

# ESA に関する FAQ : ESA で Sophos や McAfee を有効にした場合、さらにデスクトップのウイルス対策が必要ですか。

## 目次

### [はじめに](#)

[ESA で Sophos や McAfee を有効にした場合、さらにデスクトップのウイルス対策が必要ですか](#)

[。](#)

## 概要

この資料はウイルスがエンドユーザ用のローカル アンチウイ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導入されるか例を記述したものです。

## ESA で Sophos や McAfee を有効にした場合、さらにデスクトップのウイルス対策が必要ですか。

はい。 アンチウイ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メール Security アプライアンス (ESA) で有効にされて。 層にされた縦深防御 アプローチのためのエンタープライズ ネットワーク セキュリティ呼び出しの最良の方法。 それはエンドユーザを ESA のようなこのような理由でローカルで提供します、またデスクトップ アンチウイルス多くのエンタープライズ ネットワークがだけでなく、サーバ側のアンチウイルスを設定することを選択したことです。

ウイルスは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、エンタープライズ 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 attachments 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、各アンチウイルス 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 ウィルスはパススルー エンタープライズ 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 アンチウイルス 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。