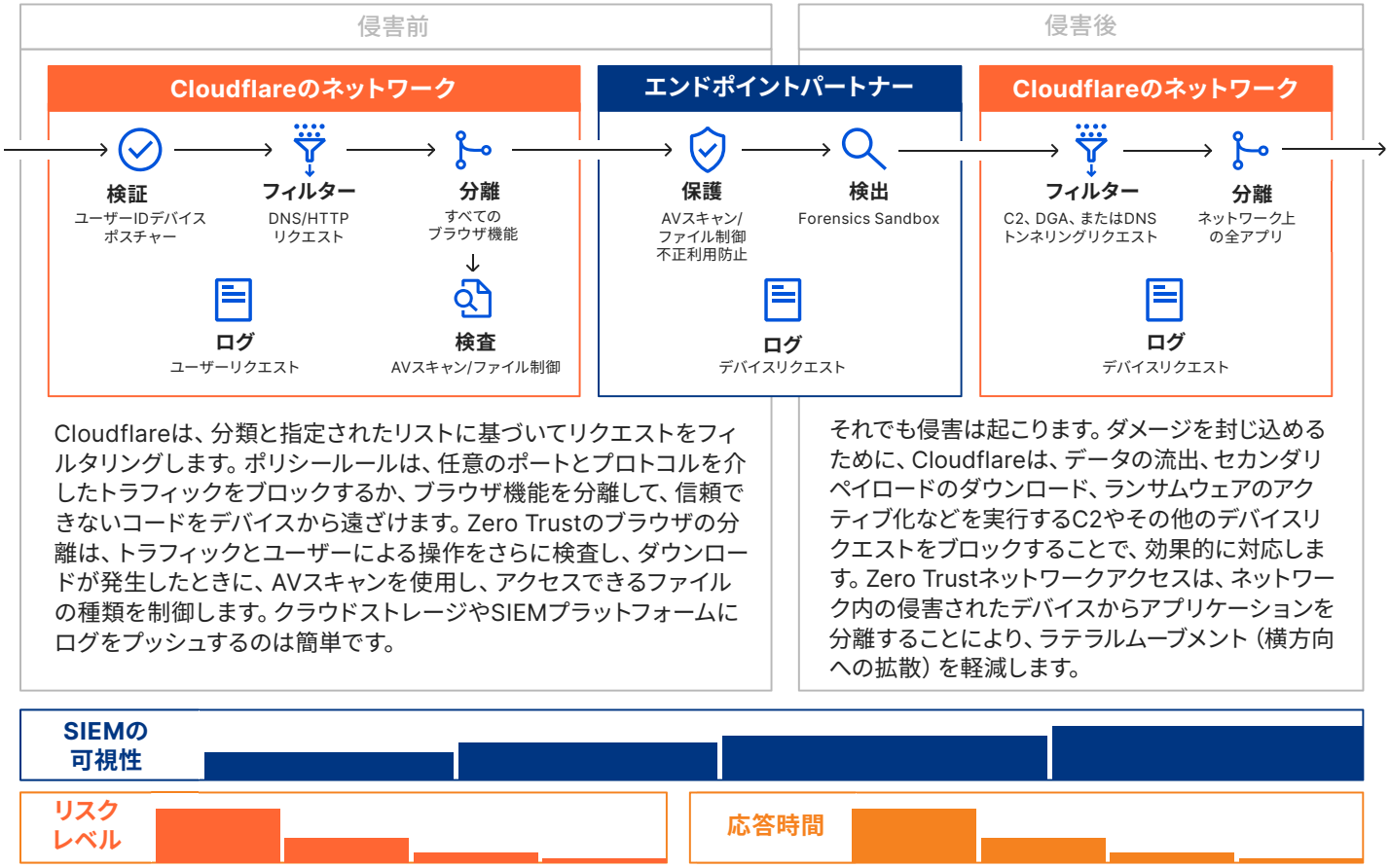
よりシンプルで効果的な脅威防御

マルウェア、フィッシング、暗号マイニングなど、攻撃の形はさまざま。その影響を軽減します

絶えず変化する脅威の状況に対応するために、階層的な防御を組み込むことはベストプラクティスですが、セキュリティを向上させるためにあまりにも多くの異なるツールを使用することは、コストがかかり、複雑であるだけでなく、パフォーマンスにも影響を及ぼします。小規模な組織では、リスクを軽減するためにより簡単な方法を求めており、中規模の組織ではより効果的な反応も必要となるほか、大組織では1か所で可視化する必要性もあります。

Cloudflareは、かつてないほど多くのセキュリティサービスを(ブラウザ内で行われるすべてのエンドポイントコンピューティングを移行することさえも) 大規模なエニーキャストエッジネットワーク上で動作する1つのZero Trustプラットフォームに統合します。脅威に対する防御の向上は、Zero Trustから始まります。つまり、デバイスが企業のリソースに接続する前に安全に管理されていることを検証します。

ソリューション：ネットワークとエンドポイントセキュリティ全体で統合された脅威対策



Cloudflareは、分類と指定されたリストに基づいてリクエストをフィルタリングします。ポリシールールは、任意のポートとプロトコルを介したトラフィックをブロックするか、ブラウザ機能を分離して、信頼できないコードをデバイスから遠ざけます。Zero Trustのブラウザの分離は、トラフィックとユーザーによる操作をさらに検査し、ダウンロードが発生したときに、AVスキャンを使用し、アクセスできるファイルの種類を制御します。クラウドストレージやSIEMプラットフォームにログをプッシュするのは簡単です。

それでも侵害は起こります。ダメージを封じ込めるために、Cloudflareは、データの流出、セカンダリペイロードのダウンロード、ランサムウェアのアクティブ化などを実行するC2やその他のデバイスリクエストをブロックすることで、効果的に対応します。Zero Trustネットワークアクセスは、ネットワーク内の侵害されたデバイスからアプリケーションを分離することにより、ラテラルムーブメント（横方向への拡散）を軽減します。

Cloudflare Oneインテリジェンスプラットフォーム

ポリシールールごとにブロック、分離、またはSIEMへログプッシュするためのセキュリティリスク用カテゴリ

マルウェア	新たに表示されたドメイン	DGAドメイン	スパイウェア
フィッシング	新しいドメイン	DNSトンネリング	スパム
暗号マイニング	到達不能ドメイン	C2とボットネット	アノニマイザー

Cloudflareの知見は、ネットワークデータとエコシステムにより、既知の脅威や新たな脅威を効果的にブロックします。 しかし...

- ベンダーがどんなに脅威の検出とフィードの供給に奔走しても
- どれほど多くのデータや機械学習が使用されても
- どれほど頻繁に知見を更新し、即座に実装しても

...フィルターや検査は脅威を必ずしも100%ブロックできない

さらに、社内のセキュリティチームは、従業員の利便性を削ぐことなく、組織にリスクをもたらす全サイトをブロックすることはできません。そのようなことがあれば、脅威による損害よりも、生産性やITチケットの処理の方に、さらに損失がかかる可能性があります。

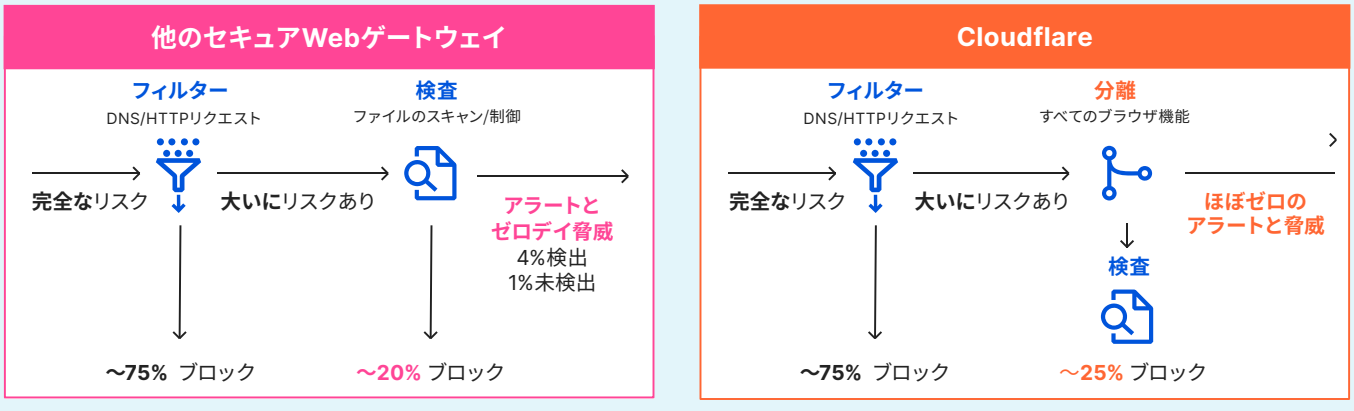
そのため、インターネットブラウジングにはZero Trustのアプローチが必要です。 Cloudflareブラウザ分離は...

- 完璧なユーザーエクスペリエンスで超高速
- ブロックされていない全サイトをコスト効率良く使用

未分類	リスク高	リスク低

近日公開：

- 移動中だけでなく、使用中のデータを検査して制御します。
- ダウンロードしたファイルを保存する場所を指定します。
- フォームに資格情報が入力されないようにします。



Cloudflare Zero TrustのEnterpriseプランアカウントのご利用については、本日すぐに弊社までお問い合わせください。