連邦政府機関 オンラインセキュリティの 再構成

サイバー脅威や攻撃者の追跡よりも優れた分離モデルでマルウェア、ランサムウェア、スパイウェア、ゼロデイ攻撃からユーザーとデータを保護しましょう。

eBook

MENLO SECURITY

政府機関でも
サイバーセキュリティは回避できません。

ここ数年、連邦政府機関ではセキュリティインシデントが多発しており、その数はますます増加しています。セキュリテインシデントは国家安全保障とグローバルサプライチェーンにとってリスクになっています。

これまでにも社会保障番号や個人の健康記録をはじめとするHIPAAで保護された情報など、膨大な量の個人を特定できる情報（PII）が流出しています。セキュリティインシデントは市民の個人情報の窃取や攻撃に対する脆弱性に起因するため、政府のシステムの完全性に疑問が持たれます。

多くの場合、政府機関で使用している一般的なセキュリティツールや手法ではシステムとデータを保護できません。2020年9月の攻撃[1]ではVPNの既知の弱点を悪用して政府機関の複数のユーザーの認証情報が窃取されましたが、近年の攻撃ではこのように深刻な被害が目立ちます。

> 米国会計検査院はサイバーセキュリティ戦略の開発とシステムの保護に加え、重要なインフラストラクチャ、個人情報、知的財産やPIIなどの機密データを保護するために、政府機関が取るべき**措置を強調**しています。しかし、軍以外の機関では年間80億ドル以上をサイバーセキュリティに**費やしている**にもかかわらず、脅威は存在し続けています。

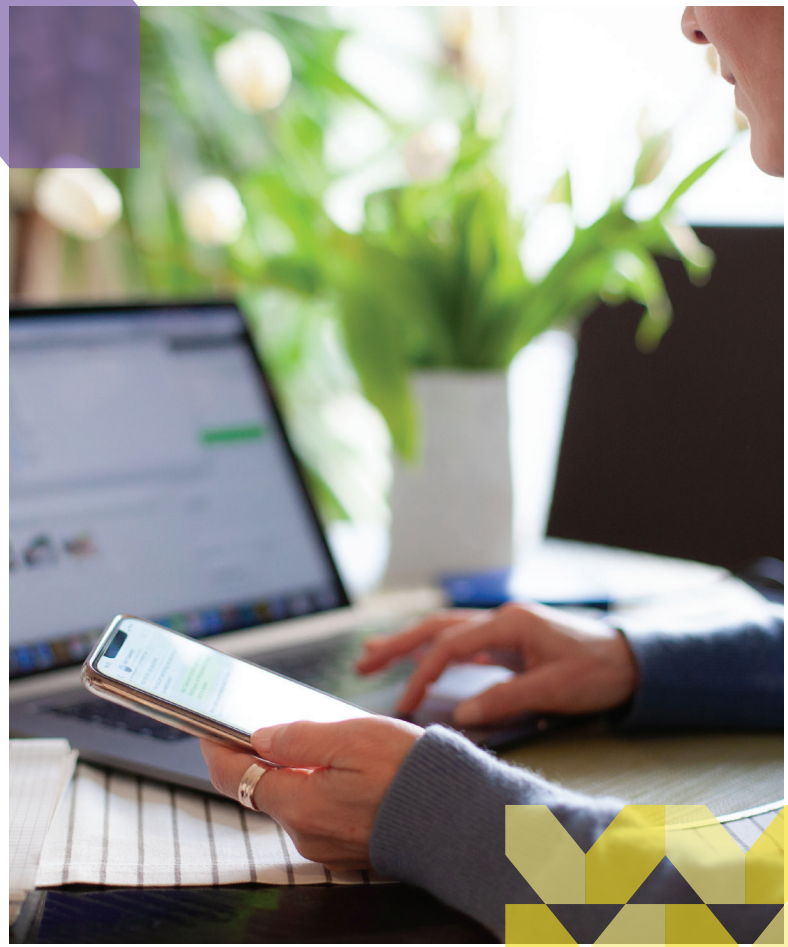
攻撃者はフィッシングメール、不正なWebサイト、破壊的なコードが仕込まれた添付ファイルなどを使用して政府のシステムに侵入し、データの窃取や任務の妨害を試みます。特に被害が深刻なのはゼロデイ攻撃です。この攻撃では不正なコードが何ヵ月も休眠状態で潜伏した後にシステムやデータの破壊や乗っ取りなどの被害が発生するため、検知したときにはすでに手遅れになります。

ここで、ひとつの疑問が生じます。政府機関はセキュリティを確保するためにソフトウェアと機器に大規模な投資をしているにもかかわらず、なぜサイバー攻撃は増加し、被害が絶えないのでしょうか[2]。

人間の習性との戦い

定期的なトレーニング[3]と頻繁な警告[4]を受けているにもかかわらず、フィッシングメールのリンクをクリックしたり不審なWebサイトにアクセスするユーザーが後を絶ちません。Menlo Securityが連邦政府の職員を対象に90日間にわたって実施した調査でも危険な傾向が見られました。その調査結果を全ユーザーに換算すると、調査対象の政府機関の職員だけで1ヵ月に10万以上の危険なURLにアクセスしていることになるのです。そのリスクを政府全体にまで拡大すると、データやシステムに対するサイバー攻撃を既存のツールだけで防止することが不可能なのは明らかです。

1 https://www.nextgov.com/cybersecurity/2020/09/hackers-take-data-further-reconnaissance-breach-federal-agency/168791/
2 https://www.latimes.com/politics/story/2020-08-28/federal-work-from-home-cybersecurity
3 https://public.cyber.mil/training/phishing-awareness/
4 https://www.cio.gov/assets/resources/telework-infographic.pdf



COVID-19の影響：
エンドポイントの増加によって脆弱性も増加しています。

COVID-19の対応策としてリモートワークが一斉に開始されました。それによって、連邦政府職員の生産性が維持され、政府全体のITモダナイゼーションへの取り組みも加速されました。退役軍人省[5]などの一部の機関では、すでにデジタルトランスフォーメーションのプログラムが開始されていたこともあり、「テレワークの最大化」が急速に進みました。

ただし、リモートのエンドポイント数が増えるとセキュリティリスクも増加します。リモートワーカーのシステムは可視化が不十分な上に、家庭用Wi-Fiの多くは政府機関のネットワークよりも安全性が大幅に劣ります。

6月、PRAC（パンデミック対応説明責任委員会）は環境保護庁と国家偵察局の懸念として「機密以外の作業を在宅で行う職員の過失による機密情報の流出と開示」を報告しています[6]。

リモートワークは今後も長期的に継続される可能性が高く、機密データへのリモートアクセスが増加するなど、リモートワークの環境はシステムとユーザーを狙った攻撃の格好の標的です。

5 https://governmentciomedia.com/va-digital-modernization-foundation-covid-19-response
6 https://www.oversight.gov/sites/default/files/oig-reports/Top%20Challenges%20Facing%20Federal%20Agencies%20-%20COVID-19%20Emergency%20Relief%20and%20Response%20Efforts_1.pdf

予算を増加してもリスクは解消されません。

政府機関はエンドポイント保護、エンタープライズ向けウイルス対策、侵入検知などへの大規模投資を続けていますが、これらのテクノロジでは基本的な問題は解決できません。感染したシステムや不正なシステムにユーザーのシステムが直接接続している限り不正なコードをダウンロードするリスクは存在し続けます。

既存のセキュリティツールは攻撃の発生やシグネチャを確認してから対処する事後対応が主軸のため、それだけではエッジデバイスやIoTデバイスなどを含めたネットワーク全体のシステムとデータを保護することはできません。

サイバーソリューションは、動作に透明性がある必要があります。これにより、複数のゲートやプロセスによって課せられるシステムの負荷や遅延の影響なしに、ユーザーは業務を進めることができます。政府機関はITモダナイゼーションの実現のため、スケーラビリティ、予測可能なSLAと費用対効果を向上するクラウドとSaaSをベースにした運用へ移行する必要があります。

2021年度予算教書で大統領が提案した連邦政府の
サイバーセキュリティ予算：

188億ドル

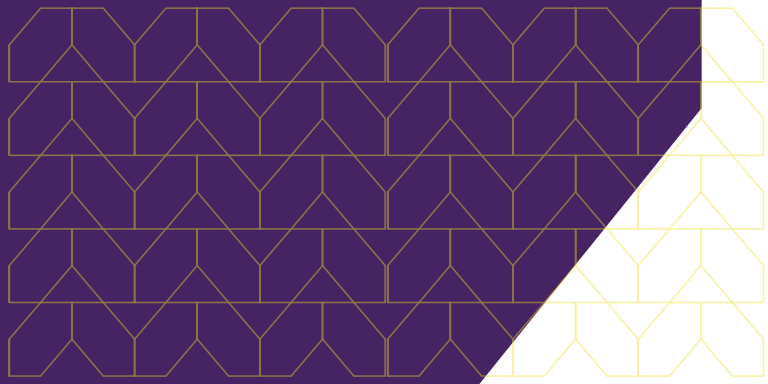
2020年度の予算と同等であるものの2019年度の実際の支出を**18億ドル**以上上回っています。

35万

毎日出現する新しいマルウェアと
不審なアプリケーション

7億

2020年に予測されるマルウェアの検知数



ネットワーク保護の
前提条件を変えましょう。

サイバーセキュリティの製品やサービスの多くは、ネットワークの境界で検知すれば攻撃を阻止できるという単純な考えに基づいて設計されています。しかし、フィッシングメールのように、ユーザーの単純なミスから、セキュリティの仕組みを回避させてしまう攻撃も存在します。未知の攻撃の特定は困難なため、不正なコードを検知するだけでは完璧とはいえません。また、多くの政府機関が使用しているオンプレミス製品は、ユーザーやデータが同じ場所に存在しないと効果を発揮できません。そのため、これらの製品ではすり抜けてしまう脅威に対応する追加の製品が必要になってしまいます。

新しいマルウェアの変種は毎日出現するため、多くのセキュリティ製品はパッチと攻撃シグネチャの更新を定期的に適用する必要があります。しかし、この更新のサイクルを延々と繰り返したところで基本的な問題は解決されないため、ユーザーによる不正なソフトウェアが潜在するWebやメール、ドキュメントへのアクセスを防ぐことはできません。

理論的にはリモートユーザーを脅威から保護するはずのVPNも解決策にはなりません。COVID-19によって多くの政府機関のユーザーが急速にリモートワークに移行しましたが、攻撃者はVPNの弱点を悪用して保護されたシステムにアクセスしています[7]。この場合も問題はセキュリティ製品のアプローチが不十分なことにあり、ネットワーク境界で攻撃を検知して無効化する一方で、ユーザーの通信、検索、コラボレーションもオンラインで行われています。

[7] https://us-cert.cisa.gov/ncas/alerts/aa20-099a

不完全なセキュリティの代償は
データ流出にとどまりません。

セキュリティオペレーションセンター（SOC）の多くは過剰な負荷を抱えています。誤検知のアラームの対応に多くの時間とリソースが費やされます。また、感染したシステムを再構成するために内部と市民向けの両方のサービスを数時間から数日、あるいはそれ以上停止することもあります。これは人件費（疲弊した職員への対応を含む）から公的機関の信頼性まであらゆる要素に影響し、政府機関の業務が中断する可能性もあります。

それに加えて、定期的なサイバー衛生には膨大な時間と労力が必要です。また、更新の間、VPNなどを24時間年中無休で稼働させるシステム[8]も停止することになります。

従来のセキュリティソフトウェアはハードウェアのコストも高額です。一部のツールでは定期的なハードウェアの更新が必要ですが、ソフトウェアと同等かそれ以上の費用がかかることもあります。しかも、そのようなツールで保護したところでソフトウェアのバグ、認識されないネットワークトラフィック、不正なサイトへのユーザーの転送などによってITセキュリティチームのアラート確認作業が軽減されることはありません。

必要なのはAV、マルウェア対策、侵入検知ツールのみに依存した保護ではなく、リスクの高いオンラインリソースからユーザーを分離するソリューションです。それによって、フィッシングメール、不正なWebサイト、感染したダウンロードを悪用したマルウェア、ランサムウェア、スパイウェア、ゼロデイ攻撃などの一般的な攻撃から100%保護できます。

今こそ境界の防御ではなく、主軸をアイソレーションへ移す直接的なアプローチを採用すべきです。

[8] https://us-cert.cisa.gov/ncas/alerts/aa20-073a

真のゼロトラストは
認証以上の効果があります。

ゼロトラストアーキテクチャの効果は絶大ですが、「ゼロトラスト」を名乗るモデルの多くはリソースにオンラインでアクセスするなど、その名のとおりに実践されていません。既存のゼロトラストはリソースへのアクセスを制限しているにすぎず、ユーザーのデバイスとオンラインデータは直接接続しているため悪用されるリスクがあります。

「アイソレーション」のアプローチでは、エンドユーザーとオンラインの間に仮想の「エアギャップ」が作成されます。ノートPCのWebブラウザで直接Webサイトを開く代わりに、クラウドの仮想コンテナによって、対象となるWebサイトのすべてのコンテンツが取得され実行されます。

マルウェアは破棄可能なコンテナに封じ込め、クラウドプラットフォームによって検知されたフィッシングWebサイトは入力制限モードになり、ユーザーには警告文が表示されます。真のゼロトラストセキュリティではこのように、Webリソースはすべて信頼できないという前提に基づいてユーザーは実質的にすべての潜在的な脅威から分離されます。

Webアイソレーションは生産性が向上します。

分離のワークフローを使用することにより、ユーザーのデバイスはサイトに直接接続しないため、電子メールのリンクのクリックやWebサイトの閲覧を通してマルウェアをネットワーク環境に侵入させることは不可能になります。また、ユーザーに対してプロセスは完全に透過的であり、待ち時間やパフォーマンスを犠牲にすることはありません。

アイソレーションモデルでは生産性も向上します。ネットワークはこれまでWebと内部のトラフィックの両方をサポートするように設計されてきましたが、SaaSアプリとマルチメディアサイトへの移行によってWebのニーズは大幅に増加しています。多くの場合、帯域幅を制御する技術により、一部のユーザーや使用時のパフォーマンスに影響が出ます。また、YouTubeやVimeoなどの動画サイトやCNNなどのニュースサイトでは快適に視聴できるように、デフォルトで高解像度のコンテンツを提供しているため多くの帯域幅を消費します。

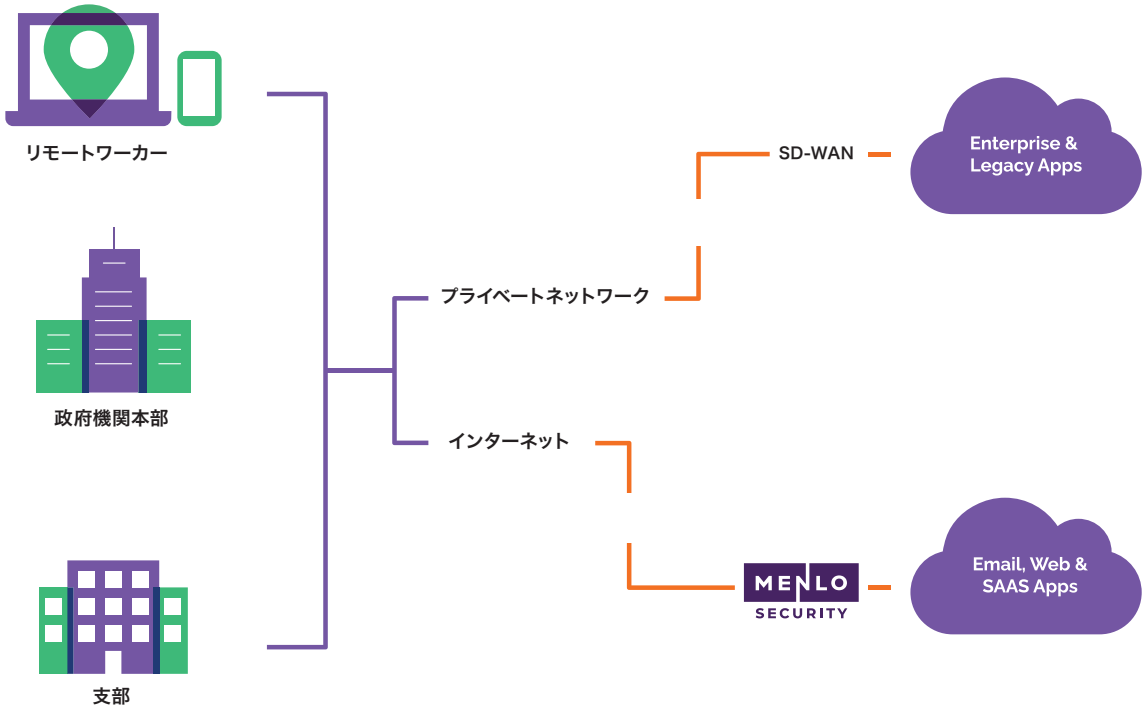
Webのトラフィックを内部ネットワークからスプリットし、政府機関のポリシーに準拠した解像度を動画に使用する（解像度を自動的に制限する）ようクラウドセキュリティプラットフォームを構成すると、仮想サイトのコンテンツの品質を著しく低下させずにエンドユーザーのデバイスに高速に配信することができます。また、それによって接続条件の範囲も広がり、連邦政府の職員はこれまで使用できなかったWebリソースにもアクセスできるようになります。

ボトルネックが解消します。

レイテンシーは生産性に直接影響します。モバイルデバイスや家庭用Wi-Fiへの接続に加え、VPNによって負荷が追加されればトラフィックが遅延する可能性があります。そうなれば、ファイル転送やSaaSアプリの応答の遅延、ビデオ会議の中断やフリーズなど、ユーザーにも影響が及びます。

また、速度低下は政府機関の施設、特に帯域幅を理由にインターネット接続が制限されている場所にも影響します。

このような問題は、クラウドベースのアイソレーションプラットフォームを使用することで解決できます。VPNのスプリットトンネルのアプローチは容易に導入でき、機密以外のトラフィックをクラウドのアイソレーションプラットフォームに直接送信すれば帯域幅の負担が軽減されます。機密以外の情報を処理するためにトラフィックのバックホールに政府のネットワークを使用したり、インターネットアクセスポイント（IAP）や信頼できるインターネット接続（TIC）を経由する必要がなくなり、DoDIN（国防総省情報ネットワーク）や.govのネットワークのリスクが緩和されます。



セキュリティ戦略の進化に不可欠です。

クラウドベースのアイソレーションプラットフォームではデジタルトランスフォーメーション戦略が完全にサポートされ、パブリック、プライベート、ハイブリッドのすべてのクラウド環境と簡単に連携できます。また、既存のネットワークだけでなく将来的な環境の移行もサポートされるため、管理の簡略化とセキュリティ強化のために「総入れ替え」をする必要もありません。

このアプローチのITとセキュリティの管理には以下のような利点もあります。

一元管理

プロトコルをすべてのユーザーに一括して適用でき、Webセキュリティも数十万人のユーザーに対して一括して有効化できます。また、Webの動作がトランスペアレントになりユーザーの接続が可視化されるため、ポリシーの適用を容易に確認できます。

即時の拡張

クラウドの機能を使用できるため、職員のデバイスにエンドポイントソフトウェアをインストールする必要がなくなります。また、プラットフォームは規模の拡大や要件の変化に合わせて自動的に拡張されます。

強力なデータ損失保護機能

クラウドアイソレーションモデルでは過失と不正の両方の内部の脅威からデータを保護できます。データ損失防止（DLP）エンジンでは可視化は制限され、データは難読化されてDLPのスタックからは確認できません。それに対してクラウドアイソレーションでは、保護された環境からのすべてのデータ（ファイル、POSTとPUTのパラメーターなど）が100%可視化されます。また、既存のDLPソリューションとの連携によってセキュリティレベルも向上します。

組織全体の可視化

ユーザーがクリックしたリンクとそのリンク先を確認して、より効果的なサイバー戦略を開発できます。また、包括的でわかりやすいダッシュボードを使用して不審なアクティビティを特定して詳細に分析できます。

ユーザーIDの匿名化

政府機関のユーザーは、連邦政府機関からのトラフィックであることをサイトの所有者に知られずにオンラインリソースを使用する必要があります。また、政府機関の職員が感染したサイトを閲覧すると、攻撃者がその情報を悪用して攻撃を仕掛ける可能性があるため、Webリクエストの送信元を保護することも重要です。クラウドアイソレーションでは、政府機関のネットワークではなく仮想サーバーがリクエストの送信元になり、発信元のIPアドレスも効果的に隠匿されます。

既存のインフラストラクチャとの統合

クラウドアイソレーションソリューションでは既存のSD-WANが強化され、インターネットのトラフィックをクラウドサービスに直接送信できます。また、クラウドアイソレーションをモバイルデバイス管理（MDM）ツールと連携させるとスマートフォンやタブレットも保護できるため、リモートワーク戦略を完全にサポートできます。

あらゆる場所のミッションをサポートします。

テレワーク、現場でのデータ収集、飛行機の整備など、リモートで作業する場合、データ、アプリ、コラボレーションツールへの高速で信頼性の高いアクセスは不可欠です。前に説明したように、TICやIAPからのネットワークトラフィックの分離には帯域幅全体にとって大きなメリットがあります。

安全性に優れたクラウドプラットフォームモデルはMicrosoft 365、G Suite、Box、Salesforce、ServiceNowなど、さまざまなツールとの連携が可能なため、効果的なコラボレーションと生産性の向上も実現します。SaaSアプリは仮想ブラウザでWebサイトのように実行できるため、電子メールの添付ファイルなど、あらゆるドキュメントを安全に開いて共有できます。

アイソレーションモデルでは機密データへのアクセスが**読み取り専用**に制限されるため、ドキュメントのダウンロードにかかる時間が

80%

も削減されます。

あらゆる場所の生産性とセキュリティが向上します。

既存のセキュリティ対策は機能しているとはいえません。生産性と信頼性が向上するどころか攻撃者が新たな脅威を生み出し、セキュリティチームが慌てて対処するという状況が続いています。セキュリティスタックの効果が99.9%であっても、わずか0.1%とはいえシステムとデータには脆弱性が残されています。

攻撃者の後を追うのではなく、攻撃者の何歩も先を行く必要があります。Isolation Core™を搭載したMenlo Security Cloud Platformでは、マルウェア、ランサムウェア、ゼロデイ攻撃に対して妥協のないセキュリティが提供されます。また、使いやすく包括的な管理機能により帯域幅が最適化され、パフォーマンスも向上します。

さらに、フィッシングメールや不審なWebサイトの問題を解決できるため、重要なシステムやデータに対する脅威の大半が排除されます。可視性に優れた動作によりユーザーエクスペリエンスも向上します。その結果、Menlo Security Cloud Platformを導入した政府機関の職員は本来の業務に集中して取り組むことができます。

ランサムウェア、マルウェア、ゼロデイ攻撃を今すぐ撃退しましょう。

フィッシングや不正なWebサイトによる脅威を完全に阻止して、すべてのユーザーのオンラインパフォーマンスを改善する方法をご覧ください。

menlosecurity.com/solutions/government

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com

© 2021 Menlo Security, All RIghts Reserved.

MENLO SECURITY