WHITEPAPER

RapidMiner SaaS
Platform Security

RAPIDMINER

RAPIDMINER

目次

概要

RapidMinerのクラウドプラットフォームは、多様な分析チームが企業全体で強力なAIソリューションを作成、デプロイ、スケールできるように構築されました。しかし、それを行う前には、データが完全に自身のコントロール下にあり、認証されていないグループがそれらにアクセスしたり、関与することがないよう、適切な管理が確立されている必要があることを私たちは認識しています。

この資料では、RapidMinerのインフラが最高水準のエンタープライズセキュリティの維持にどのように役立っているかを詳しく見ていきます。**マルチテナントセキュリティ、ユーザーレベルセキュリティ、インフラストラクチャセキュリティ**、そして顧客のデータ管理に対する私たち自身のポリシーにより、お客様がガバナンスとコンプライアンスに気を取られる時間を減らし、データからアクション可能な知見を得る時間を増やす方法を探っていきます。

「過去五年間で、主にIoTによって利用可能なデータ量が急激に増加しただけでなく、この生データの洪水を知見に変え、最終的にはアクションに変える新しいツールが開発されてきました。」

– ACHIEVING BUSINESS IMPACT WITH DATA,
マッキンゼー・アンド・カンパニー

マルチテナント セキュリティ – テナントの分離

RapidMinerのクラウドプラットフォームはマルチテナントサービスであり、これは共通のプラットフォームをすべての顧客に対してグローバルにサービスを提供することを意味します。このアプローチは外部アプリケーションとの統合も容易にし、環境のメンテナンスの負担を軽減し、私たちの競争力の維持に繋がります。しかし、当然のことながら、企業の管理者は外部ベンダーにコントロールを委ねることに懸念を抱くでしょう。自身の組織だけがデータやプロジェクトを利用できることを保証することが、それらの懸念に対処する最初のステップです。

テナントは以下の三つの重要な方法で完全に分離されています。

- **データの分離**: 各ユーザーのデータは個別に保存されています。認可システムは企業や権限を基にユーザーにアクセスを許可します。テナントが所有しているデータは、作成した企業に属していないユーザーに見えたり、共有されることはありません。逆に言うと、外部テナントが所有しているデータへは、どんな手段であれ干渉することはできません。また、すべてのデータファイルはテナントごとにユニークなキーで暗号化されています。
- **プロジェクトの分離**: 同様に、RapidMinerの認可システムは、テナント外のユーザーによるプロジェクトへのアクセスを完全にブロックします。これには、データやモデル、アプリ、その他ユースケース固有のあらゆるコンテンツが含まれます。

- **実行レイヤー (Kubernetes)**: RapidMinerのワークフローの実行はKubernetesのPod内部で行われます。各Podは一つのワークフローの実行に対して生成され、その後は速やかに停止、削除されます。そのため、(テナント内外の)ワークフロー間で操作が交わることはありません。

インフラストラクチャ セキュリティ

クラウドでは、セキュリティメカニズムのほとんどが裏側にあります。RapidMinerでは顧客に力を与えるインフラストラクチャのバックエンドが完全にセキュアであることを保証するために、詳細な手順を踏んでいます。バックエンドのセキュリティを保証する、主な策が以下です。

- **Webアプリケーションファイアウォール**: 厳しく設定されているWebアプリケーションのファイアウォールが、クロスサイトスクリプティング(XSS)やSQLインジェクションなどの、既知のほとんどの攻撃からすべてのアプリケーションコンポーネントを保護します。
- **サイト証明書**: 私たちのすべてのhttpsエンドポイントには、セキュアな通信を保証するためにサイト証明書が含まれています。
- **踏み台ホスト**: 私たちの管理者でさえ、ログインしてインフラから直接作業することはできません。すべてのアクセスは、特に厳重な踏み台ホストを通して行われます。
- **脆弱性スキャン**: 私たちは定期的な脆弱性スキャンを行い、サードパーティのライブラリからもたらされる潜在的なリスクを検出し、できるだけ早く修正するようにしています。
- **ペネトレーションテスト**: ペネトレーションテストが外部企業によって定期的に行われ、リスクの発見やリスクの軽減を行っています。テストの完了後は、発見された事項をすぐに修正するための標準的な手順を実行しています。
- **災害復旧**: 最終的な保障として、バックアップが定期的に作成され、保管されています。プラットフォーム全体はplatform-as-codeパラダイムを基にしているため、大規模な、そしてめったに起こらない世界的な障害や攻撃のなかでも、すぐに復旧できるようになっています。

ユーザーレベル セキュリティ

RapidMinerのクラウドプラットフォームのユーザーレベルセキュリティは、次の三層で構成されたフレームワークを基にしています: **認証**(ユーザー本人であることの確認)、**認可**(ユーザーが閲覧できるデータとプロジェクトの決定)、**暗号化**(承認されたユーザーにのみデータが使用できるようにする)。

データセキュリティ実装モデル

認証

認証レイヤーでは、ユーザー本人であることを確認することで、ログインの安全性を確保します。RapidMinerでは、認証はアクセス管理ツールの業界リーダーであるKeycloakで管理されます。

RapidMinerの推奨は、ユーザー認証を自身の組織でのアイデンティティプロバイダ(IdP)と統合することです。RapidMinerはLDAPやSAML、OAuthのような標準的なプロトコルを使用したあらゆるIdPとの統合をサポートしています。二要素認証(2FA)や多要素認証(MFA)、パスワードの複雑性に関する要件やポリシーなど、最先端の認証機能もサポートされています。

認可

RapidMinerの認可モデルは、常にセキュリティ制約を気にしながら、コラボレーションの促進に目を向けています。

データレベル

RapidMinerのデータカタログ(ユーザーがデータセットを追加したり、外部データとの接続を作成できる場所)に保存されているすべてのデータセットは、独立した権限を持ちます。データの所有者が、完全な読み込み・書き込み権限を持つ人、内容を閲覧のみできる人、存在すらわからない人を決めることができます。これにより、自身の会社やユースケースごとの必要性に応じて、各データセットはコラボレーションのために共有することも、完全に隠すこともできます。

プロジェクトレベル

プロジェクトには、モデルやワークフロー、コード、自動分析の結果など、データ分析のためにユーザーが作成したすべてのものが含まれます。プロジェクトの所有者は、プロジェクトに誰が参加できるかを決めます。参加者は追加や編集ができ、一般的には、与えられたユースケースに対して解決策を考えるために一緒に作業を行います。

またプロジェクトの所有者は、ユースケースを閲覧する必要はありますが、データパイプラインの作成やモデルの作成には積極的に参加しないユーザーに対して、閲覧のみの権限を付与することもできます

RapidMinerの認可システムでは、外部のユーザーはどのような方法であれプロジェクトに対してアクセスや変更ができないことを保証しています。

本番環境で、RapidMinerの管理者は各ユーザーにジョブの実行やスケジューリングを許可する特別な権限を割り当てることができます。

暗号化

暗号化の目的は、停止時も稼働中もデータのプライバシーを保証することです。暗号化されたデータは復号キーなしにアクセスすることはできません。

RapidMinerはデータ保管のバックエンドにAmazon S3を使用しています。AES-256アルゴリズムを使用して、停止時のS3の暗号化が行われています。データがネットワーク上を移動する際は、データの保護にTLS(Transport Layer Security)が使用されています。

RapidMinerセキュリティポリシー

プラットフォームレベルのすべての対策に加えて、RapidMinerでは以下の内部セキュリティ制約やポリシーに従うことをお約束します。私たちは、セキュリティがたゆまぬ努力のたまものであり、製品開発から運用、セールスまで、組織全体に根付かせる必要があることを理解しています。セキュリティは常に開発プロセスの早い段階で考慮され、すべての開発プロセスの一部であり、システムの監視や運用においても重要なものです。

またRapidMinerでは、企業のリーダー、財務、製品、エンジニアチームのメンバーからなるセキュリティ協議会を設置し、すべてのセキュリティポリシーが守られているか監視しています。これにより、組織の規範が各部署で守られ、従業員一人一人が顧客の機密情報保護に対する役割を認識するようにしています。

コンプライアンス

RapidMinerのセキュリティはSOC IIに準拠しています。プライバシーや処理の完全性のようなカテゴリに対して、独立したサードパーティの監査役によってテストされ、認定を受けたSOC IIのポリシーや規制を実装しています。これは、私たちのポリシーや基準が経験豊富な外部組織に検証されるだけでなく、それらを保つ私たちの能力も検証されることを意味しています。

またRapidMinerはヨーロッパユーザーのためにGDPRの要件にも準拠しています。

インシデント管理

RapidMinerには、セキュリティインシデントを公表し、対応するプロセスをまとめた、セキュリティインシデント管理プランがあります。このプランには、役割や責任、万が一問題が発生した際に解決策を作るのに必要な内部と外部のコミュニケーションなどが含まれています。

ポリシーのアップグレード

RapidMinerプラットフォームの全てのソフトウェア要素は、最新のセキュリティパッチに継続的にアップグレードされていきます(OSライブラリ、ソフトウェアの依存関係、ミドルウェア、ソフトウェアなど)。

内部ロギングと監査

RapidMinerのスタッフには、プラットフォームのアクセスを管理する厳しいルールがあり、必要なメンテナンス操作に制限されています。ユーザーデータへのアクセスは、サポートインシデント内のユーザーによる**明確なリクエストがない限り、許可されていません。** RapidMinerのクラウド内での管理者の行動は、後の監査のためにすべて記録されます。

まとめ

RapidMinerでは、クラウドプラットフォーム内の顧客のデータを保護するために、プラットフォーム内と、セキュリティに対する社内での強力なカルチャーの両方を通じて、包括的な対策を行っています。

マルチテナントのセキュリティは、セキュリティを犠牲にすることなく、ベンダーにインフラを任せる利益を得ながら、自身の組織のデータやプロジェクトへのアクセスが完全に自身のコントロール下にあることを保証します。

ペネトレーションテストや脆弱性のスキャン、災害復旧プロトコルにより、私たちのバックエンドが完全にセキュアで、信頼に値するものだと信じていただけたと思います。

ユーザーレベルのセキュリティにより、プラットフォーム全体からデータセットレベルまで、コンテンツに誰がアクセスできるのか完全にコントロールすることができます。またデータは暗号化され、追跡も容易です。

最後に、RapidMinerの内部セキュリティポリシーは、独立した監査人によってテストされ、SOC IIに準拠していることが認定されました。これは、お客様が自由にイノベーションを起こし、自身のビジネスのやり方を変えられるよう、エンタープライズセキュリティにおける最高水準の維持に、私たちが信頼できる存在であることを意味しています。

主な機能

クラウド

- テナントの分離（データ、プロジェクト、実行）

認証

- 二段階認証(2FA)
- SAML認証サポート
- OAuth 2.0 サポート

認可

- シングルファイルによるきめ細かな認証
- プロジェクトベースの認可

データの保護

- TLS（Transport Layer Security）サポート
- LDAPプロパティの暗号化
- 休止時の暗号化

インフラストラクチャ

- 堅牢なバックエンドインフラ
- 継続的なシステムアップグレード（ユーザーは特に操作不要）

ポリシー

- SOC II準拠
- GDPR準拠

RAPIDMINER

変革のペースを加速させたい企業にとって、RapidMinerは競争優位性を突き抜けるための人材、専門知識、データを集めたインパクトを増強する、エンタープライズ対応のデータサイエンスプラットフォームです。RapidMinerのデータサイエンスプラットフォームは、全AIライフサイクルに関わるすべてのユーザーをサポートしています。RapidMiner AcademyとCoE(Center of Excellence)メソロジーは、顧客の経験やリソースのレベルにかかわらず、顧客の成功を保証します。2007年以降、150か国で100万人以上の専門家と40,000以上の組織が、RapidMinerを使用してデータサイエンスを自身のビジネスに近づけています。