ESA FAQ: Do I still need desktop anti−virus if I enable Sophos or McAfee Anti−Virus on my ESA?

Document ID: 118101

Contributed by Nasir Shakour and Robert Sherwin, Cisco TAC Engineers.

Jul 29, 2014

Contents

Introduction

This document describes examples of how viruses are introduced into an enterprise network and Cisco's recommendation for having local anti−virus for end−users.

Do I still need desktop anti−virus if I enable Sophos or McAfee Anti−Virus on my ESA?

Yes. With anti−virus licensed and enabled on the Email Secuirty Appliance (ESA), this only a first layer defense to preventing viruses from reaching end−users. Best practices in enterprise network security call for a layered defense−in−depth approach. It is for this reason that many enterprise networks have chosen to not only implement server−side anti−virus, such as the ESA provides, but also desktop anti−virus locally for end−users.

Viruses are carried into an enterprise network in many ways besides via email. Malicious web pages can inject viruses. An infected laptop may be brought in from an outside network. Infected files brought in on removeable media and loaded to an enterprise machine are a daily occurence for unknowing end−users. Malware authors use social engineering to have their infected attachements, code, and messages actively aware and find ways to bypass standard security measures. These are just a few, simple methods that a virus may be introduced into an enterprise network.

Not every virus scanner will catch every virus, and not every anti−virus vendor updates their virus definition files at the same time. In addition, depending on how viruses enter the enterprise network, not every virus scanner will see all viruses. For example, a web−based virus would not pass through the enterprise email system, or an internally infected computer may send email−borne viruses from within your network and avoids passing through through the ESA.

Cisco recommends that you have a up−to−date local anti−virus application or security suite that will provide an additional layer of protection for all end−users with−in an enterprise network. It is vital to maintain a multi−layered virus defense system to guard against virus entry on all fronts for your network.