MENLO SECURITY

Everywhere Access（どこからでもアクセス）：

ハイブリッドワークのための ゼロトラスト革命

ホワイトペーパー

デジタルトランスフォーメーションの進行に伴い、リモートワークが増え、多くの人がマネージドかアンマネージドかを問わず、さまざまなデバイスやロケーションから重要なビジネスアプリケーションやデータにアクセスするようになっています。 サードパーティ（パートナーや請負業者など）は特定のアプリケーションにアクセスする必要があり、その際、企業がエンドポイントを制御することはほとんどありません。 企業は、2 つの重要な問題を同時に解決する必要があります。つまり、これらのリソースをきめ細かく制御することで、アプリケーションへの安全でシームレスなアクセスを提供する一方で、こうした作業に関連するリスクを軽減することが求められます。

デジタルトランスフォーメーションのもう 1 つの重要な側面として、クラウド移行が進むなか、アプリケーションはブラウザベースへと変わってきています。 ブラウザは多くの人が使い慣れている一方で、リスクが生じる可能性があります。 ブラウザベースのアプリケーションを使えば、たしかにコストが抑えられ、アジリティも高まります。しかし同時に、可視性の不足が危惧されます。 パッチを当てて、特定のクライアントソフトウェアエージェントを導入し、Web セキュリティとアプリアクセスガバナンスに多額の投資を行っているにもかかわらず、可視性を十分に確保できないというケースもあります。 たとえポリシーを設定していても、その効果を監視・検証することができなければ、万全とはいえません。 誰かがアプリケーションにアクセスしたことは分かっていても、そこで何をしているのか判別できないということもありえます。 いずれのアプローチも、認証情報の盗み出しやデバイス侵害のリスクに対応することはできません。

Menlo Security のソリューションは、どこからでもアクセスできるようにする「安全設計」のアプローチを採っています。 ユーザーがどこにいて、どのようなデバイスを使っていたとしても、社内リソースや SaaS アプリケーション に、いつでも安全にアクセスできることが必要です。 安全設計のソリューションには、ゼロトラストアクセスが不可欠です。 つまり、アクセス要求を継続的に検証するようにし、たとえデバイスやネットワークそのものへの侵入を許してしまったとしても、不正アクセスやデータ侵害のリスクを最小限に抑えられるようにしておく必要があります。 ポリシーが意図したとおりに機能していることを確認・立証するには、アプリケーションアクセスの可視性が不可欠です。

セキュアなアクセスには可視性が不可欠

Menlo Secure Application Access は、暗号化された VPN トンネルを許可することはなく、アプリケーションへのユーザーのアクセスを個別に制御し、VPN や従来の ZTNA に起因する可視性の問題に対処します。 Menlo Browsing Forensics は、どのサイトにアクセスして、何をしたのかなど、Menlo Secure Cloud Browser でのユーザーの行動を記録します。フォレンジックを、特定のユーザーや、BYOD ユーザー、サードパーティに対して設定しておき、DLP アラートやフィッシング攻撃などのイベントをトリガーとして実行させることができます。

Secure Application Access と Browsing Forensics の組み合わせにより、以下のことが可能になります。

- ゼロトラストアーキテクチャを有効に機能させ、ユーザーの行動を監視することで、ゼロトラストポリシーが実行されていることを確認する。
- 危険な行動を追跡し、コピー / 貼り付けやアップロード / ダウンロードなどの潜在的な脅威を特定する。
- ユーザーの行動を知ることで、どのような意図があるのかを明らかにし、情報に基づいた意思決定を行う。

Browsing Forensics は、ユーザーの行動を細かく把握することで、Secure Application Access を補完します。 このような可視性により、ユーザーの行動を監視して、ポリシーが守られていることを確認し、潜在的な脅威を特定することができます。

どこからでもアクセス可能なゼロトラストセキュリティの主なメリットは以下の通りです。

- **セキュリティの強化 -** 不正アクセスやデータ侵害を防止します
- **生産性の向上 -** ユーザーがどこにいて、どのようなデバイスを使っていたとしても、効率的に作業が行えます
- **コスト削減 -** コストのかさむ VPN インフラストラクチャと管理が必要ありません
- **ユーザーエクスペリエンスの向上 -** シームレスで安全なアクセスエクスペリエンスが実現します

Menlo Secure Application Access は、Menlo Secure Cloud Browser を利用して、アプリケーションとユーザーを包括的に保護します。 Menlo Security は、安全設計とゼロトラストアクセスをサポートしており、侵害されたエンドポイント、脆弱なブラウザ、不正なリクエストからアプリケーションを保護しつつ、どこからでもアクセスできるようにします。 Menlo Browsing Forensics は、ブラウジングセッションを完全に可視化することで、延々と続く改善ループを終わらせます。

重大な課題

アプリケーションアクセスの課題を俯瞰的に見ると、大小あらゆる規模の組織が何十年も前から克服を試みている問題が複数あることが分かります。 必要なアプリケーションへのアクセスを可能にし、保護しようとする場合、主に次のような課題があります。

- ブラウザをメインのアクセス方式とする場合、権限の不正利用を防止するためのゼロトラストセキュリティが必要であること。
- 企業の管理下にないアンマネージドデバイスからも安全にアクセスできるようにする必要があること。
- VDI の使用を最小限に抑えたり、VPN を入れ替えるといった、アクセスシステムの刷新が望まれること。

これらの課題はそれぞれが固有の問題を引き起こし、ほとんどの組織で以下にあげるようないくつかのシナリオに直面しています。

課題

ゼロトラストの対象をネットワーク以外にも広げる

ゼロトラストという概念は、2010 年に導入されて以来、企業の目標となっている。 継続的な認証と承認、および暗黙の信頼の排除というゼロトラストの基本理念は、当然のことながら、ネットワークにおいて最初に採り入れられました。 当時はアプリケーションの大半がネットワーク上に置かれており、ほとんどのユーザーがネットワーク上にいるか、ごく稀なケースとして VPN 経由でアプリにアクセスしていました。 ゼロトラストネットワークアクセス（ZTNA）が流行語になったことがあります。

しかし、のちにデジタルトランスフォーメーションが起こり、アプリケーションはクラウドへと移行して、リモートワークが一般化しました。現在では、ゼロトラストをネットワークに限定して考えるのは適切ではありません。もはやネットワーク上にエンタープライズアプリは存在せず、ユーザーがそれらにアクセスする必要もなくなっています。 今日のゼロトラストアクセスは、ネットワークの中にあるものはすべて信頼してもかまわないというペリメータベースのモデルに依存するのではなく、場所がどこであれ、本質的に信頼できるものは何もないという考え方が前提となっています。 ユーザーは認証・承認を受けなければならず、アプリケーションへのアクセスは、どこにいるかに関係なく、業務を遂行するのに必要なアプリのみに限定される必要があります。

ゼロトラストモデルに欠けている最後の要素が可視性です。 制御がしっかり機能しているかどうかを確認（場合によっては、証明）することができなければ、変更に対して保守的になりがちで、問題が発生してからしか行動を起こさなくなってしまいます。

課題

アンマネージドデバイスからアプリケーションに安全にアクセスできるようにする

アプリケーションが登場して以降、企業ではアンマネージドデバイスで作業するユーザーにアプリケーションアクセスを提供することを目指してきました。 従業員が自分のノート PC、タブレット、モバイルデバイスからアプリケーションやデータにアクセスできるようにすることで、組織に必要なビジネスアジリティが実現します。 このようなアクセスをビジネスパートナーや請負業者などのサードパーティにまで広げることができれば、さらなる利点がもたらされます。 アンマネージドデバイスからアプリへのアクセスが可能になることによるメリットは明白です。しかし残念ながら、制約もあります。 たとえば、アプリケーションサーバーとその中にあるデータに対する脅威、およびデータ流出やプライバシー侵害といった現実的なリスクがこれに相当します。

今では、ほとんどのアプリケーションにブラウザからアクセスできます。アクセスが簡素化されるように思われますが、実際はまったく逆です。なぜなら、これまでほとんどのセキュリティツールでブラウザのトラフィックが検知されることはなかったからです。 アンマネージドデバイスに対する可視性と制御が不足しているため、疑わしいブラウザの動作を検知したり、事前に対策を講じたりといったことは事実上不可能です。

この課題の中心には、あらゆるアンマネージドデバイスへのアクセスを可能にするという包括的な課題がありますが、ユーザーのタイプについても解消すべき問題が存在します。

BYOD

アンマネージドデバイスからのユーザーアクセスについての議論で、最初に話題に上るのが BYOD です。 多くの企業で何らかの BYOD ポリシーを適用していますが、リスクは常に存在します。 企業が管理しているデバイスを仕事でのみ使用するようにすることは可能ですが、こういった制約が個人のデバイスにまで行きわたるという保証はありません。 自宅のコンピューターやノート PC などは、行動を把握しきれない他のユーザーと共有される可能性があります。デバイスが共有されている場合や、もしくは単に仕事以外の用途で使われている場合、ユーザーが何をしているのかを知る術はありません。 危険な Web サイトへのアクセス、ソーシャルネットワークでの情報共有、疑わしいコンテンツのダウンロード、怪しい Web ベースアプリケーションへのアクセスなどが行われている可能性があります。 特にデバイスが他者と共有されている場合、アンマネージドエンドポイントでどのブラウザが使用されているのかや、ブラウザが定期的に更新されているかどうかを確認するのは困難です。

BYOD をフルに活用するには、エンタープライズアプリとリソースを保護しつつ、アプリケーションとリソースに容易にアクセスできるソリューションを選ぶ必要があります。

サードパーティ

このユーザーカテゴリーには、請負業者やビジネスパートナーのほか、合併・買収シナリオの双方の当事者など、特殊なグループも含まれます。 これらのユーザーのアクセスは、タスクの実行に必要な アプリケーションのみに限定される必要があります。 ユーザー / グループがアプリを使用しているときや、リソースにアクセスしているときの制御についても、細かく具体的に決めておくようにします。 サードパーティのアクセスを安全に有効化するには、どのようなソリューションを使う場合であっても、そのグループで必要とされるものの見極めを厳密に行い、それ以外は許可しないようにすることが重要です。他のユーザーへの影響を最小限に抑えつつ、制御を容易に適用・変更できることが、有用なソリューションの条件です。

課題

レガシアクセスシステムのモダナイズ

Everywhere Access 戦略の重要な目標の 1 つが、ユーザーのニーズと仕事で使用するアプリケーションに合わせて、従来のアクセス方式をアップグレードする方法を特定することです。 レガシシステムには、仮想デスクトップインフラストラクチャ（VDI）や仮想プライベートネットワーク（VPN）などがあり、どちらもほとんどのアプリケーションがエンタープライズネットワーク上に置かれていた時代を反映したものとなっています。 現在は、クラウド内にアプリケーションが置かれていることが多く、ユーザーはあらゆる場所でこれらを使用します。従来のアクセス方式は、このような現実を反映していません。 もっとも一般的なアクセス方式である VDI と VPN は、パンデミックが起こり、即時の対応が必要になったときに急速に普及しましたが、時間が経ち、デジタルトランスフォーメーションが進むにつれ、ビジネスの現実からかけ離れたものとなっていきました。

VDI

VDI の概念は比較的単純で、企業が仮想デスクトップを管理・保護しながら、データの保護と保存を集約サーバーで一元的に行うというものです。 しかし残念ながら、VDI の現実ははるかに複雑であることが分かってきました。 今ではサーバーを集約することはなくなり、クラウド管理にフォーカスするようになった IT チームにとって 、ハードウェア / ソフトウェアスタックの保守とアップグレードのタスクは大きな負担となっています。VDI が正しい選択肢となるケースもないわけではありませんが、アプリケーションが置かれている場所や、IT チームの持つスキル、ユーザーが期待するエクスペリエンスなどの諸要因により、VDI はほとんどの組織の現状にそぐわないものとなっています。

VDI は、可視性の面でも問題があります。 SOC チームと IT チームの間でよく知られている一般的なセキュリティツールは、VDI シナリオでは役に立ちません。 集中型のモニタリングとログ解析のツールが必要であり、VDI ベンダーから直接入手しなければならないケースが多いため、コストがかさみ、ベンダーの固定化につながります。 もう 1 つの要素が、エンドユーザー監視ツールです。VDI はレスポンスに時間がかかることで知られていますが、このツールはもともとこの問題を解消するために設計されたものです。 これにより、購入、展開、保守を必要とする特殊なツールがまた 1 つ増えることになります。

VPN

アプリケーションが エンタープライズネットワークに置かれていた時代に生まれたもう 1 つのアクセス方式が VPN です。VPN では、ユーザーは「ネットワーク上」にいる体験をすることになります。実際そのとおりなのですが、残念ながら、ほとんどのアプリケーションはもはやネットワーク上に置かれてはいません。

ユーザーエクスペリエンスが標準以下であるだけでなく、VPN に起因するデータ侵害が多く発生していることからも分かるように、トラフィックがネットワークに入り、クラウドを経由して戻ってくるため、セキュリティリスクがきわめて高くなっています。ユーザーの認証情報の盗み出しや、デバイスへの侵入が原因で侵害が発生した事例もあります。 巧みなフィッシング攻撃によりユーザーの認証情報を盗み出し、VPN への侵入に成功した攻撃者は、他の認証プロセスを経ることなく、あらゆるビジネスシステムにアクセスするのに必要な情報を瞬時に手にすることになります。 別の事例では、インシデントの原因は VPN 技術の脆弱性にありました。この脆弱性を攻撃者がすかさず悪用したわけです。 また、VPN は機能を実行するためにネットワークに接続している必要があるため、攻撃の標的にもなります。 個々の課題が何であれ、中心となる問題は VPN の仕組みに関係しています。VPN は、ユーザーを特定のアプリケーションではなく、ネットワーク全体に接続する設計になっています。

VPN で生じる可視性の問題は、VDI 環境のものほど特殊ではないものの、それでもやっかいであることに変わりはありません。セッションの可視性を得るには、ディープパケットインスペクション、ネットワークフロー解析、ネットワークログレビューなど時間のかかる調査手法が必要になってきます。

真のゼロトラストの実現に向けて、ネットワークの介在をなくす

先駆的な組織では、サイバーセキュリティ戦略を進化させ、ブラウザセキュリティに重点を置くようになっています。 アクセス制御を広範囲にわたるネットワークレベルのものからブラウザベースに変えることで、露出を減らし、アクセスを特定のアプリケーションのみに制限できます。 今日の企業の現実として、パートナーや請負業者のエンドポイントを確実に保護することは不可能です。同様に、パートナーや請負業者の行動を完全に制御することもできません。 デバイスやネットワークのロケーションベースの制御などはもはや論外です。

ソリューション

Menlo Security の Secure Application Access

レガシアクセス方式とアンマネージドデバイスに対処

Menlo Secure Application Access を導入することで、侵入を受けたエンドポイントのアプリケーションに重要な保護を提供しつつ、アプリケーションサーバーの感染トラフィックからユーザーを保護することができます。 複雑なインフラストラクチャを使用したり、ネットワーク全体へのアクセスを許可したりする従来の技術とは異なり、Menlo Security は、ユーザー、グループ、ソース IP、地理位置情報に関するポリシーを用いて、必要なものだけへのアクセスを許可します。

Menlo Secure Application Access は、Menlo Secure Cloud Browser を用いてアプリケーションと通信することで、それらのアプリケーションを保護します。 ユーザーは、発信元のサーバーにアクセスするのではなく、Menlo Secure Cloud Browser と対話します。この強化型のリモートブラウザは、アプリケーションをレンダリングして表示し、エンドポイントデバイスのユーザーのローカルブラウザ内にコンテンツを配信します。 アクセスの提供に加え、ローカルブラウザと Secure Cloud Browser の組み合わせにより、コンテンツベースの攻撃からユーザーを保護します。 ネットワークをベースとした従来のアクセス環境とは違い、Menlo Security のアーキテクチャは、パラメータの改ざん、Web スクレイピング、API の悪用など、多くの問題が含まれる可能性のある不正なリクエストからアプリケーションを保護します。 Menlo Cloud がアプリケーションとエンドポイントを分離し、Menlo Cloud 内の AI 駆動型保護機能によりすべてのリクエストを検査することで、このような保護が実現します。エンドポイントが何らかの侵害を受けたとしても、攻撃者がサーバーに直接アクセスしてリクエストを送ることはできません。すべてのアプリケーションリクエストは、エンドポイントブラウザではなく、Menlo Secure Cloud Browser から実行されます。

エンタープライズアプリにある貴重なデータのさらなる保護のために、Menlo Secure Application Access はアプリケーションをきめ細かく制御します。 制御には次のものが含まれ、知的財産の保護、データ流出の防止などに使用できます。

- ダウンロード / アップロード
- リードオンリー / リードライト
- アプリケーションとドキュメントの電子透かし
- データ編集
- コピー / 貼り付け

Menlo Secure Cloud Browser もしくはブラウザ拡張機能を使うことで、エージェントを介さずにアプリケーションに安全にアクセスできます。 RDP 接続や SSH 接続を必要とするレガシアプリケーションの場合、非ブラウザベースのアプリケーション用の Menlo Security Client を使うことで、安全なアクセスを確保できます。

Menlo Security の Browsing Forensics

「Everywhere Access（どこからでもアクセス）」に不可欠な可視性とは

ブラウザセキュリティにフォーカスしたサイバーセキュリティ戦略により、ユーザーエコシステムが必要なアプリケーションのみに安全にアクセスできるようにすることが可能です。 そのうえで、Menlo Browsing Forensics がユーザーのブラウザセッションとサードパーティの行動の詳細なビューにより全体像を把握します。これによって、アクセスポリシーが目的どおりに機能していることを確認できます。 この 2 つの組み合わせにより、エンドポイントとアプリケーションが分離され、これまでセキュリティチームによる情報収集が不可能とされていたユーザーの行動について把握するための重要な可視性が得られます。

まとめ（要点）

現代社会において事業を行うには、ユーザーがさまざまなアンマネージドデバイスから、いつでも、どこからでもアプリケーションとデータにアクセスできるようにする必要があります。従来のセキュリティ管理を続けていては、デバイスの侵害やセキュリティ対策の不備から組織を保護することはできません。 ですが、最新のセキュリティソリューションならばそれが可能です。Menlo Secure Application Access と Menlo Browser Forensics を組み合わせることで、脆弱なレガシハードウェア、侵害を受けたエンドポイントやサーバー、内部脅威、サードパーティ攻撃やサプライチェーン攻撃から組織を守るのに必要なセキュリティ、制御、可視性がもたらされます。

未来の働き方には、どこからでもアクセスできることと、安全設計が欠かせません。それを支えるのが、ブラウザから始まるゼロトラストです。 Menlo Security ならば、企業の管理下にあるネットワークを超えて、ユーザーとアプリを追跡できます。

ゼロトラストについての 10 の質問

1. ゼロトラストはネットワークと結び付いていますか？

リモートワーク、クラウドベースのアプリケーション、BYOD ポリシーを取り巻く今日の状況を踏まえると、ゼロトラストソリューションをネットワークペリメータと結び付けた場合、有効性が大きく制限されることになります。今日の動的な環境においてセキュリティを強化するには、ユーザーやグループ、ユーザーがアクセスする必要のある特定のアプリ、業務の遂行に必要な正確なアクセスレベルに基づき、ゼロトラストアクセスを設定する必要があります。ゼロトラストアクセスを優先させることで、ユーザーがどこにいるかに関係なく、適切な権限を持つユーザーのみに特定のリソースへのアクセスを許可することができます。これにより、セキュリティ侵害による潜在的な影響が大幅に軽減されます。

2. ユーザー / グループごとにアクセスを差別化することは可能ですか？ 可能な場合、ポリシーの変更は簡単に行えますか？

高度にカスタマイズ可能な制御を導入できるかどうかが、最小権限のアクセスモデルを確立する際の鍵になります。 しかし、組織は絶えず変化しており、俊敏性を維持するには、一元化された使いやすい管理インターフェースの存在が欠かせません。新規ユーザーの追加、ロールの変更、アプリケーションの追加、新たな脅威の発生といった事態に応じて、セキュリティチームと IT チームがアクセスを迅速に調整できることが求められます。 強力なセキュリティ対策と効率的な管理機能を組み合わせることで、生産性を高めつつ、機密データを効果的に保護することができます。

3. どのようにしてエンドポイントでアプリケーションをマルウェアから保護しますか？

マルウェアは、アプリケーションそのものの脆弱性を悪用したり、または基盤のオペレーティングシステムを経由してアプリケーションに侵入してきます。 高度な脅威の場合、偽装ファイルや、不正なリンク、さらには感染した Web サイトを通じて、ユーザーをあざむき、マルウェアをインストールさせます。 従来のセキュリティ技術では、こうした感染を防ごうとして困難に直面するケースが少なくありません。これは、これらのセキュリティ製品の大多数がネットワークトラフィックを監視し、既知のマルウェアシグネチャを検出する設計になっているためです。 これらの防御機能では、ブラウザトラフィックから侵入してくる脅威を「見る」ことができません。 この弱点を克服するには、ネットワークを分離するための技術を探す必要があります。これにより、たとえエンドポイントが感染したとしても、直接アプリケーションにアクセスされずにすみます。

4. データ漏洩防止（DLP）制御の利用は可能ですか？その場合、どのような制御を利用できますか？

エンタープライズアプリケーションに安全にアクセスして、機密データが組織の管理下から外部に漏れ出るのを防ぐには、データ流出防御機能が非常に重要になってきます。 検討が推奨されるデータ流出防御制御には次のようなものがあります。

- 電子透かし
- データ編集
- コピー / 貼り付け制御
- Web サイトのリードオンリー / リードライト制御
- アップロード / ダウンロード制御

5. 正規ユーザーのデバイス / 認証情報を手に入れた場合、侵入者はどのようなことができますか？ラテラルムーブメントの移動は可能ですか？

ユーザーが必要とする特定のアプリケーションに限りアクセスを許可することが重要になってきます。 システム内にこのような障壁を設けておくことで、侵入者が初期アクセスを獲得した場合に引き起こされる可能性のある損害が制限され、ラテラルムーブメントを防ぐことができます。 このような制御によって、たとえ 1 つのアプリケーションが侵害されたとしても、侵入者が組織のネットワーク全体にアクセスすることがないようにしておく必要があります。

6. VPN は今も使われていますか？使われているとしたら、なぜですか？

今では、ユーザーが企業のネットワークに接続しなくても、アプリケーションにアクセスできるようになっています。 パンデミックが起きたことで、リモートユーザーがミッションクリティカルなアプリにアクセスするための環境が必要になり、その結果、VPN のような従来のアプローチの持つ欠陥の多くが明らかになりました。 VPN は、ユーザーを特定のアプリケーションではなく、ネットワーク全体に接続します。そのため、ユーザーの認証情報を複製したり、デバイスを盗むことで、VPN への侵入に成功した攻撃者は、企業ネットワーク全体にアクセスするのに必要な情報を瞬時に手に入れることができます。

7. ユーザーの行動を確認するのにどのくらいの時間がかかりますか？

一部のアクセス制御手法は、アプリケーション内のユーザー活動を追跡する機能を備えておらず、包括的な監査のための集中管理型のログ記録機能を提供しない場合が多いです。 その場合、解決に必要なユーザー行動を確認するのは至難の業です。

8. セキュリティチームは潜在的な内部脅威をどうやって取り除きますか？何台のデバイスが対象となり、どのくらい時間がかかりますか？

通常、アプリケーションアクセスに関する潜在的な内部脅威を取り除くには、ブラウザトラフィックを把握することのできない多数のプラットフォームで情報を徹底的に調べる必要があります。 しかし残念ながら、こうした調査は推測の域を出ないことが少なくありません。 ユーザーの行動と意図を知るために、細部を容易に把握できるソリューションが必要です。特に、「危険な」ユーザーと見なされる場合には、このような可視性が欠かせません。

9. アプリケーションへのユーザーアクセスの監査はどのように行われますか？

従来のネットワークベースのアクセス技術には可視性が不足しています。そのため、ユーザーのアプリケーションアクセスの監査は、セキュリティ、IT、コンプライアンスのチームにとって深刻な問題となっています。 効果的なソリューションには、ブラウザトラフィックの可視性が組み込まれていることから、有効なセキュリティポリシーを適用し、これらの制御をしっかりと機能させることができるほか、曖昧さを排除して調査を実行するための詳細情報も提供されます。

10. 使用された認証情報や閲覧された資産など、ユーザーのアプリケーションアクセス行動を再現するのは難しいですか？

この質問に対する答えは、従来のアクセス方式の限界を露呈するものといえます。 ユーザーの調査では、何よりも時間が重要になってきます。また、推測は許されません。

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