現代のファイアウォールに潜むリスク

ファイアウォールが攻撃で悪用されるのを防ぐ方法を、3つの柱となるフレームワークを中心に説明します。

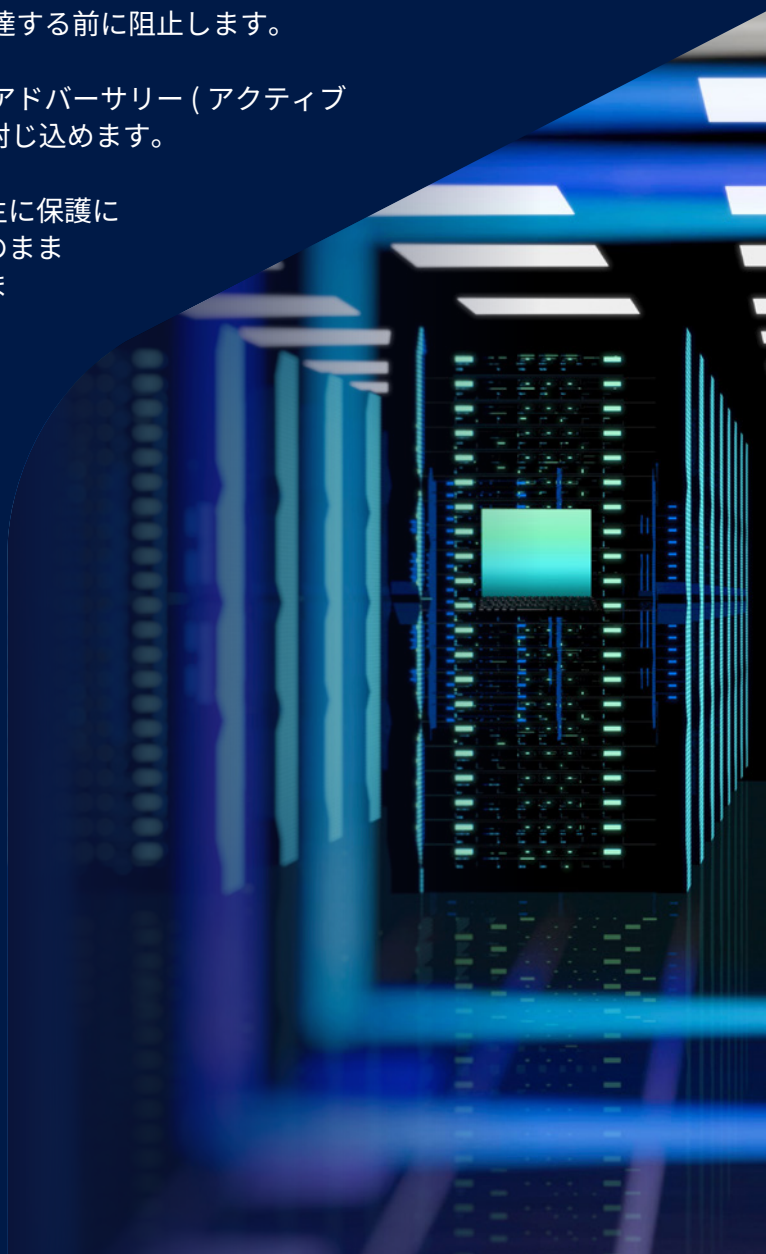
エグゼクティブサマリー

ネットワークファイアウォールは、かつてないレベルの標的型攻撃に直面しています。ファイアウォールの脆弱性を悪用する攻撃のニュースが毎日のように報道されており、懸念すべき真実が明らかになっています。それは、ネットワークを保護するように設計されたファイアウォールが、高度なスキルを有する攻撃者の主要な標的となっており、それ自体が大きなリスクとなっていることです。[1] これらの攻撃は、ファイアウォールソフトウェアの脆弱性だけでなく、ネットワークセキュリティに対する組織のアプローチにおける基本的な弱点を悪用しています。

このホワイトペーパーでは、脅威の展開前、展開時、展開後の各段階に対応する、最新のネットワークセキュリティの 3 つの柱となる包括的なフレームワークを紹介します。

- **強化：**セキュアバイデザインの原則、自動パッチ適用、設定の監査、ゼロトラストのアクセス制御により、アタックサーフェスをプロアクティブに削減します。
- **保護：**高度なトラフィックインスペクション、AI を活用した脅威検知、妥協のない高性能なセキュリティにより、脅威がネットワークに到達する前に阻止します。
- **検知と対応：**ネットワーク上で活動するアクティブアドバーサリー (アクティブな攻撃者) が攻撃を完了する前に特定し、自動的に封じ込めます。

多くのネットワークセキュリティソリューションは、主に保護に重点を置いているため、ネットワークインフラは脆弱のままとなり、進行中の攻撃を特定して対応することができません。このホワイトペーパーでは、ネットワークセキュリティの専門家と IT チームに、3 つの柱のすべてを効果的に実装するための実践的なロードマップを提供します。



現在の脅威動向

ファイアウォールは完全に包囲されている

ネットワークファイアウォールは、信頼できる内部ネットワークと敵対的な外部環境の境界に置かれています。このように特別な位置に置かれていることから、攻撃者にとって非常に価値の高い標的となっています。主要なファイアウォールベンダーに対する攻撃が相次いで報じられています。その中には、本番環境で修正が適用されていなかった既知の脆弱性を悪用するものもあれば、不適切なデフォルト設定や、攻撃者に悪用される弱点となる設計上の欠陥を狙うものもあります。[2]

2,000 以上

Mythos がわずか 7 週間で発見したゼロデイ脆弱性

最先端の AI が登場し、エージェント型 AI を活用した サイバー攻撃への懸念はさらに高まっています。Anthropic の Claude Mythos モデルは、わずか数週間のうちに 2,000 件を超える新たなゼロデイ脆弱性を発見し、攻撃者と防御側の双方にとって大きな転換点の到来を示しました。

最前線の AI に関する報道では、AI による脆弱性の大規模な発見が多く見られます。しかし本当に重要なのは、AI が攻撃と防御のスピードを加速させ、脆弱性が明らかになってから実際の被害に至るまでの時間を大幅に短縮していることです。これにより、攻撃者は以前よりも迅速かつ大規模に、少ない抵抗で行動できるようになります。

その結果は、個々の組織が対応できる能力をはるかに超えています。攻撃者がファイアウォールの侵害に成功すると、ネットワークへ直接アクセスできるだけでなく、認証情報や、組織のサプライヤーや顧客のアクセス権を入手する可能性があります。その結果、組織を取り巻く環境全体を掌握できるほどの強力な権限を手にすることになります。

ネットワークセキュリティのための 3 つの柱

効果的なネットワークセキュリティには、脅威の展開前、展開時、展開後のライフサイクル全体にわたって対応できる包括的なアプローチが必要です。このアプローチによって、独立しながらも相互に連携する 3 つの異なる防御の柱が作成されます。

強化

アタックサーフェスの削減

リスクを最小限に抑え、露出を減らし、攻撃に対するインフラストラクチャを強化するためのソリューションを設計、構築、保守する

保護

ネットワークに侵入する前に攻撃をブロック

攻撃者やエクスプロイトがネットワークに侵入するのを特定してブロックするために、可能な限り最高の保護機能を導入する

検知と対応

アクティブな攻撃の進行を阻止

検知と対応を活用して、アクティブアドバーサリーを自動的に特定して隔離する

重大な弱点

多くネットワークファイアウォールは、トラフィックフィルタリング、脅威対策、侵入防止システムなどのリアルタイムの保護機能に重点を置いています。これらの機能は不可欠ですが、リアルタイムのトラフィックインスペクションのみに依存すると、組織は脆弱なままとなります。

日々の報道からも分かるように、多くのファイアウォールや IT 部門は、環境を十分に強化できておらず、アタックサーフェスを削減できていません。その結果、脆弱性を抱えたファイアウォールが運用され続け、パッチ管理の負担は増大しています。さらに、サポートが終了した製品が依然として重要なシステムで使用されているほか、セキュリティ上の弱点があるにもかかわらず、リモートアクセス VPN への依存も続いています。一方で、進行中の攻撃をビジネスへの影響が生じる前に検知して阻止するための検知と対応機能は、多くのファイアウォール環境において十分に導入されておらず、場合によってはまったく備わっていません。

この不均衡を解消するためには、軽視されてきた防御の柱に意識的に注力することが不可欠です。特に強化は、レジリエントなセキュリティポスチャの基盤を成す重要な要素です。

ネットワークインフラストラクチャの強化 — リスクの軽減

強化とは、アタックサーフェスを積極的に削減し、攻撃者が発見して悪用する前に弱点を取り除くことです。

基本的な強化戦略

1. **エクスポージャーの最小化：**インターネットに公開されているシステムやインフラを定期的に確認し、潜在的な侵入口の数を削減します。

2. **システムがセキュアバイデザインであることを確認します。**セキュリティを基盤とした設計された製品を選択します。

3. **設定を監査し、ソフトウェアやファームウェアを最新の状態で維持します。**継続的な監視により、セキュリティハイジーンを維持します。

4. **侵害されたアイデンティティが攻撃ベクトルとして利用されるリスクを排除します。**アクセスと認証情報を厳格に管理します。多要素認証 (MFA) をあらゆる場所に導入するとともに、VPN からゼロトラストネットワークアクセス (ZTNA) への移行を進めます。

エクスポージャーの最小化

ネットワークインフラストラクチャを定期的に確認し、各コンポーネントのライフサイクル状況を評価することで、サポート終了が近づいている製品や更新が必要な製品を把握します。サポート終了が近づいているコンポーネントがある場合は、事前に計画を立てて更新または置き換えを進めます。旧式化したテクノロジーの刷新に必要な投資は、サポート対象外のシステムを悪用したランサムウェア攻撃がもたらす可能性がある損害と比較すれば、はるかに小さな負担です。

これは、ネットワークインフラストラクチャを簡素化および統合する機会にもあります。ファイアウォール、VPN、ZTNA、SD-WAN、DNS セキュリティ、Web フィルタリングをそれぞれ個別の製品やデバイスで運用している場合は、これらの機能を単一のプラットフォームに統合することを検討してください。環境内で運用するデバイスやソリューションの数を削減することで、複雑さを軽減し、運用効率を向上させるとともに、セキュリティ全体のレジリエンス強化につながります。

インフラストラクチャを最新の状態に保つことも重要です。ファームウェアやソフトウェアのアップデートには、攻撃者が悪用する可能性のある脆弱性に対する重要なセキュリティパッチが含まれていることが多くあります。パッチ適用には時間を要する場合がありますが、ランサムウェア攻撃による被害への対応と比べれば、その影響ははるかに小さいものです。

システムがセキュアバイデザインであることを確認する

企業はセキュリティ製品を必要としているだけでなく、そのセキュリティ製品自体が安全であることを同じように求めています。

サイバーセキュリティ業界は、根本的な事実を認識する必要があります。企業はセキュリティ製品を必要としているだけでなく、そのセキュリティ製品自体が安全であることを同じように求めています。攻撃者が組織を防御するためのツールそのものを狙うようになった今、企業には、脅威から組織を守るだけでなく、攻撃への耐性があるセキュリティ製品が不可欠です。組織は、セキュリティと透明性に対して真摯に取り組んでいるベンダーを評価すべきです。これには、侵害事案の発生を透明性をもって公表することも含まれます。たとえ困難な判断を伴う場合であっても、そのような誠実な情報開示こそが正しい対応と言えます。

セキュアバイデザインの主な原則を以下に示します。

- デフォルトで MFA がすべてのシステムに統合されている。
- デフォルトのパスワードと認証情報が排除されている。
- セキュリティパッチの自動適用が可能であり、運用の中断が最小限に抑えられている。
- 迅速かつ透明性の高い脆弱性開示プロセス。
- 定期的なセキュリティ監査と侵入テスト。
- 安全な開発ライフサイクルの実践が製品設計に組み込まれている。

設定を監査し、システムを最新の状態で維持する

ネットワークファイアウォールは複雑であるため、設定ミスやリスクの高い設定が発生しやすく、意図せずに攻撃の起点となる可能性があります。重要な課題は、何が誤って設定され、これらのエクスポージャーが存在する場所を把握することです。簡単に問題を特定できる場合もありますが、多くの場合、ギャップは悪用されるまで隠れています。多くのファイアウォールは、リスクの高い設定に関する洞察はまったく提供しません。このような洞察を提供するファイアウォールを利用してください。

パッチ疲れは現実的な問題ですが、回避することが可能です。従来のパッチ適用プロセスでは、運用に大きな負担がかかります。セキュリティの脆弱性は、AI によって驚異的な速度で発見できるようになりました。必要なアップデートが頻繁に実行されると、管理チームの負担が大きくなる可能性があります。多くのファイアウォールは「自動アップデート」をうたっていますが、実際には管理者がメンテナンス時間を確保し、ファームウェアを更新したうえで、デバイスを再起動する必要があります。

組織は、パッチを本当に自動的に適用できない理由は何かという、シンプルな問いを自らに投げかけるべきです。この理由は、多くのベンダーはリアルタイムのワイヤレスセキュリティアップデートをサポートするようにソフトウェアを構築していないことにあります。しかし、最新のアーキテクチャアプローチでは、次のような自動ホットフィックス機能を実現できます。

- 管理者の作業なしでセキュリティパッチを自動的に適用。
- システムのダウンタイムや再起動が不要。
- メジャーなファームウェアリリースを待たずに修正を適用。
- 脆弱性が悪用されるリスクにさらされる期間を、数か月から数時間または数日に短縮。

設定ミスは、攻撃者にとってのもう 1 つの一般的な侵入口です。複雑化したファイアウォールルール、不十分なポリシー変更管理、時間の経過とともに生じる設定のズレによって、本来保護されるべきアクセス経路が意図せず開放されたままになることがあります。

課題は、管理者は設定ミスをどのように把握できるのか？という点です。従来のファイアウォールでは、設定のセキュリティに関する洞察が提供されません。最新のアプローチには、次のようなセキュリティ状態の自動チェック機能が含まれています。

- ファイアウォールの設定を、確立されたベストプラクティスおよび CIS (Center for Internet Security) ベンチマークに照らして継続的に監査。
- チェック項目の合格または不合格をダッシュボードで可視化。
- 評価した各項目への重要度レベルの割り当て。
- ドリルダウンを有効にして、設定をすばやく調整し、意図的な例外を文書化。

これらの機能により、従来のファイアウォールに欠けていた可視性が提供され、時間の経過とともに必要となる設定が変更されても、最適なセキュリティポスチャを維持できます。

侵害されたアイデンティティが攻撃ベクトルとして利用されるリスクを排除する

2025 年にソフォスが調査したインシデントの 67% は、認証情報の侵害から始まっており [3]、アイデンティティベースの攻撃を排除することがセキュリティ強化における最重要課題となっています。そのためには、「何も信頼せず、すべてを検証する」というゼロトラストの原則を採用する必要があります。

リモートアクセス VPN を依然として使用している組織は、リモートアクセス VPN からの移行を最優先事項として取り扱う必要があります。ZTNA は、ゼロトラストの原則に準拠した VPN の最新の代替手段となります。ZTNA は、ネットワーク全体への広範なアクセス権を付与する代わりに、特定のアプリケーションやリソースへのアクセスのみを許可します。デバイスが侵害された場合、ZTNA は修復が完了するまで、そのデバイスからのアクセスを自動的に制限または遮断できます。

たとえ攻撃者が、ZTNA 経由で接続されたデバイスの侵害に成功したとしても、アクセスできるのはそのユーザーに許可された特定のアプリケーションに限られます。ネットワーク全体にアクセスできるわけではありません。セキュリティ境界は、ネットワークの外周ではなく、重要なアプリケーションやデータを中心に構築されるようになります。

67%

2025 年にソフォスが調査したインシデントのうち、アイデンティティの侵害が起点になったインシデントの割合

ZTNA は、VPN と比較して以下の 6 つの主な利点を提供します。

1. **MFA の適用：**すべてのアクセスに対して例外なく MFA を要求することで、認証情報の侵害やブルートフォース攻撃を起点とする攻撃を大幅に抑制できます。

2. **アクセスポリシーの一部にデバイスのセキュリティ状態を活用：**デバイスコンプライアンスとセキュリティ状態は、アクセス権を決定するときに継続的に評価されます。

3. **どこからでも利用可能：**ZTNA は、ユーザーが企業ネットワークに接続している場合でも、リモートで作業している場合でも同じように機能し、働く場所に関係なく一貫したセキュリティを提供します。

4. **透過的な接続：**最新の ZTNA ソリューションは、VPN でしばしば問題となる接続の不安定さを解消し、利用者にとって透過的で信頼性の高い接続環境を実現します。

5. **可視化の強化：**組織は、ユーザーがどのリソースにアクセスしているかを明確に把握できるため、より適切なキャパシティプランニングやライセンス管理を実現できます。

6. **管理の簡素化：**ユーザーの追加や削除、新しいアプリケーションの展開、アクセスポリシーの管理といった運用作業は、従来の VPN と比べて ZTNA の方が容易に行えます。

強化戦略には、リモートアクセス VPN の排除と、あらゆる場所に MFA を適用することによるゼロトラストアーキテクチャの導入を含める必要があります。

保護 – ゲートウェイでの脅威のブロック

包括的な保護機能を導入し、ネットワークに到達する前に脅威を特定してブロックします。これには、高度な TLS インスペクション、AI を活用したゼロデイ脅威の検知、そしてセキュリティを犠牲にすることなく高いパフォーマンスを実現するインテリジェントなトラフィック分析が含まれます。

最新の保護要件

- **高性能な TLS 1.3 インスペクション：**Web トラフィックの大半は暗号化されており、攻撃者は暗号化されたチャネル内にマルウェアや C&C トラフィックを隠すケースが増えています。ファイアウォールは、TLS トラフィックをインテリジェントに復号および検査し、セキュリティ要件とプライバシーへの配慮、さらにはパフォーマンスへの影響とのバランスを考慮したポリシーベースのルールを適用する必要があります。

- **ハードウェアアクセラレーション：**暗号化操作とトラフィックインスペクションには、膨大な計算リソースが必要となります。最新のファイアウォールアーキテクチャでは、信頼できるアプリケーションの通信や暗号処理をハードウェアアクセラレーションにオフロードすることで、信頼できないトラフィックの詳細な検査にリソースを集中できるようにする必要があります。

- **AI を活用したゼロデイ脅威対策：**シグネチャベースの検知は依然として有効な手法ですが、新たな脅威への対応という観点では十分ではありません AI を活用した静的ファイル解析とランタイムの動的サンドボックスを組み合わせることで、ゼロデイ脅威がネットワークに到達する前に特定してブロックすることが可能になります。これらの脅威は、従来のシグネチャベースのシステムでは完全に見逃される可能性があります。

防御機能およびパフォーマンスは、低下するのではなく、時間の経過とともに向上していくべきです。プログラマブルなアーキテクチャ上に構築されたファイアウォールは、ソフトウェアアップデートによって防御機能とパフォーマンスの両方を強化でき、ハードウェア投資の有効なライフサイクルを延長します。新たなセキュリティ機能が追加されるにつれて処理性能が低下する従来型のファイアウォールとは異なり、最新のアーキテクチャでは、継続的な最適化によりパフォーマンスを維持、あるいは向上させることが可能です。

検知と対応 – 進行中の攻撃の阻止

攻撃者が防御を突破した場合でも、その侵入を迅速に検知し、脅威を自動的に封じ込めることが可能です。NDR (Network Detection and Response) をさまざまな製品と連携させることで、攻撃者が目的を達成する前に侵害されたシステムを特定し隔離することができます。

NDR (Network Detection and Response)

NDR (Network Detection and Response) は、AI と動作解析を使用して、ネットワークにすでに侵入して活動している攻撃者を特定します。受信トラフィックを分析する境界防御とは異なり、NDR は侵害の兆候を検知するために、以下のような内部ネットワークのトラフィックパターンを分析します。

- システム間の異常なラテラルムーブメント。
- 不審な外部ホストへのコマンド＆コントロール通信。
- 異常なデータアクセスパターン。
- 権限昇格の試み。
- 内部リソースをスキャンする偵察活動。

以前は、NDR はエンタープライズ向けの機能とされ、専用製品と大規模な投資を必要とするものでした。先進的な中堅企業では、NDR 機能をファイアウォールプラットフォームに統合し、これまでエンタープライズ向けだった重要な機能をでも利用可能にしています。

自動対応

検知機能のみで対応機能がなければ、侵害の事実を管理者に通知するにとどまり、多くの場合、被害を防ぐには遅すぎます。自動対応機能は、迅速な封じ込めを可能にします。

ファイアウォール、エンドポイントプロテクション、メールセキュリティ、MDR アナリストによる検知など、セキュリティインフラのどこかで脅威が検知された場合に、すべてのセキュリティ製品にわたって対応を自動的に調整できるセキュリティソリューションが求められます。これにより、侵害されたデバイスが他のシステムと通信することを遮断し、アプリケーションおよびデータへのアクセスをブロックするとともに、ラテラルムーブメントを防止できます。

88% のランサムウェア攻撃が業務時間外に実行されている現代において、このような自動対応は特に有用です。[4]「金曜夜のシナリオ」を考えてみましょう。攻撃者はセキュリティ担当者が不在となる金曜の夜遅くにデバイスを侵害します。自動対応がなければ、攻撃者は週末を通じてラテラルムーブメントを行い、権限を昇格させ、ランサムウェアを展開することができます。組織が侵害を認識するのは、月曜の朝にファイルが暗号化され、身代金要求が表示されたときです。

製品が連携して自動的に対応できれば、初期侵害の時点で即座に隔離が実行されます。攻撃者は隔離されたセグメントに封じ込められ、それ以上攻撃を進行させることができなくなります。セキュリティチームが月曜の朝に確認するのは、全社的に広がったランサムウェアの被害ではなく、封じ込めた脅威に関するアラートになります。

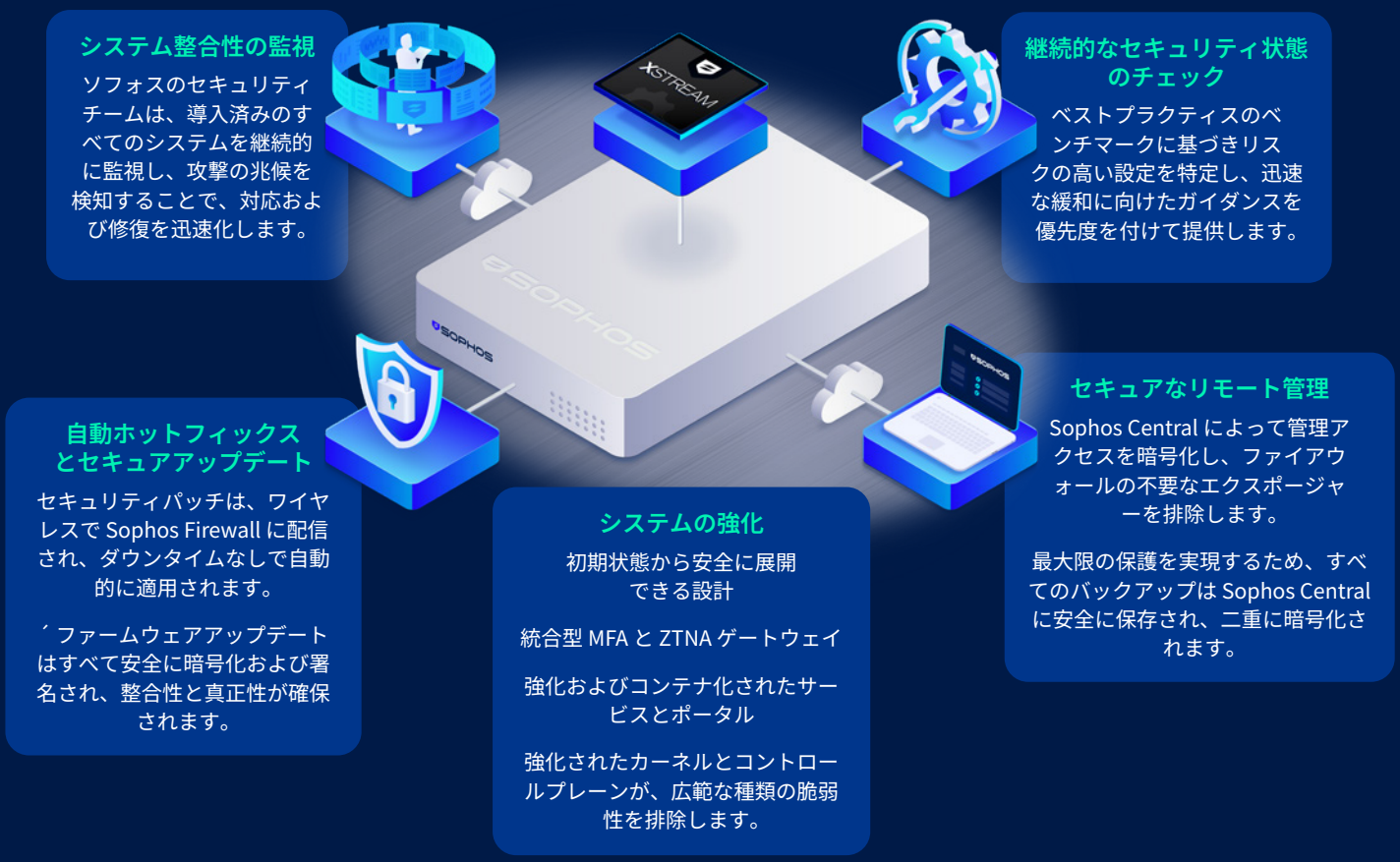
88%

営業時間外に展開されたランサムウェア攻撃の割合

Sophos Firewall：完全なソリューション

このホワイトペーパーで示した 3 つの柱となるフレームワークはセキュリティのベストプラクティスを示すものですが、これを効果的に実装するには、3 つの柱すべてを支えるインフラストラクチャを選択することが重要です。

Sophos Firewall は、3 つの領域すべてにわたって大規模な投資を行っている数少ないソリューションの一つであり、他の製品では得られない多くの機能を提供しています。



セキュアバイデザイン

Sophos Firewall は、セキュアバイデザインの包括的なアプローチを通じて強化に対応し、セキュアなインフラストラクチャを維持するために通常求められる負担を排除します。

自動ホットフィックス機能：パッチ疲れの解消

Sophos Firewall の独自の自動ホットフィックス機能は、脆弱性が露出する期間という概念を根本的に変えます。

- セキュリティパッチは、ソフォスによる開発および検証が完了すると同時に、ワイヤレスで自動的に配信されます。
- パッチは、管理者による操作なしで適用されます。
- ダウンタイムや再起動は必要ありません。
- メジャーなファームウェアリリースを待たずにホットフィックスが適用され、継続的な保護を保証します。

このアーキテクチャの利点により、脆弱性が悪用されるリスクにさらされる期間が数か月から数時間または数日に短縮されます。ソフォスが脆弱性を発見しパッチを適用すると、Sophos Firewall のすべての顧客は即座に保護されます。管理者がスケジュール調整やメンテナンス期間を確保する必要はありません。

真に自動化され、ゼロダウンタイムでセキュリティパッチを適用できる主要なファイアウォールベンダーは他に存在しません。この機能だけでも、セキュリティ強化における変革的な改善を実現します。

セキュリティ状態のチェック：設定の継続的な監査

Sophos Firewall のセキュリティ状態のチェック機能は、これまでにないレベルで設定を可視化します。

- CIS ベンチマークおよび業界のベストプラクティスに照らして、ファイアウォールの多くの設定を継続的に監査します。
- コントロールセンターのダッシュボード上で、チェック項目の成功と不合格を直接表示します。
- 評価対象の各項目に重要度レベル (緊急、高、中、低) を割り当てます。
- ドリルダウンを有効にして、設定をすばやく調整したり、意図的な例外を文書化したりできます。
- ベストプラクティスの進化に応じて自動的に更新されます。

このプロアクティブな構成監視により、設定が時間の経過とともに変化しても、セキュリティポスチャが最適な状態に維持されます。管理者は、攻撃者が発見し悪用する前に、リスクの高い設定について即座にアラートを受け取ります。

リモートからの整合性監視

ソフォスは、すべての Sophos Firewall の導入環境全体を一元的に監視している点で独自の強みを持ちます。Sophos XDR (Extended Detection and Response) Linux Sensor の統合により、次のようなシステムの整合性を監視できます。

- 不正な設定変更。
- ルールのエクスポート。
- ファイルの改ざん。
- 悪意のあるプログラムの試行。

この統合センサーにより、ソフォスのセキュリティチームは、すべての顧客の導入環境全体を対象に攻撃の兆候をプロアクティブに監視できます。これは、現時点で他のファイアウォールベンダーが提供していない独自のセキュリティレイヤーです。脅威が検知されると、ソフォスは即座に対応し顧客の修復を支援すると同時に、他のすべての顧客を保護するための自動ホットフィックスを配信します。

多要素認証の統合とゼロトラストネットワークアクセス

Sophos Firewall は、すべての管理アクセスにわたって MFA を統合的に適用します。統合型の ZTNA ゲートウェイも含まれているため、ZTNA を容易に適用および展開でき、脆弱なリモートアクセス VPN からの移行も可能になります。

強力な保護機能とパフォーマンス

多くのベンダーが強力な保護機能を提供していますが、Sophos Firewall は異なるアプローチを採用しています。パフォーマンスが低下するために重要なセキュリティ機能を無効化せざるを得ないような状況を招くことなく、包括的なセキュリティを提供します。

Xstream FastPath アーキテクチャ

Sophos Firewall のプログラマブルな Xstream アーキテクチャは、トラフィックをインテリジェントに管理し、最大限のセキュリティとパフォーマンスを両立します。このアプローチにより、TLS インスペクション、サンドボックス、IPS などの包括的なセキュリティ機能を有効にしても、パフォーマンスが低下することはありません。Sophos Firewall は、AI を活用したゼロデイ脅威対策も統合し、新たな脅威を特定します。

パフォーマンスと保護の継続的な改善

新しいセキュリティ機能が追加されるにつれて動作が遅くなる従来型のファイアウォールとは異なり、Sophos Firewall のプログラマブルアーキテクチャは、ソフトウェアアップデートを通じて**保護性能とパフォーマンスの両方**を強化できます。顧客は、ハードウェアアップグレードを必要とせず、ハードウェア投資に対する継続的な改善を受けることができます。保護とパフォーマンスは劣化するのではなく、時間とともに向上します。

比類のない検知と対応

多くのネットワークファイアウォールには、検知および対応機能がほとんど備わっていません。攻撃者が境界防御を突破した場合、従来型のファイアウォールには、その侵入を検知したり対応したりする仕組みがありません。これは、組織を高度な攻撃に対して脆弱な状態にする重大なギャップです。

Sophos Firewall は、自動化された検知と対応機能を提供する点で独自の強みを持ちます。

統合型 NDR (Network Detection and Response)：

以前は、NDR はエンタープライズ向けの機能とされ、専用製品と大規模な投資を必要とするものでした。Sophos Firewall は、NDR を基本的な保護サブスクリプションに含まれる標準機能として提供しています。

これにより、あらゆる規模の組織にエンタープライズグレードの脅威検知機能が提供され、境界防御を突破した攻撃者であっても、その目的を達成する前に検知することが可能になります。

Synchronized Security：製品間の自動対応を可能に

検知機能のみで対応機能がなければ、侵害の事実を管理者に通知するにとどまり、多くの場合、被害を防ぐには遅すぎます。Sophos Firewall の Synchronized Security は、セキュリティインフラ全体にわたって自動化された協調的な対応を可能にします。

ファイアウォール、エンドポイントプロテクション、メールセキュリティ、Workspace Protection、MDR のアナリストなど、ソフォスのいずれかの製品やサービスが脅威を検知すると、Synchronized Security は自動的に次の処理を実行します。

- 感染したデバイスが他のシステムと通信しないように隔離。
- アプリケーションやデータへのアクセスのブロック。
- ネットワーク全体でのラテラルムーブメントの防止。
- セキュリティチームが調査して修復するまで、脅威を封じ込め。

「金曜夜のシナリオ」は、自動化された対応の重要な価値を示しています。

自動対応がない場合：セキュリティスタッフが不在の金曜の夕方遅くに、攻撃者がデバイスを侵害しました。攻撃者は週末を通じてラテラルムーブメントを行い、権限を昇格させ、ランサムウェアを展開しました。組織が侵害を認識するのは、月曜の朝にファイルが暗号化され、身代金要求が表示されたときです。

Synchronized Security がある場合：最初の侵害が発生すると、即座に自動隔離が開始されます。攻撃者は隔離されたセグメントに封じ込められ、それ以上攻撃を進行させることができなくなります。セキュリティチームが月曜の朝に確認するのは、全社的に広がったランサムウェアの被害ではなく、封じ込めた脅威に関するアラートになります。

この自動化された対応機能は、24 時間 365 日体制でセキュリティを運用していない組織にとって特に有効であり、従来の NDR ベンダーがこれまで対象としてこなかった中堅企業にとって極めて重要です。

まとめ

ファイアウォールはリスクを軽減しているか？それともリスクを生み出していないか？

ネットワークファイアウォールは、かつてない攻撃のプレッシャーに直面しています。いくつもの主要なファイアウォールベンダーにおける脆弱性を報じるニュースは、不都合な真実を明らかにしています。ネットワークを保護するように設計されたシステムが、高度な攻撃者の主要な標的になっているのです。

本ホワイトペーパーで提示する 3 つの柱となるフレームワーク (強化、保護、検知と対応) は、脅威の展開前、展開時、展開後のすべての段階に対応する包括的なネットワークセキュリティアプローチを提供します。残念ながら、多くのファイアウォールベンダーは保護機能の柱のみに専念しており、強化と検知と対応機能に重大なギャップが残されています。

このフレームワークを効果的に実装するには、3 つの柱すべてにバランスよく投資しているインフラストラクチャを選定することが求められます。組織は、以下の点を考慮してファイアウォールベンダーを評価する必要があります。

- 単なる表明ではなく、実装を裏付ける証拠とともに示されるセキュアバイデザインへのコミットメント。
- ダウンタイムとパッチ疲れを解消する**自動パッチ適用機能**。
- セキュリティポスチャを可視化する**設定監査**。
- **MFA と ZTNA を含む**統合型のゼロトラスト。
- **進行中の脅威を特定する NDR**。
- **人間の介入なしで脅威を封じ込める**自動対応機能。

老朽化したインフラや不十分なインフラを置き換えるコストは、既知の脆弱性を悪用したランサムウェア攻撃から復旧するコストよりも大幅に低くなります。自組織が次のニュースの見出しになる前に、行動を起こすべき時です。

セキュリティはすべての関係者に共通する責任です。ベンダーは安全な製品を構築する必要があります。組織は、それらを適切に導入し、継続的に維持管理し、サポート終了時には廃止しなければなりません。双方が責任を果たすことで、エコシステムを劇的に安全にすることが可能です。

自問すべき重要な質問：**ファイアウォールはリスクを軽減しているか？それともリスクを生み出していないか？**

その答えは、インフラが現代のネットワークセキュリティの 3 つの柱すべてに対応しているか、あるいは攻撃者に悪用される重大なギャップを残しているかにかかっています。

1、2、3、4 2026 年版アクティブアドバーサリーレポート - ソフォス。

Sophos Firewall の詳細については、**Sophos.com/Firewall** をご覧ください。

ソフォス株式会社営業部
Email：sales@sophos.co.jp