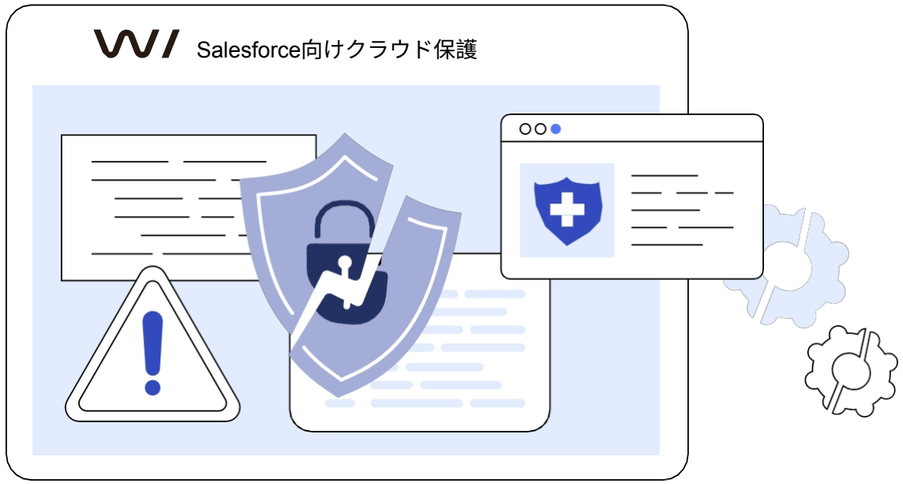
eBook

ヘルスケア・ライフサイエンス業界最新動向



当社のパートナーであるWithSecureが、ヘルスケア・ライフサイエンス業界の課題にどのように取り組んでいるかをご覧ください。業界全体の課題からSalesforce管理者のニーズに至るまで、WithSecureが包括的に対応します。

WithSecure Cloud Protectionは、ISO 27001およびISAE 3000 Type 2の認証を取得したサイバーセキュリティソリューションです。ユーザーに被害を与え、業務を妨害する可能性のあるマルウェア、フィッシング、ゼロデイ脅威からSalesforce環境を保護するように設計されています。

WithSecureが、ヘルスケア・ライフサイエンス業界の組織がSalesforce内のデータ、ユーザー、およびカスタマイズ内容を保護するのを支援する方法を以下にご紹介します。

機密データの保護

マルウェアやフィッシングから組織を守ります。重要なSalesforceデータ、患者記録、デジタルワークフローに対する脅威を、リアルタイムに検知・阻止します。

ゼロデイ攻撃対策の導入

悪用が急速に広がるのを防ぎます。認定済みの検知技術を活用し、既知および未知のマルウェアが拡散する前に阻止します。

事業継続の確保

システムのダウンタイム、調査の遅延、または評判の低下を引き起こすインシデントを軽減することで、業務の継続性と信頼を確立します。

Salesforce 管理者が、ネイティブかつリアルタイムの脅威検知機能を活用してセキュリティ体制を強化する方法を、ぜひご覧ください。

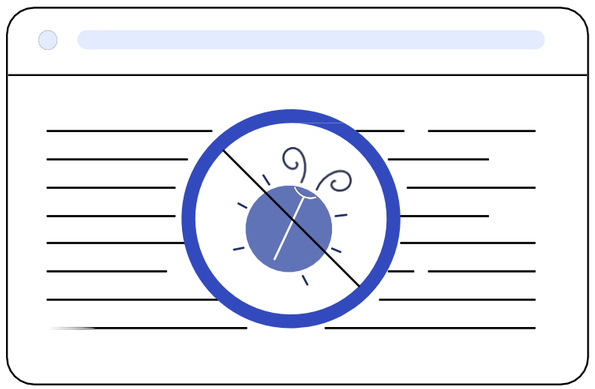
ソリューション

WithSecure Cloud Protectionは、Salesforceプラットフォームにネイティブに統合され、最も必要な場所でリアルタイムの保護を実現します。
これにより、トラフィックの迂回や追加インフラの導入、遅延が発生することはありません。

ファイル経由のマルウェアから保護します。

課題：アップロードされたファイルは、従来のエンドポイントやメールセキュリティを迂回して、CRM環境に直接侵入する可能性があります。このようなマルウェアは、潜伏したままになることもあれば、ダウンロード時にすぐに活性化することもあります。

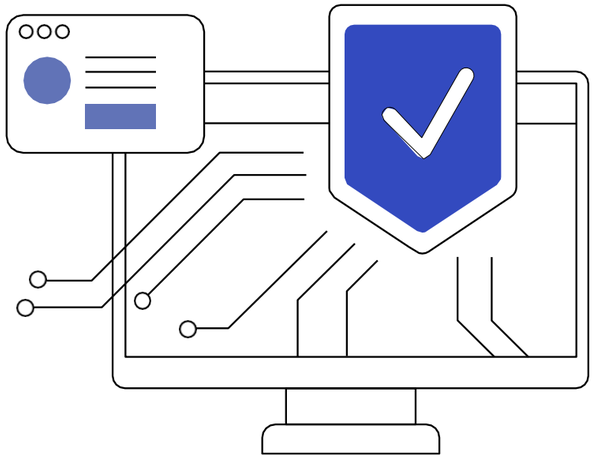
ソリューション：WithSecure Cloud Protectionは、Salesforceを介してアップロードまたはダウンロードされるすべてのファイルをリアルタイムに解析し、受賞歴のある高い検知精度を持つキュリティエンジンで、通常のマルウェアやゼロデイマルウェアを検知・ブロックします。これにより、組織は安心してファイルのアップロードを受け入れ、デジタル患者体験をサポートできます。



フィッシング攻撃がユーザーに届く前に阻止します。

課題：Salesforceユーザーは、フィールド、添付ファイル、またはカスタムオブジェクトに埋め込まれた悪意のあるリンクに騙される可能性があります。

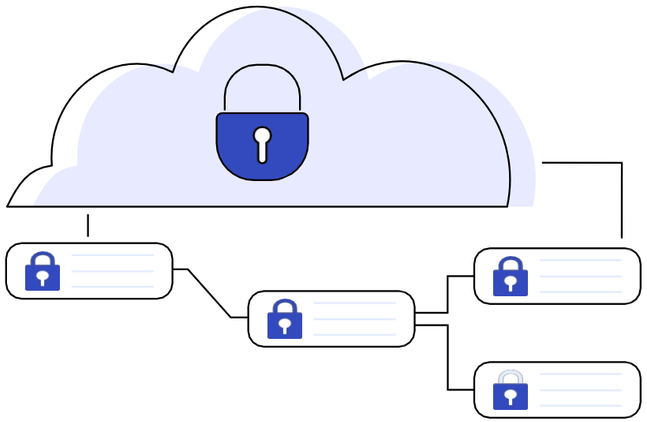
解決策：WithSecure Cloud Protectionは、SalesforceにアップロードされるすべてのurlおよびQRコードをリアルタイムで検査します。悪意のある宛先へのアクセスをブロックし、不審なリンクにフラグを立てることで、インタラクションの時点でフィッシング攻撃や認証情報の盗難を未然に防ぎます。



重要なシステムの可用性を維持

課題：サイバーインシデントは、接続されたシステム間で急速に波及する可能性があります。封じ込めや調査を行うには、多くの場合、統合機能、ワークフロー、またはアクセスを停止させる必要があります。

解決策：WithSecure Cloud Protectionは、脅威をリアルタイムで防止することで、医療機関がSalesforceのワークフローの混乱を回避できるよう支援します。脅威が侵入または実行される前に阻止するため、インシデント発生後の調査や隔離の必要性を低減します。



拡大する攻撃対象領域を保護する。

課題：ワークフローの自動化ややり取りのデジタル化のために、AIを活用したツールを導入する組織が増えています。これにより、攻撃の侵入経路が増え、攻撃者が既存の防御を迂回できるようになる可能性があります。

解決策：WithSecure Cloud Protectionは、従来のポータルやAgentforceを含む新しいツールのセキュリティを確保します。これにより、人間によるやり取りとAI駆動のやり取りの両方において、脅威がリアルタイムでブロックされることが保証されます。

シナリオ

この例では、Salesforce管理者がWithSecure Cloud Protectionを活用し、セキュリティおよびコンプライアンスに関する共同責任モデルにおける自らの役割をどのように果たせるかを考えてみましょう。

エマ・ライス

Salesforce管理者

エマは、所属組織の Salesforce プラットフォームを管理し、ケース管理やケア調整といった内部ワークフローに加え、患者の受付やパートナーポータルなどの外部ワークフローもサポートしています。彼女は IT 部門、コンプライアンス部門、臨床チームと緊密に連携しています。日々の業務には、システムパフォーマンスの維持、新機能の導入、および他チームから指摘されたリスクへの対応が含まれます。

エマの優先事項は、稼働率、イノベーション、費用対効果の高いリスク低減といったCIOレベルの目標と、しばしば一致しています。

彼女の目標

- Salesforceの運用を安全かつ安定的に維持する
- 機密性の高い患者データの保護
- リスクを軽減しつつイノベーションを推進する
- 外部ITベンダーとのやり取りに費やす時間を削減する

彼女の課題

- ファイル、リンク、またはフォームを介してSalesforceに侵入する脅威に対する可視性が限られている
- ワークフローを妨げる内部セキュリティ対策
- 運用を停滞させる脅威の調査
- イノベーションとリスクのバランス

WithSecureは、以下の支援を通じてエマの課題を解決します：

患者がアップロードしたファイルに対してリアルタイムのマルウェアスキャンを実行

エマは「WithSecure Cloud Protection」を活用し、Experience Cloudポータルを通じて患者や検査機関からアップロードされたすべてのファイルをリアルタイムスキャンしています。マルウェアは、拡散したりダウンロードされたりする前に即座にブロックされます。

インシデントへの対応を迅速化し、業務への支障を軽減

WithSecureは、脅威が活動を開始する前にブロックし、エマやセキュリティチームが迅速に対応できるアラートやログを提供します。

Salesforceレコード内のフィッシングリンクを検出

WithSecureのリアルタイムURLおよびQRコード分析により、Emmaのユーザーを標的としたフィッシング攻撃を阻止します。攻撃者がメッセージ、レコード、または添付ファイルにフィッシングリンクを埋め込もうとすると、システムは直ちにアクセスをブロックします。

拡大するエコシステム全体にわたる可視性と制御を確保

WithSecure Cloud Protectionは、イノベーションによってリスクが増大しないよう支援します。そのネイティブ統合機能により、エマとそのチームは、Agentforceを活用したトリアージや患者の振り分けを拡大する際、追加ツールの導入や複雑さの増加を最小限に抑えることができます。

WITH secure

WithSecureの詳細はこちら