ネットワーク境界が消失
シマンテックにお
任せください

クラウドアプリケーション、モバイルデバイス、リモートワーカーの増加でネットワーク境界という概念がなくなり、従来のセキュリティを見直すときが来ています。

Symantec™

第 1 章

クラウド時代のセキュリティ

今急増しているセキュリティ課題にはクラウド時代のネットワーク保護で対応する必要があります。

モバイルユーザー、リモートオフィス、クラウドアプリケーションの保護は万全でしょうか。終わることのない、ますます高度化するサイバーセキュリティ攻撃に対抗しながら、変わり続けるコンプライアンス義務にどう対応すればよいのでしょうか。

バックホーリングでは、支店やリモートオフィスから会社のデータセンターにインターネットトラフィックが送られ、データセンターでセキュリティや脅威防止ポリシーが適用されます。このモデルは、企業のクラウド化に伴い一般的ではなくなりつつあります。プライベートマルチプロトコルラベルスイッチング（MPLS）リンク経由でのトラフィックのバックホーリングが非常に高額なことや、バックホーリングによって遅延の問題が発生し、クラウドアプリケーションや Web にアクセスしようとする社外の従業員に影響が及んでいることが原因です。今や、従業員はクラウド型のセキュリティサービスに直接アクセスできるようになり、バックホーリングが不要になっています。そしてセキュリティポリシーは、トラフィックが直接 Web やクラウドアプリケーションに移動するときに適用されます。

2017 年

13 件中 1 件

ゲートウェイで分析した URL のうち、
悪質であることが判明した URL の割合

2016 年の 20 件中 1 件から増加しています。

提案:

- クラウドベースのセキュア Web ゲートウェイをセキュリティインフラの基盤にし、ユーザーとデータを場所に関係なく保護する
- ネットワークのパフォーマンスを犠牲にせず、手頃な価格で必要なセキュリティを確保する
- 業界トップクラスの脅威防止テクノロジーを導入する
- 統合セキュリティポリシーでオンプレミスおよびリモート/モバイルユーザーを保護する
- 効果的でシームレスな保護を実現できる包括的なソリューションを選択する

暗号化されたトラフィックに隠れているマルウェアは、従来のネットワーク防御をすり抜けることができます。現在のほとんどのインターネットトラフィックは暗号化されており、暗号化を悪用してマルウェアを拡散するケースが増えています。

第 2 章

高度なクラウド型のセキュア Web ゲートウェイで防御を構築

クラウド時代には、Web およびクラウドアプリケーションの基本的なセキュリティにとどまらない保護を提供するセキュア Web ゲートウェイ（SWG）が必要です。

セキュア Web ゲートウェイ（SWG）は、Web やクラウドアプリケーションへのデータフローを迅速に保護し、暗号化されている場合でも、独自の方法でトラフィックをスキャンし、マルウェアや情報セキュリティコンプライアンス違反を検出します。このため、SWG はネットワークセキュリティスタックの基盤として最適です。高度なクラウド型のセキュア Web ゲートウェイの機能は、従来の基本的な機能（会社が認めた Web 使用ポリシーの適用など）だけにとどまりません。脅威インテリジェンスデータを使用して URL のリスクを評価するので、従業員が危険なサイトにアクセスすることはありません。また、検査技術が組み込まれているため、トラフィックをチェックしてサイバー脅威、情報漏えいを検出することが可能です。また、Web 隔離などの革新的な技術を組み込むことでユーザー向けの脅威防止機能を強化している SWG もあります。フル機能の SWG は、直面している重要なセキュリティおよびコンプライアンスの課題を解決するために必要なすべての機能を提供します。何よりも、クラウドで提供されるので、ユーザーのトラフィックをルーティングして常に SWG を経由させることができ、ユーザーは場所や使用デバイスに関係なく保護されます。

提案:

- **暗号化されたトラフィックを選択的に検査して、マルウェアとコンプライアンス違反を正確に検出する。**
  - SSL/TLS で暗号化されたトラフィックを迅速かつ安全に検査して、企業が必要とする保護とユーザーが求めるパフォーマンスの両方を実現します。現在、ほとんどのインターネットトラフィックは暗号化されています。したがって、ネットワークセキュリティ機能によってトラフィックを復号し、セキュリティおよびデータコンプライアンス検査エンジンに渡すことが重要です。ユーザーの Web ブラウザを直接標的とする新たな種類の脅威を防止することも重要な要件となっています。
- **リスクが潜む Web サイトへのアクセスを保護する。電子メールに埋め込まれた URL へのアクセスを保護し、企業のアクセス資格情報をフィッシングサイトに入力してしまうのを防ぐ。**
  - Web 隔離によって、ユーザーの Web ブラウザを標的とする脅威やフィッシング攻撃から従業員のデバイスを守ります。Web 隔離では Web セッションをエンドポイントから隔離して実行し、安全に処理された情報のみをブラウザに送信します。これにより、Web サイトからのゼロデイマルウェアの侵入を遮断します。

第 2 章

高度なクラウド型のセキュア Web ゲートウェイで防御を構築

- **暗号化されているかどうかに関係なく、すべての Web トラフィックにデータプライバシーおよび保護ポリシーを自動的に適用し、ダッシュボードとオンラインレポートを使用して活動を監視する。**

  – 復号された SSL/TLS トラフィックを任意の情報漏えい防止（DLP）システムに送信して正確かつ迅速に分析します。規制コンプライアンスに対応し、データを保護します。

- **使用中のクラウドアプリケーションを正確に特定し、そのリスクを評価し、ユーザー、グループ、場所などによってアクセスを制御する。**

  – クラウドアクセスセキュリティブローカー（CASB）ソリューションで制御することで、クラウドアプリケーションを保護し、パブリッククラウドとの間でやりとりされるデータを保護します。従業員が使用するすべてのクラウドアプリケーション（Office 365 などの「既知」のクラウドアプリケーションと、従業員が自分で用意した「シャドー IT」クラウドアプリケーション）を可視化して、従業員が会社のクラウド使用ポリシーに準拠するようにします。

- **クラウド SWG をオンプレミスおよびモバイルエンドポイント保護と統合する。**

  – ネットワークセキュリティとエンドポイントにインストール済みのセキュリティとを統合することで、ネットワークからエンドポイントまで包括的に対応する多層型保護を実現し、モバイルデバイスのアプリケーション管理を簡素化します。インターネットに直接接続するモバイルユーザーやリモートユーザーを含むすべてのエンタープライズエンドポイントを保護する多層型防御を実現します。

- **SD-WAN のパフォーマンスと柔軟性を活用しながらリモートオフィス/支店の従業員をネットワークに接続する。**

  – リモートトラフィックをクラウドセキュリティにルーティングする SD-WAN デバイスなどを利用することで、リモートオフィスおよびモバイル利用の従業員の保護が容易になります。ファイアウォールまたはプロキシの設定を変更するか、またはユーザーのデバイスを少し調整するだけで容易に実現できます。

第 3 章

低コストで高いセキュリティとパフォーマンスを実現

クラウドサービスとして提供されるネットワークセキュリティを利用すれば、従業員を保護するために必要なすべての機能が手に入ります。

ユーザーの場所や使用しているデバイスに関係なく、一貫したポリシーがユーザーに適用されます。何よりも、ネットワークセキュリティスタック全体がクラウドで提供されるので、包括的なセキュリティを迅速かつ手軽に利用できます。必要なものはすべて費用効果の高い 1 つのサービスに統合されています。新しいユーザーのサブスクリプションを追加するだけで、必要に応じて導入を拡張できます。

インターネットへの直接接続による効率化

クラウド型のセキュリティなら、従業員はセキュリティサービスを経由して Web 上の場所やクラウドアプリケーションに接続するので（Direct-to-Net セキュリティ機能）、オフィスでもモバイルユーザーに対しても優れたパフォーマンスを提供できます。また、オフィスをクラウドへ簡単に接続できる SD-WAN ソリューションが統合されたサービスもあります。

効率的な SSL/TLS 暗号化スキャン

重要な SSL/TLS トラフィックの検査によって、遅延が発生したりコンピューティングリソースが浪費されたりすることがないようにしてください。次世代ファイアウォールなどの適切ではないデバイスを使用すると、パフォーマンスが大幅に低下することがあります。

単一エージェントでのネットワークセキュリティアクセス

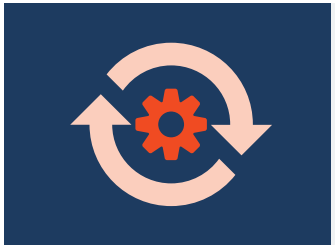
さまざまなリモートデバイスやモバイルデバイスを経由してネットワークに接続する従業員が増えています。各従業員がクラウド型ネットワークサービスに接続できるようにエージェントを 1 つ追加します。そうすれば、この単一の軽量エージェントが、包括的なエンドポイントセキュリティを提供し、さらに Web トラフィックをクラウド内のネットワークセキュリティスタックにリダイレクトします。

第 4 章

Office 365 などのアプリケーションの可視化、リスクの最小化、コンプライアンスの維持

CASB による制御を使用して、使用中のクラウドアプリケーションを正確に特定し、そのリスクを評価し、ユーザー、グループ、場所などによってアクセスを制御します。

規制遵守には、機密データを場所に関係なく可視化し、制御することが必要になります。これにはクラウドアプリケーションで共有されているドキュメント内のデータに加え、従業員が IT 部門の承認を得ずに導入しているアプリケーション（いわゆるシャドー IT）のデータも含まれます。CASB の機能は、Office 365 などのパブリッククラウドアプリケーションとの間でやりとりされるデータを保護します。

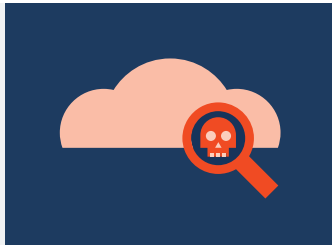


使用中のアプリケーションを正確に特定

広範なクラウドアプリケーションとサービスを対象として、ユーザー活動を詳細に可視化し、コンテンツとコンテキストベースのきめ細かいポリシーを適用します。クラウドアプリケーションの使用を継続的に監視し、機密データの共有を検出します。従業員がクラウド使用ポリシーに従うようにします。

クラウドアプリケーションのリスクを評価

従業員が使用しているすべてのクラウドの多数の属性を調べます。危険な活動、悪質なふるまい、マルウェア脅威を特定し、リアルタイムでブロックして情報を保護します。



クラウドアプリケーションへのアクセスを制御

クラウド属性データに基づき、ユーザー、グループ、場所などによってアクセスおよび制御ポリシーを設定します。重要なコンプライアンス関連データを特定および分類し、そのデータがクラウドアプリケーションでどのようにアップロード、ダウンロード、共有されているのかを監視します。

第 5 章

セキュリティポリシー管理を統合して簡素化と一貫性を実現

オンプレミス環境とクラウド環境にわたってポリシーを迅速に定義して導入し、急速に変化する規制要件や企業の義務に対応します。

対応のためにセキュリティインフラを変更すると運用が複雑化することがあります。事前に計画しておかないと、クラウドプラットフォームとオンプレミスプラットフォームで異なるポリシーが必要になり、2 つのシステムをそれぞれ管理することになりかねません。オンプレミスとクラウドに同様の機能を導入し、単一のポリシーセットで両方の環境を管理することができるソリューションを選択すれば、管理がシンプルになります。クラウドに完全移行する場合は、ワンクリックで既存のセキュリティポリシーをクラウドネットワークセキュリティサービスに移行できるソリューションを探します。

クラウドベースのセキュリティへの移行を簡素化

新しいクラウド型セキュリティに自動的に移行するオンプレミスポリシーを指定します。

一貫したポリシーを作成して管理

一度定義してすべてのセキュアゲートウェイにプッシュすることで新しいポリシーを作成します。これにより、オンプレミスとクラウドのセキュリティが混在するハイブリッド環境で一貫してポリシーを適用できます。

既存の投資を最大限に活用

可能な場合はインプレースセキュリティシステムを活用します。DLP への投資を活用し、クラウドへと拡張します。必要な場合はメインデータセンターでオンプレミス SWG を維持しますが、支店やモバイルユーザーはクラウドへ移行します。さらに、すべての環境（プライベート、パブリック、物理、仮想、クラウド、またはハイブリッド）を単一の管理コンソールから管理します。

第 6 章

結論: 境界が消えても心配ありません。クラウド型ネットワークが対応します

シマンテックのクラウド型 Web Security Service は、高パフォーマンスのグローバルクラウドサービスで提供される堅牢なエンタープライズクラスのセキュリティ機能を使用して、本社、支店、リモートおよびローミングユーザー、企業データを場所に関係なく保護します。

高度なネットワークセキュリティ機能

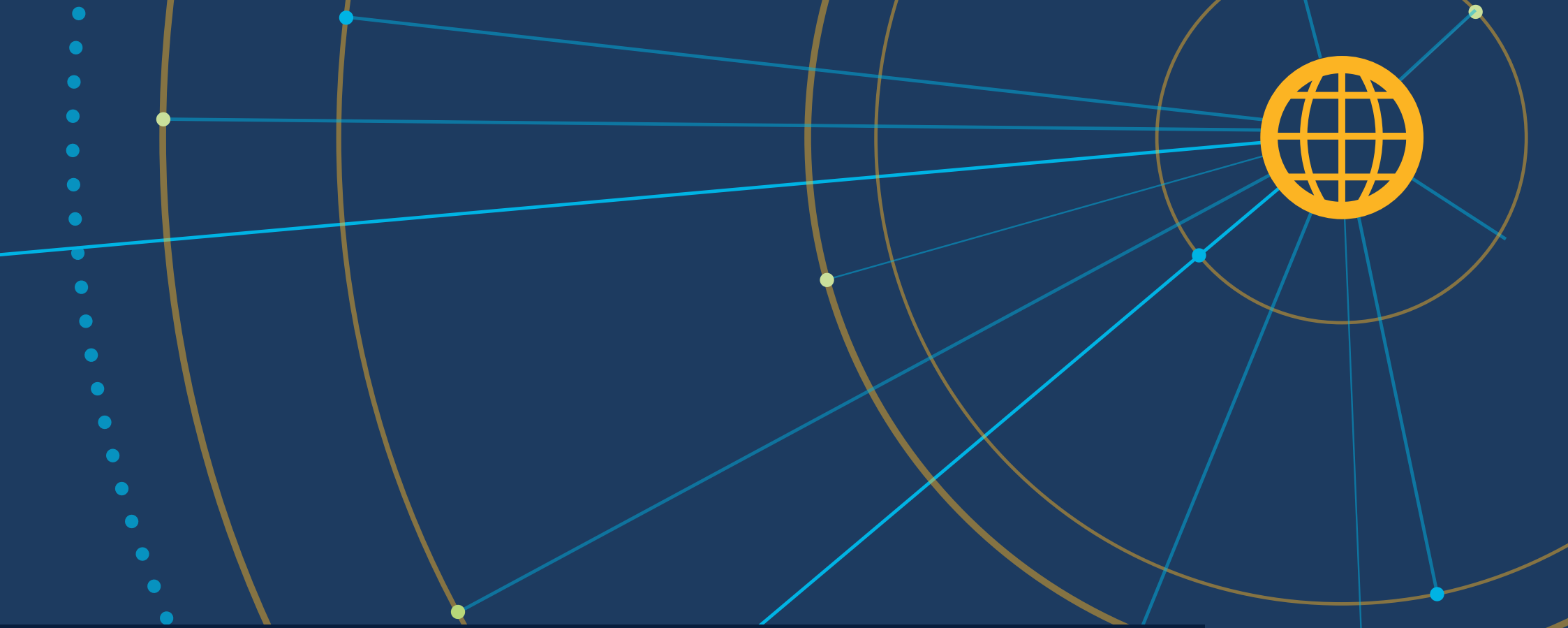
クラウド型の Web Security Service は、Gartner 社のセキュア Web ゲートウェイ部門のマジック・クアドラントで 11 年連続でリーダーに選出されている Symantec ProxySG と同じ高度なプロキシ技術に基づいて動作します。ネットワークセキュリティスタック全体の基盤となるサービスであり、中心となる高度なセキュア Web ゲートウェイに加え、マルウェア分析、サンドボックス、Web 隔離、クラウドアプリケーション制御 (CASB)、情報漏えい防止、統合 SD-WAN などの機能を備えています。どの機能でも、独自の脅威インテリジェンスを活用して従業員がアクセスしようとするあらゆる Web サイトのリスクを判断しています。

グローバルクラウドネットワーク: 実証済みのパフォーマンス

回復力の高い分散型のグローバルクラウドデータセンターインフラにより、稼働率 99.999% の SLA を提供します。Microsoft、Amazon、Google などとのネットワークピアリング接続や、大規模なファイルをクラウドストレージアプリケーション間で迅速に移動する TCP ウィンドウの最適化などによって、パフォーマンスを最適化します。

統合された保護によるシンプルな運用

エンドポイントにもセキュリティソリューションの導入が必要です。そこでシマンテックは、受賞歴のある Symantec Endpoint Protection (SEP) を Web Security Service に統合しました。これらの製品を連携して使用すれば、エンドポイントをインストールして管理するためのエージェントが 1 つ少なくなります。Web トラフィックを Web Security Service へルーティングするように SEP を設定して、ネットワークセキュリティポリシーを適用することができます。これにより、シマンテック独自のエンドポイントおよびネットワークセキュリティ多層防御サービスが実現し、境界のない世界でユーザーの安全を守ります。



詳細はこちら:

symantec.com/ja/jp/products/web-and-cloud-security

シマンテックについて

シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、シマンテックのノートン製品と LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。詳しくは、www.symantec.com/ja/jp をご覧ください。または、Facebook、Twitter、LinkedIn のシマンテックのページをご覧ください。

株式会社シマンテック〒107-0052 東京都港区赤坂1-11-44赤坂インターシティ | www.symantec.com/ja/jp

19C210137_SB_VANISHING_PERIMETER_JP