

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します。
- すべての主要チャネル (CASB、SWG、電子メール、エンドポイント) に適用されるエンタープライズクラスのDLP、統合管理、ポリシー構成、報告機能を備えています。
- 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。
- シャドウ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、生成AIを含む企業が承認したSaaSアプリケーションの使用を最大限に可視化し、管理を提供します。業界をリードするData Loss Prevention (DLP)で機密データを保護しながら、詳細なアクセス管理とマルウェア保護を提供することで、現代の脅威から守ります。

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、シャドウ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。

Policy ID	Group	Access Method	Device	Location	Action
91432	CU Admin	Any	Any	Any	Direct App Access
11982	Any	Any	Any	Any	Secure App Access DLP Download DLP Upload
13014	Any	Any	Any	Any	Secure App Access DLP Download DLP Upload
22426	Any	Direct App	Managed Mob	Any	Secure App Access DLP Upload

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。複数のサードパーティ製のアンチマルウェアエンジンを搭載したマルウェアスキャンを呼び出すための予約データパターンもあります。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、ポルトレス暗号化、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を制御を実行できます。

Object Name	Primary Key	Field Name	Type	Max Length	Action	Security Level
PrimaryGroup	Key	string	40	None (Pls)		
	Index	string	400	Encrypt	AS	
	Contact	string	400	Encrypt	AS	

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が保護するアプリケーションへの機密データの移動、未承認のアプリケーションへの機密アップロード、管理されていないデバイスへの機密ダウンロード、上位グループやユーザーの機密データの移動など、Forcepointが識別した機密データの詳細が表示されません。

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。その代わりに、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、機密データのスクリー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クリーンが可能で

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API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。

ID	Condition	Action
17999	(User Group = All Scanned Users) AND (Data Pattern = PI-Confidential)	Allow Classify
111038	(User Group = All Scanned Users)	Allow
97493	(User Group = All Scanned Users) AND (Data Pattern = SecretData) AND (Path = /file/Name/Date)	Deny Notify External Stealing Generate Alert

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照合パターンは、プロキシポリシー全体で共有されるカスタムまたは事前定義された一致パターンのいずれかであることができ、機密データやマルウェアを統合的に管理できます。



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 CASBはForcepoint DLPと完全に統合して動作しますが、Internet Content Adaptation Protocol (ICAP) をサポートするオンプレミスDLPシステムでも動作します。これにより、ユーザーは、Forcepoint ONEが機密データを持っているとフラグを立てた管理対象SaaSまたはIaaSクラウドストレージ内の保存中のファイルを、TLS暗号化を使用してオンプレミスDLPシステムに送信できるようにします。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と対応 (SOAR)。**
Forcepoint ONE CASBは、Forcepoint ONEと選択したSOARプラットフォーム間の双方向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 CASBは、DLPマッチパターン内の任意のデータ分類子からの分類メタデータを使用できます。
- **エンドポイント管理。** SAMLログインプロセスの一環として、Forcepoint ONE CASBは、Windows、Mac、Android、iOSデバイスに保存された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で管理されていることを確認します。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 CASBの違い

- **最も広範なSaaS可視性:** 800,000以上のSaaSアプリケーションを構成する最大の既知データベースと、40以上の属性の評価によるリスク評価。
- **業界をリードするデータセキュリティ:** Forcepoint DLPポリシーをエンドポイント、ネットワーク、クラウド、Web、電子メールなどを問わずすべての主要チャネルに拡張することで、データがどこにあっても保護します。1700以上の事前定義済みテンプレート、ポリシー、分類子と組み合わせた単一のコンソールによる統合ポリシーの実施に役立ち、90カ国および150以上の地域の規制要件を満たすことができます。
- **SaaSアプリケーションのエージェントレスアクセス:** エージェントレスリバースプロキシ配備により、管理されていないデバイスからのあらゆるアプリケーションへの摩擦なくゼロトラストアクセスを提供します。BYODやサードパーティパートナーまたは請負業者のデバイスなどの管理されていないデバイスからのアクセスを保護します。
- **あらゆるアプリケーション管理:** Field Programmable SASE Logic (FPSL) を使用した拡張可能な制御で、一般的でないアプリケーションやカスタムアプリケーションを含むあらゆるWebベースのアプリケーションを管理します。これにより、企業アカウントと個人アカウントを区別するシンプルなログイン管理、ユーザーが外部でファイルを共有するのを防止するなどのクラウドサービスごとにより洗練された特定の管理など、標準で利用できないユースケースが無制限に開きます。

* Forcepoint DLPとの統合には、別途のアドオンSKUが必要です。

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。	<ul style="list-style-type: none"> → 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。
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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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ケー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。	<ul style="list-style-type: none"> → 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。
CASBフォワードプロキシ用、非Webアプリケーション用ZTNA用に統合された単一のエージェント。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。	<ul style="list-style-type: none"> → 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。
Forcepoint DLP との統合により、クラウド、ネットワーク、エンドポイント、Web、電子メールなどのすべてのチャンネルで統合されたデータ保護ポリシーを適用します。*	<ul style="list-style-type: none"> → 複雑さを減らし、価値実現までの時間を短縮します。 → データの可視性と制御を強化します。
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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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。	<ul style="list-style-type: none"> → 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。

* Forcepoint DLPおよびRisk-Adaptive Protectionの統合には、別途のアドオンSKUが必要です。

forcepoint.com/contact