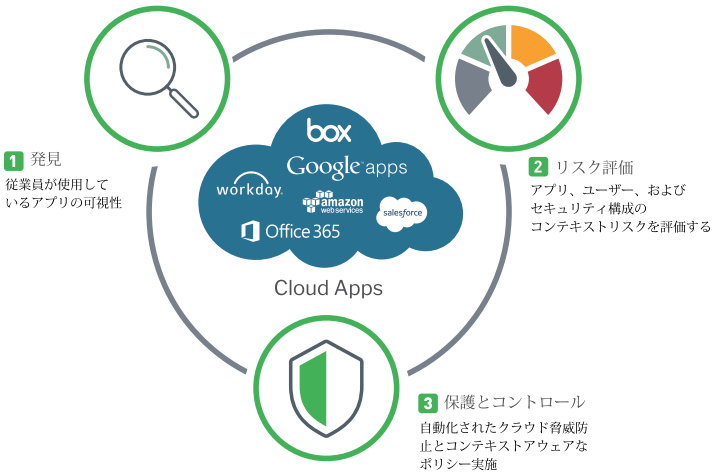
FORCEPOINT

Forcepoint CASB

クラウドアプリケーションの利用を発見し、リスクを分析し、SaaSおよびカスタムアプリケーションに適切な統制を実施

発見、 評価、 保護

Forcepoint CASBはクラウドアプリのデータに対するセキュリティを強化しているため、エンドユーザーは制限なしにお気に入りのアプリにアクセスできます。



The Forcepoint CASBの価値

- 認可されていないすべてのクラウドの使用を発見してリスクの優先付けをする（Shadow IT） - アプリケーションがガバナンスルールを満たし、コンプライアンスの問題を回避しているかどうかをすばやく簡単に判断する
- BYODの力を最大限に引き出し、従業員の生産性とコスト削減を向上させながら、従業員とクラウド内の企業リソースのセキュリティを確保
- クラウド内の異常で危険なユーザーの行動を特定し、悪意のあるユーザーを阻止し、組織の基準を満たしていないユーザーの活動を抑える
- ガバナンスや規定のルールに違反した許可されていないユーザーに、機密クラウドデータを公開するリスクを軽減する
- rootアカウントの乗っ取りに関連する影響を防ぐために不適切と思われる特権の昇格を特定する
- 正当なユーザーまたは脅威実行者に対して、地理情報に紐づくアクセスおよび活動監視を実装する
- 未使用アカウントのコンプライアンス、ライセンス、およびコスト削減のためにアプリケーションの使用状況を追跡する

Forcepoint CASBは、認可されているクラウドアプリケーションと認可されていないクラウドアプリケーションの両方に対する可視性と制御を提供します。

Forcepoint CASBソリューションコンポーネント — Cloud Governance | Cloud Protection | Cloud Security Suite

機能グループ	機能説明	Cloud Governance	Cloud Protection	Cloud Security Suite
アプリケーションの可視性とリスク	Cloud App Discovery — 既存のログファイルを活用して、使用されているクラウドアプリの検出と分類を自動化。	•		•
	Cloud App Risk Scoring — 規制および業界の認証とベストプラクティスに基づいて、各クラウドアプリの全体的なリスクを評価。	•		•
	Cloud App Usage Summary — 各クラウドアプリケーションのユーザー数、アクティビティ、トラフィック量、および通常の利用時間等のサマリ情報。	•		•
	Adavanced Risk Metrics — 各アプリケーションの詳細なクラウドアプリのリスク指標。	•		•
	Customizable Risk Metrics — カスタマイズ可能な重み付けによる詳細なクラウドアプリのリスク指標。	•		•
	Continuous Discovery — ログファイルの自動スキャンと検出レポートの生成を定期的にスケジュール。	•		•
	Centralized Discovery Dashboard — 集計されたディスカバリ結果、以前のアクティビティに対して基準化された現在の使用状況、および使用状況の傾向。	•		•
	App Catalog & Risk Updates — クラウドアプリカタログの自動更新と利用可能なリスクプロパティの変更。	•		•
	Activity Log Collections — クラウドアプリAPIを介してユーザーと特権ユーザーの基本的なアクティビティログを収集。	•		•
アカウントとデータ	Data Classification — 機密または規制データを識別してカタログ化します。法令順守を確実にするためのデータ (例：PCI, SOX, HIPAA等)。	•		•
	User Governance — 運用コストを削減し、セキュリティ上の脅威を最小限に抑えるために、非アクティブまたは孤立したアカウント（元従業員など）、および外部ユーザー（請負業者など）を識別。	•		•
	App Governance — 業界の一連のベストプラクティス/規制要件に対するセキュリティ設定のベンチマーク(例： PCI DSS, NIST, HIPAA等)。	•		•
	Integrated Remediation Workflow — 組み込み型の組織ワークフローを活用して、Forcepoint CASBまたはサードパーティのチケットシステムとの統合により、リスク軽減タスクを割り当てて完了させる。	•		•
リアルタイムアクティビティ監視と分析 (available in inline/proxy)	Activity Monitoring & Analytics — ユーザー、グループ、場所、デバイス、アプリケーションの動作などによるリアルタイムのアクティビティ監視と分析。		•	•
	Privileged User Monitoring — 特権ユーザーおよび管理者のリアルタイムアクティビティ監視およびリポート。		•	•
	Enterprise Siem Integration — ArcSight、Splunk、Q1 Labsなどの主要なSIEMソリューションにアクティビティログを直接入力するためのアダプタ。		•	•

Forcepoint CASBソリューションコンポーネント — Cloud Governance | Cloud Protection | Cloud Security Suite

機能グループ	機能説明	Cloud Governance	Cloud Protection	Cloud Security Suite
リアルタイムアクティビティ監視と分析 (available in inline/proxy)	Automatic Anomaly Detection — リスクの高いインサイダー攻撃や外部からの攻撃など、継続的な行動の監視と異常な活動の検出。		•	•
	Real-Time Threat Prevention — アクティビティの異常と危険なIPアドレスを関連付けます。ポリシーを適用して、アプリのアラート、ブロック、検疫、またはID確認を要求したり、アプリ内の特定のアクションを要求。		•	•
	Data Leak Prevention — 100以上のファイルタイプと何百もの定義済みデータタイプ（例：PCI、PII、PHI、HIPPA、SOX）のための保存データ分類とリアルタイムコンテンツ検査。		•	•
	Multi-Factor Authentication — 異常または高リスクの活動が検出された場合のリスクベースの本人確認。		•	•
	Single Sign-On — SAMLベースのアプリケーションにアクセスするための組み込みまたはサードパーティのSSOの活用。		•	•
	Dynamic Alerts — SMS/Eメールによるポリシー違反または活動しきい値のリアルタイム通知。		•	•
	Mobile & Endpoint Access Control — ブラウザまたはリッチモバイルアプリのどちらから発信された場合でも、管理対象デバイスと管理対象外デバイスの固有のポリシー。		•	•
	Location Based Access Controls — ユーザーの場所またはクラウドサービスの場所に基づいてアクセスを制限。		•	•
	Mdm Integration — 既存のMDM展開を活用してエンドポイント登録とクラウドアクセスを管理。		•	•
	Custom Policies — ビジュアルポリシーエディタにより、さまざまな属性に基づいてカスタムポリシーを簡単に設定。		•	•
高度なククラウド	Performance Optimization — キャッシュとコンテンツの最適化を通じてクラウドアプリへのアクセスを加速。	•	•	•
	Centralized Threat Intelligence — エンタープライズデータベーステーブル、ファイル共有に格納されているファイル、およびクラウドアプリケーションに格納されているデータに対する脅威の統合ビュー。	•	•	•
管理者とアクセス	Siem Integration — 既存のSIEM環境と統合するためにCommon Event Formatでディスカバリーデータを生成。	•	•	•
	Enterprise Directory Integration — ユーザー、グループ、組織のレポートおよびポリシーに既存のADまたはLDAPディレクトリインフラストラクチャを使用。	•	•	•
	Role-Based Admin — 資産、ポリシー、およびシステム設定を編集するための権限を定義。	•	•	•
	Enterprise Reporting — カスタマイズされたレポートを編集および保存する機能を備えた事前定義されたレポートを含む柔軟なレポートオプション。	•	•	•
	Encryption Broker – Forcepoint CASBがキーローテーションを処理し、完全な監査を提供しながら、クラウドサービスプロバイダに独自のキー（BYOK）または暗号化を提供。			•

なぜForcepoint CASBなのか

DLP統合

Forcepoint CASBはDLPソリューションと統合して、オンプレミスからクラウド環境までをカバーする統一データ保護を提供します。また、Webセキュリティ、電子メールセキュリティ、次世代ファイアウォールなどのソリューションとも統合されています。

ビルトインクラウドUEBA

Forcepoint CASBは、脅威の可能性とビジネスへの影響に基づいてリスクプロファイルを作成します。 SOCチームとインシデント対応チームにリスク優先のアラートを提供するために、何千ものアプリとアクティビティに基づく分析を利用します。

Bring Your Own Device (BYOD)

Forcepoint CASBは、APIとフォワード/リバースプロキシのサポートにより、最も包括的なユースケースを網羅しています。 これにより、管理されていないデバイスに対してきめ細かいデバイスとアクティビティの制御が提供されます。

あらゆるアプリのクラウド監視と制御

Forcepoint CASBは、カスタムアプリケーションを含むあらゆるアプリケーションを製品変更なしでサポートするための柔軟な製品アーキテクチャを備えています。 ユーザーは、数時間から数日でアプリケーションの使用状況を完全に監査および保護できます。

迅速な価値実現

APIとプロキシモードの両方の長所から選択して、実装を促進し、クラウド環境のリスクを軽減します。

機能と利点

- App Discovery, Governance, Compliance, 1つのソリューションでの分析と保護
- APIまたはプロキシモード、あるいはその両方の展開オプション
- モバイルデバイスとエンドポイントデバイスのきめ細かいポリシーにより、管理対象デバイスと管理対象外デバイスのアクセス制御とデータ保護が可能になります
- 一般的なアプリの詳細リポート（Office365 AWS、Salesforce、Dropbox、G-suite、Boxなど）
- オンプレミスとクラウド環境にまたがるForcepointエコシステム製品の一部
- エンタープライズディレクトリ、SIEM、およびMDMと統合する
- サービスとしてのアイデンティティ（IDaaS）パートナー（Centrify、Ping、Oktaなど）との相互運用性の認定
- 異常および脅威の検出機能をクラウドアプリに拡張する
- IPレピュテーションデータにより、より正確なリスク軽減ポリシーを作成および実施できます
- リスク要因を分析し、アプリを並べて比較して、クラウド環境に最適なオプションを見つける

forcepoint.com/contact

[CASB-GLOBAL-DATASHEET-US-EN] 100055.030619