Lookout

KEVIN MAHAFFEY MIKE MURRAY

モバイル リスクの全容:

モバイル活用時に企業が把握しておくべき リスクのすべて

モバイル リスクの全容:

モバイル活用時に企業が把握しておくべきリスクのすべて

企業におけるリスク管理を変えるべきときが来ています。モバイル端末はいまや個人の生活だけでなく企業活動にも欠かせないものとなりましたが、多くの企業では未だ、PC のエンドポイントにばかり目を向けています。

PC に影響を与えるリスク要素の多くはモバイル エンドポイントにもあてはまりますが、既存の PC のセキュリティ対策を社内の全モバイル端末に拡張するだけでは効果がありません。モバイルのリスクにも対処できるようリスク管理を進化させ、モバイル独自のセキュリティを設計する必要があります。

この進化を後押しするため、Lookout はモバイル リスク マトリクスを作成しました。このマトリクスをベースにすることで、セキュリティ担当者はモバイル端末に関するリスクの全容を把握することができます。また、モバイル リスクの発生率を示すデータも掲載しています。

モバイル リスク マトリクス

リスクの要素	攻撃ベクター: アプリ	端末	ネットワーク	ウェブ/コンテンツ
脅威	アプリの脅威 悪意のあるアプリが情報を搾取したり、端末に損害を与え、不正なリモートアクセス権を取得する。	端末の脅威 攻撃者が高レベルの権限を取得し、壊滅的なデータ損失を引き起こす。	ネットワークの脅威 Wi-Fi またはセルラー ネットワーク接続を介してデータが搾取される。	ウェブ/コンテンツの脅威 フィッシング E メールや SMS メッセージからアクセスする悪意のある URL。
脆弱性	アプリの脆弱性 アプリに存在する脆弱性。	端末の脆弱性 OSに存在する脆弱性。	ネットワークの脆弱性 モバイル端末はPCよりネットワーク攻撃の標的になりやすい。	ウェブ/コンテンツの脆弱性 ビデオ、写真などの不正なコンテンツによって、端末への不正アクセスが可能になる。
ビヘイビア & 設定	アプリのビヘイビア & 設定 不要に機密情報にアクセスしたり、データ漏洩のリスクが高いアプリ。	端末のビヘイビア & 設定 Android の USB デバッグや非公式のアプリ ストアからのアプリのインストール。	ネットワークのビヘイビア & 設定 不正な設定のルーター、不明なキャプティブ ポータル、コンテンツ フィルタリング。	ウェブ/コンテンツのビヘイビア & 設定 証明書を暗号化していなかったり、データを漏洩するウェブサイト。

モバイル リスク マトリクスは、こちらから印刷できます。

Lookout は、世界各国の企業と個人のアクティブ ユーザーから収集した、モバイルのコード、端末のソフトウェア、ウェブ、ネットワーク攻撃に関する膨大なデータを取りまとめ、当社の 10 年間におよぶモバイルの脅威と脆弱性に関する研究を活用し、このマトリクスを作成しました。

企業はそれぞれのビジネスの状況に応じてモバイル リスク マトリクスの各要素を評価することができます。例えば、iOS を狙ったスパイウェアの全体的な発生率はそれほど高くありません。しかし、経営層がモバイル端末で重要な企業機密を扱うことがある企業では、これら経営層は高リスク ターゲットとなるため、経営層のモバイル端末のリスク レベルは高とみなし、適切なセキュリティ対策を施すことができます。

モバイルの脅威について理解する

テレビのニュースやオンライン メディア、新聞紙上で、モバイルの脅威が頻繁に取り上げられるようになりました。モバイルの脅威は高度化を続けています。本格的なモバイル スパイ攻撃の最たる例が、iOS や Android を狙った「ペガサス」というスパイウェアです。ペガサスは、モバイル リスク マトリクスでは端末の脅威に分類されています。ペガサスを使った攻撃には、フィッシング (ウェブ / コンテンツの脅威) やソフトウェアの脆弱性が悪用されました。これは、モバイルの脅威を理解するうえで重要なポイントです。悪意のある攻撃はあらゆる媒介を通じてデータを搾取しようと試みているのです。

アプリの脅威について

悪意のあるモバイル アプリは、情報を盗んだり、端末に物理的な損害を与えたり、ユーザーや企業の活動を監視するなど、数々の不正行為を働きます。アプリの脅威には、正規のモバイル アプリであるにも関わらず悪意のあるコードを注入されたもの、ユーザー権限を不正に取得されたり誤って付与したためにマルウェアアプリに感染するケース、懐中電灯アプリを装っているが実際は不正な営利目的ですべての個人情報にアクセスするように目的を隠蔽した不正アプリなどがあげられます。

多くの企業はモバイル端末管理 (MDM) ソリューションが悪意のあるアプリから保護してくれると考えていますが、必ずしもそうではありません。公式アプリストアの利用を禁止しても、ユーザーはスマートフォンにアプリを「サイドロード（公式アプリストア以外からアプリをインストールすること）」することが可能です。実際に、Lookout は企業が支給している端末で悪意のあるアプリケーションを多数検知しています。

アプリ脅威の発生率

2016 年第 4 四半期および 2017 年第 1 四半期において、Lookout で保護している企業利用の Android 端末 1,000 台のうち 47 台でアプリベースの脅威が発生し、iOS 端末では 1,000 台のうち 1 台発生しました。[1]

アプリの脅威対策

アプリの脅威に対する包括的な対策を実施するには、モバイル脅威対策だけでなく、次のことが必要です。

- 企業が管理する端末を対象としたモバイル端末管理 (MDM) およびモバイル アプリケーション管理 (MAM) ソリューション
- 侵入検知システム (IDS) および侵入防御システム (IPS)
- モバイル固有の脅威情報を、脅威インテリジェンスやネットワーク管理を介して把握する (ファイアウォールでモバイル通信における「C＆C」サーバーのブラックリストに登録するなど)
- URL フィルタリング / ウェブ セキュリティ コントロールを介したモバイル アプリのダウンロードの検知および調査

[1] 分析したデータは、2016 年 4 月 15 日から 2017 年 4 月 16 日にかけて、世界中の Lookout の個人および企業ユーザーのセンサーから収集したものです。分析した企業ユーザーのデータは、金融機関、医療機関、政府機関、その他主要な業界で利用されている Android および iOS 端末が対象です。個人ユーザーのデータにおいては、世界各国の個人ユーザーが利用する Android および iOS 端末が対象となっており、その数は 1 億台以上にのぼります。

端末の脅威について

モバイル端末の OS やファームウェアに対する脅威は、壊滅的なデータ損失を引き起こす可能性が極めて高くなります。OS を侵害することで、攻撃者が通常のアプリに与えられるよりも高いレベルの権限を取得できるためです。

発生率は低いものの影響が大きい顕著な例として、「ペガサス」という スパイウェアがあります。これは、iOS と Android 端末の両方が攻撃対象になっています。「ペガサス」は、ソーシャル エンジニアリング型フィッシング SMS を 1 回タップさせるだけでジェイルブレイクを行います。これにより、攻撃者は端末のカメラやマイクを有効にして、端末の周囲の会話を盗聴し、被害者の行動を追跡したり、エンドツーエンドのチャット クライアントからメッセージを盗み見ることもできます。

端末の脅威にさらされることで問題となるのは、端末が侵害されることで端末上のその他すべてのセキュリティや管理機能が無効になる可能性がある点です。例えば、根本的な問題として、モバイル端末自身が侵害されると、企業のデータを安全に格納しているコンテナ (MDM および MAM ソリューションを含む) まで侵害される恐れがあります。

また、モバイル端末を多要素認証として利用している場合は、端末が侵害されることでモバイル端末に配置されている「ソフト トークン」まで侵害される恐れがあるため、事態はさらに深刻になります。

Lookout のセキュリティ研究者は、このような端末を侵害する攻撃がバンキング型トロイの木馬で採用されているのを何度も発見しています。攻撃者は、モバイル端末を侵害し、入力されたユーザーのパスワードと 2 要素認証の情報を盗み、SMS トークンを使って銀行にログインできるようになるのです。

つまり、端末自身を保護しなければどのようなセキュリティ対策が施されていても無意味な結果になりかねませんし、モバイル端末自身を 2 要素認証のアクセストークンとして利用することにも危険がはらむ結果になるのです。

ネットワークの脅威について

ネットワークの脅威は、Wi-Fi、セルラー、その他のネットワークを介した TLS/SSL セッションの確立方法における脆弱性を悪用します。このような攻撃は、攻撃者によって直接実行されるか、自動化された手法を使うマルウェアを通じて行われます。このようなインシデントの例には、中間者攻撃、認証なりすまし、TLS/SSL ストリップ攻撃、TLS/SSL 暗号化ダウングレードなどがあります。

ネットワークからの攻撃にあってもファイアウォール内であれば安全であるケースが多いので、ネットワーク攻撃自体はそれほど多くはありませんでした。しかしここ数年、モバイル端末でネットワーク接続するケースが増大し、モバイル端末が社内ネットワークではなく、他のネットワークに接続している時間のほうが長くなっています。このような環境の変化により、社内ネットワーク接続だけだった際には発生率が低かった、ネットワーク攻撃に対する懸念が一気に高まっています。

ネットワークの脅威発生率

昨年、企業利用のモバイル端末において中間者攻撃に遭遇した端末は、1000 台のうち 10 台未満 (0.8%) でした。

このような中間者攻撃には、教育現場などで行われるコンテンツ フィルタリングなど、故意ではないデータの傍受も含まれている点に注目する必要があります。しかし、悪意がなくてもこのような傍受は事実上、転送中のデータを他者から見られないようにするために導入されたデータ保護手法に対する「攻撃」です。

ウェブ / コンテンツの脅威について

悪意のあるコンテンツは、正規のログイン ページを装ったウェブサイトにユーザーを転送する特定のリンクを含むフィッシング メールやテキスト メッセージを介して配信されます。例えば、「ペガサス」はソーシャル エンジニアリング型フィッシング SMS を送付する攻撃手法を取っています。ユーザーが誤って SMS をクリックすると、ブラウザの脆弱性を悪用した後に、端末のカーネルの脆弱性を悪用します。

IBM が 2011 年に行った調査によると、フィッシング ページに認証情報を入力してしまうモバイル端末ユーザー数は、PC ユーザーの 3 倍にのぼります。フィッシング メッセージには通常、ドライブバイ ダウンロードを実行したり悪意のあるコードを端末に注入したりする、悪意のあるウェブサイトに誘導するリンクが含まれています。

ウェブ / コンテンツの脅威対策

ウェブ / コンテンツの脅威は攻撃の入り口となることが多いため、これら脅威に注意を向けることはきわめて重要です。ウェブ / コンテンツの脅威の予防をすることで、攻撃プロセス全体を早期に停止できる効果が期待できます。例えば、「ペガサス」の攻撃では悪意のある SMS が送信され、ユーザーの端末にトロイの木馬をインストールするドライブバイ ダウンロードを実行させました。

ウェブ / コンテンツの脅威対策には、モバイル脅威対策 (MTD) ソリューションに加えて、モバイル端末を狙うフィッシング対策、モバイル端末でのウェブコンテンツ フィルタリング対策、ソーシャル ネットワークを通じて発生するフィッシング攻撃からユーザーを保護するソーシャル メディア セキュリティ ツールが、ゲートウェイセキュリティに導入されているかの確認が必要です。例えば、2016 年にイスラエル国防軍を ViperRAT トロイの木馬攻撃に感染させた手口は、モバイル端末を狙ったフィッシングでした。

モバイル ソフトウェアの脆弱性を理解する

モバイル環境の保護における課題は、モバイルを狙った脅威だけではありません。アプリや端末自体にも、セキュリティ インシデントの発生率を高める脆弱性が存在します。

アプリの脆弱性について

モバイル アプリには、PC のソフトウェアと同様の脆弱性があります。しかしモバイル アプリでは、その脆弱性が一層大きな問題となります。ほとんどのモバイル アプリはエンドユーザーによって選ばれ、小規模のデベロッパーによって開発されているためです。一方 PC のアプリケーションは多くの場合、IT 部門によって調査され、大規模なソフトウェア企業が開発しています。

アプリの脆弱性発生率

Lookout のセキュリティ研究者は、Android と iOS で人気の高い生産性改善アプリとビジネス アプリを詳しく分析しました。調査の結果、多様な脆弱性が見つかり、それぞれ攻撃者に必要な知識やエンド ユーザーへの影響に違いが見られます。その幅広い脆弱性の中でも、Lookout が発見した最も高リスクで高度化されたアプリの不具合は、アプリに表示される情報だけでなく、被害者のクラウド サービスのアカウントや、そのアカウントに関連付けられたすべての情報まで盗まれる恐れがありました。

広く蔓延したアプリの脆弱性が公開されている例として、Android の addJavascriptInterface の危険な使い方があります。Lookout は 90,000 以上 のアプリでこの脆弱性を見つけました。パッチを配布して解決するのは到底不可能な問題です。

アプリの脆弱性対策

モバイル アプリで転送中のデータに対するセキュリティ コントロールは近年改善されつつありますが、著名なソフトウェア開発企業がリリースしたアプリでさえも、企業やユーザーをリスクにさらすセキュリティ上の不具合が含まれています。

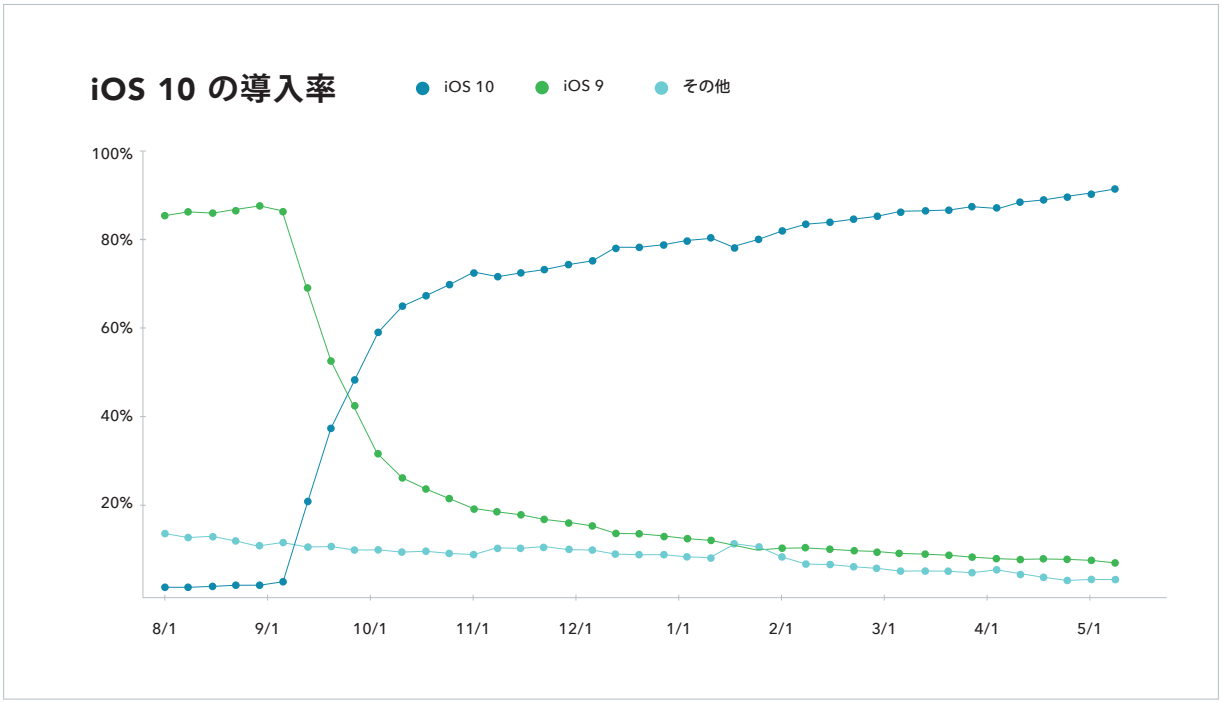
アプリのセキュリティ調査を行っていると、転送中のデータに対する不十分なセキュリティ コントロールが見つかることが珍しくありません。そこから派生して、意図せず機密情報を漏洩したり、悪意のある人物に被害者の端末を直接攻撃する機会を提供するなど、大きな問題が起こる可能性があります。このようなリスクの影響は、攻撃者の知識や目的により、最小限にとどまるものから壊滅的な被害をもたらすものまでさまざまです。

ユーザーや企業の機密データを扱うモバイル アプリの利用をサポートする組織が増えるにつれて、アプリの脆弱性を悪用し機密情報にアクセスしようとする攻撃者はますますこの分野を狙うはずです。

端末の脆弱性について

モバイル端末もまた、数多くの既知の脆弱性に悩まされています。Google と Apple は、端末の脆弱性について多数の修正が行われていることを知らせるセキュリティ速報を定期的にリリースしています。

企業は「脆弱性半減期」、つまり新しいパッチのリリースから社内のモバイル端末へのアップデートの完全な適用までの所要時間を追跡することで、端末の脆弱性によるリスクを測定できます。一般に、個人端末の業務利用 (BYOD) に基づくモバイル活用は、会社所有の端末に基づくものよりも脆弱性半減期が長期化する傾向があります。また、iOS 端末よりも Android 端末のほうが長期化します。どちらのモバイル プラットフォームも、脆弱性対応期間は PC における脆弱性半減期よりも大幅に長くなり、脆弱性管理ベンダーの Qualys は 30 日間と評価しています。



Mixpanel 提供のこちらのデータによると、iOS は 8 か月以内に iOS 10 の導入率 90% 以上を達成しました。

端末の脆弱性発生率

Lookout で保護されている個人用端末のうち、2017 年 4 月時点で iOS オペレーティング システムをバージョン 10.3 以上にアップデートしているユーザーはわずか 43% で、10.2 が 42%、9.3.5 が 6% です。

つまり、多くのユーザーは最新のセキュリティ アップデートを適用していない端末を使っています。iOS ユーザーの 15% に、WebKit (Safari の基盤となるブラウザ エンジン)、App Store および多数の iOS アプリに関する iOS の脆弱性があります。

Samsung Galaxy S6 ユーザーの場合、92% が最新バージョンのオペレーティング システム、7.0 Nougat にアップデートしていません。

ネットワークの脆弱性について

ネットワークの脆弱性によって端末がネットワーク経由で攻撃され、端末 OS の脆弱性が狙われてセキュリティが侵害されたり、データが傍受されたりします。

例えば、2017 年 3 月の Black Hat Asia で行われたトークショーでは、研究者が iOS サンドボックスを完全にバイパスし、ユーザーが一切介入することなく、Wi-Fi 経由で iOS 端末の脆弱性をリモートで悪用する方法が紹介されました。さらに最近でも、SC Magazine の記事によると、不具合を修正するため Apple が iOS バージョン 10.3.1 をリリースしました。この不具合は Wi-Fi 経由で悪用可能で、その脆弱な端末に接続できる範囲内で iOS の不具合を悪用される恐れがありました。

ネットワークの脆弱性発生率

Windows XP 以降、ほぼすべてのエンドポイント セキュリティ にはファイアウォールとホストベースの侵入検知 / 予防 (HIDS / HIPS) ソリューションが含まれていますが、モバイル端末には同レベルの保護がなく、従来のラップトップよりももっと敵対的なネットワークにさらされる恐れがあります。

ウェブ / コンテンツの脆弱性について

ウェブ ページ、ビデオ、写真など、不正なコンテンツによって特定の脆弱性が引き起こされ、対象のアプリや OS のコンポーネントを悪用して端末に不正にアクセスされる恐れがあります。

よく知られている例が Stagefright です。これはビデオ ファイルから端末の脆弱性を悪用して Android のメディア処理ライブラリにアクセスする方法で、あらゆる媒介を通じて悪用されました。このような媒介には、MMS メッセージや、ウェブ経由のファイル ダウンロードなどメディア ファイルを処理する任意のチャンネルが含まれます。

ウェブ / コンテンツの脆弱性対策

ほぼすべてのウェブ / コンテンツの脆弱性は、アプリや端末の脆弱性と関連しています。しかし、企業はアプリや端末の脆弱性悪用を予防し補完する、ウェブ / コンテンツの脆弱性を保護する対策を別途検討する必要があります。ウェブ経由で狙われるコンテンツの脆弱性については、既存のウェブコンテンツのファイアウォールを活用できます (建物内または VPN 内の場合など)。さらに、E メールのコンテンツからの保護によってモバイル フィッシングを防止したり、ソーシャル メディア用セキュリティ製品を使って、脆弱性を引き起こそうとするコンテンツがモバイル端末に到達できないように保護を強化することができます。

ビヘイビア & 設定について理解する

多くの従業員はセキュリティに詳しくないため、高いリスクにさらされる危険があります。個人のモバイル端末を業務にも使用し、その端末の設定が組織のセキュリティ ポリシーに違反していることも多々あります。安全性を確保できるなら BYOD ポリシーを有効にしたいと考えている企業もあるでしょう。安全なモバイル活用を実現するには、まずビヘイビア & 設定の可視化がその第 1 歩となります。

アプリのビヘイビア＆設定について

機密情報を扱うアプリは企業データの漏洩につながりかねません。

以下に例を示します。

- IT 管理者によって管理されていない、企業の機密データやクラウド ストレージ サービスにアクセスするアプリ。
- クレジット カードや個人情報などコンプライアンス要件の対象となるデータにアクセスするにも関わらず、データの使用、転送、保存が十分に保護されていないアプリ。

アプリのビヘイビア＆設定に起因するリスク発生率

2016 年第 4 半期から 2017 年第 1 四半期にかけて、Lookout で保護されている企業モバイル端末のうち、iOS 端末の 11% でアプリのサイドロードが発生しました。また、29% のアプリが連絡先にアクセス、38% が GPS にアクセス、8% がカレンダーにアクセス、10% がマイクにアクセス、25% がカメラにアクセスしています。

iOS における企業向け アプリ全体では、43% が Facebook に接続し、14% が Twitter に接続しています。

端末のビヘイビア＆設定について

端末のビヘイビア＆設定に起因するリスクの大半は、ジェイルブレイクまたはルート化したモバイル端末を使う従業員からもたらされますが、端末でパスコードを有効にしていなかったというごく単純なケースもあります。リスクの要因となるビヘイビア＆設定は、Android の USB デバッグ、非公式アプリ ストアからのアプリのインストール、iOS での特定のエンタープライズ設定プロファイルなどです。このような例の多くは、MDM で対処できます。

端末のビヘイビア＆設定に起因するリスク発生率

Lookout で保護されている企業モバイル端末のうち、ジェイルブレイクした iOS 端末は 1,000 台のうち 1 台、ルート化した Android 端末は 1,000 台のうち 5 台でした。

ネットワークのビヘイビア＆設定について

ネットワークのビヘイビア＆設定は、公共 Wi-Fi を使用する従業員のリスクと考えればよく理解できます。公共 Wi-Fi に接続する「無謀な」エンドユーザーが多いほど企業データに対するリスクが大きくなります。

従業員の多くは、出張中に空港、ホテル、カフェ、公共施設で Wi-Fi を使用して不正な設定のルーター、不明なキャプティブ ポータル、コンテンツのフィルタリングを通してトラフィックを解読するネットワークに接続してしまっても、まったくわかりません。

ネットワークのビヘイビア＆設定に起因するリスク

ネットワークのビヘイビア＆設定に起因するリスクは、従業員が所有するすべての端末が公共ネットワークに接続する回数と同じ頻度と考えることができるため、大きなリスクと言えます。グローバル 企業ではこの結果は膨大な数になり、これはモバイルでデータ漏洩する可能性がある新たなリスクを示しています。

ウェブ / コンテンツのビヘイビア＆設定について

従業員は誤って不明な差出人からの E メールの添付ファイルを開いたり、SMS メッセージやその他のメッセージ アプリでリンクをクリックしたりすることがあります。添付ファイルにはあらゆるタイプのコンテンツが含まれていますが、メディア ファイルが添付されていることもあります。これらのファイルにアクセスすると、悪意のあるコンテンツや悪意のあるウェブページによるエクスプロイトやフィッシングのリスクにさらされる可能性が高まります。

さまざまなモバイル リスクから企業を保護するには

モバイル環境にセキュリティを拡張するためのステップとして、モバイル リスク マトリクスの各要素について検討し、環境に応じてそのリスクを管理するための戦略を立ててください。

モバイルの活用方法は企業によって異なります。企業ごとに異なるニーズ、つまり固有のビジネス機能があります。企業ごとのリスクの可能性や影響を評価することで、最適なセキュリティ戦略を計画できるようになります。

このプロセスを行うにあたり、セキュリティ部門は 2 つの重要な質問に回答しなければなりません。

1. 現在のモバイル環境で、マトリクスの各要素のリスクをどう評価したか
2. そのモバイル リスクの要素について、現在どのようにコントロールしているか

多くのセキュリティ部門は、ほとんどのリスクについてごく限られた情報しか得られていないことに気づき、また既存のソリューションではこれらのリスクをコントロールする方法が限られていることにも気づきます。

> 「エンドポイントおよびモバイルのセキュリティを担当するセキュリティ / リスク マネージャは、ただちにモバイル脅威対策 (MTD) ツールの評価を開始し、EMM を補完するためこれらのソリューションを徐々に実装しなければならない」
>
> **Gartner Predicts 2017:Endpoint and Mobile Security□2016 □ 11 □**

これらの制限に気づくことで、「セキュリティ担当者は Gartner が推奨するモバイル脅威対策 (MTD) ツールの評価を開始し、EMM を補完するためこれらのソリューションを徐々に実装することを検討し始めるでしょう。」

リスク全体を把握することでセキュリティ担当者は効果的なモバイル脅威対策、モバイル アプリのレピュテーション、モバイル脆弱性管理を実現し、従業員は安全に、モバイル テクノロジーを活用して最大限の生産性をあげることが可能になります。

□□□□□

Kevin Mahaffey

Lookout の共同設立者兼 CTO

Kevin の投稿を読む

Mike Murray

セキュリティ インテリジェンス担当副社長

Mike の投稿を読む