

Symantec™ Critical System Protection

マルチプラットフォーム環境におけるホストベースの侵入防止ソリューション

ビジネスがさまざまな形でネットワークに依存する現在、企業は必要な情報資産をニーズに応じてインターネット上で公開しつつ、同時にそれを不正なアクセスから保護しなければなりません。そのためには既存のウイルス対策やゲートウェイタイプのファイアウォールだけでなく、侵入対象となり得るホストの状態を常に監視する侵入防止ソリューションが必要です。

製品の概要

ホストベースの侵入防止システムSymantec Critical System Protectionはセキュリティイベントのログファイル、動作するプロセスのふるまい、ユーザー認証等を常時監視します。検出された不審なプロセスの動作等に対し設定したポリシーに従った対策を自動的に行うことにより、顧客情報の流出やWebページの改ざんといった被害を引き起こす不正アクセスからサーバーを保護します。

また、管理者は集中管理コンソールから、セキュリティポリシーの設定、配備、監視を行えるほか、アラートへの対応、マルチプラットフォーム環境におけるシステムアクティビティに関するレポート生成を行うことが可能です。

〈キーポイント〉

- ふるまいの詳細を定義することにより、さらに高い精度でエクスプロイトの検出が可能
- 各種システムの設定、USBメモリなどの外部デバイスのアクセス制限、ドライブのマウント制御などを行うことにより、各種リソースの不正使用および情報への不正なアクセスを防止
- 集中管理コンソールに統合されているポリシーエディターにより、マルチプラットフォーム環境における脅威の検出と対応のためのセキュリティポリシーを容易にカスタマイズ
- 脅威の分析を的確に行うための、チャートやグラフでの視覚的なレポートニング
- Windows、Solaris、AIX、HP-UX、Linuxなどのマルチプラットフォームをサポート
- 世界をリードするインターネットセキュリティの専門機関、Symantec Security Responseによる信頼の支援体制

製品の特長

ミッションクリティカルなホストを保護するために、複数のソースを監視

Symantec Critical System Protectionは対象となるホスト上にSymantec Critical System Protectionエージェントを展開し、次のソースを監視します。

- イベントおよびカスタムログ
Windows環境では、Windowsアプリケーション、システム、セキュリティのイベントログを、UNIX環境では、syslog、wtmp、C2、プロセスアカウントのログを、イベントコレクタが自動的に監視。
- 監査ポリシー
監査コレクタがローカル監査ポリシーに対する変更を検出。
- ファイルおよびディレクトリ
ファイルコレクタが、指定されたファイルやディレクトリを監視し、作成、編集、削除、または名前の変更があったかどうかを検出。
- Windowsレジストリ
レジストリコレクタがWindowsレジストリ内の変更を監視。
- システムプロセス
プロセスコレクタがシステムプロセスを監視。プロセスの開始や停止を報告したり、プロセスをエージェントにより実行させないように設定したりすることも可能（プロセスマネージメント機能）。

カスタマイズ可能なポリシーに基づき、検出とレスポンスをリアルタイムで自動的に実行

Symantec Critical System Protectionエージェントは、収集されたすべてのイベントに対しリアルタイムで処理を行い、セキュリティポリシーとの適合性をチェックし、ポリシーで予め設定されたレスポンスを自動的に実行します。ポリシーは関連性のあるルールの集まりで構成され、監視を行うために必要な情報または無視する情報を指定したり、不審なふるまいなどを検出した際に実行するレスポンスを指定したりすることが可能です。このポリシーはユーザー自身によってカスタマイズすることもできます。自動的に実行されるレスポンスには、次のようなものがあります。

- 管理コンソールへの通知、レポートニング
- 電子メール/SNMPトラップによる通知
- セッションの切断
- ユーザーアカウントの停止
- コマンドプロセスの実行（スクリプト）
- セキュリティサーバーへのログ出力

多機能なコンソールを使用して効率良く管理し、迅速に対応

管理者は集中管理が可能なコンソールを用いて、監視とレスポンスを行うためのポリシーの作成と適用、インシデントを分析するためのログの収集など、さまざまなタスクを実行することが可能です。また、LiveUpdate™機能によって、ソフトウェアコンポーネントやセキュリティコンテンツのアップデート等も行うことができ、常に最新の脅威に備えることができます。そして、リアルタイムのレポート機能では、チャートやグラフによる包括的な傾向分析ができ、ドリルダウンで詳細情報を容易に閲覧できます。

Symantec Security Responseによる信頼の支援体制

Symantec Security Responseは、グローバルに展開するインターネットセキュリティ全般に関するリサーチチームとテクニカルサポートチームで構成されています。ウイルスやワームをはじめ、悪意のあるプログラム、不正侵入の手法、OSやアプリケーションの脆弱性とそれを利用した攻撃方法などに関する調査/研究、また、それに基づくシマンテック製品の支援を行っています。そして、インターネット上における脅威の動向を365日24時間体制で監視し、情報発信、ソリューションとサポートを世界中のユーザーに提供しています。

システム要件

Symantec™ Critical System Protection 5.1

Symantec Critical System Protection Agent

- Microsoft Windows
Windows Server 2003 R2 Standard / Enterprise Edition (32bit)
Windows Server 2003 R2 Standard / Enterprise x64 Edition
Windows 2000 Professional / Server / Advanced Server
Windows NT Server
- Linux
SUSE Linux Enterprise 8/9
Red Hat Enterprise Linux ES 3.0/4.0
- UNIX
Solaris 8/9/10 (SPARCプラットフォーム)
HP-UX 11i 11.11/11.23 (PA-RISCプラットフォーム)、
11.23 (Itanium2プラットフォーム)
IBM AIX 5L 5.1/5.2/5.3 (POWERプラットフォーム)

Symantec Critical System Protection 5.0 Management Server

Windows Server 2003 / Windows 2000 Server
Microsoft SQL Server

Symantec Critical System Protection 5.0 Management Console

Windows XP / Windows Server 2003 / Windows 2000 Server

製品に関する最新の情報

シマンテックのWebサイトをご覧ください。

<http://www.symantec.com/jp/business>