ファイルおよびリンクベースのサイバー脅威から Agentforce のワークフローを保護

ファイルや URL、チャットに潜むマルウェアやフィッシングの脅威からユーザーを保護する WithSecure™ Cloud Protection for Salesforce が、Agentforce の AI エージェントのワークフローにも対応しました

Agentforce は高速に動作するため、セキュリティはそれ以上の速度で動かなければなりません

Salesforce Agentforce は、組織と顧客の関わり方を変革しつつあります。AI エージェントは会話の処理やファイルの取得、ワークフローの自動化を驚異的な速さで行いますが、その速さ自体が新たなセキュリティ上の盲点を生み出し、脅威となります。

Agentforce によって共有されるファイルやリンク、あるいはチャットコンテンツは、デフォルトではスキャンされません。つまり、フィッシングリンクやマルウェアがポータルやフォーム、あるいは Slack や WhatsApp などの連携ツールをすり抜けてしまい、従来型のセキュリティツールがそれらを見つけて処理する前に拡散してしまう可能性があるのです。

WithSecure™ Cloud Protection が、この問題を解決します

WithSecure™ Cloud Protection は、Salesforce にネイティブ実装された唯一のリアルタイムソリューションであり、Agentforce ワークフロー内でファイルや URL がアップロード、取得、またはクリックされた瞬間にスキャンを実行し、ユーザーやシステムに脅威が到達する前にそれを阻止します。

Agentforce は、顧客体験の拡大を支援します。ウィズセキュアは、その拡大を安全に行えるよう支援します。

WITH secure

どのように自律型 AI を守るのか

エージェントが動く速度でリアルタイムに保護
AI エージェントは秒単位で動作するため、防御システムも同じ速度で動く必要があります。ファイルと URL が即座にスキャンされるため、脅威が拡散する前に阻止できます。

Salesforce ネイティブ、拡張できる設計
100% Salesforce ネイティブです。外部へのルーティングやポータルは必要無く、トレードオフも発生しません。Agentforce 拡張機能の利用には追加費用はかかりません。

セキュリティチームのための可視性と制御機能
脅威の行動やシステムの利用状況を監視するための監査ログ、アラート、カスタムダッシュボードを利用できます。

業務を止めず、円滑かつ安全に遂行
エージェントの作業効率を低下させたり、コラボレーションを妨げたりすることなく、ワークフローを保護します。

責任共有モデルと新しい攻撃経路

エージェントは高速で動作します。そして、脅威も同じです。

Agentforce のワークフローは、脅威がすり抜けることのできる新たな経路を作り出します：ユーザーがアップロードしたコンテンツはエージェントによって即座に処理されるため、従来型のセキュリティ対策を経由することなく、従業員や顧客に転送されてしまいます。

エージェントのワークフローは、デフォルトではスキャンされません。

ファイルやリンク、チャットコンテンツは、デフォルトではスキャンされません。また、AI エージェントはフィッシングやマルウェア、不審な行動を認識しません。つまり、悪意のあるコンテンツはマシンレベルの速度で拡散し、瞬く間に広がる可能性があるということです。

データを守るのは、ユーザーの責任です。

責任共有モデルにおいては、Salesforce に出入りするデータのセキュリティを確保するのは、クラウドサービスの顧客であるユーザーの責任です。人間が操作する場合でも、エージェントが操作する場合でも、データがクリーンで安全であり、適切に管理されていることを確認しなければなりません。

保護対策を怠った場合、Agentforce は脅威を高速に拡散するシステムになりかねません。

Agentforce は何を保護し、いつ起動するのか

Agentforce は高速で動作します。画像に隠されたマルウェアや共有フォーム内のフィッシングリンク、あるいは脅威が埋め込まれた古いファイルなどがエージェントによって処理された場合、それらが瞬時に Salesforce 環境全体に拡散する可能性があります。

WithSecure™ Cloud Protection for Salesforce は、脅威がシステムに侵入や移動したり、システムから離脱したりする可能性のある重要なポイントで保護を行うため、システムパフォーマンスを低下させることなく、即座に脅威を検知することができます。

- アップロード時：ポータル、フォーム、接続済みアプリ経由で追加されたファイルと URL
- ダウンロード時：ユーザーがコンテンツをダウンロードした時
- クリック時：アクセス試行時に URL 保護を起動
- エージェントによる取得時：エージェントがファイルまたは URL を取得する際にリアルタイムでスキャン
- アウトバウンドでの利用：エージェントが顧客とコンテンツを共有する前にスキャン
- API および統合ポイント：Slack、WhatsApp、email-to-case などのツールを含む

Salesforce 環境内のすべてのデータがクリーンであることを確認し、人間とエージェント両方のワークフローをカバーすることで、エージェントが動作する速度でセキュリティを維持できるよう支援します。

主な機能

- アップロード、ダウンロード、クリック、エージェントの取得時にファイルと URL をリアルタイムでスキャン
- フォーム、チャット、Slack 連携を含む Agentforce ワークフロー全体に保護を拡張
- マルチエンジン分析とグローバル脅威インテリジェンスによる高度なマルウェア対策
- 行動分析によるゼロデイ攻撃検知のためのサンドボックス機能
- フィッシングリンク、偽装ファイルタイプ、悪意のある QR コードの検知
- ドメインおよび短縮 URL 分析によるクリック時の URL 保護
- パスワードで保護されたアーカイブファイルおよび大容量ファイルのディープスキャン
- Salesforce 標準オブジェクトおよびカスタムオブジェクトの完全サポート
- 環境全体に保存されているコンテンツの自動およびオンデマンドスキャン
- セキュリティを可視化するリアルタイムダッシュボード、監査証跡、カスタマイズ可能なアラート
- 脅威追跡のための Salesforce ネイティブなレポートを標準で装備し、カスタマイズも可能
- イベントおよび検知ログを 24 ヶ月間保持
- 構造化ログの書き出しによる SIEM 連携
- Salesforce 内での完全なデプロイ：外部ポータルやトラフィックのルーティングは不要
- Agentforce 拡張機能が付属：追加費用や複雑な設定は不要
- サンドボックス環境と本番環境の両方に対応
- EU、米国、日本などにおける地域内のデータレジデンシー管理
- Salesforce 内での自動アップデートとメンテナンス不要の運用

エージェント型 AI の仕組みに基づいて Agentforce を保護

AppExchange から入手

Salesforce Agentforce は業務効率を向上させますが、リアルタイムの脅威対策を伴わない場合、リスクも増大させてしまう可能性があります。WithSecure™ Cloud Protection は、ファイルおよびリンク、そしてエージェントが処理するコンテンツがアップロードされ、取得され、外部へ送信される瞬間に、それらをスキャンする唯一の Salesforce ネイティブなソリューションです。ルーティングも遅延もなく、ミドルウェアも不要です。最速のワークフローに、高速でスムーズな保護を提供します。

エージェントが動く速度でセキュリティを確保

AI エージェントは秒単位で動作するため、セキュリティもそれ以上の速度で動く必要があります

- アップロード、ダウンロード、クリック、エージェントによる取得時に、ファイルと URL をリアルタイムでスキャン
- 脅威がユーザーに到達したり、ワークフロー全体に拡散したりする前に検知
- 人間によるワークフローと自動化されたワークフローの両方を、パフォーマンスを低下させることなく保護

シンプル、スケーラブル、そしてシームレス

ストレスが無く管理が容易な、ガバナンスのために構築されたセキュリティです

- 外部へのルーティングやポータルが不要で、クリック操作によってデプロイ可能
- 100% Salesforce ネイティブで、自動アップデートと設定ログを装備
- コンプライアンスと制御のための監査対応ログとリアルタイムの可視性

エージェントが触れるものすべてを信頼できる状態に

エージェントがクリーンで信頼できるデータのみを扱い、フルスピードで動作できるように維持します

- エージェントからのアクセスやエージェントへの引き渡しの前に、すべてのファイル、リンク、QR コードをスキャン
- 画像、アーカイブ、共有コンテンツ内のマルウェアを検知
- 非構造化コンテンツが自動化における盲点にならないように保護

ウィズセキュア株式会社
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.withsecure.com/
2025/11

ウィズセキュア：サイバーセキュリティにおける信頼できるパートナー

ウィズセキュアは、エンドツーエンドのサイバーセキュリティ企業として包括的なサイバーセキュリティサービスを提供し、社内の研究部門と現場での豊富な経験に基づいた深い理解に基づいて、受賞歴のあるセキュリティテクノロジーを開発しています。

認証取得済みで監査対応済み

WithSecure™ Cloud Protection for Salesforce は、最高レベルのパフォーマンスを維持するため、継続的に Salesforce による厳格なセキュリティレビューを受けています。また、お客様のコンプライアンス要件を満たすため、ISO 27001、ISAE 3000 Type 2（SOC2 Type 2 相当）の認証も取得しています。