

Cisco Security Agent の ROI: エンドポイントにおける侵入保護エージェントの展開

シグニチャアップデート競争の回避

Cisco® Security Agent ソリューションは、企業におけるエンドポイントセキュリティの機能やソリューションを単一の製品に統合します。このソリューションには、ホストベースの侵入検知および侵入保護、ファイル整合性モニタリング、Windows NT イベント監査、分散型ファイアウォールまたはパーソナルファイアウォール、悪質なモバイルコードからの保護などが含まれます。

Cisco Security Agent を展開すると、セキュリティ戦略の簡素化、複数製品の管理による作業負荷の軽減、またそれらの製品にかかるソフトウェアおよび保守ライセンスの年間費用の削減が可能になります。

シグニチャアップデート競争の回避

シグニチャおよびウイルス定義は、侵入検知システムおよびアンチウイルスシステムの中心的な要素です。これらのソリューションは、その性質上、既知の脆弱性だけに基いているため、これらのシグニチャの実装と保守を行う管理上の負荷およびコスト面での負担が定期的発生します。この「アップデート競争」を回避する唯一の方法は、アプリケーションを予防的に保護して、検出される侵入だけでなく未知の侵入も防止することです。

Intrusion Detection System (IDS) およびアンチウイルス製品は、シグニチャアップデートに完全に依存しています。ベンダーは、これらのシグニチャアップデートを定期的または不正利用が発見される

たびに配信します。たとえば、侵入のシグニチャアップデートでは、8時間対応が一般的です。1か月ごとにしかアップデートを提供しないベンダーもあります。ユーザまたは管理者がアップデートをダウンロードする必要がある場合も、社内シグニチャサーバ上で自動アップデートテクノロジーを使用している場合も、システムの信頼性はユーザしだいになっています（自動アップデートの場合でも、デバイスがネットワークに接続されている状態で、ユーザ自身がログインを行う必要があります）。

自動アップデートを利用すると、脆弱性の発見からベンダーによるフィックスの提供までの時間が短縮されますが、セキュリティを重視する企業は、新しいパッチを徹底的にテストしてから、実稼動中のシステム上に展開しています。このテストでは、平均1～2日かけて、重要なシステムと互換性があることと、特定の攻撃に関するフィックスが通常の処理を妨げないことが確認されます。そして、このテストには管理上のコストがかかるだけでなく、アップデートがインストールされるまでの間、システムが危険にさらされます。



アラート および False Positive の管理

パターンおよびシグニチャの照合テクノロジーでは、False Positive および False Negative が発生する傾向があります。つまり、展開されたシグニチャが、実際には正常なホストおよびネットワーク動作が実行されたときに、誤って、悪質な行為の可能性があるとアラームを發します。この False Positive によって管理コンソールの表示が埋め尽くされるため、製品および管理者の効率が低下し、管理者は不確実なセキュリティアラートへの対応を強いられます。

Cisco Security Agent は、シグニチャを展開せずに、アプリケーションの動作を確認するため、False Positive の影響を受けません。また、エージェントと企業の両方のレベルでの関連付けと、高精度の防止判定を実行します。コンソールにもイベントが送信されますが、件数は少なくなります。送信されるイベントは、管理者に通知される必要のある正当なイベントです。

「また、この規模の企業では、ログファイルに記録される 500,000 件以上の項目を IT 管理者が毎日管理しています。Activis 社の調査によると、ファイアウォール 1 台につき 1 日あたり 200,000 ~ 300,000 件のログ項目と 20 件のアラートが出力されます。同様に、ネットワーク センサー 1 台につき 20 ~ 50 件、サーバ 1 台につき 1 ~ 20 件のコンソールアラートが出力されることがこの調査で判明しています。」

Computerworld、2001 年 11 月 30 日

サービス パックがリリースされるまでのアプリケーションのセキュリティ

ワームによる攻撃の結果から、セキュリティパッチのリリース後もアプリケーションが脆弱なままであることが明らかになっています。これは、専任の管理者が配置されていても、最近リリースされたホットフィックスやパッチをサーバに適用できていないことを示しています。

「優れた管理者や高度なクラッカーによって証明されているとおり、無関係なフィックスを除くすべてのパッチを定期的に適用しているネットワーク管理者が非常に少ないことが、本当の問題です。多くの原因がありますが、最も重大な問題は、パッチのダウンロード、テスト、適用を行う時間が不足していることと、主要ソフトウェアパッケージに影響を与える脆弱性が大量にあることの 2 点です。これらの問題が重なって、攻撃対象となる無防備なサーバおよびデスクトップが溢れています。」

eWeek、2003 年 1 月 27 日



Cisco Security Agent のようなアプリケーション中心のセキュリティアプローチでも、サーバにパッチをインストールする作業はなくなりません。しかし、一定期間の全ホットフィックスが集約されたテスト済みのベンダーサーバパックがリリースされるまでの間、ホストを保護できます。サービスパックは、問題ごとへの対処ではなく、一定の期間をおいて慎重にリリースされます。

「最近の調査では、過去 12 か月間にリリースされた必須のセキュリティパッチおよびセキュリティアップデートの数が膨大であったため、この作業によって、多くの企業のネットワークセキュリティが危機に陥っていることが結論付けられています。この調査は、ドイツ Articon-Integralis AG 社の子会社である英国のセキュリティサービスプロバイダー Activis 社によって実施されました。わずか 8 台のファイアウォールと 9 台のサーバで構成された IT インフラストラクチャを持つ企業のセキュリティ管理者が、過去 9 か月間だけで 1315 件のアップデートを行う必要があったことが判明しています。これは、1 日あたり 5 件のアップデートに相当します。この数は、主要ソフトウェアベンダーおよびセキュリティベンダーからこの期間内にリリースされたアップデートおよびパッチの合計数に基づいています。」

Computerworld、2001 年 11 月 30 日

侵入とその損失の防止による ROI

シグニチャでは防止できない、新しい未知の攻撃による損害のコストは甚大です。ウィルスの増殖により、ユーザのダウンタイム、機密情報の損失、世評の低下、システム再構築にかかるコストなど、数十億ドルの損害が発生しました。

CSI による 2002 年の調査では、回答企業のうち 90 % が、従来型のセキュリティソリューションを展開していたにもかかわらず、2001 年に何らかの侵入を受けています。侵入により発生したコストは企業ごとに異なりますが、現在の危険度を評価する際、以下の数字は考慮に入れる価値があります。

- 調査会社 Computer Economics 社によると、以下の攻撃が原因で発生した世界的な損害額の概算が明らかになっています。
 - Slammer : 10 億ドル
 - Bugbear : 9.5 億ドル
 - Nimda : 6.35 億ドル
 - Code Red : 26.2 億ドル
 - SirCam : 11.5 億ドル
- American Society for Industrial Security とコンサルティング企業 PricewaterhouseCoopers 社の調査によると、2001 年、Fortune 1000 企業では機密情報の盗難により 590 億ドルの損失が発生しています。
- Meta Group 社の 2003 年の調査によると、90 % 以上の企業がアンチウィルスソフトウェアを使用しているにもかかわらず、多くの企業が年平均 283,000 ドルの金銭的被害を受けています。
- [CSIS]CSI/FBI の 2003 年の調査によると、251 社で 2.02 億ドル以上の損失が報告されています。

まとめ

Cisco Security Agent のような予防的なセキュリティソリューションを実装すると、以下の理由により、高い投資回収率が実現されます。

- サーバおよびデスクトップの冗長化および二重化テクノロジーの代用または置き換えとして機能する
- シグニチャアップデートの作業負荷がない

- シグニチャアップデートの谷間でも危険にさらされない
- False Positive およびイベント管理の作業負荷がない
- ネットワークのダウンタイムが発生しにくくなる

シグニチャベースの製品では防御できない新しい未知の攻撃に対して、システムが保護されます。

これらの攻撃を受けると、システムのダウンタイム、世評の低下、機密情報の損失など、大きな被害が発生します。

©2003 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-6670-2992

電話でのお問合せは、以下の時間帯で受け付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先