Paidyはマルチクラウドの可視性のためにOrca Securityに信頼をおき、クラウドセキュリティ管理コストで2つのFTEと年間50万ドルを節約しています。



所在地
東京

業界
金融サービス

クラウド環境
AWS、Azure、GCP

「Paidyには12のAWSアカウントがあります。各アカウントの内容は不明でした。Orcaに接続することで、各アカウントで実行されているものが30分以内に把握することができました。こういった迅速な解決法は他にはないでしょう。



Jeremy Turner
シニア クラウド セキュリティ エンジニア
Paidy

クラウドセキュリティの課題

- 何百人ものデベロッパーにとって、複数のクラウドでマイクロサービスを数十のアカウントにプッシュし、クラウドエステート内ですべてのアセットを追跡し保護することは困難となっています。
- 自社でソリューションを構築するコストは年間で2つのFTEが最低かかり、その後、維持するために年間50万ドルかかります。
- PIIを積極的に保護し、越境プライバシールールや個人情報保護法などの日本の規制への遵守が課題。

クラウドセキュリティの結果

- クラウドエステートの可視性を取得するまでに30分かかりました。「差し迫った危機」を特定したOrca Securityに、12のAWSアカウントを接続しました。
- 面倒なクラウドセキュリティ作業を年間50万ドル削減
- PIIを特定して保護できることを監査人に証明可能
- 加盟店への迅速な導入が収益の増加を実現

Paidy -クラウドにおける日本の金融機関

Paidyは、日本のマスマーケットや企業にカードレス決済などの金融サービスを届けるフィンテックのリーダーです。そのソリューションは、革新的なオンラインとモバイル決済、P2P送金、個人ファイナンス、マーチャント決済の最前線にあります。Paidyを使用すると、ユーザーはメールアドレスと携帯電話番号だけを使用してチェックアウトできます。クレジットカードや事前登録は不要です。詐欺を防ぐために、SMS経由でPINを使用してすべてのトランザクションが認証されます。ユーザーは今すぐ購入し、翌月に一括して支払うことができます。

Paidyのプラットフォーム全体はクラウドで実行されます。主に複数のAWSアカウントですが、AzureとGCPもあります。複数のテストと開発環境があります。プラットフォームが金融取引を処理する場合、セキュリティは一番の懸念事項です。CISOのFelix Beatty氏は、Paidyの全体的なセキュリティポスチャーの最適化を担当しています。

「当社は基本的にクラウド内の金融機関です」とBeatty氏は述べています。「当社は急速に成長し、1年以内に300万人以上の顧客を獲得しました。さらに改善できるビジネスの領域があり、クラウドセキュリティもその一部です。ほとんどのサービスは今日クラウドで実行されているため、迅速に解決できるようには、重要な問題をすぐに表面化できるクラウドセキュリティソリューションが必要です。



「エージェントはLinuxカーネルでは機能しないかもしれません。Windowsのバージョンでも同様です。いろいろな要素が絡み合っています。エージェントに数年対処した後、Orcaをインストールして使用するのがどれほど簡単か分かり、エージェントレスのアプローチは主要なイノベーションであり、ゲームチェンジャーであることが分かりました」と、Turner氏は述べています。

Jeremy Turner
Paidy シニアクラウドセキュリティエンジニア

Paidyの大規模なクラウド環境では、全体にわたる可視性が課題になります

Paidyプラットフォームですべてのものを可視化することは、最大の課題の1つです。「当社には大きく複雑なクラウド環境があります。こうした動的なアセットを、すべて管理することは困難です」とBeatty氏は述べています。「何百人ものデベロッパーが、可能な限り速くマイクロサービスをクラウドにプッシュし、インスタンスを上下にスピンし、バックアップの作成、S3バケットの作成、高速で移動するため、今現在何があるのか知ることは非常に難しいのです。「当社のクラウドアセット全てのセキュリティポスチャーは何であるか？」を知る必要があります。

シニアクラウドセキュリティエンジニアのJeremy Turner氏は、Beatty氏の右腕としてクラウド環境のセキュリティを確保しています。Paidy入社以前から二人はチームを組み、セキュリティの課題にアプローチする方法を理解しています。

機能する場合は、セキュリティエージェントは素晴らしいものですが、通常はそうなりません

「長い間この問題に取り組んできました」「セキュリティと脆弱性に対処するものは通常、エージェントをインストールする必要があることを学びました。しばらく情報セキュリティで働けば、エージェントが壊れていることが分かります。エージェントを更新する必要があり、それが他のセキュリティ脆弱性へのベクトルになる可能性があります。」

Turner氏は、機能してくれている限りはエージェントが素晴らしいことを認めています。「通常、エージェントはそうではありません。依存関係など、考えるべきことがあります。エージェントはLinuxカーネルでは機能しないかもしれません。Windowsのバージョンでも同じです。いろいろな要素が絡み合っています。エージェントに数年対処した後、Orcaをインストールして使用するのがどれほど簡単か分かりました。エージェントレスのアプローチは主要なイノベーションであり、ゲームチェンジャーです。



レガシーの脆弱性スキャナとAWSツールは適していません。

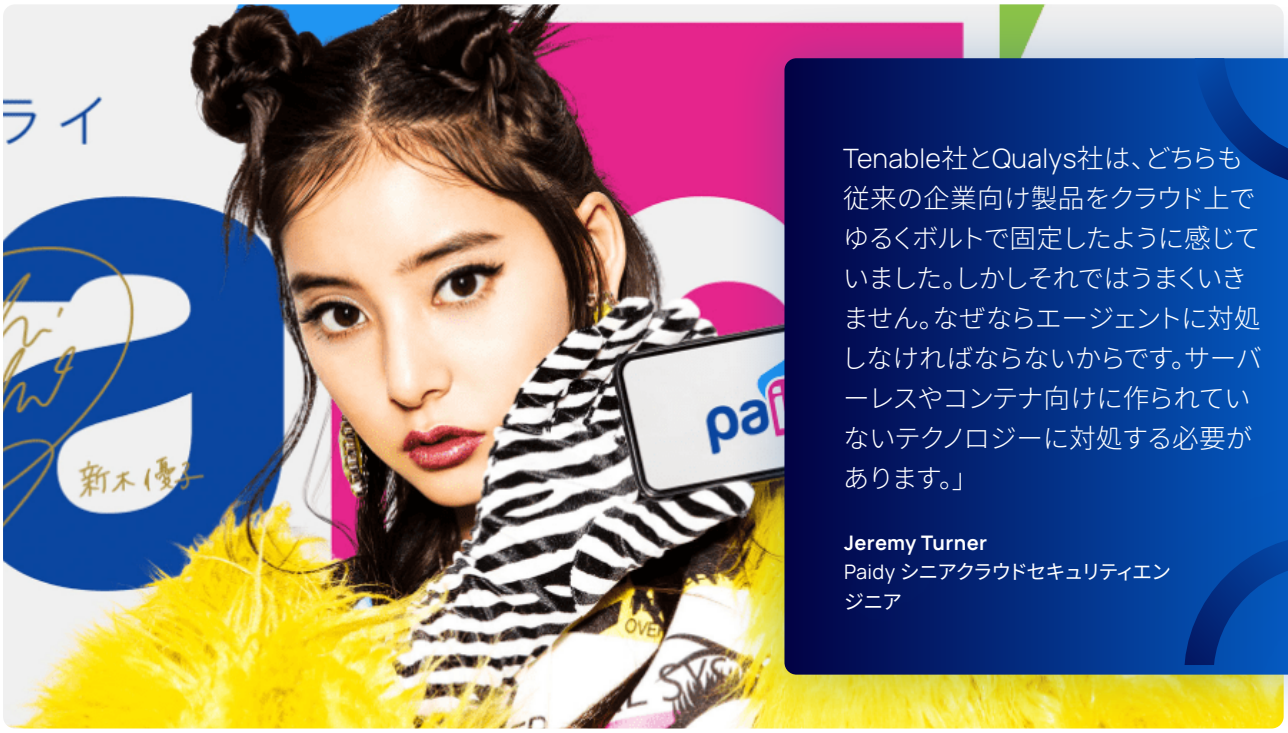
Paidyセキュリティチームには、クラウドに適応したさまざまなレガシーツールの経験がありました。Turner氏はこう言います。「企業環境またはテストにおいて、Trend Micro、Qualys、Tenableを使用してきました。Tenable社とQualys社は、どちらも従来の企業向け製品をクラウド上でゆるくボルトで固定したように感じていました。しかしそれではうまくいきません。なぜならエージェントに対処しなければならないからです。サーバーレスやコンテナ向けに作られていないテクノロジーに対処する必要があります。」

Paidyは、ネットワークスキャナを使用することを排除しました。Turner氏によれば、「認証されていないスキャナーとの経験があるので、可視性が限られており、ダウンタイムを作成できることは知っていました。

「認証済みスキャナは、より多くの脆弱性データを提供するかもしれませんが、設定し、そして権限を昇格させる多くの作業が必要です。これにより、エンタープライズはリスクが発生します。なぜなら、別の共有アカウントとパスワードが基本的にあるからです。」

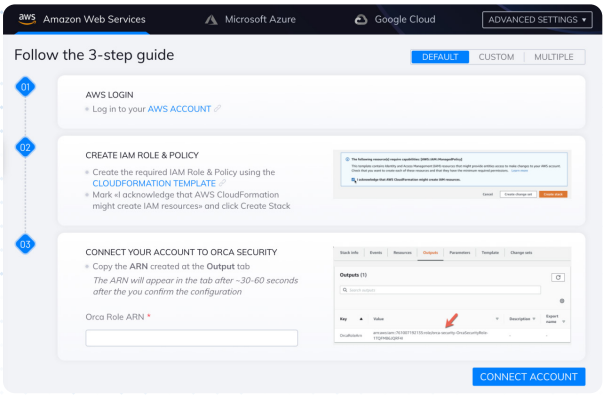
Amazonなどのクラウドプロバイダは、セキュリティスキャンツールを提供します。「脆弱性スキャナであるAmazonのAWS Inspectorはエージェントが必要です。通常、Amazon AMIに入っていますが、特定のAMIのみで機能します」「AWS GuardDutyは、脆弱性スキャンとコンプライアンスチェックをチェックします。しかし、報告は最大の問題です。データを使用することは困難である場合があります。脆弱性の一覧をポップアウトすると、それらについて何をすべきか理解することは私たち次第です。」

Beatty氏によると、「複数のAWSアカウントがあり、マルチクラウドであるため、生じていることすべてを監視できる単一のビューを持つことは困難でした。マルチクラウドの可視性は、当社において一番の問題でした。第二に、例えばAWSサービスや類似ものを使用して、ツールを調整する



> Tenable社とQualys社は、どちらも従来の企業向け製品をクラウド上でゆるくボルトで固定したように感じていました。しかしそれではうまくいきません。なぜならエージェントに対処しなければならないからです。サーバーレスやコンテナ向けに作られていないテクノロジーに対処する必要があります。」
>
> **Jeremy Turner**
> Paidy シニアクラウドセキュリティエンジニア

時間とリソースがありません。エージェントを必要としないサービスを使用したいのです - 定期的に更新する必要がなく、単に機能する場所です。」Paidyでは、Orca Securityがこれらのニーズなどすべてを満たします。



Orca SideScanning™は、必要な可視性を提供

Orca Securityプラットフォームは、他のセキュリティツールとは大きく異なります。SaaSとして提供され、側面からクラウドブロックストレージを帯域外から読み取ります。したがって、SideScanning™とよばれます。お客様のクラウド環境内ではコードは実行されません。代わりに、Orcaはクラウド環境の読み取り専用モデルを構築し、その後潜在的なセキュリティ問題を評価するためにスキャンします。

完全な可視性を持つことは、Turner氏が最も高く評価していることです。「可視性は、すべての組織が抱えている問題です。Orcaは、脅威の状況を広く深く迅速に見通すことができました。」とTurner氏は述べています。「データを取り出し表示すると人々の目が覚めます。Orcaは、おそらく2～3年前からテスト環境で存在していた、システムの「差し迫った危機」を表面化したという事例がありました。

システムは、完全に旧式のOSを実行していました。Orcaがこのことを特定すると、エンジニアがすぐに対処するチケットを作成しました。システムがUATと生産に入る前に、脆弱性を検出できたことは幸運でした。」

Beatty氏は、可視性という価値に同意しています。「目の前にある問題を見落とすことはありません。Orcaのダッシュボードが「差し迫った危険」と表示する以上に明確なものはありません。」

Orcaはアカウントのスプロールの問題でもPaidyに役に立っています。「12のAWSアカウントを実行しています」とTurner氏は述べています。各アカウント内容は不明でした。Orcaにプラグインすることで、各アカウントで実行されているものが30分以内で表面化できました。こういった迅速な解決法は他にはないでしょう。

アセット管理は、OcraがPaidyに提供するもう一つの機能です。Orcaは、各アセットの場所、メタデータ、脆弱性リストのインベントリを提供します。「インスタンスを選び、誰がログインしているか、ログインに失敗した試みがどれほどあり、またはその上にインストールされているパッケージを見ることができることは最高です。すべてのインスタンスごとにエージェントに依存せず、これを実行できることに感謝しています」とTurner氏は述べています。

Orca Securityは、PIIを特定して保護し、Paidyのコンプライアンスへの取り組みを緩和します

Paidyは、Orca Securityプラットフォームでより多くの経験を得るにつれて、チームは生成するデータを使用するより多くの方法を見つけています。「フィンテック企業として、データの害を及ぼす組み合わせに大変気を払っていますが、Orcaはこれを支援してくれます」とTurner氏は述べています。「たとえば、サービスを使用する際に、ユーザーは携帯電話番号を入力しなければなりません。しかし、銀行口座情報と購入履歴を組み合わせたホームページアドレスまたはメールアドレスを取り扱う場合、PIIの問題と日本のデータプライバシー規制に足を踏み入れることになります。」

Turner氏はOrcaがPIIを保護する方法を説明しています。OrcaがPIIを疑っているかどうかを知ることができます。「このサーバーにはpaidy.comに属していないメールアドレスが含まれています。何が起こっていますか？」というビーコンのようなものです。これに基づいて問題について調査できます。今のところ、ツールは「ここに有害なデータの組み合わせがあります」とは言えませんが、どこを探せばよいかを示してくれます。データサイエンスチームがデータベース結合を作成し、データの組み合わせがこのように有毒になったという状況がありました。Orcaのおかげで未然に防ぐことができました。」

Paidyは、多くのデータプライバシー法を遵守しなければなりません。日本の越境プライバシールールは、EUのGDPRに類似しており、2004年に個人情報保護法が成立しました。Orcaは、Paidyが個人情報を完全に特定して暗号化できることを監査人に証明しています。Paidyは、脆弱なPIIをスキャンする機能があることを簡単に知ることができます。

Turner氏は、JiraとのOrca Securityの統合を利用してチケットを開きます。そしてこれはワークフローのトリガーとなり、人やプロセスが適切な措置を取ることができます。例えば、機密データを暗号化したり、あるいはOrcaが見つけた他の問題を修正したりすることです。



Orca Securityについて

Orca Securityは、特許出願中のSideScanning™テクノロジーを活用し、AWS、Azure、GCP向けにクラウド全体のワークロードのディープなセキュリティとコンプライアンスを提供します。クラウドプロバイダへ読み取り専用及び影響のない統合を瞬時に行った後、Orca Securityは脆弱性、マルウェア、設定の誤り、横方向の動きのリスク、認証のリスク、安全ではない高リスクデータを検出し、エージェントをデプロイせずに根本的な問題、アクセス可能性、ブラスト半径に基づいてリスクを優先させます。

最初のクラウドアカウントに数分で接続し、
ご自身の目でお確かめください：orca.securityを見る

© Copyright Orca Security 2021この資料で参照されているすべての商標、サービスマーク、商号はそれぞれの所有者に帰属します。