Mac용 Symantec™ Endpoint Protection 14.3 RU1 클라이언트 설명서

2020년 11월

Symantec Endpoint Protection의 Mac 보호 방법

Symantec Endpoint Protection에서는 여러 보호 계층을 합쳐 시스템을 바이러스 및 스파이웨어 공격과 침입 시도로부터 보호합니다.

보호 유형에서는 각 보호 계층을 설명합니다.

Table 1: 보호 유형

차단	설명
바이러스 및 스파이웨어 차단	Symantec Endpoint Protection에는 예약 바이러스 검사, 요청 시 검사 및 백그라운드에서 실행되어 바이러스를 모니터링하는 자동 보호가 포함되어 있습니다. 바이러스가 발견되면 Symantec Endpoint Protection에서 이를 제거합니다. 바이러스 및 스파이웨어 차단 기능으로 Mac을 보호하는 방법
네트워크 위협 요소 차단	Symantec Endpoint Protection에서는 네트워크 계층에서 데이터를 가로챕니다. 시그니처를 사용하여 패킷 또는 패킷 스트림을 검사합니다. 네트워크 공격 또는 브라우저 공격에 해당하는 패턴을 찾아 개별적으로 각 패킷을 검사합니다. 네트워크 위협 요소 차단에는 다음이 포함됩니다. • 침입 차단: 운영 체제 구성 요소 및 응용 프로그램 계층에서 공격을 탐지합니다. Symantec Endpoint Protection에서 네트워크 위협 요소가 탐지되면 이를 차단합니다. • 방화벽: 방화벽 정책 및 규칙에 따라 네트워크 트래픽을 허용하거나 차단합니다. (버전 14.2부터.) 네트워크 위협 요소 차단 기능으로 Mac을 보호하는 방법
장치 제어	Symantec Endpoint Protection Manager 관리자가 장치 제어 정책을 구성합니다. 이 정책에서 장치 이름, 장치 공급업체, 장치 모델 또는 일련 번호를 기준으로 장치를 차단하거나 차단 해제할 수 있습니다. 중앙 관리 클라이언트의 경우 고급 탭에서 장치 제어에 대한 설정을 볼 수 있습니다. 단독 실행 클라이언트에는 장치 제어를 사용할 수 없습니다. Mac용 Symantec Endpoint Protection 클라이언트에 대한 장치 제어
엔드포인트 탐지 및 응답	Symantec Endpoint Protection Manager 관리자는 의심스러운 네트워크 활동을 감지하고 노출할 수 있는 수단을 제공하는 활동 레코더 정책을 구성합니다.

클라이언트는 바이러스 정의, IPS 정의 및 제품 업데이트를 사용자 시스템에 자동으로 다운로드합니다.

바이러스 정의, 침입 차단 정의 및 클라이언트 소프트웨어 업데이트

바이러스 및 스파이웨어 차단 기능으로 Mac을 보호하는 방법

Symantec Endpoint Protection에서는 바이러스 정의를 사용하여 예약 검사 및 수동 검사 도중 알려진 바이러스를 탐지합니다. 자동 보호 기능은 바이러스 정의를 사용하여 시스템 활동을 지속적으로 검사합니다.

Symantec Endpoint Protection에서 바이러스 또는 기타 보안 위험 요소를 발견하면 사용자에게 알립니다. 다음 중 하나에 해당되는 경우 바이러스 또는 기타 보안 위험 요소가 발견된 것입니다.

- 자동 보호 기능이 시스템을 모니터링하는 중 바이러스를 발견한 경우
- 자동 보호 기능이 예약 검사 또는 수동 검사를 통해 바이러스를 발견한 경우

기본 설정으로 실행된 경우 Symantec Endpoint Protection은(는) 발견된 바이러스를 자동 복구하려고 시도합니다. 파일을 복구할 수 없는 경우 클라이언트는 해당 파일을 안전하게 검역소에 보관하여 시스템이 손상을 입지 않도록 합니다. 일반적으로 클라이언트는 이러한 복구 작업을 자동으로 수행합니다. 시스템에서 바이러스가 발견되면 이에 대한 정보를 시만텍에 제출할 수 있습니다.

일부 경우 발견한 감염된 파일을 복구, 삭제 또는 복원할지 선택하라는 메시지가 표시됩니다. 사용자의 선택에 따라 감염된 파일이 클라이언트에서 처리됩니다.

감염 및 위험 요소 탐지 관련 메시지에 응답

시만텍에 보안 정보 제출 실행 또는 실행 중지

네트워크 위협 요소 차단 기능으로 Mac을 보호하는 방법

네트워크 위협 요소 차단에는 다음 보호 기술이 포함됩니다.

- 침입 차단
- 방화벽

침입 차단

침입 차단은 네트워크 공격을 자동으로 탐지하고 차단합니다. 침입 차단은 클라이언트 시스템을 보호하는 내부 방어 계층입니다. 침입 차단은 IPS(침입 차단 시스템)라고도 합니다.

침입 차단은 네트워크 계층에서 데이터를 가로챕니다. 시그니처를 사용하여 패킷 또는 패킷 스트림을 검사합니다. 네트워크 공격 또는 브라우저 공격에 해당하는 패턴을 찾아 개별적으로 각 패킷을 검사합니다. 침입 차단은 운영 체제 구성 요소 및 응용 프로그램 계층에서 공격을 탐지합니다.

침입 차단은 시그니처를 사용하여 클라이언트 시스템에서 공격을 식별합니다. 알려진 공격의 경우 침입 차단이 시그니처와 일치하는 패킷을 자동으로 삭제합니다.

방화벽

방화벽은 네트워크 트래픽을 모니터링하고 잠재적으로 해로운 트래픽을 차단하여 Mac 시스템을 보호합니다. Symantec Endpoint Protection 방화벽은 단독 실행 클라이언트에 사용할 수 없습니다.

Symantec Endpoint Protection 방화벽은 전송 및 인터넷 계층에서 트래픽을 모니터링합니다. 내장 Mac 방화벽은 Symantec Endpoint Protection 방화벽이 트래픽을 모니터링한 후 더 높은 계층인 응용 프로그램 계층에서 트래픽을 모니터링합니다. 따라서 두 방화벽을 모두 실행하여 동시에 실행할 수 있습니다.

방화벽은 다음 유형의 규칙을 사용하여 네트워크 트래픽을 허용 또는 차단합니다.

- 기본 규칙
- 사용자 정의 규칙
- 내장 규칙
- 보호 규칙

이러한 규칙에는 포트 검사 감지, 서비스 거부 탐지, MAC 위장 접근 방지, 스마트 DHCP 및 스마트 DNS가 포함됩니다. 방화벽 설정은 오로지 Symantec Endpoint Protection Manager 관리자만 제어할 수 있습니다. 사용자는 관리자가 Mac을 통한 클라이언트 제어를 허용한 경우에만 방화벽을 실행하거나 실행 중지할 수 있습니다.

방화벽 보호는 버전 14.2에서 추가되었습니다.

침입 차단 관리

Mac 클라이언트의 방화벽 보호 관리

Mac용 Symantec Endpoint Protection의 운영 체제 호환성

Mac용 Symantec Endpoint Protection에서는 다음 운영 체제 버전을 지원합니다.

- macOS 10.15 ~ 10.15.5
- macOS 10.14
- macOS 10.13

이전 Mac 운영 체제 버전에 대한 지원과 관련된 추가 정보는 Mac compatibility with the Endpoint Protection client(영문)를 참조하십시오.

Symantec Endpoint Protection for macOS 10.13 이상의 커널 확장 인증

Release notes, new fixes, and system requirements for all versions of Endpoint Protection(영문)

Mac용 Symantec Endpoint Protection 클라이언트 설치

원격 강제 설치를 사용할 수 없거나 사용을 원치 않는 경우 Mac 시스템에 직접 Symantec Endpoint Protection 클라이언트를 설치할 수 있습니다. 클라이언트가 단독 실행형이든 중앙 관리형이든 단계는 유사합니다.

관리되는 클라이언트를 설치하는 유일한 방법은 Symantec Endpoint Protection Manager에서 생성된 패키지를 사용하는 것입니다. Mac 클라이언트로 클라이언트-서버 통신 설정을 가져와서 언제든지 단독 실행 클라이언트를 중앙 관리 클라이언트로 전환할 수 있습니다.

NOTE
Mac용 Symantec Endpoint Protection 클라이언트가 타사 원격 배포 소프트웨어 사용에 대비하도록 하려면 Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper(영문)를 참조하십시오.

Table 2: Mac 클라이언트를 설치하는 방법

설치 파일을 다운로드한 경우	1. Mac 시스템의 폴더로 해당 컨텐츠를 추출한 다음 폴더를 여십시오. 2. `SEP_MAC`을 여십시오. 3. `Symantec Endpoint Protection.dmg`를 Mac 시스템의 데스크톱에 복사하십시오. 4. `Symantec Endpoint Protection.dmg`를 두 번 눌러 파일을 가상 디스크로 마운트하십시오. 그러면 Mac용 Symantec Endpoint Protection 클라이언트가 설치됩니다.
Broadcom 지원 포털에서 받은 클라이언트 설치 패키지 .zip이 있는 경우	1. Mac 시스템의 바탕 화면에 파일을 복사합니다. 이 파일의 이름은 `Symantec Endpoint Protection.zip` 또는 `Symantec_Endpoint_Protection_version_Mac_Client.zip`일 수 있으며, 여기서version부분은 제품 버전입니다. 2. 연결 프로그램 **> Archive Utility**를 마우스 오른쪽 버튼으로 눌러 파일의 컨텐츠를 추출하십시오. 3. 최종 폴더를 여십시오. 그러면 Mac용 Symantec Endpoint Protection 클라이언트가 설치됩니다.

생성된 가상 디스크 이미지 또는 폴더에는 응용 프로그램 설치 프로그램과 추가 리소스 폴더가 포함되어 있습니다. 설치가 성공하려면 두 항목이 동일한 위치에 있어야 합니다. 설치 프로그램을 다른 위치에 복사하면 추가 리소스도 복사해야 합니다.

Mac용 Symantec Endpoint Protection 클라이언트를 설치하려면 다음과 같이 하십시오.

1. `Symantec Endpoint Protection ##`를 두 번 누르십시오.
2. 설치를 눌러 설치를 시작하십시오.
3. Symantec Endpoint Protection 클라이언트 설치에 필요한 도우미 도구를 설치하려면 Mac 관리자의 사용자 이름과 암호를 입력한 다음 도우미 설치**(Install Helper)**를 누르십시오.
4. 설치 후 Symantec Endpoint Protection 클라이언트 설정을 계속 완료하려면 계속을 누르십시오.
5. Symantec Endpoint Protection 클라이언트를 설정하려면 다음 단계를 수행하십시오.

Symantec Endpoint Protection 시스템 확장 인증	보안 및 개인 정보 보호 대화 상자의 일반 탭에서 응용 프로그램 **"Symantec Endpoint Protection"**의 시스템 소프트웨어가 차단되어 로드할 수 없습니다. 옆의 허용을 누르십시오. 필요한 경우 잠금 아이콘을 눌러 변경하십시오. Symantec Endpoint Protection의 완벽한 작동을 위해서는 시스템 확장을 인증해야 합니다. Symantec Endpoint Protection for macOS 10.15 이상의 시스템 확장 인증
전체 디스크 액세스 허용	보안 및 개인 정보 보호 대화 상자의 개인 정보 보호 탭에서 **Symantec** 시스템 확장이 Mac 장치의 모든 사용자에 대한 데이터 및 관리 설정에 액세스할 수 있는지 확인하십시오. 필요한 경우 잠금 아이콘을 눌러 변경하십시오.
네트워크 프로필 변경 허용	**Symantec Endpoint Protection**에서 네트워크 콘텐츠를 필터링하려고 합니다.라는 메시지가 표시되면 허용을 누르십시오.

6. 완료를 누르십시오.

Symantec Endpoint Protection for macOS 10.15 이상의 시스템 확장 인증

시스템 확장 인증 요구는 macOS 10.15의 보안 기능입니다. Symantec Endpoint Protection의 완벽한 작동을 위해서는 시스템 확장을 인증해야 합니다.

Symantec Endpoint Protection의 시스템 확장을 인증하려면 Symantec Endpoint Protection 클라이언트 설정 시 보안 및 개인 정보 보호 대화 상자의 일반 탭에서 응용 프로그램 **"Symantec Endpoint Protection"**의 시스템 소프트웨어가 차단되어 로드할 수 없습니다. 옆의 허용을 누르십시오.

Mac용 Symantec Endpoint Protection 클라이언트 설치

Mac용 Symantec Endpoint Protection 클라이언트에 대한 업그레이드 프롬프트

Symantec Endpoint Protection Manager 관리자가 클라이언트 설치 설정을 포함한 클라이언트 설치 패키지를 할당하여 관리되는 클라이언트 시스템을 자동으로 업그레이드할 수 있습니다.

Mac에 로그온되어 있는 경우 설치를 완료하기 위해 재시작하라는 프롬프트가 나타날 수 있습니다. 클라이언트 설치 설정을 기준으로 이 재시작을 지연시킬 수 있습니다.

Mac에 로그온되어 있지 않다면 설치에서 Mac을 자동으로 재시작합니다.

Symantec Endpoint Protection 클라이언트 시작

해결해야 할 문제가 없다면 Symantec Endpoint Protection 클라이언트를 열 때 보호 중**(You are Protected)**이라는 메시지가 페이지의 맨 위에 표시됩니다. 문제를 해결해야 할 경우에는 해결을 누르십시오.

Symantec Endpoint Protection 클라이언트는 수행할 수 있는 주요 태스크를 표시합니다.

Table 3: Symantec Endpoint Protection 클라이언트 페이지

옵션	설명
보안	시스템의 보호 상태를 보여 줍니다.
검사	시스템을 검사할 수 있습니다. 빠른 검사를 실행할지 또는 전체 검사를 실행할지 선택할 수 있습니다. 파일 또는 폴더를 끌어 와서 검사할 수도 있습니다. 수동 검사 실행
LiveUpdate	LiveUpdate를 실행하여 Symantec Endpoint Protection의 정의 및 제품 파일을 업데이트합니다. Symantec Endpoint Protection에서 컨텐츠를 즉시 업데이트
고급	바이러스 및 스파이웨어 차단, 네트워크 위협 요소 차단 및 LiveUpdate에 대한 자세한 옵션을 제공합니다.

Symantec Endpoint Protection에서의 Mac 보호 기능 관리

Symantec Endpoint Protection의 기본 설정은 다양한 유형의 멀웨어로부터 Mac을 보호합니다. 클라이언트가 멀웨어를 자동으로 처리하거나 사용자가 멀웨어를 처리하는 방법을 선택할 수 있습니다.

관리자가 지정한 설정에 따라, 다음 태스크를 수행하여 보호 기능을 편리하게 관리할 수 있습니다.

NOTE
관리자가 이러한 태스크에 대한 제어를 사용자에게 제공하지 않았을 수도 있습니다.

Table 4: 시스템 보호

단계	설명
1단계: 바이러스 및 스파이웨어 차단 기능과 네트워크 위협 요소 차단 기능이 둘 다 실행되고 있는지 확인	이러한 보호 기능이 실행되고 있는 경우에는 녹색 확인 표시와 함께 보호 중**(You are Protected)**이라는 메시지가 표시된 보안 페이지가 나타납니다. 바이러스 및 스파이웨어 차단 실행 및 실행 중지 네트워크 위협 요소 차단 실행 또는 실행 중지
2단계: 소프트웨어 및 정의가 최신 상태인지 확인	보안 페이지에는 바이러스 및 스파이웨어 차단과 네트워크 위협 요소 차단의 정의가 마지막으로 업데이트된 시간이 표시되어 있습니다. 마지막 제품 업데이트 시간은 **LiveUpdate**에서 확인할 수 있습니다. 소프트웨어 버전 번호를 확인하려면 도움말 **>** 정보를 누르십시오.
3단계: 필요한 경우 소프트웨어 또는 정의 업데이트	Symantec Endpoint Protection 클라이언트에서 **LiveUpdate**를 눌러 소프트웨어 및 정의를 즉시 업데이트하십시오. 바이러스 정의, 침입 차단 정의 및 클라이언트 소프트웨어 업데이트
4단계: 검사 실행	검사가 정기적으로 실행되도록 예약하거나 지금 바로 검사를 실행할 수 있습니다. 예약 검사 설정 수동 검사 실행

바이러스 및 스파이웨어 차단 설정 관리

제품 라이센스 연장

메뉴 표시줄에서 Symantec Endpoint Protection 클라이언트 아이콘 아래에 Symantec Endpoint Protection의 라이센스가 만료되었다는 메시지가 표시될 수 있습니다. Symantec Endpoint Protection 클라이언트는 라이센스를 사용하여 다음 항목을 업데이트합니다.

- 클라이언트 소프트웨어
- 바이러스 및 스파이웨어 검사와 침입 차단을 위한 보호 정의 파일

클라이언트는 평가판 라이센스 또는 유료 라이센스를 사용할 수 있습니다. 라이센스가 만료된 경우 클라이언트는 정의 또는 클라이언트 소프트웨어를 업데이트하지 않습니다.

이러한 라이센스 유형의 경우 해당 라이센스를 업데이트하거나 연장하려면 관리자에게 문의해야 합니다.

감염 및 위험 요소 탐지 관련 메시지에 응답

Mac용 Symantec Endpoint Protection 클라이언트에서 장치 제어 실행 또는 실행 중지

Symantec Endpoint Protection Manager 관리자가 장치 제어 정책을 사용하여 관리되는 클라이언트를 구성할 수 있습니다. 이 정책에서 장치 이름, 장치 공급업체, 장치 모델 또는 일련 번호를 기준으로 장치를 차단하거나 차단 해제할 수 있습니다.

고급 페이지에서 작업 **>** 보안 기록**(Security History)**을 눌러 장치 제어 활동을 확인할 수 있습니다.

장치 제어를 위한 Symantec Endpoint Protection 클라이언트의 설정을 사용하여 장치 제어를 실행하거나 실행 중지할 수 있습니다. 장치 제어를 실행한 경우 선택적으로 장치가 차단되거나 차단 해제될 때 통지를 실행하거나 실행 중지할 수 있습니다.

설정을 변경하려면 Mac 관리자 인증 정보를 사용하여 인증해야 합니다. 이러한 설정이 회색으로 표시되는 경우 사용자가 이 기능을 실행하거나 실행 중지하지 못하도록 관리자가 기능을 잠근 것입니다.

Symantec Endpoint Protection 클라이언트 인터페이스를 통해 차단되거나 차단 해제되는 장치를 추가하거나 편집할 수 없습니다.

> **NOTE**
> Symantec Endpoint Protection Manager의 장치 제어 정책은 장치 제어 설정을 제어합니다. 다음 하트비트에 이러한 설정에 수행한 모든 변경 사항이 정책에 기술된 설정으로 되돌아갑니다.

단독 실행 클라이언트에는 장치 제어를 사용할 수 없습니다.

Mac 클라이언트용 WSS 트래픽 리디렉션

WTR(Web Security Service(WSS) 트래픽 리디렉션)은 Symantec Web Security Service로의 트래픽 리디렉션을 자동화하고 Symantec Endpoint Protection을(를) 사용하는 각 시스템의 웹 트래픽을 보호합니다.

관리자는 프록시 구성 URL, 선택적 Symantec Web Security Service 루트 인증서 등 WSS 트래픽 리디렉션에 사용되는 설정을 제어합니다. 이러한 설정은 Symantec Endpoint Protection Manager 관리자만 구성할 수 있으며 Symantec Endpoint Protection 클라이언트 UI에 표시되지 않습니다. Mac에서 프록시 구성 파일 URL은 시스템 환경설정 **>** 네트워크의 프록시에서 볼 수 있습니다. 클라우드 서비스 인증서는 키체인에 표시됩니다.

WSS 트래픽 리디렉션은 Safari, Chrome 및 Firefox 버전 65 이상의 웹 브라우저에서 지원됩니다. 14.2 RU1 이전 버전의 Symantec Endpoint Protection만 Safari와 Chrome을 지원합니다.

Mac용 Symantec Endpoint Protection 클라이언트 제거

메뉴 표시줄에 있는 클라이언트 아이콘을 통해 Mac용 Symantec Endpoint Protection 클라이언트를 제거합니다. Mac용 Symantec Endpoint Protection 클라이언트를 제거하려면 관리 사용자 인증 정보가 필요합니다.

> **NOTE**
> Symantec Endpoint Protection 클라이언트를 제거한 후에는 제거를 완료하기 위해 클라이언트 시스템을 재시작하라는 메시지가 표시됩니다. 시작하기 전에 완료되지 않은 모든 작업을 저장하고 열려 있는 모든 응용 프로그램을 닫았는지 확인하십시오.

Mac용 Symantec Endpoint Protection 클라이언트를 제거하려면 다음과 같이 하십시오.

1. Mac 클라이언트 시스템에서 Symantec Endpoint Protection 클라이언트를 연 다음 **Symantec Endpoint Protection > Symantec Endpoint Protection** 제거를 누르십시오.
2. 제거를 다시 눌러 제거를 시작하십시오.
3. Symantec Endpoint Protection 클라이언트 제거에 필요한 도우미 도구를 설치하려면 Mac 관리자의 사용자 이름과 암호를 입력한 다음 도우미 설치**(Install Helper)**를 누르십시오.
4. **Symantec Endpoint Protection**이(가) 시스템 확장 프로그램을 수정하려고 합니다. 대화 상자에서 Mac 관리자의 사용자 이름 및 암호를 입력한 다음 확인을 누르십시오.

   클라이언트를 제거하려면 암호를 입력하라는 메시지가 나타날 수도 있습니다. 이 암호는 Mac의 관리 암호와는 다를 수 있습니다.
5. 제거가 완료되면 지금 재시작을 누르십시오.

제거가 실패하면 대체 방법을 사용하여 제거해야 할 수 있습니다. 다음 항목을 참조하십시오.

Uninstall Symantec Endpoint Protection(영문)

바이러스 정의, 침입 차단 정의 및 클라이언트 소프트웨어 업데이트

시만텍 제품은 현재 알려진 정보에 기반하여 새로 발견된 위협 요소로부터 시스템을 보호합니다. 시만텍은 이와 같은 정보를 LiveUpdate를 통해 Symantec Endpoint Protection에 제공하고 있습니다. LiveUpdate는 인터넷 연결을 통해 시스템을 위한 제품 업데이트 및 정의 업데이트를 수신합니다.

정의 업데이트는 최신 위협 요소 차단 기술을 사용하여 시만텍 제품을 최신 상태로 유지하는 파일입니다. LiveUpdate는 시만텍 인터넷 사이트에서 새로운 침입 차단 시그니처나 바이러스 정의 파일을 가져온 다음 이 파일로 기존의 파일을 대체합니다.

제품 업데이트는 설치된 클라이언트의 향상된 기능입니다. 제품 업데이트는 일반적으로 운영 체제 또는 하드웨어와의 호환성 확장, 성능 문제 조정 또는 제품 오류 수정을 목적으로 생성됩니다. 제품 업데이트는 필요할 때마다 릴리스됩니다. 클라이언트는 LiveUpdate 서버에서 직접 제품 업데이트를 수신합니다. 제품 업데이트와 정의 업데이트를 함께 컨텐츠 업데이트라고 합니다.

Table 5: 시스템에서 컨텐츠를 업데이트하는 방법

태스크	설명
컨텐츠를 즉시 업데이트	LiveUpdate를 즉시 실행할 수 있습니다. Symantec Endpoint Protection에서 컨텐츠를 즉시 업데이트

Symantec Endpoint Protection에서의 Mac 보호 기능 관리

Symantec Endpoint Protection에서 컨텐츠를 즉시 업데이트

LiveUpdate를 사용하여 정의 및 제품 파일을 즉시 업데이트할 수 있습니다. 다음과 같은 경우 LiveUpdate를 수동으로 실행해야 합니다.

- 최근에 클라이언트 소프트웨어를 설치한 경우.
- 마지막 검사 이후 오랜 시간이 경과된 경우.
- 바이러스 또는 기타 멀웨어 문제가 의심스러운 경우.

Symantec Endpoint Protection에서 컨텐츠를 즉시 업데이트하려면 다음과 같이 하십시오.

다음 방법 중 하나로 LiveUpdate를 시작하십시오.

- 메뉴 표시줄에서 Symantec Endpoint Protection 아이콘을 마우스 오른쪽 단추로 누른 다음 **LiveUpdate**를 누르십시오.
- Symantec Endpoint Protection 클라이언트를 연 다음 **LiveUpdate**를 누르십시오.

LiveUpdate는 구성된 LiveUpdate 서버에 연결하여, 사용할 수 있는 업데이트를 확인한 다음 이를 자동으로 다운로드 및 설치합니다. 다운로드 진행 상태가 상태 표시줄에 나타납니다.

바이러스 정의, 침입 차단 정의 및 클라이언트 소프트웨어 업데이트

예약에 따라 Symantec Endpoint Protection에서 컨텐츠 업데이트

관리되는 **Mac** 클라이언트의 예약

기본적으로 관리되는 Mac 클라이언트는 Symantec Endpoint Protection Manager에서 4시간마다 한 번씩 LiveUpdate가 실행되는 예약을 수신합니다. Symantec Endpoint Protection Manager 관리자가 이 예약을 제어합니다. 관리되는 클라이언트는 관리자가 생성한 예약을 제거, 수정 또는 확인하거나 새 예약을 생성할 수 있습니다.

단독 실행 **Mac** 클라이언트의 예약

예약 작업을 생성하여 예약된 시간 간격으로 LiveUpdate를 자동으로 실행할 수 있습니다. 시스템을 사용하지 않는 동안 LiveUpdate를 실행하도록 예약하는 것이 좋습니다.

예약에 따라 **Symantec Endpoint Protection**에서 컨텐츠를 업데이트하려면 다음과 같이 하십시오.

1. Symantec Endpoint Protection 클라이언트의 고급 페이지에서 제품 설정**(Product Settings)**을 누른 다음 예약된 **LiveUpdate(Scheduled LiveUpdate)**의 설정 아이콘을 누르십시오.

   현재 예약이 표시됩니다.

2. LiveUpdate 예약 드롭다운 메뉴에서 주기를 선택하십시오.

   초기 설정은 **4**시간마다 실행하는 것입니다. 매일 또는 매주 실행하도록 선택할 수도 있습니다. 이 경우 시간을 선택하거나 요일과 시간을 각각 선택합니다.

3. 변경 사항 적용을 누르십시오.

Symantec Endpoint Protection에서 컨텐츠를 즉시 업데이트

바이러스 정의, 침입 차단 정의 및 클라이언트 소프트웨어 업데이트

프록시 서버를 통한 관리 서버 연결 정보

Symantec Endpoint Protection에서 사용자의 인증 정보를 사용하여 프록시 서버를 통해 관리 서버에 연결할 수 있도록 허용할지를 확인할 수 있습니다. 인증 정보를 `symdaemon` 프로세스에서 액세스할 수 있도록 허용할지 묻는 메시지가 표시됩니다.

이 메시지에서 항상 허용을 눌러야 합니다. 그렇지 않으면 클라이언트가 LiveUpdate 서버와 통신할 때마다 동일한 메시지가 계속 표시됩니다. 거부를 누르면 클라이언트가 소프트웨어나 정의의 업데이트를 받을 수 없습니다.

바이러스 정의, 침입 차단 정의 및 클라이언트 소프트웨어 업데이트

바이러스 및 스파이웨어 차단 설정 관리

기본적으로 Symantec Endpoint Protection에서는 시스템이 시작되는 즉시 네트워크 위협 요소를 비롯한 바이러스 및 보안 위험 요소로부터 보호합니다. 프로그램이 실행되는 동안 바이러스를 검사하는 자동 보호 기능은 바이러스 및 스파이웨어 차단 기능에 포함되어 있습니다. 또한 시스템에서 바이러스나 보안 위험 요소가 존재할 수 있는 모든 활동을 모니터링합니다. 자동 보호는 바이러스가 시스템을 감염시키지 못하도록 차단하므로 자동 보호를 항상 실행 상태로 유지해야 합니다.

중앙 관리 클라이언트의 경우 이러한 설정을 어느 정도 제어할 수 있는지는 관리자가 클라이언트를 구성한 방식에 따라 달라집니다. 또한 이러한 설정에 수행한 모든 변경 사항은 다음 하트비트에서 정책에 기술된 설정으로 되돌아갑니다.

바이러스 및 스파이웨어 보호 관리에서는 Mac에서 바이러스 및 스파이웨어 차단 기능을 관리하기 위해 수행할 수 있는 태스크를 설명합니다.

Table 6: 바이러스 및 스파이웨어 차단 관리

단계	설명
1단계: 바이러스 및 스파이웨어 차단 실행 또는 실행 중지	바이러스 및 스파이웨어 차단 기능을 편리하게 실행 및 실행 중지할 수 있습니다. 이 기능은 실행 상태로 두는 것이 좋습니다. 바이러스 및 스파이웨어 차단 실행 및 실행 중지
2단계: 자동 보호 설정 사용자 정의	자동 보호는 바이러스 및 스파이웨어 차단의 중요한 부분입니다. 이러한 옵션은 고급 페이지에서 구성할 수 있습니다. 자동 보호 설정 및 검사 영역 설정 구성
3단계: 시스템에서 바이러스 검사	바이러스 검사는 예약에 따라 실행되거나 즉시 실행되도록 설정할 수 있습니다. 예약 검사 설정 검사를 일시 중지, 유휴 상태로 설정 및 중지 수동 검사 실행
4단계: Symantec Endpoint Protection에서 바이러스가 탐지되었을 때의 반응	Symantec Endpoint Protection에서는 시스템 검사 시 다음을 수행할 수 있습니다. • 사용자가 수행할 수 있는 작업을 알려 줍니다. • 사용자가 수행한 보호 작업에 대해 알려 줍니다. 감염 및 위험 요소 탐지 관련 메시지에 응답

바이러스 및 스파이웨어 차단 실행 및 실행 중지

자동 보호와 함께 바이러스 및 스파이웨어 차단은 기본적으로 실행됩니다.

특정 옵션을 설정하여 자동 보호를 더욱 구체적으로 제어해 볼 수 있습니다.

바이러스 및 스파이웨어 차단이 실행 중지된 경우에는 바이러스 및 스파이웨어 차단이 실행 중지됨이라는 메시지와 함께 빨간색 "x" 표시가 상태 페이지에 나타납니다. 이 보호 기능이 실행 중지되어 있다면 가능한 한 빨리 다시 실행해야 합니다.

NOTE
예약 검사는 바이러스 및 스파이웨어 차단의 실행 여부와 상관 없이 진행됩니다. 관리자에 의해 Symantec Endpoint Protection 설정 일부에 대한 액세스가 제한될 수 있습니다. 따라서 이러한 설정을 실행 중지하거나 검사를 예약하거나 보호 옵션을 사용자 정의하지 못할 수 있습니다. 이러한 설정을 변경하기 위해서는 Mac 관리자 암호를 제공해야 할 수 있습니다.

바이러스 및 스파이웨어 차단을 실행 및 실행 중지하려면 다음과 같이 하십시오.

1. 바이러스 및 스파이웨어 차단을 실행하려면 Symantec Endpoint Protection 클라이언트의 고급 페이지에서 내 **Mac** 보호**(Protect My Mac)**를 누른 다음 자동 검사**(Automatic Scans)**를 실행하십시오.
2. 바이러스 및 스파이웨어 차단을 실행 중지하려면 Symantec Endpoint Protection 클라이언트의 고급 페이지에서 내 **Mac** 보호**(Protect My Mac)**를 누른 다음 자동 검사**(Automatic Scans)**를 실행 중지하십시오.

자동 보호 설정 및 검사 영역 설정 구성

바이러스 및 스파이웨어 차단 설정 관리

감염 및 위험 요소 탐지 관련 메시지에 응답

자동 보호 설정 및 검사 영역 설정 구성

중앙 관리 클라이언트에서는 관리자가 허용하는 경우, 자동 보호가 바이러스를 모니터링하고 감염된 파일을 복구하는 방법을 사용자 정의할 수 있습니다.

자동 보호 설정은 내 **Mac** 보호**(Protect My Mac)** 아래에 옵션으로 나타납니다. 자동 보호를 실행하려면 자동 검사**(Automatic Scans)**를 실행해야 합니다.

검사 영역 설정**(Scan Zone Settings)**에서는 검사에 포함하거나 검사에서 제외할 파일을 지정할 수 있습니다.

자동 보호 설정을 구성하려면 다음과 같이 하십시오.

1. Symantec Endpoint Protection 클라이언트의 고급 페이지에서 내 **Mac** 보호**(Protect My Mac)**를 누른 다음 자동 검사**(Automatic Scans)**의 설정 아이콘을 누르십시오.
2. 다음과 같은 옵션을 변경하십시오.

자동 검역소	복구할 수 없는 파일을 검역소로 보낼지 여부를 선택할 수 있습니다.
자동 복구	감염된 파일이 발견될 때 자동 보호가 파일을 자동으로 복구하도록 선택할 수 있습니다.
검사	데이터 디스크 및 기타 모든 디스크를 선택할 수 있습니다.
압축 파일 검사	자동 보호 검사에 압축 파일을 포함할지 여부를 선택할 수 있습니다. 압축된 파일과 압축된 파일 안의 파일이 검사에 포함됩니다.

WARNING
자동 복구를 선택하지 않을 경우, 자동 검역소를 선택하더라도 감염된 파일이 검역소로 이동되지 않습니다. 감염된 파일을 복구할지 묻는 메시지가 표시됩니다. 파일을 복구하지 않으면 파일이 시스템에 남게 됩니다. 자동 복구를 선택하고 자동 검역소를 선택하지 않을 경우 감염된 파일이 삭제됩니다.

3. 완료를 누르십시오.

검사 영역 설정을 구성하려면 다음과 같이 하십시오.

1. Symantec Endpoint Protection 클라이언트의 고급 페이지에서 내 **Mac** 보호**(Protect My Mac)**를 누른 다음 검사 영역 설정**(Scan Zone Settings)**의 설정 아이콘을 누르십시오.
2. 다음과 같은 옵션을 변경하십시오.

모두 검사	시스템에서 액세스하는 모든 파일과 프로세스를 검사합니다.
다음만 검사	지정한 파일 또는 폴더만 검사에 포함됩니다.
검사 안 함	검사에서 제외되도록 지정한 파일이나 폴더를 제외하고 모든 파일을 검사합니다.
기본값 사용	이 옵션을 선택하면 모두 검사됩니다.

3. 확인을 누르십시오.

바이러스 및 스파이웨어 차단 기능으로 Mac을 보호하는 방법

바이러스 및 스파이웨어 차단 실행 및 실행 중지

검역소에 보관된 파일 관리

예약 검사 설정

중앙 관리 클라이언트를 사용하고 있다면 Symantec Endpoint Protection에서 기본 검사가 자동으로 실행됩니다. 관리자가 허용하는 경우, 예약 검사를 추가로 설정할 수 있습니다.

NOTE
단독 실행 클라이언트에서는 사용자 정의 검사를 실행해야 합니다. 가능한 한 빨리 전체 수동 검사를 수행한 다음 정기 예약 검사를 설정하는 것이 좋습니다. 검사(예약 검사와 수동 검사 둘 다 포함)를 일시 중지하거나 지연시킬 수 있습니다.

중앙 관리 클라이언트에서는 매일 오후 8시에 자동 복구가 실행된 상태로 기본 검사가 실행됩니다.

수동 검사 실행

예약 검사를 설정하려면 다음과 같이 하십시오.

1. Symantec Endpoint Protection 클라이언트의 고급 페이지에서 내 **Mac** 보호**(Protect My Mac)**를 누른 다음 예약 검사의 설정 아이콘을 누르십시오.
2. 대화 상자에서 예약 검사 추가를 누르거나, 현재 예약 검사를 누른 다음 편집을 눌러 설정을 조정하십시오.
3. 검사 항목 탭에서는 다음과 같은 옵션을 설정할 수 있습니다.

드라이브	하드 드라이브 및 이동식 드라이브에 대한 검사 여부를 선택할 수 있습니다.
폴더	홈 폴더(활성 사용자), 응용 프로그램 및 라이브러리 파일을 검사하도록 선택할 수 있습니다. 홈 폴더의 예약 검사 시간에 사용자가 로그온되어 있지 않으면 검사가 실행되지 않습니다.
검사 옵션	다음 옵션 중에서 선택할 수 있습니다. • 압축 파일 검사 • 자동 복구 • 자동 검역소 • 유휴 시간 검사 실행

4. 검사 예약 탭에서 다음과 같은 옵션을 설정할 수 있습니다.

검사 예약	시간 단위, 매일, 매주 또는 매월의 특정 간격으로 검사가 실행되도록 설정할 수 있습니다. 새 검사를 예약할 때 기본적으로 특정 간격으로 실행이 선택됩니다.
실행 간격	이 옵션은 특정 간격으로 실행을 검사 예약에 대해 선택한 경우에 사용할 수 있습니다.
시작 시간	이 옵션은 매일, 매주 또는 매월을 검사 예약에 대해 선택한 경우에 사용할 수 있습니다. 검사를 실행할 시간을 선택할 수 있습니다. 검사를 실행하면 시스템의 성능이 저하될 수 있으므로 보통 근무 시간 외 시간을 선택해야 합니다.
실행	이 옵션은 매주 또는 매월을 검사 예약에 대해 선택한 경우에 사용할 수 있습니다. 검사를 실행할 요일 또는 날짜를 선택할 수 있습니다. 검사를 실행하면 시스템의 성능이 저하될 수 있으므로 보통 근무 시간 외 시간을 선택하는 것이 좋습니다.

5. 조정 탭에서는 검사 성능이 최적화되는 방식을 조정할 수 있습니다.
6. 확인을 누르십시오.
7. 완료를 누르십시오.

검사를 일시 중지, 유휴 상태로 설정 및 중지

Symantec Endpoint Protection에서의 Mac 보호 기능 관리

감염 및 위험 요소 탐지 관련 메시지에 응답

시만텍에 보안 정보 제출 실행 또는 실행 중지

수동 검사 실행

일부 파일은 수동으로 검사해야 할 수도 있습니다. 예를 들어 Symantec Endpoint Protection 설치 이전에 시스템에 저장된 파일을 검사해야 되는 경우입니다. 또는 예약 검사에서 제외시킨 일부 파일에 대해서도 수동으로 검사해야 합니다.

NOTE
검사(예약 검사와 수동 검사 둘 다 포함)를 일시 중지하거나 지연시킬 수 있습니다.

수동 검사를 실행하려면 다음과 같이 하십시오.

Symantec Endpoint Protection 클라이언트의 검사 페이지에서 다음 중 하나를 수행하십시오.

- 빠른 검사를 시작하려면 빠른 검사**(Quick Scan)**를 누른 다음 빠른 검사 시작**(Start a Quick Scan)**을 누르십시오.
- 전체 검사를 시작하려면 전체 검사를 누른 다음 전체 검사 시작**(Start a Full Scan)**을 누르십시오.
- 파일 또는 폴더를 검사하려면 파일 검사**(File Scan)**를 누른 다음 파일 선택**(Select a file)**을 누르십시오. 찾기 창이 열리며 숨겨진 파일 표시 및 압축된 파일 검사를 선택할 수 있습니다. 또한 자동 복구 및 자동 검역소를 실행하도록 선택할 수도 있습니다.

검사를 일시 중지, 유휴 상태로 설정 및 중지

예약 검사 설정

시만텍에 보안 정보 제출 실행 또는 실행 중지

검사를 일시 중지, 유휴 상태로 설정 및 중지

일시 중지 기능을 사용하면 검사를 중지했다가 선택한 다른 시간에 다시 시작할 수 있습니다. 또한 어느 검사든지 아무 때나 중지 및 취소할 수 있습니다. 이러한 기능을 사용하는 데 관리자 권한은 필요하지 않습니다.

검사를 다시 시작하면 검사가 중지된 지점부터 시작됩니다.

NOTE
클라이언트가 압축 파일을 검사하는 도중 검사를 일시 중지한 경우 클라이언트에서 해당 일시 중지 요청에 응답하는 데 몇 분이 소요될 수 있습니다.

유휴를 실행하는 경우 검사를 유휴 상태로 설정할 수 있지만 이는 검사가 시작되기 전에만 가능합니다. 진행 중인 검사를 유휴 상태로 설정할 수는 없습니다.

실행 중인 예약 검사를 일시 중지하거나 중지하려면 다음과 같이 하십시오.

1. 검사 진행률 대화 상자에서 일시 중지를 누르십시오.
2. 검사 진행률 대화 상자에서 계속을 눌러 검사를 계속하거나 중지를 눌러 검사를 중지하십시오. 완료를 눌러 창을 닫을 수도 있습니다.

실행 중인 수동 검사를 일시 중지하거나 중지하려면 다음과 같이 하십시오.

1. 검사 진행률 대화 상자에서 일시 중지를 눌러 검사를 일시 중지하십시오.
2. 실행 중인 수동 검사를 중지하려면 취소를 누르고 검사를 계속하려면 계속을 누르십시오.

시작되기 전의 검사를 유휴 상태로 설정하려면 다음과 같이 하십시오.

1. 창이 나타나면 드롭다운 메뉴를 눌러 유휴 상태로 설정할 값을 선택하십시오. 15분처럼 짧은 시간이나 하루처럼 긴 시간 동안 유휴 상태로 설정할 수 있습니다.
2. 확인을 눌러 검사를 유휴 상태로 설정하십시오.

   검사를 예약된 대로 실행하려는 경우에는 다른 작업을 수행할 필요가 없습니다.

예약 검사 설정

수동 검사 실행

감염 및 위험 요소 탐지 관련 메시지에 응답

사용자는 시스템의 감염 여부를 확인할 수 있으며, 보안을 강화하거나 성능을 향상시키려는 경우 몇 가지 추가 태스크를 수행할 수 있습니다.

관리자는 클라이언트를 관리하거나, 단독 실행 클라이언트를 실행할 수 있습니다. 수행 가능한 보호 태스크는 클라이언트에 대한 관리자의 제어 수준에 따라 다릅니다.

Symantec Endpoint Protection에서 바이러스나 보안 위험 요소를 발견한 경우 해당 위험 요소에 대해 작업을 수행할지 확인하는 메시지가 표시됩니다. 관리자가 선택한 설정에 따라 클라이언트에서 자동으로 수행된 작업에 대해 통지될 수도 있습니다.

Table 7: 감염 관련 메시지에 응답

메시지 컨텐츠	필요한 작업
감염된 파일이 복구됨	없음
감염된 파일 복구에 대한 승인을 요청함	복구를 승인합니다. 이 옵션은 자동 보호 기본 설정에 따라 결정됩니다. 바이러스 및 스파이웨어 차단 설정 관리 감염된 파일을 자동으로 복구하는 옵션이 선택 해제된 경우 수동으로 복구해야 합니다. 감염된 파일 복구
감염된 파일을 복구할 수 없음	검역소의 감염된 파일을 관리합니다. 검역소에 보관된 파일 관리

바이러스 및 스파이웨어 차단 기능으로 Mac을 보호하는 방법

감염된 파일 복구

감염된 파일이 자동으로 복구되지 않거나 검역소에 보관되지 않은 경우 검사 결과 목록의 파일을 복구할 수 있습니다. 시스템의 하드 디스크나 이동식 미디어의 파일을 수동으로 복구할 수 있습니다.

감염된 파일을 복구하려면 다음과 같이 하십시오.

1. 검사 결과 목록에서 복구할 파일을 선택한 다음 복구를 누르십시오.

   Mac 찾기 또는 검색 메뉴에서 파일을 마우스 오른쪽 버튼으로 누를 수도 있습니다.
2. 필요에 따라 반복하십시오.
3. 감염된 다른 파일을 검사하려면 다른 검사를 실행해야 합니다.
4. 복구된 파일을 점검하여 제대로 작동하는지 확인하십시오.

바이러스 및 스파이웨어 차단 설정 관리

검역소에 보관된 파일 관리

검역소에 보관된 파일 관리

기본적으로 클라이언트는 파일에서 바이러스를 탐지하면 이를 제거하려고 시도합니다. 바이러스를 제거할 수 없으면 해당 파일이 시스템의 검역소에 보관됩니다. Symantec Endpoint Protection에서 파일의 보안 위험 요소를 탐지하면 해당 파일을 먼저 검역소에 보관합니다. 그런 다음 위험 요소의 부작용을 복구합니다.

바이러스 정의를 업데이트할 때 클라이언트는 자동으로 검역소를 확인합니다. 검역소에서 해당 항목을 재검사할 수 있습니다. 최신 정의 업데이트에 의해 검역소에 보관된 파일이 제거되거나 복구될 수 있습니다.

검역소에 보관된 파일을 관리하려면 다음과 같이 하십시오.

1. Symantec Endpoint Protection 클라이언트의 고급 페이지에서 작업 **>** 보안 기록 **>** 검역소를 누르십시오.
2. 관리할 파일을 선택한 다음 적절한 옵션을 선택하십시오.

복구	이 옵션을 선택하면 검역소에 보관된 파일에 대한 복구가 시도됩니다. 바이러스 정의는 파일이 검역소에 보관된 날짜 이후의 버전이어야 합니다.
삭제	이 옵션을 선택하면 검역소에서 더 이상 필요하지 않은 파일이 삭제됩니다.
복원	검역소에 보관된 파일에 바이러스가 없는 것이 확실할 경우 해당 파일을 시스템의 원래 위치로 복원할 수 있습니다. 이 옵션은 해당 파일을 검사하거나 복구를 시도하지 않습니다.

감염 및 위험 요소 탐지 관련 메시지에 응답

시만텍에 보안 정보 제출 실행 또는 실행 중지

Symantec Endpoint Protection에서는 탐지된 위협 요소에 대한 익명화된 정보를 시만텍에 제출할 수 있습니다. 시만텍은 이러한 정보를 사용하여 변형된 새 대상 위협 요소로부터 클라이언트 시스템을 보호합니다. 사용자가 제출하는 모든 데이터는 위협 요소에 대응하고 시스템 보호를 사용자 정의하기 위한 시만텍의 역량을 강화해 줍니다.

시만텍 원격 측정에서 수집하는 데이터에는 직접적으로 식별할 수 없는 익명 요소가 포함될 수 있습니다. 시만텍은 개별 사용자를 식별하기 위해 원격 측정 데이터를 사용할 필요성도 의도도 없습니다.

기본적으로 클라이언트 시스템은 탐지 관련 정보를 시만텍에 전송합니다. 이 설정을 실행 상태로 두는 것이 좋긴 하지만 제출을 실행 중지할 수도 있습니다.

이 옵션은 바이러스 탐지 관련 정보만 보냅니다.

NOTE
이 옵션을 실행 상태로 두는 것이 좋습니다.

시만텍에 익명 보안 정보 제출을 실행하거나 실행 중지하려면 다음과 같이 하십시오.

Symantec Endpoint Protection 클라이언트의 고급 페이지에서 제품 설정**(Product Settings)**을 누른 다음 보안 정보 제출**(Security Info Submission)**을 실행하거나 실행 중지하십시오.

예약 검사 설정

수동 검사 실행

침입 차단 관리

기본적인 침입 차단 설정을 통해 Mac 클라이언트를 보호할 수 있습니다. 하지만 자신의 보호 기능을 관리하려는 경우에는 침입 차단을 네트워크 위협 요소 차단의 일부로 관리할 수 있습니다.

Table 8: 침입 차단 관리

단계	설명
1단계: 침입 차단에 대해 알아보기	침입 차단에서 네트워크 공격을 탐지하고 차단하는 방법에 대해 알아봅니다. 네트워크 위협 요소 차단 기능으로 Mac을 보호하는 방법
2단계: 최신 IPS 시그니처 다운로드	기본적으로 최신 시그니처는 클라이언트에 자동으로 다운로드됩니다. 하지만 사용자가 시그니처를 즉시 다운로드할 수도 있습니다. Symantec Endpoint Protection에서 컨텐츠를 즉시 업데이트
3단계: 침입 차단 실행 또는 실행 중지	문제 해결을 위해 또는 클라이언트 시스템의 오탐지 수가 지나치게 많은 경우 침입 차단을 실행 중지해야 될 수 있습니다. 일반적으로 침입 차단은 실행 중지하지 않는 것이 좋습니다. 네트워크 위협 요소 차단 실행 또는 실행 중지
4단계: 침입 차단 통지 실행	Symantec Endpoint Protection에서 공격을 탐지한 경우 나타날 통지를 구성할 수 있습니다. 네트워크 위협 요소 차단 통지 실행 및 실행 중지

Mac 클라이언트의 방화벽 보호 관리

Mac용 Symantec Endpoint Protection 방화벽은 이벤트, 정책 및 명령이 포함되는 Symantec Endpoint Protection에 완벽히 통합되는 방화벽 보호 기능을 제공합니다. Symantec Endpoint Protection 방화벽은 관리되는 클라이언트에서만 사용할 수 있습니다.

NOTE
Mac용 Symantec Endpoint Protection 방화벽은 운영 체제의 내장 방화벽과 통합되지 않습니다. 대신 동시에 실행됩니다. 운영 체제 방화벽은 응용 프로그램 계층에서 검사하지만 Symantec Endpoint Protection 방화벽은 더 낮은 계층(IP 및 전송)에서 검사합니다. Mac용 Symantec Endpoint Protection 방화벽은 Peer-to-Peer 차단 규칙을 제공하지 않지만 사용자 정의 방화벽 규칙을 사용하여 일부를 생성할 수 있습니다.

Table 9: 방화벽 보호 관리

단계	설명
1단계: 방화벽 보호에 대해 알아보기	방화벽 보호 기능이 트래픽을 모니터링하고 일반적인 공격 벡터를 차단하는 방법을 알아보십시오. 네트워크 위협 요소 차단 기능으로 Mac을 보호하는 방법
2단계: 방화벽 실행 또는 실행 중지	허용되어야 하는 트래픽이 차단되는 경우와 같이 문제 해결이 필요한 경우 방화벽을 실행 중지해야 할 수 있습니다. 일반적으로 방화벽은 실행 중지하면 안 됩니다. 네트워크 위협 요소 차단 실행 또는 실행 중지

네트워크 위협 요소 차단 실행 또는 실행 중지

일반적으로 시스템에서 네트워크 위협 요소 차단 구성 요소를 실행 중지하면 시스템의 보안 수준이 떨어집니다. 하지만 오탐지를 방지하기 위해 침입 차단을 실행 중지하거나, 차단된 트래픽 문제를 해결하기 위해 방화벽을 실행 중지해야 할 수도 있습니다. 침입 차단 및 방화벽은 네트워크 위협 요소 차단의 일부입니다.

중앙 관리 클라이언트의 경우 이러한 설정을 어느 정도 제어할 수 있는지는 관리자가 클라이언트를 구성한 방식에 따라 달라집니다. 또한 이러한 설정에 수행한 모든 변경 사항은 다음 하트비트에서 정책에 기술된 설정으로 되돌아갑니다.

단독 실행 클라이언트의 경우 방화벽을 사용할 수 없습니다.

네트워크 위협 요소 차단을 실행하거나 실행 중지하려면 다음과 같이 하십시오.

1. Symantec Endpoint Protection 클라이언트의 고급 페이지에서 네트워크 위협 요소 차단을 누르십시오.
2. 침입 차단을 실행 또는 실행 중지하려면 침입 차단을 실행하거나 실행 중지하십시오.
3. 방화벽을 실행 또는 실행 중지하려면 방화벽을 실행하거나 실행 중지하십시오.
4. 침입 차단 및 방화벽에 대한 통지를 실행 또는 실행 중지하려면 취약점 보호**(Vulnerability Protection)**의 설정 아이콘을 누른 다음 대화 상자에서 취약점 보호 통지 표시**(Display Vulnerability Protection Notifications)**를 선택하거나 선택 해제하십시오.
5. 완료를 누르십시오.

이러한 구성 요소를 실행 중지한 경우에는 최상의 시스템 보호를 위해 가능한 한 빨리 이 기능을 다시 실행하는 것이 좋습니다.

침입 차단 관리

Mac 클라이언트의 방화벽 보호 관리


Symantec
A Division of Broadcom