paloalto NETWORKS | PRISMA BY PALO ALTO NETWORKS

効果的な SASE ソリューションの 10 の原則

目次

はじめに

新型コロナウイルス感染症の拡大に伴い変化した企業運営のあり方は、もはや過去に戻ることはありません。急増するリモート ワーカーが自宅から必要なサービスやアプリケーション、そしてデータにアクセスするため、組織はネットワーク接続が途切れることがなく、セキュリティも確保されたものへと変革するために取り組んでいます。

組織は感染症が拡大する前から、レガシー技術がもたらす課題を抱えていました。進化し続けるトラフィックの種類とセキュリティの脅威に対処することが、非常に難しくなっていたのです。ビジネス要件の変化に対処するため、ファイアウォール、セキュア Web ゲートウェイ (SWG)、クラウド アクセス セキュリティ ブローカー (CASB) ソリューション、ソフトウェア定義型広域ネットワーク (SD-WAN) などの、さまざまなポイント製品を取り入れていかざるを得なくなっていました。そのような中で従来の課題にさらなる追い打ちをかけたのが、今回の感染症の拡大でした。企業はプライバシーとセキュリティを確保しながら、世界的なリモート ワークの導入の動きに迅速に対応する必要がありました。

セキュア アクセス サービス エッジ (SASE) は、2018 年に誕生した概念です。Gartner が提唱した SASE(「サシー」と発音)は、ネットワーク サービスとそのセキュリティを共通のクラウドアーキテクチャから提供し、組織がクラウドとモビリティを最大限に活用できることを目的としています。SASE ソリューションでは、一貫したセキュリティ サービスを提供するとともに、あらゆる種類のクラウド アプリケーション (パブリック クラウド、プライベート クラウド、SaaS など) に共通のフレームワークからアクセスできるようにする必要があります。

組織では、複数のポイント製品を使用するのではなく、単一のクラウド型 SASE ソリューションを導入することで、複雑さを軽減し、リモート ワーカーや支社を迅速に配置および拡大して、あらゆる場所のユーザーに一貫したセキュリティを適用できるようになります。しかも、技術、人、資金といったリソースを削減しながら、これらすべてを実現できるのです。

この e ブックでは、効果的な SASE を実現するための 10 の原則について解説します。

原則 1: ソフトウェア定義型広域ネットワーク

問題点

企業各社では、支社を会社のネットワークに接続し、ローカルのインターネット ブレイクアウトを提供するための手法として、コストのかかるマルチプロトコル ラベル スイッチング (MPLS) 接続に代わる、ソフトウェア定義型広域ネットワーク (SD-WAN) の採用が進んできました。しかし、従来の SD-WAN ソリューションは数多くの問題をもたらしています。伝統的なパケット ルーティング モデルを採用し、クラウドへの対応が済んでいる企業にそのモデルを無理やり適用させようとしているからです。さらに従来のソリューションはスケーリングが難しく、ネットワーキングや可視化などの支社向けのサービスを追加する必要もあるため、コストと複雑性は増すばかりです。

SASE の方策

SASE ソリューションの場合、ブランチ アーキテクチャは完全なクラウド型となります。組織ではセキュリティやネットワーキングなどの支社向けのサービスを有効化して、完全にクラウドから提供できるようになるため、WAN の管理を簡素化して投資収益率 (ROI) を向上させることができます。

重要なポイント

SD-WAN を簡素化するには、SASE のような、クラウド型の自律したソリューションを検討する必要があります。アプリケーションの可視性を高めて、SaaS、クラウド、Unified Communications as a Service (UCaaS) をはじめとするアプリケーションの SLA を策定するには、パケットベースではなくアプリケーション定義の SD-WAN であることが必要です。さらに SASE はネットワーキングとセキュリティを集約するソリューションであるため、効果的な SASE ソリューションは、複数ベンダーの異種製品を組み合わせる他のアプローチとは異なり、一貫性のある各種ポリシーを備えた統合 SD-WAN を包括的プラットフォームの一部として提供する必要があります。

「2020 年の時点で、ソフトウェア定義型広域ネットワーク (SD-WAN) を利用している顧客の約 35% がセキュア アクセス サービス エッジ (SASE) を導入済みです。この数は 2024 年までに 60% 以上に達するでしょう」

2020 年の Gartner マジック クアドラント (WAN エッジ インフラストラクチャ部門)

原則 2: ゼロ トラスト ネットワーク アクセス

問題点

企業では依然として、ユーザーとデータの安全を維持するのに必要なセキュリティ保護機能やポリシーを備えることができていません。ゼロ トラスト ネットワーク アクセス (ZTNA) では、アプリケーションに接続しようとするユーザーは最初にゲートウェイ経由で認証を受けないとアクセス権を得られません。これによって、セキュリティ管理者がユーザーを識別してポリシーを作成できるようになり、アクセスの制限、データ損失の最小化、潜在的な脅威の迅速な軽減が実現されます。

多くの ZTNA 製品はソフトウェア定義の境界 (SDP) アーキテクチャに基づいていますが、このアーキテクチャではコンテンツ インスペクションが行われないため、各アプリケーションで利用可能な保護の種類に不一致が生じます。一貫した保護を提供するには、ZTNA モデルに追加の制御を定義して、すべてのアプリケーションのすべてのトラフィックを対象とする検査を確立しなければなりません。

SASE の方策

SASE は ZTNA の基本方針に基づいており、その方針を SASE ソリューション内の他のすべてのサービスに適用しています。ユーザー、デバイス、アプリケーションを接続元に関係なく識別できるため、ポリシーの作成と管理が簡素化されます。SASE では、複数のネットワーキング サービスが単一の統合クラウド フレームワークに組み込まれるため、ゲートウェイへの接続に伴う複雑さはありません。

重要なポイント

SASE ソリューションは、データ損失防止 (DLP) と脅威防御のポリシーを一貫して適用するために、アプリケーションの保護を目的とした ZTNA を組み込みつつ、その他のセキュリティ サービスも提供する必要があります。これは、アクセス制御自体はユーザーを証明する手段として役立つものの、ユーザーの行動やアクションが組織に被害をもたらさないことを確認するには、他のセキュリティ制御も必要になるためです。また、これらの制御をすべてのアプリケーションへのアクセスに拡張する必要もあります。

「多くの企業は、従業員が使用しているアプリを規制していません。未承認アプリのインストールを AUP で禁止している企業はわずか 62% でした」

Verizon Mobile Security Index 2020 レポート

原則 3: クラウド アクセス セキュリティ ブローカー

問題点

多くの組織が、クラウド アクセス セキュリティ ブローカー (CASB) を使用して、データの場所を可視化し (SaaS アプリなど)、ユーザー アクセスに企業ポリシーを適用して、ハッカーからデータを保護しています。CASB は、SaaS プロバイダおよび従業員用のゲートウェイを提供する、クラウドベースのセキュリティ ポリシー適用ポイントです。

SASE の方策

統合プラットフォームを構築して、あらゆる種類のアプリケーションに対応するセキュリティ制御を関係者が管理できるようにするには、CASB のセキュリティ サービスも SASE ソリューションに組み込む必要があります。SASE ソリューションを使用することにより、ユーザーのいる場所に関係なく、現在使用中の SaaS アプリケーションとデータの送信先を把握できるようになります。

重要なポイント

SASE ソリューションでは、インライン制御と API ベースの SaaS 制御の両方を組み込んで、ガバナンス、アクセス制御、データ保護を実現する必要があります。優れた可視性、管理性、セキュリティ、新たに出現する脅威に対するゼロデイ保護を提供するには、コンテキスト制御に加えてインラインと API ベースのセキュリティを SASE に組み込む必要があります。この組み合わせはマルチモード CASB とも呼ばれます。

原則 4: サービスとしてのファイアウォール

問題点

物理ファイアウォールまたは仮想ファイアウォールは、本社、支社、データ センター、クラウドなど、アプリケーションやユーザーが存在するあらゆる場所に必要です。あらゆる場所でユーザーとアプリのリモート化が急速に進み、無数のファイアウォールを管理しなければならなくなったことが、組織に大きな負担を強いています。サービスとしてのファイアウォール (FWaaS) は、ファイアウォール機能をクラウドベース サービスとして提供できるよう導入するための手法であり、優れた FWaaS サービスは次世代ファイアウォールと同等の機能を提供することができます。

SASE の方策

SASE ソリューションの統合プラットフォームには FWaaS が組み込まれており、次世代ファイアウォールと同等のサービスがクラウド型のサービスとして提供されます。FWaaS サービス モデルを SASE フレームワークに含めることによって、組織では単一プラットフォームで簡単に導入を管理できるようになります。

重要なポイント

SASE ソリューションでは、ネットワーク セキュリティ ポリシーをクラウドに実装することによって、次世代ファイアウォールの保護機能と同等の FWaaS 機能を実現する必要があります。SASE ソリューションから提供される機能が、基本的なポート ブロックや最低限のファイアウォール保護だけにならないようにすることが重要です。次世代ファイアウォールに搭載されているのと同じ機能に加え、脅威防御サービスや DNS セキュリティなどの、クラウドベースのセキュリティで提供される機能が必要になります。

「2020 年現在、新たに展開された支社でのファイアウォールの導入において FWaaS が占める割合は最大 5% ですが、2025 年までには 30% が FWaaS に切り替わるでしょう」

2020 年の Gartner マジック クアドラント (ネットワーク ファイアウォール部門)

原則 5: セキュア Web ゲートウェイ

問題点

組織では、悪意のある Web サイトや不適切な Web サイトに従業員やデバイスがアクセスすることのないよう保護するために、セキュア Web ゲートウェイ (SWG) が使用されています。DNS セキュリティを備えた SWG を使用することで、不適切なコンテンツ (ポルノ、ギャンブルなど) や、組織の方針で業務中の閲覧を禁じている Web サイト (Netflix に代表される配信サービスなど) をブロックできます。ただし SWG は個別のアプライアンスやサービスとして提供されるため、職場やリモートで作業中のユーザーに一貫したポリシーを適用できなくなります。

SASE の方策

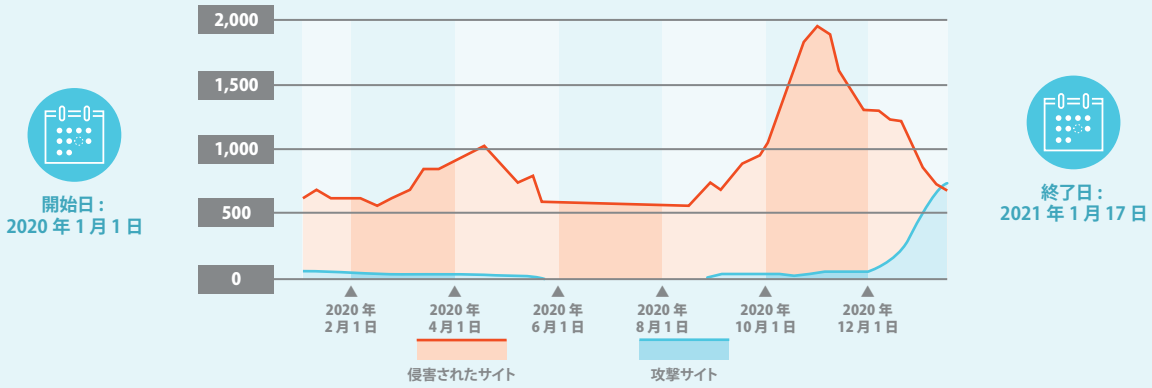
SWG は、SASE ソリューションで提供する必要のある数多くのセキュリティ サービスの 1 つにすぎません。SASE プラットフォームが提供するクラウド SWG が、ネットワーク全体にわたる完全な可視化と統制を提供することで、ユーザーはどこにいても、クラウドベース アプリやその他の Web サービスを安全に利用できるようになります。また、組織の拡大とリモート ユーザー数の増加に合わせて自動的にスケーリングできるため、SASE のクラウド SWG は組織の成長を後押しする存在になります。

重要なポイント

SASE ソリューションには従来の SWG と同等のセキュリティ サービスが含まれているため、組織は Web へのアクセスを制御し、セキュリティ ポリシーを適用して敵対的な Web サイトや不適切なコンテンツからユーザーを保護することができます。DNS セキュリティと明示的なプロキシが融合された SWG は、組織による SASE アーキテクチャへの移行を支援するシンプルなオンボーディング機構を提供します。

Google 透明性レポート : マルウェアのホスティングが確認されたサイト (2020 年 1 月～ 2021 年 1 月)

https://transparencyreport.google.com/safe-browsing/overview?hl=en



原則 6: デジタル エクスペリエンス モニタリング

問題点

ユーザー エクスペリエンスは、従業員の満足度や生産性を高めるために非常に重要です。場所を選ばない働き方を従業員が求めるようになった現在、デジタル エクスペリエンスは必要不可欠です。その中でネットワークやデバイス側のモノの可視化という難題に取り組む IT チームは、大きな労働力を要する手動のトラブルシューティング作業による問題解決を余儀なくされています。

SASE の方策

Autonomous Digital Experience Monitoring (ADEM) が提供するエンドツーエンドの可視性と洞察を、シームレスなデジタル ユーザー エクスペリエンスの構築に役立てることができます。SASE に組み込まれた ADEM が提供する、サービス配信パス全体を対象としたセグメント単位の洞察により、組織では実トラフィックと合成トラフィックの分析を行って、デジタル エクスペリエンスの問題が発生した場合でも自律的な修復を実行できます。

重要なポイント

従業員が場所を選ばない働き方をするようになった現在、ユーザー エクスペリエンスの最適化は欠かせません。ユーザーと IT チームの両方にメリットをもたらすには、SASE ソリューションに ADEM を組み込むことで包括的な可視性と自動修復を実現し、エンドポイント デバイス、Wi-Fi、ネットワーク パス、アプリケーションのパフォーマンスに関する詳細な洞察を得られるようにする必要があります。

「2025 年には IT リーダーに、社内での技術関連の取り組みの 70% に対して、ユーザー エクスペリエンス指標の報告義務が課せられるようになります。Gartner の調査では、この割合は 2019 年はわずか 15% にとどまっています」

デジタル エクスペリエンス モニタリングに関する 2020 年の Gartner マーケット ガイド

原則 7: 脅威防御

問題点

ランサムウェアの攻撃が毎日発生するなど、大小さまざまな規模の侵害が発生する昨今の状況において、組織のデータと従業員を保護するための鍵となるのが脅威防御です。マルウェア対策から侵入防御、ファイル ブロックまでさまざまな脅威防御ツールが提供されており、組織はこれらを使用して脅威を阻止できます。ただし、こうしたポイント製品が必要とするソリューションがそれぞれ異なることで管理や統合が難しくなり、脅威の特定と対応にかかる時間も長くなりすぎてしまう場合がほとんどです。

SASE の方策

SASE ソリューションでは、このようなポイント製品やサービスがすべて単一のクラウド プラットフォームに統合されます。これにより、ネットワークとクラウド環境全体にまたがるすべての脅威や脆弱性の管理と監視が簡素化されます。SASE には機械学習機能を組み込む必要があります。これにより、未知の脅威をほぼリアルタイムで防御できるだけでなく、可視性とセキュリティを、未知の IoT デバイスをはじめとするあらゆるデバイスに提供できるようになります。

重要なポイント

従業員とデータを保護するには、最新の脅威インテリジェンスを使用してエクスプロイトやマルウェアを阻止することがとても重要です。脅威に迅速に対応して修正を行えるようにするため、SASE ソリューションのフレームワークに脅威防御ツールを組み込む必要があります。また、ファイルベースや Web ベースの未知の脅威を瞬時に阻止するため、インライン機械学習を組み込む必要もあります。さらにポリシーの自動推奨機能があれば、時間を節約して人的ミスが発生する余地を減らすことができます。

脅威の検出と対応の難易度が昨今上昇した理由

ESG Master Survey Results: The Threat Detection and Response Landscape

原則 8: モノのインターネット

問題点

多くの組織では、モノのインターネット (IoT) デバイスが管理されないまま企業ネットワークに接続されています。そして、そのことがセキュリティ ギャップをもたらしています。こうしたデバイスは脆弱性を抱えていることが多く、更新ファイルのインストールもユーザー頼みで、IT チームがアクセス先を十分に把握できるほどの可視性もないからです。高額な IoT のセキュリティ センサーやアプライアンスでも、提供されるソリューションは限定的であり、業務上の非効率性や課題が生じます。

SASE の方策

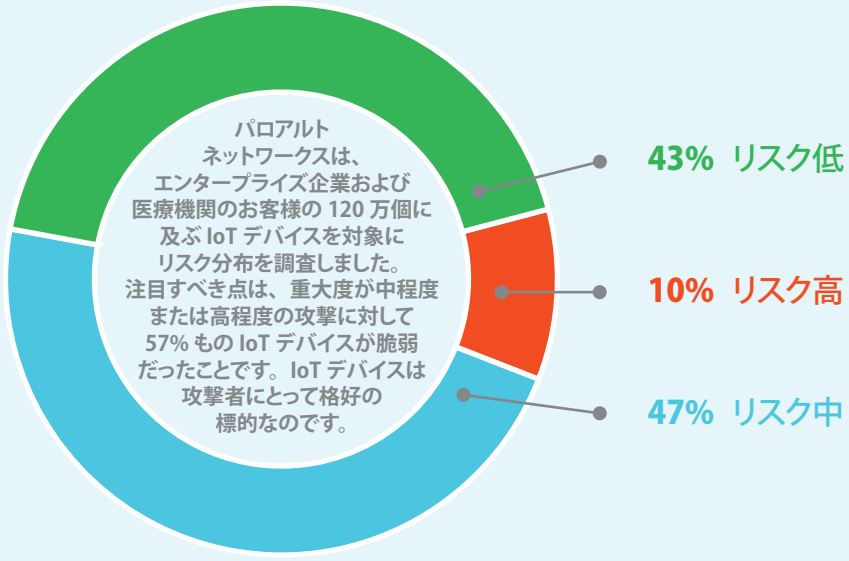
SASE では IoT セキュリティをプラットフォームに統合し、リモートの支社、拠点、作業者に対する保護をクラウドから提供する必要があります。また、クラウドを利用することで、デバイスを正確に検出して完全な可視性をもたらし、ポリシーを適用してネットワーク全体のセキュリティを確保することができるため、IoT セキュリティ ソリューションを追加する必要がなくなります。

重要なポイント

従来の技術が次世代の技術へと転換を遂げる中、スマート サーモスタットやスマート照明システムなどの IoT デバイスの導入が多くの組織で進んでいます。企業ネットワークに接続しているときに保護する必要のあるデバイスは、もはやスマートフォン、スマートウォッチ、ノート PC だけではありません。組織の自律性を高めて、脅威の特定と修正を瞬時に実行するために、SASE ソリューションには機械学習と AI が組み込まれている必要があります。

「IoT デバイスの 57% は重大度が中程度または高程度の攻撃に対して脆弱です。IoT デバイスは攻撃者にとって格好の標的なのです」

2020 年の Unit 42 IoT 脅威レポート (Palo Alto Networks)



原則 9: データ損失防止

問題点

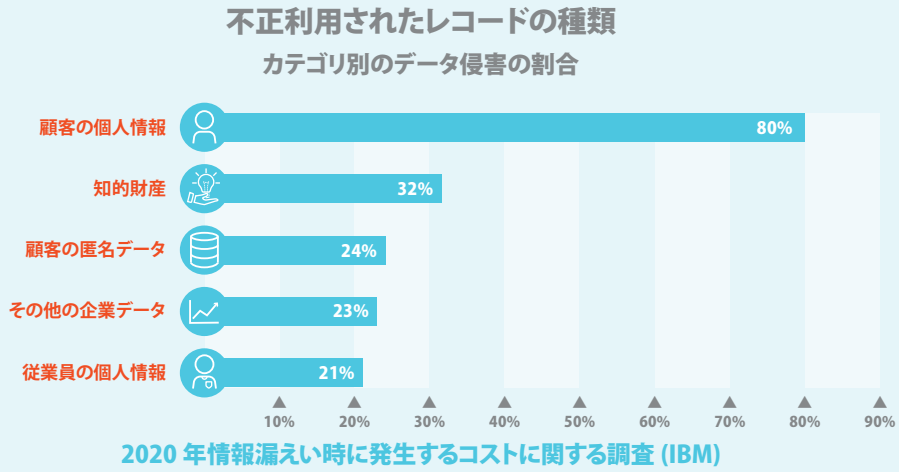
data loss prevention(データ損失防止 - DLP) ツールは、機密データを保護し、データの損失、盗難、悪用を確実に防ぎます。DLP は、DLP が導入された環境内 (ネットワーク、エンドポイント、クラウドなど) のデータと出口ポイントを通過するデータを監視する複合ソリューションで、ポリシーが侵害されると、主要な関係者にも通知が届きます。DLP は、HIPAA、PCI DSS、GDPR などが定めるコンプライアンス要件への対応に欠かせない、データ セキュリティとコンプライアンスに必要な非常に重要なソリューションです。従来の DLP の核となっているのは、当初はオンプレミスの境界用に設計され、その後クラウド用途のために拡張および適応された、旧式の技術です。こうした DLP は、数多くの機能、一貫性を欠くポリシー、設定、回避策が混在することで非常に複雑化しており、大規模な導入が難しく、コストも非常にかかります。デジタル トランスフォーメーションを実現して新しいデータ使用モデルに移行するには、データ保護のアプローチを刷新しなければなりません。

SASE の方策

SASE のアプローチにおける DLP は、データそのものに軸を置いた単一のクラウド型ソリューションとして、あらゆる場所に適用されます。休止中、移動中、使用中の機密データに対して、同じポリシーがデータの場所に関係なく適用されます。SASE アーキテクチャにおける DLP はもはやスタンドアロンのソリューションではなく、組織の既存の制御ポイントに組み込まれるため、複数のツールを導入、管理する必要がなくなります。SASE では、拡張性に優れたシンプルなアーキテクチャを使用して、組織の念願だった包括的なデータ保護ソリューションを実現することができます。さらにグローバル トラフィックへのアクセスを利用することで、効果的な機械学習も実現できます。

重要なポイント

DLP は、組織全体での機密データの保護とコンプライアンスの確保に欠かせないツールです。そうした目的を達成するには、SASE ソリューションに DLP のコア機能が含まれている必要があります。DLP は SASE にクラウド型のサービスとして組み込まれ、ネットワーク、クラウド、ユーザーなど、あらゆる場所の機密データを正確に、一貫して特定、監視、保護します。



原則 10: プラットフォームの拡張性

問題点

多くの組織がクラウドへの移行を進めていますが、異なるベンダーが提供する複数のクラウドベース サービスを追加、統合することで複雑さが増す可能性があります。たった 1 つであらゆる課題をすべて解決できるようなツールを見つけることは難しいため、複数のソリューションを相互に連携させて、セキュリティ ギャップをなくすことが重要になります。ただし残念ながら、サードパーティのサービスとスムーズに統合できるよう設計されたクラウド ソリューションは必ずしも多くなく、ベンダーは往々にして統合に取り組む組織を積極的に支援しようとはしません。

SASE の方策

SASE ソリューションでは、サードパーティのサービスと簡単に統合できるプラットフォームを提供して、それらのサービスとの統合と、管理者のプロセスの簡素化を実現する必要があります。統合可能なプラットフォームがあれば、組織は SASE プロバイダの全面的なサポートを得ながら、サービスを簡単に追加することができます。

重要なポイント

拡張性に優れた SASE ソリューションがあれば、組織はプラットフォームにサービスを簡単に追加して、考えられるすべての使用例に対応できるようになります。ポイント ソリューションを相互に統合できないという阻害要因が解消されれば、組織は既存のサードパーティのサービスで能力と機能を強化してニーズを満たせるようになります。

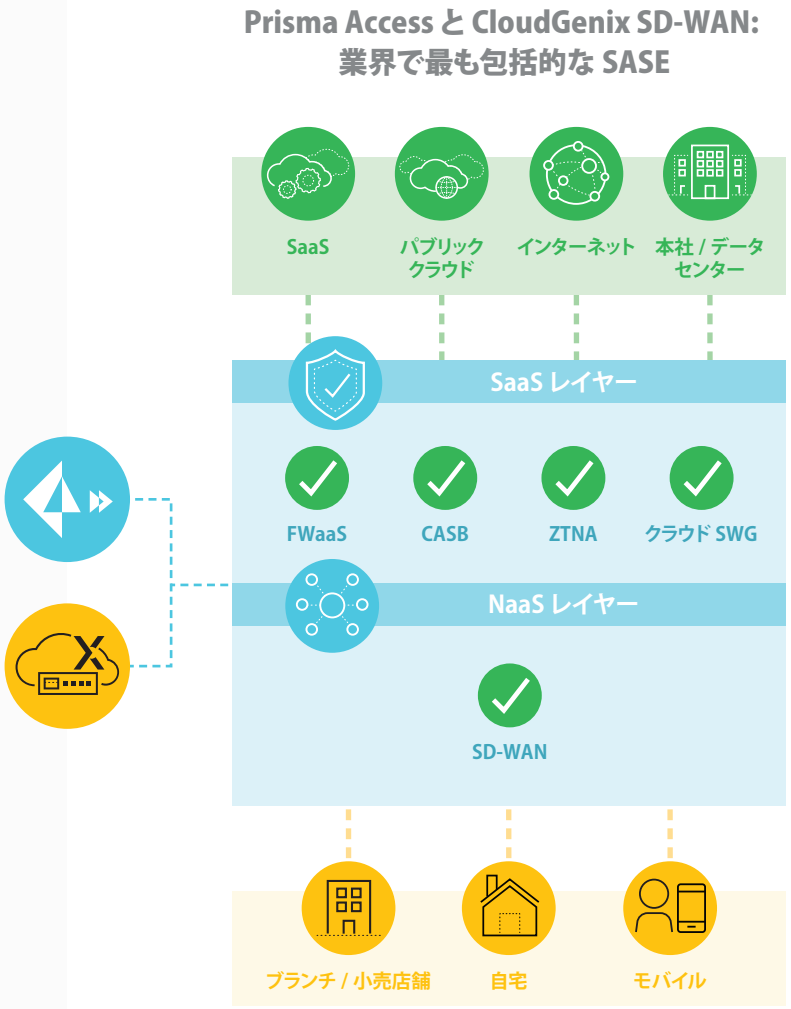
「セキュリティとリスク管理のリーダーは、SWG、CASB、DNS、ZTNA、リモート ブラウザ分離の機能をベンダー 1 社に移行させて、複雑さを低減する必要があります」

2019 年 The Future of Network Security Is in the Cloud(Gartner)

パロアルトネットワークスによるサポートのアプローチ

パロアルトネットワークスは、Prisma® Access および CloudGenix® SD-WAN 製品を通じて、業界最高水準の包括性を備えた SASE ソリューションを提供します。Prisma Access は、クラウド型のセキュリティによってサイバー攻撃を阻止するだけでなく、あらゆるアプリケーションのすべてのトラフィックを、すべてのポート上で一貫して保護します。CloudGenix SD-WAN は、ネットワークおよびセキュリティ運用の簡素化と、優れたユーザー エクスペリエンスの提供を機械学習と自動化によって実現する、業界初の次世代 SD-WAN ソリューションです。

Prisma Access と CloudGenix SD-WAN を緊密に統合させることで、リモート ユーザーとブランチ拠点に幅広いセキュリティと接続性を確実に提供しながら、組織のリモート ワークを推進できるようになります。Prisma Access では、ポイント製品につきものの単一目的のテクノロジ オーバーレイを作成するのではなく、クラウドベースの共通インフラストラクチャを使用して複数の種類のセキュリティ サービスを提供します。さらに CloudGenix SD-WAN との連携により、複数のネットワーキング サービスを融合して 1 つの包括的なソリューションを提供できます。さらに、パロアルトネットワークスと数百のサードパーティ フィードから自動収集される脅威データで構築された、包括的な脅威インテリジェンスを活用できます。



おわりに

組織のリモート ワーク化がますます進みクラウド移行も加速する中、ネットワーキングとネットワーキング セキュリティのニーズを包括的な SASE ソリューションで解消する手法は、検討に値する有力な選択肢だと考えます。セキュア アクセス サービス エッジがビジネス戦略にもたらす最大のメリットを 3 つ示します。

1

管理とオペレーションを簡素化できる

- ネットワーキング機能とネットワーク セキュリティ機能を単一のクラウド型サービスに集約し、単一のコンソールから管理できる。
- ブランチ拠点のデプロイメントや継続的管理を自動化できる。
- 機械学習とデータ サイエンスの手法を使ってネットワーク運用を簡素化し、ネットワーク トラブル チケットを削減できる。

2

スケーリングとパフォーマンスに制約がない

- クラウドネイティブのアーキテクチャを活用して、100 以上の拠点で構成されるグローバル ハイパフォーマンス ネットワーク上で柔軟にスケーリングできる。
- ブランチ サービスをクラウドから提供することで、WAN 管理を簡素化し最大 243% の ROI を実現できる。
- レイヤー 7 のアプリケーション定義インテリジェンスで、詳細な可視性、きめ細かいポリシー、的確なパス判定を実現できる。

3

優れたユーザー エクスペリエンスを届けられる

- ユーザーの場所に関係なく、一貫性のあるセキュリティとコンプライアンスを維持できる。
- クラウド、SaaS、UCaaS を含むすべてのアプリの SLA を達成できる。

ネットワーク全体を包括的に可視化し、強力な保護機能とパフォーマンスを単一の統合クラウド型プラットフォームで提供できる SASE ソリューションこそ、確かな成果を得られる SASE ソリューションだと言えます。

パロアルトネットワークスの SASE 製品についてはこちらをご覧ください： Prisma Access • CloudGenix SD-WAN

〒 100-0011
東京都千代田区内幸町 2 丁目 1 番 6 号
日比谷パークフロント 15 階
電話番号 : 03-6205-8061
www.paloaltonetworks.jp