Data Sheet

Menlo Security Browser Posture Manager

ベンチマークされた実績のあるポリシーを使って組織の攻撃対象を削減

悪質な攻撃者が検知回避型攻撃（HEAT：Highly Evasive and Adaptive Threat）を使って脆弱なブラウザを標的にすることが増えているため、エンタープライズブラウザを保護する必要性が、かつてないほど高まっています。 ブラウザはビジネスで最も広く使用されているアプリケーションであるにもかかわらず、ほとんどの企業はブラウザを適切に管理することができていません。

問題の大きな部分は、「ブラウザの管理」が実際に何を意味するのかということにあります。 Google Chromeには何千ものポリシーがありますが、一般的に使われるのはそのうちのごく一部です。 Microsoft Edgeの傾向も同じで、数千個のポリシーのうち、適用されているものは平均して数十個に過ぎません。 検討すべきポリシーがこれほど多いと、ただでさえ忙しいセキュリティチームが、どのポリシーが重要なのかを正確に把握することは不可能です。 その結果、ブラウザ設定の約45%がエラーを返し、60%以上が明示的な拡張ポリシーを持っています。

知っておくべきこと：

エンタープライズブラウザは2027年までに、エンタープライズアプリケーションの中核的な要素になるでしょう。[1]

Chromeは約4週間ごとにOSの完全リリースを行っています。 セキュリティ修正やソフトウェア更新などのマイナーアップデートは、2〜3週間ごとに行われています。[2]

2022年11月から2023年11月の間に、「緊急」または「重要」に分類されるCVEが175件発行されました。

2023年には、133個の新機能がChromiumに追加されました。

1 https://resources.menlosecurity.com/all-content/state-of-browser-security-defending-browsers-against-zero-hour-phishing-attacks, Emerging Tech: Security — The Future of Enterprise Browsers – Gartner, April 23. 2 https://support.google.com/chrome/a/answer/3168106?hl=en#:~:text=Chrome%20releases%20a%20full%20OS,happen%20every%202%E2%80%933%20weeks

検討すべきポリシーの数が膨大であるだけでなく、ブラウザ自体も絶えず変化しています。 Google Chromeは月に1回、完全なOSリリースを行い、2〜3週間ごとにセキュリティ修正やソフトウェア更新を含むマイナーリリースを行っています。 Microsoft Edgeは現在、Chromiumのスケジュールに従い、4週間ごとにメジャーリリースを行う予定です。更新がセキュリティやバグ修正に基づくものか、新機能の追加に基づくものかにかかわらず、サポートポリシーを最新の状態に保つ作業は、リリースのたびに困難になります。2023年にChromeに導入された新しい設定には、次のようなものがあります：

- **HttpsUpgradesEnabled** ：この設定により、トラフィックのほとんどがHTTPではなくHTTPSを使用するようになります。
- **SafeBrowsingDeepScanningEnabled**：この設定は、ファイルスキャンがどの程度適切に機能するかの懸念、またGoogleと共有されるファイルについてのプライバシー/DLPの問題にも影響します。
- **PasswordSharingEnabled**：Google Canaryで有効になっているこのオプションは、パスワードを家族など他のユーザーと共有できるようにするためのものです。 どのような目的であれ、この設定は企業での使用には不適切と考えられます。
- **HelpMeWriteSettings**：この機能はGmailとGoogle Docsですでに利用可能で、生成AIを使ってテキストを作成します。 他の生成AIの使用と同様に、発生する可能性のあるプライバシーやDLPの問題と利点を比較して検討することが重要です。
- **DomainReliabilityAllowed**：この機能は、ユーザーがGoogleのドメインをリクエストしてそれにアクセスできることを確認するために設計されており、プライバシーに影響を及ぼします。
- **WindowManagementAllowedForUrls**：この設定は、付随するブロックオプションもそうですが、攻撃対象を削減するために導入されたものでしょう。 しかしこれは、セキュリティチームが選択した他の方法と競合する可能性もあります。

これらのさまざまなポリシーオプションは、影響を深く理解してどのように適用するかを決定する必要があり、更新の度にそのような選択肢が多数提示されます。 ブラウザの更新頻度はさらに高まる見込みですが、その理由の一つは、Chromeや他の多くのブラウザのベースとなっているChromiumがオープンソースのプロジェクトだからです。 ほとんどのセキュリティ専門家が同意するように、オープンソースソフトウェアは、クローズドシステムやプロプライエタリシステムでは得られないレベルのテスト、透明性、説明責任を提供します。 しかし欠点があるとすれば、それはオープンソースプロジェクトが提供している可視性そのものにあります。 悪意のある集団はコメントや変更をチェックして、セキュリティ修正をまだ受け取っていないユーザーを狙ったエクスプロイトを作成する可能性があります。：これは「n-dayエクスプロイト」と呼ばれる攻撃です。[2]

ブラウザで独自にポリシーを選択する際の最も困難な側面の1つは、どの変更が企業のセキュリティにとって有意義なのかを判断することです。 この質問に自ら対処する最善の方法は、継続的なデータ駆動型ベンチマークですが、これは最もコストがかかり、難しい方法でもあります。 このプロセスには時間がかかるだけでなく、ほとんどの組織には存在しないセキュリティ担当者も必要になります。

ブラウザは、攻撃者にとって最初の足掛かりとなります。 ブラウザを標的とする脅威、特にHEAT攻撃に分類される脅威の頻度と複雑さが増すにつれ、ブラウザの攻撃可能な領域を保護する重要性はますます高まります。 Menlo Securityの研究者は、回避的と分類される攻撃が206%増加したことを観察しました。[3]

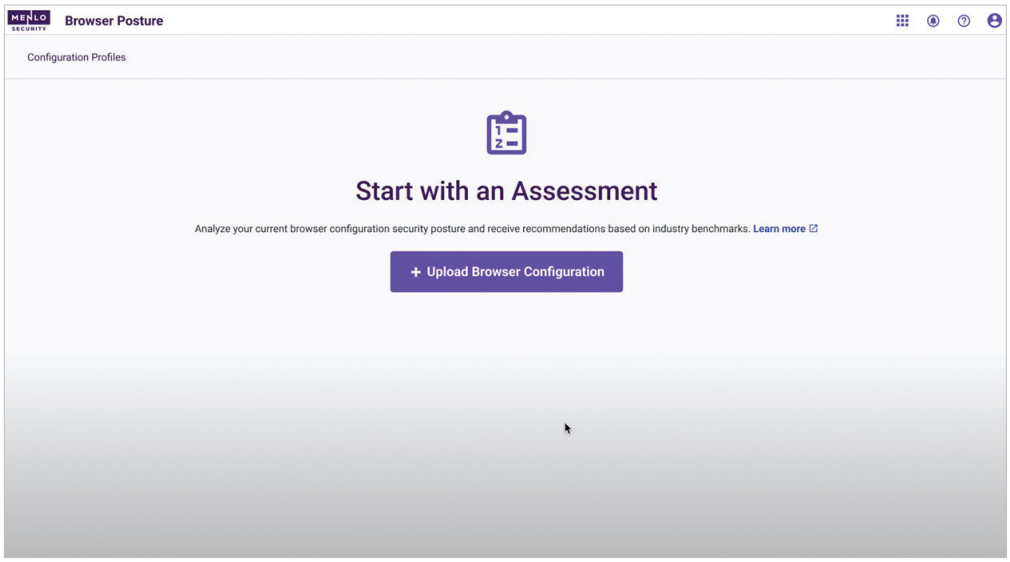
どうすればこの変化についていけるのでしょうか?

ブラウザ内では非常に多くの変更が継続的に発生しているため、すべてに対応するのは非常に困難です。 しかし、Menlo Browser Posture Managerがあれば、その心配はありません。 Menlo Securityはブラウザの変更を常に監視しており、いつでも最新のベンチマークと比較して自分のブラウザの状態を確認できます。

3 https://resources.menlosecurity.com/all-content/state-of-browser-security-defending-browsers-against-zero-hour-phishing-attacks

専門家から実世界のブラウザポリシーのベンチマークを入手

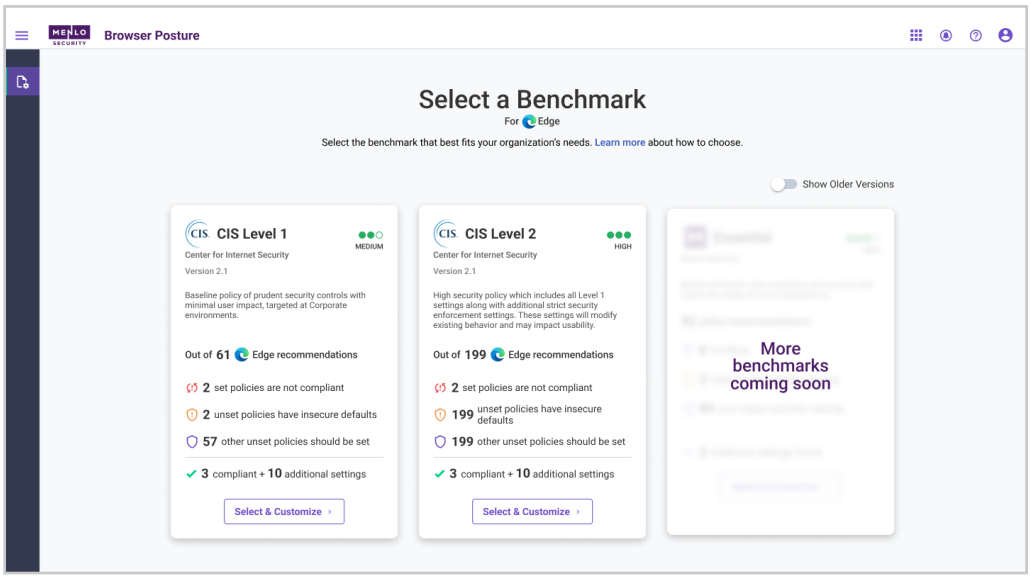
企業向けブラウザセキュリティのリーダーであるMenlo Securityは、新しいBrower Posture Managerにより、このプロセスを簡素化して自動化します。 数回のクリックで、お客様のブラウザセキュリティポリシーが様々なポリシーベンチマークとどのように比較されるのかを厳密に確認することができます。 セキュリティチームが設定ファイルをアップロードするだけで、Menlo Securityがクラス最高の設定内容と比較します。



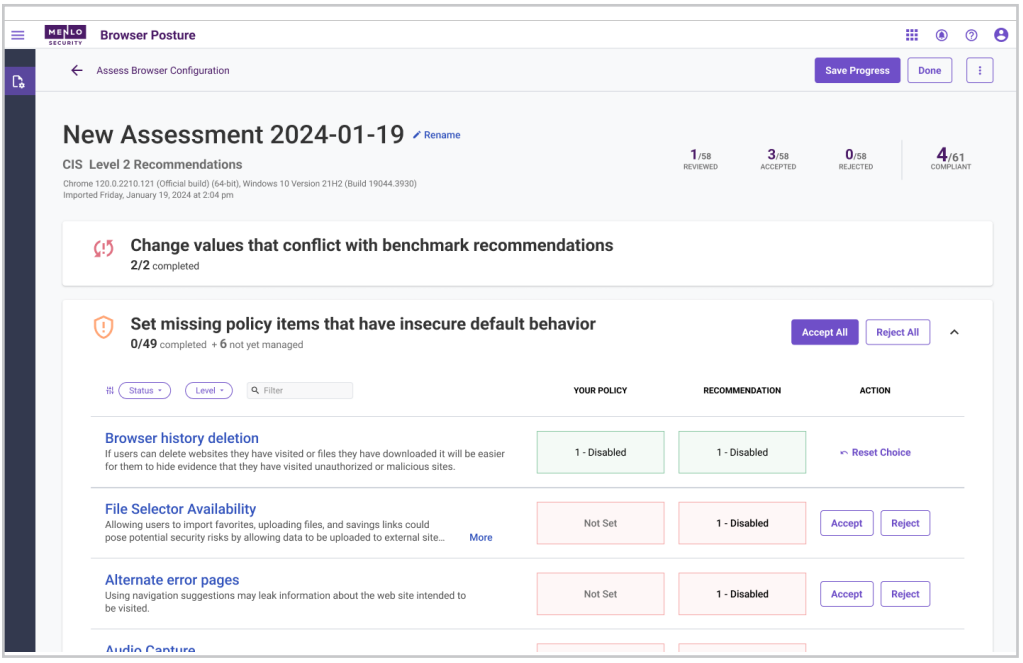
ベンチマークされたポリシーとの比較には、次のようなものがあります：

- Web Bluetooth APIの使用を制御
- Web USB APIの使用を制御
- Chromeリモートデスクトップコントロールへのアクセスを制限
- セキュリティ更新のタイムリーな適用

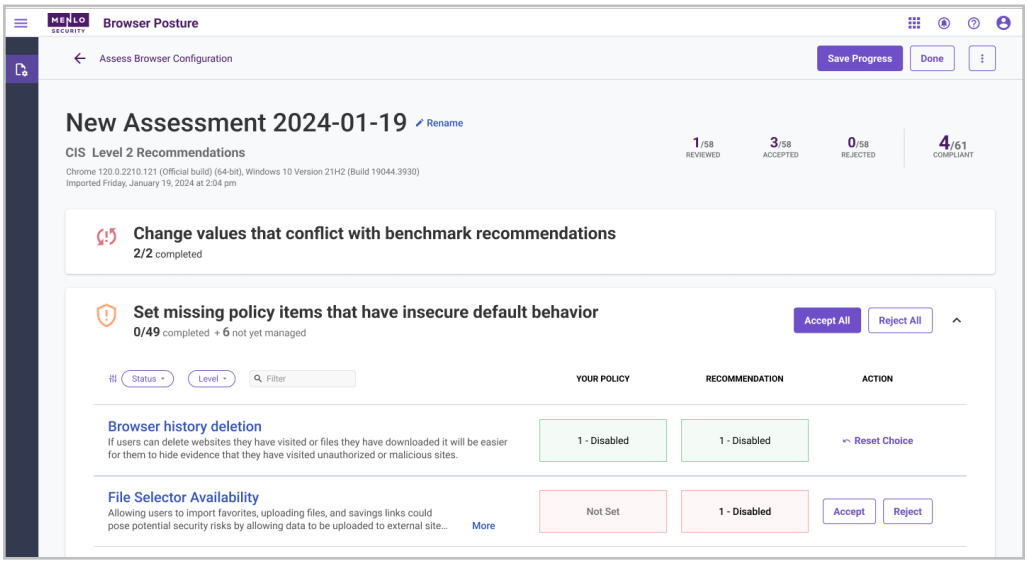
Menlo Security Browser Posture Managerを使用すると、職場で使用されるブラウザの90%以上を占めるChromiumベースのブラウザ（Google ChromeやMicrosoft Edge）を管理することができます。



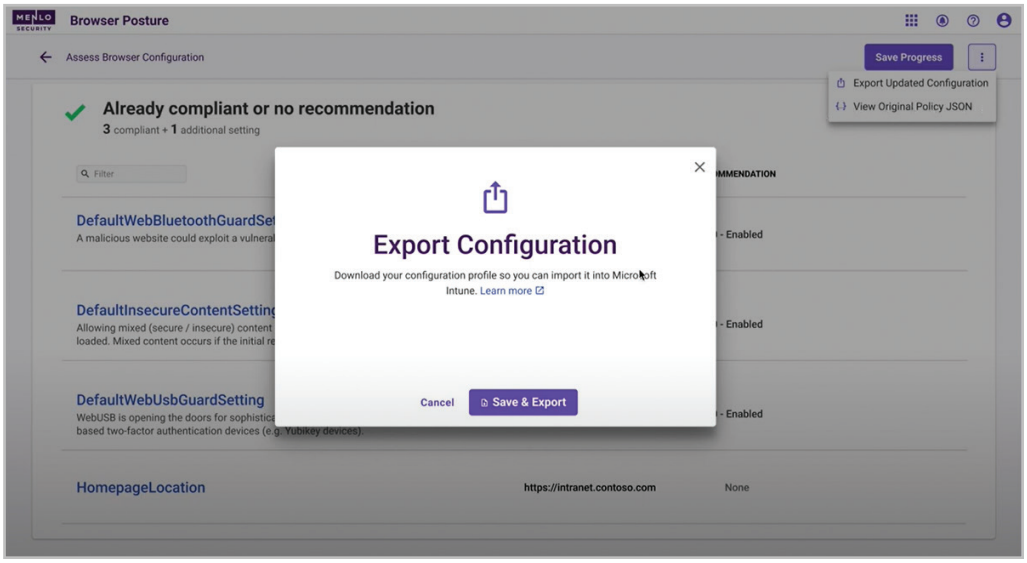
Menlo Securityは、お使いのブラウザの設定とベストプラクティスのベンチマークとの間の相違点を特定するだけでなく、セキュリティに影響を及ぼす可能性のある順に、何を変更すべきかについて具体的な提案を行います。



ユーザーが評価結果をクリックすると、Menlo Securityはさらに詳しい情報を提供します。 それぞれの具体的なポリシーを示すだけでなく、詳細を説明します。 これにより、ポリシーの変更を承認または拒否するために必要な詳細情報が得られます。環境 と ユーザー を 最もよく理解しているのは、お客様自身だからです。



どのポリシーが適切かを決定すれば、後は設定をエクスポートするだけです。



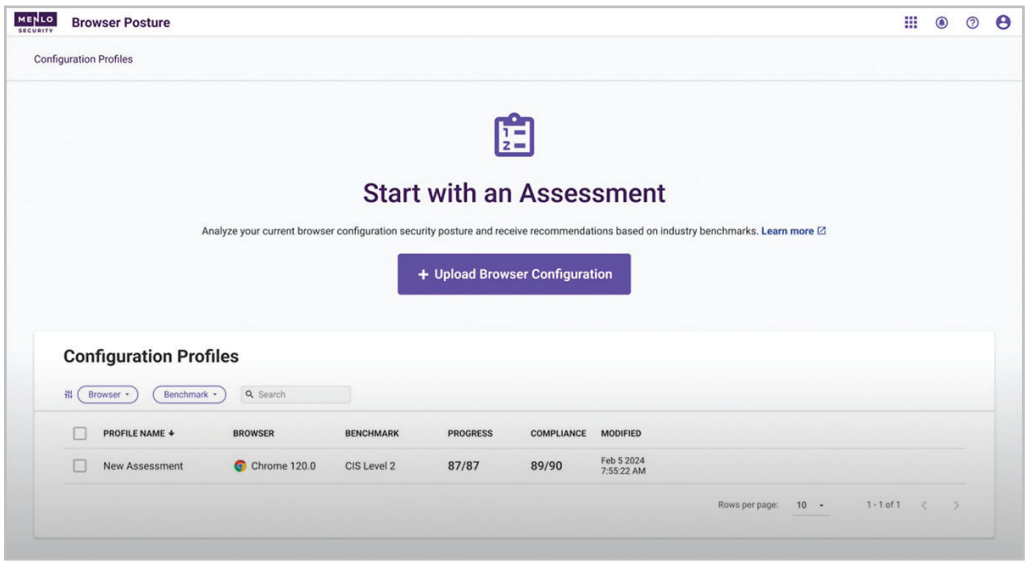
Menlo Securityは、安全なブラウザポリシーの取得と維持を1、2、3の簡単な手順で実現します。

1. **アップロード** ブラウザ設定をリストアップしたJSONファイルをアップロードして、プロセスを開始します。

2. **レビュー** Menlo Browser Posture Managerが、お客様の設定とベンチマークの専門家の設定を比較します。 Menlo Securityはさらに踏み込んで、ベンチマークと異なる設定やセキュリティのベストプラクティスから外れた設定を指摘します。

3. **デプロイ** 自社の状況に最も適したセキュリティプロファイルのセットを選択または適用すれば、Menlo Securityが導入展開のプロセスを簡素化します。 Microsoft Intuneを活用して既存のブラウザの設定管理を行うことも、Intuneとの統合によってプロセスを自動化することもできます。

Menlo Securityはまた、設定をプッシュアウトする前に、レビューされていないポリシーの推奨事項をリマインドしてくれます。 そして、これらのベンチマークとの比較をいつでも見直せるように、評価は自動的に保存されます。



Menlo Securityでブラウザを管理

Browser Posture Managerを使用すれば、セキュリティチーム、企業の経営陣、そしてユーザーを同時に満足させることができます。 ブラウザを標的とした検知回避型攻撃（HEAT：Highly Evasive and Advanced Threat）が急増する中、攻撃対象は急速に拡大しています。 エンタープライズブラウザのセキュリティポリシーに自信を持ち、ポリシーを自動的に展開および更新する方法があれば、ユーザーにセキュリティ侵害のリスクを負わせることなく、エンタープライズブラウザのセキュリティを制御できるようになります。

Menlo Securityについて

Menlo Securityは、ITおよびセキュリティチームが既存のブラウザを適切に管理し、ユーザを保護し、アプリケーションへのアクセスと企業データを保護することで、包括的なブラウザセキュリティアプローチを提供し、ブラウザの攻撃対象領域を排除します。

Menloは、リアルタイムで動的なポリシー制御を行い、回避的なマルウェア、ゼロアワーフィッシング攻撃、ランサムウェアのペイロードがエンドポイントや企業システムに感染するのを効果的に阻止することで、企業が既存のブラウザを保護することを可能にします。

お問い合わせ：
www.menlosecurity.jp
japan@menlosecurity.com

Menlo Securityについて

Menlo Securityは、Menlo Secure Cloud Browserによって高度に回避的な脅威を排除し、生産性を維持します。 Menlo Securityは、クラウドベースのセキュリティが目指す、導入展開が容易なゼロトラストアクセスを実現します。 Menlo Secure Cloud Browserは、エンドユーザーがオンラインで業務を行う間、ユーザーからは見えない形でサイバー攻撃から防御し、同時にセキュリティチームの運用負担を軽減します。

Menlo Securityは、ユーザーを保護してアプリケーションへのアクセスを確保し、完全なエンタープライズブラウザソリューションを提供します。 Menlo Securityなら、ワンクリックでブラウザセキュリティポリシーを導入することができ、SaaSやプライベートアプリケーションへのアクセスを保護して、ラストワンマイルまで企業データを守ります。 信頼と実績のあるサイバー防御により、あらゆるブラウザでデジタルトランスフォーメーションを保護します。

Menlo Securityと共に、安心してビジネスを前進させましょう。