では、サブジェクトの ID と属性を理解することが重要です。誰がアクセスを要求しているのか、どのアセットにアクセスする必要があるのか、そのトランザクションの目的、そして、時間、方法、機能に応じてアクセスをどのように制限するべきかを決定する必要があります。

アクセスの決定が下されたら、ID と ID 属性の保存、管理、キュレート、および更新を一貫性のある保護された方法で行わなければなりません。ほとんどの組織では、この情報を管理するために、ID 管理、ディレクトリサーバー、および認証情報管理のためのシステムを少なくとも 1 つ使用しています。また、これらのアクセスの決定を継続的に再評価して、時間が経過しても有効であることを確認する必要もあります。

ゼロトラスト・アーキテクチャの実装に関する検討事項

ゼロトラストセキュリティのアプローチを導入するには、通常、セキュリティと IT に関する考え方とプロセスを変える必要がありますが、その上、必要とされる技術的な機能も数多くあります。以下のセクションでは、ゼロトラスト・アーキテクチャの導入において検討すべき、オペレーティングシステムと ID 管理ソリューションの主要な機能について説明します。

オペレーティングシステムの機能

オペレーティングシステムは、組織の IT 環境とゼロトラスト・アーキテクチャの基盤になります。

Red Hat
Enterprise Linux

信頼境界とは

信頼境界とは、通信に参加しているサブジェクトが信頼の状態を変更するコンポーネントの間を論理的に分離することであり、通常は「信頼できる」と「信頼できない」の 2 つの状態に分けます。一般に、信頼できない状態から信頼できる状態に移行するには、次の 2 つのことが必要です。

- **認証**：サブジェクトの ID の確認および検証
- **認可**：アセットへのアクセス権とアクセスの必要性の確認および検証

信頼できるオペレーティングシステムのサプライチェーン

ゼロトラストモデルでは、オペレーティングシステムが最大限の安全性を備えており、デフォルトですべてのアクセスを拒否できる必要があります。リスクを軽減するために、信頼できるソフトウェア・サプライチェーンを通じて提供されるセキュリティ重視のオペレーティングシステムを選択しましょう。以下を提供するオペレーティングシステム・ベンダーを検討してください。

- オペレーティングシステム全体の静的コード分析：プログラミングスタイル、メモリー参照方法、および入力ストリームの検証におけるエラーを特定し、コーディングのベストプラクティスに確実に準拠できるようにする。
- 非予測的な方法でアプリケーションを実行し、メモリーセグメントを割り当てるコンパイラーフラグ：スタック破壊を防ぎ、メモリーの破損を軽減し、CFI (Control-Flow Integrity) のハードウェアサポートを提供する。
- 広範な品質エンジニアリング (QE) テスト：出荷前にセキュリティ上の欠陥を最小限に抑える。
- 脆弱性パッチ適用プロセス：既知の脆弱性に対して定期的に修正を提供する。

強制アクセス制御

オペレーティングシステムは、リソースへのアクセスを個別に分離して制御できることも必要です。Security-Enhanced Linux (SELinux) などの強制アクセス制御 (MAC) テクノロジーは、一元的に管理されるセキュリティポリシーに従ってそれを実行します。以下のオペレーティングシステム機能が必要になります。

- ファイル、プロセス、ユーザー、およびアプリケーションの制御を詳細にカスタマイズできる組み込みの MAC：不適切な権限昇格のリスクを最小限に抑える。
- デフォルトですべてのアクセスを拒否する機能：ゼロトラストの原則に沿うため。

先進的でスケーラブルなポリシーベースの暗号化

データとネットワークトラフィックの暗号化は、IT 環境と組織の保護を強化します。連邦情報処理標準 (FIPS) 140 などの業界標準では、システム全体の暗号化設定が求められます。ポリシーベースの暗号化により、システム全体に一貫した構成を適用して、コンプライアンス要件を満たすことができます。以下を含むオペレーティングシステムを選択してください。

- ポリシーベースの暗号化制御：システム全体に一貫した設定を適用するため。
- FIPS 140 などの一般的なセキュリティ基準に対応するデフォルトプロファイル。
- ポリシーの自動適用および実行：管理を効率化し、エラーを削減し、ポリシーで明確に許可されている場合にのみファイルとソフトウェアボリュームを復号化するため。
- カスタマイズ可能なポリシーと設定：組織のニーズに対応するため。

アプリケーションの許可リスト

アプリケーションの許可リストは、特定のユーザーがシステム上で実行することを許可されている、承認済みアプリケーションまたは実行可能ファイルのインデックスを指定する手法です。この手法は強制アクセス制御 (アプリケーションの動作を制御できるが、どのアプリケーションが信頼されているかを認識できない) を補完するものです。

認可されていないアプリケーションがシステムまたはネットワーク上で動作するのを検出および防止するために、ファイル・アクセス・ポリシー・デーモン (fapolicyd) のような組み込みのアプリケーション許可リスト機能を提供するオペレーティングシステムと、定義済みでカスタマイズ可能な許可リストポリシーを選択しましょう。

Red Hat
Enterprise Linux

ハードウェアベースのルート・オブ・トラスト

ハードウェアベースのルート・オブ・トラスト機能は、システムの整合性を確認し、システムが変更または改ざんされないようにするために役立ちます。暗号化シークレットをソフトウェアから、スマートカード、ハードウェア・セキュリティ・モジュール (HSM)、トラステッド・プラットフォーム・モジュール (TPM) などの改ざん防止ハードウェアデバイスに移行できるオペレーティングシステムを選択しましょう。

コンプライアンススキャン

企業や業界の基準や規制に準拠していないと、コストがかかり、組織にリスクが生じることがあります。Open Security Content Automation Protocol (OpenSCAP) などのシステムスキャンツールは、監査を容易にし、準拠していないシステムを修正するために役立ちます。以下を提供するオペレーティングシステムが必要です。

- 定義済みでカスタマイズ可能なコンプライアンス・プロファイルを備えた組み込みのスキャンツール。
- 監査を容易にし、ドリフトを示すレポート作成機能とベースライン生成機能。
- 非準拠のシステムの自動修正。
- 大規模な管理のための自動化および他のツールとの統合。

トランザクションの監視およびロギング

監視とロギングにより、ユーザーアクションを監査して、悪意のあるアクションが発生したかどうかを判別できます。セッション記録とログ集計のツールは、組織の環境でのアクションに関するインサイトを得るために役立ちます。以下を提供するオペレーティングシステムを選択してください。

- 状況に応じたインサイトを提供する、入力、出力、システム状態、および環境変数のロギング。
- 改ざんを防ぐためのシステム外ログストレージ。
- 監査を単純化するためのカスタマイズ可能な記録設定。

主要なセキュリティ基準

- FIPS 140
- コモンクライテリア (CC)
- セキュリティ技術導入ガイド (STIG)

独立した認証とセキュリティ証明書

オペレーティングシステムがセキュリティ基準に準拠していることがサードパーティによって認証されれば、組織はさらに確信を持って運用することができます。一般的な基準に準拠するオペレーティングシステムを選択してください。

ID 管理ソリューションの機能

ID 管理ソリューションには、ID、その属性、認証情報、証明書、そしてアセットへのアクセスの認可と認証に必要なその他のアイテムが含まれます。

ID ストア

ドメインコントローラーを使用すると、ユーザー、サービス、およびホストの ID、アクセス、ポリシーを管理できます。一元化された ID ストアとドメインコントローラーによって、管理オーバーヘッドを削減し、セキュリティ管理を単純化し、環境全体で一貫性を確保することができます。一元化された ID 管理機能を提供し、運用を効率化して一貫性を向上するソリューションを検討してください。選択するソリューションは、現在使用しているものだけでなく、将来使用する予定のインフラストラクチャ・フットプリントとプラットフォームもサポートする必要があります。

Red Hat
Enterprise Linux

主要な認証タイプ

- 通常のパスワード、ワンタイムパスワード、強化されたパスワード
- リモート認証ダイヤルイン・ユーザー・サービス (RADIUS)
- 初期認証用の公開鍵暗号 (PKINIT)

他の ID 管理システムとの統合

ほとんどの組織はすでに、Linux 環境や Windows 環境用の ID 管理システムを少なくとも 1 つは使用しています。これらのシステムを単一の総合的なソリューションに統合することで、運用を一元化し、組織全体で一貫性を確保することができます。混合環境で ID を管理するために、Microsoft Active Directory などの一般的なツールと連携する ID 管理ソリューションを選択しましょう。

ポリシー管理

ID 管理に対するポリシーベースのアプローチは、一貫性、効率、およびセキュリティの向上に役立ちます。一元化されたインタフェースからポリシーベースの制御を設定および適用できる ID 管理ソリューションを使用することで、ID、アクセス、リソースを適切に構成できるようになります。以下の機能が必要です。

- ロールベースのアクセス制御 (RBAC) およびポリシーベースのアクセス制御。
- カスタマイズ可能な ID およびアクセスポリシー。
- 認証および認可管理。
- セッション記録、監査、ロギング。

多要素認証

多要素認証 (MFA) は、アクセスを許可する前に、本人確認を行うための複数のチェックを要求することで、セキュリティ層を追加するものです。構成可能な認証タイプを提供し、ハードウェアトークンとスマートカードを介して MFA をサポートする ID 管理ソリューションを選択してください。

一般的な証明書のプロトコルおよび基準

- X.509
- 自動証明書管理環境 (ACME)
- 簡易証明書登録プロトコル (SCEP)
- Secure Sockets Layer (SSL)
- トランスポート層セキュリティ (TLS)

証明書管理

デジタル証明書には、ユーザー、アプリケーション、Web サイトなどのサブジェクトの ID を認証するために必要な情報が含まれています。これらは、最小権限の原則に従って作成、監視、更新、および廃止する必要があります。以下を提供する ID 管理ソリューションを選択してください。

- ユーザー、ホスト、およびサービス証明書の完全なライフサイクル管理。
- 一般的なプロトコルと基準のサポート。
- タイムリーな更新を行うための証明書の有効期限の自動追跡。
- 公開鍵基盤 (PKI) 認証のサポート。

シングルサインオン

サービス、デバイス、サーバーごとに個別のアクセス認証が必要です。シングルサインオン (SSO) システムは、中央の ID サービスを使用してアクセスを単純化し、サーバーが認証済みのユーザーをチェックできるようにします。そのためユーザーは一度の認証で、複数のサービスにアクセスすることができます。現在使用しているサービスと将来使用する予定のサービスだけでなく、Web 認証もサポートする ID 管理ソリューションを選択してください。

Red Hat Enterprise Linux でゼロトラストの基盤を構築する

Red Hat は、ゼロトラスト・アーキテクチャの設計、構築、管理に使用できる基本的なテクノロジーを提供します。Red Hat® Enterprise Linux は、ゼロトラストモデルの導入に必要なセキュリティ・テクノロジー、制御、認証、およびサポートを提供します。これは、信頼できるサプライチェーン、SELinux のアクセス制御、システム全体の暗号化ポリシー、アプリケーション許可リスト、ハードウェアベースのルート・オブ・トラスト、セッション記録機能、およびシステムロールをもたらすものであり、この概要で説明

エキスパートによるサービスでデプロイを迅速化

Red Hat は、Red Hat のプラットフォームと製品に基づくゼロトラスト・アーキテクチャの導入を支援するサービスを提供しています。

- Red Hat Open Innovation Labs は、エンジニアとオープンソースのエキスパートが連携する参加型の研修プログラムで、実際のビジネス成果を達成するために役立ちます。
- Red Hat サービス：Zero Trust Adoption Journey は、現在の状況の評価と、ゼロトラスト・アーキテクチャの構築計画の作成を支援するコンサルティング契約です。

しているオペレーティングシステムの要件をすべて満たしています。また、OpenSCAP スキャナーが組み込まれており、Red Hat Insights の予測分析および修復サービスも含まれています。そして、Red Hat Enterprise Linux は、CC、FIPS 140、STIG、Section 508 などの多くの政府のセキュリティ基準に認定されています。

Red Hat Enterprise Linux に含まれる Red Hat Identity Management は、ID 管理の一元化、セキュリティ制御の適用、環境全体でのセキュリティ基準への準拠を支援します。ID 管理インフラストラクチャを単純化しながら、ゼロトラストのベストプラクティスを実装するために必要な機能を提供します。標準のインタフェースを通じて Microsoft Active Directory、軽量ディレクトリ・アクセス・プロトコル (LDAP)、およびその他のサードパーティ製ソリューションと統合できます。Red Hat Identity Management は、証明書ベースの認証および認可技術もサポートしています。

Red Hat Enterprise Linux と Red Hat Identity Management は、他の Red Hat ポートフォリオと統合し、ゼロトラスト・アーキテクチャの統合基盤を提供します。

- Red Hat Single Sign-On は、一般的な基準に基づく Web シングルサインオン機能を提供します。
- Red Hat Satellite は、Red Hat Enterprise Linux 環境を効率的かつ安全に、コンプライアンスに則して実行し続けるために役立つインフラストラクチャ管理製品です。
- Red Hat Ansible® Automation Platform は、大規模な IT 自動化を構築、運用、管理するためのエンタープライズ・フレームワークを提供します。
- Red Hat Certificate System は、スマートカードのプロビジョニング、証明書タイプのカスタマイズ、シークレットストレージの保護などの高度な管理作業をサポートする認証局です。
- Red Hat Directory Server は、オペレーティングシステムから独立した、ネットワークベースのスケーラブルなレジストリで、分散ディレクトリトポロジーの ID およびアプリケーション情報を一元的に格納できます。

次のステップ

- Red Hat Enterprise Linux のセキュリティの詳細をご覧ください。
- Red Hat のアプローチ：ハイブリッドクラウド・セキュリティをお読みください。

アジア太平洋
+65 6490 4200
apac@redhat.com

オーストラリア
1 800 733 428

インド
+91 22 3987 8888

インドネシア
001 803 440 224

日本
03 4590 7472

韓国
080 708 0880

マレーシア
1 800 812 678

ニュージーランド
0800 450 503

シンガポール
800 448 1430

中国
800 810 2100

香港
800 901 222

台湾
0800 666 052

fb.com/RedHatJapan
twitter.com/RedHatJapan
linkedin.com/company/red-hat

jp.redhat.com
F31712_0522_KVM