ESA FAQ:ESA에서 Sophos 또는 McAfee Anti-Virus를 활성화할 경우 데스크톱 안티바이러스가 계속 필요합니까?

목차

소개

이 문서에서는 엔터프라이즈 네트워크에 바이러스가 유입되는 방법과 최종 사용자를 위한 로컬 안티바이러스 사용에 대한 Cisco의 권장 사항에 대해 설명합니다.

ESA에서 Sophos 또는 McAfee Anti-Virus를 활성화할 경우 데스크톱 안티바이러스가 계속 필요합니까?

예. ESA(Email Security Appliance)에서 안티바이러스 라이센스가 부여되고 활성화된 경우, 이는 바이러스가 최종 사용자에게 감염되지 않도록 방지하는 첫 번째 레이어 방어만 가능합니다. 엔터프라이즈 네트워크 보안 모범 사례에서는 계층화된 심층 방어 방식을 요구합니다.이러한 이유로 많은 엔터프라이즈 네트워크에서 ESA가 제공하는 것과 같은 서버측 안티바이러스를 구현할 뿐만 아니라 최종 사용자를 위해 로컬로 데스크톱 안티바이러스를 구현하도록 선택했습니다.

바이러스는 이메일 외에도 여러 가지 방법으로 엔터프라이즈 네트워크에 전파됩니다.악성 웹 페이지에서 바이러스를 주입할 수 있습니다. 감염된 랩톱을 외부 네트워크에서 가져올 수 있습니다. 감염된 파일은 원격 가능한 미디어에 가져와 엔터프라이즈 시스템에 로드되어 엔드 유저를 모르는 경우가 많습니다. 악성코드 개발자는 소셜 엔지니어링을 사용하여 감염된 첨부 파일, 코드 및 메시지를 적극적으로 인식하고 표준 보안 조치를 우회할 방법을 찾습니다. 엔터프라이즈 네트워크에 바이러스가 유입될 수 있는 간단한 몇 가지 방법입니다.

모든 바이러스 검사 프로그램이 모든 바이러스를 탐지하는 것은 아니며, 모든 안티바이러스 공급업체가 바이러스 정의 파일을 동시에 업데이트하는 것은 아닙니다.또한 바이러스가 엔터프라이즈 네트워크에 유입되는 방식에 따라 모든 바이러스 스캐너에서 모든 바이러스가 표시되는 것은 아닙니다.예를 들어, 웹 기반 바이러스가 엔터프라이즈 이메일 시스템을 통과하지 못하거나 내부적으로 감염된 컴퓨터가 네트워크 내에서 이메일 기반 바이러스를 전송하여 ESA를 통과하는 것을 방지할 수 있습니다.

Cisco는 엔터프라이즈 네트워크에 있는 모든 최종 사용자에게 추가 보호 계층을 제공할 최신 로컬 안티바이러스 애플리케이션 또는 보안 제품군을 권장합니다. 네트워크의 모든 전선에서 바이러스 침투를 방지하기 위해서는 멀티레이어 바이러스 방어 시스템을 유지해야 합니다.