okta

Okta ソリューションにより セキュリティインシデントへの 対応を自動化

Okta Japan 株式会社
〒150-0002 東京都渋谷区渋谷 2 丁目 24-12
渋谷スクランブルスクエア 38 階
Marketing-Japan@okta.com

セキュリティ脅威には即時の対応が不可欠。自動化とセキュリティオーケストレーションの強化により実現。

このように短い時間に起こる破壊的なハッキングが多発しているため、組織は不審な活動を特定した瞬間に迅速なアクションを取れる体制を敷いていなければなりません。侵入者からの大損害を被る前に漏えい食い止めるには、人が行動するよりも迅速にセキュリティ対応を始めなければいけません。つまり、インシデント対応をできる限り効率的に行うと同時に、自動化することが理想的には求められます。

セキュリティ部門が脅威に対して効果的なアクションを迅速に取れるほど、安全が担保できます。

セキュリティ攻撃は、一瞬のうちに発生します。Verizon社が2016年に発行した「データ漏洩/侵害調査報告書（DBIR）」によると、フィッシングメールを受信した人のうち、30%がメールを開封しています。平均すると、メール開封までの時間はわずか1分40秒で、悪質なリンクや添付ファイルを開いてしまうまでの時間は3分45秒と報告されています。

5分もかからずに、安全なはずのネットワークやアプリケーション、データ、そしてユーザー情報が漏えいしてしまうのです。

数字で見るデータ漏えい

サイバー犯罪は継続的に発生。近年は悪用のためにユーザー資格情報を狙う攻撃が増加

13.3億ドル
2016年に米国企業が被った、サイバー犯罪による金銭的損失[1]

362万ドル
1回のデータ漏えいにかかる平均のコスト[2]

30%
フィッシング攻撃のメッセージを受信者が開封した割合[7]

1分40秒
受信者がフィッシングメールを開封するまでの平均時間[8]

9,576件
2016年に報告されたフィッシングの件数[3]

91%
フィッシング攻撃で受信者の資格情報が盗み取られた割合[4]

74%
2017年前半に発生したデータ漏えいのうち、アイデンティティ盗難の割合[5]

3分45秒
受信者が悪質なリンクや添付ファイルをクリックするまでの平均時間[9]

出典：
1. https://www.statista.com/markets/424/topic/1065/cyber-crime/　2. https://www.ibm.com/security/data-breach/index.html/
3、4、6、7、8、9. http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf
5. https://www.statista.com/statistics/329593/frequency-share-incident-classifiaction-patterns/

脅威に効果的な対策とは？

最初のステップは、資格情報をできるだけ安全に保つことです。資格情報を保護する主な方法としては、多要素認証（MFA）の導入が挙げられます。MFAにより、ユーザーに過大な負荷を強いることなく、より安全性の高い認証ポリシーを策定できます。資格情報を保護する上でMFAは重要な役割を果たしており、攻撃者対策の最前線として機能します。

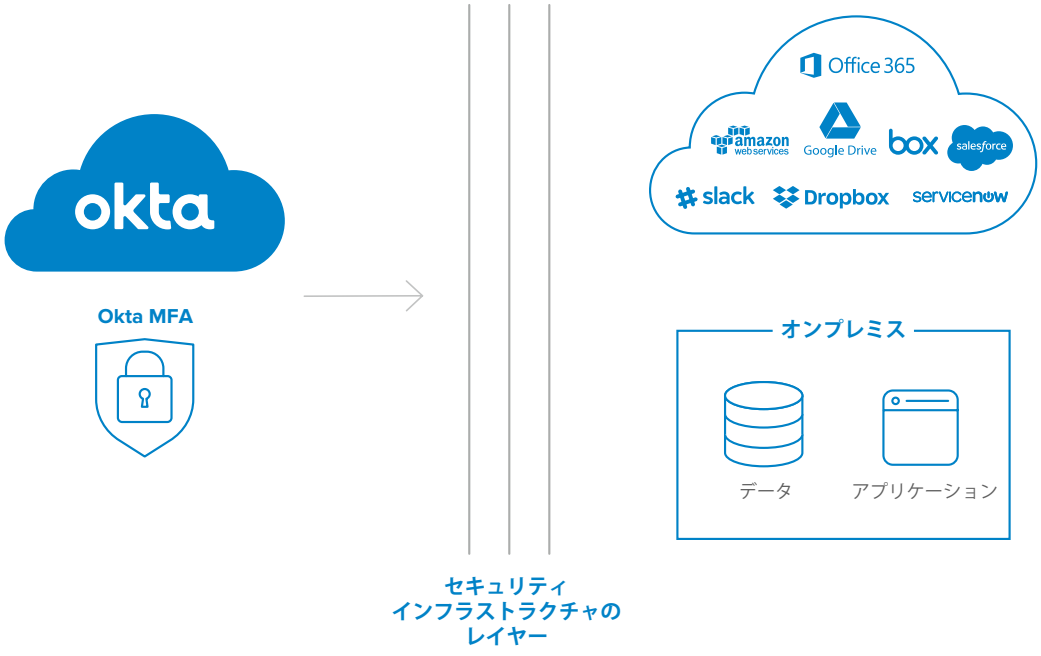
資格情報を守る追加のセキュリティレイヤーを設置することで、組織はユーザーの活動を可視化し、不審な行動を検知しやすくなります。システムにログインしようとするユーザーが不審または悪質とみなされた場合、システムはすぐにセキュリティアナリストにアラートを出し、即座のアクションを促す必要があります。また、ポリシーベースの自動対応により、認証のステップアップを即座に強制したり不審なユーザーを一時停止したりすることが理想的です。いずれの場合も、攻撃者が企業に実害をもたらす前に阻止することができます。

攻撃の頻度やスピードが高くなると、複雑な環境を手動で保護することは不可能です。アイデンティティ管理、分析、およびセキュリティの自動化を行う高度なツールを使い、企業の安全を守る必要があります。アイデンティティの保護は、セキュリティ体制を強化するうえで非常に重要です。

これこそ、Oktaが最も効果を発揮する分野でもあります。

Oktaは、セキュアな認証とMFAで、企業のクラウドとオンプレミスのインフラストラクチャに、アイデンティティベースのセキュリティ境界を提供します。さらに、Oktaが連携しているさまざまなセキュリティ企業が、組織における安全確保に必要なレベルの自動化を実現しています。

Oktaは、アイデンティティレイヤーをはじめとして、企業のセキュリティインフラストラクチャのその他の部分とも連携する、一元化された監視および自動化の機能を提供します。これにより、セキュリティアナリストは、必要な情報をすぐに利用して、あらゆる攻撃を封じ込め組織の資産を保護することが可能です。



Okta MFA は既存のセキュリティインフラストラクチャと連携して、クラウドおよびオンプレミスのアプリケーションやデータを保護します。

Oktaが提案するアイデンティティ主導セキュリティの仕組み

セキュリティインフラストラクチャは数多くのシステムから構成されており、それぞれがトラフィックを監視し、不審な活動を検出し、データへのアクセスや関連付けを通じてアラートを生成する機能を担っています。これらのシステムは、不審かつ不正なログイン試行だけでなく、機密情報へのアクセスや、CRMからの連絡先情報ダウンロードを試みるなど、ログイン後の不審な活動についても検出します。

Oktaはこれらのシステムと連携し、脅威が疑われたり特定された場合、ユーザーに追加の認証を求め、不審な活動の調査が完了するまでアカウントを一時停止するといったアクションを、即時かつ確実に実施できるようにします。

これらの対応は、企業の選択に応じて、半自動、または全自動のワークフローの一環として組み込むことができます。どちらの方法をとる場合でも、Oktaは、ユーザーにとって使いやすく、組み込みが容易で、自動化レベルや対象とするインシデント対応の種類を柔軟に設定できます。

Oktaによるセキュリティ対応の自動化

Oktaのセキュリティパートナーエコシステムは広がり続けており、アナリティクスシステム、セキュリティオーケストレーション、ファイアウォール、VPN、クラウドアクセスセキュリティブローカ（CASB）とも連携しています。既存セキュリティインフラストラクチャを構成する各要素では、応答を自動化する経路がそれぞれ異なっています。Oktaは、それらのワークフローすべてとシームレスに連携できます。既存インフラストラクチャの一部であっても連携は可能です。

悪意のユーザーをブロックする方法は数多くあります。Oktaは、1つの方法のみを採用するわけではありません。ワークフロー、自動対応のレベル、ソフトウェアの種類、ソフトウェアプロバイダの選択後、それらと連携して機能します。Oktaでは、実現する自動化レベル、連携するパートナー、やり取りを行うセキュリティシステムの種類を柔軟に選択できます。

セキュリティシステムが不審なユーザーを検出した場合、Oktaは任意の数のポリシーを適用できます。たとえば、ユーザーに最初から認証をやり直すよう求めることから、ユーザーのアクセスを一時停止するということまで可能です。これは自動もしくはセキュリティアナリストからの指示で行うことができます。Oktaは、既存のセキュリティインフラストラクチャと統合して、より迅速かつ効率的なセキュリティポリシーの適用を実現します。

Oktaの詳しい活用例をいくつかご紹介します。

1. アナリティクスシステム

多くの組織が、IBM Qradar、Preempt、Splunk、Sumo Logicなどのセキュリティアナリティクスエンジンを使って、セキュリティアラートの管理や確認を行っています。Oktaはこれらのアナリティクスエンジンを統合して、アイデンティティベースの潜在的な脅威イベントを検出し、検出したイベントをセキュリティアナリストが詳細に調査できるようにルーティングします。

セキュリティアナリストが適切な対応を選択した後、サイクルを完了しOktaに通知し、Oktaはユーザーへのステップアップ認証の強制、ユーザーアクセスの一時停止といったアクションを実施します。

Oktaはアナリティクスシステムと連携して、ITおよびセキュリティインフラストラクチャ全体のデータの収集、監視、解析、および分析を行います。

これには、ファイアウォール、VPN、クラウドベースのアプリケーション、他のハードウェアやソフトウェアからのデータが含まれます。

Oktaとアナリティクスシステムは連携し、セキュリティエコシステム全体の関連データすべてを集約して相互に関連付けることで、ネットワーク上の不審な活動をより正確に把握し、承認された担当者に直接アラートします。

2. セキュリティのワークフローとオーケストレーション

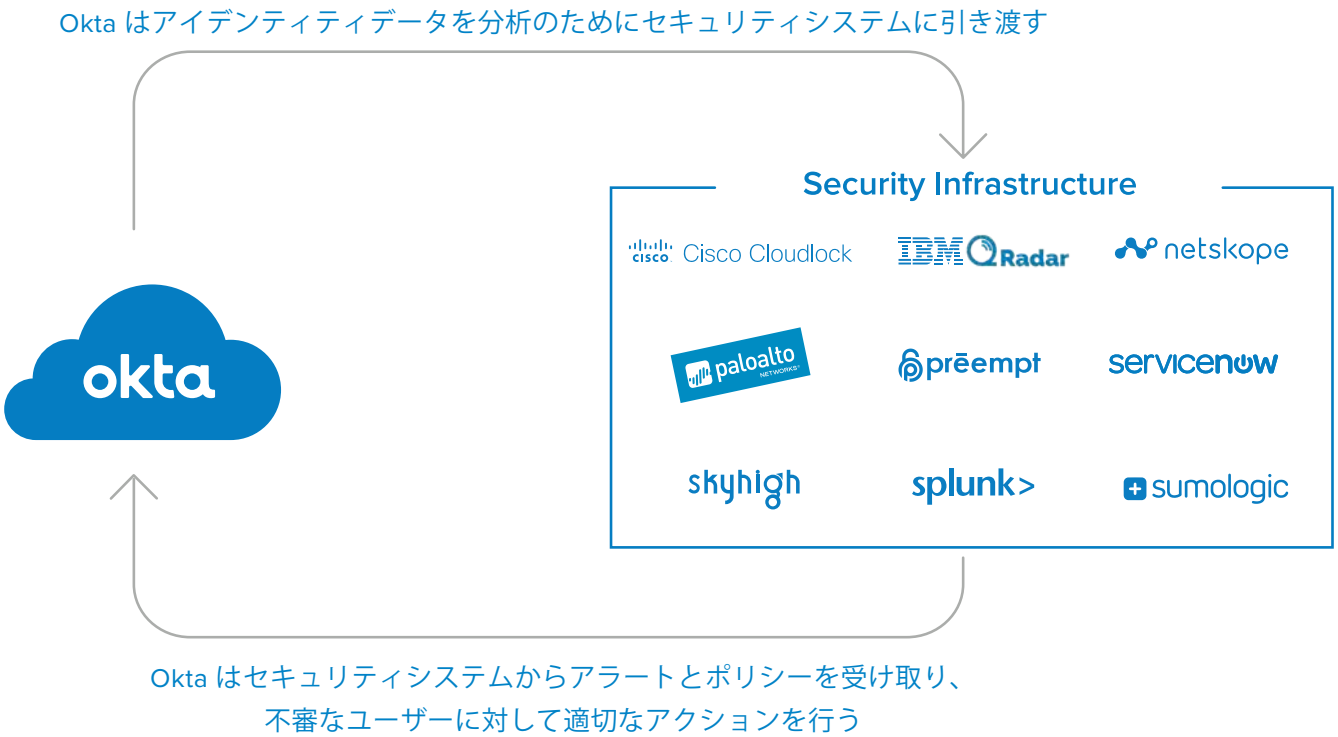
Oktaは、ServiceNowなどのワークフローオーケストレーションツールと連携し、インシデント対応をより効率的に行います。アナリティクスエンジンで不審な活動が特定されると、ServiceNowはそのアラートを受け取り、セキュリティアナリストに送信します。セキュリティアナリストは、ServiceNowに戻ってOktaのセキュリティポリシーを適用します。インシデント対応は、必要な自動化レベルに応じてカスタマイズできるため、企業のアプリケーションやサービスをアイデンティティレイヤーで戦略的に保護できます。

同様に、Palo Alto Networksのようなセキュリティプラットフォームを使って脅威を検出している場合、このシステムとの統合により、ユーザーが企業ネットワークにアクセスした時点でOktaにアラートを送信できます。Cisco Cloudlock、Netskope、SkyHighなどのCASBでコンテンツやコラボレーションシステムからの全ファイルのダウンロードなどの不審な活動を検出している場合も、Oktaにアラートを送信してアクションを実行できます。

これらのシナリオで、Oktaは不審なユーザーをセキュリティ強化グループに移し、すべてのセッションの終了、ユーザーへの再ログインの強制、多要素認証のチャレンジを強制、ポリシーに定めるその他のアクションの実行、といった1つまたは複数のネイティブアクションをトリガーします。

これらのセキュリティポリシーは、Oktaと直接通信するセキュリティシステムを使って自動で適用することも、アラートを送信したうえでOktaを使ってポリシーを適用してもらうこともできます。

Oktaを既存のセキュリティインフラストラクチャに統合することで、アイデンティティレイヤーでセキュリティポリシーを迅速に適用したり、全面的に自動化したりする機能が格段に強化されます。



Oktaを既存のインフラストラクチャに組み込むメリット

既存のセキュリティインフラストラクチャにOktaを組み込むと、次のようなメリットが得られます。

1. ユーザーのコンテキストに基づいたセキュリティレイヤーを追加できる
2. アイデンティティデータをセキュリティアナリストに提供できる
3. 効率的なセキュリティワークフローを実現できる
4. インシデント対応を自動化できる
5. ユーザーの再認証からアクセスの一時停止まで、多岐にわたるポリシーベースのセキュリティアクションを実行できる

システムをアイデンティティのレベルから保護

今日のセキュリティ攻撃の多くは、盗難または漏えいした資格情報を悪用して企業システムをハッキングするという手口によるものです。

Oktaはさまざまなセキュリティパートナーと簡単に連携できるため、強力なツールを利用し、このような脅威に迅速かつ効果的に対応できます。

Oktaをセキュリティインフラストラクチャに組み込むことで、不審なユーザーに対してポリシーを適用。脅威を知らせるアラートのセキュリティアナリストへの送信やポリシーベースの対応の自動化により、攻撃をその場で阻止することができます。

Oktaパートナーエコシステム

Oktaは有力なセキュリティパートナー各社と連携しており、そのエコシステムは拡大と進化を続け、包括的かつ効果的なセキュリティをあらゆる企業に提供しています。Oktaは、セキュリティ環境で重要な役割を果たす主要なソリューションとの連携が可能であり、アイデンティティレイヤーでのセキュリティ対応の高速化や自動化を実現しています。以下は、パートナーの一例です。

Cisco Cloudlock
IBM QRadar
netskope
paloalto NETWORKS
preempt
servicenow
skyhigh
splunk>
sumologic

アイデンティティは、新たなセキュリティ境界です。Oktaの役割は、その境界をセキュアに保つことです。

Oktaは、既存のセキュリティインフラストラクチャと統合することができます。アイデンティティデータやアイデンティティレベルの脅威への対策により、セキュリティ体制を強化するご支援をいたします。Oktaにお問い合わせください。

Oktaについて

Oktaは、社員、顧客、パートナーのアイデンティティとアクセスを安全に管理するベンダーニュートラルなサービスプロバイダーです。Oktaが提供するプラットフォーム「Okta Identity Cloud」により、クラウド、オンプレミスを問わず、適切な人に適切なテクノロジーを適切なタイミングで安全に利用できるようにします。6,500以上のアプリケーションとの事前統合が完了している「Okta Integration Network」を活用して、お客様は簡単かつ迅速にビジネスで必要とするアプリケーションを設定できます。JetBlue、Nordstrom、Slack、Teach for America、Twilioを含む8,950以上のお客様がOktaを活用して、社員、顧客、パートナーのアイデンティティを保護しています。

Oktaの Webサイト:
http://www.okta.com/jp/

Oktaのブログを購読:
http://www.okta.com/blog

Oktaを Twitter でフォロー:
www.twitter.com/okta