SOPHOS

Cybersecurity made simple.

Sophos Endpoint for Windows

도움말

목차

Sophos Endpoint for Windows 정보 1
Sophos Endpoint 2
상태 3
이벤트 5
설정 7
방법 9
    파일 스캔 9
    컴퓨터 또는 서버 스캔 9
    위협을 정리합니다 9
    보안 설정을 변경합니다 9
    지금 업데이트 10
    문제 해결 10
    컴퓨터 암호화 10
    암호를 잊어버린 경우의 컴퓨터 액세스 11
내 파일 전송이 차단된 이유는 무엇입니까? 13
지원 14
법적 고지 사항 15

1 Sophos Endpoint for Windows 정보

이 도움말 파일은 Sophos Endpoint for Windows에 대한 정보를 제공하고 절차를 단계별로 설명합니다.

2 Sophos Endpoint

Sophos Endpoint는 컴퓨터와 서버에서 실행되면서 시스템을 보호합니다.

제한
여기에 설명된 일부 기능이 제공되지 않을 수 있습니다. 이는 현재 보유 중인 라이선스에 따라 달라집니다.

Sophos Endpoint는 Sophos Central Admin에서 중앙식으로 구성 및 관리됩니다.

그러나, 컴퓨터 또는 서버에서 사용자가 몇 가지 작업을 수행할 수 있습니다.

- 컴퓨터의 상태를 확인합니다.
- 파일, 컴퓨터 또는 서버에 대해 위협을 스캔합니다.
- 검색된 위협과 같은 컴퓨터 또는 서버의 이벤트 세부 정보를 확인합니다.
- 위협을 정리합니다.
- 보안 설정을 변경합니다. 예를 들어, 문제 해결을 위해 기능을 끌 수 있습니다.
- 업데이트.
- 문제 해결.

참고
위협을 정리하거나 설정을 변경하려면 관리자 로그인을 사용하여 변조 방지 암호를 입력해야 합니다.

관련 개념

상태 (페이지 3)
보안 상태를 확인하고 컴퓨터 또는 서버를 스캔할 수 있습니다.

이벤트 (페이지 5)
이벤트 페이지는 검색된 위협과 같은 컴퓨터 또는 서버의 이벤트를 표시합니다.

관련 작업

파일 스캔 (페이지 9)
개별 파일을 스캔할 수 있습니다.

컴퓨터 또는 서버 스캔 (페이지 9)
컴퓨터 또는 서버를 스캔하려면 다음 지침을 따르십시오.

위협을 정리합니다 (페이지 9)
검색된 위협을 정리하려면 다음 지침을 따르십시오.

보안 설정을 변경합니다 (페이지 9)
보안 설정을 변경하려면 다음 지침을 따르십시오.

지금 업데이트 (페이지 10)
바이러스 정의를 업데이트하려면 다음 지침을 따르십시오.

문제 해결 (페이지 10)
문제를 해결하려면 다음 지침을 따르십시오.

3 상태

보안 상태를 확인하고 컴퓨터 또는 서버를 스캔할 수 있습니다.

제한
여기에 설명된 일부 기능이 제공되지 않을 수 있습니다. 이는 현재 보유 중인 라이선스에 따라 달라집니다.

상태 페이지에서 다음을 수행할 수 있습니다.

- 컴퓨터 또는 서버의 보안 상태를 확인합니다.
- 컴퓨터 또는 서버에서 위협을 스캔합니다.
- 설치된 기능 및 기능의 보안 상태를 확인합니다.

참고
페이지 오른쪽 하단에 있는 정보 링크를 사용하여 바이러스 정의를 업데이트하거나 제품의 문제를 해결할 수 있습니다.

보안 상태

상태를 표시하는 페이지의 상단 부분에 있는 아이콘입니다.

설정	설명
 녹색.	경고가 없거나 낮은 우선순위 경고입니다.
 빨간색.	높은 우선순위 경고입니다.
 노란색.	중간 우선순위 경고입니다.
 회색.	상태를 알 수 없습니다.

이 아래에, 설치된 모든 기능이 개별 보안 상태와 함께 표시됩니다.

컴퓨터 스캔

스캔을 클릭하여 컴퓨터 또는 서버의 모든 파일에서 위협을 스캔합니다.

스캔이 완료되면 스캔 결과 요약이 표시됩니다. 위협이 검색되면 이벤트 페이지로 이동하여 자세한 내용을 확인할 수 있습니다.

4 이벤트

이벤트 페이지는 검색된 위협과 같은 컴퓨터 또는 서버의 이벤트를 표시합니다.

제한
여기에 설명된 일부 기능이 제공되지 않을 수 있습니다. 이는 현재 보유 중인 라이선스에 따라 달라집니다.

예를 들어, 조치를 수행해야 하는 이벤트만 표시하거나 특정 이벤트 유형만 검색하기 위해 이벤트를 필터링할 수 있습니다.

이벤트 목록

목록에는 다음이 표시됩니다.

- 심각도. 목록 맨 왼쪽의 아이콘은 이벤트가 높은 우선 우선순위, 중간 우선순위 또는 알림인지 표시합니다.
- 소스. 목록 왼쪽의 아이콘은 이벤트를 보고한 Sophos 기능을 나타냅니다.
- 이벤트가 발생한 날짜 및 시간.
- 이벤트의 설명.
- 조치를 취할 수 있는 링크(작업이 필요한 경우). 이는 관리자로 로그인한 경우에만 표시됩니다.

각 이벤트의 세부 정보를 보려면 오른쪽에 있는 화살표를 클릭하여 확장합니다.

수행할 수 있는 작업은 Sophos Central Admin에서 제공되는 것과 동일합니다. Sophos Central Admin 도움말의 경고 페이지에 있는 목록을 참조하십시오.

다음 유형을 기준으로 이벤트를 필터링할 수 있습니다.

이벤트 유형	설명
악성코드 및 PUA	악성코드는 악성 소프트웨어를 통칭하는 용어입니다. 여기에는 바이러스, 웜, 트로이 목마, 스파이웨어가 포함됩니다. PUA(잠재적으로 원치 않은 응용 프로그램)는 전화 걸기, 원격 관리 도구, 해킹 도구처럼 악의적이지는 않지만 일반적으로 대부분의 비즈니스 네트워크에 적합하지 않은 것으로 간주되는 프로그램입니다.
웹 위협	웹 위협에는 악성 웹 사이트, 분류되지 않은 웹 사이트, 위험한 다운로드가 포함됩니다. 예를 들어, 성인 웹 사이트 또는 소셜 미디어 같은 일부 웹 사이트는 일반적으로 비즈니스 네트워크에 적합하지 않은 것으로 간주됩니다. 이러한 사이트를 차단할 수 있습니다.

이벤트 유형	설명
악성 행위	악의적인 동작은 컴퓨터 또는 서버에서 이미 실행 중인 소프트웨어에서 검색된 의심스러운 동작입니다. 랜섬웨어는 랜섬을 지불하기 전까지는 파일에 대한 액세스를 거부하는 악성 소프트웨어입니다.
제어된 항목	이 범주에는 다음이 포함됩니다. • 보안 위협은 아니지만 사무실에서 사용하기에 적합하지 않은 것으로 판단되는 응용 프로그램. • 주변기기 및 이동식 미디어. • 사무실에서 사용하기에 적합하지 않은 위험한 다운로드 또는 웹 사이트. • 누출을 원하지 않는 민감한 정보(예를 들어, 개인 또는 금융 세부 정보)를 포함하는 파일.
악성 트래픽	악성 트래픽은 컴퓨터 또는 서버를 제어하기 위한 가능한 시도를 나타내는 컴퓨터 간 트래픽입니다("명령 및 제어" 공격).
보안 취약점	Sophos가 방지할 수 있는 익스플로잇에는 응용 프로그램 하이재킹과 브라우저, 브라우저 플러그인, Java 응용 프로그램, 미디어 응용 프로그램, Microsoft Office 응용 프로그램의 취약점을 악용할 수 있는 익스플로잇이 포함됩니다.

5 설정

이 컴퓨터 또는 서버의 보안 설정을 일시적으로 변경할 수 있습니다.

문제 해결을 위해 이를 수행해야 할 수 있습니다. 예를 들어, 컴퓨터에 문제를 유발하는 기능이 있을 경우 해당 기능을 끌 수 있습니다.

제한
여기에 설명된 일부 기능이 제공되지 않을 수 있습니다. 이는 현재 보유 중인 라이선스에 따라 달라집니다.

제한
설정 페이지는 변조 방지 암호를 입력한 경우에만 제공됩니다(Sophos Central 관리자에서 제공).

설정을 변경하는 방법

Sophos Central Policy를 최대 4시간 동안 재정의하여 문제를 해결합니다 확인란을 선택합니다.

이제 이 페이지에서 변경 사항을 적용할 수 있습니다. 변경 사항은 귀하(또는 다른 관리자)가 Sophos Central Admin에서 적용한 정책을 임시로 재정의합니다.

4시간 후에, 설정은 중앙 집중식 적용 정책 설정으로 다시 자동 변경됩니다.

원하는 경우 설정을 더 빨리 변경할 수 있습니다. 개별 기능의 경우 슬라이드 제어를 사용하여 이 작업을 수행할 수 없습니다. 대신, Sophos Central Policy를 최대 4시간 동안 재정의하여 문제를 해결합니다의 설정을 끕니다.

Deep Learning (딥 러닝)

Deep Learning은 고급 머신 러닝을 사용하여 위협을 탐지합니다. 딥 러닝은 서명을 사용하지 않고 맬웨어 및 사용자 동의 없이 설치된 응용 프로그램을 식별합니다.

실시간 스캔

실시간 스캔은 사용자가 항목에 액세스하려고 할 때 해당 항목을 스캔하며 항목이 깨끗하지 않은 경우 액세스를 거부합니다. 다음을 선택할 수 있습니다.

- 파일: 이 기능은 로컬 파일, 그리고 네트워크 공유(정책에서 이를 선택한 경우)를 스캔합니다.
- 인터넷: 이 기능은 인터넷 원본을 스캔합니다. 이 기능은 진행 중인 다운로드를 스캔하고, 악성 웹 사이트에 대한 액세스를 차단하고, 평판이 낮은 웹 사이트를 검색할 수 있습니다.

사용자 제어

- 주변기기 제어를 사용하여 주변기기 및 이동식 미디어에 대한 액세스를 제어할 수 있습니다.
- 응용 프로그램 제어를 사용하여 보안 위협은 아니지만 사무실에서 사용하기에 적합하지 않은 것으로 판단되는 응용 프로그램을 검색 및 차단할 수 있습니다.

- 웹 제어를 사용하여 위험한 다운로드를 차단하고, 사용자가 방문 가능한 사이트를 제어하고, 데이터 손실을 방지할 수 있습니다.
- 데이터 손실 방지를 사용하여 민감한 데이터를 포함하는 파일의 전송을 모니터링 및 제한할 수 있습니다.
- 변조 방지를 통해 변경 사항을 제한할 수 있습니다. 이 기능이 켜져 있으면, 로컬 관리자는 보안 설정을 변경하거나 Sophos Endpoint를 제거하는 데 암호가 필요합니다.

런타임 보호

런타임 보호는 엔드포인트 컴퓨터의 의심스럽거나 악의적인 행위 또는 트래픽을 검색하여 위협으로부터 보호합니다. 다음을 선택할 수 있습니다.

- 랜섬웨어 검색: 이 기능은 파일에 대한 액세스를 제한한 다음 이를 해제하는 대가로 금전을 요구하는 악성코드를 차단합니다.
- 세이프 브라우징: 이 기능은 악성코드에 의한 취약점 공격으로부터 웹 브라우저를 보호합니다.
- 보안 취약점 공격 완화: 이 기능은 악성코드에 의한 취약점 공격을 받기 가장 쉬운 응용 프로그램(예: Java 응용 프로그램)을 보호합니다.
- 네트워크 위협 보호: 이 기능은 엔드포인트 컴퓨터를 장악할 가능성이 있는 것으로 나타나는 엔드포인트 컴퓨터와 서버 간의 트래픽을 검색합니다. 여기에는 네트워크 통신을 스캔하여 운영 체제 또는 응용 프로그램에 피해를 주기 전에 위협을 파악하고 차단하는 패킷 검사가 포함됩니다.

  참고
  네트워크 위협 보호를 끄면 EDR 기능, 격리 및 Stonewalling(격벽)도 꺼집니다.

- 악성 행위 검색: 악의적이거나 의심스러운 것으로 알려진 동작을 검색하고 차단합니다.

컴퓨터 제어

컴퓨터와 서버에서 Windows 방화벽(및 기타 등록된 방화벽)을 모니터링할 수 있습니다.

6 방법 ...

6.1 파일 스캔

개별 파일을 스캔할 수 있습니다.

파일을 스캔하려면 다음과 같이 하십시오.

- 탐색기에서 마우스 오른쪽 버튼으로 파일을 클릭하고 스캔을 선택합니다.

6.2 컴퓨터 또는 서버 스캔

컴퓨터 또는 서버를 스캔하려면 다음 지침을 따르십시오.

컴퓨터 또는 서버의 모든 파일을 스캔하려면:

1. 상태 페이지 또는 검색 페이지로 이동합니다.
2. 스캔을 클릭합니다.
   스캔이 완료되면 스캔 결과 요약이 표시됩니다.
3. 위협이 검색되면 이벤트 페이지로 이동하여 자세한 내용을 확인할 수 있습니다.

6.3 위협을 정리합니다

검색된 위협을 정리하려면 다음 지침을 따르십시오.

위협을 정리하려면 다음과 같이 하십시오.

1. 관리자 로그인을 클릭하고 변조 방지 암호(Sophos Central 관리자자 제공)를 입력합니다.
2. 이벤트 페이지로 이동하여 검색된 위협의 세부 정보를 봅니다.
3. 위협 세부 정보 옆의 작업 링크를 참조합니다.

수행할 수 있는 작업은 Sophos Central Admin에서 제공되는 것과 동일합니다. Sophos Central Admin 도움말의 경고 페이지에 있는 목록을 참조하십시오.

6.4 보안 설정을 변경합니다

보안 설정을 변경하려면 다음 지침을 따르십시오.

보안 설정을 변경하려면:

1. 인터페이스 오른쪽 상단의 관리자 로그인을 클릭합니다.
2. 변조 방지 암호(Sophos Central 관리자자 제공)를 입력합니다.
   이제 메뉴 모음에 설정 링크가 표시됩니다.
3. 설정 페이지로 이동합니다.
4. Sophos Central Policy를 최대 4시간 동안 재정의하여 문제를 해결합니다 확인란을 선택합니다.
5. 페이지의 슬라이드 제어를 사용하여 보안 기능을 끕니다.

4시간이 지나면 설정은 중앙 집중식 적용 정책 설정으로 다시 자동으로 변경됩니다.

참고
원하는 경우 설정을 더 빨리 변경할 수 있습니다. 개별 기능의 경우 슬라이드 제어를 사용하여 이 작업을 수행할 수 없습니다. 대신, Sophos Central Policy를 최대 4시간 동안 재정의하여 문제를 해결합니다를 선택 취소합니다.

6.5 지금 업데이트

바이러스 정의를 업데이트하려면 다음 지침을 따르십시오.

업데이트하려면 다음과 같이 하십시오.

1. 정보를 클릭합니다.
2. 지금 업데이트를 클릭합니다.

6.6 문제 해결

문제를 해결하려면 다음 지침을 따르십시오.

문제를 해결하려면 다음과 같이 하십시오.

1. 정보를 클릭합니다.
2. Endpoint Self Help Tool 열기을 클릭하여 문제에 대한 데이터를 수집하거나 링크를 따라 커뮤니티 포럼으로 이동합니다.

6.7 컴퓨터 암호화

컴퓨터를 암호화하려면 다음 지침을 따르십시오.

제한
Device Encryption은 엔드포인트 컴퓨터에서만 사용할 수 있습니다.

Device Encryption은 Windows BitLocker 기술을 사용하여 컴퓨터의 하드웨어 디스크를 암호화합니다. 귀하의 관리자가 귀하가 컴퓨터에 액세스할 때마다 인증을 해야 하는지 여부를 정의합니다.

인증이 필요하지 않다면 귀하가 Sophos Central 정책을 수신하고 나서 컴퓨터를 다시 시작하자마자 하드 디스크의 암호화가 자동으로 시작됩니다. 여기서 귀하가 수행해야 할 작업은 없습니다.

인증해야 할 경우 다음과 같이 하십시오.

1. Sophos Device Encryption 대화 상자가 표시되면 이 대화 상자의 지시 사항을 따르십시오. 구체적인 지시 사항은 시스템과 관리자가 정의한 정책 설정에 따라 달라집니다.
    - Device Encryption 정책에 따라 인증을 위해 PIN 또는 암호가 필요한 경우, 화면의 지시 사항에 따라 PIN 또는 암호를 만듭니다.

        참고
        PIN 또는 암호를 만들 때 주의하십시오. 사전 부팅 환경에서만 미국-영어 키보드 레이아웃을 지원합니다. 지금 특수 문자와 함께 PIN 또는 암호를 만들 경우, 나중에 로그인하기 위해 입력할 때 다른 키를 사용해야 할 수 있습니다.

- Device Encryption 정책에 따라 인증을 위해 USB 키가 필요한 경우, USB 플래시 드라이브를 컴퓨터에 연결해야 합니다. USB 플래시 드라이브는 NTFS, FAT 또는 FAT32로 포맷해야 합니다.

2. 다시 시작하고 암호화를 클릭하면 컴퓨터가 다시 시작되고 하드 디스크를 암호화합니다. 평상시대로 작업할 수 있습니다.

참고
나중에 하기를 선택하여 대화 상자를 닫을 수 있습니다. 그러나, 다음에 로그인할 때 대화 상자가 다시 나타납니다.

Sophos Central이 시스템 볼륨을 암호화하면 데이터 볼륨의 암호화가 시작됩니다. USB 드라이브와 같은 이동식 데이터 볼륨은 암호화되지 않습니다.

컴퓨터에 로그인할 때 PIN, 암호 또는 USB 키를 사용하여 시스템 볼륨을 잠금 해제해야 할 수 있습니다. 데이터 볼륨은 자동으로 잠금 해제되지 않습니다.

6.8 암호를 잊어버린 경우의 컴퓨터 액세스

다음 단계에 따라 컴퓨터에 액세스합니다.

PIN, 암호 또는 USB 키를 잊어버려서 컴퓨터에 로그인할 수 없는 경우 복구 키가 필요합니다.

Sophos Device Encryption을 사용하는 경우 복구 키는 Sophos Central에 저장되어 있습니다. 복구 키를 얻으려면 다음 중 하나를 수행하십시오.

- Sophos Self Service Portal에 로그인하고 도움말의 지침을 따릅니다.
- 관리자에게 귀하의 복구 키를 검색해 줄 것을 요청합니다. Self Service Portal을 사용할 수 없는 경우 이렇게 하십시오.

관련 작업
BitLocker 복구 사용 (페이지 11)
컴퓨터를 복구하려면 다음 지침을 따르십시오.

6.8.1 BitLocker 복구 사용

컴퓨터를 복구하려면 다음 지침을 따르십시오.

컴퓨터를 복구하려면 다음과 같이 하십시오.

1. 컴퓨터를 다시 시작하고 BitLocker 로그온 화면에서 Esc 키를 누릅니다.
2. BitLocker 복구 화면에서 복구 키 ID를 찾습니다.
   복구 키 ID가 잠깐 동안 표시됩니다. 다시 표시하려면 컴퓨터를 다시 시작해야 합니다.
3. 관리자에게 연락해 복구 키 ID를 알려 줍니다.
   관리자가 Sophos Central에서 사용자의 컴퓨터에 대한 복구 키를 찾아서 키를 알려주어야 합니다.
4. BitLocker 복구 화면에서 복구 키를 입력합니다.
   이제 컴퓨터를 시작할 수 있습니다.
5. 메시지가 나타나면 화면의 지시 사항에 따라 새 BitLocker PIN 또는 암호를 만드십시오.

   Windows 7을 실행하는 컴퓨터에서는 아무 지침도 표시되지 않습니다. 해당 PIN/암호를 수동으로 재설정해야 합니다.

컴퓨터에 다시 액세스할 수 있습니다.

참고
복구 키는 한 번만 사용할 수 있습니다. 컴퓨터를 나중에 다시 복구해야 하는 경우 새 복구 키를 받아야 합니다.

7 내 파일 전송이 차단된 이유는 무엇입니까?

파일 전송(예를 들어, 파일 복사, 이동 또는 이메일 전송)이 차단되었음을 나타내는 메시지가 표시될 수 있습니다.

이 메시지는 보유해서는 안 되는 민감한 정보를 사용자에게 무심코 전송하지 않도록 금지하는 정책을 회사에서 설정했기 때문에 표시됩니다.

다음과 같은 두 가지 유형의 메시지가 있습니다.

메시지	설명
전송이 차단됨	"파일 전송 차단됨" 메시지를 수신한 경우 파일을 전송할 수 없습니다. 관리자가 이 메시지에 몇 가지 자문을 추가했을 수 있습니다.
전송을 허용할 수 있음	"파일 전송 요청 차단됨" 메시지를 수신한 경우 파일 전송 여부를 확인할 수 있습니다. 관리자가 이 메시지에 몇 가지 자문을 추가했을 수 있습니다. 계속해도 안전하다는 확신이 있다면 허용을 클릭하십시오.

8 지원

다음 방법을 통해 Sophos 제품에 대한 기술 지원을 받을 수 있습니다.

- community.sophos.com/에서 Sophos Community를 방문하고 같은 문제를 겪고 있는 다른 사용자들을 검색합니다.
- www.sophos.com/ko-kr/support.aspx에서 Sophos 지원 기술 자료를 방문합니다.
- www.sophos.com/ko-kr/support/documentation.aspx에서 제품 설명서를 다운로드합니다.
- https://secure2.sophos.com/ko-kr/support/contact-support/support-query.aspx에서 당사 지원팀의 티켓을 열어봅니다.

9 법적 고지 사항