

マルウェアの 完全な阻止

連邦政府機関の新しい保護戦略

eBook



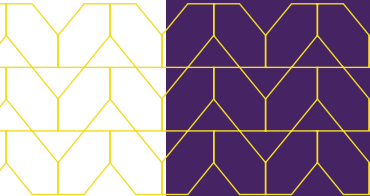
サイバーセキュリティは動く標的 です。

政府機関は攻撃の標的にされないよう強固な保護が必要です。

攻撃者は新しいエクスプロイト、マルウェア、スパイウェア、ランサムウェアの変種を絶えず生み出しています。政府機関の職場環境が進化する中で、新たな脅威に対してどのように保護すればいいのでしょうか。リモートワーカーが大幅に増加したことによりネットワークリソースに対するニーズが大幅に増加し、エンドポイントと攻撃ベクトルも爆発的に増加しています。

リスクと帯域幅への影響を制限するために、多くの政府機関では一部のオンラインリソースを制限していますが、そのために職員の生産性が低下することもあります。また、ITスタッフはリモートワーカーの技術的な問題に対処し、誤報を含む大量のアラームを追跡するなど、常に過剰な業務に追われています。

FISMAの要件に準拠していても、それは必要最低限のセキュリティにすぎません。サイバーソリューションの大半は事後対応型のため、ネットワークが攻撃されてから脅威の検知や対応が実行されます。しかし、それでは手遅れになる可能性があります。



コンプライアンスはセキュリティではありません。連邦政府の基準を満たしているだけのサイバーソリューションでは、組織はWebやクラウドの脅威にさらされるリスクがあります。

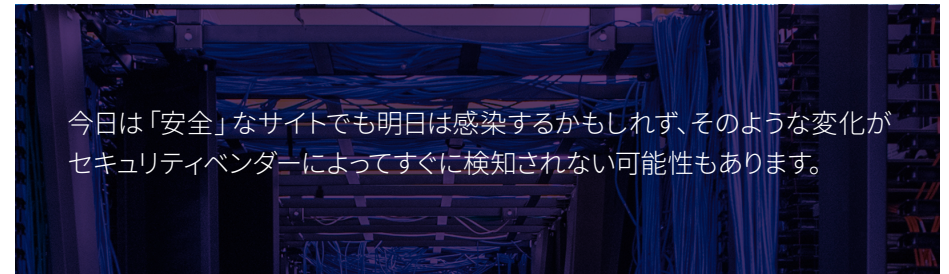




Web、メール、クラウドアプリへのアクセスを制限すると業務に影響します。

連邦政府の業務の大半はオンラインで行われているため、「未検証」のWebサイトへのアクセスを制限すると政府機関の業務効率が損なわれます。ニュースや動画のサイトなどのリソースは、帯域幅に影響するため制限されることがあります。しかし、このような制限によって職員の生産性が低下することもあります。

より多くのWebサイトにアクセスすれば、それだけマルウェアがダウンロードされるリスクも高くなると結論づけるのは論理的ですが、それは「検知して軽減する」という観点からの話です。考えてみてください。あるサイトをブロックしているということは、他のサイトが安全であることを確信しているということです。



今日は「安全」なサイトでも明日は感染するかもしれず、そのような変化がセキュリティベンダーによってすぐに検知されない可能性もあります。

シグネチャの更新が開発、配信、およびインストールされる必要があり、ホワイトリストも更新される必要があります。しかし、その間に多くの被害が発生します。また、帯域幅とセキュリティリソースに問題がある場合、セキュリティの課題はインフラストラクチャだけでは済みません。



問題はインフラストラクチャだけではありません。

2020年のテレワークへの移行がおおむね順調であったため、今後政府機関では通勤する必要のないリモートワーカーの採用が増加するでしょう¹。しかし、リモートワーカーは政府機関のオフィスネットワーク内のユーザーのように保護できません。接続にVPNを使用し、信頼できるインターネット接続 (TIC) でトラフィックを送信すると、不安定なホームネットワークの既知の問題である接続速度の低下に加え、VPNが攻撃の標的になるリスクも上昇します。

TIC 3.0でこれらの問題を解決しようとしても、このセキュリティテクノロジーでは根本的な問題を解決できないだけでなく、運用はサポートされず、ネットワークも保護されず、リソースを浪費するだけです。

旧式のソリューションでは対応できません。

サイバー業界では常にテクノロジーへの追加の投資が求められ、終わりのないアップデートとアップグレードが繰り返されています。オンプレミスのソリューションにはハードウェアの定期的な更新が必要ですが、それにはコストも時間もかかります。また、オンサイトのセキュアWebゲートウェイは大人数のリモートワーカーをサポートするように設計されておらず、クラウドベースのオプションも限られています。

業界ではサイバーソリューションを拡張するとサーバーと容量だけでなく、管理とメンテナンスも増えると言われ、クラウドベースのソリューションでさえ拡張が問題になることがあります。

インフラストラクチャへの投資を増やしたところで、検知ベースのソリューションを採用している限り、すべてのマルウェア攻撃を阻止することはできません。また、ITリソースにとってメンテナンス、管理、アップグレードは大きな負担となり、セキュリティスタッフはアラートの追跡に多くの時間を費やし、信頼性の高い安全なパフォーマンスの確保に集中することができません。

しかし、マルウェアによるネットワークへの侵入やデータの窃取を阻止する簡単で効果的な方法がないわけではありません。



¹ <https://fcw.com/articles/2020/11/19/senate-hsgac-telework-hearing.aspx>

攻撃を検知する代わりに、脅威をアイソレーションしましょう。

検知は事後対応型の対策です。ゴールキーパーがネットを守るように、すり抜けようとする攻撃を阻止することを期待しながら待っているだけです。それに対してアイソレーションは、すべてのオンラインリソースが攻撃される可能性があることを前提とする真のゼロトラストセキュリティです。クラウドベースのアイソレーションでは、攻撃をかわす代わりに、オンプレミスかリモートかにかかわらず、ユーザーのデバイスとWebサイトやWebドキュメントの間に仮想のエアギャップが作成されるため、不正なダウンロードが侵入する隙はありません。

アイソレーションと堅牢な管理制御を使用するクラウドベースのプラットフォームは、ユーザーとWebリソースの間の安全な仲介役として機能します。Webサイトはすべてのマルウェアを排除してから仮想ブラウザで開きます。そのプロセスは透過的なので、ユーザーは通常通りにサイトを開き、クリックしてページを移動したり、ビデオを視聴したり、ドキュメントを閲覧したりすることができます。また、コンテンツはクラウドにとどまるため、ユーザーが隠されたコードをデバイスにダウンロードすることはありません。

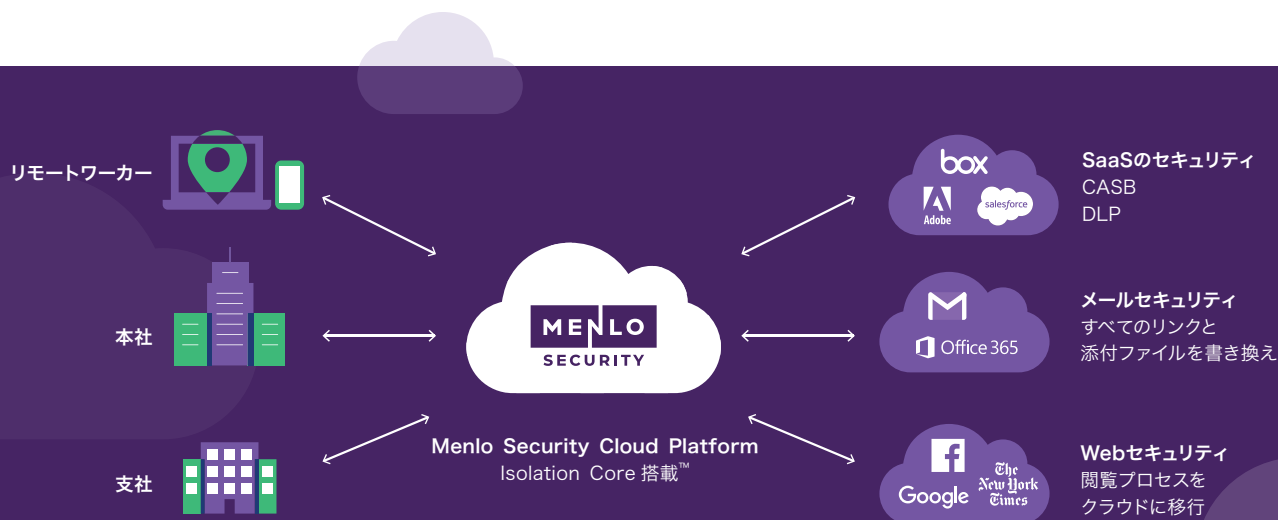
クラウドアイソレーションモデルでは、仮想のエアギャップを作成してマルウェアのダウンロードが阻止されるのに加え、コンテンツ量の多いニュースや動画のサイトを含め、すべてのオンラインリソースにアクセスできます。また、このプラットフォームは政府機関のユーザーとIT組織にとって以下のようなメリットもあります。

- メールリンクを安全な仮想環境で開くことができるため、フィッシングのリスクが最小化されます。
- WebサイトのドキュメントはHTML5を使用してリモートで表示されます(元のドキュメントはTIC経由でダウンロードできます)。
- 連邦政府のIPアドレスは攻撃者には隠匿されます。
- すべてのHTTPストラフィックはSSLベースの攻撃から保護するために検査され、一般的なDLPをバイパスする行為が阻止されます。

アイソレーションを活用したMenlo Security Cloud Platformではこれらすべてのメリットに加え、リソースの使用と複雑さを低減する機能も提供されます。また、Menlo Securityのソリューションでは帯域幅の要件と遅延が大幅に減少します。



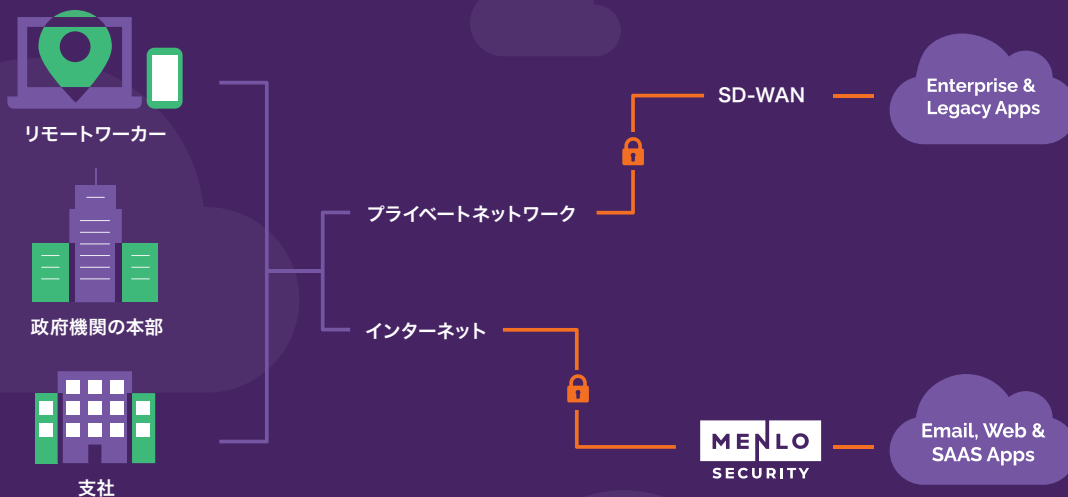
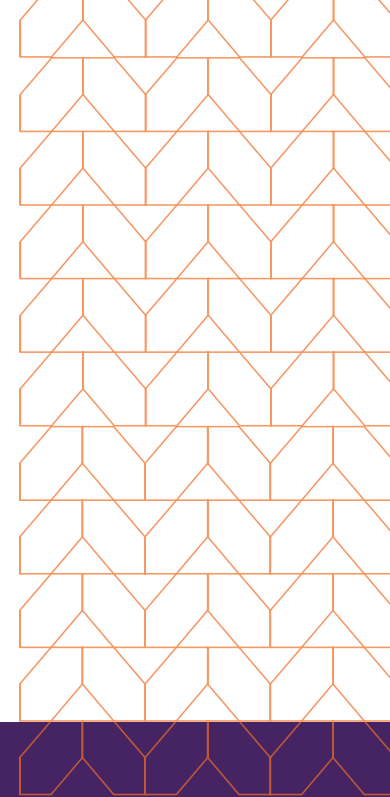
グラフィック、動画、対話型などを含め、弊社のクラウドプラットフォームでは帯域幅を6倍以上節約できます。



オンラインソースからマルウェアをダウンロードすることがないため、政府機関はシステムのクリーンアップと再構成にかかるコストと時間を節約できます。また、メンテナンスとシステム管理のコストも大幅に削減され、クラウドプラットフォームの使用によって高価なハードウェアの更新やソフトウェアのアップグレードも不要になります。

セキュリティチームは膨大なアラートの追跡、ホワイトリストと脅威シグネチャの更新、脅威と脆弱性の検知と対応など、多くの作業に追われていますが、Menlo Securityソリューションを使用することで、これらの作業は不要になり、スタッフの作業負荷が大幅に軽減されます。

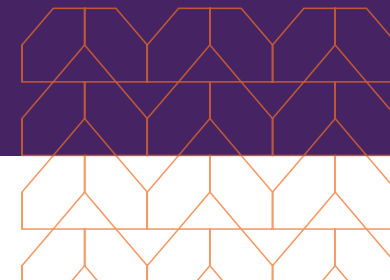
検知ベースのセキュリティテクノロジーにすでかなりの投資をしている場合でも、Menlo Securityソリューションなら既存のセキュリティスタックとシームレスに連携させてその機能を強化できます。また、Menlo Securityなら脅威の検知が不十分なツールもより柔軟で安全なソリューションに容易に移行できます。



スプリットVPNソリューションなら効果的に保護できます。

VPNは内部リソースにアクセスするリモートユーザーには必要とされますが、リモートワーカーが増加するとライセンスや容量の追加などのコストがかかり、移行の障害になることもあります。

Menlo Security Cloud PlatformにWebトラフィックを直接送信すれば、ユーザーがVPNを使用するのは安全なネットワークが必要なときだけに制限できます。その結果、パフォーマンスの向上とオーバーヘッドの減少が実現し、管理も簡略化されます。



真のセキュリティは完璧なセキュリティです。

今後、リモートワーカーはオンラインリソースをますます利用するようになるでしょう。Menlo Securityのアイソレーションテクノロジーでは、接続する場所にかかわらずユーザーがサポートされ、政府機関の業務に必要なツールと情報への透過的で高速なアクセスが提供されます。

Menlo Security Cloud Platformは軍を含む多様な政府機関に採用された実績のある特許取得済みのプロアクティブなソリューションです。実装が容易でグローバルに拡張でき、セキュリティアラートが減少するなど、すぐに効果を発揮します。また、プロセスが簡略化されるため、政府機関のリモートワーカーの生産性が向上し、不注意によってマルウェアをダウンロードすることもあります。

セキュリティ侵害の90%がWebサイトやメールが起点となっていることを考えると、検知ベースのセキュリティではデータ、システム、スタッフを十分に保護することはできません。しかし、このような注目を浴びるようなセキュリティ侵害は避けたいものです。アイソレーションならマルウェア、スパイウェア、ランサムウェア、ゼロデイ攻撃のネットワークへの侵入を完全に阻止できます。



マルウェアの追跡より 効果的な方法があります。

Menlo Security Cloud Platformの独自のアイソレーションテクノロジーによってマルウェアを完全に阻止する方法の詳細とデモについては以下をクリックしてください。

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com



© 2021 Menlo Security, All Rights Reserved.

