Forcepoint

データシート

Forcepoint ONE

主な利点：

- 2015年以来、99.99%の稼働率を確認済み
- 自動スケーリングによる遅延最小化&スループット最大化
- SAML互換のIdPとのフレキシブルな統合
- 統合管理コンソール
- AD同期エージェントまたはSCIMプロビジョニングによるユーザーオンボードの加速
- AJAX-VMを使用したリバースプロキシにより、オンデバイスエージェントなしであらゆる管理対象ウェブアプリケーションを保護
- 動作中のデータをスキャンし、ユーザーとウェブアプリケーション間のマルウェアやデータ流出をブロック
- 保管中のデータをスキャンし、マルウェアを隔離して多くの一般的SaaSおよびIaaSストレージ製品における危険データ共有を制御
- SaaSおよびIaaSの構造化・非構造化データを暗号化し、データプライバシーを確保
- 特定の HTTP/S リクエスト メソッドをブロックする機能により、SaaS またはプライベート Web アプリケーションとのユーザー インタラクションをきめ細かく制御

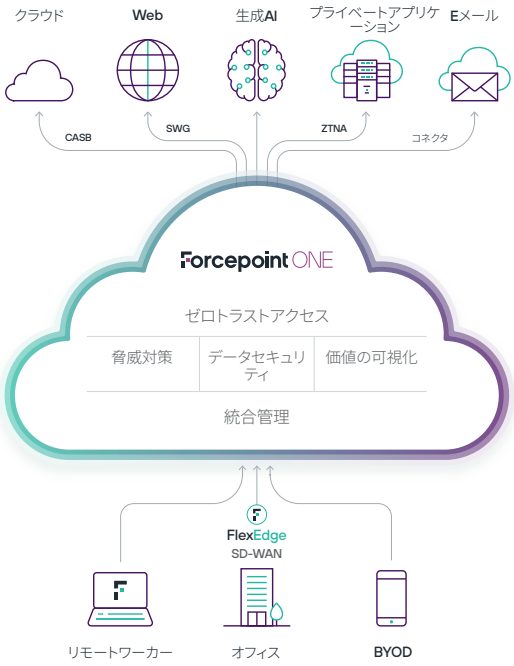
Forcepoint ONEは、変化し続けるリモート・ハイブリッド労働環境に迅速に適応しなければならない分散型企業や政府機関向けに、あらゆる場所のデータ保護を実行するクラウドサービスです。従業員、請負業者、その他のユーザーは、攻撃者を締め出し、機密データへの侵入を防ぎながら、ウェブ、クラウド（SaasおよびIaaS）、プライベートアプリケーション上のビジネス情報への制御されたアクセスを安全に実行できるようになります。その結果、リモートでもオフィスでも、Forcepoint ONEによりユーザーの生産性とビジネス効率が高まります。

Forcepoint ONEは、3つの安全なアクセスゲートウェイと、多様な共有脅威保護およびデータセキュリティサービスを含むZero Trustと、SASEセキュリティ技術を結合し、すべてクラウドネイティブプラットフォームに構築した。このアプローチにより、組織はすべてのチャネルで統合ポリシーを管理し、脅威や機密データを排除できます。

→ **Webセキュリティ。**カテゴリとリスクスコアに基づくWebサイトへのアクセスのブロック、マルウェアのダウンロードのブロック、機密データのアップロードのブロック、シャドウITの検出と制御など、あらゆるWebサイトとのあらゆるやり取りを監視および制御します。

→ **Cloud Access Security Broker (CASB)。**ID、ロケーション、デバイス、グループに基づき、企業のSaaSアプリに対してきめ細かいアクセス制御を適用するエージェントベースまたはエージェントレスのソリューションです。プライベートアプリケーションに対しては、リアルタイムできめ細かなアクセス制御を実行します。一般的なSaaSやIaaSの保管データをスキャンし、マルウェアや機密データを検出し、必要に応じて修復します。エージェントレス・オプションを使用すれば、BYODや請負業者とのアクセスが容易になります。

→ **Zero Trust Network Access (ZTNA)。**エージェントベースまたはエージェントレスのソリューションにより、VPNを使用せずにプライベートアプリケーションへのきめ細かなアクセスが可能になります。非HTTP（S）アプリケーションにはエージェントベースのソリューションが必要です。



3つのゲートウェイ全てに共通する機能は以下の通りです。

- → **コンテキストアクセス制御Web、**クラウド、またはプライベート アプリケーションへのアクセスは、デバイス の種類、デバイスの状態、ユーザの動作行動、およびユーザ グループに基づいて制御されます。
- → **Data Loss Prevention (DLP)。**ファイルとテキストは、重要なデータのアップロードとダウンロード時にスキャンされ、必要に応じてブロック、追跡、暗号化、または修正されます。190を超えるDLPルールが事前に定義されているため、法令順守の合理化と迅速な価値実現に役立ちます。Forcepointとの容易な統合 Enterprise DLP は、エンドポイント、ネットワーク、Web、クラウドサービスなど、あらゆる場所でデータセキュリティを実現します。
- → **マルウェアスキャン。**ファイルのアップロード・ダウンロード時にマルウェアをスキャンし、検出時はブロックします。
- → **統合管理コンソール。**設定、監視、レポート作成に。
- → **Insights。**カスタマイズ可能なウィジェットと視覚化を備えたセキュリティ分析ダッシュボードが、経済価値評価など、セキュリティ体制の経時的影響を表示します。
- → **オンデバイスエージェント。**WindowsとmacOSの場合。
- → **99.99%のサービス稼働率。**

Forcepoint ONEには、以下のアドオン機能も含まれます。

- → **クラウドセキュリティ体制管理（CSPM）。**AWS、Azure、GCPテナント設定をスキャンし、リスクのある構成を検出し、手動・自動による修復を実行します。
- → **SaaSセキュリティ体制管理（SSPM）。**Salesforce、ServiceNow、Office 365テナント設定をスキャンし、リスクのある構成を検出し、手動・自動による修復を実行します。
- → **統合 Content Disemble Reconstruction（CDR; コンテンツの無害化と再構築）を使用したリモート ブラウザ分離（RBI）。**ユーザーは、クラウドホスティングされたVMでブラウザを実行することにより、ローカルデバイス上のWebベースのマルウェアから保護されます。CDRを使用すると、組み込みのマルウェアからドキュメントおよびイメージのダウンロードを削除し、再構築することができます。ユーザーが開く前に これには、ステガノグラフィを使用してイメージファイルに埋め込まれたマルウェアの削除が含まれます。
- → **Forcepoint分類。**AIを活用した提案を行い、タグ付け精度を高めるデータ分類を実行します。
- → **高度なマルウェア検出および防止 (AMDP)**。制御されたマルウェアサンドボックス内のファイルの動作を分析し、非表示および悪意のあるコンテンツを特定します。

Forcepoint ONEの機能とメリット

範囲	特徴	利点
プラットフォーム全体	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です。 → 保存データの高速スキャン：アプリケーションテナントのコンテンツ全体をスキャンする場合、従来のように数日かかることなく、数時間で作業が完了します。
	SAML互換のIdPとの統合。SAMLリレーまたはACSプロキシモード。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。
	SCIMの統合。現在のAzure 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Azure AD テナント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。
	コンテクスチュアル・アクセス制御。ユーザーグループ、デバイスタイプ、ロケーション、時刻に基づき、ユーザーにForcepoint ONEへのアクセスを許可します。オプション：「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。	→ 不審なログイン試行を検知・ブロックし、盗まれたパスワードに関連するリスクを軽減します。 → アクセスをきめ細かく制御し、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。
	非 Web アプリケーションの SWG、CASB 転送プロキシ、および ZTNA に対するエージェントベースのサポート。	→ エージェント展開を簡素化します（選択されたMDMシステム経由の展開を含む）。 → 低CPU・低メモリ使用。 → 自動ローテーションにより自己生成される証明書でセキュリティを確保し、ITオーバーヘッドを削減します。
	すべてのアプリケーション、ユーザ、およびデバイスにわたるすべてのシステム機能を管理する統合管理コンソール。	→ 統合コンソールにより、複雑さと価値を実現するまでの時間が短縮され、可視性と制御性が向上します。
	Insights使用により、カスタマイズ可能なウィジェットと視覚化を備えたセキュリティ分析ダッシュボードが、経済価値評価など、セキュリティ体制の経時的影響を表示します。	→ 時間の経過と共にリスクを測定し、セキュリティ体制を強化します。 → クラウドセキュリティ・プラットフォームの経済的影響を推定します。
ウェブベースアプリ向けのCASB、SWG、ZTNA	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がないか検証します。ログ収集、ブロック（SWGだけのオプション）、隔離、暗号化、DRMの適用、透かしやファイル追跡の適用など、適切な修復アクションを実行します。Forcepoint Enterprise DLPと簡単に統合でき、エンドポイント、ネットワーク、ウェブ、クラウドサービスなど、あらゆる場所にデータセキュリティを提供します。	→ ユーザーと任意のウェブアプリケーションまたはウェブサイト間で転送中のデータ漏洩やマルウェアの拡散リスクを軽減します。 → Enterprise DLPポリシーをSSEチャネルに簡単に拡張します。
	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、必要に応じてブロックします。	→ 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。
	Forcepoint ThreatSeekerは、複数のスキャンエンジンを使用し、マルウェア、フィッシング攻撃、ランサムウェアなどの最新の脅威トレンドをリアルタイムで可視化するクラウドベースのセキュリティインテリジェンス・ネットワークを提供します。	→ 年中無休で稼働する自動システムが、世界中のForcepointソリューションに脅威インテリジェンスを配信し、進化する脅威からデータとアプリケーションを保護します。
ウェブベースアプリケーション向けのCASBとZTNA	AJAX-VMによるエージェントレス・リバースプロキシ。リバースプロキシは、コアPOPとエッジPOPで実行されるソフトウェアです。AJAX-VMは、エンドユーザーのブラウザ内で実行されるJava Script抽象化レイヤーです。Forcepoint ONEはこの二機能を連携させ、任意デバイスと管理対象ウェブアプリケーション間のトラフィック管理を実行します。エージェントソフトウェアをデバイス上で稼働させる必要はありません。	→ あらゆるウェブベースのアプリケーションで動作します（その他のリバースプロキシソリューションではサポートできないロングテールアプリケーションやカスタムアプリケーションも含まれます）。 → BYODや請負業者用のエージェント・インストールは不要です。 → エージェントレスDLPを提供します。 → 最新ブラウザに対応するあらゆるデバイスで動作します。

範囲	特徴	利点
SWG	監視、ログ、コントロールアクセス Forcepoint ONEリアルタイムスキャンエンジンを使用したDLPおよびマルウェアスキャンを使用する、企業のWindowsおよびMacエンドポイントからの任意のWebサイト。	→ 受け入れ可能な使用ポリシーを適用します。 → シャドウIT使用状況を監視します。 → URLディレクトリパスレベルのアクセス制御を実行します。 → あらゆるウェブサイトへの機密データアップロードをブロックします。あらゆるウェブサイトからのマルウェアダウンロードをブロックします。 → 分散施行アーキテクチャがForcepoint ONEバックプレーン経由のトラフィックを削減し、ワイヤスピードに近いスループットを実現します。
CASB	クラウド内の保管データに対するDLPとマルウェアスキャンを実行します。SaaSおよびIaaSストレージ内の構造化・非構造化データをスキャンしてマルウェアや機密データを検出してログを収集し、隔離、暗号化、パブリック共有の削除など、適切な保護措置を講じます。	→ 最近追加されたファイルだけでなく、履歴データのスキャンも実行します。 → 画像ファイルにOCRを適用し、機密テキストデータを検出します。機密データを含むファイルのパブリック共有をオフにします。クラウドに保存されたマルウェアを隔離します。 → 事前定義されたデータパターンの広範なライブラリにより、セットアップ時間が短縮されます。
	データ暗号化。管理対象のSaaSおよびIaaS内の機密構造化データと非構造化データを暗号化します。	→ 機密データが許可されたユーザーのみに表示されるようにします。
	シャドーITの検出と制御。	→ 企業のファイアウォールとプロキシサーバーからログを収集し、シャドーITの使用を検出します。 → 企業が承認した代替手段を推奨するコーチングメッセージを提供しながら、シャドーITアプリケーションのユーザー使用をブロックします。
CSPM	クラウドセキュリティ体制管理。さまざまな業界や地域のベースラインとカスタムベースラインに従い、AWS、GCP、Azure管理者コンソールSaaSのセキュリティ設定構成をスキャンします。.	→ 修復のため、リスクのある設定にフラグを立てます。必要に応じ、ワンクリック修復または自動修復を適用します。
SSPM	SaaSセキュリティ体制の管理。さまざまな業界や地域のベースラインとカスタムベースラインに従い、一般的なSaaSテナントのセキュリティ設定構成をスキャンします。	→ 修復のため、リスクのある設定にフラグを立てます。必要に応じ、ワンクリック修復または自動修復を適用します。
AMDP	SWG を補完して、サンドボックス環境内のファイルの動作を分析し、マルウェアを検出および防止します。	→ マルウェアとランサムウェアのダウンロードに対する保護。
RBIとCDR	コンテンツの無害化と再構築によるリモートブラウザ分離Forcepoint ONE Web Securityには、「未分類」および「新規登録」サイトの「必須」レベルのRBIが付属しており、RBIのオプションライセンスを使用して拡張することで、より多くのWebカテゴリをカバーすることができます。クラウドホスティングされたVMでブラウザを実行し、エンドユーザーデバイスをWebベースのマルウェアのリスクから切り離すことで、抽象化の層を提供します。ユーザーがドキュメントをあるいはイメージファイルをダウンロードするとき、ファイルから有効なビジネス情報を抽出し、抽出した情報が適切に構成されていることを確認し、その情報を目的地に運ぶための新しいファイルを構築するCDRを適用する。	→ Web閲覧において、いつもと変わらないエクスペリエンスを提供。 → Google Workspaceのような最新のクラウドアプリケーションから従来の技術の上に構築されたスイートまで、広範なウェブロケーションにレンダリング機能を提供します。 → 機密性の高いWebアプリデータをBYODのブラウザキャッシュに含めず、ウェブサイトのデータ共有機能を制限し、市場をリードするDLPと統合します。 → CDRで処理されたファイルには、マルウェアは含まれません。これには、情報隠蔽技術使用の画像ファイルに埋め込まれたマルウェアの削除も含まれます。