



CHECK POINT CAPSULE CLOUD

製品の特徴

- IPS、アプリケーション制御、URLフィルタリング、アンチウイルス、アンチボット、脅威エミュレーションを統合
- 世界各地のデータセンターにサービス・インフラを設置
- iOS、Android、Windows、Macの各プラットフォームに対応
- シングル・サインオン (SSO)
- ログをプッシュしてローカルに保存またはオンラインで表示
- Active Directoryの統合によるアイデンティティ認識が可能

製品の利点

- 社内のセキュリティ・ポリシーをモバイル・デバイスにも適用
- モバイル・デバイスで不審なファイルのダウンロード、不正なWebサイトへのアクセス、およびボットによる被害をブロック
- セキュリティの境界の外側にいるモバイル・ユーザを保護
- チェック・ポイントのセキュリティ対策をリモート・オフィスまで拡張、新たなアプライアンスは不要
- Webアクセス経路の脅威をリアルタイムでブロック
- 社内のデバイスとモバイル・デバイスの両方に共通のセキュリティ・ポリシーを適用
- チェック・ポイントのセキュリティ・アーキテクチャ、Software Bladeの保護機能をクラウド・サービスとして提供
- ソフトウェアを常に最新かつ最適な状態に維持

課題

従来の企業ネットワークのセキュリティ・ポリシーは、ネットワーク内部にあるすべてのデバイスやデータを保護することを目的としていました。しかし、この数年で企業ネットワークは大きく様変わりし、業務データが外部からアクセスされるようになったほか、データそのものもネットワークの境界の外へ持ち出されるようになりました。事業継続性のニーズの高まりや、モバイル・デバイスの導入に伴って発生するリスクはいま、企業のセキュリティ担当者に大きな課題を突きつけています。

社内の業務データにリモートからアクセスする社員が増えると、企業のインフラストラクチャに新たな隙間が生じます。モバイル・デバイスに起因して、ユーザや組織を新たな攻撃源にさらす可能性もあります。この事実を理解していない場合、リモート・アクセスの利用者が無意識に不正なサイトにアクセスしたり、ウイルスをダウンロードしてしまったりするケースも十分に考えられます。モバイル・デバイスを利用する社員が増え、さまざまな場所から業務データを利用する傾向が進むと、こうしたセキュリティの「盲点」はさらに拡大します。

ある調査では、年間 1,160 万台ものモバイル・デバイスがマルウェアに感染¹しているという結果が出ています。このため、企業では社内のデバイスを対象とする保護機能を、モバイル・デバイスやリモート・オフィスにも適用する必要性が高まっています。

解決策

Check Point Capsule Cloud を利用することにより、企業のセキュリティ対策の範囲外にいるモバイル・ユーザにも最新の保護機能を常時適用することが可能となり、あらゆる業務におけるセキュリティの継続性が実現します。

チェック・ポイントの各種 Software Blade の保護機能をクラウド・サービスとして利用する Check Point Capsule Cloud は、場所を選ばずネットワークやユーザを保護できるほか、不審なファイルのダウンロードや不正な Web サイトへのアクセス、ボットの活動を被害が出る前にブロックできます。

Check Point Capsule Cloud は、安全な VPN トンネルを介したモバイル・デバイスからのすべてのトラフィックを企業のポリシーが施行されたクラウドへ導くことにより、リアルタイムの保護を提供しています。社内のデバイスとオフサイトのデバイスの両方に適用される共通のポリシーは、セキュリティの設定ツールである SmartDashboard で一元的に管理するか、純粋なクラウド環境の場合は直感的な Web ユーザ・インタフェースを使用してリモートで管理できます。

チェック・ポイントのセキュリティ・エキスパートおよび世界各地のデータセンターで 365 日 24 時間運用されるサービスにより、企業のネットワークやユーザに対し常に最新の保護機能が適用されます。企業内部および境界の外側からの利用を問わず企業の資産やデータ、デバイスが確実に保護されます。

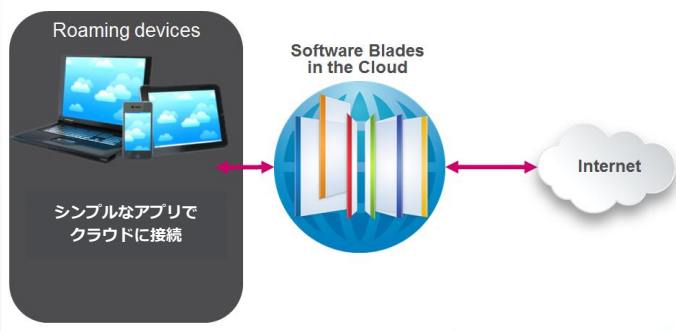
¹ Source: Kindsight Security Labs Malware Report 2014

社内のセキュリティ・ポリシーをモバイル・デバイスにも適用

Check Point Capsule Cloud は、社内のネットワークのセキュリティ・ポリシーをモバイル・デバイスやリモート・オフィスにも適用して、場所を選ばない保護対策を実現します。また、チェック・ポイントの Security Management サーバを使用し、クラウドのネットワーク・オブジェクトを適切なポリシー・ルールに追加するだけで、クラウドのモバイル・デバイス・ポリシーを他のゲートウェイと同じように管理することが可能です。有効にしたポリシーは自社運用環境のすべてのゲートウェイに自動配信され、クラウドにも社内のセキュリティ・ポリシーが適用されます。

セキュリティの境界の外側にいるモバイル・ユーザを保護

Check Point Capsule Cloud により、iOS や Android のタブレット端末およびスマートフォン、またはノート PC などのモバイル・デバイスをさらに積極的に利用できます。モバイル・デバイスのすべてのトラフィックは、安全な VPN トンネルを通じてクラウド・サービスに転送されます。ユーザ・データがネットワークの境界を素通りすることはなく、発信と着信のどちらのトラフィックもパケット単位でスキャンされ、安全性が確保されます。



不審なファイル、不正な Web サイト、ボットによる被害を阻止

Check Point Capsule Cloud を導入すれば、チェック・ポイントの Software Blade の保護機能をクラウド・サービスとして利用し、場所を選ばずユーザやネットワークを保護できます。モバイル・ユーザに限らず、リモート・オフィスでもローカルのアプライアンスをクラウドに接続すればセキュリティ・サービスの利用が可能になり、新たなハードウェアを追加せずにセキュリティを強化できます。

また、Check Point ThreatCloud は、IPS、アプリケーション制御、URL フィルタリング、アンチウイルス、アンチボット、脅威エミュレーションを統合して、最新の保護機能を提供します。悪意のあるファイルのダウンロード、危険な Web サイトへのアクセスやボットの通信による、ユーザやリモート・オフィスへの被害発生を未然に防止します。

統合型の管理プラットフォームで包括的な可視性を維持

Check Point Capsule Cloud の管理は、チェック・ポイントの Security Management サーバから行われ、導入済みのチェック・ポイント製品とシームレスな統合が実現します。ログはクラウドから直接 Security Management サーバに送信されるため、アクティビティの一元的な監視が可能です。

直感的に使える Web ユーザ・インタフェースからでもポリシーは管理できます。いずれのブラウザでも容易に利用できるインタフェースで、追加ライセンスやインストールも必要ありません。Security Management サーバに集められたすべてのログが Web ユーザ・インタフェースから参照できるため、Check Point Capsule Cloud の包括的な可視性が担保され、詳細な管理が可能になります。

クライアントのシームレスなインストールと配布

容易に導入可能な Check Point Capsule Cloud は、クライアントのインストール時にグループ・ポリシー・オブジェクト (GPO) の配布とシングル・サインオン (SSO) をサポートしています。また、インストールしたクライアントの設定は自動で行われ、管理者の手間が省けます。さらに、Check Point Capsule Cloud は Active Directory との統合によりアイデンティティ認識も実現します。さらに、接続したネットワークを識別し、企業 LAN の中で作業する場合は、クラウド向けの接続を自動的に切断できます

Check Point ThreatCloud

新たに検出された脅威の情報は ThreatCloud に送信され、他のチェック・ポイント・ゲートウェイの保護に利用されます。新しい脅威のシグネチャは、他のチェック・ポイント・ゲートウェイやクラウドにも配信されるため、脅威の拡散は未然に防止されます。こうした継続的な連携により、最新の脅威データベースを備えた業界最先端の脅威対策ネットワークが実現します。

仕様

提供されるテクノロジー	
<ul style="list-style-type: none"> IPS アプリケーション制御 URL フィルタリング アンチウイルス 	<ul style="list-style-type: none"> アンチボット Threat Emulation VPN (IPSec)
クライアント・プラットフォームのサポート	
<ul style="list-style-type: none"> iOS 5.0以降 Android 4.0以降 Windows Vista Enterprise SP1 以降 	<ul style="list-style-type: none"> Windows 7 Enterprise, Professional, Ultimate Windows 8.0および8.1 Enterprise Mac OS 10.6以降

最新のプラットフォームは SecureKnowledge [sk102501](#) を参照ください。

製品に関する お問い合わせ

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿 5-5-3 建成新宿ビル 6F
Tel : 03 (5367) 2500 E-mail : info_jp@checkpoint.com Web : www.checkpoint.co.jp