次世代ネットワーク セキュリティの 購入基準

次世代ネットワーク セキュリティの購入基準

はじめに

今日の攻撃者は進化を続けており、対抗するための防御策が追いついていないのが現状です。攻撃を分かりにくくしたり悪意のあるコードを Web ページなどのファイルに隠したりすることで、正規のネットワーク トラフィックのプロファイリングと特定をますます困難にしています。状況は良くなるどころか悪化しています。攻撃側はアジャイル開発やテストの採用により、攻撃防止のためのネットワーク セキュリティ デバイスの多くをマルウェアに回避させるようにまでなりました。このため、従来の境界セキュリティ アーキテクチャでは不十分となり、セキュリティ向上を追求し、ネットワークに侵入する脅威にフォーカスする必要があります。

境界アーキテクチャの多くは、保護やポリシーがポートやプロトコルに限定された第 1 世代ネットワーク セキュリティ デバイスにより構成されます。比較的新しい次世代ファイアウォール（NGFW）では、従来のようにポートやプロトコルの保護に限定されないまでも、アプリケーションの利用を重視するあまり、脅威防御がおろそかになっている場合が少なくありません。

こうした弱点を補うものとして、ネットワーク セキュリティ デバイスや NGFW のサプライヤの多くが、従来の侵入防御システムのほか、さまざまな非統合型の製品を追加で提供してきました。しかし、それでは巧妙な攻撃や高度なマルウェアが及ぼすリスクに対応できません。このようなソリューションは通常、感染を把握して封じ込め、迅速に修復するための機能を備えていないため、いったん感染してしまうと、役に立ちません。

こうした背景から、総合的なコンテキスト認識とネットワーク トラフィックの詳細な分析を実現するきめ細かいアクセス制御と多層的な脅威保護を 1 つにまとめた、次世代ネットワーク セキュリティ デバイスが登場しました。これらのデバイスでは、網羅的なコンテキスト認識とセキュリティの自動化により、現代の流動的な IT 環境やネットワークの高速化、そして高度な脅威への対応に必要な、可視性と俊敏性を実現しています。

次世代ネットワーク セキュリティではさらに、ネットワーク トポロジ、脅威、レピュテーション データを関連付ける機能も必要です。また、使用中のアプリケーション、アプリケーションを使用している従業員（またはグループ）、セッション内のコンテンツ（ファイル タイプ）、および、セッション内に疑わしい挙動がないかなどに基づいて、セキュリティ ポリシーを適用できる必要があります。脅威防御に対して統合的なアプローチを提供する次世代ネットワーク セキュリティ デバイスには、ますます高度化する攻撃に、単一のビューと管理プラットフォームで対応できるツールが搭載されています。一連の攻撃全体（攻撃前、攻撃中、攻撃後）に対してより安全に保護できるだけでなく、既存のセキュリティ投資も最大限に活用できます。

次世代ネットワーク セキュリティの本バイヤーズ ガイドでは、次世代セキュリティ ソリューションを検討すべき理由を詳しく解説しています。ネットワーク セキュリティ機器に求められる最も重要な機能を分析し、購入に必要な知識を取り入れることで、現時点では実装困難な未来の機能をマーキテクチャのもとに詰め込んだ製品に惑わされずに、本当に必要なものを入手できます。

次世代セキュリティ推進の背景

テクノロジーの革新

組織が従業員にテクノロジーを提供する方法は、根本的な変化を遂げています。社内ネットワークの内外で、モバイル デバイスによる重要データへのアクセスを許可することは、もはや目新しいことではなく、当たり前のこととなりました。組織は導入時間の短縮とコスト削減のため、戦略的な外部委託と Software as a Service の導入を推進しています。しかし、そのために企業データがインターネット上に拡散し、社内のセキュリティ チームの目や手の届かないところに行ってしまいがちです。

同時に、仮想化とクラウド コンピューティングは、データセンターの構築やデータ保管場所のあり方を根本的に変化させ、重要データの保護が一層困難になりました。こうした変化が激しくモバイル性の高い、動的な分散コンピューティング環境において、可視性、制御、脅威対策を提供する必要性は増しています。

このような状況では、十分なセキュリティの実現は困難を伴います。以下のような制限を持つ第 1 世代ネットワーク セキュリティ ツールを考慮する場合はなおさらです。

- モバイル デバイス、仮想ホストの急増、クラウド アプリケーション、暗号化されたトラフィックなど、エクスプロイトの手段となりえる死角があるため、保護が必要な対象を十分に把握できない
- ポートとプロトコルのみに基づくセキュリティ ポリシーしか採用していない場合、正規の Web トラフィックと攻撃とを判別できない
- ユーザを適切にセグメント化し、ロールに基づいてアプリケーションへのアクセスを提供することができない
- マルウェアがデバイスを侵害してデータ損失を引き起こす前に、受信ファイルを分析、または発信 Web サイトを確認してマルウェアをブロックすることができない
- ポリシーの定義と管理、セキュリティ分析、攻撃への対応、損害の緩和のすべてを、一元的に統合された管理コンソールから実行できない

さらに、新しいクラウドベース アーキテクチャやモバイル テクノロジー アーキテクチャにより、特定のデバイスがネットワークにいつ接続し、どこから接続しているべきかについてのこれまでの常識が通用しなくなっているため、保護を目的としたネットワーク セキュリティ制御の使用も飛躍的に複雑化しています。第 1 世代ネットワーク セキュリティ ツールでは、セキュリティ ポリシーの定義および適用の判定において、動的なネットワーク トポロジやネットワーク動作を考慮するために必要な可視性を十分に得られません。

社内テクノロジーの進化に合わせてセキュリティに取り組むには、新しいネットワーク セキュリティ機能の導入が必要なことは明らかです。

高度な攻撃

攻撃側の成功は、防御の回避能力にかかっています。現在、攻撃側はさまざまなテクニックを駆使して、攻撃の検出と防御を困難にしています。表 1 は、このような回避戦略の一部を取り上げ、第 1 世代のネットワーク セキュリティ デバイスではなぜ対応が困難なのかを説明しています。

表 1. 高度な回避テクニック、および第 1 世代ネットワーク セキュリティ デバイスの対応能力の限界

回避戦略	説明	第 1 世代デバイスによる検出の課題
ポート ホッピング	マルウェアは、セッション中に使用されたポートをランダムに選択したり、攻撃中に複数のポートを使用したりできます。	第 1 世代デバイスは、ネットワーク ヘッダーに指定されたポートでセキュリティ ポリシーを適用します。そのポートおよび許可する動作はポリシーの設定の中で定義する必要があります。アプリケーションがランダムにポートを選択すると、セキュリティ ポリシーを回避できます。マルウェアが使用する可能性があるポートごとにポリシーを設定することは不可能です。
カプセル化	攻撃者は、ポート 80（HTTP）または 443（SSL）などのオープン プロトコル内に攻撃トラフィックを埋め込むことができます。	第 1 世代のネットワーク セキュリティ アクセス制御は、ポートとプロトコルに基づいていて、ポリシー アクション（許可、ログ、ブロック）においてきめ細かい処理ができません。たとえば、攻撃がポート 80 に埋め込まれた場合、第 1 世代デバイスは通常、攻撃トラフィックを通過させてしまいます。それ以外の選択肢としては、ポート 80 のトラフィックをすべてブロックしてしまうしかないためです。
ゼロデイ攻撃	攻撃者は新たにランダムに変化し（ポリモルフィック）既知のシグネチャのないマルウェアをホストの侵害に用います。	第 1 世代ネットワーク セキュリティ デバイスは、受信ファイルまたは外部への Web 接続から、標的型攻撃に関連する侵害および動作の兆候を分析できません。
コマンド アンド コントロール(C&C)による回避	攻撃者は、さまざまなテクニック（Fast Flux など）を使用して、侵害されたデバイスとボット ネットワーク上のコントローラとの間の通信を隠します。	第 1 世代ネットワーク セキュリティ デバイスは通信トラフィックをプロファイリングしません。また、クラウドベースのレピュテーション サービスに問い合わせて Web サイトの通信の妥当性を判定することもできません。つまり、第 1 世代デバイスは、侵害されたコンピュータが制御元から指示を受けようとしても検出できないのです。
水平トラフィック	攻撃者が一旦企業ネットワークに侵入すると、侵害されたホストは偵察を実行し、その後他のホストを攻撃して組織内を計画的に移動して、最終的な標的（通常は高価値のデータ）へと向かいます。	第 1 世代ネットワーク セキュリティ デバイスは内部通信トラフィックをプロファイリングしないため、倉庫のフロアに設置されたデバイスが経理部のネットワークにログインしたり、大量のデータを外部の Web サイトに送信したりしても、こうした異常なトラフィックを検出してアラートを発したり、ブロックしたりすることができません。
暗号化されたトラフィック	ブラウザやオペレーティング システムで SSL 暗号化を自由に利用できるため、攻撃者は C&C ネットワーク、流出サイト、およびその他の攻撃標的への通信セッションを暗号化できます。	第 1 世代ネットワーク セキュリティ デバイスは通常、SSL 接続の復号機能を搭載していないため、暗号化されたセッションを解釈できません。したがって、これらのデバイスには、セッション内のペイロードを調査したり、不正なアクティビティにポリシーを適用したりする手段がありません。
サンドボックス回避	攻撃者は、マルウェアを仮想マシン上で実行して悪意のあるファイルを検出するサンドボックス機能に対して、自身のマルウェア ファイルをテストしています。しかも、テスト対象となるサンドボックスは複数に及びます。高度なマルウェアは、仮想マシン上で実行されていることを感知すると、その正体を隠します。	データをエンドポイント インテリジェンスやクラウド インテリジェンスに照合すると、侵害の兆候を特定し、マルウェア感染を早期に検出できる場合がありますが、第 1 世代のネットワーク セキュリティ デバイスには、こうした照合機能がありません。

パフォーマンスに対するニーズ

コンピュータの処理能力とネットワーク速度の向上に伴い、ビデオなどの新たなアプリケーションがこれまでにない勢いで帯域を消費するようになっています。ネットワークが高速化するにつれ、ネットワーク上のセキュリティ ポリシーを検査して適用する必要性も同様に高まります。マルチギガビット ネットワーク接続の時代においてはネットワーク セキュリティ デバイスも、入出力トラフィックや水平方向のトラフィックを、ドロップしたり攻撃を見逃したりすることなく、最大の接続速度で検査できる必要があります。中規模企業やブランチ オフィスから、データセンターやサービス プロバイダーへの導入まで、あらゆる規模の組織に対し、コスト効果の高い性能を提供する必要があります。

同時に、今日の高度な攻撃は、その起点が組織内のネットワーク内にある場合や、ネットワークの深部で増殖する場合があるため、ネットワーク境界上で攻撃トラフィックを検査するだけではもはや不十分です。こうした攻撃に対抗するには、セキュリティ脅威に対する検査とポリシーを、10 Gbps 接続が一般的なコア データセンターなどの深部にまで適用する必要があります。

従来のネットワーク セキュリティ デバイス アーキテクチャは、ディープ パケット インスペクションおよびポリシー適用を、このようなマルチギガビット ネットワーク速度で実行できるようには設計されていません。ステートフル ファイアウォールにしろ、ポリシーに基づいて各パケットを複数回検査する Unified Threat Management（UTM）デバイスにしろ、第 1 世代のセキュリティ デバイスは、このような最新のネットワーク ニーズには対応できません。こうしたことも次世代ネットワーク セキュリティの推進要因となっています。

さらに、分散環境の大規模企業では、すべてのネットワーク サブセクションに一貫したネットワーク セキュリティ ポリシーを適用することが不可欠です。これには、数百台ものデバイスを透過的にサポートし、グローバルおよびローカルのポリシーを簡単に適用できる一元管理機能が必要です。

最後に、インターネット上で発生する新たな攻撃をすべて検出することは不可能です。よって、悪意のある Web サイトや IP アドレス、ファイルの識別に役立つ充実したクラウドベースのインテリジェンス機能を活用できることは、高度な攻撃者に対抗したい企業にとっては重要な要件となります。

アーキテクチャの革新

第 1 世代ネットワーク セキュリティ アプライアンスは現時点で 10 年もセキュリティを提供しており、こうしたデバイスの多くは耐用期間を終えつつあります。

このことは、企業にとっては、ネットワーク セキュリティ アーキテクチャを見直すきっかけとなります。モビリティ、仮想化、クラウド コンピューティングが従来の IT アーキテクチャを崩壊させているコンピューティング新時代にあって、スケーラビリティと効果のニーズを満たすデバイスの導入を検討する必要があります。

こうしたアーキテクチャの革新はさらに、ネットワーク セキュリティ運用と脅威の両方の管理に使用されている基本プロセスを再確認する機会も提供します。組織は従来の運用中心の機能（たとえばファイアウォール管理）を統合コンソールを備えた最先端の脅威管理プラットフォームに取り込むことで、運用管理を合理化し、セキュリティを一元化できます。こうした変化は、コスト効率とセキュリティ効果の向上に向け、複雑性を低減し、管理上の負担を軽減します。

新しいセキュリティ アプローチでは、どんなに防御しても一部の脅威は成功するものだと仮定します。つまり、次世代セキュリティでは修復を支援して、攻撃前、攻撃中、攻撃後を通して、セキュリティを間断なく提供する必要があります。

次に次世代ネットワーク セキュリティ デバイスの購入基準について検討します。

次世代ネットワーク セキュリティの購入基準

次世代ネットワーク セキュリティ プラットフォームは将来におけるネットワーク セキュリティの基盤となるため、何を選択するかはきわめて重要です。また、前述した推進要因が示すような背景により、ネットワーク セキュリティの重要性は増すばかりです。では、次世代ネットワーク セキュリティ プラットフォームに必要とされる主な条件をいくつか検討してみましょう。

可視性

見えないものを守ることはできません。よって、環境（プロトコルは問いません）内でアクティブなアプリケーションを識別できるだけでなく、接続している無数のホスト、インフラストラクチャ、ユーザも識別できる必要があります。こうした可視性により、ネットワークおよびユーザ動作のコンテキストを適用して任意の接続の意図を判定し、ブロックすべきかどうかを判定できます。表 2 に十分な可視性を実現するのに必要な機能の一覧を示します。

表 2. 次世代ネットワーク セキュリティ デバイスの可視性の要件

要件	説明	重要性
継続的な検出	ネットワーク上のホストやアプリケーションを継続的に検出します。これにはクライアント側のオペレーティング システム、ブラウザ、仮想環境、モバイル デバイスも含まれます。	新しいデバイスは速やかに認識され、管理されないデバイスによるリスクを回避します。急速に変化する環境に合わせて、防御をリアルタイムに適合させます。
ネットワーク マッピング	全ホスト、アプリケーション、ユーザ、および環境内のその他の資産をすべてカバーするリアルタイム ネットワーク マップを維持します。	この情報を使って脆弱性を判定し、影響に基づいてセキュリティ イベントに優先順位をつけることができます。新規デバイスによって、防御の迅速な強化が要求される場合もあります。
IP セキュリティ インテリジェンス	サイトのレピュテーションと外部サーバ接続を判定します。カスタム ブラックリストとホワイトリストをサポートします。	こうしたインテリジェンスを使用して、悪意のあるサイトへの接続をブロックしたり、リスクがある、または非生産的な、ポリシーに準拠しないサイトへの接続を制御したりできます。
ネットワーク アクティビティのプロファイリング	特定のユーザ、デバイス、アプリケーションがどのようにネットワーク リソースを使用しているか判定します。	ベースラインを把握することで、ネットワークで何が「通常」のアクティビティかを判定し、攻撃検出の基準とします。

脅威の有効性

次世代ネットワーク セキュリティ プラットフォームは、既知と新出の両方の脅威に対する保護を提供しつつ、ピーク使用時でも効果を維持できる必要があります。表 3 に必要な機能を示します。

表 3. 次世代ネットワーク セキュリティ デバイスに必要な脅威防御機能

要件	説明	重要性
優れた検出機能	シグネチャベース、脆弱性ベース、異常ベースなど、さまざまな検出手段を使用して、誤検出（問題と報告されたが実際は問題ではないセキュリティの検査結果）と検出漏れ（完全に見逃されてしまったセキュリティの問題）の両方を低減します。	関連する脅威も検出されるため、攻撃の検出漏れも誤検出も発生しません。検出は「回避不能」です。きわめて正確で、なりすましは不可能です。
コンテンツ検出	ネットワークを通過するファイル タイプを検出し、報告します。ポリシーで特定のファイル タイプをブロックしたり、アクティビティを監視したりできます。	これによって組織内外の知的財産を管理できるようになります。さらに、疑わしいファイル タイプを検査、制御できます（たとえば、特定のネットワーク ゾーンや重要なホストで実行可能ファイルを停止できます）。
異常アクティビティの検出	ベースラインのネットワーク動作と実際の動作とを比較して、「通常」の許容範囲外のアクティビティを明示します。	潜在的な攻撃がネットワーク上で異常な動作を示した場合、ピンポイントで検出できます。シグネチャが不明でも、動作が疑わしい攻撃であれば検出します。

きめ細かい制御

ネットワーク セキュリティ デバイスには、従業員の業務の妨げとなることなく安全なアクセスを実現することが求められます。これには、アプリケーションと Web サイトの両方について、検出や対応をカスタマイズできるきめ細かなセキュリティ ポリシーが必要です。具体的な機能を表 4 に示します。

表 4. 次世代セキュリティ デバイスのセキュリティ ポリシー要件

要件	説明	重要性
セキュリティ ポリシーの一貫性	ネットワーク、ゾーン、アプリケーション、ユーザ、Web サイト、ファイル タイプ、ホスト アクセスなど、すべてのセキュリティ管理対象を網羅する、統一された具体的なポリシーを作成します。	特定のユーザおよびグループがネットワーク上で使用を許可されるアプリケーションと Web サイトの数と種類を制限して、攻撃可能範囲を縮小します。ポリシーの生成と管理機能を共通のコンソールとエンフォースメント ポイントのセットに一元化して、ポリシー適用を容易にします。
ポリシー例外のサポート	特定のユーザやグループが特定のアプリケーションやコンテンツにアクセスできるように、個別のポリシーを適用します。	異なるユーザ層に異なるポリシーを必要とするビジネス ニーズをサポートする機能を提供します。たとえば、Facebook チャットは承認された汎用アプリケーションではなくても、一部の従業員（マーケティング部門など）には必要な機能である場合があります。
アクセス制御オプション	各アプリケーションに適切なレベルのセキュリティを提供します。その際、トラフィック通過の許可（詳細検査あり、またはなし）、接続の監視、トラフィックのブロックなどの機能が必要です。ブロックは、徹底的なブロック、接続リセットを伴うブロック、またはユーザをランディング ページに強制移動させてポリシーに同意させて責任を負わせるインタラクティブなブロックなど、柔軟に行えることが求められます。	こうしたアクセス制御の柔軟性がないと、従業員がセキュリティ チームに仕事を妨害されていると不満を覚えてしまう可能性があります。
選択的なアプリケーション機能のサポート	アプリケーション内の機能を把握し、それらの機能のうちどれがそのアプリケーションまたは特定の Web サイトでサポートされるかについて、きめ細かなポリシーが設定できます。	特定のアプリケーション機能に対する固有の許容度を設定して、攻撃対象を縮小します。きめ細かな制御により、特定のユーザに対してはアプリケーション機能を必要な場合にのみ有効にすることが可能です。
カスタムルールの策定	お客様がルールを作成および調整できるようにします。	汎用ポリシーでは標的型攻撃に対して防御できない場合、重要な資産を保護するために必要な防御をプロビジョニングする柔軟性を組織に提供します。また、固有のコンプライアンス要件を満たす機能も提供します。

自動化

組織の多くは、高度な攻撃者に対抗するためにリソースを拡充する余裕がありません。俊敏かつ効果的に対応するには、次世代ネットワーク セキュリティでセキュリティ ポリシーのプロビジョニングとチューニングを自動化し、これらのポリシーを社内に一貫して適用できる必要があります。セキュリティ ポリシー管理の自動化に重要な機能を表 5 に示します。

表 5. 次世代セキュリティ デバイスの自動化の要件

要件	説明	重要性
自動化された影響評価	ホストの脆弱性インテリジェンス、ネットワーク トポロジー、攻撃コンテキストと脅威とを照合して、アクション可能なセキュリティ イベントの数を減少させます。	毎日数千ものセキュリティ イベントを手動でふるい分けることは事実上不可能で、有意なアラートが無視されることにもなります。リソースは組織への影響が大きいイベントに重点的に投入するべきです。
ポリシーの自動最適化とチューニング	ネットワークをパッシブにプロファイリングし、新規および更新されたルールを推奨することで最新の防御を提供します。新しい攻撃シグネチャを自動的に適用して、新出の攻撃をブロックします。不明なアプリケーションを自動的にブロックします。	環境に対してポリシーを最適化する負担を軽減します。動的な IT 環境（モバイル、仮想）においても、保護をチューニングされた状態で維持します。
ユーザ ID の関連付け	DHCP や Active Directory リソースと連携することで、セキュリティ イベントを実際のユーザやデバイスに関連付けます。	どのユーザが攻撃されているか、または企業ポリシーに違反しているかを、IP アドレスとユーザを手作業で照合することなく、自動的に確認できます。
異常な動作の検疫	ベースラインから大きくかけ離れた動作を示すユーザやデバイスをネットワーク上の検疫に配置し、脅威の検査を詳細に行います。	手動のチューニングを減らし、ネットワーク セキュリティ チームにリソースが不足していても、対応できるようにします。それにより、異常なアクティビティに迅速に対応します。
ネットワークの自動セグメント化	検出を活用してネットワークのセグメント化を行います。	脅威防御機能とネットワークに組み込まれたセキュリティ機能との連携により、脅威を迅速に封じ込めます。

高度なマルウェア防御

マルウェア攻撃の高度化に伴い、ネットワーク上でのマルウェア検出が難しくなっています。また、侵入されてしまった場合は、修復が一層困難になっています。大規模なクラウドベースのマルウェア インテリジェンスでリアルタイム情報を企業内およびその他の企業と共有しない限り、攻撃に勝つのは非常に困難です。また、何もない状態ではどのようなセキュリティ制御も効果を発揮できないため、ネットワーク上の防御、エンドポイントでの保護機能、脅威と修復アクティビティを追跡する管理コンソールの間に調整が必要になります。表 6 に必要な保護の種類を示します。

表 6. 次世代セキュリティ デバイスに必要とされる高度なマルウェア防御

要件	説明	重要性
インラインでのマルウェアの検出とブロック	マルウェアに感染したファイルがネットワークに侵入または通過しようとしていることを検出してブロックします。	アウトオブバンド デバイスがインバウンド マルウェアに対してのみアラートを発するのに対し、インラインに導入したデバイスは、既知の悪意のあるファイルがエンドポイントに感染する前にブロックできます。
違反検出とブロック	マルウェアに感染したファイルが C&C サーバと通信しようとしていることを検出してブロックします。	マルウェアが感染に成功すると、ハッキングに使うユーティリティ（ルートキットなど）を追加でダウンロードしたり、さらなる指示を仰いだりするために、外部の C&C サーバと接続を確立しようとします。こうしたアクティビティは、マルウェアによる被害を拡大します。
クラウドベースのマルウェア インテリジェンス	クラウドベースのリポジトリを使用して、受信ファイルがマルウェアかどうかを判定し、保護されたサンドボックス環境で疑わしいファイルを分析できます。	毎日何百万もの新規のマルウェア サンプルが出現する中からマルウェアの兆候を発見するには、数十億のサンプルを分析する必要があります。この作業をオンプレミスの機器だけで行うのは不可能です。
継続的な分析とレトロスペクティブ アラート	マルウェア判定が当初の分析以降に変化した場合に、アラートを発します。ネットワークに侵入したマルウェアをトラッキングし、侵入ポイント、伝達経路、使用されたプロトコル、影響を受けるユーザとホストを特定します。	ネットワークへの侵入中は休止状態を保つマルウェアは検出を回避してしまう場合があるため、悪意の有無の判定タイミングにかかわらず、マルウェアの増加をトラッキングし、アラートを発する機能が必要です。
エンドポイント保護との統合	侵害の兆候とマルウェアの判定をネットワークおよびエンドポイント エンフォースメント ポイントで共有します。共通のクラウドインテリジェンス機能を使用して、一貫性のある適用を実現します。	追加のコンテキスト、修復、エンドポイント動作のリアルタイム分析により感染を検出し、ネットワーク レイヤでブロック ルールを適用します。また逆に、ネットワーク侵入時に検出されたマルウェアに基づき、エンドポイント デバイスでの保護を提供します。

パフォーマンス、拡張性、柔軟性

複雑なポリシーを高速で分析して適用するという次世代ネットワーク セキュリティ デバイスの厳しい要件を考えると、パフォーマンスと、マルチギガビット ネットワークに対応できる能力が重要な購入条件となります。さらに、必要とされる導入モデルが何であってもサポートでき、今後の変化に柔軟に対応できれば、急速に進化する市場で投資を保護できます。表 7 にこうした要件の詳細と、それらが重要である理由を示します。

表 7. 次世代セキュリティ デバイスのパフォーマンス、拡張性、柔軟性の要件

要件	説明	重要性
高速環境専用に最適化	ラインレート パケット分析およびポリシー適用に対応しています。ハードウェアはスループットおよび精度が最適化されています（シングルパス インスペクション エンジンなど）。	ネットワークの高速化やセキュリティ機能の増加に伴ってディープ パケットの可視性と脅威への対応も同様に進化し、保護のためにライン スピードが犠牲になることがないようにする必要があります。
検証済みのパフォーマンス	多数のユースケースおよび導入シナリオについて、サードパーティがパフォーマンスを検証しています。	独立して製品テストを行う NSS Labs や ICSA Labs などのサードパーティ機関にテストを依頼すると、次世代ネットワーク セキュリティ ソリューションが、必要とされるネットワーク ボリュームの処理と脅威保護を両立できているかどうかを検証できます。
耐障害性	復元力のあるハードウェア アーキテクチャと、可用性に優れた導入に対応できるアーキテクチャで、ネットワークの可用性要件を満たします。保護するネットワークに応じて、ポートをフェール オープン、バイパス、フェール クローズにできる機能を提供します。	ネットワーク セキュリティ デバイスが理由で予期しないダウンタイムが発生することは許されません。99.999 % の可用性を期待するのが当然ということは、1 年間（暦年）に発生する予定外のダウンタイムは実質 0 分であることが求められるということです。

柔軟なライセンス	ライセンスにより、複数の動作モードでのソフトウェアの有効化をサポートします。これには、NGIPS、アクセスおよびアプリケーション制御、NGFW、URL フィルタリング、高度なマルウェア防御が含まれ、すべて 1 台のデバイスに搭載されます。	現在および将来要件が変化しても、セキュリティ ニーズを満たす機能を提供できる柔軟な導入が可能です。また、これらのデバイスのプロビジョニング、スペアリング、管理を簡素化します。
モジュール型ネットワーク接続	さまざまなメディア インターフェイスに対応した多様な接続スピードを提供し、ネットワーク接続の拡張に合わせて段階的にサポートします。ネットワーク帯域幅要件の拡張に従って、現場での増設やアップグレードを可能にします。	次世代ネットワーク セキュリティ デバイスを既存のネットワークに取り込むための拡張性と柔軟性を提供し、将来的な拡張と保護の要件をサポートします。ネットワークの再構成による中断を軽減します。

管理と拡張性

情報リスクを管理するには、ネットワークを知り、ポリシーを設定して企業全体に適用できる必要があります。また、組織が使用する管理モデルをサポートし、ネットワークやセキュリティの運用上の統合を支援する、またはこれらを別個の機能としたまま、共通プラットフォームの利点を維持する柔軟性も求められます。最後に、企業の既存のセキュリティ制御をサポートし、かつ追加機能にも対応できる堅牢なエコシステムを実現できる次世代ネットワーク セキュリティ プラットフォームを選択すべきです。表 8 にデバイスが満たすべき要件を示します。

表 8. 次世代セキュリティ デバイスに求められる管理と拡張性の要件

要件	説明	重要性
ユニファイド マネジメント	何百にも及ぶアプライアンスを集中管理する、単一インターフェイスによる一元管理コンソールを提供します。	運用を合理化して管理にかかる負荷を軽減します。これは人員が不足している、あるいはセキュリティの専門性に乏しい組織にとって特に重要です。
一元化されたエンタープライズ セキュリティ ポリシー	エンフォースメント ポイント（アプライアンス、モバイル デバイス、仮想アプライアンス）にかかわらず、一貫したポリシー セットを適用します。	ファイアウォール、IPS デバイス、マルウェア検出アプライアンスに対して複数のポリシーを管理することは、管理業務を複雑にします。ポリシーを 1 つだけ設定して、デバイスが企業内のどこに所在するかにかかわらず、一貫して適用します。
ロールベースの管理	階層構造のユーザ ロールを提供することで、ネットワーク管理者とセキュリティ マネージャの権限を区別し、それぞれの役割を明確にします。	管理ロールや責任範囲に影響することなく次世代ネットワーク セキュリティ デバイスを共通プラットフォームに統合できるようにします。運用機能が適切な運用規律のもとで確実に処理されるようにします。
既存のアイデンティティ ストアとの統合	統合に基づいて社内のユーザおよびグループへの変更を、自動的にインポート（および更新）します。	セキュリティ ポリシーを組織内の特定の従業員またはグループに適用することで、ネットワーク セキュリティが柔軟にビジネス要件をサポートできるようにします。
包括的な管理レポート	システムの運用状況や、攻撃と脅威に関する現況についての重要な情報を表示するエグゼクティブ ダッシュボードを提供します。また、攻撃や制御について、各種レポート テンプレートに基づいたドキュメントを提供します。レポートは必要に応じてカスタマイズすることも可能です。	表示される傾向、イベント詳細、統計を利用して、管理者はシステムを常に適切にチューニングされた状態に保つことができます。また、インシデント対応プロセス（攻撃の調査）やコンプライアンス準拠（制御の実証）のためのドキュメントを作成できる必要もあります。
オープン性	保護メカニズム、ポリシー、ルール、シグニチャを透過的にし、初期の設定を編集することもできます。ルール開発者のエコシステムを推進します。その成果物を使用して、最適な保護と便宜性を実現できます。	保護をすべて 1 つのベンダーに頼るのはリスクが高いことは、多くの例からも明らかです。オープンであることでこうした依存を防ぎ、独自の環境に合わせて保護をカスタマイズする余地を与えます。
サードパーティ ソリューションの統合	脆弱性管理システム、ネットワーク可視化、セキュリティ情報およびイベント管理（SIEM）アプリケーション、ネットワーク アクセス コントロール（NAC）、ネットワーク調査、イベント対応ワークフローなどのサードパーティ テクノロジーのオープン API を使ってソリューション エコシステムをサポートします。	既存のセキュリティ テクノロジーをサポートし、インテリジェンスを共有して対応を調整することで、セキュリティの導入および計画業務をシンプルにします。

まとめ

クラウド コンピューティングや仮想化、モビリティなどの革新により、テクノロジー サービスのプロビジョニングや提供方法は変わり続けています。そうした中で重要な資産を攻撃から保護するため、変化に対応できる柔軟な仕組みを実現する必要があります。また同時に、脅威の数は増加し、巧妙化が進んでいます。今日の攻撃者は高度な戦術で攻撃をわかりにくくしているため、正確でスケーラブルなネットワーク セキュリティの重要性は高まるばかりです。

スケーラビリティについて確実に言えることは、将来のデバイスやネットワークは、現在のものよりも優れた機能とパフォーマンスを備えているであろうということだけです。攻撃の高度化を受けて、ネットワーク セキュリティ機能もそれに対応する必要があり、専用デバイスのラインレート検査が不可欠です。これが、攻撃者を不利な立場に追い込む唯一の方法です。

そこで、次世代ネットワーク セキュリティの出番です。次世代ネットワーク セキュリティは、第 1 世代製品の限界を超え、適切なアプリケーション動作を理解してプロファイリングし、そのベースラインをもとに異常なアクティビティを検出（およびブロック）するために必要な、きめ細かなアプリケーション制御を実現します。また、今日の動的なネットワーク インフラストラクチャを考慮すると、ネットワークのフルな可視性は、今まで意識することのなかったデバイスや従業員を保護するための状況認識と情報取得に不可欠です。

しかし、こうした広範な制御機能や可視化機能も、次世代ネットワーク セキュリティ デバイスの設定や運用が一元化されたコンソールから簡単に行えなければ効力を発揮できません。適切な自動化によって、管理者は最も重要なアラートに優先的に対応できるようになります。また、ネットワークで起きている事象に応じてセキュリティ ポリシーは自動的にチューニングされます。こうした機能により、環境が変化しても継続的に効果を発揮し、関連性を保持できるネットワーク セキュリティ防御をプロビジョニングできるようになります。

最後に、あらゆる次世代ネットワーク セキュリティ プラットフォームは、エンタープライズ クラスでなければなりません。つまり、環境が持つパフォーマンスと耐障害性の要求に合わせて拡張するだけでは不十分ということです。セキュリティ ポリシーをすべてのエンフォースメント ポイントで一元管理し、さまざまなセキュリティ機能（ファイアウォール、IPS、マルウェア検出）をサポートできること、そして既存システムと統合できるオープンな環境が必要です。

ネットワーク セキュリティの専門家にとっては、テクノロジー インフラストラクチャの保護に使用するプラットフォームが急激に進化する、胸が躍るような時代です。このバイヤーズ ガイドが、次世代ネットワーク セキュリティの購入に必要な知識を提供し、お客様の企業が最適な判断を下すための一助となることを願っています。

シスコの次世代ネットワーク セキュリティ ソリューション

シスコは、業界有数の包括的かつ高度な脅威保護製品およびソリューションのポートフォリオを提供します。シスコが提供する脅威中心型の運用アプローチは、複雑さを軽減しながら、優れた可視性、継続的な制御、高度な脅威保護を拡張ネットワークおよび一連の攻撃全体に対して提供します。

詳細については、cisco.com/go/security を参照してください。

C07-736799-00 02/16