CloudSOC™
Security for SaaS

Symantec

Symantec CloudSOC は、安心してクラウドアプリを利用できるように企業を保護します。

データを保護

従業員は、機密性の高い会社の情報を Office 365、Google、Box、Dropbox、Salesforce などの許可されたクラウドアプリケーションに保存し、共有します。このようなデータを、過失または故意による情報漏えいから保護します。

脅威を防御

クラウドアプリのアカウントは、多くの場合、インターネットから直接アクセスできます。このようなアカウントは、悪意を持つ人物やマルウェアの標的となります。クラウドアカウントの侵害による影響から企業を保護します。

セキュリティインシデントに対応

セキュリティインシデントが発生した場合、クラウドのセキュリティイベントにすばやく対応するために必要な内容、日時、対象者、方法に関する情報を取得します。

規制コンプライアンスを維持

政府機関や業界団体による法規制は、データプライバシーとセキュリティを維持するために、リスク分析、監視、システムの文書化を義務付けています。そのような要件を、使いやすいシステムで満たすことができます。

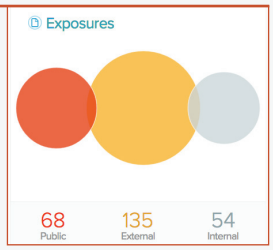
SaaS のためのセキュリティ

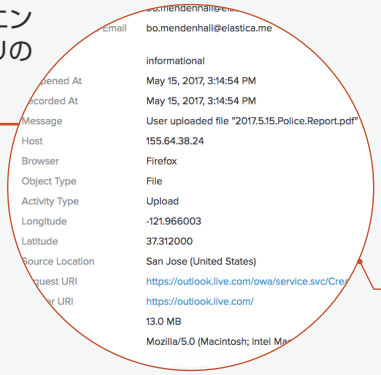
機密データを分類

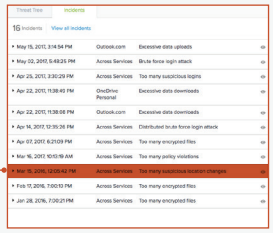
機械学習ベースの ContentIQ™ でクラウドアプリ内の機密データを自動的に分類および追跡し、コンプライアンス関連のデータ、機密データ、カスタムフォームのデータを高い精度で特定します。

リスクの高い共有の特定および修復

クラウド内のデータのブロック、コーチング、アラート生成、暗号化、共有解除、その他の方法での保護を実行できるポリシーでデータの漏えいを防止し、リスクを低減します。CloudSOC の ContentIQ DLP を使用するか、シマンテックエンタープライズ DLP を拡張して、クラウドアプリのデータを保護します。





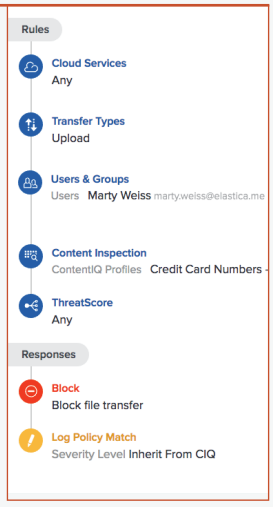


ユーザー活動を詳しく追跡

データサイエンスに基づく StreamIQ™ でクラウドとのトランザクションをきめ細かく検出し、可視化とポリシー制御の微調整を行います。このインライン機能により、許可されたアプリと未許可のアプリによるトランザクションを可視化し、予防的な制御を実現します。

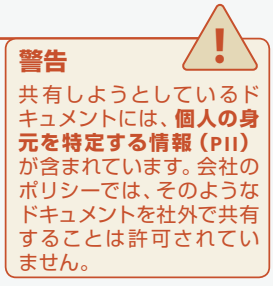
きめ細かいポリシーを適用して、データを保護

自動制御により、機密データの暗号化、ブロック、共有解除、適応型多要素認証のトリガーを行い、情報漏えいを防止します。アクション、オブジェクトタイプ、データ分類、ユーザー、ThreatScore™、アプリなどによって定義することで、きめ細かいポリシー制御を行います。



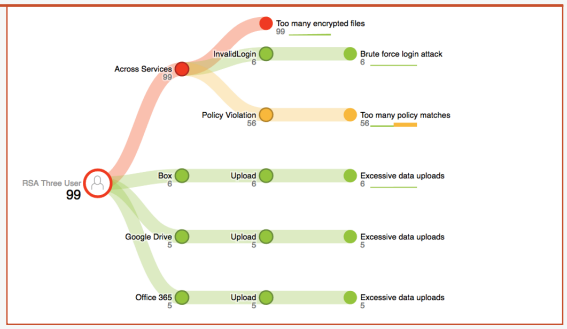
適切なクラウドの使用方法をユーザーに案内

ユーザーがリスクの高い行動をとろうとしたときにユーザーに自動的に警告し、セキュリティレスポンスのアクションを通知します。



ユーザーふるまい分析でクラウドアカウントを保護

ユーザーふるまい分析と、リスクの高い活動を行っているアカウントをブロック、検疫、またはアラートを生成する措置を自動的にトリガーできる数値化されたユーザー ThreatScore で、リスクの高いユーザー行動や、総当たり攻撃、ランサムウェアなどの悪質な活動を検出します。



SaaS のためのセキュリティ（続き）

クラウドでマルウェアを検出および緩和

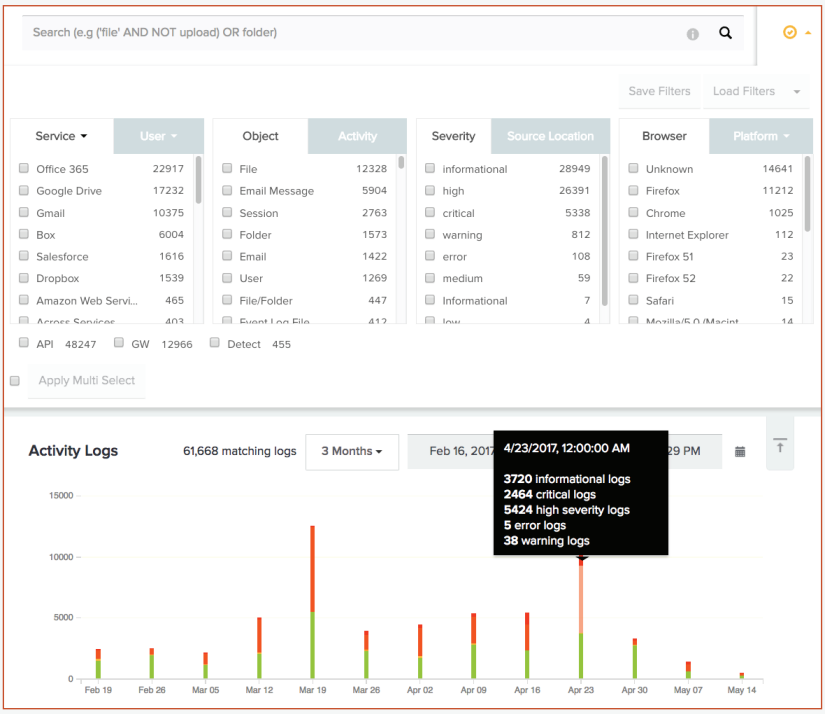
クラウドでのファイルインサイト、マルウェア対策、ファイル分析、サンドボックスを備えた、業界をリードするシマンテックの高度な保護により、クラウドアカウントに侵入するマルウェアから企業を保護します。

規制要件を遵守

CloudSOC のデータセキュリティ機能を使用して、PII、PHI、およびその他の規制対象データの特定、監視、暗号化を行い、データへのアクセスを制御します。地域のデータセンターを使用して地域内でデータを保管します。

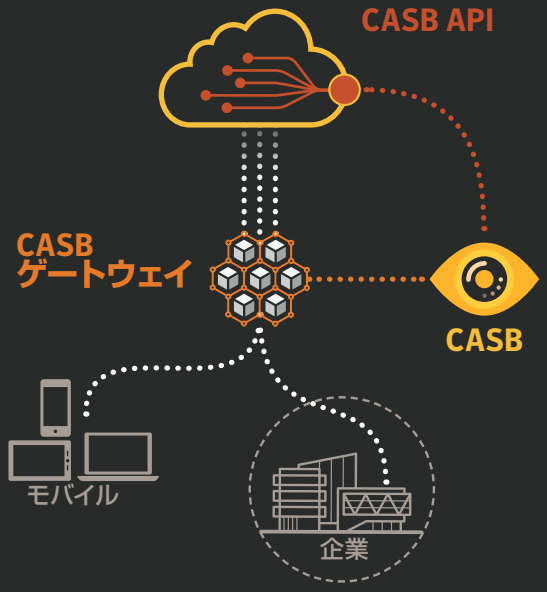
インシデントを調査し、すばやく対応

ユーザー、脅威、ポリシー、サービス活動の可視化によりセキュリティの問題を特定し、アクションをユーザー、アプリ、データに簡単に結び付けます。強力な検索とフィルタのオプションを使用して、コンテキストでログをすばやく見つけて確認し、CloudSOC から提供されるインテリジェンスを使用して SIEM 主導の調査を強化します。



Security for SaaS のしくみ

SaaS 用 CASB では、クラウドのデータと活動を監視することで、データを保護し、脅威から防御し、インシデント対応にインテリジェンスを提供します。CloudSOC では、API ベースの Securlets と CASB ゲートウェイを使用してクラウドの活動を監視し、機械学習に基づく高い精度の監視とポリシー制御を、見やすく使いやすいダッシュボードを通じて提供します。



SaaS のための高度なセキュリティ

API ベースでアプリ固有の Securlets により、許可された企業アカウントを保護

SaaS のためのプレミアムセキュリティ

API ベースでアプリ固有の Securlets により、許可された企業アカウントを保護

CASB ゲートウェイのアプリ固有の Gatelet で、任意のアカウントに関連するアプリ固有のトラフィックを保護

Office 365、Google G Suite、Box、Dropbox、Salesforce、GitHub、Jive、DocuSign、ServiceNow に対応しています。

Amazon Web Services と Microsoft Azure IaaS にも対応しています。

Symantec

主な機能

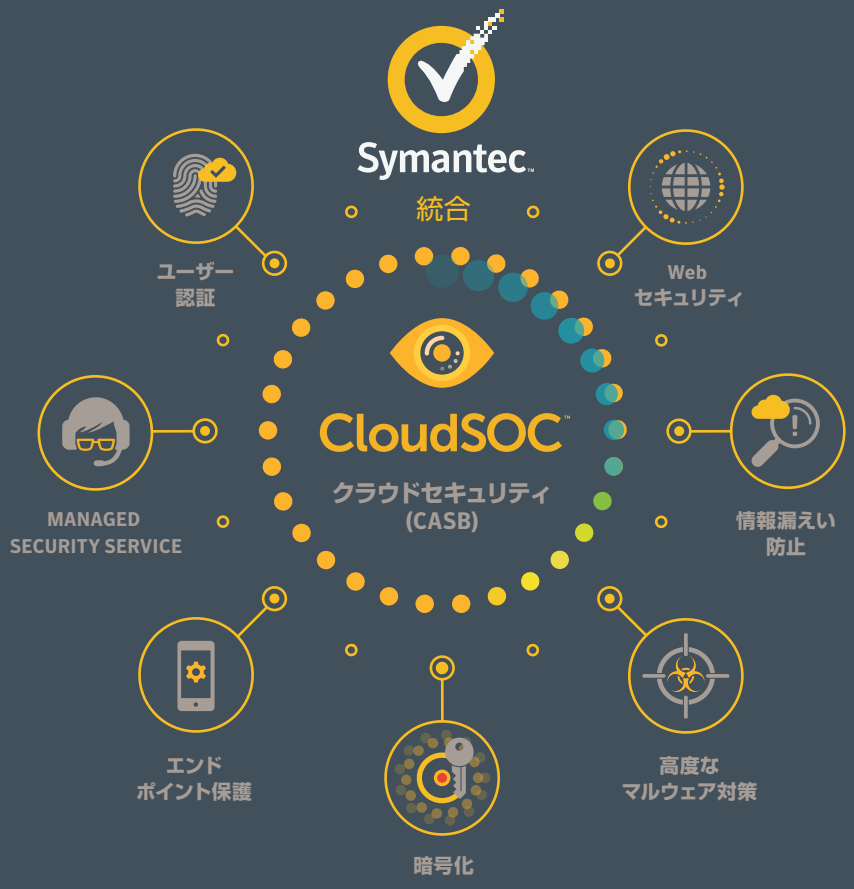
包括的なアプリ対応範囲	API の統合とインラインのトラフィック分析によって、Office 365、G Suite、Box、Dropbox、Salesforce、AWS、Azure などの許可された SaaS および IaaS プラットフォームの使用を監視および制御します。
ContentIQ™ DLP	ユーザー活動によって危険にさらされる PII、PCI、PHI、ソースコードなどの機密データを自動的に特定し、ポリシー制御を実行して情報漏えいを防止します。機械学習、カスタム辞書、事前定義済み辞書、学習されたカスタムフォームのプロファイルを利用して、高い精度の結果を達成します。
StreamIQ™ による活動監視	クラウドアプリとリアルタイムのクラウドアプリケーショントラフィックからイベントを抽出し、ユーザー、アクション、アプリ、ファイル、データ、デバイスなどの詳細なデータを提供します。独自のデータサイエンスに基づく技術により、多種多様なクラウドアプリケーションによるトランザクションを詳細に可視化できます。
ユーザー中心の ThreatScore™	CloudSOC のユーザーふるまい分析（UBA）は、StreamIQ と機械学習によるインテリジェンスを活用して、個別化されたユーザープロファイルの維持、ユーザーアクティビティのマッピング、そしてライブユーザーの ThreatScore 作成を自動的に行います。
ポリシーの適用	ThreatScore またはコンテンツの分類に基づいてきめ細かいコンテキスト認識型のポリシーを適用し、データの露出を防止し、アクセス、共有などのアプリ固有のアクションを制御します。
インシデント調査	分かりやすいインシデント事後分析ツールを使用して、クラウドでの活動履歴を詳細に分析できます。
高度な視覚化	使いやすいフィルタ、ピボットビュー、自由形式の検索、すぐに役立つコンテンツを使用して、目的の情報を詳しく調査できます。
コンプライアンスの実施	クラウドでの HIPAA、PCI、PII などの機密データの保存方法、共有方法、アクセス方法を制御するポリシーを適用します。統合された暗号化と多要素ユーザー認証で規制対象データを自動的に保護します。
容易な展開	CloudSOC は、企業に合わせてさまざまな展開オプションを用意しています。CloudSOC と統合された Symantec DLP、認証、暗号化、脅威防止、セキュア Web ゲートウェイソリューションとの間で、統合認証、統合エンドポイントオプション、プロキシチェーン、インテリジェンスの共有、統合ポリシー管理などを利用できます。

仕様

使いやすさと管理
ユーザー、ポリシー、脅威、サービス、違反、場所を監視する管理ダッシュボード
アプリ固有のダッシュボード
カスタマイズ可能なウィジェットでカスタマイズできるダッシュボード
新しいアプリの簡単なオンラインストアアクティブ化
RBAC
標準レポートとカスタムレポート
ユーザーとデバイスの配備、アクセス、制御
SAML ベースのシングルサインオンソリューション（Okta、Ping、ADFS、VIP など）
LDAP ベースのユーザーディレクトリ（Active Directory、UnboundID、Open Directory など）
モバイルアプリのサポートと MDM プラットフォームの相互運用性で、IPSec VPN トンネルを経由してクラウドトラフィックを管理
OPSWAT Gears ホストチェックでデバイスの管理とセキュリティ体制のチェックを行い、会社のデバイスと個人所有のデバイス両方からのアクセスを管理
データセキュリティと DLP
コンテンツタイプ: FERPA、GLBA、HIPAA、PCI、PII、ビジネス、コンピューティング、暗号鍵、設計、暗号化、エンジニアリング、医療、法関連、ソースコード
ファイル分類: アニメーション、コミュニケーション、データベース、パブリッシング、カプセル化、実行可能ファイル
ブラックリストとホワイトリストのコンテンツプロファイル
統合された Symantec DLP
暗号化と DRM: PGP によるシマンテックの暗号化、Cloud Data Protection、SafeNet
脅威検知
最もリスクの高いユーザー、インシデント、サービス、場所、重大度のダッシュボードビュー
リスクの高いユーザー行動と ThreatScore で構成される脅威マップの表示
ユーザー活動の概要と詳細ログ
ファイルレピュテーション、マルウェア検出、クラウドサンドボックスを備えた統合型 Symantec Cynic
ポリシーの適用
UBA ベースの ThreatScore、サービス、アクション、ユーザー、日付、時刻、リスク、ブラウザ、デバイス、場所、オブジェクト、コンテンツに基づくきめ細かいポリシー制御
導入前のポリシー影響分析
ポリシー主導の活動ログ
ポリシーのアクション: 管理者とユーザーへの通知、多要素認証、ブロック、検疫、ログアウト、リダイレクト、リーガルホールド、アクセスの監視と強制、データの露出、ファイル共有、および転送の制御を行うためのその他のクラウドアプリ固有のアクション
ログとデータ
ログを主体とした視覚化とグラフ
ブール検索ときめ細かいフィルタ: サーバー、ユーザー、オブジェクト、活動、重大度、場所、ブラウザ、プラットフォーム、デバイス、ソース
活動ログの概要: サービス、アクション、ユーザー、日付、時刻、リスク
詳細なログデータ: サービス、アクション、ユーザー、日付、時刻、リスク、ブラウザ、ポリシー、場所、オブジェクト、コンテンツ、URL、デバイスの詳細
SIEM のエクスポート形式: CEF、CSV、LEEF

セキュリティを強化すると同時に複雑さを軽減

既存のセキュリティインフラと統合されるクラウドセキュリティソリューションを導入します。シマンテックの CloudSOC ソリューションにより、セキュリティ対応範囲を拡大し、運用の複雑さを軽減し、最適なユーザーエクスペリエンスを実現できます。



Symantec CloudSOC CASB およびシマンテックエンタープライズセキュリティシステムとの業界をリードする統合の詳細については、**go.symantec.com/casb** をご覧ください。

CloudSOC の概要

Data Science Powered™ Symantec CloudSOC プラットフォームを利用することで、企業は安全性とコンプライアンスを確保しながら、クラウドアプリケーションやクラウドサービスを安心して活用できます。CloudSOC プラットフォームが備えている一連の機能は、シャドー IT の監査、侵入および脅威のリアルタイム検出、情報漏えいおよびコンプライアンス違反からの保護、インシデントの事後分析に使用できるアカウント活動履歴の調査など、クラウドアプリセキュリティのライフサイクル全体をカバーできます。

シマンテックについて

シマンテックコーポレーション（NASDAQ: SYMC）はサイバーセキュリティ業界をリードする世界的企業です。さまざまな場所に保管されている大切なデータを守るため、企業や政府機関、個人のお客様を支援しています。エンドポイントからクラウド、インフラまでを高度な攻撃から守るため、世界中の企業がシマンテックの戦略的統合ソリューションを選択しています。また、世界中で 5 千万以上の個人やご家庭が、自宅などで使用するデバイスそしてデジタルライフを守るために、ノートンと LifeLock 社の製品を使用しています。シマンテックのサイバーインテリジェンスネットワークは民間が運営するネットワークとしては世界最大規模を誇ります。このネットワークが、先進的な脅威をいち早く発見し、お客様を守ります。

詳しくは www.symantec.com/ja/jp をご覧ください。

Symantec

www.symantec.com/ja/jp/ 〒107-0052 東京都港区赤坂1-11-44 赤坂インターシティ