APPGATE SDP
ユニバーサル・ゼロ・トラスト・ネットワーク・アクセス (ZTNA)

ソリューションの概要

Appgate SDPは、業界をリードする普遍的なゼロトラストネットワークアクセス（ZTNA）ソリューションであり、現代の分散ワークフォースのセキュリティ課題に対応します。Appgate SDPは、クラウドやハイブリッド・インフラにきめ細かく、コンテキストを意識したアクセス制御を 提供し、柔軟性を損なうことなく強固なセキュリティを確保します。Appgate SDP は、ソフトウェア定義の境界(SDP)モデルを採用し、ユーザー／デバイスと、彼らが必要とする 特定のリソースとの間にダイナミックな1対1のネットワーク接続を作成します。このアプローチにより、ハイブリッドおよびクラウド環境におけるセキュリティとパフォーマンスの 両方に最適化されたダイレクトルーティングを備えた、スケーラブルで分散された可用性の高いアーキテクチャが実現され、きめ細かな「セグメント・オブ・ワン」ネットワークリソースへのアクセスが可能になります。

主要コンポーネント

1. コントローラーポリシー決定ポイント
2. ゲートウェイ: ポリシー実施ポイント
3. クライアント：エンドユーザー機器ソフトウェア
4. コネクター: ローカル・リソース・トラフィック処理用のマルチクライアント・アプライアンス

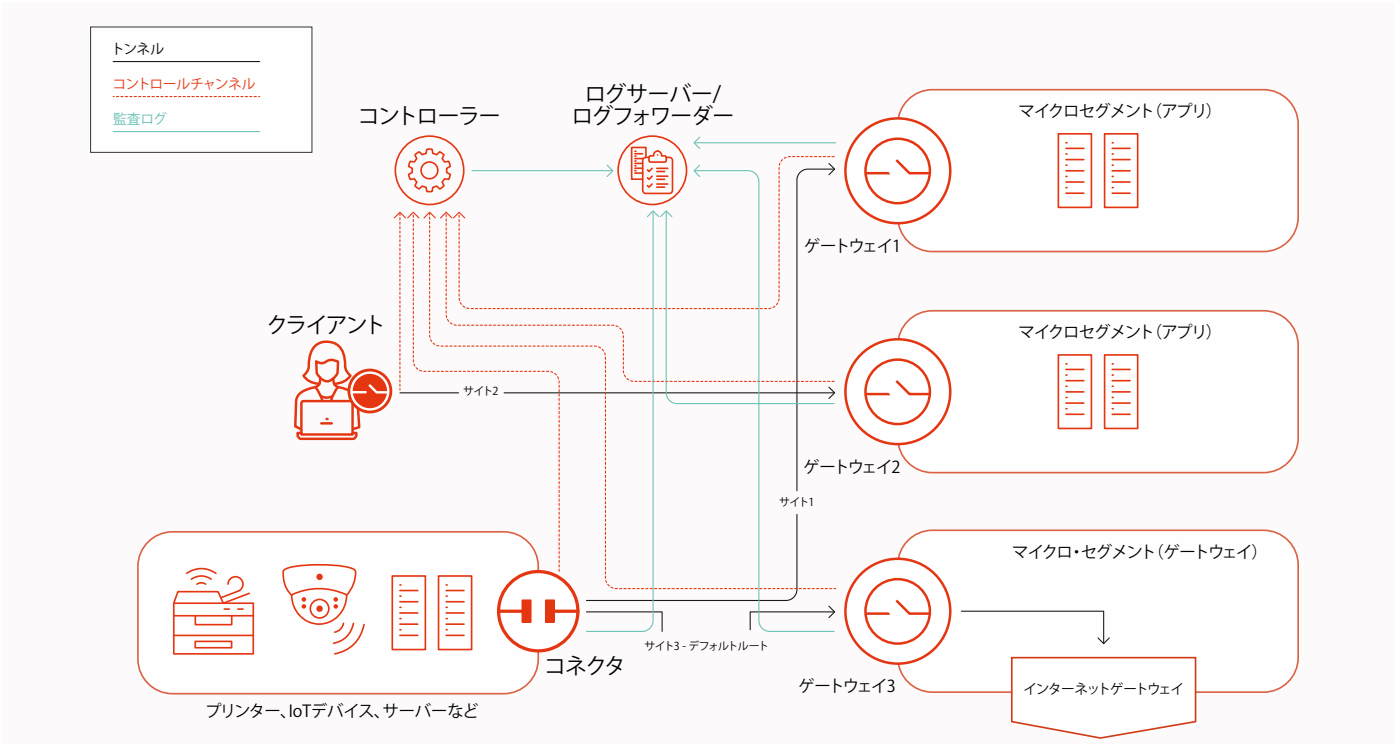
技術仕様

- 認証: コンポーネント間の信頼関係のためのPKIベースのアルゴリズム
- アクセス制御: ユーザー、環境、インフラ属性に基づくリアルタイムポリシー評価
- ネットワーク・セキュリティクライアント・ネットワーク・ドライバ経由で確立された安全なトンネル
- 互換性:
  - アイデンティティ・プロバイダ（IdP）: Appgate SDPはIdPにとらわれず、外部LDAP（AD）、LDAP証明書、OIDC、RADIUS、SAML IdPによる認証をサポートします。
  - OSサポート: すべての主要なデスクトップ、サーバー、モバイルオペレーティングシステム
  - インフラストラクチャー：主要なクラウドおよび仮想化プラットフォーム

Appgate SDPは、統一されたポリシー・モデルを通じて、キャンパス内であろうと遠隔地であろうと、デバイスや場所に関係なくすべてのユーザにユニバーサルなZTNAを提供します。このソリューションは、検証されたアイデンティティとコンテキストに基づいて、ユーザとリソース間の個別化された安全な接続を動的に作成します。シングルパケット認証（SPA）は、ポートが公開されていないネットワークを不可視化し、シングルパケットで暗号的に検証されたユーザのみに通信チャネルへのアクセスを許可します。Appgate SDPは、ユーザ、ワークロード、リソースをマイクロセグメント化するために、ジャスト・イン・タイムのセッションベースのマイクロファイアウォールを確立することで、最小特権の原則を実施します。動的なライブ・エンタイトルメントは、コンテキストとリスクに基づいて、ほぼリアルタイムでアクセスを修正します。Appgate SDPを使用することで、企業はネットワーク・インフラストラクチャ全体におけるデータの移動方法を完全に制御することができます。

主な特徴:

1. 高度な信頼モデル: 独自の6レイヤートラストモデルを実装し、初期認証にとどまらず、リソース接続の時点でアクセスを検証することで、セキュリティを拡張します。
2. インテリジェント・アクセス・コントロール：複数の要素に基づいてユーザーとデバイスを認証し、エンタイトルメント・トークンを発行して正確なアクセス管理を行うコントロール・システムを活用。
3. ブラウザベースのアクセス: フルクライアントと同レベルのセキュリティを維持しながら、ウェブブラウザを介したクライアントレス・アクセスのためのポータルを提供。
4. IoTとレガシーデバイスの統合: センサーからサーバーまで、さまざまなデバイスを安全に搭載し、アクセスを管理するコネクター・コンポーネントを備えています。
5. ダイナミック・マイクロ・ファイアウォール: セッションごとに個別のファイアウォールインスタンスを作成し、きめ細かな制御と保護リソースの不可視化を実現します。
6. 簡素化されたリモート・リソース・アクセス: ポート443のアウトバウンド接続のみを必要とするコネクタを通じて、分散リソースの容易な統合を可能にします。
7. 包括的な監査: 柔軟で強力な監査ロギングのための ログフォワーダーが含まれており、コ ンプライアンスとセキュリ ティ監視のニーズをサポートし ます。
8. 柔軟な展開: 従来のネットワーク境界線から独立して動作し、ソフトウェア仮想化を活用してクラウドやハイブリッド環境にシームレスに統合。



Appgate SDPの分散アーキテクチャは、必要な場所にアプライアンスを展開する柔軟性を提供します。各アプライアンスはステートレス マシンであり、さまざまな機能を提供するように設定できます：各アプライアンスはステートレスマシンであり、さまざま な機能（コントローラ、ゲートウェイ、ログサーバー、ログフォワーダー、メトリックスアグリゲーター、ポータルまたはコネクタ）を提供するように構成できます

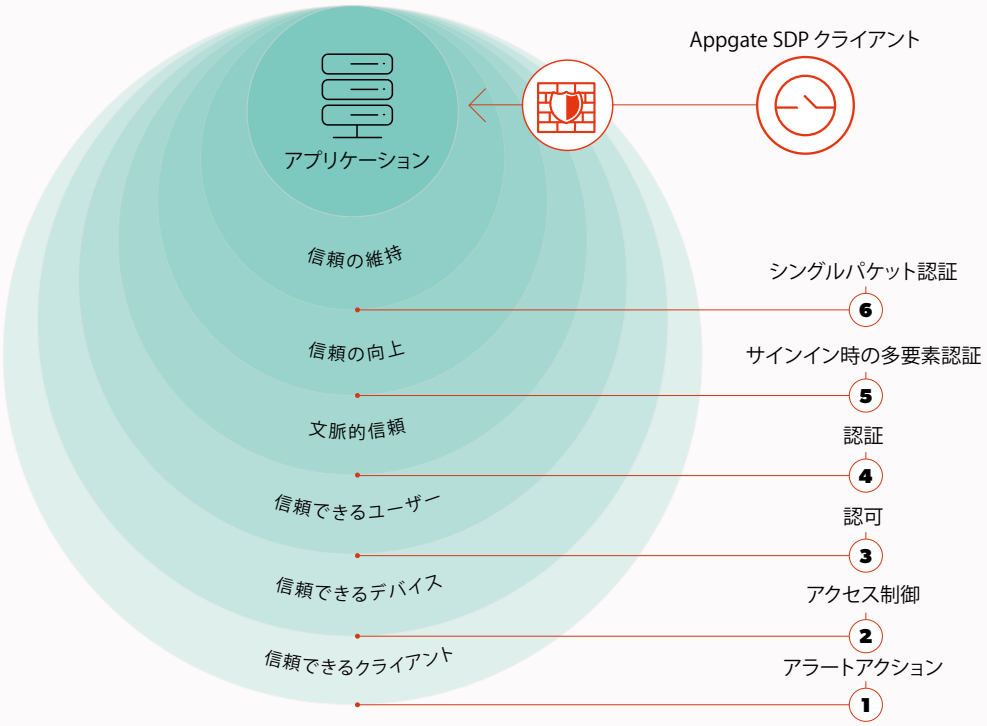
運用フロー

1. クライアント認証がコントローラに送信されます。
2. コントローラは、認可されたリソースを含む暗号署名されたトークンを発行します。
3. クライアントが安全なトンネルとルーティングルールを確立します。
4. ゲートウェイがリアルタイムの条件付きアクセスチェックを適用します。
5. セキュアトンネル経由でアクセスが許可されます：クライアント→ゲートウェイ→サバー
6. ログサーバーはすべてのアクセスイベントを記録します。
7. オプション：ログフォワーダーは、SIEM/IDSシステムと統合します。

信頼の確立6層モデル

Appgate SDPは、マルチレイヤーの認可モデルを使用して、すべてのユーザーアクセ ス試行に対してリアルタイムでコンテキストを考慮した制御を提供します。以下の番号は、以下の図のプロセスレイヤーに対応しています。

1. シングルパケット認証 (SPA): SPAは、Appgate SDPシステム（つまり、コンポーネント/インフラストラクチャ）を 権限のないユーザーから不可視にし、事前共有キーを持つクライアントにのみ通信チャネ ルを開かせます。Appgate SDPは、クライアントが使用するプロファイルに含まれる1つまたは複数のSPA鍵を受け付けます。
2. サインイン時の多要素認証（MFA）：ユーザーのデバイスを登録することで、2 つ目の（信頼できる）認証要素として機能し、盗まれた認証情報による不正アクセスの試みをブロックしてセキュリティを強化します。設定されたMFAであればどのようなものでも使用でき、一度デバイス（またはブラウザ）を登録すれば、サインインのたびにユーザーがMFAを実行する必要はなくなります。
3. 認証: このレイヤーは、SAML や OIDC などの定義された信頼できるソースに対して、ユーザーとデバイ スの認証情報を検証します。
4. 認可: ポリシーの割り当て基準は、ユーザー／デバイスの属性を評価し、各ユーザー／デバイスに特定の権限セットを割り当てることを可能にします。
5. アクセス制御: このレイヤでは、ユーザートラフィックをエンタイトルメントと比較し、アクセスポリシーを実施し、アクセス条件を検証し、必要に応じてユーザにアクション（MFAなど）を促します。Appgate SDPは、エンタイトルメントで定義された保護リソースのホスト、ポート、プロトコルに基づき、各ユーザ／デバイスのアクセスを動的に管理します。
6. アラートアクション: このレイヤは、潜在的な脅威にプロアクティブに対処するために、未承認のポートスキャンなどの高リスクの動作をブロックし、アラートとともにログに記録するトリガーシステムとして機能します。



Appgateの6層信頼モデルは、最初の認証を超えてセキュリティを拡張し、リソース接続の時点で継続的にアクセスを検証します。

セキュリティ仕様

- SPA: セキュリティ強化のため、AES-256-GCM暗号を使用。
- アプライアンス証明書: SHA512、RSA 暗号化、キーサイズ 4096 を使用してコントローラが生成。コントローラとクライアントの安全な通信を保証するため、厳格な制約を持つ認証局として機能します。
- クレームとエンタイトルメントトークンの暗号化: トークンの保護に AES-256-CTR 暗号を使用。
- データベースの暗号化: 保存データの保護に AES-256-CTR 暗号を使用。
- バックアップファイルの暗号化: GPG対称暗号化（AES-256-CFB）で保護し、データの完全性と機密性を確保します。
- FIPSコンプライアンス: デスクトップクライアントの場合、Appgate SDPはwolfCryptモジュールを活用してFIPS 140-3標準に準拠しています。

通信プロトコルと暗号化

- TLSv1.3: すべての通信のデフォルトプロトコルで、必要に応じてTLSv1.2をフォールバックとして使用します。
- アプライアンス間通信: TLS13-AES256-GCM-SHA384 および ECDHE-RSA-AES256-GCMSHA384暗号を使用し、相互証明書ベースの認証と DN チェックにより保護されます。
- クライアントおよび管理者からアプライアンスへの通信: デフォルトでは、TLS13-AES256-GCMSHA384 および ECDHE-RSA-AES-256-GCM-SHA384 暗号が使用されます。
- SSHからアプライアンスへの通信: SAES-256-CTR、AES-192-CTR、およびAES-128-CTR暗号をサポートします。
- クライアントからゲートウェイへのトンネル: TLS13-AES256-GCM-SHA384およびECDHE-RSA-AES256-GCM-SHA384暗号と相互証明書ベースの認証を使用。

重要な機能

- MDMサポート: モバイルデバイスを安全に管理します。
- マルチトンネルVPN: 複数の同時VPN接続を可能にします。
- IPv6サポート: IPv6ネットワークとの互換性を確保します。
- ヘルスチェック・プローブ・サービス: システムの健全性を監視し、維持します。
- Metrics Aggregator and Prometheus Exporter: システム・メトリクスの収集とエクスポート。
- プロキシプロトコルのサポート: プロキシサーバーとの互換性を化します。
- SPA: 基盤となるネットワーク・インフラストラクチャを隠蔽することで、セキュリティのレイヤーを追加します。
- 高可用性: システムの信頼性とアップタイムを保証します。
- マルチサイトのサポート: Appgate SDPを複数の地域に展開できます。
- ユーザーごとのファイアウォール: 個々のユーザープロファイルに基づくきめ細かなアクセス制御を提供します。
- ロードバランシング: 複数のサーバーにトラフィックを分散し、最適なパフォーマンスを実現します。
- 基準スクリプトでの外部 REST 呼び出し: 外部データに基づく動的なアクセス制御の決定を可能にします。

テクノロジー統合

- エンドポイント検出と応答 (EDR): CrowdStrikeとSentinelOne
- ITサービス管理 (ITSM): ServiceNow
- マイクロセグメンテーション: IllumioとColorTokens
- セキュリティインシデント・イベント管理 (SIEM): Splunk、Sumo Logic、Falcon LogScale、Elasticsearch、OpenSearch、DataDog、Coralogix、Azure Monitoring、AWS Kinesis、およびTCPフォワーディングを受け付けるすべてのSIEMツール

付加価値クラウドサービス

AppgateのZero Trustプラットフォーム（ZTP）は、Appgate SDPの機能を強化するクラウドネイティブなソリューションであり、多様なIT環境にZTNAを実装するための堅牢なフレームワークを提供します。柔軟な導入モデル、アイデンティティ中心のアクセス制御を行う統合ポリシーエンジン、最小権限アクセスを強制する動的なネットワークセグメンテーションを特徴としています。ZTPは継続的な多要素認証と認可を提供し、ユーザの行動とデバイスの姿勢にリアルタイムで適応します。普遍的なリソースをカバーすることで、ハイブリッド環境やマルチクラウド環境で一貫したZero Trustポリシーを提供し、運用効率を高めながらセキュリティ体制を大幅に改善します。

- アプリケーション・ディスカバリー: アプリケーション・ディスカバリーは、組織がVPNベースのリモート・アクセスから最新の安全なZTNAモデルへ迅速に移行するユニークな機会を提供します。この機能は、高度な機械学習（ML）システムを採用し、ユーザーの行動とアクセスパターンを長期にわたって観察します。このデータを分析することで、Application Discoveryは実用的な洞察を生成し、管理者はアクセス・ポリシーを定義して微調整できるようになり、組織のセキュリティ目標に沿った特定のリソースにアクセスできるのは許可されたユーザーだけになります。組織がホスト型または接続型のデプロイメントを採用する際、Application Discoveryを活用することで、シームレスなユーザー・エクスペリエンスを維持しながら、進化するセキュリティ脅威への対応能力を大幅に強化することができます。

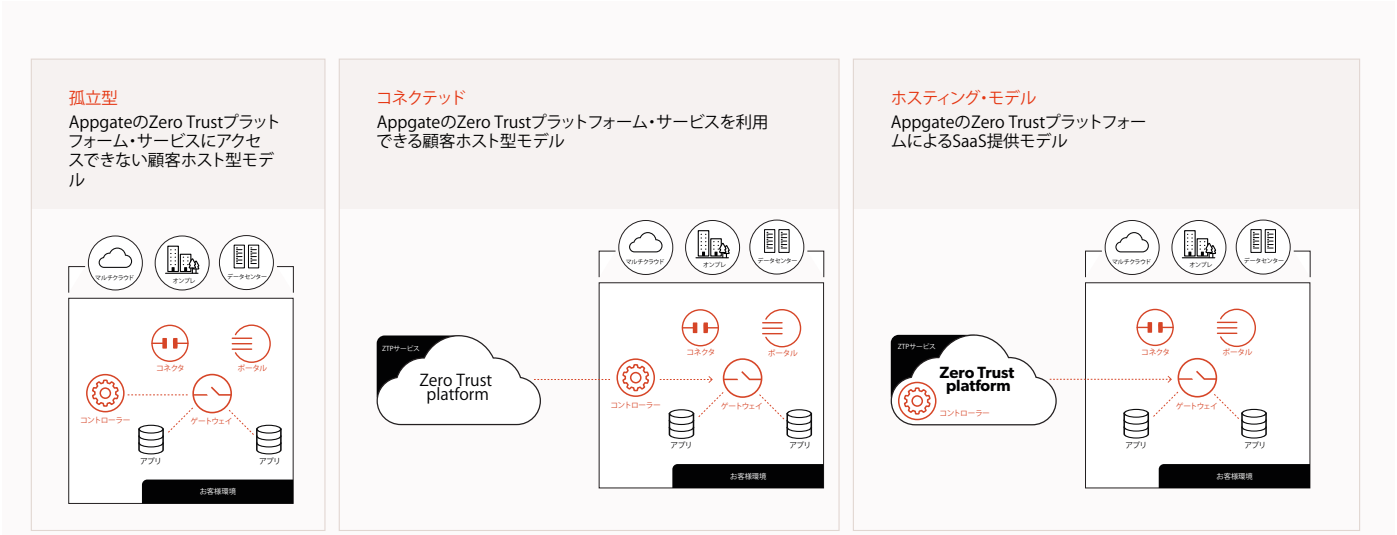
- リスク・エンジン: リスク・エンジンは、サードパーティのIT、セキュリティ、およびビジネス・ソリューションによって収集されたセキュリティ状況の洞察によって、アクセス・ポリシーを強化します。主要なセキュリティ・ツールとの統合が組み込まれており、クリックするだけで設定できるインターフェイスにより、カスタムAPIスクリプトのコストと複雑さを排除します。

- リスクアラート: リスクアラートサービスにより、Appgate SDPのダイナミックポリシーエンジンは、デバイスやユーザのセキュリティ態勢の変化を示すサードパーティサービスからの情報に対応することができます。.

- ポリシーアナライザ: ポリシーアナライザは、ポリシーの作成と管理プロセスを合理化するために設計された強力なツールです。管理者は、運用を簡素化しながら、組織の攻撃対象領域を減らすことができます。ポリシーアナライザは、リアルタイムのデータと分析を活用することで、組織は安全に破棄できるポリシーと権限を特定し、重複するリソースを持つ権限を発見し、他の方法では見逃される可能性のある設定をハイライトすることができます。このプロアクティブなアプローチは、セキュリティを強化し、規制コンプライアンスを簡素化するため、ホスト型または接続型の導入に移行する組織にとって不可欠な資産となります。

展開の柔軟性

Appgate SDPは、クラウド、オンプレミス、ハイブリッド環境に展開することができ、組織の特定のニーズに適応する汎用性の高いソリューションを提供します。ソフトウェア定義のため、従来のハードウェアベースのソリューションの制約を受けることなく、迅速な展開と拡張が可能です。



Appgate SDPは、分離型、接続型、ホスト型など、さまざまな導入モデルによる選択肢と柔軟性を提供します。

Appgate SDPのメリット

複雑な環境と高度なセキュリティ要件に対応: ベンダークラウドに依存することなく制御を維持し、拡張性を活用して統一された相互運用可能なセキュリティエコシステムを構築します。	ユーザーエクスペリエンスの向上: 自動ゲートウェイとサイトフェイルオーバーを提供する同時ダイレクトマルチトンネル接続により、あらゆる従業員や承認された第三者に一貫した接続エクスペリエンスを提供します。
セキュリティ体制の強化：すべてのリソースを遮蔽して攻撃面えなくし、リスクを考慮したZero Trustの最小権限アクセスによって横の動きを阻止し、包括的なネットワークの可視性を実現し、堅牢なZero Trust基盤を構築します。	IT管理者とセキュリティ管理者の時間を最小化します：統一されたポリシーエンジンにより、作業時間を短縮し、アクセスプロビジョニングを自動化し、トラブルチケットを最小限に抑えます。
ネットワークに革命をもたらします：トポロジー全体にわたってセキュアなユニバーサルアクセスエクスペリエンスを重ね合わせ、セキュアなカフェスタイルの接続性でネットワークに革命をもたらし、冗長な接続コストを排除することで運用コストを削減します。	テクノロジー投資の強化：業界標準のさまざまな監視ツールやレポート作成ツールとシームレスに統合し、アクセス関連のセキュリティリスクやイベントを一元的に関連付けます。また、エンドポイントの検出と対応（EDR）などのサードパーティ・サービスによるセキュリティ状況の洞察を可能にし、コンテキストとリスクに基づいて動的なアクセス制御ポリシーを強化します。

結論

Appgate SDPは、アイデンティティとコンテキストに基づいてユーザーを動的に認証および認可するZTNAモデルを実装することで、組織に大きな利益をもたらし、不正アクセスのリスクを最小限に抑えます。また、きめ細かなアクセス制御により、ネットワークのセグメンテーションを強化し、ネットワーク内での横方向の動きを制限します。ハイブリッド環境への柔軟な導入オプション、既存のセキュリティ・ツールとのシームレスな統合、堅牢なエンドツーエンドの暗号化により、セキュリティをさらに強化し、管理を簡素化することで、最新のゼロトラスト・セキュリティ戦略に対応します。

About Appgate

Appgateは、組織の最も貴重な資産とアプリケーションを保護します。Appgateは、Zero Trust Network Access（ZTNA）とオンライン詐欺防止におけるマーケットリーダーです。Appgate の製品には、Appgate SDP for Universal ZTNAと360 FraudProtectionがあります。Appgateのサービスには、脅威アドバイザリ分析およびZTNA実装が含まれます。Appgateは、世界中の企業や政府機関を保護しています。詳細は appgate.com. をご覧ください。

appgate