



Check Point Endpoint Security

単一のエンドポイント・セキュリティ・エージェントにより
包括的な保護と管理の簡素化を実現

Contents

本書の内容

概要	3
エンドポイントを保護するための課題	4
新たな戦略：エンドポイント・セキュリティの統合	5
エンドポイント・セキュリティの統合がパフォーマンスにもたらすメリット	8
Check Point Endpoint Security	8
結論/製品の詳細について	10

概要

情報セキュリティについて懸念している企業の多くは、エンドポイントは企業のセキュリティにとってまさにアキレス腱であるということを認識しています。今日のエンドポイントは、3つの重大なリスクを内包しています。第1のリスクは、最近の攻撃の多くが悪意のあるWebサイトを利用するなどのさまざまな手法を用いることにより、従来型の境界セキュリティを突破して企業ネットワーク内部およびエンドポイントまで到達できるようになっていることです。第2のリスクは、持ち運び可能なエンドポイントが増加したことで、1つのエンドポイントが従来型境界セキュリティの内側と外側の両方で使用されるようになっていることです。そして第3のリスクは、ネットワーク管理者は、各エンドポイント機器に複数のエージェントを導入し、それらのセキュリティ・ポリシーを配布および管理しなければならず、エンドポイントは、企業ネットワークを安全に維持する上で大きな負担になっているということです。

適切なセキュリティ対策が施されていないエンドポイントは、高い確率で脆弱性を攻撃されます。脆弱性を悪用された場合には、データが盗まれたり業務の中断を余儀なくされるなどの被害が発生するほか、セキュリティに関する法律や規則を遵守していなかったとして罰金や罰則を科せられるおそれがあります。

これらの課題に対処するため、最近では、幅広いエンドポイント・セキュリティ技術が統合され、集中管理に対応したエージェントを導入するなどの新しい戦略を採用する企業が増えています。これは確かに正しい戦略ではありますが、この方法で成果を上げるためには、エンドポイントにとっての主要なセキュリティ・リスクをすべてカバーできる機能がそのソリューションに搭載されていなければなりません。これに加えて、エンドポイントのセキュリティ管理に伴う負担が最小限であり、エンドユーザからは透過的に動作し、そしてソリューション全体を単一のコンソールから容易かつ効率的に管理できることも重要となります。この技術白書では、これらのセキュリティ・リスクと、チェック・ポイントの統合エンドポイント・セキュリティ・ソリューションである Check Point Endpoint Security™ について解説します。

エンドポイントを保護するための課題

ネットワーク・セキュリティ管理者の立場からすると、PCやネットワーク、インターネットが企業環境に浸透してからというもの、技術インフラストラクチャとデータ保護を両立することはより困難になっており、実際問題として、それらの安全性は以前よりも低下しています。ネットワーク技術が企業に普及し始めた当初、セキュリティ対策が講じられていたのは主にネットワークの境界部分でした。これは、内部システムへの侵入を試みる外部からの攻撃を防ぐことを目的としていました。その後、ハッカーや犯罪者は新たな方法で脆弱性を攻撃するようになり、これに対抗するために新しいセキュリティ・ソリューションが次から次へと登場しています。今日では、多層防御のアプローチで包括的な保護を実現し、潜在的な脆弱性が見過ごされないようにすることが、ネットワーク・セキュリティ/情報セキュリティ対策の一般原則とされています。

そして現在、固有のセキュリティ対策が必要とされる新たな主要リスク要因として専門家が注意を呼びかけているのが、エンドポイントです。エンドポイントとは、組織のネットワークに接続されるあらゆるコンピューティング・デバイスのことを指します。デスクトップPCやノートPCだけでなく、各種モバイル・デバイスを始め、ストレージ、I/O、無線接続機能などを備えた電子デバイス、さらには工業用制御システムや重要なインフラストラクチャ用のプログラム可能なロジック・コントローラを備えたIPネットワーク接続デバイスなどがこれに該当します。

エンドポイントには、さまざまな種類の攻撃が行われます。特に、一般的なネットワーク・プロトコルに脆弱性がある場合、開いているポートや監視されていないポートから不正アクセスを受ける可能性があります。また、ソフトウェアのデータ・バッファ・サイズに関するプログラミング・エラーを悪用する攻撃もしばしば発生しています。この種の攻撃は、標的のシステムでバッファ・オーバーフローを引き起こさせ、メモリのスタック領域やヒープ領域を上書きして、悪意あるコードを実行させることを目的としています。現在、多くのPCはオペレーティング・システム(OS)にMicrosoft Windowsを採用しており、Windowsプラットフォームを採用するデバイスは数億台にも上るため、Windowsはハッカーたちの格好の標的となっています。ただし、IPを使用するエンドポイントは、そのOSの種類にかかわらず、すべて攻撃を受ける可能性があります。そしてこのエンドポイントが、企業ネットワークにおける新たなアキレス腱となっているのです。

エンドポイントが内包する3つの大きなリスク

今日のエンドポイントは、企業ITに対する3つの重大なリスクを内包しています。第1のリスクは、最近の攻撃の多くは、エンドポイントがアクセスするWebアプリケーションを介して従来型の境界セキュリティを突破し、企業ネットワークの内部にまで到達できるということです。Webブラウザに脆弱性がある場合、悪意のあるWebページを表示するだけでその脆弱性を悪用される可能性があります。クロスサイト・スクリプティングなどWebベースの攻撃の多くは、ほとんどすべてのWebブラウザに影響します。Webベースのネットワーク・アクセスがもたらすその他の脅威としては、cookieなどのローカル・ファイルの漏洩、ローカル・プログラムや悪意あるコードの実行、脆弱性のあるPCの完全な乗っ取りなどが挙げられます。

第2のリスクは、持ち運び可能なエンドポイントが増加し、1つのエンドポイントが従来型の境界セキュリティの内外で使用されるようになってきていることです。ある調査によると、現在、世界で出荷される全PCのうち約半分がノートPCであり、その数はさらに増え続けています。セキュリティ・ソフトウェアがローカルで動作していないエンドポイントを、境界ベースのセキュリティ対策によって保護されないネットワーク外部で使用した場合、さまざまなリスクにさらされることになります。

第3のリスクは、各物理デバイスにポリシー・ベースのセキュリティ・ソフトウェアを導入して管理しなければならないネットワーク管理者にとって、エンドポイントは、企業防衛上の大きな負担になっているということです。セキュリティ・ソフトウェアを導入し、最新のアップデートとシグネチャ・ファイルを適用して、ポリシーおよび設定の一貫性を保つという作業を手動で行うのには、多大な時間と労力が必要とされます。特にこれは、モバイル・エンドポイントが数千台もあるような大規模環境において顕著です。

1 出典：451 Group

新たな戦略：エンドポイント・セキュリティの統合

賢明なITセキュリティ・マネージャは、エンドポイント、特に企業の境界セキュリティの外で使用されるモバイル・デバイスを、リスクを抱えた脆弱な「孤島」のようなものと捉えています。エンドポイントの脆弱性が悪用されないようにするには、各エンドポイントに包括的なエンドポイント・セキュリティ機能を導入する必要があります。

ほとんどの企業では、パーソナル・ファイアウォールやアンチウイルス・ソフトウェアといったスタンドアロンのポイント・セキュリティ・ソリューションをすでにエンドポイントに導入しています。しかし、数百～数千台のPCが存在する環境の場合、この方法は管理者に多大な負担を強いることになります。例えば、あるエンドポイント・エージェントのソフトウェア・アップデートが提供された場合は、アップデートをエンドポイントに配布する前に、毎回厳格なテスト・サイクルを実施して、パフォーマンスや互換性の問題がないかどうかをチェックしなければなりません。企業環境においては、1つのデバイスに3種類以上のエンドポイント・セキュリティ・エージェントが導入されることも珍しくないため、このアップデート・プロセスは、多大な時間とコストを要する難しい作業になる場合があります。

この問題を解決する新しい戦略は、各PC上の複数のエンドポイント・セキュリティ機能を統合し、さらにITセキュリティ担当者が単一のコンソールから集中的に導入と管理を行えるようにすることです。セキュリティ機能を統合すると、導入および管理の作業が簡素化され、これによって全体的な運用管理コストが削減されます。エージェントが1つに統合されることで、1つのエージェントについてのみテスト・サイクルを実施すればよくなるほか、エージェントに含まれる各機能の互換性も保証されることとなります。ただし、強固なエンドポイント・セキュリティを実現するためには、統合エンドポイント・ソリューションにどのような機能が含まれているのかを慎重に検討する必要があります。包括的なセキュリティ機能が統合されていない場合は、包括的なエンドポイント・セキュリティを実現することはできないからです。

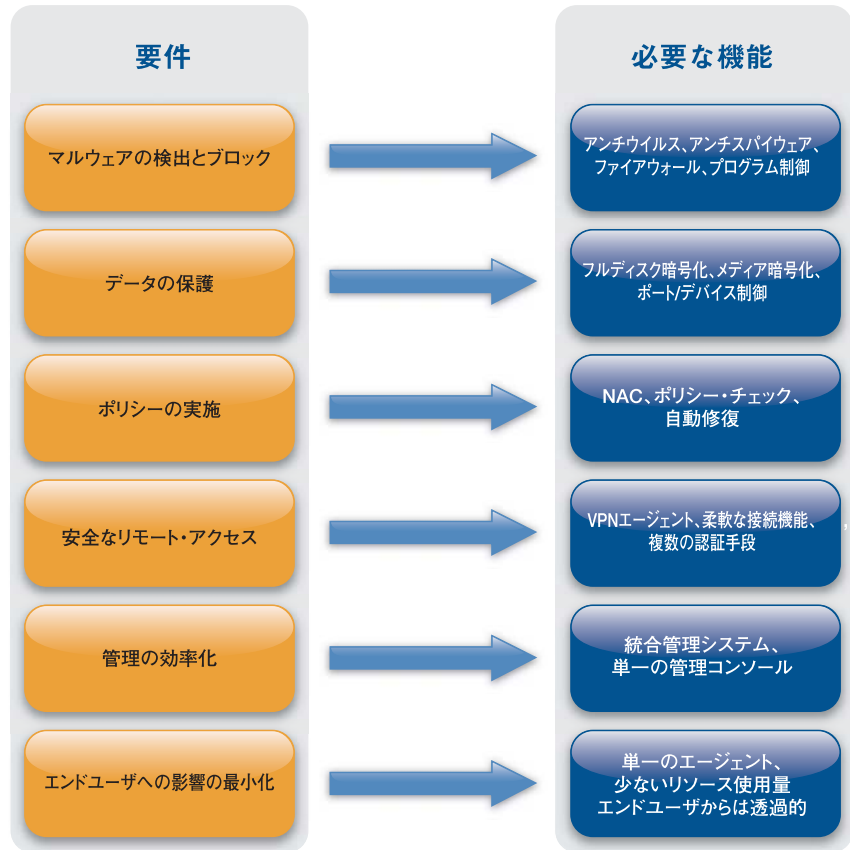
包括的なエンドポイント・セキュリティを実現するには、少なくとも次のことを行える必要があります。

- マルウェアの検出とブロック
- データの保護
- ポリシーの実施
- 安全なリモート・アクセス
- 管理の効率化
- エンドユーザへの影響の最小化

1. マルウェアの検出とブロック

通常、エンドポイント上のマルウェアを検出し、実行できないようにすることは、ファイアウォールやアンチウイルス/アンチスパイウェアの機能を提供するポイント・ソリューションを導入することによって実現できます。これらのセキュリティ・アプリケーションは、マルウェアを検出およびブロックするという一連の要件に特化した重要かつ固有の機能を提供します。

着信/発信トラフィックを制御するための中核機能を提供するファイアウォールとプログラム制御は、これらのセキュリティ機能の中で特に重要な機能です。悪意のあるコードなどの望ましくないトラフィックを遮断し、どのアプリケーションにネットワーク・アクセスを許可するかを制御して、エンドポイントをハッカーから見えないようにすることができるのは、ファイアウォールだけです。製品の成り立ち上、アンチウイルス機能を中心に構成されているエンドポイント・セキュリティ・スイートも存在しますが、防御の最前線に配置される機能として最もふさわしいのは、エンドポイントPCの着信/発信トラフィックの両方を制御することのできるファイアウォールです。



統合エンドポイント・セキュリティの要件

アンチウイルス機能は、ウイルスの侵入を検出・阻止するために使用されます。優れたアンチウイルス・アプリケーションは、シグネチャ・マッチングとヒューリスティック技術など、複数の検出手法を併用します。シグネチャ・マッチングは、当該ファイルを、既知の悪意あるコードが登録されたデータベースと照合することによってウイルスを検出する手法です。一方のヒューリスティック技術は、ファイルの出所やコードの振る舞いを既知の脅威と比較することによってウイルスを検出します。

アンチスパイウェア機能は、ワームやトロイの木馬、アドウェア、キーロガーなどの侵入を防止します。スパイウェアがエンドポイントにインストールされるのをリアルタイムで阻止する機能、すでにインストールされているスパイウェアを検出して駆除する機能を備えています。

管理者にとって重要なのは、これらすべての機能を集中管理し、エンドポイントがセキュリティ・ポリシーを遵守しているかどうかを一元的に把握する機能が備わっていることです。例えば、PC上で定期的にスキャンを実行するようにスケジュールを設定する機能や、各PCについてのレポート（PCのポリシー遵守レベル、過去1週間で完全ウイルス・スキャンを実施したPCの割合、現在ウイルスに感染しているPCの数など）を作成する機能が必要になります。

2. データの保護

ノートPCをはじめとするモバイル・デバイスは、盗まれたり紛失したりする可能性が高く、そのデータを保護することは極めて重要です。エンドポイントが第三者の手に渡った場合、データが暗号化されていないならば、容易にデータを盗み見られ、場合によってはそれらを悪用されることも考えられます。エンドポイントのデータを保護する手段としては、フルディスク暗号化、メディア暗号化、ポート/デバイス制御といった機能が挙げられます。

暗号化は、特別な情報を知っている者でなければ、データを読み取れないようにする技術です。通常、暗号化の解除（復号化）には「鍵」を使用します。暗号化は、ファイルやフォルダ・レベル、あるいはディスクなどのストレージ・メディア・レベルで行うことができます。従来のエンドポイント向け暗号化技術は、使用方法が煩雑であるうえに、システムのパフォーマンスを大きく損なっていました。しかし、最近の暗号化ソリューションではこうした問題は解決されており、世界で数百万台ものエンドポイントに導入されるまでになっています。

ポート/デバイス制御は比較的新しい技術で、エンドポイントの各ポートの使用を集中管理できるようにします。例えば、エンドポイント上の重要なデータが、USBメモリなどのパーソナル・ストレージ・デバイスに許可なくコピーされるのを防止できます。また、マルウェアが外部ストレージ・デバイス経由でエンドポイントに侵入し、さらに企業ネットワークに拡散するのを防ぐことも可能です。

3. ポリシーの実施

この機能により、ネットワークへのアクセスを許可する前に、エンドポイントにセキュリティ・ポリシーを遵守させることができます。基本的なレベルでは、管理者が策定したセキュリティ・ポリシーやルールを各エンドポイントが遵守しているかどうかをチェックできます。例えば、アンチウイルス・ソフトウェアやアプリケーションのバージョンが最新であるか、重要なパッチが適用されているか、禁止されているプログラムが実行されていないかなどを調べることが可能です。これらのポリシー・チェックをクリアできなかったエンドポイントについては、ネットワークへのアクセスを拒否することができます。

異機種が混在する企業ネットワークでこれらのことを実施するには、異なるベンダーのゲートウェイおよび認証システムと連携できる必要があります。業界標準である802.1x認証がサポートされていれば、マルチベンダー環境でもネットワーク・アクセス制御（NAC）を行うことができます。また、ポリシーを遵守していないエンドポイントが自動的にアップデートを取得してインストールできるようにするため、自動修復機能をサポートしていることも求められます。その他の要件としては、オンデマンドでポリシーを実施する機能が挙げられます。これは、エージェント・ソフトウェアをインストールすることなく、自社の管理下でないエンドポイントでセキュリティ・ポリシーを実施するための機能で、セッションの機密性を確保したり、スパイウェアを検出・無効化したりするために使用されます。例えば、自社の社員がインターネット・カフェや空港のキオスクなどにあるPCから、SSL VPNゲートウェイ経由で企業ネットワークにアクセスする場合、管理者は、これらのマシンの安全性を確保しなければなりません。また、リモート・アクセス・セッションが終了した後、これらのPCに情報が残らないようにセッションの機密性を確保する必要があります。

4. 安全なリモート・アクセス

モバイル・コンピュータの普及に伴い、リモート・アクセスを安全に行えることは、エンドポイント・セキュリティを確保するうえでの重要な要件になっています。安全なリモート・アクセスを行うために必要な技術としては、リモート・アクセス・エージェント、柔軟な接続機能、複数の認証手段が挙げられます。

VPN (Virtual Private Network) 技術は、企業のネットワーク・ゲートウェイへの安全なリモート・アクセスを実現する最も一般的な手段です。VPNによるリモート・アクセス・リンクでは、暗号化された安全なアクセス・トンネルを構築して、データの盗聴や改ざんを防止することにより、通信の安全性を確保します。

接続機能の面では、ダイヤルアップ、ケーブル・モデム、DSL接続での動的/固定IPアドレス割り当てに柔軟に対応している必要があります。リモート・ユーザの実際のIPアドレスを含むIPパケットをカプセル化し、リモート接続しているユーザがオフィス内にいるかのように見せかけることで、エージェントとリモート・アクセス・ゲートウェイ間のルーティング問題を解決することができます。

認証機能については、SecurIDトークン、ユーザ名/パスワード、RADIUS、TACACS、バイOMETRICSをサポートしている必要があります。

5. 管理の効率化

エンドポイント・セキュリティを統合する目的の1つに、すべてのセキュリティ機能を単一のコンソールから管理可能にするということがあります。管理機能では、すべてのエンドポイント・セキュリティ—企業の各エンドポイントに導入されたすべてのセキュリティ機能—の設定、ポリシー管理、レポート、および分析を一元的に行える必要があります。これにより、次のような点で管理の効率化が実現されます。

- 管理作業の集中化と委譲
- すべてのエンドポイント・セキュリティ機能の監視とレポートを集中化
- セキュリティ・インシデントの監視、発見、フォレンジック調査を効率化
- 包括的なレポート機能により、監査と法令遵守を支援
- ITスタッフがオンサイトで作業したり、エンドユーザーを関与させたりすることなく、素早く簡単にソフトウェアを導入可能
- エンドポイント・セキュリティとネットワーク・セキュリティ・イベント管理を統合

6. エンドユーザーへの影響の最小化

統合エンドポイント・セキュリティ・ソリューションを選択するにあたっては、エンドユーザーへの影響が最小限で、その作業を妨げないものであることも重要なポイントとなります。理想的なのは、すべてのセキュリティ機能が単一のエージェントに統合されているながら、メモリなどのリソース使用量が最小限に抑えられていることです。多くのエンドポイント・セキュリティ・スイートは、実際にはエージェントが単一化されておらず、3~5種類、場合によってはさらに多くのソフトウェア・モジュールをPCにロードします。このため、メモリやCPUリソースを大量に消費し、業務アプリケーションのパフォーマンスを低下させます。また、セキュリティ・ソフトウェアのアップデートやパッチの適用といったメンテナンス作業をエンドユーザーが手動で行わなければならない場合、ユーザーの不満はさらに高まります。エージェントの数が少なければ、そのぶん管理は容易になり、パフォーマンスが向上し、ユーザーの関与が少なくて済むほか、より強固なセキュリティが実現されます。

エンドポイント・セキュリティの統合がパフォーマンスにもたらすメリット

すべてのエンドポイント・セキュリティ機能を統合すると、エージェントのリソース使用量が少なくて済み、エンドポイント・システムへの影響も小さくなるため、システム自体のパフォーマンスが向上します。また、エージェント・モジュールの数が少なければ、そのぶん導入と管理が容易になります。

Check Point Endpoint Security

Check Point Endpoint Securityは、エンドポイント・セキュリティを統合してトータルな保護、管理、および高いパフォーマンスを実現し、従来型のエンドポイント・セキュリティ・ソリューションに代わる手段を提供します。Check Point Endpoint Securityでは、エンドポイントを包括的に保護するために必要なすべての主要セキュリティ機能が単一のエージェントに統合されています。エージェントが1つであるためリソース使用量が少なくて済むほか、エンドユーザーの関与を必要としない集中管理も実現されています。

Check Point Endpoint Securityに統合されている機能

機能	説明
ファイアウォール	ファイアウォールの分野における15年間に及ぶリーダーシップと、幅広い導入実績を誇るZoneAlarm®のパーソナル・ファイアウォール技術に基づき、着信/発信トラフィックに対するプロアクティブな保護機能を提供します。悪意のあるコードによってエンドポイントPCのセキュリティが侵害されるのを防止する、望ましくないトラフィックを遮断する、脆弱性のあるシステムを探しているハッカーからエンドポイントを隠す(ステルス・モード)などの機能を搭載しています。
プログラム制御	通常のファイアウォール・ルールを使用してアプリケーションの振る舞いを制御します。ネットワーク・アクセスを試みるPCアプリケーションのリストが自動的に作成されるため、潜在的なネットワークの脆弱性を素早く効率的に把握し、保護できます。許可されたプログラムのなりすましや改ざん、乗っ取りも防止できます。
Program Advisor	世界中の数百万台のPCから収集されたリアルタイムのデータに基づき、ほとんどのアプリケーション・ポリシーの決定を自動化できます。信頼できるアプリケーションとマルウェアが登録されたチェック・ポイントのデータベースに基づいて最善と考えられるポリシーを即座に適用し、プログラムの通信を許可またはブロックできます。また、悪意があると判断されたプログラムの実行を自動的に停止することもできます。
ネットワーク・アクセス制御(NAC)	ネットワークへのアクセスを制御し、VPNによるアクセスと内部ネットワーク・アクセスの両方にエンドポイント・ポリシーを適用します。NAC機能は、チェック・ポイントのゲートウェイや主要なネットワーク機器ベンダーのインフラストラクチャ・デバイスと連携できます。また、業界標準の802.1x認証をサポートしているため、チェック・ポイントのインフラストラクチャを使用するかどうかにかかわらず、マルチベンダー・ネットワーク環境でNACを実施できます。
アンチウイルス	高性能な統合アンチウイルス技術により、ウイルスなどのマルウェアを検出してエンドポイントから駆除します。ウイルス検出は、シグネチャ、振る舞いブロック機能、およびヒューリスティック分析機能を組み合わせて行われるため、業界最高レベルの検出率が実現されています。
アンチスパイウェア	機密データが盗み出される、内部ネットワークで輻輳が発生する、PCのパフォーマンス低下によってヘルプデスクへの問い合わせが増えるといった、スパイウェアに起因するさまざまな問題から企業を保護します。シグネチャのアップデートは管理者の設定に基づいて強制的に実施できるため、エンドポイントのアンチスパイウェア機能を常に最新の状態に維持することができます。
データ・セキュリティ*	Check Point Endpoint Securityは、Pointsec®の先進のデータ・セキュリティ機能を搭載しています。起動前認証、フルディスク暗号化、メディア暗号化、ポート管理という効果的な機能の組み合わせにより、包括的なデータ保護を実現します。フルディスク暗号化は、容易に導入できる強力な暗号化機能とアクセス制御機能を提供し、ハードディスク上のすべてのデータを確実に保護します。この暗号化はエンドユーザーからは透過的に行われます。メディア暗号化は、組織内のポリシーで許可されたUSBフラッシュ・ドライブなどのリムーバブル・メディアに対する強力な強制実施可能な暗号化機能を提供します。ポート制御は、データ検査、集中監査、およびポート管理の組み合わせにより、データの入出力を包括的に制御して、情報漏洩を防ぎます。
リモート・アクセス	Check Point Endpoint Securityは、数々の賞を受賞したVPN-1®SecureClient™をベースとする先進のIPSec VPNクライアントを統合した唯一のエンドポイント・ソリューションです。この機能により、エンドポイント・セキュリティに必要な不可欠な要素である安全なリモート・アクセス機能が提供されます。このIPSec VPN機能は、単一のエンドポイント・セキュリティ・エージェントに完全統合されており、他のエンドポイント・セキュリティ機能と同じインタフェース、同じシステムトレイ・アイコンを使用してリモート・アクセスを行うことができます。
統合管理	組織固有のニーズに合わせてエンドポイント・セキュリティ・ポリシーを拡張およびカスタマイズできる強力な管理ツールが提供されます。エンドポイントがネットワーク間、ロケーション間、ゲートウェイ間で移動する際に、自動的に適用される個別のポリシーを定義することもできます。Check Point Endpoint Securityは、導入環境とセキュリティ・ポリシーの管理に必要な時間と労力を最小限に抑えることで、ビジネスを効率的かつ円滑に、そして安全に遂行できるようにします。
チェック・ポイントの統一セキュリティ・アーキテクチャとの統合	Check Point Endpoint Securityは、チェック・ポイントの統一セキュリティ・アーキテクチャに基づいているため、管理者は、他のチェック・ポイント製品と同様に、管理システムのSmartCenter™またはProvider-1®を使用して、エンドポイント・セキュリティとNACを管理できます。製品ごとにサーバを用意したりログインし直したりする必要がないため、管理作業に伴う時間とコスト、複雑さを軽減しながら、企業全体のセキュリティを向上させることが可能になります。

*データ・セキュリティ機能が統合されたバージョンは、2008年第2四半期にリリースされる予定です。

結論/製品の詳細について

セキュリティ機能が統合されていないエンドポイントは、ネットワーク・セキュリティ/情報セキュリティにとっての新たな Achilles 踵となります。業界で最も包括的なエンドポイント・セキュリティ・ソリューションである Check Point Endpoint Security を導入することにより、エンドポイントのセキュリティ機能を統合し、企業全体のエンドポイント・セキュリティ管理を簡素化することができます。Check Point Endpoint Security では、業界最高水準のファイアウォール、ネットワーク・アクセス制御 (NAC)、プログラム制御、アンチウイルス、アンチスパイウェア、データ・セキュリティ、およびリモート・アクセスの各機能が、集中管理可能な単一のエージェントに統合されています。このため、複数のエンドポイント・セキュリティ・エージェントを管理する必要がなく、エンドポイント・セキュリティの管理に要する時間と労力を大幅に削減できます。

チェック・ポイントは、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理の分野におけるグローバル・リーダーです。Check Point Endpoint Security の詳細については、チェック・ポイントの担当者までお問い合わせください。

製品情報

http://www.checkpoint.co.jp/products/endpoint_security

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおけるトップ企業として、世界中の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティおよびVPN市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースに対する広範なセキュリティ保護を実現する、統一されたセキュリティ・アーキテクチャを提供しています。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、PointSec製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

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

E-mail : info_jp@checkpoint.com

Tel : 03 (5367) 2500

<http://www.checkpoint.co.jp/>

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check PointEndpoint Security, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, IntegritySecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, the puresecurity logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSP, SmartMap, SmartPortal, SmartUpdate, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, UTM-1 Total Security, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm ForceField, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labs のロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Check Point Endpoint Security

P/N:502809-J 2008.03

※記載された製品仕様は予告無く変更される場合があります。