MENLO SECURITY

ブラウザセキュリティ サービスエッジ

ブラウザセキュリティの課題を解決し、SSE（Security Service Edge）の本来の目標を達成

SaaSおよびクラウドコンピューティングへの移行という世界的なトレンドや生成AIの爆発的な普及は、世界的パンデミックとも組み合わさり、私たちの働き方や働く場所に劇的な変化をもたらしました。それに伴い、ITを取り巻く業務環境やワークフローも急速に変化しています。これらの変化によって従来型のテクノロジーの多くが影響を受け、その効果にも変化が見られます。変化に対応するために、ITチームには迅速な対応が求められましたが、その結果、従来型のシステムの一部はそのままの形でクラウドに詰め込まれることになりました。

セキュリティサービスエッジ：クラウドへの水平移動？

セキュリティサービスエッジ（SSE）は、急激な変化が起きた2020年よりも前に登場したテクノロジーで、主要なネットワークサービスについてベンダーの集約とクラウドベースの管理を行うことで、いくつかの変化に対処しようとしてきました。これらのサービスには、ゼロトラストアクセス、クラウドアクセスセキュリティブローカー（CASB）、セキュアWebゲートウェイ（SWG）などが含まれます。しかし残念ながら、アプライアンスからクラウド上のソフトウェアに単純に移行しただけでは、現代のユーザーのニーズの変化には対応できません。しかもこの「クラウドへの水平移動」は、導入展開と管理にさらなるコストがかかることが判明し、SSEは必要以上に複雑になっています。その結果ITチームは、複雑なネットワーク変更要件やクライアントの導入展開における課題や、終わりのない設定作業のような長く複雑なSSEの導入展開に苦労することになりました。

SOLUTION BRIEF

SSEのデメリット

コストと複雑さ

業界アナリストがSSEを考え出してそれに名前を与えた後、業界では激しい争奪戦が起こりました。大手企業がSSEの部品を入手するために中小企業を買収したため、買収から統合までに長い時間とコストがかかり、その結果（多くの場合顧客側に）以下のようなデメリットが生じました：

- ベンダーが買収および統合のためのコストを転嫁したため、SSE製品は購入者や業界アナリストからは高価なものに見えました。
- 統合に伴う問題により、SSE製品には複数の管理コンソールが必要となり、場合によってはユーザーエクスペリエンスがまったく異なるものになることもありました。たとえば、人気のアナリストによるセキュリティサービスエッジ（SSE）[1] に関する記事では、最大3つのコンソールを備えた製品までは除外しないという基準が示されています。

ネットワーク統合

企業のネットワークを、トランプのカードを使って慎重に作られた家だと想像してみて下さい。そこにはパブリッククラウドがあり、プライベートデータセンターがあり、すべての支店が繊細なWANリンクで接続されています。すべては、GRE[2] トンネル（安全な経路と考えてください）、慎重に計画されたIPアドレス範囲（CIDR[3] ブロック）、信頼できるファイアウォールやルーターなどでまとめられています。

そこにクラウドベースのセキュリティ（SSE）を追加しようとするのは、カードでできた家に突然新しいものをねじ込もうとしているようなものです。そのために必要なことは：

- **新しいデータ経路の確保：**SSEプロバイダーへの経路を確保するために、ファイアウォールやその他のDMZ[4] に穴を開ける方法を見つけます
- **トンネルの統合：**従来のセキュアな経路とSSEプロバイダーからの新しい経路を統合します
- **セキュリティポリシーの整理：**既存のセキュリティルールとSSEサービスのセキュリティルールの競合を特定して解決します
- **ルーティングテーブルの調整：**変更に対応するためにネットワークのロードマップを更新します

セキュリティフォーラムで、人々がこれらの課題について絶えず議論しているのも不思議ではありません！
複雑なネットワークにSSEを導入することで、バランスを取るのが難しくなる可能性がありますし、たとえこれらの課題をすべて解決したとしても、SSEは昨今の組織における主要なワークスペースとなっているブラウザには対応していないのです。

[1] SASEは、厳密にはSSEのスーパーセットとされていますが、実際にはこれら2つのソリューションで名前が挙がるベンダーは異なっており、両者が異なる製品であることを示しています。SSEはサブセットであるにも関わらず、多くのSSE製品には最大3つの管理インターフェースが含まれています。
[2] Generic Routing Encapsulation
[3] Classless Inter-Domain Routing
[4] Demilitarized Zone（非武装地帯）：世界中のIT部門が使う比喩表現で、データセンターの境界を表し、通常は「データセンター」側と「インターネットルーター」側の2つのファイアウォールの間に配置されます。

ブラウザセキュリティの課題

SSEが提供している防御は、ブラウザを標的とした攻撃やデータ窃取を阻止することはできません。これらの課題を防御レイヤーごとに見てみましょう：

- SSE SWGが提供する防御は、依然としてネットワークセキュリティ指向のままです。ほとんどのSWGでは、個々のデータパケットに脅威が含まれていないかどうかを完全に調べることができます。しかし、HTMLスマグリングなどの攻撃では、複数のHTTPパケットにマルウェアが埋め込まれ、さらに複数のパケットを集約するデバイスでの検知を防ぐために、無作為にパケットへの埋め込みをスキップします。Webセッション全体を処理するのは、ネットワークレイヤーではなくアプリケーションとして機能するフルブラウザだけなのです。そのため、完全なブラウザコンテキストを使って攻撃を防ぐことができるのは、ブラウザセキュリティのみであるということになります。
- SSEが提供するCASBは、SWGと同様にネットワーク指向ではありますが、アプリケーション層の制御も試みています。とはいえ、CASBの中核機能はクラウドへのアクセスと利用を管理することです。CASBの中には、パスワードで保護され暗号化されたファイルのダウンロードを認識してフラグを立てることができるものもありますが、これらのファイルをブロックしたり、暗号化されたファイルを復号化して検査できるようにパスワードの入力を促したりできるのは、専用のブラウザセキュリティだけです。もしかするとCASBベンダーは、どのような組織にも脆弱な内部Webアプリケーションがあることを忘れているのかもしれません。

SSEは従来型のネットワークセキュリティをクラウド側から管理しますが、依然としてインフラストラクチャに重点を置いたネットワークセキュリティであることに変わりはありません。最新のコンピューティング環境とは、場所やデバイスに関係なく、アプリケーションとアプリケーションへのアクセスを提供するものです。Menlo Browser SSEは、ネットワークではなくアプリケーションにフォーカスしています。

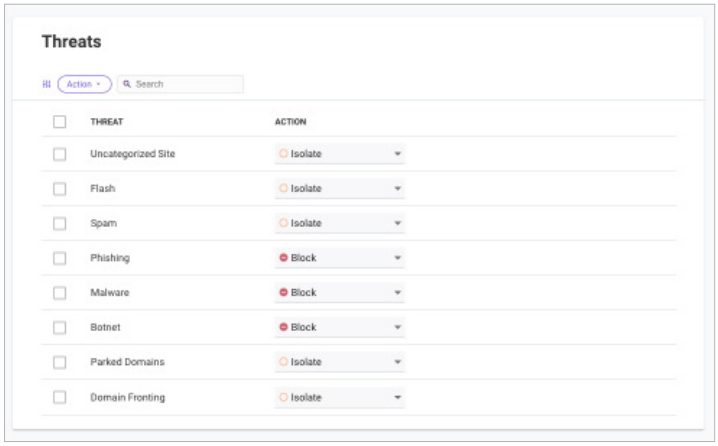
SSEの目標を達成し、ブラウザセキュリティの課題を解決する

ほとんどのユーザーは、多くのアプリケーションにWebブラウザ経由でアクセスしているため、ブラウザを考慮に入れないアプローチを採用する場合には大きなリスクが生じます。Menlo Security のブラウザSSE ソリューションを導入すれば、包括的なブラウザセキュリティと組み合わせてSSEの目標を達成することができ、すべてのユーザー活動におけるブラウザセキュリティの課題を大規模に解決します。その間、ユーザーは使い慣れたブラウザを使い続けることができます。

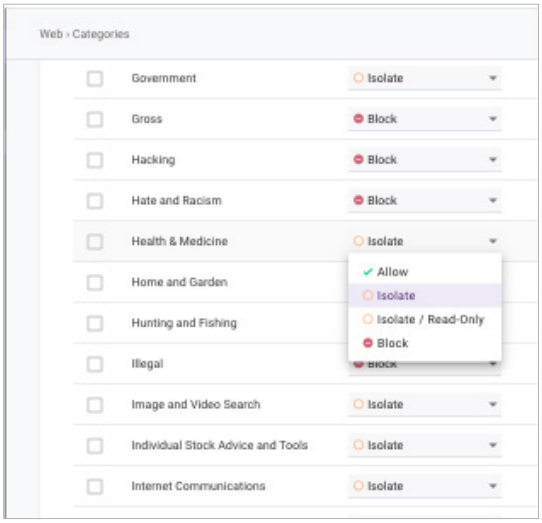
セキュアWebゲートウェイではブラウザセキュリティの課題を解決できない

SSE SWGは既知の脅威を阻止しますが、Menlo Security のブラウザSSE ソリューションの中核機能であるSecure Cloud Browserは、すべてのWebトラフィックを危険なものとして扱うことで、ゼロデイフィッシングや回避型ランサムウェアを阻止します。

Menlo Secure Enterprise Browserは、SWGのすべての機能に加え、さらに多くの機能を提供します。SWG機能の中核にはトラフィックのカテゴリー分けとURLフィルタリングが含まれ、カテゴリー分けされていないURLの一部をブロックすることができます。しかしSWGはネットワークデバイスであり、HTTP/S経由で送信されるすべての内容を確認することはできません。ブラウザセキュリティの課題を解決するためには、ネットワークセキュリティよりもアプリケーションセキュリティが重要です。SWGによる防御しか無い場合、ローカルブラウザは完全なWebトランザクションを読み込んでしまうため、そのセッションに埋め込まれたマルウェアの影響を受ける可能性があります。Secure Cloud Browserは、HTMLスマグリングや暗号化されたファイル内のマルウェア、LURE攻撃などの、SWGでは阻止できない検知回避型脅威（HEAT）を阻止します。



SWGでは脅威を分離（アイソレーション）できません



SWGはWebセッションを分離（アイソレーション）できません

SaaS Governance

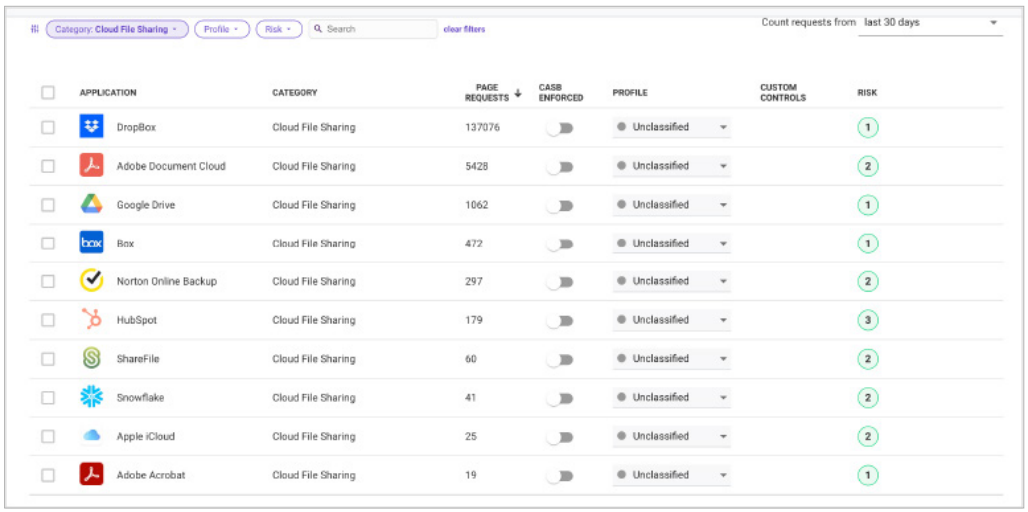
現在主流となっているSSE CASBは、どのユーザーが許可されるか、どのSaaSサイトが許可されるかを制御します。これらの制御に加えて、SSE CASBにはデータ漏洩防止の機能も含まれる場合がありますが、多くの場合それだけでは不十分です。

Menlo SecurityのブラウザSSEソリューションが提供するSaaS Governanceは、直感的な管理ワークフローとユーザーフレンドリーなエクスペリエンスを活用し、CASBと同等の制御を可能にします。

Menlo SaaS Governanceは、数千におよぶ既知のWebアプリケーションの厳選されたリストをベースとしており、その数は常に増加しています。

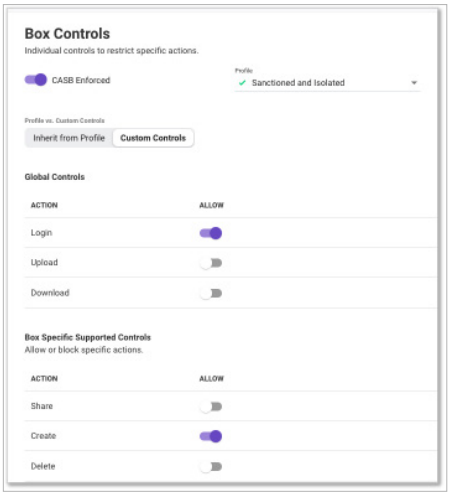
直感的で高速なSaaSガバナンスのワークフロー

Cloud Application Discoveryは、組織内のSaaS利用を管理するために必要な情報を提供します。



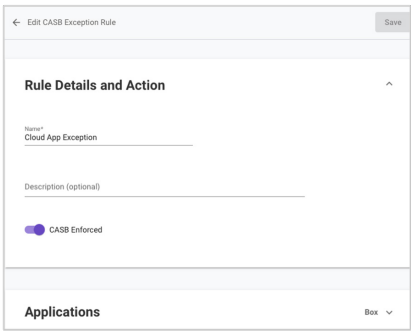
この図では、Cloud Application Discoveryが重要なデータセキュリティとDLPカテゴリー（クラウドファイル共有）でフィルタリングされています

ルールは、セキュリティと柔軟性のユニークな組み合わせを提供し、アプリケーションごとにルールを割り当てることができます。以下はBox.comのルール管理の例ですが、どのCASBもこれを再現することはできませんでした。Menlo Securityはブラウザセッションを分離してHTMLをサニタイズし、機械学習を適用してフィッシング攻撃を阻止します。

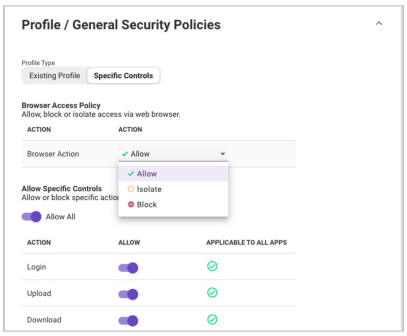


Menlo Securityでは、アプリケーションごとにルールを割り当てることができます

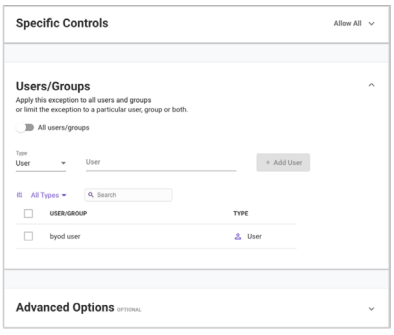
例外：最小権限アクセスにおいては、Webプロパティのデフォルトルールが常にすべてのユーザーとグループに適用されなければなりません。しかしMenlo Cloud Governanceは、他のMenlo Securityのポリシーと同様に、同じレベルの粒度でデフォルトルールの例外を提供します。以下の図は、クラウドガバナンスでの例外属性の一部を示しています。さらに、すべての主要なサードパーティ認証プロバイダーとMenlo Securityとの包括的な統合により、ユーザーがサービスにログインする際に、ログイン許可に対する時間と場所両方の制御が可能です。



この例外はbox.comに適用されます



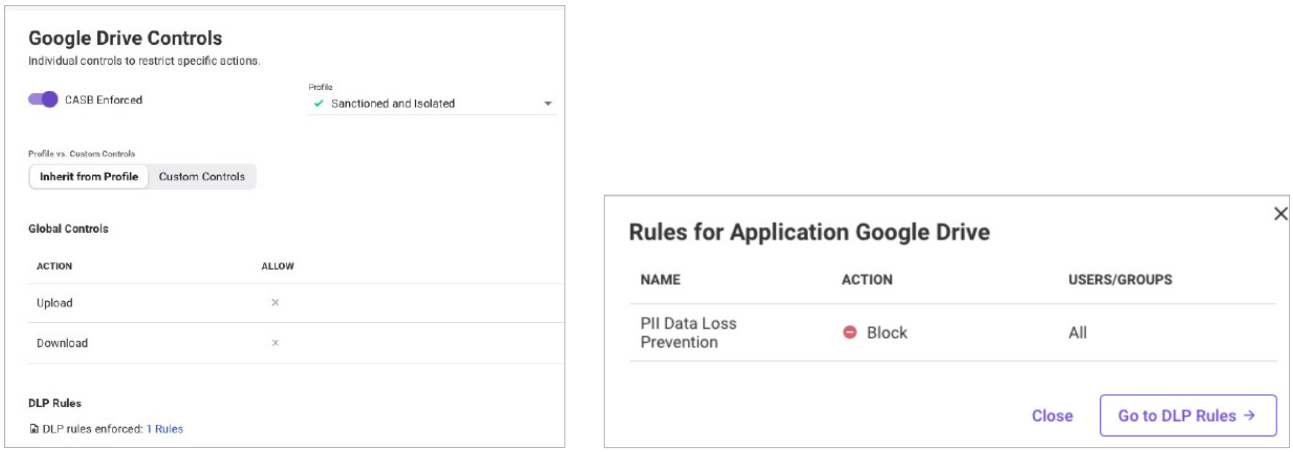
この例外により、Webサイトのデフォルトルールでは許可されていなかったファイルのアップロードまたはダウンロードが許可されます



ここでは、例外を単一のユーザーに割り当てています

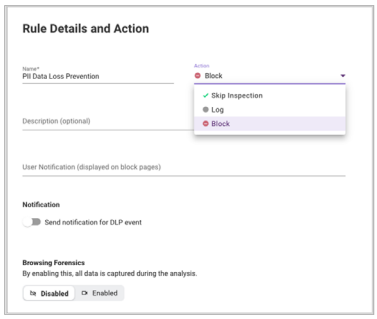
データ漏洩防止（DLP）

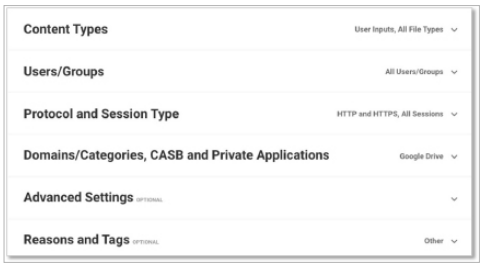
Menlo SaaS Governanceには400個におよぶDLP辞書が組み込まれ、顧客の要件に基づいてさらに追加できる柔軟性を備えており、強力なブラウザ中心のデータ漏洩防止（DLP）制御が可能です。辞書はテンプレートにまとめることができ、単一の辞書または辞書のテンプレートをDLPルールにバインドすることができます。DLPルールを作成した後、それをSaaSガバナンスプロファイルにバインドすることができます。



上の図から、GoogleドライブのDLPルールは、個人を特定できる情報（PII：Personally Identifiable Information）の流出を防ぐことを目的としていることがわかります

以下に、DLPルールの詳細な例を示します。左側のペインには高レベルのルール属性が表示され、DLPルールに関連したWebセッションをMenlo Browsing Forensicsがキャプチャするかどうかが示されています。中央のペインには、このルールには6つのDLP辞書が含まれることが示されています。右側のペインには、さらに6つの拡張可能なルール属性が表示され、直感的な順序で表示されています。





最も厳格に管理し、ポリシー例外を慎重に検討したとしても、大規模な組織では事故や不正行為が発生する可能性があります。Menlo Security Browsing Forensicsは、記録されたWebセッションにSOCの担当者が即座にアクセスできるため、検知したインシデントの迅速な解決が可能です。上記のSaaSアプリケーションに関連づけられたDLPルールに見られるように、Menlo Browsing ForensicsはMenlo SaaS Governanceと統合されています。

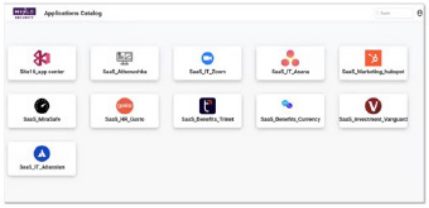
Menlo SaaS Governanceは、厳選された3,000個におよぶSaaSアプリケーションの使用に関して、シンプルなワークフローと管理しやすい制御を可能にします。Browser SSEはブラウザ中心のDLPとBrowsing Forensicsによって SaaSアプリケーションを制御し、ブラウザのセキュリティギャップを解消します。

ゼロトラストアクセス

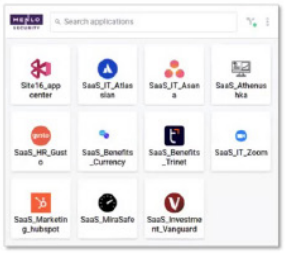
ゼロトラストの基本原則には、ユーザーとデバイスの検証と認証、最小権限アクセス、継続的な監視と検証が含まれます。これらの原則の多くは、ゼロトラストネットワークアクセス（ZTNA）として初めてネットワークに実装されました。しかし、私たちは現在アプリケーション中心の世界に住んでおり、ZTNAはゼロトラストアクセス（ZTA）へと進化しています。しかし残念ながら、ほとんどのゼロトラスト製品はブラウザのセキュリティギャップを埋めることができていません。

Menlo SecurityのブラウザSSEソリューションは、Menlo Secure Application Accessを通じてゼロトラストアクセスを提供します。これは迅速に導入展開でき、単一のコンソールから簡単に管理できます。Menlo Secure Application AccessをMenlo Secure Cloud Browserと組み合わせることで、包括的なゼロトラストアクセスを実現します。

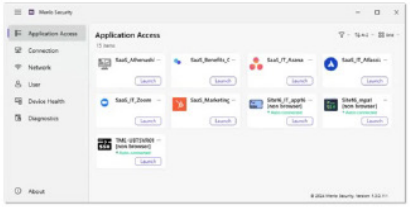
現在主流のSSE ZTNAは、ほぼ例外なくクライアント経由で提供されるため、導入展開および管理のために多くのデスクトップソフトウェアが必要になります。それとは対照的に、Menlo Securityのゼロトラストアクセスソリューションはユーザーのブラウザを通じて社内外のWebプロパティへのアクセスを行います。クライアントレスのアクセスは、契約社員やゲストが関与する場合、あるいはBYODなど、さまざまなユースケースにおいて最適です。



Secure Application Access
Webポータル画面



Secure Application Access
ブラウザ拡張画面



Secure Application Access
Menlo Security Client画面

ブラウザに重点を置いたZTAは、許可された社内アプリケーションやSaaSアプリケーションへの、最小権限ベースのセキュアなアクセスを実現します。また、Secure Cloud Browserを通じてデータが保護されるため、従来のVPNを廃止してトラフィックのバックホールを無くすことができます。

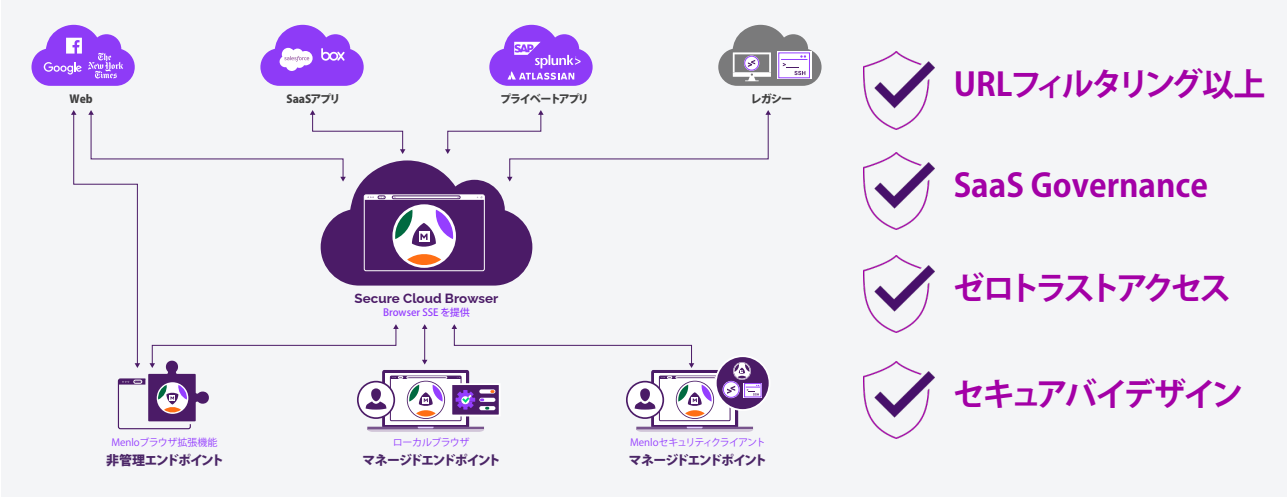
ZTAにおけるMenlo Securityのデータ漏洩防止（DLP）ソリューションのメリットを理解するためには、次の2つの形式のデータリスクを理解することが重要です：

- **ダウンロード：**内部Webサイトからのコンテンツのダウンロードは、データ流出における重要なベクトルです。Menlo Securityのポリシーでは、ユーザーが社内のWebアプリケーションからファイルやアーカイブをダウンロードすることを完全に禁止することも、Menlo SecurityのDLPがスキャンして許可されていないコンテンツが含まれていないことを確認してからダウンロードを許可することもできます。
- **アップロード：**インターネットへのコンテンツのアップロードは、もう一つの重要なデータ流出ベクトルです。Menlo Securityのポリシーでは、ユーザーが特定のWebサイトにファイルやアーカイブをアップロードすることを禁止したり、アップロードを完全にブロックしたりできます。または、Menlo SecurityのDLPがファイルやアーカイブをスキャンして許可されていないコンテンツがないかどうかを確認した後に、ユーザーにファイルやアーカイブのアップロードを許可することもできます。さらに、Menlo Securityはペースト時にもポリシーを適用しますから、データ流出におけるもう一つの重要なベクトルも排除することができます。

Menlo SaaS Governanceと同様に、Menlo Browsing ForensicsはMenlo Secure Application Accessと統合されています。この組み合わせにより、許可されたユーザーは必要なコンテンツのみにアクセスできるようになり、ブラウジングセッション中のユーザー行動を完全に把握することができます。最小権限アクセスと完全な可視性は、ゼロトラストへの道のりにおける2つの重要なステップです。

まとめ

Webブラウザは現代の企業で最も広く使用されているアプリケーションであり、人々が業務を行うワークスペースでもあります。ブラウザへの依存が進み、アプリケーションがクラウドに移行し続ける状況下で、ブラウザのセキュリティ課題を解消することが急務となっていますが、これは他のSSE製品では解決できない問題です。
Menlo SecurityのブラウザSSEソリューションなら、2つでも3つでもなく単一の管理コンソールによってブラウザのセキュリティギャップを解消し、SSEの目標を達成できます。ユーザーは、毎月数十億件の保護されたWebセッションにも対応できるクラウドベースのセキュリティを使用して、好きなブラウザで業務を継続することができます。Menlo SecurityのブラウザSSEソリューションは、現代の組織がゼロトラストに求めるセキュリティ、可視性、インシデント対応支援を提供します。



Menlo SecurityのブラウザSSE：Secure Enterprise Browserソリューションに組み込まれています

人々の働き方を安全に守る方法について、詳しくはmenlosecurity.jpをご覧いただくか、japan@menlosecurity.comまでメールでお問い合わせください。

メンロ・セキュリティ・ジャパン株式会社
住所：〒100-0004 東京都千代田区大手町 1-6-1 大手町ビル 4F FINOLAB
Webサイト：https://www.menlosecurity.jp
お問い合わせ先：japan@menlosecurity.com