

ESA FAQ: Heb ik nog steeds desktop anti-virus nodig als ik Sophos of McAfee Anti-Virus inschakelen op mijn ESA?

Inhoud

[Inleiding](#)

[Heb ik nog steeds desktop anti-virus nodig als ik Sophos of McAfee Anti-Virus op mijn ESA inschakelt?](#)

Inleiding

In dit document worden voorbeelden beschreven van de manier waarop virussen in een ondernemingsnetwerk worden geïntroduceerd en wordt de aanbeveling van Cisco beschreven voor het hebben van lokale antivirusprogramma's voor eindgebruikers.

Heb ik nog steeds desktop anti-virus nodig als ik Sophos of McAfee Anti-Virus op mijn ESA inschakelt?

Ja. Met anti-virus gelicentieerd en ingeschakeld op de Email Security Applicatie (ESA) is dit slechts een eerstelijnsverdediging om te voorkomen dat virussen de eindgebruikers bereiken. De beste praktijken op het gebied van bedrijfsnetwerkbeveiliging vereisen een gelaagde verdediging-in-diepte benadering. Om deze reden hebben veel ondernemingsnetwerken ervoor gekozen om niet alleen server-side anti-virus te implementeren, zoals de ESA biedt, maar ook desktop anti-virus lokaal voor eindgebruikers.

Virussen worden op vele manieren in een ondernemingsnetwerk gebracht, behalve via e-mail. Kwaadaardige webpagina's kunnen virussen injecteren. Een geïnfectede laptop kan van een buitennetwerk worden gebracht. Geïnfectede bestanden die op verwijderbare media worden ingevoerd en in een bedrijfsmachine worden geladen, zijn een dagelijkse praktijk voor onbekenden. Malware auteurs gebruiken social engineering om hun geïnfectede bijlagen, code en berichten actief bewust te maken en manieren te vinden om standaard beveiligingsmaatregelen te omzeilen. Dit zijn slechts een paar eenvoudige methoden die ervoor zorgen dat een virus kan worden geïntroduceerd in een ondernemingsnetwerk.

Niet elke virusscanner zal elk virus vangen, en niet elke anti-virusverkoper werkt hun virusdefinitie bestanden op hetzelfde moment. Bovendien, afhankelijk van hoe virussen het ondernemingsnetwerk binnenkomen, niet zal elke virusscanner alle virussen zien. Zo zou een webgebaseerd virus niet door het e-mailsysteem van de onderneming gaan, of een intern geïnfectede computer kan e-mailvirussen verzenden vanuit uw netwerk en vermijdt het passeren door de ESA.

Cisco raadt u aan een bijgewerkte lokale antivirusapplicatie of beveiligingssuite te hebben die een extra beschermingslaag biedt voor alle eindgebruikers die in een ondernemingsnetwerk werken. Het is van vitaal belang om een meerlaagse virusverdediging te onderhouden om te beschermen tegen het binnendringen van virussen op alle fronten voor uw netwerk.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.