Forcepoint

データシート

Forcepoint ONE

Cloud Access Security Broker

エージェントレスリバースプロキシ、フォワードプロキシ、APIモードを備えたマルチモードCASB。

主な利点：

- 2015年以来、99.99%の稼働率を確認済み
- オートスケーリングとAWS上の300以上のポイント・オブ・プレゼンス（POP）がレイテンシを最小限に抑えて スループットを最大化
- 統合管理コンソールによる 反復的・冗長構成管理の 削減
- CASB、SWG、ZTNA向け 統合管理デバイスエージェントで 導入を簡素化
- Active Directory同期エージェント による ユーザーオンボーディングの加速
- 移動中のデータをスキャンすることにより、あらゆるデバイスや管理対象SaaSのアプリケーションのユーザー間での マルウェアやデータ流出を 阻止します。
- フィールドプログラマブルSASEロジック は特定のHTTP/Sリクエストメソッドを阻止できるため、管理対象のSaaSウェブページにおけるあらゆる要素を きめ細かく 制御することができます
- 選択したSaaSやIaaSの保存データをスキャンすることにより、移動中のデータスキャンとは独立してマルウェアや機密データを識別します。
- 管理対象のSaaSアプリケーションの ファイルレベルを暗号化することにより、データへのアクセスを完全にブロックすることなく、データのプライバシーとデータ主権を確保します。
- シャドーITレポートは、無認可アプリケーションのリスク識別に役立ちます
- デジタル著作権管理（DRM）は、機密データ保護の新たな方法で フレキシビリティを向上させます。

Forcepoint ONE Cloud Access Security Broker（CASB）は、Forcepoint ONE クラウドプラットフォームの3つの基本ゲートウェイの1つです。管理対象のSaaSアプリケーション とシャドーITアプリケーションへのアクセスを制御しつつ、データ損失防止（DLP）とマルウェアからの保護を提供します。

エージェントレス・リバースプロキシモード

エージェントレス・リバースプロキシモードは、Forcepoint ONEに統合されたDLPとマルウェアスキャンを活用し、最新ブラウザを使用しているあらゆるデバイスへのきめ細かなアクセスを 提供します。BYODや請負業者のデバイスからの アクセスを監視・制御するのに最適です。Forcepoint ONEの特許取得の SAML 2.0準拠のIdPとの統合を活用し、ユーザーをForcepoint ONEリバースプロキシに誘導して、SaaSアプリケーションとの補完セッションを 確立します。

図1：AJAX/VMを備えたForcepoint ONE CASBエージェントレス・リバースプロキシ。

Forcepoint ONEエージェントレス・リバースプロキシモードは、Forcepoint ONE独自のAJAX/VMテクノロジーと組み合わせ、ユーザーのブラウザー内で実行されることで、適切なURLとcookieの書き換えを確実に実行し、あらゆるSaaSアプリケーションとの 互換性を提供します。リバースプロキシモードでアプリ使用状況を制御・監視するための主な機能は、プロキシポリシー、フィールドレベルの暗号化、シャドーIT レポート、リバースプロキシレポートです。

プロキシポリシー

管理対象SaaSアプリケーション間の移動データのアクセス制御オプションと、関連するDLPおよびマルウェアのスキャンオプションは、プロキシポリシーで設定されます。管理者はこれにより、管理対象SaaSアプリケーションへのアクセスを、直接的アプリケーションアクセス、拒否、または安全なアプリケーションアクセスとして設定することができます（全ての トラフィックがリバースプロキシを通過し、DLPおよびマルウェアのスキャンを 実行する選択肢もあります）。ポリシー適用 基準には、ユーザーグループ、アクセス方法 （ブラウザー、非ブラウザー・クライアント・アプリケーション、または全て）、デバイスOS、デバイスプロファイル、場所などがあります。

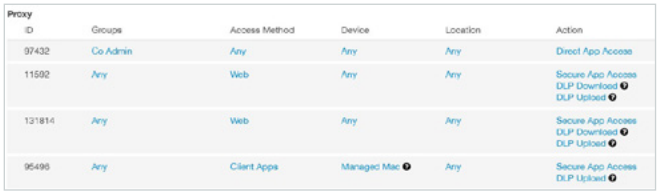

図2：管理対象SaaSアプリケーションのプロキシポリシーリスト

単一アプリケーションに複数のプロキシポリシー・リストを含めることが可能です。これらのポリシーは、ポリシー内の全ての一致基準が接続要求に一致するポリシーが見つかるまで、順番に 評価されます。その後、適切な施行アクションが 適用されます。

安全なアプリケーション・アクセスが指定されると、単一プロキシ ポリシーには、SaaSアプリケーションへのアップロード用DLPおよびマルウェアスキャンポリシーのリスト、そして SaaSアプリケーションからのダウンロード用の 別リストなどが含まれます。さらに、管理対象 SaaSアプリケーションでフィールドレベルの暗号化が有効になっている場合にプロキシ ポリシーを使用すると、フィールドセキュリティレベルに基づいて フィールドを暗号化せずに表示するか、ユーザーロケーションをデータ作成場所と一致させるかを 指定できます。これにより、データのプライバシーとデータ主権がサポートされます

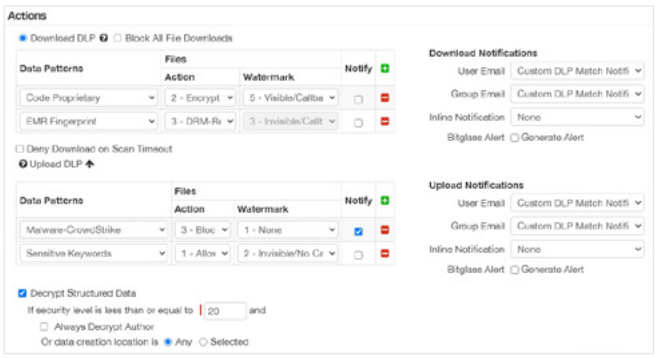

図3：安全なアプリケーションアクセス接続のためのプロキシポリシー詳細。

単一プロキシポリシー内でダウンロードDLPポリシーを使用すると、機密データとマルウェアの両方のダウンロードが制御できます。また、アップロードDLPポリシーを使用すると、機密データとマルウェアのアップロードが 制御できます。ドロップダウンメニューを 使用するだけで、一致データパターン、ファイルアクション、透かし・追跡の制御を指定できます。また、一致内容に関する通知を行いたい場合も、チェックボックスをクリックするだけで実行できます。

Forcepoint ONEには、PII、PHI、個人財務データに関する地域や業界の標準を施行するのに役立つ、190超の定義済みデータパターンが 含まれています。CrowdStrikeまたはBitdefenderによる マルウェアスキャン呼び出しのための予約済みデータパターンも2種類 含まれています。また、単純なレギュラー・エクスプレッションから 複雑なブール式までを網羅したカスタムデータパターンや、記録識別のための特別なデータパターンを 作成することもできます。特別な一致パターンには、データベース一致（完全一致を使用）、標準フォームとの類似（ファイル・フィンガープリントを使用）、任意HTTP/S 要求メソッド（フィールドプログラマブルSASEロジック《FPSL》を使用）が含まれています。

ダウンロード・プロキシポリシー用のファイルアクションは、暗号化、阻止（コンテンツを阻止メッセージに置き換え）、拒否（転送しない）、DRM適用、透かし、追跡です。

アップロード・プロキシポリシー用のファイルアクションは、暗号化（Office 365、Google Workspace、Salesforceの場合）、阻止 （コンテンツを阻止メッセージに置き換え）、拒否（転送しない）、データマスク（Salesforce Chatter、O365 Teams、 Slackの場合）、透かし、追跡です。

フィールドレベルの暗号化

エージェントレス・リバースプロキシモードは、完全なAES256ビットの暗号化またはトークン化、組み込みの キーストアまたは独自のキー管理相互運用プロトコル（KMIP）キーストア、ボールトレス暗号化、トークン化をサポートして、多くの一般的SaaSアプリケーションで 構造化データを暗号化します。さらに各フィールドのセキュリティレベルを指定し、ユーザーに対していつフィールドをデクリプトするかの制御を実行できます。

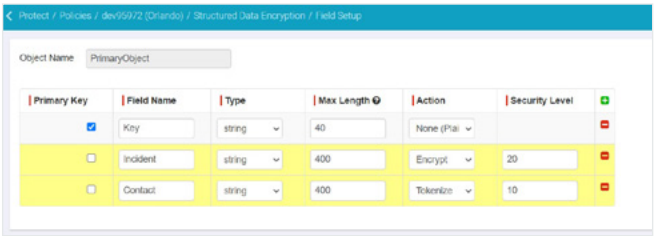

図4：フィールドレベル暗号化設定。

シャドーITレポート

エージェントレス・リバースプロキシモードは、シャドー ITレポートをサポートします。シャドーITの使用状況は、手動インポートまたは Forcepoint ONE syslogコレクターを介し、企業のファイアウォールとプロキシサーバーのログデータから収集されます。レポートには、Forcepoint ONEが計算した 信頼格付けによるアプリケーション分布と、個々のアプリケーションやソースIPアドレスにドリルダウンしたアクセス上位アプリケーションが表示され、Webトラフィックに対する組織のリスク姿勢を理解するのに 役立てられます。また、Forcepoint ONE CASBでは、フォワードプロキシモードでシャドーITトラフィックを制御することもできます（下記参照）。

図5：シャドーIT検出レポート。

リバースプロキシモードは、リバースプロキシを通過する管理対象SaaSトラフィックに関する 広範な洞察レポートを提供します。レポートには、データセキュリティダッシュボードと脅威ダッシュボードの両方の「移動データセクション」とプロキシログレポートが含まれます。データセキュリティダッシュボードには、Forcepoint ONEプラットフォームが識別した機密データ詳細が表示されます。これには、Forcepoint ONEプラットフォームによって保護されたアプリケーションが送受信する機密データの移動、無認可アプリケーションへの機密データのアップロード、管理対象外デバイスへの機密データのダウンロード、機密データを移動している上位グループやユーザー が含まれます。

脅威ダッシュボードには、データセキュリティダッシュボードと同じ種類のメトリクスが含まれますが、とりわけマルウェアとサイバー脅威に対応しています。

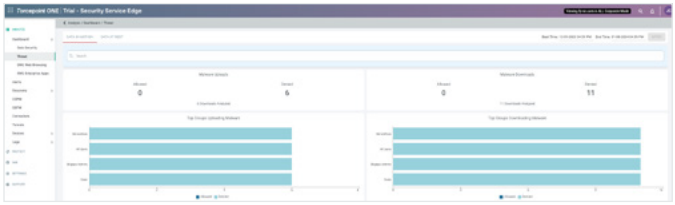

図6：プロキシダッシュボード

プロキシログレポートは、時間経過とともにアプリケーションのアクティビティ、透かし、DLP・DRMのアクティビティを把握します。また、最近のイベントを概要、監査、データ漏洩のカテゴリ別に一覧表示 します。

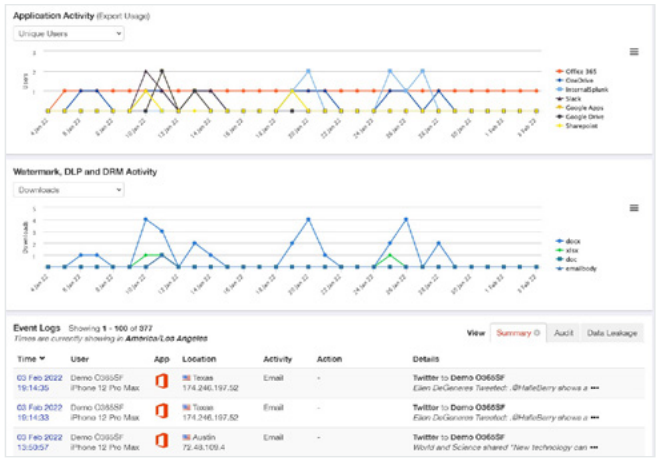

図7：プロキシログレポート

フォワードプロキシモード

フォワードプロキシモードは、WindowsまたはMacOS用のForcepoint ONE統合エージェントを使用します。すべての管理対象SaaSトラフィックは 引き続きForcepoint ONEリバースプロキシを通過しますが、ユーザーデバイスに接続するためにURLを書き換える必要は ありません。フォワードプロキシモードは、プロキシポリシーによるDLPおよびマルウェアスキンの強制実行など、エージェントレス・リバースプロキシモードの全機能をサポートしますが、MicroSoft Outlookクライアントや Slackクライアントなどの 非ブラウザークライアントの使用もサポートします。さらに、フォワードプロキシモードはシャドーIT 制御をサポートします。

シャドーIT制御

シャドーIT制御により、管理対象のSaaSプロキシポリシーのように順番に評価されるプロキシポリシーを使用して、任意のシャドーITアプリケーションへのアクセスを制御することができます。ただし、シャドーITアプリケーションのプロキシポリシーでは、アップロード・ダウンロード時のDLPおよびマルウェアのスキャンは 適用されません。その代わり、以下の接続制御オプションに制限されます: アプリケーション読み取り専用モードによるレンダリング、コーチング (会社が 承認した代替アプリケーションの推奨事項を表示し、オリジナルのシャドーITアプリケーションへのアクセスを許可または拒否)、またはコーチングメッセージなしに アクセスを 拒否。

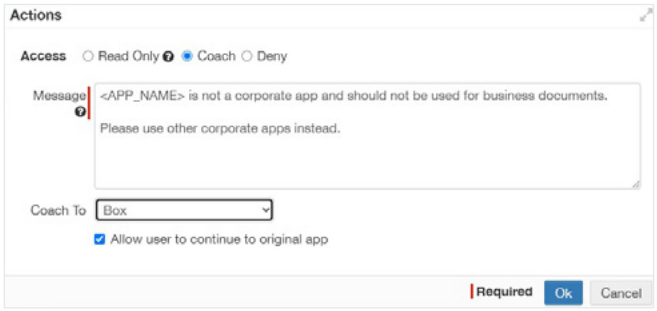

図8:コーチオプションを示すシャドーITプロキシポリシーの詳細。

シャドーITアプリケーションに対するDLPおよびマルウェアスキャンポリシーを サポートする必要がある場合は、代わりにSWGコンテンツポリシーを 使用してください。

APIモード

APIモードでは、CASBはSaaSまたはIaaS テナントへのAPI呼び出しを使用して、保存データに機密データやマルウェアが含まれていないかスキャンし、共有の制限、隔離、コピー、分類メタデータ追加、ファイル所有者への通知といった 自動修復アクションを実行します。履歴ファイルのスキャンをサポートし、機密データのスキャン前に 画像ファイルと画像のみのPDFファイルにOCRを適用できます。APIモードは、Google Workspace、Office 365、Salesforce、ServiceNow、Box、Dropbox、Atlassian Confluence、Github、Webex Teams、Slack、AWS、GCP、Azureなど、多くの一般的なSaaSやIaaSですぐに使用できます。API モードにより、新たなファイルや古いファイルの更新が リバースプロキシを迂回した場合も 機密データのスキャンが可能です。

APIポリシー

APIポリシーは、IaaSとSaaS内のデータスキャンを制御します。プロキシポリシーと同様、複数のAIPポリシーを単一のSaaSアプリケーションに適用し、順番に評価することができます。

図9:APIポリシーのリスト。

ポリシー内では、ユーザー グループ、DLP データ パターン、ファイル パス、ファイル名、共有ステータス (外部、内部、パブリック、またはすべて)、ファイル サイズ、所有者、ユーザー名との共有、作成日、および変更日に基づいて一致基準を指定できます。API ポリシーで使用されるデータ一致パターンは、プロキシ ポリシーと SWG コンテンツ ポリシー間で共有されるカスタム一致パターンまたは定義済み一致パターンのいずれかにすることができ、機密データとマルウェアを統合的に制御できます。

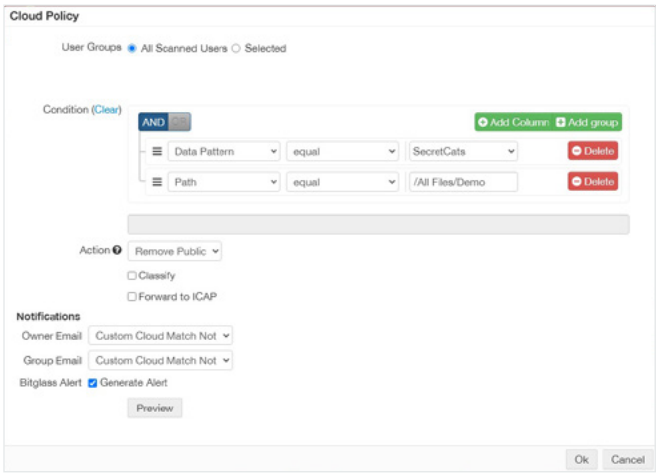

図10:APIポリシー詳細

スキャンされたファイル条件が一致すると、共有変更 (パブリックの削除、パブリックと外部の削除、全削除)、許可、隔離、コピー作成、暗号化などのAPIポリシーアクションが可能となります。

CASBサードパーティ統合

Forcepoint ONE CASBは、以下に概説するさまざまなその他のデータセキュリティシステムを統合するために 構成することもできます。

- → **セキュリティ情報およびイベント管理（SIEM）。** Forcepoint ONEは、syslogをサポートしているあらゆるシステムと 統合できます。これにより、サードパーティーのアプリケーションは Forcepoint ONEからログをアップロードし、視覚化 や分析を実行することが可能となります。
- → **オンプレミスDLPシステム。** Forcepoint ONE は、インターネット・コンテンツ・アダプテーション・プロトコル（ICAP）を サポートしている オンプレミスのDLPシステムと 統合できます。これにより、お客様は Forcepoint ONEによって機密データが含まれているとフラグ付けされた、管理対象のSaaSまたはIaaSクラウドストレージ内の 保存ファイルを、TLS暗号化を使用してオンプレミスのDLPシステムに送信することが できます。ファイルには、送受信先 IPアドレスやファイル所有者メールアドレスなどのデータが 追加されます。
- → **セキュリティ・オーケストレーション・アンド・レスポンス（SOAR）。** Forcepoint ONEは、Forcepoint ONEと選択したSOAR プラットフォーム間の双方向の統合をサポートします。この場合、SOARプラットフォームは Forcepoint ONEと別のツール内のアクティビティを 自動化するために使用されます。
- → **Data Classification。** Forcepoint ONEは、DLP一致パターン内で、任意のデータ分類子からの分類メタデータを 使用することができます。.
- → **エンドポイント管理。** Forcepoint ONEは、SAML ログインプロセスの一環として、Windows、Mac、Android、または IOSデバイスに保存されているクライアント証明書を検証し、エンドポイント管理システムによって管理されていると確認することができます。このナレッジにより、管理者は管理対象デバイスと管理対象外デバイスからログインするユーザーに対して、異なるアクセスポリシーを適用することができます。

Forcepoint ONEプラットフォーム機能

Forcepoint ONE CASBは、Forcepoint ONEプラットフォームに組み込まれた 以下の機能もサポートしています：

- → **プラットフォームレベルのコンテキストアクセス制御。** ユーザーは、ユーザーの場所、デバイスの種類、デバイスの状態、ユーザーの行動、ユーザーグループを考慮したForcepoint ONEログインポリシーに従って認証されない限り、3つの基本ゲートウェイのいずれにも アクセスできません。新しいデバイスからのユーザーログインが検出された場合、またはクライアントIPアドレスに基づくと「不可能な移動」が検出された場合、盗まれた認証情報の使用を防ぐため、ユーザーに多機能認証（MFA） チャレンジを提示することができます。
- → **SWG、CASB、ZTNAの** 構成、監視、レポート作成のための 統合管理コンソール。管理者は、プライベートWebアプリケーションの SWG、CASB、ZTNA全体で DLP一致パターンを再利用し、すべてのトラフィックと異常を統合ビューで 確認できます。
- → **独自の自動生成および** 自動ローテーション証明書を備えた、WindowsまたはmacOS 用の統合オンデバイスエージェント。
- → **Active Directory同期エージェント** は、現在の Active Directoryユーザーおよびグループを、Forcepoint ONE ユーザーおよびグループに同期します。
- → **AWS上の自動スケーリング分散アーキテクチャ** は、300を超える拠点をもち、2014年以来99.99%の サービス稼働率を確認済みです。

Forcepoint ONE CASBの機能と利点

特徴	利点
世界中で300を超えるPOPを備えたAWS上の自動スケーリング分散アーキテクチャ。	→ 99.99%の稼働率。 → 遅延を最小化：多くの場合、アプリケーションに直接アクセスするよりも高速となります。 → タイムアウトなしでSlackトラフィックのインラインプロキシを可能にします。
SAMLリレーまたはACSプロキシモード内での、任意のSAML互換IdPとの統合。オプション：Microsoft ADFS使用のビルトインIdP。	→ フレキシブルな導入。 → DDOS攻撃からの保護（SAMLリレーモード使用時）。
Active Directory 同期エージェント。現在のADユーザーおよびグループを、Forcepoint ONEユーザーおよびグループと同期します。	→ 既存のMicrosoft ADインスタンスを活用してユーザーの迅速なオンボードを実現し、ユーザー所属グループを管理します。
ユーザーグループ、デバイスの種類、場所、時刻 に基づいたコンテキストアクセス制御、または「不可能な移動」、許可されていない場所、未知のデバイスに基づく多要素認証へのエスカレーションを実行します。ユーザーグループ、デバイスタイプ、ロケーションに基づき、個々のウェブサイトやアプリケーションに対するアクセス制御レイヤーを追加します。	→ 疑わしいログイン試行を検出・阻止します。 → パスワード盗難に伴うリスクを低減します。 → リスクとアクセスの必要性に基づき、ユーザーをセグメント化します。
オンデバイスSWG、CASBフォワードプロキシ、非ウェブアプリケーション用ZTNA向けの単一統合エージェント。MDMシステムによる展開のサポートが含まれており、自動ローテーションで自己生成される証明書を使用します。	→ エージェント配備の簡素化。 → セキュリティ強化。 → ITオーバーヘッド削減。
単一の管理者コンソールが 全てのアプリケーション、ユーザー、デバイスの全システム機能を管理します。	→ 複雑さを減らし、価値実現までの時間を短縮します。 → 可視性と制御性を高めます。
移動中のデータにDLPとマルウェアスキャンを適用します。ウェブベースのアプリケーションや ウェブサイトからダウンロード・アップロードされた添付ファイルをスキャンし、マルウェアや機密データの有無を調べ、必要に応じて転送のログ記録や阻止を実行します。	→ ユーザーと企業SaaSアプリケーション間での転送中に、データ漏洩やマルウェア拡散を阻止します。
フィールドプログラマブルSASEロジック。リクエストメソッドの任意部分に基づき、HTTP（S）リクエストメソッドの監視とログ収集を実行し、必要に応じて阻止します。	→ アプリケーション使用をよりきめ細かく制御します。 → メッセージ投稿としての機密データのアップロードをブロックします。
選択したIaaSおよびSaaSストレージの保存データに対する DLPおよびマルウェアのスキャンを実行します。画像ファイルや画像のみのPDFファイルの履歴スキャンとOCRを サポートしています。	→ 選択したSaaSおよびIaaSにおけるデータ漏えいやマルウェア拡散を阻止します。 → 新たなファイルや古いファイルの更新がリバースプロキシを迂回した場合も機密データのスキャンが 可能です。
管理対象SaaSのファイルレベルを暗号化します。	→ データへのアクセスを完全に阻止することなく、データのプライバシーとデータ主権を確保します。
ログを使用して、企業のファイアウォールやプロキシからのシャドーITレポートを実行します。	→ エージェント不要で、オンプレミスデバイスから不正なアプリケーション使用を検出します。
フォワードプロキシモードで統合エージェントを使用したシャドーIT制御。	→ 企業が認可した代替手段の使用を推奨しながら、ユーザーが特定の管理対象外アプリにアクセスできないようにします。
管理対象SaaSトラフィックの詳細レポート。	→ 管理対象外デバイスからのアクセスも含め、管理対象SaaSアプリへのアクセスを完全に可視化します