5 次世代エンドポイント セキュリティ ソリューションを選択するための 5 つのヒント

1 防止機能
サイバー攻撃を防止し、マルウェアを進入時点でリアルタイムにブロック

防止機能は、防御の最前線となります。次世代エンドポイント セキュリティ製品に次の機能が搭載されていることを確認してください。

- グローバル脅威インテリジェンス：24 時間体制でお客様を保護するため、最新の脅威を検出し、ゼロデイ攻撃を発見する、脅威調査担当者チーム。
- シグニチャベースの AV 検出：次世代エンドポイント セキュリティ ソリューションに AV 処理を実行させ、保護機能を 1 つのエージェントに統合します。
- 組み込みサンドボックス：サードパーティのサンドボックスを導入せずに、疑わしい脅威に関する静的および動的な分析を実行できます。
- プロアクティブな保護：脆弱性を特定して解決し、拡散度が低い疑わしい実行ファイルを実際に問題となる前に分析して停止します。

2 継続的な監視と記録
いつでも、どこでも、あらゆるものを監視

100 % 防止することはできません。高度なマルウェアが侵入する可能性があります。このため、次世代エンドポイント セキュリティ製品には次の機能が備わっている必要があります。

- 処理したかどうかに関係なく、エンドポイントのすべてのファイルを継続的に監視する機能。
- 悪意のある動作や侵入の痕跡を特定する機能。
- ファイル アクティビティ履歴の記録。これにより、最初から最後までセキュリティ侵害の範囲を特定できます。
- マルウェアがどこから侵入し、どこに潜んでおり、何を行っているかを可視化する機能。

3 短い検出時間
脅威の検出にかかる時間が、日、週、月単位ではなく、数時間または数分に

発生した侵害の検出にかかる業界標準の平均検出時間は 100 日です。次世代エンドポイント セキュリティ ソリューションでは、次の機能により数分または数時間でこのような違反を検出できなければなりません。

- すべてのエンドポイントでのデータ、ファイル アクティビティ、および通信の継続的な監視と相関付け
- 最新の侵入の痕跡（IoC）およびほとんどの動作指標の使用
- 脅威アラートの優先度設定。これにより、最も拡散している脅威を最初に解決できます。

4 シンプルな自動対応
迅速かつ効果的な対応

包括的かつ迅速な対応が必要です。次世代エンドポイント セキュリティ ソリューションでは、次のようにできる必要があります。

- すべてのエンドポイントで IoC またはマルウェア アーティファクトを容易に検出でき、これにより調査にかかる時間が短縮され、複雑さが低減する。
- エンドポイントおよびネットワーク全体にわたって、マルウェア侵害の状況を最初から最後まで容易に把握できる。
- PC、Mac、Linux、モバイル デバイスを対象に、自動または数回のクリックでマルウェアに体系的に対応および修復できる。

5 統合型脅威防御
サイロ型製品の使用をやめて、体系的な保護と対応を実現。

多数のサイロ型ポイント製品を使い分けることは、作業スピードを低下させます。次世代エンドポイント セキュリティ ソリューションをはじめとするセキュリティ ツールは、大規模な統合脅威防御システムでそれぞれの役割を果たし、次のことを必要とします。

- 連携してセキュリティ ギャップを解消し、セキュリティ エコシステム全体で脅威を迅速に検出できるセキュリティ テクノロジーで構成される統合システム。
- エンドポイントからネットワーク、メール、Web まで、あらゆる場所で保護を提供するクラウドベース テクノロジー。
- 脅威に関する情報とイベント データがすべてのセキュリティ ツールで共有および相関付けされ、共通の形式でセキュリティ チームに通知されること。

www.cisco.com/jp/go/ampendpoint