

ManageEngine

IT 관리를 안전하고 간편하게!

새로운 속도의 비즈니스를 위한 실시간 IT 관리 솔루션

ManageEngine 

Device Control Plus

중앙 집중식 장치 제어 및 파일 보안 관리를 위한 자동화 솔루션

Device Control Plus?

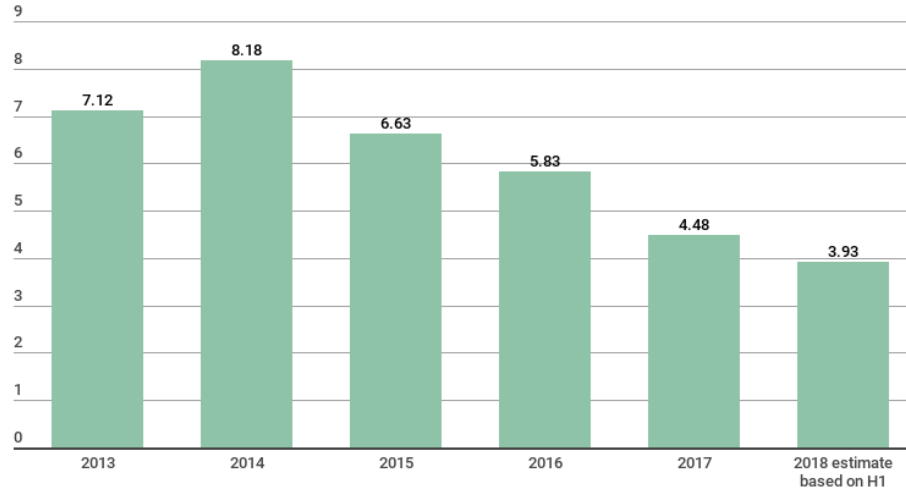
Device Control Plus는 다양한 내장 및 외부 주변 장치의 감지 및 제로 트러스트 기반 관리를 지원하는 완전한 장치 제어 및 파일 이동 관리 소프트웨어입니다.

이 제품의 정보 보안 기능은 조직이 네트워크 경계를 보호하고 데이터 손실을 효과적으로 완화하는 데 도움을 줍니다.

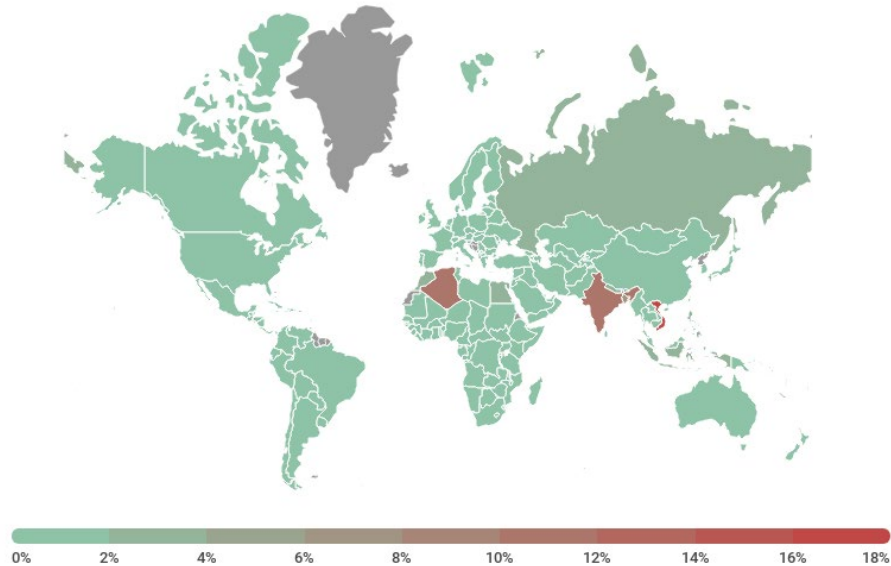
장치 제어가 조직에 중요한 이유는 무엇입니까?



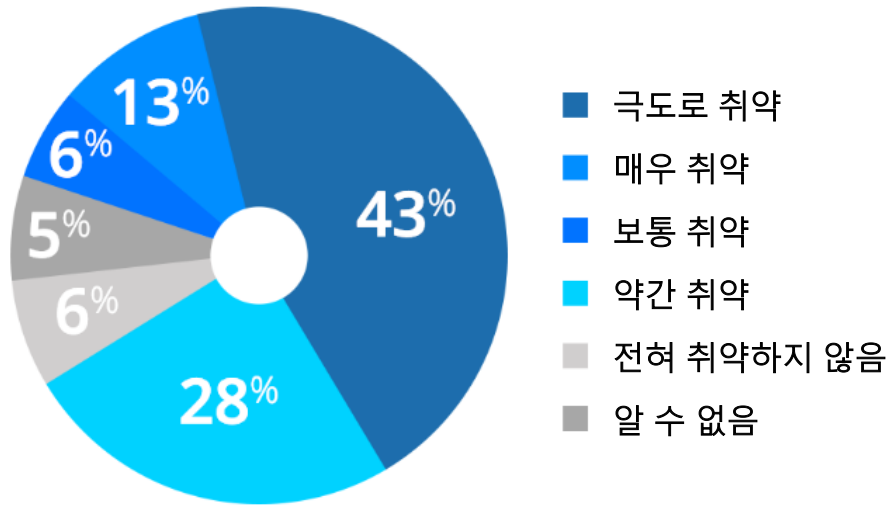
이동식 미디어에 의한 맬웨어 감염의 영향을 받은 사용자 수(백만 단위) 2013 – 2018 년



이동식 미디어를 통한 특정 악용의 영향을 받은 사용자 비율, 2018년도.



일반적으로 사용되는 장치 제어 기능은, 기업 조직에 많은 양의 보호되지 않은 파일을 여전히 남기고 있습니다. 데이터 손실을 방지하려면 강력한 소프트웨어 솔루션이 필요합니다.



다양한 부문의 많은 기업이 내부자 공격 또는 부적절한
장치 사용을 통한 데이터 손실로 위협받고 있습니다.
귀사도 그들 중 하나가 될 수 있습니다.

Who's at risk?



은행/금융



통신, 쇼핑몰



IT 기술 지원



제조/일반 기업



의료 기관



정부 공공기관

효과적인 장치 제어에 대한 장애물

- 매일 수많은 장치 연결이 발생하며, 자동 탐지 기능이 없으면 추적하기 어려울 수 있습니다.
- 다양한 사용자/역할에는 다른 수준의 접근 권한이 필요하므로 매번 접근 권한을 수동으로 할당하는 데 시간이 많이 걸릴 수 있습니다.
- 완전히 허용하거나 완전히 차단하는 것과 같은 기본적인 접근 제어는 너무 제한적이거나 비생산적이거나 안전하지 않을 수 있습니다.
- 세분화된 정책 없이는 데이터 전송 제한을 시행하기 어려울 수 있습니다.

장치 및 데이터 보안을 위한 다목적 솔루션

- 장치 제어는 스펙트럼 데이터 손실 방지 프로토콜 중에서 가장 기본적인 보안 조치 중 하나입니다.
- Device Control Plus를 사용하면 네트워크에 연결된 수많은 주변 장치를 신속하게 감지 및 관리하여, 네트워크를 보호하고 모든 내부 공격 및 악의적인 행위자를 방지할 수 있습니다.
- 또한 모든 기업의 주요 데이터를 보호하고 필요한 경우 파일 액세스 및 전송 제어, 파일 추적 및 새도잉, 임시 장치 액세스 허용 등의 기능을 통해 안전한 데이터 전송을 지원합니다.

3단계로 포괄적인 장치 제어 시행

- 제어할 한 장치 유형을 선택하고 특정 장치들을 선택합니다.
- 특정 운영 요구 사항에 따라 정책을 구성합니다.
- 해당 정책을 지정된 컴퓨터 그룹과 연계합니다.

기능 개요

- 자동 장치 탐색
- 파일 액세스 제어
- 파일 전송 제어
- 파일 추적
- 파일 새도잉 (주요 파일 복사/전송 후 복사본 보관)
- 임시 액세스
- 광범위한 보고서

자동 장치 탐색

- 내장 및 외부 주변 장치의 17개 이상의 유형을 자동으로 감지
- 검색된 각 장치를 신뢰할 수 있음, 허용됨 또는 차단됨으로 분류
- 장치 인스턴스 경로 또는 와일드카드 패턴을 기반으로, 고도로 승인된 직원(신뢰할 수 있는 직원)에 속하는 화이트리스트 장치로 구성된 '신뢰할 수 있는 장치' 목록 생성
- 승인되지 않은 장치가 네트워크 내에서 불법 활동에 들어가거나 수행하는 것을 방지.

파일 액세스 제어

- 직책 및 직무 설명에 따라 사용자에게 권한을 할당하여 역할 기반 보안을 실행.
- 최적의 제어를 위한 다양한 접근 수준 위임: 읽기 전용, 장치 내에서 파일 복사 및 수정, 장치에서 컴퓨터로 파일 이동
- 추가 예방 조치로 BitLocker로 암호화된 장치에 대해서만 파일 액세스를 활성화.

파일 전송 제어

- 사용자가 작업과 관련된 데이터만 얻을 수 있도록 파일 확장자 유형에 따라 데이터 전송을 제한.
- 이용자가 현재의 업무에 필요한 정보를 제공받을 수 있도록 정보를 이전할 수 있는 양에 대한 규정 설정.
- 필요한 정보만 조직에서 승인된 사용자가 이동 허용.

파일 추적

- 조직 내에서 발생하는 모든 파일 전송 활동에 대한 로그를 즉시 확보
- 파일 전송 작업과 관련된 모든 중요한 세부 정보를 분석.

- ✓ 파일 이름, 확장자 및 크기
- ✓ 이동한 초기 위치
- ✓ 데이터 전송에 사용되는 장치
- ✓ 장치가 연결된 컴퓨터
- ✓ 작업을 시작한 사용자



파일 새도잉 (주요 파일 복사/전송 후 복사본 보관)

- 이 기능은 원본 파일의 복사본을 안전한 위치에 저장하여 중요한 파일의 손실을 방지
- USB 장치 내에서 파일을 전송하거나 수정하면 파일 내용이 정확히 복제됨.
- 새도 복사본은 암호로 보호된 네트워크 공유에 유지됨.
- 파일 확장자 및 파일 크기에 따라 새도우 처리되는 파일 유형을 선택할 수 있음.

임시 접근 권한

- 사용자는 사용자 장치에 설치된 Agent Tray의 셀프 서비스 포털을 통해 임시 액세스를 요청할 수 있습니다. 여기서 장치 세부 정보와 요청 이유를 포함하라는 메시지가 표시됩니다.
- IT 관리자는 해당 요청을 검토하고, 콘솔 자체를 통해 또는 고유한 임시 액세스 코드/스크립트가 포함된 이메일을 사용자에게 보내 액세스 권한을 부여할 수 있습니다.
- 권한은 특정 일정을 구성하는 시간 프레임 또는 사용자가 선택한 시간에 활성화할 수 있는 기간을 기반으로 유연하게 지정할 수 있습니다.

광범위한 보고서

- 조직 내에서 발생하는 모든 장치 및 파일 전송 활동에 대한 자세한 로그를 수집합니다.
- 간편한 분석을 위한 스마트 필터(필요한 부분만 검색) 활용
- 모든 정책 위반 사항을 쉽게 찾아냅니다.
- 네트워크 안전과 사용자 요구 사항을 모두 충족하기 위해 정책을 수정하는 방법에 대한 자세한 정보를 확보 가능.
- 대시보드 정보 그래픽을 참조하면, 장치 및 파일 관련 동향을 한 눈에 볼 수 있습니다.

Device Control Plus는 조직에 어떤 도움을 주니까?

- 모든 무단 장치 침입을 방지하고 잠재적인 파일 기반 악용을 제거하여 최적의 사이버 위생을 유지.
- 권한 상승 방지 및 모든 내부 공격 차단
- 데이터 보안 비상 상황 발생 시, 신속한 복구 보장
- 컨설턴트 및 인턴과 같은 제3자 사용자의 임시 장치 액세스를 활성화하여 협업하도록 허용
- 효과적인 정책 생성 및 네트워크에 대한 향상된 가시성을 위해 항상 장치 및 파일 액세스 패턴을 알 수 있음.

감사합니다

텔레먼트 주식회사

<https://www.tmn.co.kr>

02) 588-7350

기술 질문: inforeq@tmn.co.kr

견적 요청: sales-info@tmn.co.kr

