未来の業務環境をセキュリティ保護

ニューノーマルにおいてユーザーにセキュリティを提供するためのガイド

eBook

MENLO SECURITY

目次

テレワークというニューノーマル

今や、世界中にいるほとんどのナレッジワーカーにとって、通勤は過去のものとなっています。新型コロナウイルス感染症（COVID-19）の世界的パンデミック以前でさえ、グローバル化、クラウドへの移行、利便性、進歩的な業務ポリシーの影響で、テレワークが増加する傾向がありました。COVID-19以前に戻る兆しはほとんどない現在、テレワークへの移行はさらに加速しています。

テレワーカーがオフィスから離れた場所で生産性を維持するには、業務に必要な企業／インターネットリソースに信頼できる方法で安全にアクセスする必要があります。その1つが、サービスとしてのソフトウェア（SaaS）プラットフォームや、企業ファイアウォールで保護された業務アプリケーションへのセキュアなアクセスです。

テレワーカー向けのツールキット：

クラウドアプリ

生産性およびコラボレーション	Microsoft Office 365、G Suite、Trello
ビデオ会議	Microsoft Teams、Zoom、Webex、GoToMeeting
ストレージ	OneDrive、Google Drive、Box、Dropbox
CRM	Salesforce
人事および財務会計	QuickBooks、Clockify、ClickTime
ソフトウェア開発	Pivotal、Jira、GitHub

データセンター

生産性およびコラボレーション	Exchange、SharePoint
CRM	Siebel、Oracle
ERP	SAP、Oracle
人事および財務会計	SAP

深刻なセキュリティリスクとなるテレワーカー

「信頼できる方法で企業／インターネットリソースに安全にアクセスできる方法をテレワーカーに提供する」ことは、言うは易しですが、実現することは難しい課題です。インターネットは、巧妙なサイバー脅威の巣窟となっており、大胆な攻撃が増加の一途をたどっています。サイバー攻撃者は、ソーシャルエンジニアリングを使用し、他者を信頼する人間の特性や、無関心や興味に付け込んでデバイスに侵入します。そして、デバイス内で数日、数週間、または数ヵ月潜伏して機密性の高い情報や脆弱性を収集し、ミッションクリティカルなビジネスソリューションに侵入します。

今日、ユーザー／Webサイト間接続のセキュリティ強化を目的に、Webサイトの90%でhttpsプロトコルが使用されています。一見すると、セキュリティ保護に効果をあげているように見えますが、実際には、事態を深刻にする要因となっています。SaaSプラットフォームやWebメールへのログイン時、ユーザーの認証情報は暗号化されます。ところが、従来型のセキュリティインフラストラクチャはSSL通信を監視できません。したがって、SSL通信は格好の標的となってしまうのです。情報アクセスに使用されるWebベースツールとテレワーカー間の通信を可視化および制御する機能がない場合、ユーザーのデバイスがセキュリティ侵害されているかどうかを識別することは不可能です。

90%
Webサイトの90%がhttpsプロトコルを使用

25%
フィッシングリンクの25%が従来型のWebフィルタリングソリューションを迂回

500超
ブラウザーには常に500を超える脆弱性が存在

25%
Webサイトの25%が30日で感染

セキュリティの4大脅威：

フィッシング

フィッシングは、悪意のあるリンクのクリックや悪意のあるドキュメントのダウンロードを実行させようとする一般的な攻撃戦術です。フィッシングメールは、信頼できるソース（ブランド、友人、同僚など）を装って送信され、標的を絞った攻撃もあります。業務で関わるブランドの数が増えるほど、フィッシング攻撃に対する脆弱性も高まります。驚くことに、Menlo Labsが収集したデータによると、フィッシングリンクの25%が従来のWebフィルタリングソリューションを迂回してしまいます。フィッシングは、大規模な攻撃を容易に実行できるだけでなく、ユーザーがクリックする時点での識別／阻止が難しいことから、今日のサイバー攻撃の中でも最も手強い攻撃の1つとなっています。

ランサムウェア

ランサムウェアは、ユーザーが身代金を支払うまで、ユーザーのデバイス、データ、SaaSアカウントを使用不能にするサイバー攻撃です。フィッシングと同様に、ランサムウェアも、悪意のあるリンクのクリックや細工されたファイルのダウンロードへと誘導します。

ゼロデイ

ゼロデイ攻撃は、パッチの適用されていないソフトウェア、ファームウェア、ハードウェアに存在する未知の脆弱性を狙う攻撃です。特に、クラウドアプリやSaaSプラットフォームを使用する環境では、ブラウザーは脆弱点になります。cvedetails.comによると、ブラウザーには常に500を超える脆弱点が存在します。したがって、攻撃者にとってブラウザーは格好の標的であり、デジタル／クラウドトランスフォーメーションへと舵を切った組織にとっては非常に深刻なリスクとなります。

ドライブバイ

ドライブバイ攻撃は、細工したWebサイトから悪意のあるドキュメントをダウンロードさせようとする攻撃です。一般的に、ドライブバイでは、信頼済みサイトのセキュリティを侵害し、そこから攻撃を仕掛けます。検知とブロックのアプローチに基づく従来のセキュリティインフラストラクチャでは、ブラックリストとホワイトリストを最新の状態に維持しない限り、新たに登場したドライブバイを検知することはできません。Menlo Labsが収集したデータによると、2020年4月の30日間で、グローバルWebサイトのうち、「良好」から「不良」へと移行したサイトは25%にものぼります。

既存のセキュリティソリューションが直面するネットワークパフォーマンスの問題

ほとんどの組織は、テレワーカーをセキュリティ保護する方法として、仮想プライベートネットワーク（VPN）接続を介して、中央のデータセンターにすべてのトラフィックをルーティングしています。これはハブアンドスポークネットワーキングモデルと呼ばれ、すべてのリモートトラフィックを監視し、社内セキュリティポリシーとコントロールを適用できます。

ところが、VPNを介してすべてのトラフィックをルーティングすると、遅延、パフォーマンス低下、ユーザー操作の中断を引き起こすボトルネックが発生してしまいます。たとえば、シカゴにいるリモートユーザーがインドにあるAWSサーバーに接続する場合を考えてみましょう。ユーザーのトラフィックは、Webサーバーに直接接続するのではなく、ボストンにあるデータセンターにVPNを介して接続し、そこからインドのAWSサーバーへと接続するため、伝送距離が非常に長くなります。特にSaaSプラットフォームの場合、ほとんどが常時接続されるため、ユーザーは長距離伝送とトラフィックの増加による負荷を感じます。

テレワークがニューノーマルとなり、トラフィックが増加する今、SaaSセッションのクラッシュ、頻繁に中断が発生するビデオ会議、ファイルにアクセスできない状況など、パフォーマンスにさまざまな問題が発生しています。残念ながら、多くの組織は、セキュリティよりもシームレスなブラウジングを重視しています。このような組織は、セキュリティ対策を講じることなく、スプリットトンネリングでユーザーをインターネットに直接接続しています。

インターネットトラフィックをデータセントラフィックから分離することで、VPNトラフィックは最大70%低減され、リモートアクセスの課題である帯域幅やパフォーマンスの問題を軽減できます。インターネットへの直接アクセスでWebサイト、クラウドアプリ、SaaSプラットフォームを使用できるとしても、セキュリティ対策がなくデータを危険にさらす方法は、決して適切ではありません。

セキュリティと新たな働き方を両立する実用ガイド

VPNをバイパスするインターネットトラフィックをセキュリティ保護する唯一の方法が、クラウド対応のセキュリティサービスです。クラウドセキュリティは、職場、顧客サイト、ホームオフィス、公衆Wi-Fiなど、場所を問わずユーザーにセキュリティポリシーを適用します。クラウドベースのセキュアWebゲートウェイ（SWG）は、中央のセキュリティ制御ポイントとして機能し、すべてのトラフィックをコントロールします。クラウド内のユビキタスで独立したセキュリティ階層となり、すべてのトラフィックがここを経由します。この階層でセキュリティポリシーを適用することで、ファイアウォールに保護されたユーザーや公衆Wi-Fiからログインするユーザーなど、ユーザーの場所を問わずポリシーを適用することが可能になります。

アイソレーションは、クラウド対応セキュリティサービスの基盤です。不完全な「検知と対応」のアプローチよりも格段に安全性の高い「アイソレーションまたはブロック」のアプローチを、サイバーセキュリティに適用することが可能になります。このアプローチでは、悪意のある既知のトラフィックを即座にブロックし、残りのトラフィックを取得してクラウドベースのブラウザーで実行します。

ユビキタスなクラウドによるアイソレーションを使ったWebトラフィックのセキュリティ保護では、ローカルなインターネットブレイクアウトを各ユーザーに対して簡単かつ効率的に提供することができます。SWGは、全データの可視化に加えて、URLフィルタリング、SaaSアクセス制御、データ漏洩防止（DLP）などのセキュリティ制御機能も備えています。

ユースケース

SaaSへの高速アクセスと導入展開の簡素化を可能にするローカルインターネットブレイクアウト

URLフィルタリング、SaaSアクセス制御、可視化

データとトラフィックのセキュリティ保護と可視化

DLPと可視化

ユースケース1:

ホームWi-Fiを使用するユーザーにSaaSへの高速アクセスを提供

- 遅延の短縮を目的に、POP（最寄りの接続ポイント）がユーザーの近くにあることを確認
- POP経由でローカルコンテンツにアクセス可能にする
- SaaSプラットフォームへの接続をテスト
- SLAに関する詳細とダウンタイムの履歴を尋ねる
- コーヒーショップモード（パブリックWi-Fiに接続するユーザーに適用するポリシーを改善）をリクエスト

クラウドセキュリティにより、ユーザーがあらゆる場所からWebサイト、Webアプリ、SaaSプラットフォームにアクセスでき、しかもセキュリティが犠牲になることはありません。クラウドはユビキタスな特性を持つため、ユーザーがどこからログインしても、そのトラフィックを社内セキュリティポリシーで監視およびコントロールできます。また、優れたパフォーマンスと信頼性という、Webへの直接アクセスがもたらすメリットも享受できます。

クラウドベースのSWGは、セキュアなローカルインターネットブレイクアウトをスケーラブルな方法で実現します。SWGは、クラウドで提供されるソフトウェアであるため、リモートユーザーに導入しやすく、VPNなどのレガシーネットワークアーキテクチャとの統合も可能です。スプリットトンネリングは、データセンターに伝送されるトラフィックをセキュリティ保護します。これに対してSWGは、共通の社内セキュリティポリシーですべてのインターネットトラフィックをセキュリティ保護し、あらゆるタイプのトラフィックを網羅する一貫した堅牢なセキュリティ体制を実現します。SWGとスプリットトンネリングを組み合わせることで、リモートユーザーは、社内／インターネットリソースに安全かつ高速にアクセスできるようになります。

ベンダーチェックリスト

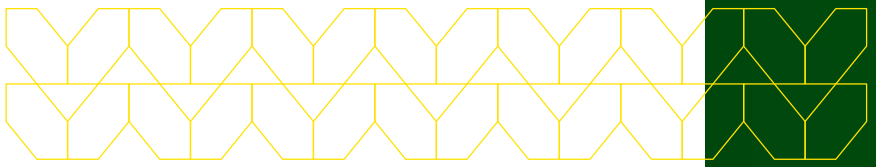
ユースケース2：

オフィス以外のユーザーを セキュリティ保護および可視化

さまざまな場所からログインするリモートユーザーに、クラウドを使用して一貫したセキュリティポリシーを適用する機能があれば、堅牢なセキュリティ体制を実現できるだけでなく、サイバー脅威の可視化も可能になります。アイソレーションまたはブロックのアプローチは、100%マルウェアフリーのメールとWebブラウジングを実現します。ユーザーは安心してWebブラウジングやクリックを実行できるようになり、組織はリスクから解放されます。

ユーザーが悪意のあるリンクのクリックや細工されたドキュメントのダウンロードを実行した場合、ホワイトリスト内のWebサイトが突然セキュリティ侵害された場合、ブラウザーにパッチを適用していない場合、そしてユーザーがマルウェアに感染した場合も、心配ありません。すべてクラウド内で実行され、ユーザーのデバイス、企業ネットワーク、ビジネスソリューションへのアクセスが切断されます。

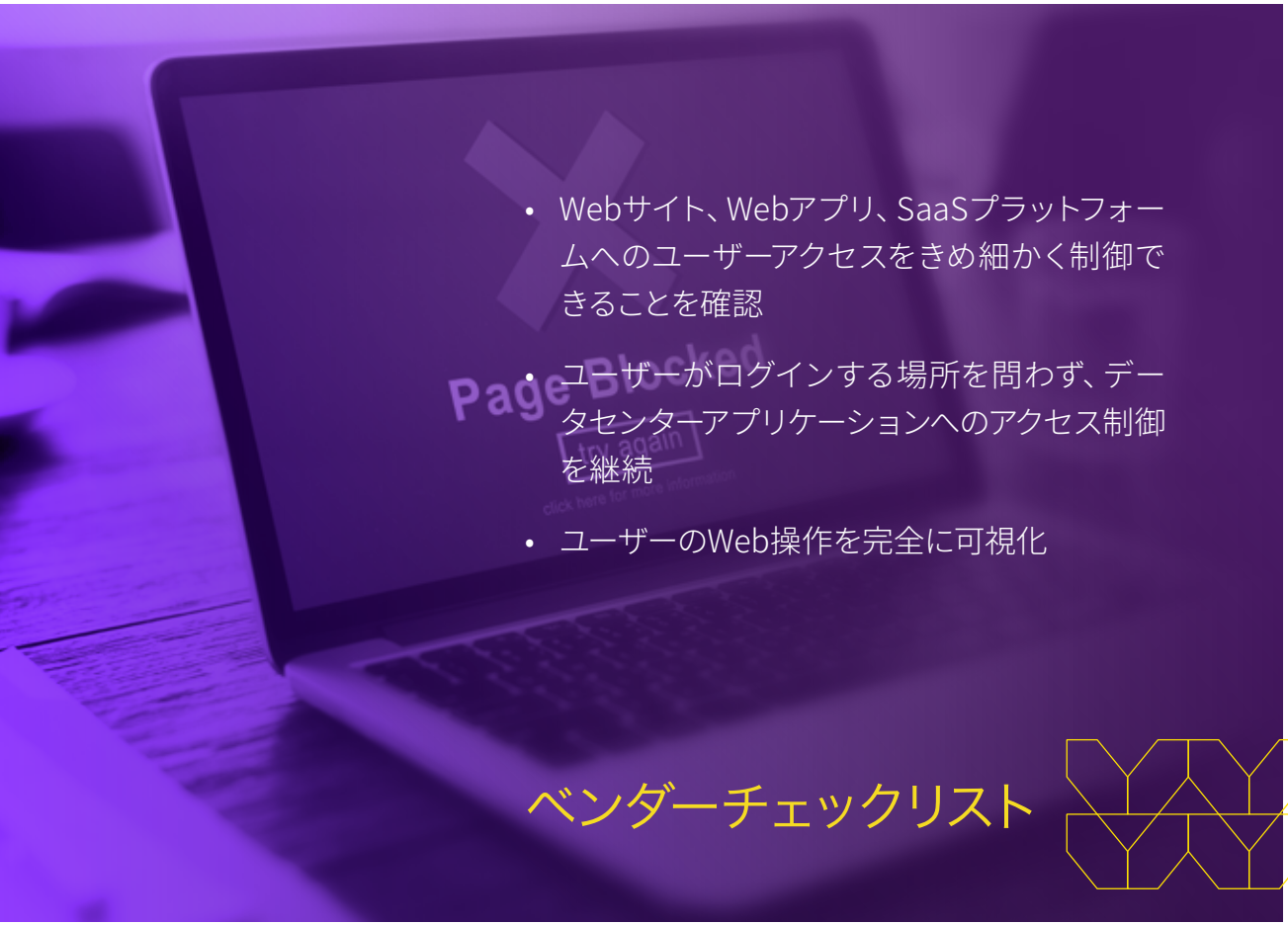
- セキュリティを損なうことなく、ドキュメントにアクセス
- ユーザーが危険なサイトにアクセスしても、セキュリティ保護を維持
- サイバーセキュリティ脅威を可視化



ベンダーチェックリスト

ユースケース3：

ユーザーによるインターネットアクセスを制御



- Webサイト、Webアプリ、SaaSプラットフォームへのユーザーアクセスをきめ細かく制御できることを確認
- ユーザーがログインする場所を問わず、データセンターアプリケーションへのアクセス制御を継続
- ユーザーのWeb操作を完全に可視化

全トラフィックへの社内セキュリティポリシーの適用は、インターネットトラフィックとSaaSプラットフォームに対するアクセス制御の強化につながります。また、URLフィルタリングにより、ユーザーのWeb操作を監視し、特定のWebサイトやクラウドベースアプリへのアクセスを制御できます。ソーシャルメディアや既知のポルノハブなど、業務中に不適切なコンテンツにアクセスすることを禁止した利用規定（AUP）を設けることも可能です。さらに、内部脅威対策プログラムの一貫として、クラウドストレージやファイル転送サイトといった未承認アプリの使用を制限する方法もあります。クラウドセキュリティは、オフィス勤務とテレワークを問わず、すべてのユーザーに一貫したアクセスポリシーを適用します。

ベンダーチェックリスト

ユースケース4:

データ漏洩防止と可視化

可視化は、堅牢なDLPプログラムを実現する鍵です。可視化には、誰がいつどのようなデータにアクセスしているかを明確に把握する必要があります。クラウドベースのSWGは、企業ファイアウォールに保護されているかどうかにかかわらず、すべてのユーザーとデバイスのデータを一貫した方法で保護します。もちろん、従来型のセキュリティインフラストラクチャでも同様の処理はできますが、VPNを介して全トラフィックをデータセンターにバックホールしなければなりません。上記で説明したように、この戦略はネットワークパフォーマンスとユーザーの生産性を低下させてしまいます。

- データとユーザーの場所に関係なく、きめ細かいDLP制御を実行
- データ分類のカバレッジを確認
- DLPプログラムに完全な可視化機能を組み込む
- イベントに基づいてアラートと通知をトリガー

ベンダーチェックリスト

テレワーカーに対応したクラウドベースSWGを導入する4つのステップ

今日のテレワーカーのニーズを考えると、従来のハブアンドスポーク型ネットワークセキュリティモデルからクラウドベースのアプローチへの移行は極めて重要であり、大きな一歩となります。ところが、多くの組織にとって、既存のセキュリティインフラストラクチャの総入れ替えは不可能です。したがって、計画に基づいた実践的なアプローチでクラウドセキュリティを導入する方法が必要です。

01

主なWebサイトカテゴリをクラウドに移行

まず、高負荷のメディアを使用するWebサイトのセキュリティ保護をクラウドに移行します。これによってVPNトラフィックを70%低減することが可能であり、帯域幅の負荷が目に見えて軽減されます。SWGによるフィルタリングでは、Webサイト上のコンテンツを取得し、クラウドで実行してから、安全なコンテンツのみをユーザーデバイスへと送信します。ニーズに基づいて、カテゴリを1つずつ移行してください。これにより、ユーザー操作が中断されることなく、無理なく学習でき、リスク軽減にもつながります。ここでのベストプラクティスとしては、帯域幅使用量の大きなWebサイトや高リスクのWebサイトから移行に着手してください。移行の効果をすぐに実感できるため、主なユーザーやステークホルダーのサポートを得やすくなります。

02

ドキュメントを確実に保護

SaaSプラットフォームとクラウドストレージは、利用率が高まり、ユーザーは高い信頼を寄せています。その一方で、企業ファイアウォールの外側にあってオンプレミスのウイルス対策／マルウェア対策ソリューションで保護できないため、格好の攻撃対象となりつつあります。そのセキュリティ機能をクラウドへと移行し、SWGですべてのコンテンツのアイソレーションを行うことで、データセンターを経由するドキュメントやクラウド上のライブドキュメントを含めたあらゆるドキュメントの保護が可能になります。

03

きめ細かいユーザーアクセスポリシーを設定

第3のステップとして、ユーザーがアクセスするWebサイトとSaaSプラットフォームの可視化とコントロールを目的に、きめ細かいユーザーアクセスポリシーを設定します。セキュリティ制御とポリシーをインターネットトラフィックへと拡張することで、侵害されたリンク、Webサイト、ドキュメントを誤ってクリックし、デバイスや企業ネットワークの感染を引き起こす不安からユーザーを解放します。

04

SSLトラフィックを検査

最後のステップとして、クラウドベースSWG経由でSSLトラフィックをルーティングします。これにより、暗号化されたSSLトラフィックを可視化し、悪意のある活動を完全に排除できます。現在、Webサイトの90%がhttpsプロトコルを使用しており、このようなWebサイトの可視化とコントロールを強化する上で不可欠な機能です。

「ほぼ安全」の壁を超える

「ほぼ安全」という現在のセキュリティパラダイムから脱却し、既知と未知の脅威から組織を完全に保護します。これは、攻撃者とのいたちごっこや運まかせのセキュリティ保護ではなく、攻撃者が侵入できない確実な保護体制の整備を指します。

SaaSのパフォーマンスを向上

低遅延接続でSaaSをフル活用することで、Office 365をはじめとするSaaSアプリケーションのメリットを最大限に引き出します。Isolation Core™ 実装のセキュリティクラウドは、セキュリティを犠牲にすることなく、クラウドの優位性を実現します。

ネイティブなユーザー操作性を実現

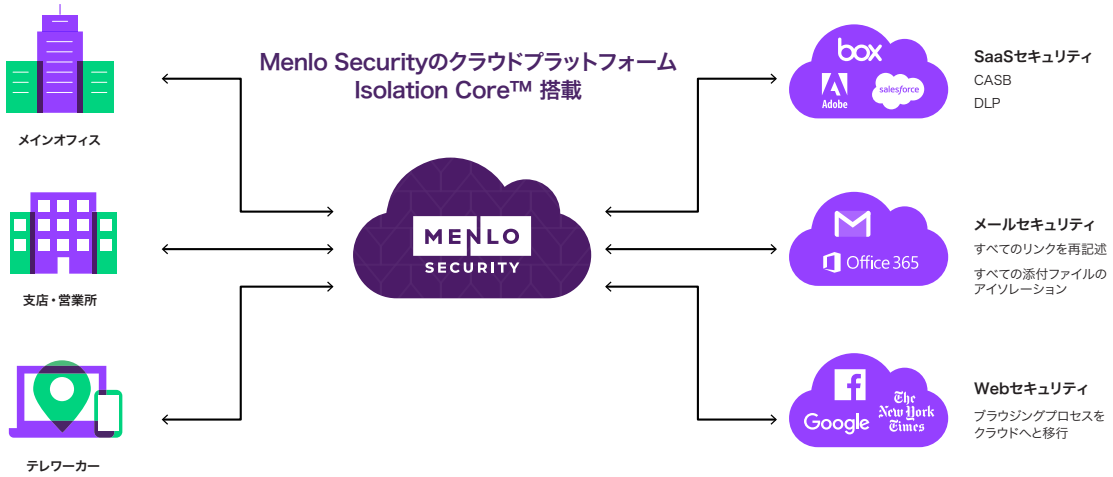
Menlo Securityは、ユーザー操作性に妥協することなく、セキュリティトランスフォーメーションを推進します。ユーザーがシステム変更に気付かないことも多いほど影響は小さい一方で、セキュリティは強化されるため、不安なくWebサイトのブラウジングやクリックを、場所を問わず実行できます。

完全なデータの可視化とポリシー制御を実現

クラウドをセキュリティ制御ポイントへと転換することで、アプリケーションとデータの完全な可視化が可能になります。Isolation Core™ は、SSL検査をインラインで実行し、すべてのユーザーとデバイスにポリシーとコントロールを適用します。

Menlo Security：妥協のないセキュリティ

セキュリティトランスフォーメーションなくして、クラウドトランスフォーメーションは実現できません。Menlo Securityは、企業／インターネットリソースへの安全で信頼できるアクセスと生産性の維持を目的に、テレワーク環境を見直すソリューションを提供しています。従来のセキュリティインフラストラクチャは、ユーザーの操作性とセキュリティを両立できませんでした。Menlo Securityは、常に変化を続ける常時接続環境で競争力を高めるには、この2つを両立する必要があることを認識しており、妥協のないセキュリティを提供しています。



お問い合わせ

業務で必要な企業／インターネットリソースに安全にアクセスする機能をテレワーカーに提供する方法について、詳しくはこちらにお問い合わせください。

www.menlosecurity.com

(650) 614 1705 | ask@menlosecurity.com

MENLO SECURITY