SOPHOS

政府機関向け
サイバーセキュリティガイド

ソフォスの脅威アナリストの専門家と業界をリードする脅威インテリジェンスにより、高度な脅威を 24時間年中無休で迅速に特定して対応します。

政府は、個々の国民に関する情報から、サイバー攻撃によって混乱させられる可能性のある国家安全保障や重要なインフラに関連する情報まで、非常に機密性の高いデータを保持しています。このような膨大な量のデータを保護することは困難ですが、そうしないと、国家にとって壊滅的な事態を招く可能性があります。IT チームの予算とリソースの縮小や請負業者とサードパーティサプライヤーの広範なネットワークの縮小は、侵害された場合に、政府のネットワークに侵入できる可能性があり、政府機関のサイバーセキュリティリスクを増大します。

ソフォスは、テクノロジーだけでは防ぐことができない人間主導の脅威を含むさまざまなサイバー攻撃から政府機関を保護します。ソフォスは、MDR (Managed Detection and Response) からエンドポイントやネットワークセキュリティまで、政府機関の防御を最適化することで IT チームが業務に専念できるようにサポートします。

政府機関における サイバーセキュリティの課題

政府機関は、金銭的または政治的動機で機密データを盗んだり操作したりするサイバー犯罪者にとって、ますます魅力的な標的になっています。政府機関の急速なデジタル化とパンデミックの結果としてのリモートシステムアクセスが大幅に増加したことにより、政府機関の攻撃対象領域が拡大しています。予想通り、政府機関のサイバー脅威は、件数と複雑さの両方において増加し続けています。

地方自治体/政府機関で働く IT プロフェッショナル 199名を対象とした 2022年のソフォスの調査では、組織の 58% が 2021年にランサムウェアの被害を受けており、ランサムウェア攻撃の割合は前年比で 70% 大幅に増加しました。回答者の 72% が、攻撃後にデータが暗号化されたと報告しており、これはすべての業界で最も高い暗号化率の 1つです。

ランサムウェアだけではありません。地方自治体/政府機関の全体的な IT 環境は、さらに困難になっています。組織の 59% が昨年攻撃の件数と複雑さが増加したと報告し、56% が攻撃の影響の増加を報告しました。

58%
2021年にランサムウェアの被害を受けた地方自治体/政府機関の割合

72%
データが暗号化された地方自治体/政府機関に対する攻撃の割合

1カ月以上
地方自治体/政府機関の 21% は、攻撃後の復旧に1か月以上かかりました

82%
ランサムウェアの被害を受けたこの機関のうち業務遂行能力に影響を与えられた組織の割合

59%
地方自治体/政府機関で、攻撃の件数と複雑さが増加したと報告した割合

58%
地方自治体/政府機関が身代金支払い後に取り戻したデータの割合

63%
データが暗号化された地方自治体/政府機関が、データの復元にバックアップを使用した割合

80%
地方自治体/政府機関のランサムウェアのサイバー保険の加入率

出典: ランサムウェアの現状 2022年版に関するソフォスのグローバル調査

これらの統計の背後には、脅威の状況におけるいくつかの変化があります。

サイバー犯罪のプロ化

昨年の最も著しい進展の 1つは、サイバー脅威経済の発展とプロ化です。犯罪グループは、初期アクセス、ランサムウェア、情報窃盗マルウェアなど、攻撃の特定のコンポーネントにますます特化し、それを他の犯罪者にサービスとして提供しています。これらの「アズ・ア・サービス」モデルは、攻撃を実行するのに必要なスキルのしきい値を下げ、攻撃者と脅威の量を増やします。

これらの専門的なサービスは、犯罪顧客に実行ガイダンスとリソースを提供して、攻撃の効果を高めます。この点を説明するために、2022年 3月、Conti RaaS (サービスとしてのランサムウェア) グループは、ランサムウェア攻撃を実行するために必要な手順を「アフィリエイト」攻撃者に指示するように設計した豊富なドキュメントとガイダンスを含むアーカイブを公開しました。

また、攻撃者は、ランサムウェアの被害者が支払いをして、ファイルを復号化した後に、「攻撃者のサービス評価」を依頼するなど、正規の IT サービスプロバイダーが実施する行動の多くを採用しています。

攻撃者の戦術、手法、手順の進化

攻撃者は、セキュリティソリューションによる阻止を回避するために、組織のセキュリティ体制の弱点を悪用することがよくあります。これには次のようなものがあります。

- **パッチが適用されていない脆弱性の悪用** – これは、昨年ソフォスのインシデント対応者が修復のために派遣された攻撃のうち、攻撃者が組織に侵入するために使用する一番よく使われた方法で、インシデントの 47% で使用されました。
- **正規の IT ツールの悪用** – IT プロフェッショナルが主に使用するツールである PowerShell、PsExec、PowerShell なども多くが攻撃者によって悪用され、盗まれたアクセスデータや認証情報を悪用されています。攻撃者は、正当なユーザーのふりをすることで、環境に入り込もうとします。

この機関のサイバーセキュリティの課題はこれだけではありません。また、政府機関は、インサイダーの脅威 (悪意のある脅威と予想外の脅威)、厳格な規制コンプライアンス要件、サードパーティベンダーのリスクなどの課題にも対処する必要があります。

政府機関向けのソフォスセキュリティ

ソフォスは、政府機関にサイバーリスクの管理や軽減ができるようにする高度なサイバーセキュリティソリューションを提供します。Sophos Adaptive Cybersecurity Ecosystem (ACE) は、市場をリードするサービスと製品の完全なポートフォリオを提供し、最先端の脅威からもお客様の防御力を高めます。これらはすべて、Sophos X-Ops の比類のない脅威、AI、セキュリティ運用の専門知識を活用します。

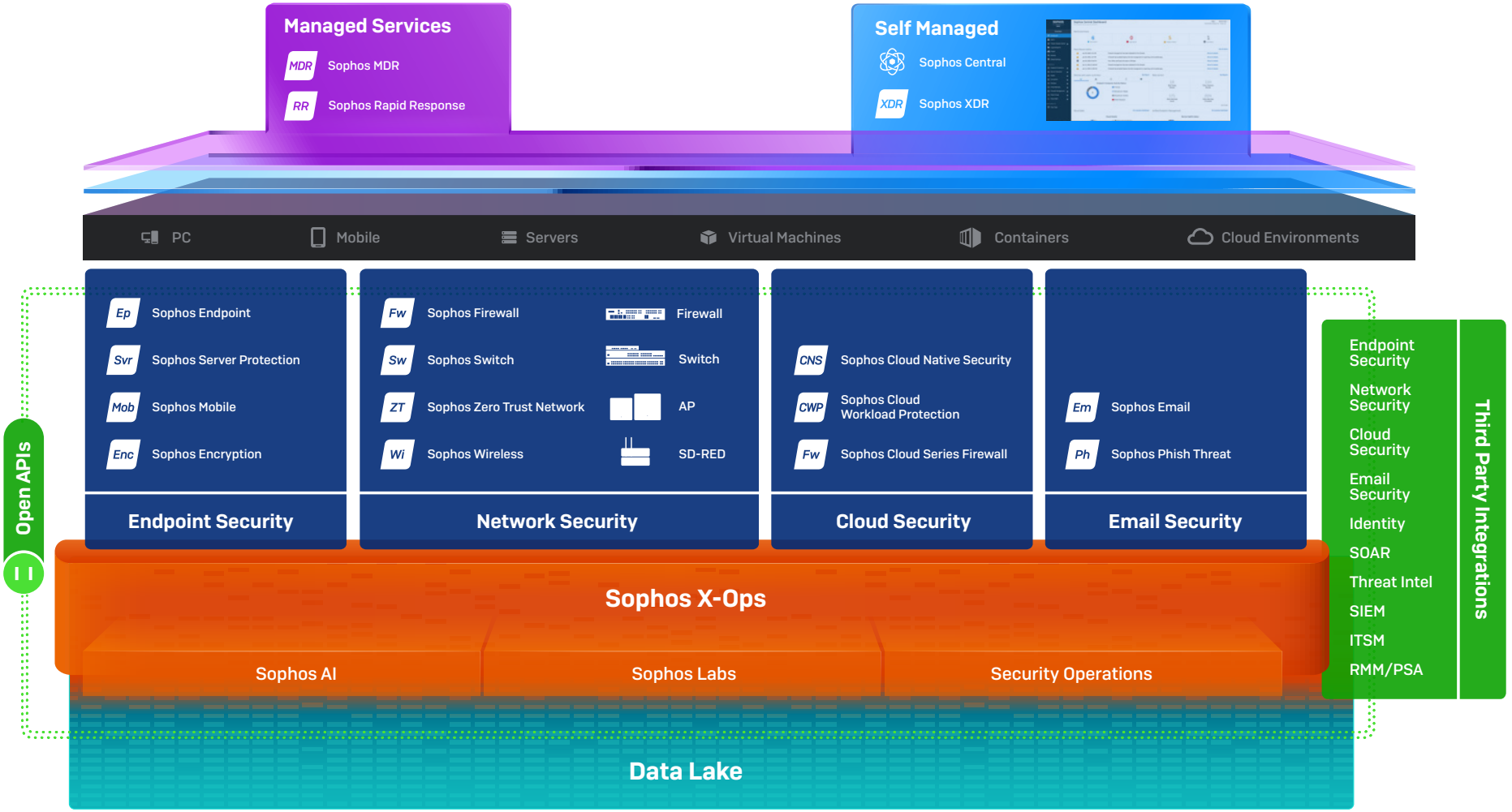
ソフォスは、世界中の **530,000社** を超えるお客様に、最先端のサイバーセキュリティの成果を提供しています。

ガートナーからリーダーに選ばれた回数は、全ベンダーの中でソフォスが最多

Gartner Peer Insights で**最高の評価**を受け、**レビュー回数が最多**の MDR サービス、エンドポイント、ファイアウォール。

2022年 8月 1日現在

Sophos Adaptive Cybersecurity Ecosystem



ユースケース

ソフォスは、政府機関が直面している最も一般的なサイバーセキュリティの課題への対処をサポートします。

ランサムウェアなどの高度な人間主導の攻撃を阻止

Sophos MDR とは、テクノロジーソリューションだけでは防ぐことができないサイバー攻撃の検出と対応に特化した専門家が 24時間年中無休体制で提供する完全に管理されたサービスです。ソフォスの専門家チームが、お客様に代わって高度な人間主導の攻撃を阻止し、業務の支障や機密顧客データの侵害が発生する前に脅威を無力化します。

「Sophos MDR のおかげで、セキュリティサポートをただ日常的に行うのでなく、より興味深い、より開発にフォーカスした作業に取り組むことができるようになりました。」

英国独立議会倫理規範局

Sophos MDR を使用すると、本格的なインシデント対応が必要な場合でも、より正確な意思決定を行うための支援が必要な場合でも、お好みのテクノロジーを使用して、専門のアナリストが数分で脅威を検出して対応できます。

次のものを使用します。

- ソフォスのエンドポイント 、ファイアウォール、クラウド、メール保護など、受賞歴を誇るソフォスのソリューション
- Microsoft、CrowdStrike、Palo Alto Networks、Fortinet、Check Point、Rapid7、Amazon Web Services (AWS)、Google、Okta、Darktrace など、他社の製品
- 当社のテクノロジーと他社のテクノロジーのあらゆる組み合わせ

Sophos MDR は、テクノロジーソリューションだけでは防ぐことができない高度な攻撃から組織を保護し、お客様の既存の投資収益率を向上させます。ソフォスは、業界で最も信頼されている MDR プロバイダーとして、政府機関が直面している脅威に関する比類のない深い知識と幅広い専門知識を兼ね揃えています。この幅広いテレメトリを活用して、ソフォスは「コミュニティがもたらす脅威に対する耐性」を作り出し、ある政府機関の顧客の防御から得た知識をこの業界の他のすべての顧客に適用して、すべての顧客の防御を強化しています。

最も信頼されている **No.1 プロバイダー**	最高レベルの評価 **4.8/5** Gartner Peer Insights	最高の保護 **38 分** 検出、調査、対応にかかった時間
多くの組織が、他のどのベンダーよりもソフォスの MDR を信頼	最も多くレビューと最も評価の高い MDR ソリューション (2022 年 8月 1日時点)	社内の最速の SOC チームよりも 5倍以上速いソフォスのアナリスト

2022年 9月現在

フィッシング攻撃からの保護

政府機関におけるフィッシング攻撃は深刻な問題となっており、政府機関が保持するデータの規模と重要性を考えると、甚大な影響を受ける可能性があります。フィッシング攻撃はより巧妙化しており、政府機関においては、認証情報を盗む通常の目的以外に、監視やスパイ目的で被害者のデバイスを乗っ取ることを目的としている場合があります。

フィッシング攻撃を阻止する最善の方法の 1つは、フィッシング詐欺を見分ける方法について従業員をトレーニングすることです。Sophos Phish Threat では、組織に向けてセキュリティ意識の向上を構築することができます。これは、自動化された攻撃シミュレーション、質の高いセキュリティ意識向上トレーニング、トレーニング結果の分析を通じて、エンドユーザーを教育およびテストをするための 30以上のセキュリティ意識向上のトレーニングモジュールが用意されています。

Sophos Email では、SPF、DKIM、DMARC 認証技術やメールヘッダーの異常解析を使用して、有名企業のなりすましや偽装の試みなどフィッシングの主な痕跡について、すべての受信メッセージをリアルタイムでスキャンすることで、信頼できる送信者のみが従業員の受信トレイに入ることができます。これにより、フィッシングメールがユーザーに届く前に、それを検出してブロックします。グループや個別のユーザー向けに複数のルール DLP ポリシーを作成し、すべてのメールや添付ファイルの財務情報、機密コンテンツ、および PII を検出して機密情報を確実に保護することで、データ流出をさらに防ぐことができます。

ほとんどのフィッシング攻撃は、メール受信者を誘導して悪意のあるリンクをクリックさせ、デバイスにマルウェアをダウンロードしたり、ハッカーに機密データへのアクセスを許可したりすることで、ネットワークへのアクセスポイントに影響を与えます。フィッシング攻撃からネットワークを強化するには、エンドポイントセキュリティを強化する必要があります。市場をリードする Sophos Intercept X Endpoint を使用して、Windows、Mac、Linux、仮想マシンなど、すべてのエンドポイントを完全に保護します。

防御を最適化するには、高度な攻撃から防御する複数の高度なセキュリティ機能を持つ多層防御が必要です。Sophos Endpoint には、次のような多層防御が含まれています。

- 不正なシステムアクセスを防止する認証情報の盗難防止。
- 攻撃者が攻撃に使用する手法を阻止するエクスプロイト対策。
- 悪意のある暗号化の試みを特定してブロックするランサムウェア対策。
- 攻撃者が防御を無効にしてペイロードを展開するのを防止するタンパープロテクション機能。

多層防御のテクノロジーを組み合わせることで、お客様の防御を最適化することができます。防御の質と多層防御の力が証明するように、ソフォスは脅威の 99.98% を事前に阻止し（AV-Test の平均スコア）、SE Labs エンドポイント保護レポートで満点を獲得しました。

ハクティビズム対策

国家が支援する敵対的なサイバー攻撃者の目的は、金銭的利益よりも政治的なサイバー戦争です。攻撃者は政府のシステムをハッキングして、重要なサービスを混乱させ、国家資産を脅かし、政府を当惑させたり信頼を損なわせたりします。いったんハッキングされると、政府機関はサイバー攻撃者が相互に連携する政府部門、サードベンダー、およびそれらと連携する企業体のシステムにアクセスするためのゲートウェイとなります。脆弱なサイバー防御、パッチが適用されていない古いシステムやアプリ、IT セキュリティインシデントの可視性が不十分なことが、政府機関がハクティビズムの標的にされる理由です。

Sophos Firewall の重要な SaaS、SD-WAN、クラウドアプリケーションのトラフィックを高速化しながら、最新の高度なサイバー脅威から強力に保護します。Sophos Firewall は、Gartner Customers' Choice for Network Firewalls 2022 の評価を獲得しており、セットアップと保守が容易な多様な最新の脅威対策テクノロジーが完全に統合されています。また、ゾーンと VLAN による柔軟で強力なセグメンテーションオプションを提供します。これにより、ネットワークで複数の信頼レベルを設定することを可能にする一方、ネットワーク内の異なる部分へのラテラルムーブメントに対する保護も強化します。

Sophos XDR は、サイバーセキュリティポスチャを完全に把握することで、定期的なパッチ管理でシステムとアプリを最新の状態に保ちます。ネットワーク、メール、クラウド、モバイルのデータソースから豊富なデータを取得し、パッチ未適用または古いソフトウェアのシステムやデバイスを特定します。

Sophos MDR (Managed Detection and Response) サービスは、攻撃経路全体を把握するための重要な可視性とコンテキストを備えた専門家が提供する 24時間年中無休のフルマネージドサービスにより、政府機関の脅威対応時間を大幅に短縮させます。これにより、テクノロジーソリューションだけでは防ぐことができないセキュリティの脅威に対して、より包括的に対応します。ソフォスの脅威ハンティングの専門家は、ネットワーク、ファイアウォール、クラウド、メール、エンドポイントセキュリティツールを活用して、ネットワーク全体からの警告を監視および調査し、疑わしいアクティビティを特定して調査し、国民のデータと機密情報がある場所に関わらず保護します。

国民のデータおよび機密データの保護

すべての政府機関は、健康情報、デジタル ID、税務情報など、国民に関する個人情報 (PII) から、機密性の高い商業企業データ、州および国家レベルの機密情報に至るまで、膨大な情報を保管しています。国家の安全と国民データのプライバシーを保護するために、このデータを保護する必要があります。

Sophos Phish Threat を使用した自動攻撃シミュレーションとセキュリティ意識の向上トレーニングにより、潜在的な脅威に注意するように従業員をトレーニングし、組織内で積極的なセキュリティ意識の向上を構築することで、重要なデータを保護します。

毎日、膨大な数のノート PC の紛失、盗難、置き忘れが発生しているため、デバイスとその中のデータの紛失や盗難に対する防御において最も重要なものは、フルディスク暗号化です。Sophos Encryption は、Windows および macOS のフルディスク暗号化により、保存されている政府データを保護できます。

Sophos ZTNA を使用すると、ネットワーク上のデータにアクセスできるユーザーを完全に制御できます。非常に細かい制御により、ラテラルムーブメントをブロックし、承認済みユーザーのみが機密データにアクセスできるようにします。

Sophos Firewall のゾーンと VLAN を介した柔軟で強力なセグメンテーションオプションは、ネットワーク上の信頼レベルを分離して、データストアに対するサイバーリスクを軽減できます。たとえば、データベースとサーバーは、他のネットワークの部分よりもより強力なセキュリティ対策を備えた DMZ に分割して、機密データをホストするサーバーを安全に保ち、他のネットワークゾーンから分離することができます。

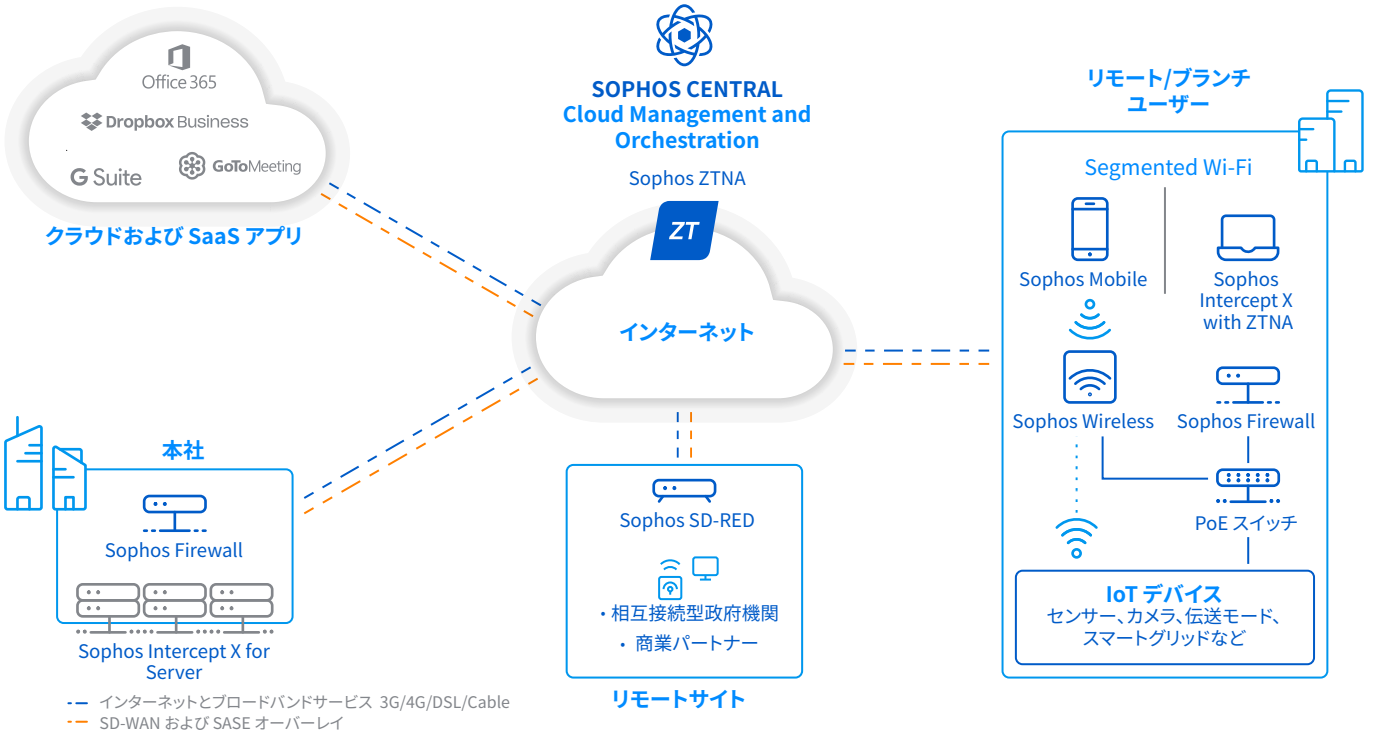
Sophos Intercept X エンドポイント保護を使用して、既知の脆弱性を軽減し、ランサムウェア、ファイルレス攻撃、エクスプロイト、マルウェアなどの最新のサイバーセキュリティ脅威をエンドポイント全体で阻止します。DLP (情報漏洩対策) 機能は機密データを特定し、メール、アップロード、ローカルコピーによる漏洩を防ぎます。

Sophos Email を使用すると、データ侵害を防ぐことができます。これにより、ユーザー向けにマルチルール DLP ポリシーを作成し、すべてのメールと添付ファイルの機密コンテンツを検出して、機密情報を確実に保護できます。また、機密データをシームレスに暗号化して、侵害を阻止します。

リモートアクセス環境の保護

政府のデータは膨大で断片化されており、多くの場合、複数の管轄区域にまたがるさまざまな政府機関や商業パートナー間で共有されています。この業界では、これらのすべてに対して安全なリモートアクセスが不可欠です。

ソフォスのセキュアアクセス製品は、リモートにある政府サイトを接続し、重要なクラウドおよび SaaS アプリケーションを提供し、データや情報を安全に共有できるようにします。これは、アプリケーションとデータへの安全なアクセスをサポートする Sophos ZTNA、リモートサイトやブランチサイトに政府のネットワークを安全に拡張するための Sophos SD-RED (Remote Ethernet Device)、簡単かつ安全なワイヤレスネットワークを実現する Sophos Wireless アクセスポイント、LAN 上での安全なアクセスを実現する Sophos Switch ネットワークアクセス レイヤー スイッチで構成されています。すべては、クラウドベースのセキュリティプラットフォームがオールインワンとなった Sophos Central によって管理されます。



インサイダー攻撃への対策

多くの政府機関において人員不足、トレーニング不足、リソース不足により、従業員が過重労働に陥り、セキュリティ侵害につながるミスを犯す可能性が高くなります。さらに、機密データへのアクセスを許可された内部関係者が権限を悪用するリスクは、政府機関が対処しなければならない重大な脅威です。

Sophos User Threat Quotient (UTQ) の実用的なインテリジェンスを使用して、最もリスクの高いユーザーやアプリケーションに関する洞察を得ることができます。これにより、セキュリティが侵害される前にポリシーを確実に適用できます。Sophos Firewall で保護をさらに強化します。これにより、ネットワーク内で使用される Web カテゴリ、アプリケーション、リムーバブルメディア、モバイルデバイスに対する完全なポリシー制御により、機密データを偶発的または悪意のある開示から保護します。IP アドレス、場所、ネットワーク、デバイスに関係なく、トラフィック シェーピング (QoS) やその他のネットワークリソースに対するユーザーベースのアクセスポリシーを使用して、ファイアウォールのすべての領域にわたりユーザーを認識できます。

代替の保護手段は、ユーザーが必要なネットワークリソースのみにアクセスできる最小権限の原則です。クラウドセキュリティポスチャ管理ソリューションである Sophos Cloud Optix では、ソフォスの AI を使用して異なるアクションを関連付け、クラウド プロバイダー コンソールの異常なアクセスパターンや場所を、ほぼリアルタイムで検出し、認証情報の悪用や窃取を特定します。IAM の関係性を完全に把握できる IAM 視覚化ツールを使用すると、IT チームは過剰な権限が付与されたアクセスを特定し、サイバー攻撃者に悪用される前に適切なサイズの IAM ポリシーを迅速かつ簡単に作成できます。

アプリケーションとネットワークの可用性の確保

政府機関は、納税や医療などの重要なサービスをオンラインで国民に提供しています。これらのサービスに対して継続的なアクセスを確保するには、政府のネットワークとアプリケーションが 24時間年中無休で利用できる必要があります。しかし、マルウェアやボット、ソーシャルエンジニアリング攻撃、DDoS 攻撃などの攻撃ベクトルにより、政府のオンライン Web やアプリケーションサービスの円滑な機能が脅かされています。

Sophos Firewall は、業界をリードする機械学習テクノロジーと SophosLabs Intelix を搭載しており、最新のドライブバイ型や標的型 Web マルウェアからの高度な保護、URL/悪意のあるサイトのフィルタリング、オフサイト保護のためのクラウドベースのフィルタリングを提供します。ソフォスのエンタープライズクラスの Web アプリケーションファイアウォールを統合し、重要な業務アプリケーションをハッキングや攻撃から保護する一方、認証済みアクセスは許可します。

Sophos Intercept X のエクスプロイト防止機能により、アプリケーションや OS の脆弱性が攻撃者によって悪用されることを防ぎます。さらに、エンドポイント保護のアプリケーションコントロールのポリシーは、政府システムでの未承認のアプリケーションの使用を制限します。

Sophos X-Ops による最新の脅威と脆弱性の開発に関する最新情報を入手している脅威の専門家が、疑わしいアクティビティを 24時間 365日検出、調査、無力化する MDR (Managed Detection and Response) サービスを使用して、攻撃者による脆弱性の悪用を阻止します。

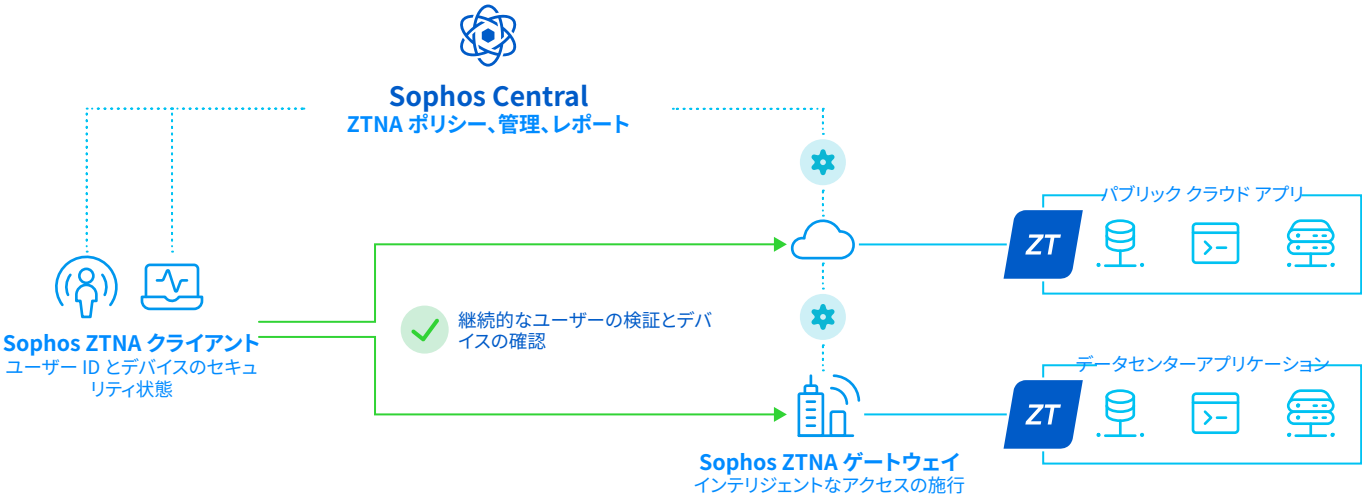
サードパーティベンダーからのリスクを軽減

ネットワークアクセスのリスクをもたらすのは、政府職員だけではありません。ソーシャルワーカーや医療スタッフ、ベンダー、商業パートナーなどのサードパーティユーザーは、さまざまなデバイスからネットワークへの継続的な外部アクセスを必要とするため、データプライバシー侵害、詐欺、認証情報の盗難のリスクを高めます。

Sophos Intercept X の AI、エクスプロイト防止、振る舞い検知、その他の高度なテクノロジーを使用して、サードパーティサプライヤを介して政府機関に侵入する脅威から防御します。さらに、強力な XDR 機能により、疑わしいアクティビティを自動的に特定し、脅威インジケーターに優先順位を付け、エンドポイントとサーバー全体で潜在的な脅威をすばやく検索できます。

24時間 365日体制の専門家によるサポートを提供します。500人以上のスペシャリストが Sophos MDR を使用して 24時間体制で、サードパーティベンダーの潜在的な脅威やインシデントをプロアクティブに探し、検証し、修復します。

Sophos ZTNA は、場所に関係なく信頼できるパートナーからのリクエストを認証する非常にきめ細かいアクセス制御により、システムへの外部アクセスに依存するサードパーティベンダーの攻撃から保護します。Sophos Endpoint と Sophos ZTNA の独自の統合により、セキュリティの侵害を受けたホストがネットワークリソースに接続するのを自動的に防ぎ、脅威が横方向に移動してネットワークに足場を築くのを防ぐことができます。



マルチクラウド環境全体でのデータの確保

政府機関でのクラウドの導入には、柔軟性、拡張性、コスト削減、コラボレーションの向上、情報の容易な共有性という利点があります。しかし、クラウドは、従来のオンプレミス環境ほど確立されていないサイバーセキュリティ対策を悪用しようとするサイバー犯罪者の主要な標的でもあります。

Sophos Cloud Native Security は、環境、ワークロード、ID 全体に、完全なマルチ クラウド セキュリティを提供します。Windows と Linux 向けの柔軟なホストとコンテナのワークロードのセキュリティにより、クラウドインフラとデータを保護します。マルチレイヤー技術は、コンテナエスケープ、カーネルエクスプロイト、権限昇格の試みなどの脅威を特定するクラウドネイティブの動作およびエクスプロイトランタイム検出を含むランサムウェアやその他の高度な攻撃から保護します。さらに、クラウドの支出を簡単に把握することもできます。アカウントが悪用されているかどうかを迅速に特定し、攻撃者が多額の請求を行う前に追い出すことができます。

まとめ：

ランサムウェア、DDoS 攻撃、エクスプロイト、フィッシングなどのサイバー攻撃は、政府機関のビジネスや評判に深刻な影響を与える可能性があります。IT 環境と機密データを保護するには、統合されたセキュリティアプローチが必要です。

ソフォスは、次世代のサービスとテクノロジーを使用して、システムとデータが存在する場所を問わず保護すると同時に、セキュリティ管理を単一のベンダーに統合できます。ソフォスのすべてのソリューションは、統合されたクラウドベース管理コンソールである Sophos Central を介して制御されます。これにより、製品間でリアルタイムの情報共有、一元管理、自動化されたインシデント対応、より深いインサイトが可能になります。これらすべてが連携することで、IT チームの効率を高めながら保護がさらに強化されます。

ソフォスが政府機関をどのように保護しているかの詳細、およびお客様の要件についてのご相談は、ソフォス営業部にお問い合わせいただくか、ソフォスのセキュリティ専門家からのコールバックをリクエストしてください。

2023-04-21 JP-WP (NP)

SOPHOS