AppOmni

HITACHI
Inspire the Next

\ SaaSテナントからの情報漏洩を防止 /

SSPMサービス AppOmni

SSPM：SaaS Security Posture Management

SaaSの使い方を誤ることで、さまざまな情報漏洩事件が起こっています

Microsoft 365の
パスワードポリシーの設定が
弱く、不正ログイン

Salesforceの仕様変更に
気づかず、ゲストユーザーから
情報アクセス可能に

GitHubから開発ソースや
システムの認証IDが流出

⚠ 取引先情報や顧客情報が流出！

AppOmniがお客さまの**SaaSテナントが安全か常時監視します!**

- セキュリティ設定不備
- 過剰なアクセス権限
- 不要な3rdパーティ サービスからのアクセス許可
- 不要なアカウントの放置

AppOmni 4 つの強み

きめ細かく診断

各SaaSの機能に応じた専門の診断項目できめ細かく診断します。また、検出したリスクに対し、対策方法などについても具体的にアドバイス。診断内容のカスタマイズも可能です。

疑わしいアクセスも検知

ログ解析により、お客さまのSaaS環境がブルートフォース攻撃や匿名ネットワークからの不審なアクセスを受けていないかを監視できます。アクセスのブロックや対策強化に役立ちます。

SaaSの仕様変更に自動追従

エキスパート機能が刻々と変化するSaaSの仕様やセキュリティ設定に合わせて、セキュリティの弱点を監視します。運用者は監視ルールの調整を気にせず運用できます。

簡単導入・運用

エージェントレスで簡単に導入でき、サービスが用意するベストプラクティスのセキュリティポリシーですぐに診断・監視を始められます。開発プラットフォームで独自のSaaSも統合監視できます。

株式会社 日立ソリューションズ

AppOmniでできること

- セキュリティ対策不備の監視
  (セキュリティ設定・権限・アカウント管理など)
- セキュリティ設定・アクセス権限・接続サービスなどのビュー
- コンプライアンス基準での評価
- 疑わしいアクセスの検知
- レポート
- ポリシーのカスタマイズ

多数のSaaSに対応！順次拡大中

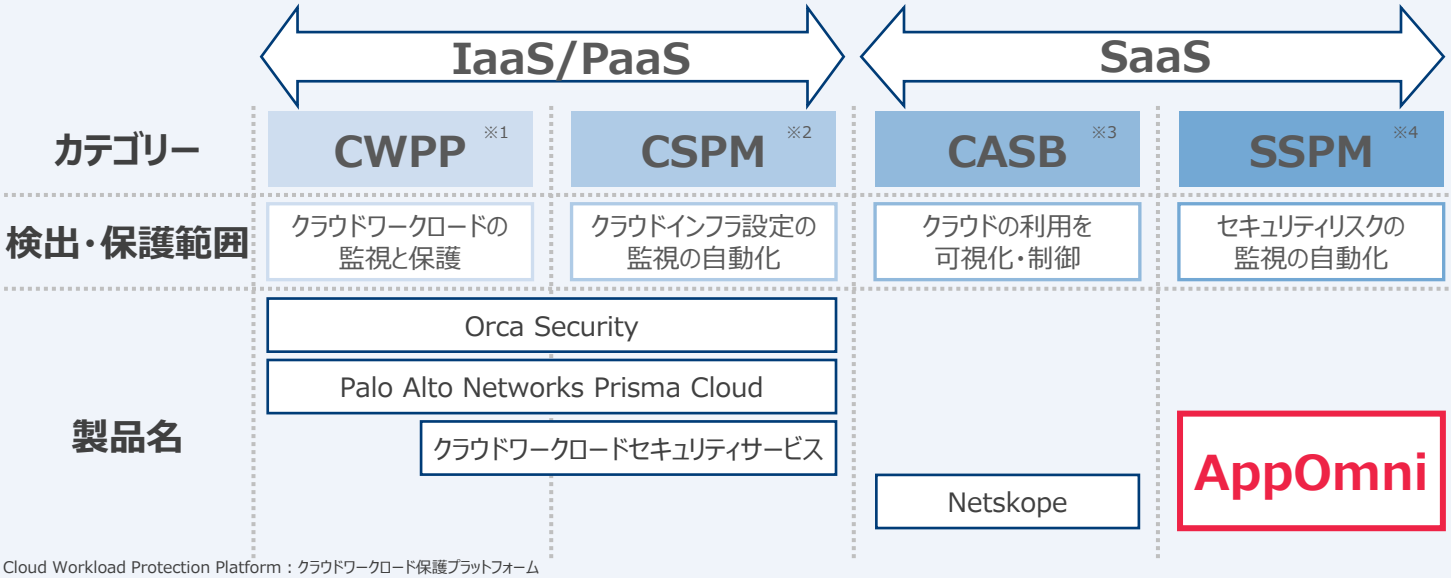
2024年5月時点 対応SaaS 38種類

- Salesforce
- Workday
- Auth0
- Jamf
- Slack
- Webex
- Microsoft 365
- GitHub
- Google Workspace
- monday.com
- Snowflake
- Zendesk
- ServiceNow
- Okta
- Jira Cloud
- PingOne
- Tableau
- Zoom

・・・and more

CSPM/CWPPと組み合わせて
クラウドのセキュリティを万全に

日立ソリューションズではさまざまな脅威に対応する多彩なソリューションをご提供しています。



※1 Cloud Workload Protection Platform：クラウドワークロード保護プラットフォーム
※2 Cloud Security Posture Management：クラウドセキュリティポスチャ管理
※3 Cloud Access Security Broker：クラウドアクセスセキュリティブローカー
※4 SaaS Security Posture Management：サーズセキュリティポスチャ管理

株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報
www.hitachi-solutions.co.jp/appomni/