ManageEngine
Endpoint Central

Datasheet

완벽한 엔드포인트 관리 및 보안을 위한 단일 콘솔

오늘의 도전 과제

기업에서 사용하는 엔드포인트의 수와 다양성이 급격히 증가함에 따라 비즈니스 운영 방식이 재정의되었습니다. 이는 또한 다양한 형태의 사이버 공격과 내부자 위협으로 이어집니다. 장치의 형태와 기능이 다양해지면서 요즘 점점 더 많은 기업이 서버, 데스크톱, 노트북, 스마트폰, 태블릿, IoT 장치 등 다양한 기업 장치를 관리하고 보호할 수 있는 단일 소프트웨어 플랫폼을 제공하는 통합 엔드포인트 관리(UEM) 모델을 찾고 있습니다.

통합 솔루션

Endpoint Central은 단일 콘솔에서 서버, 데스크톱, 모바일 장치를 모두 관리하고 보호하는 데 도움이 되는 UEM(unified Endpoint Management) 솔루션입니다. 엔드포인트 관리 수명 주기를 처음부터 끝까지 자동화하여 기업의 IT 인프라 비용 절감, 운영 효율성 달성, 생산성 향상, 네트워크 취약점 및 내부자 위협에 대응, 데이터 유출 방지, 기업 브라우저 보안을 지원합니다.

하이라이트

지원되는 운영 체제

Linux
macOS
ChromeOS
Windows
iOS
Android
Windows Phone
tvOS

세계적 평가사의 인정

IDC FORRESTER Gartner

Endpoint Central을 사용하여

- 정기적인 엔드포인트 관리 활동을 자동화합니다.
- 네트워크 전반에서 OS 및 애플리케이션 구성을 표준화합니다.
- 다양한 위협으로부터 엔드포인트를 보호합니다.
- 일상적인 문제를 해결합니다.
- IT 자산을 감사합니다.

Over 17 years	25,000	관리되는 장치 수 20 million	20	190
제품 출시 기간	제품 사용 기술자 수		번역된 언어 수	판매된 국가 수

패치 관리

- 1,000개 이상의 Windows, Mac, Linux 및 타사 앱에 대한 패치를 자동화합니다.
- 누락된 패치를 사전에 감지하고 배포합니다.
- 배포 전에 패치를 테스트하고 승인하여 보안 위험을 완화합니다.
- 중요한 제로데이 패치를 배포합니다.
- 자동 업데이트를 비활성화하고 필요에 따라 패치를 거부합니다.
- 시스템 상태 및 시스템 취약성에 대한 보고서를 받아보십시오.

소프트웨어 배포

- MSI 및 EXE 기반 애플리케이션을 설치하거나 제거합니다.
- 소프트웨어 배포 일정을 예약하고 배포 전후 작업을 수행합니다.
- 사용자가 셀프 서비스 포털을 사용하여 소프트웨어를 직접 설치할 수 있도록 합니다.
- 미리 정의된 10,000개 이상의 템플릿을 활용하여 애플리케이션을 배포합니다.
- 패키지 저장소를 만들어 소프트웨어를 설치하거나 제거할 때 여러 번 재사용할 수 있습니다. '서비스 계정' 옵션을 사용하여 특정 사용자로 소프트웨어를 설치합니다.

취약점 관리

- 취약점을 즉시 감지하고 수정하여 통합 위협 및 취약성 관리로 보안 태세를 개선합니다.
- 보안 정책을 배포하고 시스템 오류를 완화하여 보안을 강화합니다.
- ManageEngine과 CIS(Center for Internet Security)의 독점적인 파트너십을 활용하여 CIS 벤치마크 준수를 보장합니다.
- 패치가 도착하기 전에 제로데이 취약점을 신속하게 발견하고 해결 방법으로 완화 스크립트를 배포합니다.
- 수명이 다한 소프트웨어, 원격 데스크톱 공유 소프트웨어, P2P 소프트웨어와 같은 고위험 소프트웨어를 감사하고 제거하여 데이터 유출로부터 안전을 유지합니다.
- 취약성 관리의 일환으로 활성 포트를 감사하여 이상 징후를 발견합니다.

자산 관리

- 네트워크의 모든 하드웨어와 소프트웨어를 실시간으로 추적합니다.
- 소프트웨어 라이선스 규정 준수를 보장합니다.
- 실행 파일을 차단하고 금지된 소프트웨어를 제거합니다.
- 소프트웨어 사용 통계를 분석하고 소프트웨어 미터링을 사용하여 사용하지 않는 소프트웨어와 관련된 비용을 절감합니다.
- 새 소프트웨어 감지, 라이선스 미달로 인한 규정 미준수, 금지된 소프트웨어 등 특정 이벤트에 대한 알림을 받습니다.
- 하드웨어, 소프트웨어, 재고 및 라이선스 규정 준수를 위한 20개 이상의 사전 정의된 보고서를 활용합니다.

모바일 애플리케이션 관리

- IT 부서에서 승인한 사내 및 상업용 앱만 포함하는 엔터프라이즈 앱 저장소를 직접 만듭니다.
- 장치에서 회사 앱을 자동으로 설치, 업데이트, 제거하는 동시에 앱 라이선스를 관리하고 앱 권한을 사전 구성할 수 있습니다.
- 장치에서 신뢰할 수 있는 회사 앱만 실행하도록 하고, 악성/취약성 있는 앱을 블랙리스트에 추가하고, 사용자가 회사 앱을 제거하지 못하도록 합니다.

시스템 도구

- 원격으로 관리되는 시스템에서 실행 중인 작업 세부 정보 및 프로세스를 확인하여 원격으로 관리되는 시스템을 모니터링하고 분석합니다.
- Wake-on-LAN을 사용하여 원격으로 즉시 컴퓨터를 부팅하거나 부팅을 예약합니다.
- 회사 전체 또는 기술자에게만 공지 사항을 게시합니다.
- 로컬 또는 원격 워크스테이션의 디스크 조각 모음, 디스크 검사 및 디스크 정리를 예약합니다.

애플리케이션 제어

- 설치된 모든 애플리케이션과 실행 파일을 검색하고 디지털 서명에 따라 기업 승인 또는 미승인으로 분류합니다.
- 제로 트러스트 환경을 효율적으로 구축할 수 있는 다양한 모드를 제공하는 유연한 규제를 제공합니다.
- 사용자가 애플리케이션에 대한 액세스를 요청할 수 있는 번거로움 없는 애플리케이션 제어를 제공합니다.
- 관리되지 않는 애플리케이션도 자동으로 금지하는 엄격한 모드를 활성화하여 제로 트러스트 접근 방식을 채택합니다.

데이터 유출 방지

- 중앙 집중식 콘솔에서 기업 데이터 이동을 모니터링하고 규제하여 내부자 공격과 데이터 손실을 방지합니다.
- 규정 준수 및 규제 표준에 따라 기업의 중요 데이터를 스캔하고 분류합니다.
- 클라우드 업로드, 이메일 교환, 프린터 및 기타 주변 장치를 통한 데이터 전송 시도를 규제합니다.
- 정책 위반 시도에 대한 즉각적인 알림을 받고 오탐 이벤트를 수정합니다.

브라우저 보안

- 기업용 브라우저를 잠그고 브라우저 설정을 강화하여 브라우저 기반 공격을 방지합니다.
- 네트워크에서 사용 중인 여러 브라우저를 종합적으로 파악할 수 있습니다.
- STIG 및 CIS 규정 준수와 같은 브라우저 보안 구성을 적용합니다.
- 유해한 플러그인을 감지하고 제거하여 안전한 브라우징 환경을 구현합니다.
- 기업에서 승인한 웹사이트를 허용하고 원치 않는 웹앱을 차단하여 생산성과 보안을 강화합니다.

모바일 장치 관리

- BYOD 및 회사 장치의 일괄 등록 및 인증을 자동화합니다.
- OS 업데이트를 제어하고 원격 모바일 장치 문제를 해결합니다.
- 미리 정의되고 사용자 지정 가능한 보고서를 통해 조직의 모바일 자산에 대한 완벽한 가시성을 확보합니다.

모바일 보안 관리

- Wi-Fi, VPN, 이메일 등에 영향을 미치는 기업 보안 정책을 구성하고 적용합니다.
- 회사 이메일에 대한 무단 액세스를 방지하고 콘텐츠를 안전하게 배포, 저장 및 확인할 수 있습니다.
- 장치 수준 암호화 적용, BYOD 장치에서 개인 및 회사 업무 공간 격리, 잘못 배치된 장치의 위치 찾기, 잠금 및 삭제를 제공합니다.

구성

- 전체 조직을 위한 기본 구성으로 데스크톱, 컴퓨터, 애플리케이션 및 보안 설정을 표준화합니다.
- 사용자 및 컴퓨터에 대해 40개 이상의 구성을 사용하거나 자주 사용하는 구성을 위한 템플릿을 만듭니다.
- 스크립트 저장소에 있는 180개 이상의 스크립트 중에서 선택합니다.
- 네트워크에서 프린터, CD 드라이브, 휴대용 장치, 블루투스 장치, 모뎀 및 기타 주변기기와 같은 USB 장치의 사용을 사용자 및 컴퓨터 수준에서 제한하고 제어할 수 있습니다.
- 전력 계획을 적용하고, 비활성 컴퓨터를 종료하고, 시스템 가동 시간 보고서를 확인하여 효과적인 전력 관리로 친환경을 실현합니다.
- 브라우저, 방화벽 및 보안 정책을 구성하고 권한 관리를 사용하여 파일, 폴더 및 레지스트리에 대한 액세스 제어를 달성합니다.
- 비밀번호 만료 및 시스템 드라이브 공간 부족에 대한 알림을 설정합니다.

주변 장치 제어

- 중앙 콘솔에서 활성 포트 자동 감지와 함께 15개 이상의 주변 장치 유형을 효과적으로 규제하고 제한할 수 있습니다.
- 역할 기반 파일 액세스 및 파일 전송 제한을 통한 전송 제어로 기업 중요 데이터를 보호합니다.
- 정의된 기간 동안 특정 엔드포인트에 대한 주변 장치의 임시 액세스 권한을 부여할 수 있습니다.
- USB 장치가 중요한 기업 데이터에 액세스할 때 안전한 위치에 데이터를 미러링하여 데이터 손실을 사전에 방지합니다.
- 주변 장치를 통한 데이터 손실을 방지하여 장치 규정 준수 표준을 준수하고 종합적인 장치 감사 보고서를 제공합니다.

보고서

- 사용자, 컴퓨터, 그룹, OU 및 도메인에 대한 200개 이상의 기본 제공 Active Directory 보고서를 활용합니다.
- 효과적인 전력 관리로 유틸리티 요금을 절감하고 시스템 가동 시간 보고서를 확인합니다.
- 사용자 로그온 보고서를 통해 최신 사용자 로그온 세부 정보를 얻습니다.
- 감사할 패치, 구성 및 이벤트에 대한 보고서를 확인합니다.

엔드포인트 권한 관리

- 불필요한 관리자 권한을 제거하고 제한된 권한으로 비즈니스 크리티컬 애플리케이션을 실행하여 권한 상승 또는 자격 증명 손상을 기반으로 한 공격을 방지합니다.
- 애플리케이션별 권한 상승을 활성화하여 생산성을 저하시키지 않고 최소 권한 모델을 유지합니다.
- 설정된 기간이 지나면 자동으로 해지되는 애플리케이션에 대한 임시 권한 액세스를 활성화하여 임시 사용자의 요구를 처리합니다.

랜섬웨어으로부터 보호

- 랜섬웨어를 게이트키핑하여 엔드포인트 보안을 강화하는 반응형 보호를 제공합니다.
- 여러 특허를 받은 머신 러닝 지원 행동 분석은 네트워크에 침입하려는 모든 랜섬웨어를 즉시 탐지합니다.
- 모든 침입 시도에 대한 자세한 분석을 제공합니다.
- 클릭 한 번으로 데이터를 복구할 수 있는 원활한 롤백 기능을 제공합니다.

원격 제어

- 안전한 원격 제어를 활용하여 HIPAA 및 PCI DSS를 비롯한 다양한 규정 준수 규정을 준수합니다.
- 여러 사용자 간의 협업을 통해 원격 데스크톱 문제를 원활하게 해결합니다.
- 통합 비디오, 통화, 채팅, 컴퓨터 간 파일 전송 옵션이 제공됩니다.
- 감사 목적으로 전체 원격 제어 세션을 녹화합니다.
- 최종 사용자의 키보드와 마우스를 잠그고 화면을 검게 하여 원격 세션 중 기밀을 보장합니다.
- 원격 제어 작업 시 128비트 AES 암호화 프로토콜을 활용합니다.

OS 배포

- 지능형 온라인 및 오프라인 이미징 기술을 사용하여 컴퓨터가 작동 중이거나 종료된 상태이든 상관없이 자동으로 이미지를 캡처합니다.
- 이러한 이미지를 중앙 저장소에 저장하고 이동 중에도 OS 배포를 수행할 수 있습니다.
- 조직 내 다양한 역할과 부서에 맞게 배포 템플릿을 사용하여 캡처한 이미지를 사용자 지정합니다.
- 다양한 유형의 하드웨어에 번거로움 없이 배포할 수 있습니다.
- 애플리케이션 설치, 컴퓨터 설정 구성 등과 같은 배포 후 활동을 실행합니다.

BitLocker 관리

- 일부 드라이브 또는 전체 하드 드라이브에 대한 암호화를 자동화하여 컴퓨터의 데이터를 보호합니다.
- 암호 인증과 함께 향상된 PIN 보안을 위해 TPM이 설치된 컴퓨터를 식별합니다.
- 하드웨어에 결함이 있는 경우 복구 키를 사용하여 컴퓨터의 데이터를 검색하고 네트워크에서 제거된 컴퓨터의 비밀번호를 재설정합니다.
- 데이터 암호화 정책을 적용하고 FISMA, HIPAA, PCI-DSS와 같은 데이터 보호 가이드라인을 준수합니다.

차세대 바이러스 백신

- 실시간 AI 지원 멀웨어 탐지는 진화하는 위협에 대한 보호를 강화합니다.
- 자세한 보고서가 포함된 종합적인 사고 포렌식은 MITRE 전술, 기법 및 절차(TTP)에 부합합니다.
- 공격 방법, 경로 및 킬 체인 분석에 대한 심층적인 자료를 제공합니다.
- 랜섬웨어 보호를 포함한 즉각적인 침입 완화 기능으로 신속한 침입 무력화를 보장합니다.
- 네트워크 운영 중단을 최소화하면서 위협을 완화하여 비즈니스 연속성을 보장합니다.
- 원클릭 파일 복구를 통해 사용자는 간단한 클릭만으로 손상된 파일을 원래 상태로 쉽게 복원할 수 있습니다.