NGINX
Part of F5

Kubernetesアプリケーションのための ゼロトラストセキュリティ

エッジからクラウドまで総合的にアプリケーションを保護

分散型アプリ、マイクロサービス、APIを大規模に保護

サイバーセキュリティ攻撃は巧妙化し、その数も飛躍的に増えており、オンプレミス、ハイブリッド、およびマルチクラウドのKubernetes 環境において、外部と内部両方の脅威に晒されるリスクが高まっています。

セキュリティインシデントは、組織の生産性や評判の低下、規制コンプライアンス違反、機密データの盗難など、さまざまな面でコストがかかります。

従来のセキュリティモデルでは、インフラストラクチャの周囲に境界線が配置され、その内部にいるユーザーとアクティビティは信頼できると考えられてきました。しかし、昨今の分散環境では、もはや場所を信頼の根拠とすることはできません。内部のトラフィックでも脅威となる可能性を含んでいます。

そこで、Kubernetes インフラストラクチャにゼロトラストのセキュリティモデルを採用することで、セキュリティ体制を改善することが可能となります。ゼロトラストは ID ベースのセキュリティモデルで、組織の境界の内外、リモート、オンプレミス、クラウドなど、ユーザー、アプリケーション、データ、デバイスの場所に関係なく保護します。これは、決して信頼しない、常に確認する、継続的にモニタリングするという、3 つの基本原則に基づいています。

F5 NGINX は、クラスタのエッジでは NGINX Ingress Controller を使って、そして、クラスタ内には NGINX Service Mesh を使って、Kubernetes でゼロトラストセキュリティポリシーの一元的適用を実現します。さらに、NGINX App Protect を使用して、高度なサイバー攻撃に対する最新の WAF と DoS 保護をクラスタ、サービス、またはポッドレベルで展開することができます。これにより、開発者はアプリ全体でセキュリティロジックを構築、維持、複製するという負担から解放され、代わりにプラットフォームレベルでセキュリティ技術を容易に活用することが可能となります。

KubernetesのゼロトラストにNGINXを使用する理由

複雑さやオーバーヘッドを増やすことなく、エッジからクラウドまでKubernetesアプリを安全に保護します。

実用的なインサイト

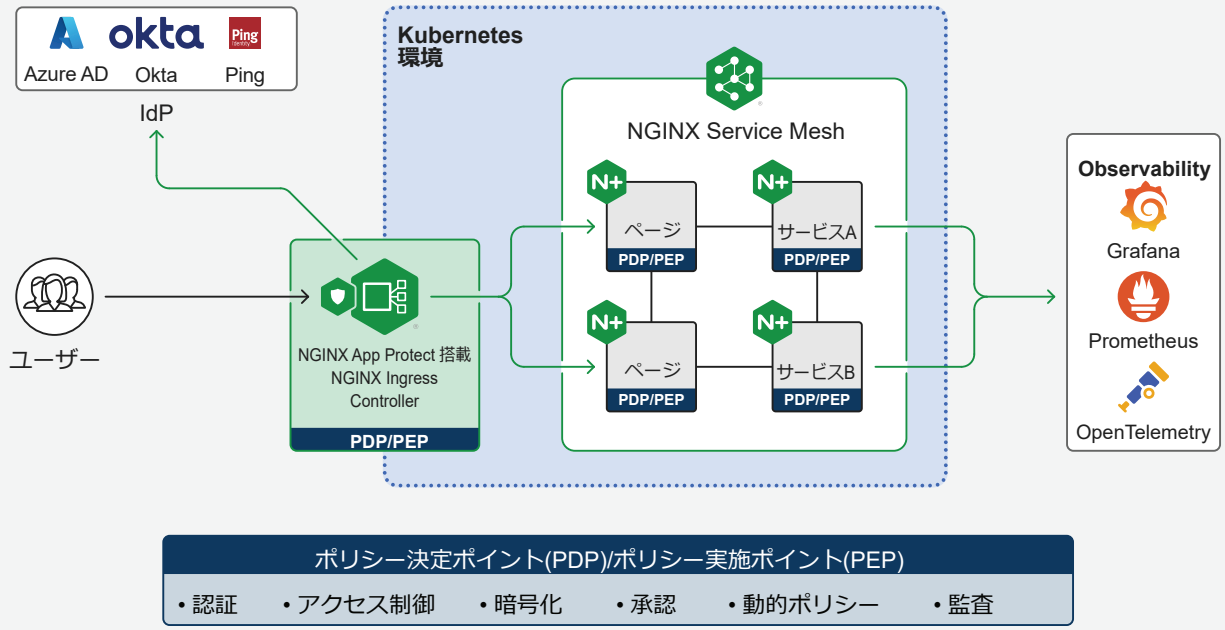
サイバーセキュリティの脅威が
組織や顧客に損害を与える前に
検出し、緩和する

デプロイメントの柔軟性

Kubernetesの実行場所に関係なく
アプリとAPIの保護を効率化し、統合する

大規模な保護

セキュリティを犠牲にすることなく、
ワークロードのピーク時の
カスタマーエクスペリエンスを向上させる



認証と承認

ゼロトラストでは、すべてのデバイス、ユーザー、サービス、およびリクエストの認証と承認が義務付けられています。NGINX には、認証および承認サービスに関するオプションがいくつかあります。それらは、HTTP Basic 認証、JWT 認証、Okta や Azure AD などの ID プロバイダーとの統合による OIDC 認証などです。NGINX を使って、サービスを認証するための安全な ID 証明書を発行し、Kubernetes クラスタ全体でアクションを実行するための権限を付与します。

データの暗号化と完全性

ゼロトラストでは、場所に関係なくすべての通信を保護することを要求します。そのためには、すべての関係者の認証と、データの機密性と整合性を確保するための暗号化の両方が必要です。ユーザーとサービス間通信では、NGINX は TLS パススルーと TLS 終端の両方をサポートします。サービス間の通信では、NGINX は認証と暗号化に mTLS を使用し、特定のサービスのみが相互通信できるようにします。

アクセスコントロールとアクセスポリシー

アクセスコントロールは、ゼロトラストアーキテクチャのもう 1 つの重要な要素です。NGINX では、組織のセキュリティニーズに合わせて簡単に調整ができるように、ロールベースのアクセス制御（RBAC）をサポートしています。RBAC を導入すると、ユーザーはチケットを発行して IT チームがそれを実行してくれるのを待たなくてもよくなります。つまり、ジョブを実行するのに必要な機能に制限付きでアクセスできるようになるのです。さまざまなチームでセルフサービスとガバナンスを実現する、きめ細かなアクセス管理機能が利用できます。

可観測性

監査、モニタリング、ロギング、トレース、およびレポート作成は、ゼロトラストの確立とセキュリティ体制の改善を成功させるための鍵です。NGINX は、詳細なリアルタイムおよび履歴メトリクスを生成し、OpenTelemetry、Grafana、Prometheus などの一般的なツールと統合します。詳細なトレースは、リクエストがエンドツーエンドでどのように処理されるのかを明らかにします。これは、アプリ、API、インフラストラクチャの健全性とパフォーマンスに関する実用的なインサイトにとって、必要な情報です。

WAF と DoS 保護

分散型アプリケーションのセキュリティをさらに強化し、OWASP Top 10 やレイヤ 7 の DoS 攻撃から保護するために、NGINX App Protect の WAF と DoS モジュールを活用します。 F5 の業界をリードするセキュリティの専門技術に基づいて構築された NGINX App Protect は、リリース速度やパフォーマンスを低下させることなく、最も高度な脅威からアプリ中心の俊敏な保護を実現します。 また、テレメトリをサードパーティ - の分析や可視化ソリューションに簡単に転送することもできます。

NGINXがどのように役立つかについては、nginx.co.jpをご覧ください。

NGINX
Part of F5