ESA常見問題：如果在ESA上啟用Sophos或McAfee防病毒，是否仍需要案頭防病毒？

目錄

[簡介](#)
[如果在ESA上啟用Sophos或McAfee防病毒，是否仍需要案頭防病毒？](#)

簡介

本文舉例說明如何將病毒引入企業網路，以及思科就為終端使用者提供本地防病毒的建議案。

如果在ESA上啟用Sophos或McAfee防病毒，是否仍需要案頭防病毒？

會。 在郵件安全裝置(ESA)上獲得防病毒許可並啟用後，這僅僅是防止病毒到達終端使用者的第一層防禦。 企業網路安全的最佳實踐要求採用分層縱深防禦方法。因此，許多企業網路選擇不僅實施伺服器端防病毒(如ESA)，而且還在本地為終端使用者實施案頭防病毒。

病毒除了通過郵件之外，還以多種方式進入企業網路。惡意網頁可能會感染病毒。 受感染的筆記型電腦可能從外部網路送入。 對於不知情的終端使用者而言，每天都會出現通過可移動介質進入並載入到企業電腦中的感染病毒檔案。 惡意軟體編寫者使用社會工程手段主動瞭解其受感染的附件、代碼和消息，並找到繞過標準安全措施的方法。 這些只是將病毒引入企業網路的一些簡單方法。

不是每個病毒掃描程式都能捕獲到每個病毒，也不是每個防病毒供應商都同時更新其病毒定義檔案。此外，根據病毒進入企業網路的方式，並非每個病毒掃描程式都能看到所有病毒。例如，基於Web的病毒不會通過企業電子郵件系統，或者內部感染的電腦可能從您的網路內部傳送電子郵件傳播病毒，並避免通過ESA。

思科建議您擁有最新的本地防病毒應用程式或安全套件，可為企業網路中的所有終端使用者提供額外的保護。 維護多層病毒防禦系統對於防止病毒進入您的網路的所有方面至關重要。