SecureSphere

機能詳細

SecureSphere の主な機能

（カッコ内は実装対象アプライアンス）

1. ダイナミックプロファイリング（WAF/DAM/DBF）
2. Web/XML/DBファイアウォール（WAF/DBF）
3. ThreatRadar: ゼロディ攻撃・ボット攻撃の防御と、ログインアカウントの不正利用対策（WAF）
4. データベース監査（DAM/DBF）
5. SecureSphere DAM/DBF データベース監査機能
10. データベース監査（DAM/DBF）
11. 相関攻撃検証（WAF/DAM/DBF）
12. IPS (Intrusion Prevention System：侵入防止システム)（WAF/DBF）
13. マネジメント&レポーティング（共通機能）
14. 配備設定オプション（共通機能）

SecureSphere ラインナップ別機能

	SecureSphere **WAF**	SecureSphere **DAM / DBF**
ダイナミック Web・XML ファイアウォール	○	n/a
ThreatRadar (ゼロディ攻撃防御)	○	n/a
データベース 検出・脆弱性検査	n/a	○
データベース アクセス・レスポンス 監査	n/a	○
ダイナミック データベースファイアウォール	n/a	○（DBFのみ）
攻撃・脆弱性 シグネチャ検知	○	○
相関攻撃検証	○	○
IPS (NW ファイアウォール)	○	○
IPS (HTTP プロトコル アノマリ)	○	n/a
IPS (SQL プロトコル アノマリ)	n/a	○
エンドポイント マルウェア対策との連携	n/a	○

ダイナミックプロファイリング

WAF DAM DBF

ダイナミックプロファイリングは SecureSphere の核となる機能であり、変化するアプリケーション環境に自動的に対応します。ダイナミックプロファイリングはアプリケーションの構成、および正常なふるまいをプロファイルとして構築するために、SecureSphere 導入後直ちにユーザと、Web/データベース間すべての通信を自動的にモニタリングします。

SecureSphere は実際のトラフィックとプロファイルの比較により、潜在的に悪意のあるどんな種類の行為も識別し防御します。

プロファイルは継続的な学習アルゴリズムにより、アプリケーションの変更を自動的に検知でき、手動による調整や設定を最小限に抑えます。この継続的にアップデートされるダイナミックプロファイルを基に、すべてのサービス（Web/XML/DB ファイアウォール、IPS）を実行します。

IMPERVA SecureSphere

IPS	ダイナミック Web ファイアウォール	ダイナミック XML ファイアウォール	ダイナミック データベース ファイアウォール

ダイナミック プロファイル

Web/XML/DB ファイアウォール

WAF DBF

SecureSphere ゲートウェイのセキュリティコンポーネントとなる各種ダイナミックファイアウォールは、外部または企業内部からのWebサイト・データベースへの攻撃・侵害に対し、ダイナミックプロファイリング情報を用いて防御します。

ダイナミック Web ファイアウォール

ダイナミック Web ファイアウォールは、ダイナミックプロファイルに含まれた正当なURL、HTTP メソッド、パラメータ、クッキー、レスポンスコードおよびHiddenフィールドといった、ユニークなWeb構成要素にフォーカスすることにより、Webアプリケーションを攻撃から保護します。プロファイルには、HTTPリクエストおよびHTTPレスポンス情報が含まれます。オープンWebアプリケーションセキュリティプロジェクト(OWASP) で最も重大な攻撃としてあげられるWebアプリケーションの脆弱性をターゲットとした攻撃であっても、ユーザとWebサーバ間の正常な相互通信を詳述したプロファイルを用いて防御します。

対象プロトコル：HTTP・HTTPS

ダイナミック XML ファイアウォール

ダイナミックXMLファイアウォールは、正当なXML URL、SOAPアクション、XML要素といった、ユニークなXML構成要素にフォーカスすることにより、XMLの脆弱性を利用した攻撃からWebを保護します。

対象プロトコル：XML・SOAP・WSDL

ダイナミック データベース ファイアウォール

ダイナミック データベース ファイアウォールは、正当なSQLクエリ、SQLクエリ毎の有効な送信元IPアドレス、SQLクエリ毎の有効なユーザ名といったユニークなSQL構成要素にフォーカスすることにより、データベースを攻撃から保護します。さらに、Webサーバを経由した攻撃だけでなく、企業内部からの不正なリクエストを含む様々な不正データベースクエリを検知し、内部からのデータベース侵害も防御します。また、監査のためにデータベースアクセスをすべて記録するか、特定のクエリだけを記録するかを定義することができます。

対象リレーショナル データベース	対象ビッグデータ ディストリビューション
Oracle, MS-SQL, DB2, Sybase ASE, Sybase IQ, MySQL, PostgreSQL, Informix, Teradata, Netezza, IMS, Progress OpenEdge, Maria DB, SAP HANA, Pivotal Greenplum	Hadoop, MongoDB, Cassandra DataStax

IMPERVA SecureSphere

IPS	ダイナミック Web ファイアウォール	ダイナミック XML ファイアウォール	ダイナミック データベース ファイアウォール

ダイナミック プロファイル

（注）WAF には DBファイアウォール機能はありません。DBF には Web/XML ファイアウォール機能はありません。

ThreatRadar　ゼロディ攻撃・ボット攻撃の防御と、ログインアカウントの不正利用対策

WAF

ThreatRadarは、Webアプリケーションファイアウォール（WAF）のユニークな追加セキュリティサービスです。ThreatRadarは、ボットネットのような大規模で、自動化された攻撃に対し自動防御機能を提供します。Imperva社はグローバルに攻撃元を追跡し随時WAFに既知の攻撃元IPリストを分配します。一旦SecureSphere WAFが既知の攻撃元IPリストを得ればThreatRadarは攻撃が始められる前に、悪意のあるトラフィックに対しアラートを発生しブロックすることができます。

また、インターネット上に流れるWebトラフィック全体の60%以上がボットによる通信であり、さらにそのほとんどが悪質な通信であることが確認されている現状を踏まえ、ThreatRadarはWebサイトへの通信を自動解析します。「人による正規・悪意な通信」、「無害・悪意なボットによる通信」を判定するエンジンを利用することで、未知・既知のボット対策を実現できます。

さらに、ThreatRadarは、90ヶ国以上に導入されている全世界の SecureSphere WAF ユーザにおいて検知された攻撃通信をImperva社のThreatRadarサーバにて情報収集・集計することで、ランキング上位に該当する攻撃の送信元IPリストをThreatRadarユーザに提供します。この情報を基にして、企業は他のWebサイトを攻撃したアウトローによる自社Webサイトへのアクセスを排除することができます。ThreatRadarは、多数の脅威に対し正確で最新の保護を提供します。

コメントスパムリスト
Comment Spam IP

ブログ、フォーラム、掲示板などのWebサイトに悪質なスパムメッセージを書き込んでいる送信元IPリストをブロックすることで、Webサーバへの通信負荷を軽減します。

悪意のある送信元リスト
Malicious IP

他のアプリケーション上で繰り返し悪意のある活動を行なっている送信元IP。これまでに、1000万以上のボットネットがリモート操作するハッカーの代わりに攻撃を実行しました。

Anonymousプロキシ/TOR IP リスト
Anonymous Proxy / TOR IP

実際の攻撃送信元を隠すために、ハッカーはAnonymousプロキシや、TOR IPをよく利用します。

フィッシングURL
Phishing URL

フィッシングをホストしているノードからの通信をブロックすることで、フィッシング サイトの出現を早期に発見することができます。
また、フィッシングサイトにオリジナルコンテンツが使われないよう、未然の対策が可能となります。

国別アクセス制御
IP GeoLocation

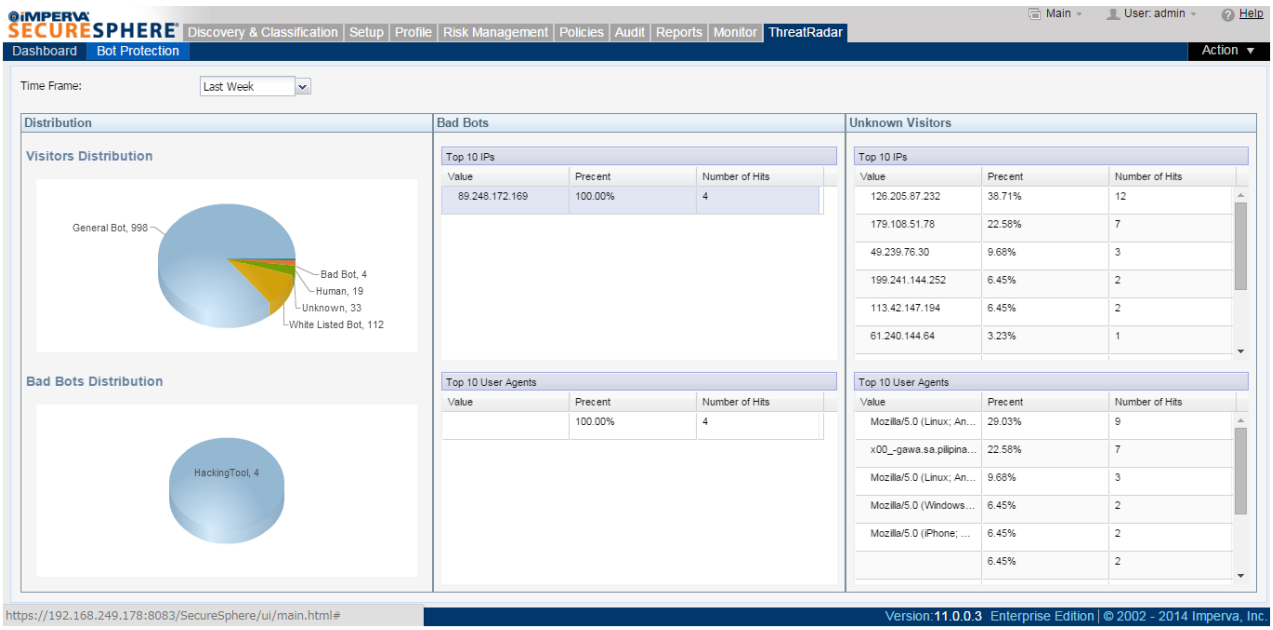
送信元からの通信許可・制御を、国単位で指定することができます。Webサイトの特性に応じて設定することで、不要なトラフィック削減を実現します。

ボット防御
Bot Protection

Webサイトへの訪問者を分類する独自のエンジンが自動的に通信を解析し、人とボットを判別します。また、二要素認証の役割を果たす CAPTCHA をログインページに表示する機能を利用することで、より精度の高い本人確認が可能となります。

ゼロディ対策用緊急シグネチャ
Emergency Feed

世界的に危険度・緊急性の高い、新たな脆弱性が発見された場合に迅速対応するカスタムシグネチャです。これは、Imperva 社のアプリケーションディフェンスセンター（ADC）による公式なシグネチャに先行して、ThreatRadar サービス利用者に提供されます。



データベース 監査

DAM DBF

データベースアクティビティの全詳細を完全キャプチャ

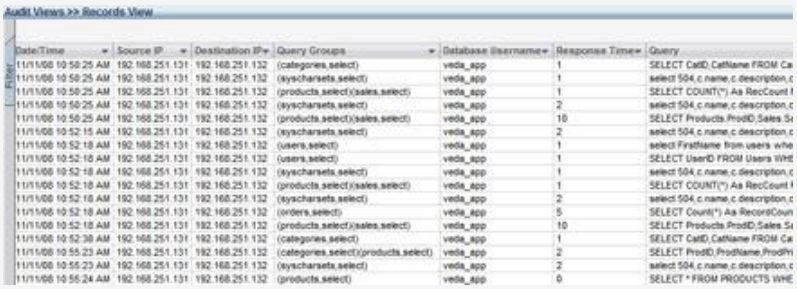
従来のデータベース監査・ファイアウォール製品は、トランザクション数が多くなると簡単には対処できなくなり、一定時間内にカスタマテーブルが10回読まれた、などといったデータベースアクティビティの集計データしか記録できなくなります。それに対しSecureSphereは、セキュリティチームおよび監査チーム両方の要求に応えるべく、どんなに大きくそして使用頻度の高いデータベースであっても、クエリレベルに至るまでのあらゆるデータベースアクティビティを完全かつ詳細に記録し、不正なアクティビティに対して、アラートを発報したり、アクセスを遮断します。

データベース フルレスポンス監査

アクセスだけでなく、レスポンス（実際に閲覧されたデータ）を完全記録

ローカルデータベースアクセス（DBA）の監視

SecureSphere専用モニタエージェントにより、ローカルコンソールからのアクセスや通信系路上、暗号化されたデータベースアクセスも監視・ブロックが可能



対象リレーショナルデータベース

Oracle, MS-SQL, DB2, Sybase ASE, Sybase IQ, MySQL, PostgreSQL, Informix, Teradata, Netezza, IMS, Progress OpenEdge, Maria DB, SAP HANA, Pivotal Greenplum

対象ビッグデータディストリビューション

Hadoop, MongoDB, Cassandra DataStax

SecureSphere DAM/DBF データベース監査機能

	リレーショナルデータベース RDBMS	ビッグデータ Big Data
対象データベース	**DB2 LUW** **DB2 for i** **DB2 for z/OS** **IMS for z/OS** **Informix** **Maria DB** **MS-SQL** **MySQL** **Netezza** **Oracle** **Pivotal Greenplum** **PostgreSQL** **Progress OpenEdge** **SAP HANA** **Sybase Anywhere** **Sybase ASE** **Sybase IQ** **Teradata**	Cassandra DataStax Hadoop Cloudera Hadoop Hortonworks Hadoop IBM BigInsights MongoDB
日時の記録	ログイン、ログアウト、SQL実行の操作日時を記録	
ユーザ情報の記録	DBユーザ名、送信元OSユーザ名、送信元アプリケーション、送信元ホスト名、送信元IP、ソースURL、 Webアプリ ユーザ名、Webクライアント IP、 Web セッションID	
操作対象データベース情報の記録	データベースのIP、データベース名、スキーマ名、テーブル名、カラム名	
記録対象オペレーション	ログイン、ログアウト、すべてのSQLオペレーション （DML、DDL、DCL、ストアドプロシージャ）、オペレーションの成功/失敗、 ローカルDBアクセス（エージェント導入必要）	
クエリの記録	クエリ全文、クエリグループ、レスポンス内容全文、レスポンスレコード件数、レスポンスタイム、バインド変数、 影響を与えた件数（更新や削除された件数）	

IPS Intrusion Prevention System : 侵入防止システム

WAF DBF

SecureSphereのIPSは、既知ワームとネットワークレベルの脅威からWeb/DB サーバの領域全体を保護します。IPSはネットワークファイアウォール、シグネチャ検出、WebプロトコルアノマリおよびSQLプロトコルアノマリの検査機能を含みます。

ネットワーク ファイアウォール

SecureSphereのネットワーク ファイアウォールは、防御されたネットワークセグメントへ入出するトラフィックに対するネットワークレイヤアクセスコントロールを提供します。Telnet、市販のリモートツールあるいはSQLといった危険なプロトコルを介して、内部のユーザが重要なサーバに不当にアクセスすることを防止できるように、ホワイトリストまたはブラックリストによる設定をサポートしています。ファイアウォール外または内部ユーザのデスクトップから、不要のポートを介してプロテクトされたネットワークセグメントへワームが蔓延することを防止することで、包括的なワーム防御においても重要な役割を担っています。

シグネチャ検知

SecureSphereは8,000を超えるシグネチャを有し、Webアプリケーション、各インフラソフトウェア(Apache、IIS、Oracleなど)、OSの既知の脆弱性をターゲットにしたWebアプリケーション攻撃、ワームおよびネットワーク攻撃から各監視対象サーバを保護します。シグネチャは、影響を受けるシステム、リスク、正確さ、頻度などの属性を、Imperva社のアプリケーションディフェンスセンター（ADC）からの情報で追加しています。SecureSphereのシグネチャ管理ウィザードを使用することで、ユーザは簡単にシグネチャディクショナリを作成することができます。シグネチャはすべてインターネット経由で自動的に更新されます。

HTTPプロトコル アノマリ

SecureSphereのプロトコル アノマリチェックは、HTTPプロトコルがRFCで要求された仕様に適合していることを確認します。例えば、不正なURL、異常に長いURL、異常に長いリクエストヘッダ、およびその他多くのプロトコル アノマリをチェックすることが可能です。HTTPプロトコルがRFCに準拠しているか確認することにより、Webサーバの脆弱性に対するワーム攻撃を防御します。

SQLプロトコル アノマリ

SQLプロトコル アノマリはSecureSphereシステムの独自機能です。攻撃者がデータベースにおける不適当なフィールド長、パラメータ値、規則に反する名前あるいはストリングを含んだ悪意のあるSQLリクエストを送る場合、SecureSphereはアラートを発報したり、リクエストを遮断します。

IMPERVA SecureSphere

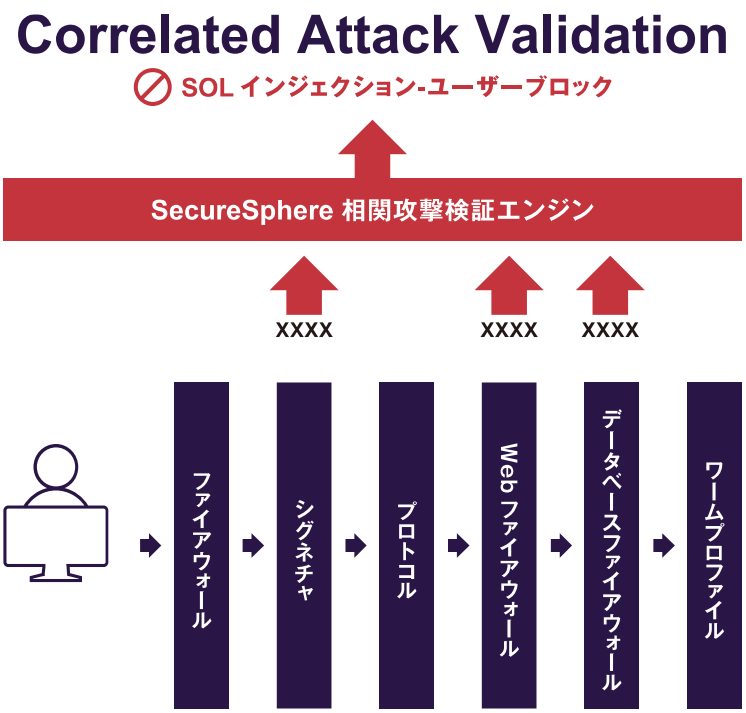
IPS	ダイナミック Web ファイアウォール	ダイナミック XML ファイアウォール	ダイナミック データベース ファイアウォール

ダイナミック プロファイル

相関攻撃検証

WAF DAM DBF

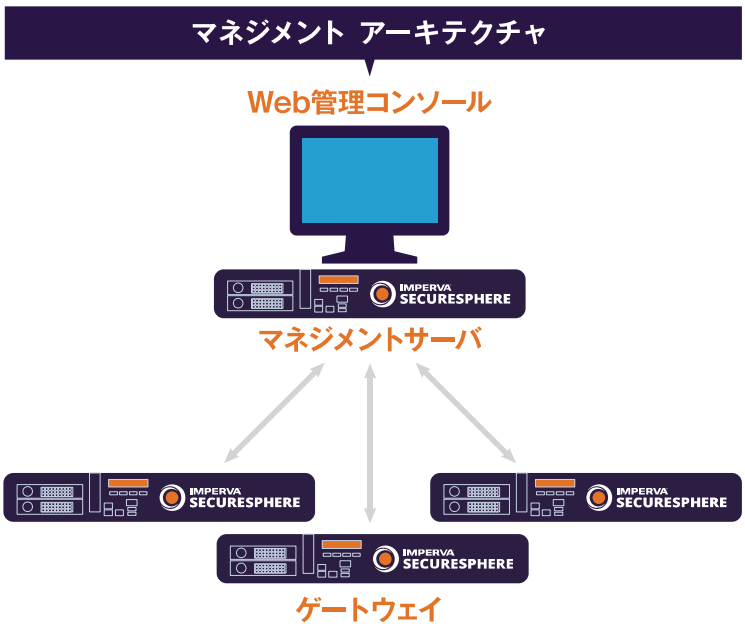
SecureSphereの相関攻撃検証エンジンは、複数のSecureSphereセキュリティサービス（ダイナミック Web ファイアウォール、ダイナミック データベース ファイアウォール、シグネチャなど）を通してクライアントユーザの行為を追跡し、イベント同士の関連を監視検証することで、ハッカー活動かどうかを識別します。例えば、もしIPSがシグネチャによりURL中の“union”という単語を検知した場合、それはSQLインジェクション攻撃を示すものかもしれませんが、単にWebサイト内の単語結合の正常処理かもしれません。しかし同じパケットが、ダイナミック Web ファイアウォール違反（“union”が通常のアプリケーション機能ではない）と、ダイナミック データベース ファイアウォール違反（異常なデータベースクエリ）の両方を引き起こす場合、相関攻撃検証は攻撃と判断しトラフィックを止めます。相関攻撃検証は、単一のイベントではなく複数の監視による違反処理に基づき、複雑で精巧な攻撃も正確に検知し防御します。



マネジメント&レポーティング　共通機能

SecureSphere MX マネジメントサーバは「Web管理コンソール」「マネジメントサーバ」「ゲートウェイ」の3層構造の管理アーキテクチャにより、複数のSecureSphereゲートウェイを同時に管理することができます。3層構造の中心に位置する MX マネジメントサーバは、一元管理しているプロファイルおよびポリシー情報を、企業全体に展開する各ゲートウェイに容易に配信することができます。

各ゲートウェイで生成されたアラート、ログ、グラフィカルレポートデータは自動的に MX マネジメントサーバで収集され、管理者へコンソール画面で提供されます。ログとイベントは、ユーザに定義されたパラメータに基づいた組織またはグループによるロールベースの管理も可能です。統合されたグラフィカルレポーティングツールは、カスタムレポートを作成し、傾向分析、監査、実行の意思決定などをサポートします。



配備設定オプション　共通機能

SecureSphere ゲートウェイはすべてのユーザの要求を満たすために、インライン/フェールオープン、インライン/HA（ハイアベイラビリティ）、スニファモードなど多くの配置オプションを提供します。また、インライン配置の場合、トランスペアレントブリッジモード、リバースプロキシモードを用意することで組織のニーズに柔軟に対応することが可能です。スニファモードの場合、ネットワークの停止時間や導入の失敗がなく、容易にゲートウェイを配置することが可能です。また、スニファモードでのブロッキング機能は、ゲートウェイによるTCPリセットが可能です。インライン/フェールオープンモードは、導入の失敗および冗長化システムのコストや複雑さを気にすることなく導入することが可能です。

インライン/HA（ハイアベイラビリティ）モードでは、アプリケーションを保護するだけでなく、十分なセキュリティ保護が常に維持されることを保証する、冗長化されたSecureSphereシステムの配備を可能にします。プライマリSecureSphereがダウン等を起こした場合、すべてのセキュリティ操作がバックアップSecureSphereシステムに切り換えられます。