MENLO SECURITY

White Paper

Zero Trust Network Access

きめ細かく、適応力があり、
コンテキストを意識したセキュリティが
分散した従業員を保護

パンデミックによって労働力の大規模な分散が起こり、ITチームは接続性とセキュリティに対する考え方を根本的に考え直す必要に迫られました。これほどの急激な環境の変化に対応するためのプランは用意されていなかったため、労働力のごく一部をサポートすることしか考えていなかった仮想プライベートネットワーク（VPN）とリモートアクセス環境は、一夜にして過負荷に陥りました。

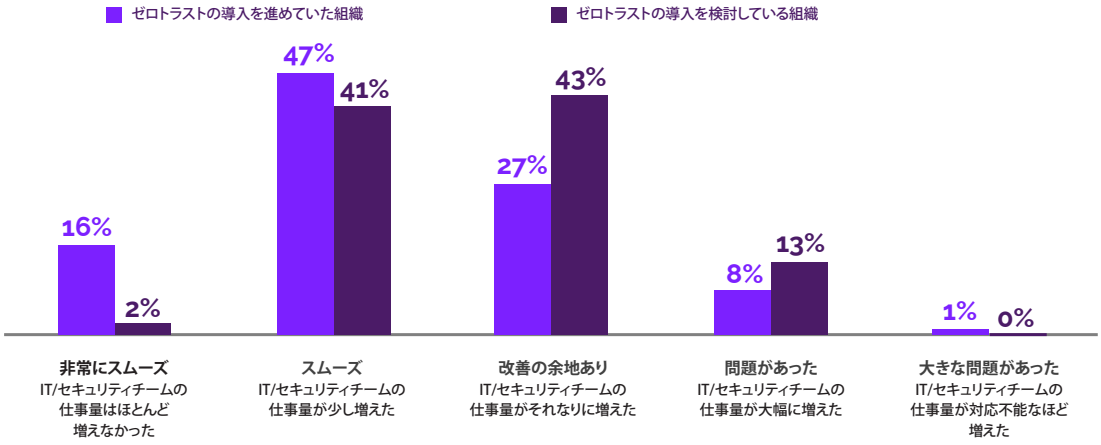
多くの企業では、いずれはこれまでのハブ&スポークモデルのネットワークアーキテクチャを廃止する必要があることを理解していました。パンデミックの前から、VPNは遅延とセキュリティ上の問題を引き起こす原因であるという批判に晒されていたからです。批判の主なポイントは、VPNアプライアンスが組織のネットワーク全体へのアクセスを許可してしまうことです。攻撃者がユーザーの認証情報を獲得した場合に接続が適切に制御されていないと、それが侵害に繋がる大きなセキュリティギャップとなりますが、侵害が増加の一途を辿る中でもその状態が続いていました。

そのため多くの組織は、過負荷に対してVPNを拡張するという長年続けて来たアプローチの代わりに、Zero Trust Network Access（ZTNA）を導入することでこの問題に対処しました。これは緊急対応という意味では期待通りの働きをしましたが、適切な計画の元でオプションを確認し、最善のソリューションを選択するという本来の手順を踏んでいないため、多くの場合必要最低限の機能しか備えていません。分散したユーザーが特定のアプリケーションにアクセスすることはできますが、強力なセキュリティ体制の構築に必要なポリシー適用や監視のための機能は実装されていないのです。本格的なZTNAソリューションが持つべき保護機能が実装されていないため、ユーザー（またはアクセス権を持つ脅威アクター）がアプリケーションに接続し、クリック、ダウンロード、または任意の操作を行うことが可能になっています。完全な制御ができないため、ITチームは異常な行動を識別できません。

ZTNAソリューションは、パンデミックという緊急事態において多くの問題を解決しましたし、パンデミックの最中であれば多少の欠点は許容されました。しかし、もし時間があり、急がされていなければ、違う判断が下されたのではないでしょうか？ 組織は購入の基準としてリストに何を載せたでしょうか？ そして、検討はどのように行われ、成功はどのように定義されたでしょうか？

ゼロトラストは非常に有用であり、ZTNAの採用は今も増え続けているため、組織は今こそセキュリティとビジネスの成果を向上させるために、合理的な意思決定をやり直すチャンスです。
このホワイトペーパーでは、そのプロセスを支援するために、ITアーキテクチャにZTNAを含めるための重要な考慮事項について解説します。さらに、ZTNA採用への道筋を設定するための重要な質問に答えます。

ゼロトラストを採用した組織では、在宅勤務への移行がスムーズに行われました



出典：Enterprise Security Group: The State of Zero Trust Security Strategies

ZTNAのユースケース

現代のデジタルかつアジャイルな組織とそのユーザーの要求を満たすために、拡張性と遅延の問題を抱えるVPNは、ZTNAソリューションによって徐々に置き換えられつつあります。この移行は非常に短期間で行われると予想されていますが、それはレガシーソリューションからの移行、またはレガシーソリューションを強化する必要性が高まっていることの証明でもあります。

ZTNAは従来型のVPNに比べて明らかなメリットと幅広い機能を提供しますが、評価が先走りすぎている面もあります。VPNも拡張すれば多くのユーザーを保護できるという現実が忘れられているのです。テクノロジーの過大評価が世代交代を促すことはよくあることですが、VPNから完全に移行することができない、または完全に移行することを望んでいない組織は、それに慌てる必要はありません。

ZTNAは従来のアクセス制御パラダイムよりもきめ細かい制御を提供しますが、VPNを完全に置き換えるわけではなく、VPNとの組み合わせで使用し、多くのユーザーのセキュリティを強化することができます。このような場合組織は、複数のリソースへのよりオープンなアクセスを必要とする一部のユーザーのためにVPNを残しておくことができます。

VPNの置き換えと拡張の先に

前頁でご紹介したのはVPNの課題を解決するためにZTNAを採用する明確なユースケースですが、組織のセキュリティ体制を改善するためのユースケースは他にもいくつかあります。これらのユースケースとメリットは次のとおりです。

コントラクタおよびサードパーティのデバイスからのアクセス

- 安全なアクセス手段を管理されていないデバイスへも拡張
- デスクトップ、ラップトップ、およびモバイルデバイスのサポート

マルチクラウドサポート、単一接続

- 単一の接続ポイントからすべてのアプリケーションへアクセス
- プライベートクラウド、パブリッククラウド、および内部データセンター
- シンプルなエンドユーザーエクスペリエンス

合併/買収時のアクセス

- パートナーリストを管理し、機密文書やアプリケーションへのアクセスを許可
- 個別のネットワークを統合する必要なしにアプリケーションに接続

ZTNAは使用中の環境に適合する必要があります

セキュリティ上の利点は明らかですが、ZTNAはさらにIT、エンドユーザー、およびビジネスからの要求を満たす必要があります。ZTNAを現在のセキュリティスタックとアーキテクチャにどのように適合させるかを決定するためには、次の4つの点を考慮することが大切です。

1. **導入展開** — ZTNAの導入は、IT部門と運用チームに不必要な負担をかけないでしょうか? ZTNAの実装はシームレスで無ければならないため、ソフトウェアクライアントが急増する恐れがあります。それを制御するためには、クライアントレスのオプションが必要です。前項で述べたように、ZTNAの採用において既存のITポリシースタックを破棄して置き換える必要はありません。しかし最終的には、Secure Access Service Edge（SASE）フレームワークのセキュリティコンポーネントであるSecurity Service Edge（SSE）への移行の基盤を構築するものでなければなりません。
2. **セキュリティ** — プライベートアプリケーションへの通信を完全に可視性し、制御できますか? ZTNAは、アプリケーション内の機密コンテンツを保護するために、情報に基づいたデータ中心の制御を行う必要があり、すべてのユーザーの操作をログに記録し、ユーザーの行動とリスクを詳細に可視化して監視しなければなりません。
3. **拡張性** — ZTNAソリューションは、エンドユーザーが業務を行う可能性のある世界中のあらゆる場所で、スケーラブルなパフォーマンスを提供できますか? ZTNAは、世界中のどこからでもアクセスできるようにし、すべての場所にセキュリティを均等に適用できなければなりません。
4. **エンドユーザー** — エンドユーザーが業務上必要とする、重要なプライベートアプリケーションにアクセスするためのソリューションは、直感的で使いやすいですか? ZTNAソリューションは、生産性とセキュリティを妨げるのではなくサポートするように、エンドユーザーに負担をかけないエクスペリエンスを提供する必要があります。

実際の導入展開

ZTNAソリューションには、クライアントレスとクライアントベースという2つのアーキテクチャ的アプローチがあります。各々の実装オプションにはそれぞれの長所と短所があり、現在および将来のニーズと整合させるために慎重に検討する必要があります。

ZTNAの成功とは、どのようなものになるのでしょうか? ネットワークの肥大化や運用コストの増加を避けながらセキュリティ体制を向上させることは、可能でしょうか?

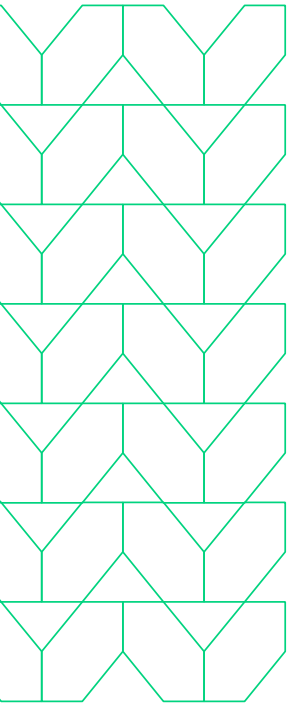
クライアントレスZTNA

クライアントレス（サービス起動型）のZTNAは、ユーザーデバイスにソフトウェアをインストールする必要の無い、ブラウザーベースのソリューションです。クライアントレスはインストールされたソフトウェアへの頻繁なアクセスを必要としないため、本質的にゼロトラストの原則に準拠しているということができます。ほとんどのユーザーはWebブラウザーを介してプライベートアプリケーションにアクセスできるため、クライアントレスのZTNAアプローチは広く適用できます。

クライアントレスZTNAソリューションの中には、リバースプロキシ接続を利用して、ユーザーが閲覧する権限を持たないWebアプリケーションやデータに直接アクセスすることを防ぐものもあります。このような場合、ユーザーは潜在的な危険から分離された「安全なレイヤー」に配置され、管理者にはより優れた管理制御と柔軟性が与えられます。

クライアントレスのメリット：

- エンドポイントにソフトウェアをインストールする必要がなく、エンドポイントが不安定になるリスクも排除できます。
- クライアントの代わりに既存のブラウザーを使用して安全な接続を作成し認証するため、企業全体への導入展開が簡単に行えます。
- Webベースの「アプリケーションダッシュボード」を使用してSaaSアプリケーションへのアクセスを認証するツールが広く普及しているため、エンドユーザーは直感的な操作が可能です。
- 管理対象のデバイスと非管理対象のデバイスのどちらへも、使いやすいWebアプリケーションへのアクセスを提供します。

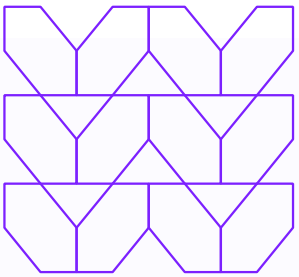


これらのメリットは、デバイスへのアクセスがIT部門の制御の範囲外にある場合など、さまざまなユースケースに適用できます：

合併/買収 — 2つの異質な企業をうまく統合するためには、リソースの可用性と共有が不可欠です。クライアントレスZTNAが無かった頃は、「スイッチの切り替え」や自動同期が使えなかったため、統合作業はIT部門にとって非効率的でコストがかかり、苛立たしいプロセスでした。クライアントレスZTNAはこれらの課題に対するシンプルなソリューションで、ユーザーが必要なアプリケーションに接続するためのポリシーをITが管理することで、ブラウザー経由で迅速にリソースにアクセスできます。

コントラクタおよびサードパーティユーザー — 合併/買収と同様に、IT部門がサードパーティのデバイスを制御することは難しいため、デバイスにエージェントをインストールしてそれを管理することは困難です。クライアントレスZTNAであれば、企業はリスクの増加を心配することなく、重要な資産やアプリケーションへのアクセスを提供することができます。IT部門はコントラクタやサードパーティユーザー専用のポリシーを作成し、アクセスをきめ細かく制御してラテラルムーブメントの可能性を排除することができます。

Bring Your Own Device (BYOD) — BYODの影響で、企業は管理されていないデバイスに悩まされ続けています。クライアントレスZTNAは、そもそもデバイスに対するガバナンスを必要としないため、これらの問題を克服することができます。セキュリティはブラウザーレベルで適用され、ユーザーが管理対象/非管理対象のさまざまなデバイスで業務を行う際でも、セキュリティは柔軟にそれらに追従します。

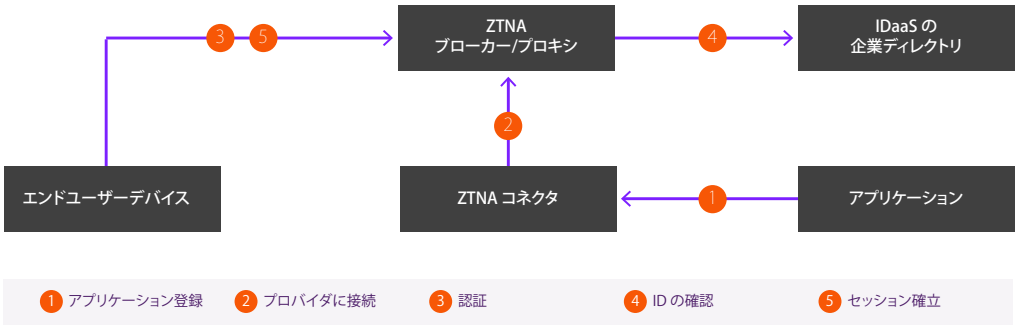


クライアントレスZTNAは、ITチームに負担をかけません

- ITによるソフトウェアの管理は不要です
- 管理対象デバイスと非管理対象デバイスを制御します
- パッチ適用の必要はありません
- 対策やトラブルシューティングが必要となる互換性問題はありません

ほとんどのZTNA製品は、クライアントレスでの導入展開が可能です。しかし、クライアントレスオプションはトラフィックの中間に配備する必要があるため、ベンダーにとってはよりコストがかかります。そのため多くのベンダーは、クライアントベースのアプローチを推奨しています。しかし組織にとっては、大量のエンドポイントにクライアントを導入展開するのは大変で、管理も難しく、アプリケーションに接続した後のセキュリティと可視性も低くなります。

サービス起動型 ZTNA の概念モデル



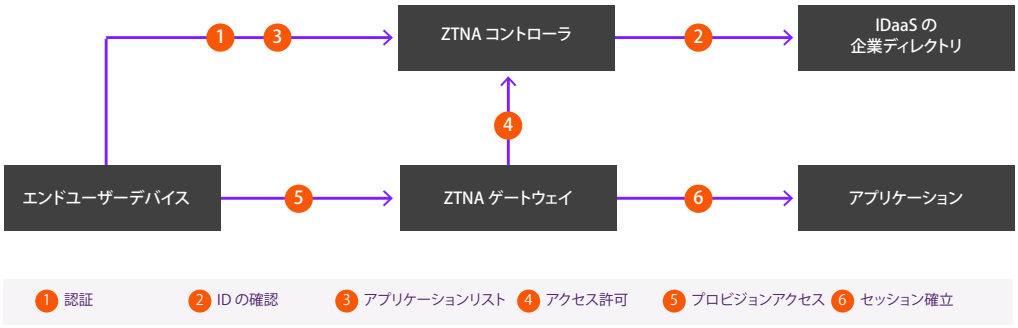
実際の導入展開

クライアントベースのZTNA

クライアントベース（またはエンドポイント起動型）のZTNAは、その名の通り、制御用エージェントと承認されたアプリケーションとの間で暗号化された接続を確立する前に、ユーザーデバイスにソフトウェアをインストールします。クライアントベースの導入展開にあたっては、IT部門がエージェントの導入、設定、パッチ適用、保守を行う必要があり、すでに過負荷になっているIT部門にさらなる責任と運用負担を強いることになります。

先に挙げたクライアントレスZTNAのメリットを考えると、クライアントベースの採用は好ましくない選択に思えるかもしれませんが、それが必要なケースもあります。また、VPN対ZTNAの議論と同様に、多くの組織では、さまざまなニーズに対応するために両方の導入オプションを利用できることが有益であると考えています。

エンドポイント起動型 ZTNA の概念モデル



クライアントベースのメリット：

- HTTP/HTTPSに制限されないため、SSH、RDP、VNC、SMB、その他のTCP接続に依存するアプリケーションなど、幅広い非HTTPアプリケーションにアクセスすることができます。
- カスタムアプリケーションやレガシーアプリケーションを含むすべてのプライベートリソースに対して、ゼロトラストを適用可能です。
- 信頼できるアクセスの基準として、さまざまなデバイスの状態チェックを使用します。

コンパイルエンジンやデータストアのような非HTTPアプリケーションへのアクセスが必要な特定のユーザー（エンジニア等）を除き、ほとんどのユーザーはクライアントレスで対応することができます。

業務を行うすべての場所にポリシーを適用

オンプレミス、プライベートクラウド、パブリッククラウド、SaaSなど、アプリケーションはあらゆる場所に存在します。クラウドベースのZTNAアーキテクチャは、これらすべてに必要なアクセス性とパフォーマンスを提供しますが、それは最低限の要件でしかありません。データセンターを超えて保護を拡大するために、プライベートアプリケーションを含むすべてのユーザーとすべてのアプリケーション間のすべてのトラフィックに対してセキュリティポリシーを適用するメカニズムが必要です。

ZTNAを最大限に活用するためには、そのソリューションが全体的なポリシー管理のための集約されたアクセスポイントとして機能する必要があります。このような広範な管理ができて初めて、物理的な場所、基盤となるインフラ、接続の種類に関係なく、すべてのネットワークトラフィックに確実にセキュリティポリシーを適用することができるのです。

VPNが本質的に許容性が高いのに対し、ZTNAは攻撃者が重大なセキュリティギャップを悪用することを防ぐ為のきめ細かい制御にフォーカスしています。組織のセキュリティ体制を強固にするためには、双方向に「信頼しない」ことが大切です。ユーザーの不正な行動や重要なアプリケーションからのデータの流出を防ぐためには、可視性と制御が双方向に行われる必要があります。

接続 + アイソレーション

ZTNAの登場は、新しいセキュリティ手法の可能性をもたらしました。この多層防御環境では、レガシーなVPNはネットワーク接続のみを提供し、ZTNAソリューションはアイソレーションレイヤーを通じてアクセスとデータを制御し、保護します。

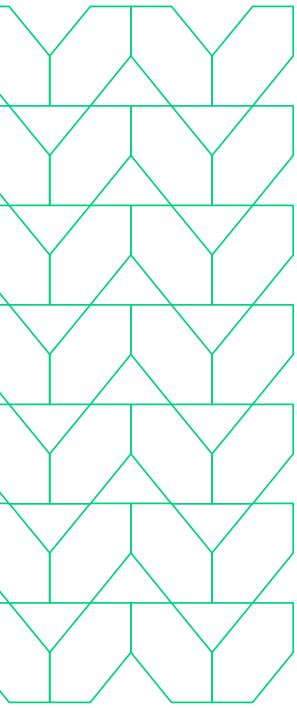
アイソレーションを適用すると、すべてのトラフィックがユーザーやエンドポイントから分離された安全なレイヤーに保持されます。この閉ざされた空間の中で、ZTNAソリューションはデータ漏洩防止（DLP）ポリシーを使ってすべてのトラフィックをスキャンし、悪意のあるファイルをスキャンし、プライベートトラフィックに対して他のリアルタイムポリシーを適用することができます。「許可」か「ブロック」しか選択肢が無く、思ったほど安全ではないVPNとは異なり、ZTNAのアイソレーション機能では、適切な権限を付与して安全に業務を行うことが可能です。単に許可またはブロックするのではなく、アイソレーションによってユーザーが自由に作業できるようにすることで、ユーザーがデバイスを切り替えてセキュリティを回避しようとすることがなくなり、悪意のある試みから完全に保護されます。

きめ細かい制御の例

Jiraユーザーがチケットや案件に添付されたスクリーンショットを閲覧できるように、ヘルプデスク用のポリシーを設定することが可能です。そしてさらに、添付ファイルにリードオンリーの権限を付与するように微調整することで、ユーザーが悪意のあるコンテンツをダウンロードまたはアップロードすることをブロックできます。

可視性とレポート作成

ZTNAソリューションは、セキュリティを適用するために常にトラフィックの経路上にあるため、組織のセキュリティを強固にするだけでなく、より深い可視化と監視機能を提供できます。ZTNAソリューションは、通過するすべてのデータを監視してすべてのユーザーの操作を記録し、ユーザー行動とリスクに関するインサイトを提供してデータ中心の制御に役立てます。ログをSIEMツールに提供してリアルタイムに可視化し、エンドポイントセキュリティと統合して継続的な承認に基づく適応型のブアクセスを実現します。これらの機能により、IT部門は自社環境で何が起こっているかを正確に把握し、規制遵守を証明するレポートを提供し、セキュリティ監査を可能にします。



セキュリティスタックを統合して SSE の基盤を構築

ZTNAの導入が迅速に進んだのは、VPNが機能しないことによる当面の問題を回避する手段だったからです。しかし緊急事態を脱した今は、ZTNAを応急処置として使用するのではなく、より広範な戦略的セキュリティ対策の一環として位置づけを変えるチャンスです。

多くの企業にとって、次の目標はSASEとSSEでしょう。SASEという用語は聞いたことがあると思いますが、SSEはより新しいセキュリティ用語で、SASEのセキュリティ機能を絞り込み、ネットワークに関するガイダンスを削除したものです。具体的には、Web、クラウドサービス、プライベートアプリケーションへのアクセスを保護することに重点を置いています。

SSEは主にクラウドベースのサービスとして提供され、アクセスコントロール、脅威防御、データセキュリティ、モニタリング、ネットワークベースとAPIベースの統合による使用許可の制御などの機能を備えています。

将来も利用可能なセキュリティスタック

SSEとSASEの中心的なテーマは、セキュリティは現在の業務からの様々な要件に容易に適応できるべきであるということです。働く場所がデータセンターの外に広がり、アプリケーションが複数のクラウドやデータセンター環境でマイクロサービスに分割され続ける中、SSEは基盤となるインフラに関係なく、ユーザー、アプリケーション、データを追跡することでクラウドへのシフトを支援します。そしてユーザーからアプリケーションへのアクセスを仲介するZTNAは、SSEとSASEを実現し、基本的なテーマを満たすための基盤的な役割を担っています。

すべてがオンプレミスで行われていた時代には、セキュリティは各々のツールがそれぞれの役割を担い、サイロ化する傾向がありました。分散型アーキテクチャの現在では、SSEによってすべてのセキュリティ機能が統合され、管理しやすいプラットフォームで集中管理、可視化、レポート作成が可能になるため、組織はセキュリティを向上させることができます。しかし、これは守らなければならない「レシピ」ではなく、大枠を決める「フレームワーク」であるため、含まれるべきすべてのテクノロジーを指定するものではありません。

SSEのビジョンは、機能を集約しデータフローを緊密に統合することで企業のコアテクノロジーを統合するというものです。ZTNAソリューションはスタンドアロンなツールではなく、セキュアWebゲートウェイ（SWG）、ファイアウォール、DLP、Cloud Access Security Broker（CASB）、Security Operations Center（SOC）、アイソレーションなどの既存および計画中のセキュリティスタックとシームレスに統合される必要があります。

SSE と ZTNA の提供

SSEを利用してデジタルとクラウドの両方のトランスフォーメーションを推進するためには、ビジネスの俊敏性を実現することが重要です。ZTNAのセキュリティは、生産性の妨げになったり既存および将来のアーキテクチャを複雑化させたりするものであってはなりませんし、そうすることもできません。SSEへの進化に向けた計画を立てる際には、クライアントレス・アーキテクチャと、アプリケーションが必要とするときにエージェントを導入展開できるオプションの両方を備えたZTNAソリューションを探すことが大切です。

ZTNAを導入するためのシンプルなソリューション

ZTNAを主にアクセス制御の手段として導入する場合でも、SSEに向けたより戦略的なステップとして導入する場合でも、メンロ・セキュリティはそれをシンプルに実現します。Menlo Private Access（MPA）を使用すれば、攻撃者の標的となる攻撃対象を大幅に拡大することなく、分散した従業員やサードパーティへの自由なアクセスを実現することが可能です。

MPAはクライアントレス・ファーストのアプローチを採用しており、ほとんどのユースケースにおいて、エンドポイントデバイスにエージェントを導入することなく、ユーザーとアクセス権限のあるアプリケーションの間でシームレスなアクセスを実現します。特定のユーザーグループやアプリケーションにエージェントが必要な場合、MPAはそのニーズに合わせてエージェントベースの導入展開も可能な柔軟性を備えています。

メンロ・セキュリティにより、従来のVPNインフラに依存することなく、あらゆるエンタープライズアプリケーションへの高速かつ安全でシームレスなアクセスが可能になります

メンロ・セキュリティのすべてのソリューションの中心にあるのがIsolation Core™で、アプリケーションやサービスを公衆のインターネット上で直接視認できないようにするものです。メンロ・セキュリティのIsolation Core™を活用するMPAは、プライベートアプリケーションに直接アクセスするのではなく、アプリケーションとエンドポイントデバイスの間にコントロールポイントを作成します。そうすることで、攻撃者がアプリケーションに直接アクセスする可能性を排除します。さらにIsolation Core™は、パラメータの改ざん、Webスクレイピング、APIの不正使用、および他のZTNAソリューションでは対処できないその他の多くの問題からアプリケーションを保護します。

Menlo Private Access のメリット

アプリケーションを横断した不正アクセスの可能性を最小化 — MPAは、ユーザーが業務に必要なアプリケーションのみにアクセスできる、直感的なゼロトラストアクセスを可能にします。アクセスは動的に評価され、ユーザーがどのデバイスから接続しているか、どのネットワークから接続しているか等の主要なデータポイントに応じて制御することができます。

無制限のグローバルなスケーラビリティ — MPAはクラウドベースのスケーラブルでセキュアなアクセスソリューションで、組織が持つレガシーなVPNを補強あるいは置き換えることができ、より優れたユーザー体験を提供し、セキュリティを向上させます。

セキュリティ成果の向上 — MPAはメンロ・セキュリティのIsolation Core™上に構築されており、きめ細かいアプリケーションアクセスを可能にします。アプリケーションへの完全なアクセスを提供するだけでなく、ユーザーにアプリケーションへの読み取り専用のアクセスを許可したり、アプリケーションへのアップロード/ダウンロードをブロックしたりすることも可能です。

将来も利用可能なセキュリティ — MPAはメンロ・セキュリティのSWGおよびCASBと直接統合されており、SSEへの移行を容易にし、効率化、コスト削減、リスク低減を実現します。

ユーザーの業務を保護するためにどのようにMPAとZTNAを導入すれば良いのかについてはmenlosecurity.com/ja-jp/をご確認下さい。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com

Menlo Securityについて

メンロ・セキュリティは、他に類を見ないアイソレーションを活用したクラウドセキュリティプラットフォームにより、企業が脅威を排除し、生産性を完全に維持することを可能にします。メンロ・セキュリティは、悪意のある攻撃を防ぐために最も安全なゼロトラストアプローチを提供し、エンドユーザーはセキュリティの存在を気にせずにオンラインで仕事をすることができ、さらにセキュリティチームの運用負担を軽減することで、クラウドセキュリティの目標を実現できる唯一のソリューションとなっています。これにより企業は安全なオンライン体験を提供することができ、ユーザーは安心して業務を行いビジネスを進めることができます。