wandera
a Jamf company

クラウドセキュリティレポート 2021

組織のデータに影響を及ぼす脅威について、エンドポイント、ユーザ、リモートアクセスツールなどの最も重要な資産を介して、2021年にすべてのユーザが迅速かつ安全に接続できるよう、ビジネスツールを構成する方法について実践的なアドバイスを提供します。

45 Mortimer Street
London W1W 8HJ
+44 (0) 203 301

アメリカ
220 Sansome Street, Suite 1400
San Francisco CA 94104
+1 (415) 935 3095

主な調査結果

- 2020年には、組織の52%がリモートデバイスでマルウェアに関連するインシデントを経験しました。2019年の37%から41%増加しています。
- 2020年にモバイルデバイス向けマルウェアに感染したデバイスのうち、感染した後も企業メールにアクセスし続けていたデバイスは37%、クラウドストレージにアクセスし続けていたデバイスは11%でした。
- 2020年には、組織の28%が、既知のセキュリティ脆弱性を持つOSを日常的に使用していました。
- パンデミック前と比べると、業務時間内の不適切なコンテンツへの接続は最大100%増加しており、大幅な増加が見られました。
- iOSデバイスと比べると、Androidデバイスは、脆弱性のあるアプリケーションがインストールされている可能性が5.3倍もありました。
- 週末のピーク時には、平日のピーク時に比べてフィッシング攻撃の頻度が6%増加しました。
- 2020年の毎週リスクのある無料Wi-Fiホットスポットに接続しているユーザの割合は4%となり、2019年の7%からの減少が見られました。
- パスワードデータを漏えいさせたアプリを使用していたデバイスが1台以上存在する組織の割合は15%となり、2019年の11%からの増加が見られました。

28%

の組織が、既知のセキュリティに対する脆弱性を持つOSを日常的に使用していました。

5.3x

iOSデバイスと比べると、Androidデバイスは、脆弱性のあるアプリケーションがインストールされている可能性が5.3倍もありました。

はじめに

2020年、多くの組織は、生産性レベルを維持しながら、ビジネススタイルを完全なリモートモデルに移行することを余儀なくされました。その結果、より多くのデバイス、ネットワーク、及びアプリをこれまで以上に多くの場所で利用できるように、ITポリシーが改訂されました。

ボーダーレスエンタープライズの到来です。ガートナーが2020年3月にCFOに対して実施した調査では、74%が一部の従業員をリモートワークに永続的に移行させる意向を持っていることが明らかになりました。

その結果、このニューノーマルに合わせて、優れたセキュリティ対策とされていたこれまでの前提が変化していくのを、今私たちは目のあたりにしています。成功しているIT運用のほとんどが、職場から離れた場所にいるユーザに必要なものを提供することに焦点を当てています。これは、分散した従業員が持つさまざまなニーズに対応するため、セキュリティ戦略の機敏性と柔軟性を高めることを意味しています。そのためにはクラウド優先のモデルが必要となります。

業界の主要な専門家は、SASE（Secure Access Service Edge）が、従来の技術から脱却する革新的な企業にとって重要なアーキテクチャモデルになると考えています。これは、SASEがネットワークとセキュリティの機能を統合して、単一のクラウドネイティブサービスに融合するからです。

SASEは未来のものかもしれませんが、企業は今すぐにでも業務に適したツールを見つける必要があります。サイバーリスクと、このリスクが組織に侵入してくる方法を理解することが重要であり、本年次レポートはそれを目的としたものです。

毎年、当社では、業務で使用するモバイルデバイスに影響を与える脅威を分析しています。当社の製品ポートフォリオが（スマートフォンやタブレット以外のデバイスを含みながら）進化に伴い、モバイル・ワークフォースに対する私たちの見解も変化してきました。当社のポートフォリオはリモートワークフォースとなるものであり、単なるモバイルデバイスではありません。

今年のレポートでは、多種多様なポータブルデバイスやプラットフォームを経由して、プライベートおよびパブリックデータセンターでホストされている多数のアプリケーションにリモート接続しているユーザを抱える実際の組織に影響を与えるような、脅威とセキュリティの傾向について見ていきます。

リスク要因1

エンドポイント

ここ数十年にわたってポータブルデバイスが導入されたことで、どこからでも共同作業をしたり、情報共有をしたりできるようになりました。2020年には、COVID-19によって従業員が在宅ワークモデルへの移行を余儀なくされた際には、大半の企業がフルタイムのリモートワーク体制へと入りました。

すべての人にとっては簡単な移行と言えるものではありませんでしたが、一部の組織、特に、フルタイムのリモートワーカーをサポートし、フルタイムのオフィスに勤務していた従業員の在宅ワークを従来より支援していた企業にとっては簡単でした。

多くの場合、IT部門は、機密性の高いビジネスデータへのアクセスを許可するデバイスと拒否するデバイスについて、厳格な決断を迅速に下す必要がありました。これにより、IT部門やセキュリティチームによっては準備ができていないことから、大きな矛盾が生じることになりました。

デバイス+デバイスタイプの増加

この10年間で、人々はスマートフォンでますます多くのインターネットトラフィックを消費するようになりました。業務関連データにも同じことが言えます。Microsoft Office 365などの生産性向上スイートや、SalesforceなどのCRMツールなどを含めた、モバイルSaaSアプリケーションが増加しています。今日の一般的な組織では企業データが含まれるデバイスまたは企業データにアクセスするデバイスのうちの60%がモバイルデバイスとなっています。

2020年以前には、モバイル業務といえば、従業員が所有する(BYOD)または、組織が所有する(COPE)スマートフォンで、接続された状態を保ちながら外出先で業務に携わる一部の従業員がほとんどでした。今では、自宅であるいはワーケーション先で、手元にあるデバイスを使ってフルタイムで仕事をする人が主流であり、選べるデバイスも豊富です。Ciscoは、2023年までに、IPネットワークに接続されたデバイスの数が世界人口の3倍を超えると予測しています。

モバイルワーカーとフルタイムのリモートワーカーとの違いが、明確化し始めています。それに伴い、従業員が使用しているワークフローの多くが、従来のリモートワークツールを使用したホームオフィスでは利用不可、または今後継続して利用できないことが明らかになってきました。

認可されたデバイスをユーザに提供するために必要な予算やサプライチェーンがないことから、ITチームの多くは従業員が自らコンピュータ機器を購入することや、中にはコンピュータ機器を選定して、自宅のワークステーションを揃えることさえも許可していることもあります。つまり、Surface Proやセカンドモニターとして機能する大画面タブレット、あるいは高解像度モニターを1台または2台搭載したMacBook Proなど、膨大なコンピューティングパワーを備えたウルトラポータブル型およびコンバーチブル型のフォームファクターを採用しているのです。以前は、固定電話を使用していた社員も、仕事とプライベートとの区別を維持するために、2台目のスマートフォンを使用しているかもしれません。このように、多種多様なデバイスが混在しており、ITチームが管理するには膨大な量です。

リモートワーカーは、自宅のインターネット回線の帯域幅に頼れなくなると、携帯電話の回線を活用してワイヤレスデバイスを接続する新しいポータブルインターネットデバイスにも依存します。家の中と外で信頼できるインターネット接続を維持するため、Verizon Jetpack、モバイルWi-Fiルーター、Mi-Fisなどの複数のポータブルネットワークオプションを利用しています。

28%

2020年には、組織の28%が既知の脆弱性が存在するOSの影響を受けました。

平均的なOSバージョン、OSおよびデバイスモデル

デバイス500台未満		500台以上
11.3	異なるOSバージョン	39.4
1.4	異なるOS	1.6
1.8	異なるデバイスモデル	2.6

平均を見ると、デバイスが500台未満の企業では、平均で11.3種類の異なるOSバージョン、1.4種類の異なるOS、1.8種類のデバイスモデルを使用しています。これに比べて、デバイスが500台を超える企業では、39.4種類の異なるOSバージョン、1.6種類の異なるOS、2.6種類の異なるデバイスモデルを使用しています。

業務に使用するハードウェアの種類が増えればソフトウェアの種類も増えますが、セキュリティ業界ではよく知られているように、ソフトウェアには脆弱性があります。当社のお客様の多くは、Android、iOS、MacOS、Windows 10を組み合わせたデバイスをサポートしています。これらのプラットフォームすべてで一貫したポリシーを標準化しようとしていますが、プラットフォームごとに制御レベルや機能性が異なり、また脆弱なOSに対するセキュリティパッチの適用方法も異なるため、容易ではありません。

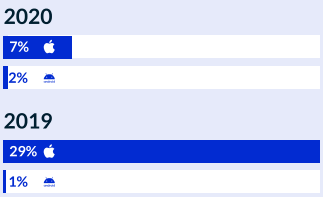
業界スポットライト

一般に、官業のデバイスの場合、セキュリティ対策が良好なことから、他のデバイスと比べて脅威が少なくなります。しかしながら、古いオペレーティングシステムを実行している場合も多く、世界平均と比較して、深刻度の低い脆弱性が存在するOSを使用するユーザが4.4倍、深刻度の高い脆弱性が存在するOSを使用するユーザが3.6倍となりました。

デバイスの標準化が出来ていないことが新たなスタンダードに

デバイスの標準化が進まないことで、ITチームに新たな課題が生じています。組織がサポートするデバイスの種類が1つしかなかった頃には、Windowsデスクトップマシンなど、1つのタイプのOSのみをサポートするだけで済みました。その中に、数バージョン、例えば3バージョン古いデバイスが一部混ざっていたとしましょう。そうだとしても、ITチームが脆弱性について把握し、監視する必要のあるOSはたったの4バージョンだけだったのです。今日では、MacOS、Windows、iOS、Androidなど、複数のプラットフォームが標準となっており、古いOSバージョンについて考えれば、かつては4つのOSバージョンで済んでいたものが、16種類ものOSバージョンになっています。ここで重要なポイントは、選択肢が増えた場合、それらの選択肢をサポートするために管理の規模を拡大する準備が必要となるということです。

脆弱なオペレーティングシステムバージョン



2020年にはiOSデバイスの7%、Androidデバイスの2%が脆弱なOSバージョンを実行していました。2019年の値は、それぞれ29%と1%でした。脆弱なiOSバージョンがこのように急減した理由としては、iMessageやFaceTimeに影響を与える大規模なiOSの脆弱性が2019年に相次いで出現したためと考えられます。

エンドポイントセキュリティのジレンマ

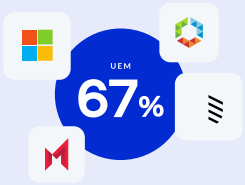
組織はエンドポイントセキュリティを強力にしたいと考えていますが、いかに契約社員が機密データにアクセスしている間、一時的にデバイスを保護するか、あるいは、いかにBYODデバイスを使用する従業員のプライバシーを尊重しつつ、何らかのセキュリティ対策を実施するか、といった、よくあるジレンマに陥ります。一般的にユーザは、セキュリティソリューションや管理ソリューションに抵抗しがちです。従業員は監視されることを望んでいませんが、これらのソリューションが悪いものを捕らえるために監視を行う必要であることは分かっています。

成功した不正アクセスの70%はエンドポイントから発生していることが分かっています。また、企業の83%が、サードパーティ（請負業者やサプライチェーンパートナなど）へのアクセスを提供することを難しいと回答しており、管理されていないエンドポイントのセキュリティを確保するためには改善が必要と考えています。

Verizonによると、企業の87%は、モバイルの脅威が他の脅威タイプを上回ると考えています。これには、モバイルデバイスが個人的なものであるために管理やセキュリティが難しく、悪意のある人物がこのセキュリティギャップを認識していることが理由として挙げられます。

ある調査では、FT 500企業の92%が、モバイルワーカーの増加がセキュリティ問題のリスクの増加を招くことを懸念していると回答しました。これらの組織のほとんどは、個人所有のデバイスの持ち込み（BYOD）ポリシーを採用しているものの、その大多数（94%）がBYODによってモバイルセキュリティリスクが増加していると答えています。

リモートワークは、人口の十分な割合がCOVID-19のワクチン接種を受けた後でも、標準的なビジネス慣行の一部となりつづけるでしょう。そのため、ITチームは、管理されているもの、管理されていないものを含めた幅広い種類のデバイスやネットワークのニーズに合うプラクティスを確立する必要があります。また、すべてのエンドポイントからSOCに脅威データを集約し、リモートデバイスがセキュリティ運用から外れないようにする必要があります。



当社のデータによると、モバイルデバイスの67%が、MobileIronやVMware Workspace ONEなどのデバイス管理ソフトウェアに登録されています。

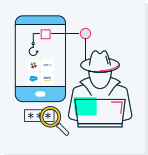
リスク要因2

ユーザ

オペレーティングシステムは、セキュリティの脅威の大部分を軽減するように構築されています。AppleとGoogleは、オペレーティングシステムやアプリストアのセキュリティを強化するために大きな進歩を遂げています。しかし、ユーザの行動によってリスクが生まれる恐れがあります。ユーザリスクを理解するためには、それぞれの攻撃がユーザの弱点をどのように悪用するかを考察する必要があります。それだけでなく、デバイスのセキュリティを弱め、攻撃の扉を開いてしまうようなユーザの行動も考察する必要があります。

標的にされる犠牲者としてのユーザ

ハッカーは、ユーザを標的にして騙すことで機密情報を渡させようとするフィッシングなどのソーシャルエンジニアリング攻撃で、堅牢なオペレーティングシステムを依然として回避しています。また、公共の Wi-Fi が安全ではないことを利用して、ユーザのトラフィックを傍受する悪質な業者もいます。さらに、PII（Personal Identifiable Information - 個人を特定できる情報）や金銭の盗難、およびその他の詐欺など、データ損失の機会にユーザをさらすような危険なアプリの犠牲になる可能性もあります。

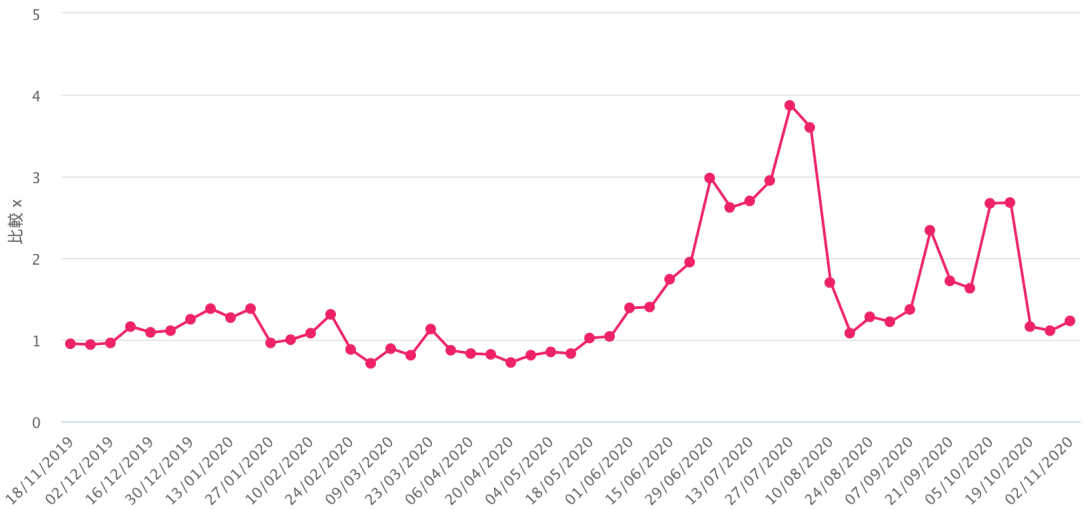


標的にされる犠牲者としてのユーザ

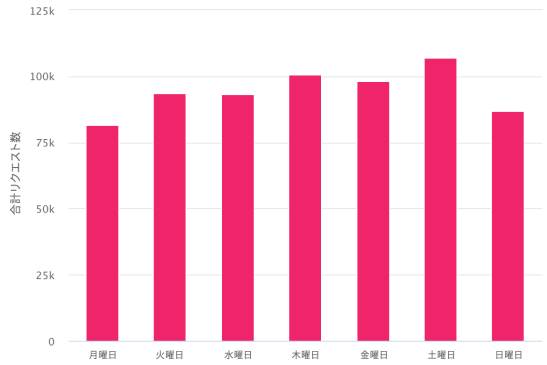
フィッシング

フィッシングは今も、ポータブルデバイス上のユーザに影響を与える最大の脅威です。フィッシング攻撃は、被害者を誘い込む可能性の高いトピックやブランド、テーマに集中して行われます。例えば、税金申告のシーズンになると、毎年、IRS、HMRC（英国）、ATO（オーストラリア）を装ったフィッシング攻撃が増加します。同様に、今年の上半期には、COVID-19に関連したフィッシングサイトへのトラフィックが増加し、さらにクロロックス社の偽のEコマースサイトさえも出現したことが確認されています。

下の図は、2020年におけるリモートワーカーを標的にしたフィッシング攻撃の増加を示しています。



2020年に出現した他のフィッシング傾向を調べる中で、ユーザに対するフィッシング攻撃は土曜日に最も行われていることが分かりました。週末のピーク時には、平日のピーク時に比べてフィッシング攻撃が6%増加しています。これは、従業員が「仕事モード」になっていないとき、精神がリラックスした状態にあることから、企業のデバイスに対するフィッシング攻撃の影響を受けやすくなるという考えを裏付けするものです。



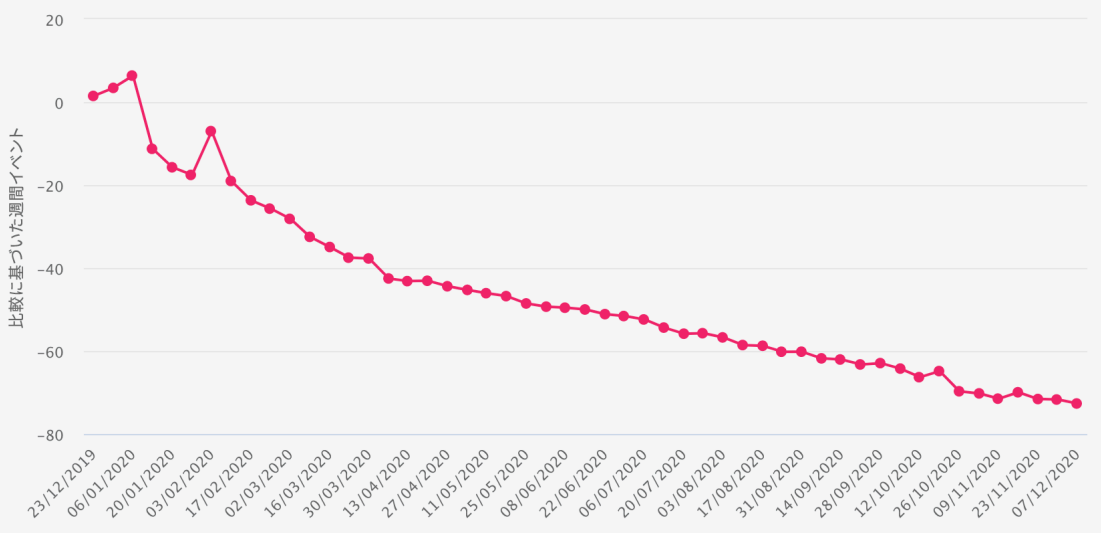
標的にされる犠牲者としてのユーザ

Wi-Fi上の中間者攻撃

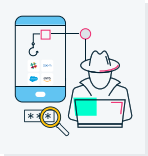
Wi-Fiは、中間者（MitM：Man-in-the-middle）攻撃が発生したときに、深刻なプライバシーリスクをもたらします。モバイルユーザに影響を与えるMitM攻撃には、主に2種類あります。1つ目は、攻撃者が偽のWi-Fiアクセスポイントなどの、ネットワークインフラストラクチャを物理的に制御できる場合で、攻撃者はその中を流れるトラフィックを盗み見ることができます。2つ目は、攻撃者が暗号化を提供するはずのネットワークプロトコルを改ざんし、保護されるべきデータが公開されてしまう場合です。驚くべきことに、従業員の80%以上が業務の遂行中に公共のWi-Fiを使用しています。正式に禁止されている場合でさえもです。

> 2020年には、毎週リスクのある無料Wi-Fiホットスポットに接続しているユーザは4%となり、2019年の7%からの減少が見られました。

MitM攻撃を含むWi-Fi脅威の影響が、2020年にどのように変化しているのかを見てみましょう。



この分析を実施したときには、明らかな理由から確実に減少すると予測していました。COVID-19 が発生する前（2020 年 2 月頃から 3 月頃）と比べると、仕事で出張する回数が減っているからです。このグラフでは、人々が仕事に復帰した 1 月に一時的に上昇した後、COVID-19 の感染者数が急増し、企業が安全を確保するために出張を中止したり、従業員に自宅で仕事をするように勧告したりした 2 月には急減しています。



標的にされる犠牲者としてのユーザ

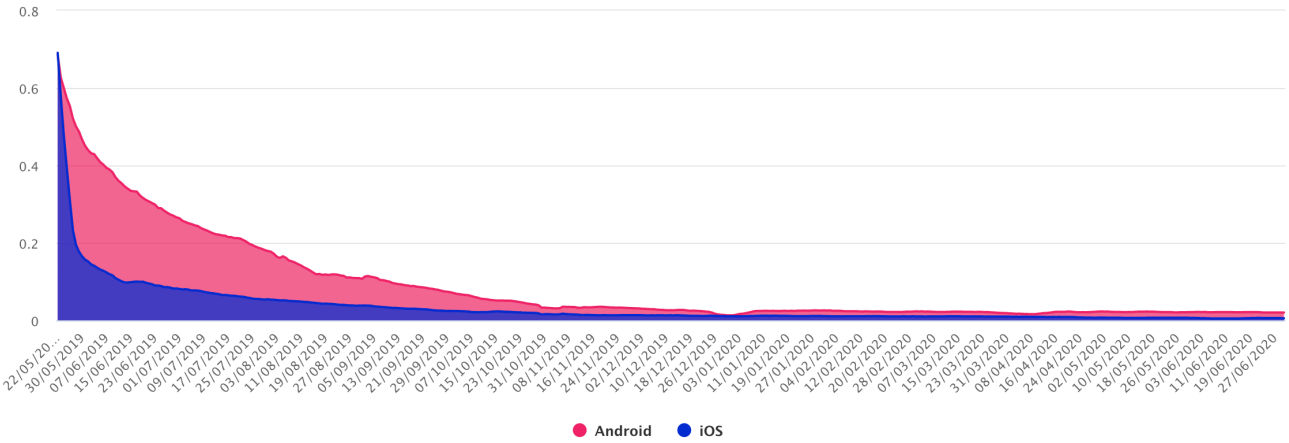
アプリのリスク

マルウェアなどの悪意のあるアプリは、検出されるのを回避するため、ますます巧妙なテクニックを使うようになりました。例えば、最新のマルウェアは、悪意のある動作を開始する前に一定期間待機します。例えば、特定のネットワーク上でのみ悪事を働いたり、ハッカーがいつでも起動できるようなコマンド&コントロールコードを隠したりしている場合があります。アプリストアが実行するような基本的なチェックでは、最新のものを検出することはできませんが、意外にも一般的な悪意のあるアプリは検出できます。

> 2020年には、企業の52%がリモートデバイスでマルウェアインシデントを経験しており、2019年の37%から増加しています。

アプリケーションに隠れているマルウェア以外にも、開発者によるアプリの構築や保護、維持が不十分なために、2019年と2020年にWhatsAppで発見された脆弱性のような、危険な脆弱性が存在する可能性もあります。

> Androidユーザは、2019年5月に古いバージョンのWhatsAppに大きな脆弱性が見つかった後、以下のグラフのようにアプリのアップデートに時間がかかりました。2019年5月中旬から7月中旬にかけて、WhatsAppの脆弱なバージョンの影響を受けた残りのデバイスのうちのおよそ85%がアップデートを行っていました。一方、同時期にアップデートされた脆弱なAndroidデバイスは約50%に過ぎませんでした。



時には、アプリに詐欺やその他の不正行為が含まれていることがあり、こういった詐欺は、開発者によってサードパーティの広告インフラストラクチャを介して導入されることがよくあります。アプリストアの公式チェックを通過したアプリの中には、デバイスの画面を埋め尽くすほどのポップアップ広告を表示して、使い物にならなくするものもありました。私たちはこういったアプリを「潜在的に不要なアプリ」と呼んでおり、200台に1台の割合でデバイスにインストールされています。

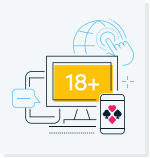
開発者の中には、不注意で暗号化を使用せず、ユーザ（およびその雇用者）をデータ損失のシナリオにさらしてしまう人もいるかもしれません。

- 2020年には、パスワードデータを漏えいさせたアプリを使用していたデバイスが1台以上存在する組織の割合は15%となり、2019年の11%からの増加が見られました。
- 2020年には、iOSデバイスはAndroidデバイスと比べて、アプリの漏えいによる影響を受ける可能性が3.2倍になりました。
- 当社の最近の分析では、未承認のアプリケーションにリスクが発生すると、そのリスクはさらに増加することが分かりました。
- マルウェアに感染したデバイスを少なくとも1台持っている企業は、他の企業に比べると、パスワードの漏えいの影響を4.4倍受けます。
- デバイスに脆弱なアプリケーションがインストールされている場合、他のユーザと比較して、クリプトジャッキングトラフィックに遭遇する可能性が59倍になります。

アプリケーションのセキュリティについて個々に検証するのは手のかかる作業ですが、必要な作業です。これまで以上に多くのデバイスが存在する中で、ユーザはさまざまなアプリケーションにアクセスすることができます。その意図が必ずしも悪いわけではありません。ITに承認されていないPDF統合ツールやその他のファイル管理ツールを使いたいとユーザが思っている場合でも、そのアプリにリスクが伴う可能性があります。IT部門は、ユーザがどのアプリを選んで仕事に使用しているのかについて2つの理由から認識する必要があります。(1)リスクを監査する必要があるため、そして(2)生産性の観点から評価する必要があるため、の2つが理由として挙げられます。安全で生産性に優れていることが証明されれば、そのアプリを受け入れて保護する必要があります。

悪い意思決定者としてのユーザ

前のセクションでは、ユーザがより受動的な役割にある状況での、ユーザから発生するリスクを確認しました。このセクションでは、意図的に企業のポリシーやセキュリティ対策を回避するなど、ユーザがより積極的な役割を果たす場合に起こるユーザ手動のリスクについて見ていきます。意図的に企業のポリシーやセキュリティ対策を回避した場合です。ユーザは、準拠していないコンテンツにアクセスしたり、デバイスのルート化、アプリケーションをサイドローディングしたり、ロック画面を無効化したりするなどして、デバイスのセキュリティに手を加えたりするなど、不注意な判断で、トラブルに巻き込まれる可能性があります。

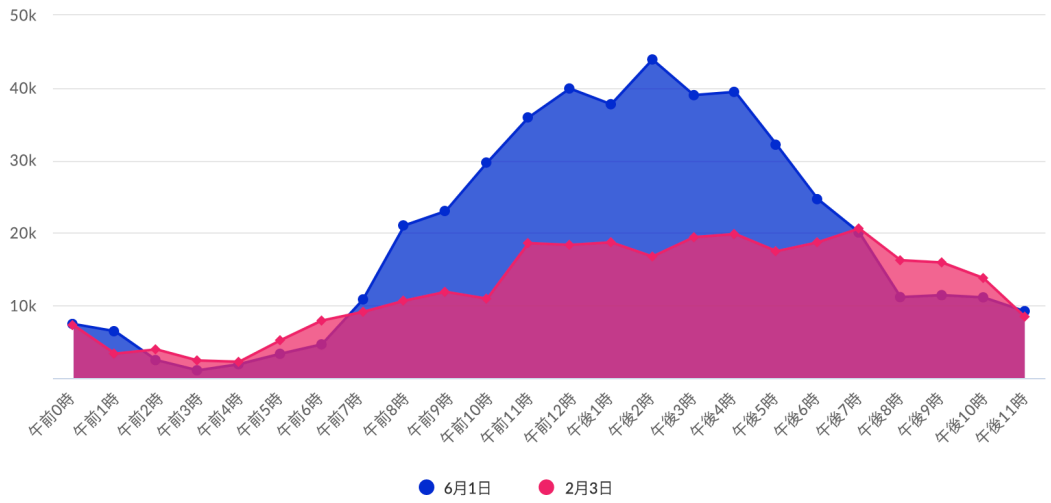


悪い意思決定者としてのユーザ

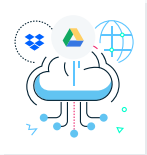
不適切なコンテンツ

インターネットの闇の部分にアクセスできるデバイスがITインフラストラクチャにあると、ビジネスにリスクが生じます。不適切なコンテンツとは、アダルト、ギャンブル、過激、違法なカテゴリーのコンテンツを指します。これらのコンテンツでは、データが漏えいしたり、暗号化されていない技術が使用されていたりするなど、組織をリスクにさらす可能性がより一層高くなります。驚くべきことに、仕事用のデバイスを使用して、インターネットの闇の部分にアクセスする人はたくさんいます。

パンデミック前と比べると、業務時間内の不適切なコンテンツへの接続は最大100%増加しており、大幅な増加が見られました。従業員がリモートワークで業務を遂行する中、デバイスの使用において許容されるポリシーが、リモートデバイス上でも遵守されているかどうかを確認する必要があるのは明らかです。



コンテンツフィルタリングは、さまざまなエンドポイントに企業の使用ポリシーを適用し、従業員とその雇用者の両者のセキュリティ、コンプライアンス、法的リスクを軽減するのに効果的な方法です。



悪い意思決定者としてのユーザ

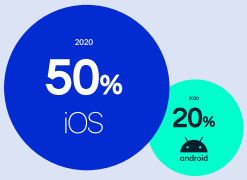
セキュリティ対策の回避

脆弱性は、常にユーザがターゲットとなっているわけではなく、意図的かどうかに関わらず、ユーザ自身が脆弱性を作り出してしまうこともあります。

ジェイルブレイク

ジェイルブレイクとデバイスのルート化を行うことで、ユーザがデバイスのオペレーティングシステムにアクセスし、不正なソフトウェア機能やアプリケーションをインストールできるようにするリスクの高い構成となります。これらの手法は、デバイスにかけられているキャリアのロックを解除しようとするユーザの間でも頻繁に使用されています。

- 2020年には、ジェイルブレイクされたiOSデバイスの数は50%増加し、ルート化されたAndroidデバイスの数も20%増加しました。
- ジェイルブレイクされたデバイスは、されていないデバイスと比べて、悪意のあるネットワークトラフィックに遭遇する可能性が28倍高くなります。
- ジェイルブレイクされたデバイスが少なくとも1台自社のネットワークに存在する企業は、他の企業と比べて、悪意のあるネットワークトラフィックに遭遇する可能性が31.6倍高くなります。
- ジェイルブレイクされたデバイスは、されていないデバイスと比べると、既知の脆弱性がインストールされているアプリケーションを持つ可能性が33倍高くなります。



2019年には、ジェイルブレイクされたiOSデバイスの数は50%増加し、ルート化されたAndroidデバイスの数も20%増加しました。

サイドローディングアプリ

一部のiOSユーザの中には、セキュリティ強化をするためのアプリをインストールする目的で意図的にモバイルデバイスをジェイルブレイクする人もいますが、ほとんどのユーザは、公式のApp Storeでは入手できないアプリケーションをインストールするために使用しています。デバイスをジェイルブレイクすることなくサードパーティのアプリをインストールすることも可能です。これは、サイドローディングアプリと呼ばれるプロセスです。ユーザは、特定の開発者を信頼するようにデバイスを構成するだけで、App Storeを介さなくても、その開発者からのアプリをインストールできるようになります。多くの企業はこの方法で、従業員用のアプリをApp Storeに公開することなくインストールしています。

Googleは、AppleがiOSで行っているようなロックダウンをAndroid OSでは行っていません。Androidのデフォルト設定では、サイドローディングされたアプリは許可されませんが、設定を変更すれば、サードパーティソースからのアプリを許可するようにできます。当社のデータでは、Androidユーザの5人に1人が、サードパーティのアプリをインストールできるようにデバイスを構成していました。

ユーザがアプリをサイドロードした場合、セキュリティリスクは高まります。AppleとGoogleが公式のアプリストアで実施しているアプリケーション審査プロセスを経由しないため、不注意でインストールされてしまったマルウェアに対するデバイスの保護機能が低下し、アプリケーションをサイドロードしたユーザのセキュリティリスクが高まります。

2020年には、仕事に使用されているAndroidデバイス10台のうちの1台に、サードパーティのアプリストア（つまりGoogle Playではないもの）がインストールされていました。

業界スポットライト – 法務

法務系の業界では、他の業界と比べて、ユーザのデバイスにサイドローディングされたアプリケーションがインストールされている可能性が2.5倍高くなりました。

業界スポットライト – 製造

製造業では、他の業界と比べて、デバイスがマルウェアに遭遇する可能性が 2 倍高くなりました。これは、ユーザの 50%以上がサードパーティのアプリストアをインストールしていることと関連している可能性があり、Android ユーザの場合、不明なソースを有効にしている可能性は 2 倍になりました。

画面ロックの無効化

驚くべきことに、モバイルデバイスで利用できる最もシンプルなセキュリティ対策の1つである「ロック画面」は、意外にも軽視されがちです。ほとんどのデバイスでは、ロック画面の設定がデフォルトで有効になっているにも関わらず、ユーザの中にはわざわざこれを無効にして、物理的な盗難が発生した場合にデバイスをより脆弱化させている人がいます。これは、不十分なセキュリティ対策を示すものでもあり、当社のデータによると、この基本的なセキュリティ対策が取り除かれたデバイスでは、他の脅威も増加していることが分かりました。

- 2020年には、仕事で使用されるデバイスの3%でロック画面が無効になっており、2019年の6%と比べると減少していました
- ロック画面を無効にしているユーザでは、他のユーザと比べて、既知の脆弱性を持つOSを実行している可能性が16倍高くなりました
- ロック画面を無効にしているユーザでは、他のユーザと比べて、メールアドレスが漏えいしている可能性が2.4倍高くなりました

業界スポットライト – ITサービス業界

ITサービス業界のユーザは、世界平均と比較して、自分のデバイスでロック画面を無効にしている可能性が2.2倍高くなっています。

2020年には、仕事で使用されるデバイスの3%でロック画面が無効になっており、2019年の6%と比べると減少していました。

リスク要因3

リモートアクセス

これまで、デバイスやオペレーティングシステムのリスクと、ユーザが起因となるリスクについて見てきました。それでは、リモートアクセスの構成が不適切な場合や、まったく保護されていない場合、機密性の高いビジネスアプリケーションには、一体どのようなリスクが生じるのでしょうか。また、リスクのあるデバイスやユーザと、ビジネスアプリケーション内にある機密データとの間に、どのような保護が必要なのでしょうか。

ビジネスアプリケーションの保護と一括りにしても、アプリケーション保護やモバイルアプリケーション管理（MAM）のことではなく、クラウド上で実行されるアプリケーションやワークロード内の機密性の高い知的財産への安全なアクセスを指します。

Cybersecurity Insidersのリモートワークフォースセキュリティレポート2020によると、組織の65%が管理されているアプリケーションに、管理されていない個人所有デバイスからアクセスすることを許可しています。

さらに、IDCのリモートアクセスおよびセキュリティの課題&機会に関するレポート（Remote Access and Security Challenges & Opportunities）では、サイバー攻撃の40%が、許可されたユーザが不正なシステムにアクセスしたことが原因となっています。

多くの場所に存在する数多くのビジネスアプリ

セキュリティ業界でよく認知されていることの1つが、アンケートの対象となったIT専門家らはクラウドを念頭に置いているということです。O'Reillyのクラウド採用に関する2020年度レポート（Cloud Adoption in 2020）に掲載されている調査データによると、組織の39%がパブリッククラウドとプライベートクラウドを組み合わせたハイブリッドモデルで展開しています。さらに、このアンケートでは、回答者の56%以上が、年内にクラウド移行プロジェクトに現在取り組んでいる、または計画していると回答しています。

39 %

ハイブリッドモデルを採用し、パブリッククラウドとプライベートクラウドを組み合わせて使用している企業の割合

56 %

アンケート回答者のうち、今年のクラウド移行プロジェクトに現在取り組んでいる、または計画中であると回答した人の割合。

このデータから、多くの組織が、多様なインフラストラクチャにまたがってデータが存在する分散型のハイブリッド環境を採用していることが分かります。一部の企業では、特定のアプリケーションの管理をいつまでも維持していますが、クラウドやSaaSソリューションにより、アプリケーションを企業の境界の外に置かれるようになったため、それらへのアクセスが、セキュリティサービスの重要な領域となっています。

パブリッククラウド、プライベートクラウド共に実績があり、あらゆる規模の企業が利用できるため、クラウドベースのアプリケーションは、導入、管理、維持が、容易でコスト効率が高いことから、現代の多くの職場で好まれています。同様に、SaaSソリューションは、開発要件やメンテナンスの負担を完全に取り除くことができるため、得てのアプリケーションに適しています。SaaSに関しては、メリットがリスクを上回ることは間違いありません。蛇口をひねれば水が出る時に、わざわざ井戸を掘る人はいません。ガートナーは、2020年だけでも、SaaSソリューションは1,050億ドル近い収益を生み出すであろうと予測しています。

多くの組織がアプリの一部をクラウドに移行し、使用するSaaSアプリの数を拡大する中、組織はこれまで以上に多くのアプリをより多くの場所で管理しています。また、Oktaによると、組織の規模が大きいほど、活用されるアプリの数も増えます。

Oktaの分析によると、世界中のあらゆる業界において、大企業が導入するアプリの数は4年間で68%増加しており、2018年末には企業当たり平均129個まで増えました。この調査が実施された時点では、企業の10%近くが200個以上のアプリを抱えていました。

最新のリモートアクセスの必要性

かつて、企業が保護しようとしていたものはデータセンター1つであり、企業はそれを物理的に管理していました。VPNやRDIなどのレガシーなリモートアクセスツールは、企業と外部との境界のインフラストラクチャ周辺に構築されており、アプリケーションがデータセンターから実行される場合に適切に機能します。「堀で囲まれた城（castle-and-moat）」方式のセキュリティモデルでは、ネットワーク内のものはすでに信頼されたものとして扱われます。つまりこれは、VPNやRDIは、ユーザのIDを確認したり、デバイスのセキュリティポスチャを確認したりする強固な方法なしに、暗黙のうちに接続を「信頼」してしまうため、潜在的な攻撃者によってネットワークセグメント全体にアクセスされてしまう可能性があることを意味します。

IDCによると、リモートアクセスツールに関連した主要なインシデントの68%では、VPNが使用されていました。さらに、サイバー攻撃の40%は、許可されたユーザが不正なシステムにアクセスすることで発生しています。

リモートアクセス戦略で、継続的なリスク評価が重要となるのはなぜでしょうか。数字を見れば明らかです。

- 2020年には、脆弱性が発生した時点で、脆弱性のあるOSを搭載していたデバイスのうち83台に1台がメールに、6台に1台がクラウドストレージにアクセスしていました。
- 2020年にモバイルマルウェアに感染したデバイスのうち、感染した後も企業メールにアクセスし続けていたデバイスは37%、クラウドストレージにアクセスし続けていたデバイスは11%でした。
- マルウェアに感染したデバイスがある企業の42%では、生産性ツールにアクセスしているデバイスが少なくとも1台存在していました。
- クラウドストレージにアクセスするデバイス200台のうちの1台で、デバイスの画面ロックが無効になっていました。
- 脆弱なオペレーティングシステムを使用するユーザがいる企業の40%以上で、これらの脆弱性のあるデバイスのうちの少なくとも1台が、クラウドストレージにアクセスしていました。
- お客様の1.3%が、Office 365やGoogle Workspaceなどの生産性ツールを使用しているデバイスでマルウェアに感染していました。
- つまり、ユーザ認証だけでは、機密性の高いビジネスデータを侵害されたデバイスから守ることは出来ません。では、何が解決策となるのでしょうか。ゼロトラストネットワークアクセスは、従来のアプローチとは根本的に変えるものです。サーバボックス、設備、物理的なデバイスは必要ありません。また、クラウド型のネットワークセキュリティは拡張性があります。そうでなければ、企業の境界を越えてクラウドへと移行するすべてのデータを保護するのに十分な数のアプライアンスを購入することは出来ません。

また、ゼロトラストネットワークでは、機密性の高いアプリケーションへのアクセスを要求するデバイスに対してリスク評価を継続的に行っており、デバイスがコンプライアンスに準拠していることを確認することが出来ます。これには、デバイスが安全なネットワーク上にあること、予測される場所にあること、感染しておらず脆弱性がないこと、また、ユーザにそのリクエストを行う権限があることなどが含まれます。

42%

マルウェアに感染したデバイスが存在する企業のうち、少なくとも1台のデバイスが生産性ツールにアクセスしていると回答した企業の割合。

2020年には、脆弱性が発生した時点で、脆弱性のあるOSを搭載していたデバイスのうち、83台に1台がメールに、6台に1台がクラウドストレージにアクセスしていました。

クラウドセキュリティレポート

推奨事項

企業のIT管理標準を定義するための試みが数十年にわたって行われてきたにもかかわらず、多くの組織では、標準化されていないことが標準であるという状況に陥っています。ビジネスでは全てのOSを使用しますし、アプリには全てのユーザがアクセスします。また、ユーザはあらゆる場所から業務を遂行することができます。

セキュアなリモートアクセスソリューションには、ブロックするのではなく有効にし、生産性の妨げとならないような柔軟性と俊敏性が必要です。今日のIT環境のニーズに合う最新のSASEセキュリティ戦略を策定するために、このチェックリストを利用されることをお勧めします。

リモートワークによって生まれる新しいユースケースに基づいて要件を整理すること

- メールへのアクセスや機密性の高いデータベースへのアクセスなど、従業員がデバイス上で何をしようとしているのか、データを細分化することでアクセス範囲を細かく設定します。
- ユースケースを評価し、リモートワーカーのための要件を定義します。
- 上記の要件から、デバイス所有モデル（サポートするデバイスの種類、誰が所有するのか、どのように管理するのかなど）を把握します。

接続性

- 接続性とクラウドアプリケーションについては、企業リソースへのアクセスを許可する前に、ユーザ、デバイス、ネットワーク、アプリについて何を知る必要があるかを決定します。
- 必要なビジネスツールのみをユーザが利用できるようにすることで、過剰な権限を持つアカウントが悪用されて、様々なのシステムが攻撃されることを防ぎます。

適正使用の定義

- 既存の利用規約を見直し、すべてのタイプのエンドポイントが組み込まれていることを確認します。
- シャドーITや不要な使用状況を管理して、規制遵守を確実にするために、適切なデバイスのサブセットごとにデバイスの使用において許容されるポリシーを実装します。

アクセス管理ポリシーを拡張してデバイスに対するリスクポスチャを組み込むこと

- モバイルを含むすべてのデバイスで企業アプリへの認証を行うため、ユーザが使いやすいIAM（IDおよびアクセス管理）ソリューションを実装します。
- デバイスのリスク評価をIAMポリシーに組み込んで、デバイスのリスクポスチャが考慮されるようにします。
- セッションの期間中、リスクポスチャが継続的に評価されるようにします。

すべてのデバイスをカバーするエンドポイント保護を導入します。特にクラウドベースのセキュリティソリューションは、広範なサイバー上の脅威やデバイスを利用する上でのリスクから保護するために重要です

- セキュリティソリューションには、強力なエンドポイント検出機能と、デバイスに到達する前に攻撃を防ぐためのネットワーク内アーキテクチャが含まれていることを確認します。
- セキュリティソリューションが、外部からのサイバー上での脅威（フィッシング、中間者攻撃、マルウェアなど）と使用行動上のリスク（サイドロードされたアプリなど）の両方に対応できるものであることを確認します。
- すべてのセキュリティツールで、エンドユーザのプライバシーを尊重しながら、脅威ベクトルに対処するためのご自身の組織のビジネスに沿った適切な設定が行われていることを確認します。
- セキュリティソリューションの機械学習機能を評価し、脅威エンジンがどのように新たな脅威を特定して保護するのかについて理解します。

デバイスレベルで制御するためにUEMを導入すること

- 該当する場合は、UEMソリューションを導入し、企業リソースを使ってデバイスをプロビジョニングしたり、継続的にデバイスのコンプライアンスを確認したりできるようにします。

このリストは頻繁に確認して、以下に基づいて変更する必要があるかどうかを検討すること

- 企業の規模や構成の変更（合併や買収など）
- データ処理の方法に影響を与える新しい規制
- 進化するIT戦略
- 従業員に影響を与えることが確認できた脅威
- 業務を遂行するために、従業員が必要とする新しいアプリケーション