目次

概要

この資料はウイルスがエンドユーザ用のローカル アンチウィルスを持っていることに関するエンタープライズ ネットワークおよび Cisco の推奨事項にどのようにの導入されるか例を記述したものです。

ESA でアンチウィルス Sophos か McAfee を有効に する場合それにもかかわらずデスクトップ アンチウィルスを必要としますか。

はい。 アンチウィルス認可されるを使っておよび、これ最初の層防御だけウイルスがエンドユーザに達することを防ぐことに電子メール Secuirty アプライアンス (ESA) で有効に されて。

ウイルスは電子メールでのほかの多くの方法でエンタープライズ ネットワークに運ばれます。 悪意のある Webページはウイルスをインジェクトできます。 感染させたラップトップは外部ネットワークから持って来られるかもしれません。 removeable メディアで持って来られ、企業 マシンにロードされる感染したファイルは無知エンドユーザ用の毎日発生です。 Malware 作成者は感染させた attachements があるのに社会工学は使用し、わかっているメッセージ アクティブにコードし、標準的なセキュリティ安全対策をバイパスする方法を見つけ出します。 これらはウイルスがエンタープライズ ネットワークに導入されるかもしれないことちょうど少数、簡単な方法です。

各ウイルス スキャナーが各ウイルスをつかまえないし、各アンチウィルス ベンダーがウイルス定義ファイルを同時にアップデートしません。 さらに、ウイルスがエンタープライズ ネットワークにどのようにによって入るか、各ウイルス スキャナーがすべてのウイルスを見ません。 たとえば、Webベース ウイルスはパススルー 企業電子メール システム、または内部で感染させたコンピュータはネットワーク内からの電子メール耐えられたウイルスを送信 するかもしれ、ESA を通ることを避けます。

Cisco はエンタープライズ ネットワークの中のすべてのエンドユーザ用に保護の追加層を提供する最新ローカル アンチウィルス アプリケーションかセキュリティ スイートがあることを推奨します。 ネットワークのためのすべての先頭のウイルス エントリに対して守るために多層ウイルス 防衛 システムを維持することは重要です。