CylancePROTECT®

Cloud

クラウドを利用したサイランス製品

- **CylancePROTECT** 管理コンソール – グループやデバイスの管理、レポート、ダッシュボード、ワークフローの機能を提供する Web アプリケーション
- **CylancePROTECT Agent** - エンドポイントのデバイスにインストールされる軽量のエージェント。このエージェントはクラウドサービスと通信して次のことを行います。

1. ポリシーを取得
2. 脅威やホストに関する情報を送信
3. コンソールを通じて送信されたコマンドを受信
4. 脅威のサンプルをアップロード（オプション）
5. エージェントの更新プログラムをダウンロード

CylancePROTECT の管理コンソールとバックエンドサービスは、アマゾンウェブサービス（AWS）上にホストされています。AWS は高い可用性、拡張性、安全性を備えたサービスであるため、CylancePROTECT は従来のセキュリティ製品よりも容易に導入できます。サイランスのクラウドサービスを利用すると、お客様は以下の作業が不要になります。

1. 管理サーバー／コンソールを構築するための、ハードウェア／リソースの調達
2. 管理サーバーの可用性やパフォーマンスの監視
3. 管理サーバーへの更新プログラムの適用
4. 監査ログ、侵入テスト、脆弱性の修正などによる管理サーバーのセキュリティ確保
5. 必要に応じた管理サーバーの拡張や増強

データ制御、プライバシー、ポータビリティ

マルチテナント – サービスのデータベースとしては、Amazon Relational Database Service（RDS）を利用しています。Amazon RDS では、パッチの適用やデータベースのバックアップが自動的に行われるため、ポイントインタイムリカバリが可能となっています。データはテナントごとに共有して物理的に隔離することができます。また、データをサイズごとに共有して論理的に隔離したり拡張性を最適化したりすることもできます。ミッションクリティカルなシステム向けのマルチゾーン導入オプションを使用することで、高い可用性が確保されるほか、組み込みの自動フェールオーバー機能により、障害発生時にプライマリデータベースから同期的にレプリケートされたセカンダリデータベースへのフェールオーバーが自動的に実行されています。サイランスは AWS GovCloud での導入をサポートしています。また、追加料金をお支払いいただくことで、お客様専用のデータベースを提供いたします。

データセキュリティ - Cylance® が収集および保存するお客様のデータは最小限に抑えられています。お客様のデータが外部に共有されることはありません。サイランスでは OAUTH タイプの認証を使用しており、機密性の高い、お客様のログイン詳細情報の閲覧は制限されています。そのため、データベースにアクセスできるメンバーでも、ログイン認証情報を取得することはできません。

データプライバシー – サンプルはサイランスに送信されると直ちに匿名化されます。どのお客様がどのファイルを送信したかを追跡することはありません。お客様のテナント識別情報に関連して取得されたすべての情報は匿名化されます。一部のデータは集約化され、各種指標を計算するために使用されます。また、個々の お客様の識別情報を料金の計算や悪用の防止に使用することはありますが、送信された個々の情報を お客様の識別情報に関連付けることはありません。たとえば、サイランスでは、お客様がサービスをご利用になっているかどうか、またどの程度ご利用になっているかを知ることができますが、お客様が取得された情報に関する詳しいレポートを生成することはできません。

お客様は CylancePROTECT に Portable Executable（PE）ファイルをアップロードすることができます。すると、アップロードされたファイルを分析することによって、脅威の痕跡などの詳細レポートも生成されます。アップロードされたファイルは、送信元を示す要素がすべて削除され、暗号化（ハッシュ）された状態でのみ参照されます。そのため、サイランスが個々のファイルを送信したお客様を特定することはできません。

データのポータビリティ – CylancePROTECT のコンソールでは、多くの情報をエクスポートすることができます。ユーザーは脅威やデバイスに関するデータを抽出して、取得したりローカルにバックアップしたりすることができます。CylancePROTECT の API を使用すれば、お客様はそうした情報をプログラムにより抽出することができます。

Cylanceについて：

Cylance は、人工知能（AI）、アルゴリズム技術、および機械学習を初めてサイバーセキュリティに応用し、企業、政府機関、およびエンドユーザーが、困難なセキュリティ問題を未然に解決できるようにします。単にブラックリストやホワイトリストで判断するのではなく、画期的な予測分析プロセスによって安全か脅威かを迅速かつ正確に識別します。洗練された機械学習と AI を、攻撃者の心理に関する独自の見識に基づいて組み合わせることで、高度な脅威に対する真の予測および防御が可能なテクノロジーとサービスを提供します。詳しくは、cylance.co.jp をご覧ください。

セキュリティ

AWS は基本的にはデータセンターであり、企業が自社専用として持っているデータセンターや他のあらゆるデータセンターと同様にセキュリティリスクは存在します。すべてのクラウドリソースは仮想プライベートクラウド（VPC）環境でホストされます。これは、CylancePROTECT ネットワークは外部からも、AWS をお使いになっている他のすべてのお客様からも、デフォルトで隔離されていることを意味します。いかなるパケットも、気付かないうちに当社のシステムに到達するようなことはありません。

外部向けのすべてのリソースは、隔離された非武装地帯（DMZ）でホストされています。DMZ とは、外部向けのファイアウォールの内側に設けられるネットワークセグメントのことです。そこには、内部向けの別のファイアウォールが存在し、当社のシステムへの直接のアクセスがブロックされます。また、AWS によって管理されているロードバランサを使用することによって、攻撃対象領域はさらに縮小します。こうしたロードバランサは、当社のいかなるリソースに対してもインターネットからの直接アクセスを受け付けず、限られたごく少数のホストへの管理されたアクセスのみを許可します。つまり、約 95% のホストは、インターネットに接続された開かれたポートを持っていないことになります。伝送中のすべてのデータは TLS によって暗号化されます。デバイスが旧式で TLS を使用できない場合は、CylancePROTECT エージェントが実行されているエンドポイントで提供される最高レベルのセキュリティ機能を使用します。

VPC 内のオペレーションに対するすべてのアクセスは、強力な暗号のみを使用するように構成された SSL VPN によって管理されます。ユーザー名、パスワード、個別の証明書、第二の二要素認証トークンが使用されます。

Amazon Identity and Access Management を使用して、どこにアクセスするときにもセキュリティポリシーが適用されます。サイランスの AWS インフラストラクチャには、デフォルトで公開されているリソースはありません。組織内のそれぞれの役割には、アクセスレベルを制限するセキュリティポリシーが定められます。AWS のあらゆるリソースへのあらゆる攻撃者によるアクセスはすべてログに記録され、頻繁に検証されます。

可用性

Amazon が運営しているネットワークは、最も良くつながるネットワークの 1 つです。AWS のデータセンターは、すべての主要なバックボーンプロバイダと密接に相互接続されています。AWS のグローバルインフラストラクチャの詳細については、Amazon の Web サイトをご覧ください。また、AWS は世界の 9 ヶ所のセンターで 100 を超えるエッジ接続を備えた大規模な相互接続ポイントを提供しており、継続的な可用性が保証されるようになります。外部の機能をわずかな操作で 9 ヶ所の主要センターのいずれかにミラーリングすることができます。

サイランスの開発運用チームは稼働時間の向上に努めており、現在は 99.95% の可用性を実現しています。計画されたメンテナンスについては、すべてお客様に通知されます。計画外の停止が発生すると、電子メールによる通知が送信され、Cylance カスタマーサポートポータルにその情報が掲載されます。クラウドサービスが予期せず停止した場合も、デバイスはすべて保護されます。CylancePROTECT Agent は、クラウド接続なしでも自律的に脅威を分析し、隔離することができます。

拡張性

AWS は、現在提供されている拡張性の非常に高いクラウドベースの Web サービスの 1 つです。最近のレポートによると、通常は 1 日のうちに、インターネットユーザーの 1/3 が、AWS でホストされている 1 つ以上のサイトにアクセスしているとのことです。AWS はすべてのインターネットトラフィックの約 1% を受信しています。人気の高いサイトの多くが AWS のみを使用しており、それをさらに超える数のサイトが何らかの形で AWS を使用しています。AWS は、アメリカ食品医薬品局、NASA ／ジェット推進研究所、アメリカ疾病管理予防センター、Comcast、Unilever、Siemens、Novartis、Instagram、Netflix、Pinterest、Salesforce.com などで使用されています。

Cylance Japan株式会社
〒100-6510
東京都千代田区丸の内1-5-1　新丸の内ビルディング10F
www.cylance.co.jp
03-6386-0061(代表)

CYLANCE

201807-DS006