

# Falcon Shield

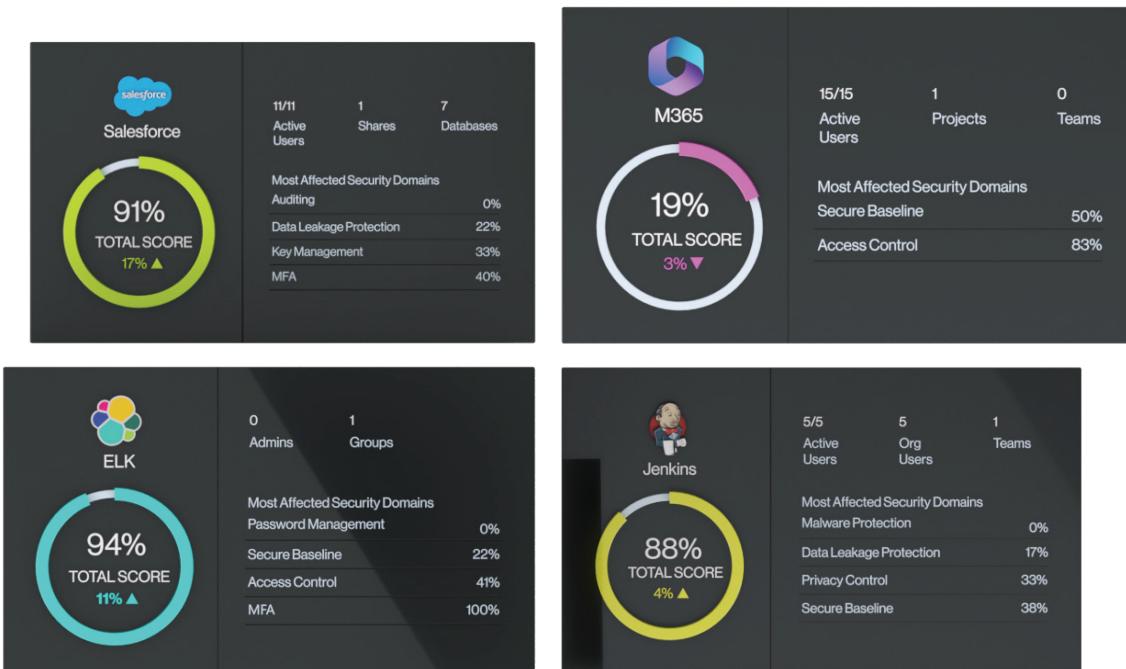
## ユースケースと主要機能

### SaaSスタック全体を保護

SaaSスタック全体にわたる深い継続的な可視性とコントロールを実現します。CrowdStrike Falcon®のSaaSセキュリティプラットフォームなら、SaaSの脅威の防止、検知、対応が可能です。アプリケーションの管理者と容易に連携して、あらゆるセキュリティドリフトを修正することができます。

### セキュリティの設定ミスを常時把握

すべてのSaaSアプリケーションと連携し、詳細なセキュリティチェックと自動/ステップバイステップの修復機能により、セキュリティ設定ミスを監視・管理します。



- **Falcon Shieldなら、次のようなことを実現できます。**

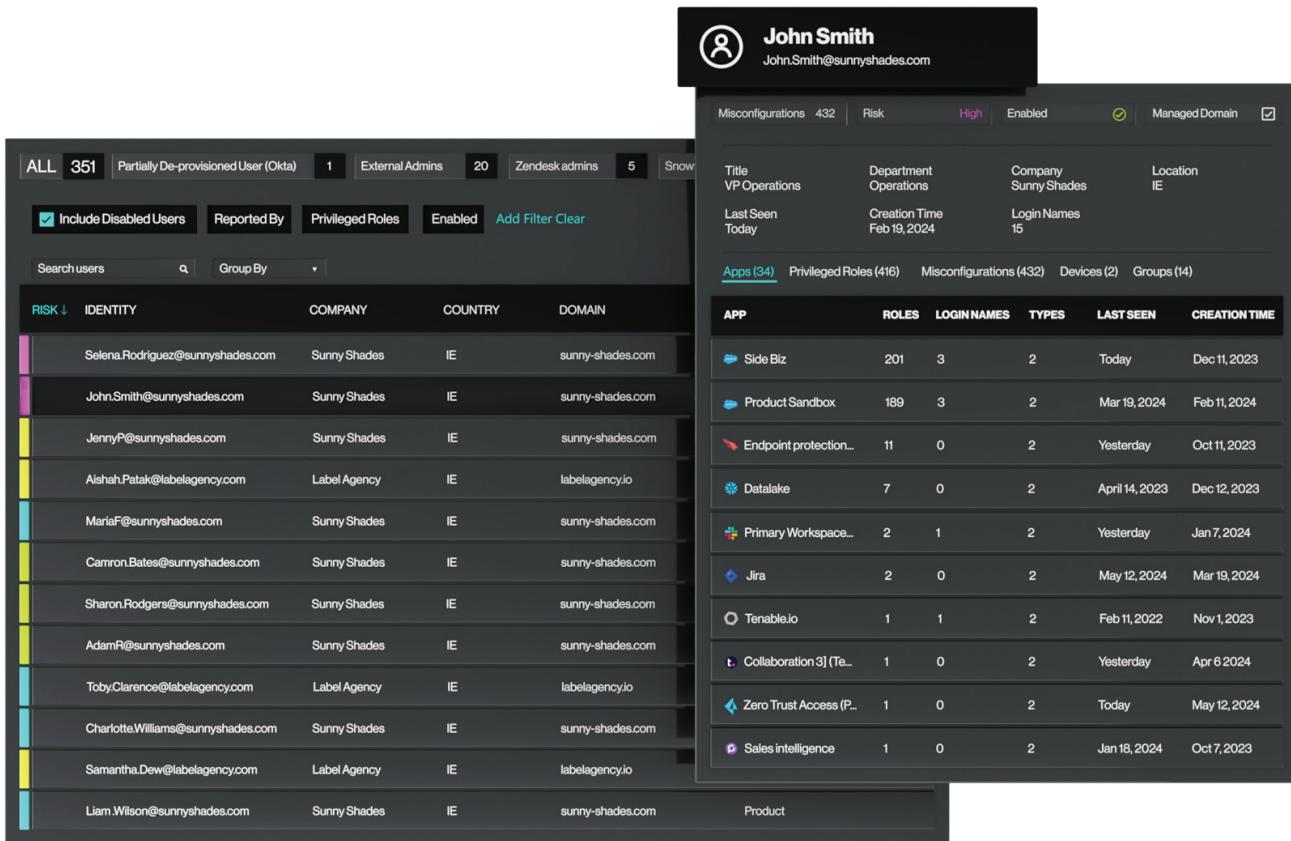
- アプリケーションの網羅性と深いセキュリティ対策
- 重大度やセキュリティドメインに基づくリスク管理の優先順位付け
- ガイド付きの修復
- コンプライアンスマッピング

## クラウドストライクソリューション

Falcon Shield

## 強力なアイデンティティセキュリティポリシーを構築

社内外のSaaSユーザーのガバナンスを強化して権限を監視し、非人間アイデンティティを保護します。



The screenshot displays the Falcon Shield web interface. At the top, a navigation bar includes links for 'Misconfigurations', 'Risk', 'High', 'Enabled', 'Managed Domain', and a user profile for 'John Smith' (John.Smith@sunnyshades.com). Below this, a search bar and filter options are shown, with 'Include Disabled Users' checked. The main content area is divided into two sections: 'IDENTITY' and 'APP'. The 'IDENTITY' section lists users with their email, company, country, and domain. The 'APP' section lists various applications with their roles, login names, types, last seen, and creation time. A 'Product' bar is visible at the bottom.

APP	ROLES	LOGIN NAMES	TYPES	LAST SEEN	CREATION TIME
Side Biz	201	3	2	Today	Dec 11, 2023
Product Sandbox	189	3	2	Mar 19, 2024	Feb 11, 2024
Endpoint protection...	11	0	2	Yesterday	Oct 11, 2023
Datalake	7	0	2	April 14, 2023	Dec 12, 2023
Primary Workspace...	2	1	2	Yesterday	Jan 7, 2024
Jira	2	0	2	May 12, 2024	Mar 19, 2024
Tenable.io	1	1	2	Feb 11, 2022	Nov 1, 2023
Collaboration 3](Te...	1	0	2	Yesterday	Apr 6, 2024
Zero Trust Access (P...	1	0	2	Today	May 12, 2024
Sales intelligence	1	0	2	Jan 18, 2024	Oct 7, 2023

### 特権ロール

特権ユーザーを特定し、設定ミスの管理、デバイス管理、サードパーティアプリケーションのアクセス管理の優先順位付けを行います。

### 権限の最適化

最小特権の原則 (PoLP) を実装し、業務運営を可能にしながら、各SaaSユーザーに必要な適切なレベルのアクセス権を確保します。

### ユーザーのプロビジョニング解除

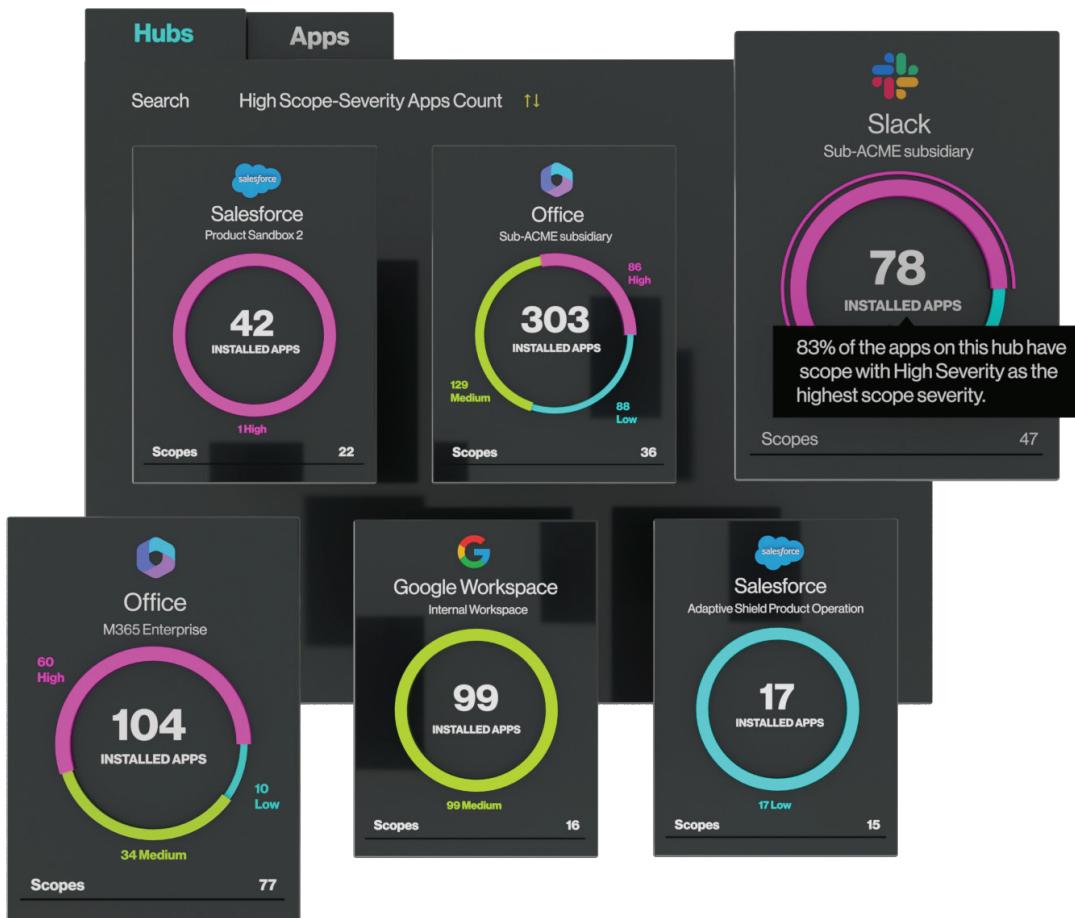
Active Directoryで無効化されているにもかかわらずSaaSアプリへのアクセス権が残っているユーザー、休眠ユーザー、外部ドメインからの特権アカウントを検知します。

### ユーザーの分類

外部ユーザー、内部ユーザー、人間以外のユーザー、その他の特定の分類のユーザーを識別できます。

## 接続されているアプリとシャドーアプリを検出

ビジネスにリスクをもたらす可能性のある、承認済み・未承認のSaaSアプリケーションや、コアとなるSaaSスタックに接続された他の連携サービスを検出し、制御します。



### アプリケーションの検出

コアとなるSaaSスタックに接続されたサードパーティアプリケーションのアクセスを検出し、制御します。

### 悪意のあるアプリケーションの検出

アクティビティモニタリングパネルを通じて、悪意のあるアプリケーションを特定し、フォレンジック情報を収集します。これらのアプリケーションは、ランサムウェアやデータ窃取・破壊のリスクをもたらします。

### 接続されたアプリケーションのリスクレベルを測定

接続されているアプリケーションを検出した後、高リスクな権限スコープを要求しているものを特定します。

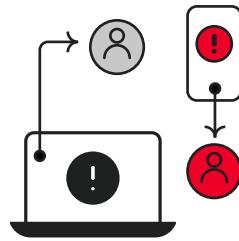
### 休眠アプリの検出

SaaSスタックにアクセスできるものの、長期間アクセスされていないリスクの高いアプリケーションを見つけることができます。

## その他のユースケース

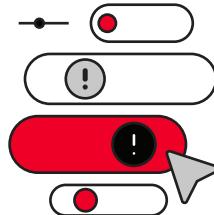
### デバイスリスクの管理

ユーザーデバイスに起因するSaaSリスクを管理し、セキュリティ状態が不十分、管理されていない、またはコンプライアンス非準拠のデバイスを使用している特権ユーザーを優先的に対処することで、包括的なゼロトラストアプローチを実現します。



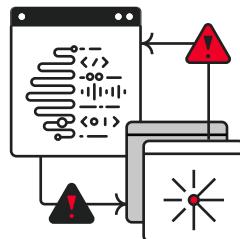
### データ露出の可視化

データ漏洩を防止し、フィッシング攻撃を制限するため、公開および外部共有されているドキュメント、ファイル、コードリポジトリ、カレンダーを検出します。



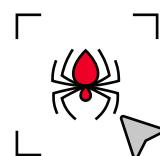
### 生成AIの管理

データ漏洩や不正アクセスを防ぐため、SaaSスタック内の生成AIツールを制御します。

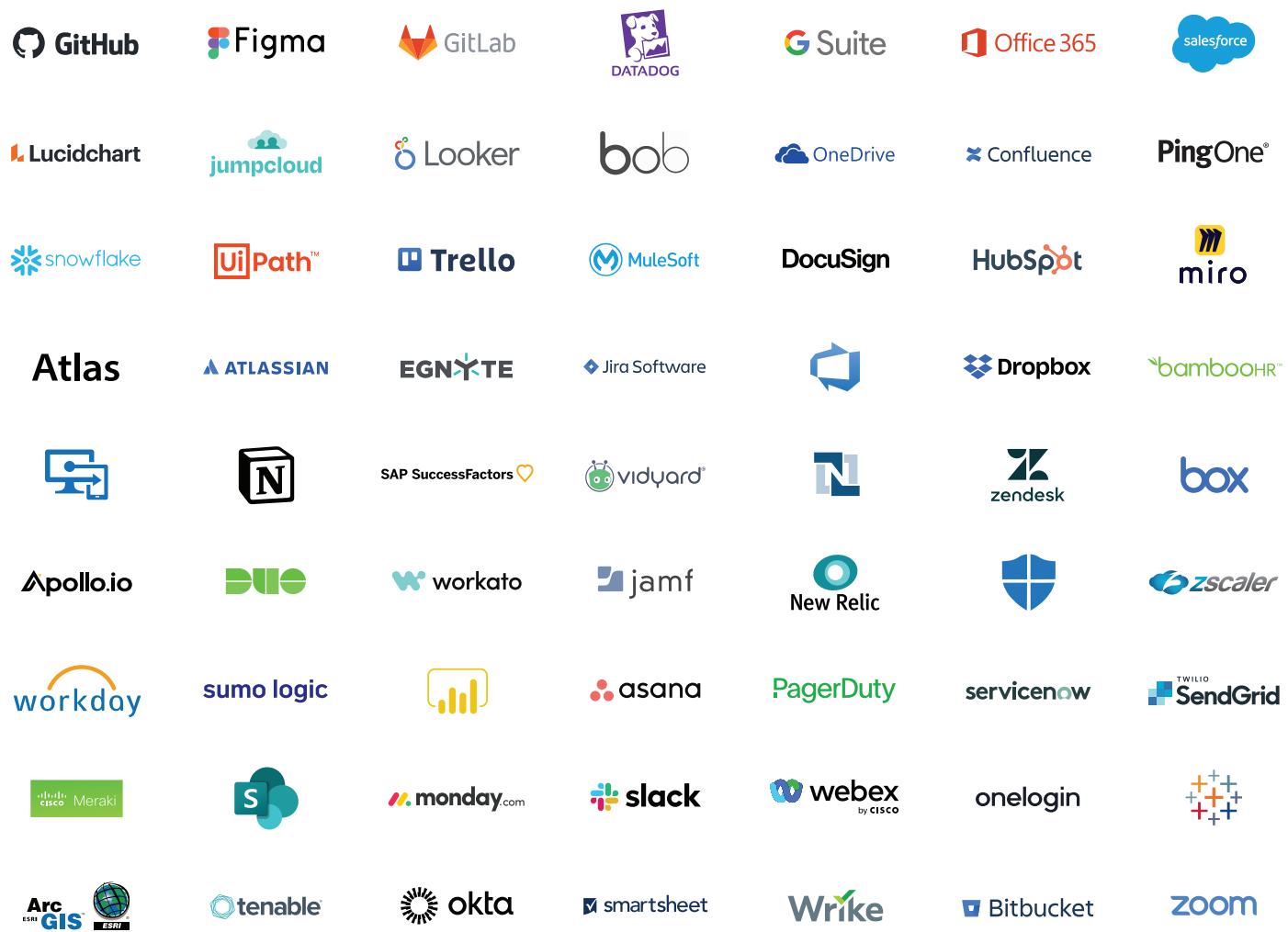


### 脅威の検知と対応

異常なアクティビティ、悪意のあるアプリケーション、または侵害の痕跡など、SaaSエコシステムから発生するアイデンティティ中心の脅威を検知し対応します。



**Falcon Shieldは、150以上のSaaSアプリケーションをすぐに利用可能な形でサポートする唯一のSSPMです**



## クラウドストライクについて

クラウドストライク (Nasdaq:CRWD) は、サイバーセキュリティのグローバルリーダーであり、エンドポイント、クラウドワークLOAD、アイデンティティ、データを含む企業におけるリスクを考える上で重要な領域を保護する世界最先端のクラウドネイティブのプラットフォームにより、現代のセキュリティを再定義しています。

CrowdStrike Falcon®プラットフォームは、CrowdStrike Security Cloudおよび世界クラスのAIを搭載し、リアルタイムな攻撃の痕跡 (IOA)、脅威インテリジェンス、進化する攻撃者の戦術、企業全体からの充実したテレメトリを活用して、超高精度の検知、自動化された保護と修復、精銳による脅威ハンティング、優先順位付けされた脆弱性のオブザーバビリティを提供します。

Falconプラットフォームは、軽量なシングルエージェント・アーキテクチャを備え、クラウド上に構築されており、迅速かつスケーラブルな展開、優れた保護とパフォーマンスを提供し、複雑さを低減し即座に価値を実現します。

**CrowdStrike: We stop breaches.**

詳細はこちら:<https://www.crowdstrike.jp/>

[デモを視聴する](#)

[お問い合わせ](#)

