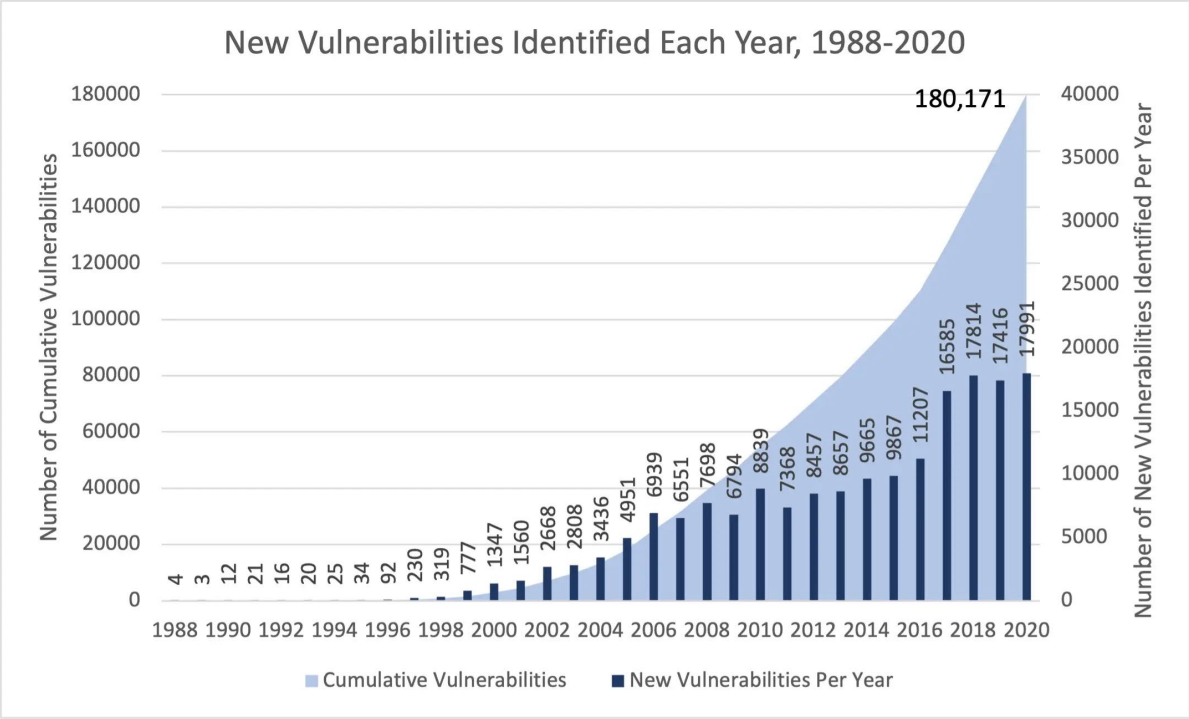
ManageEngine

Vulnerability Manager Plus

우선 순위 중심의 위협 요소 및 취약성 관리 소프트웨어 제공
엔터프라이즈용 내장된 패치 기능 적용

취약점 관리가 필요한 이유

항상 증가하는 IT 취약점 추세



Source: https://securityintelligence.com/posts/top-10-cybersecurity-vulnerabilities-2020/

엔드포인트 보안을 소홀히 하면 큰 비용이 발생할 수 있습니다.

향후 5년간 보안 손실 예상액

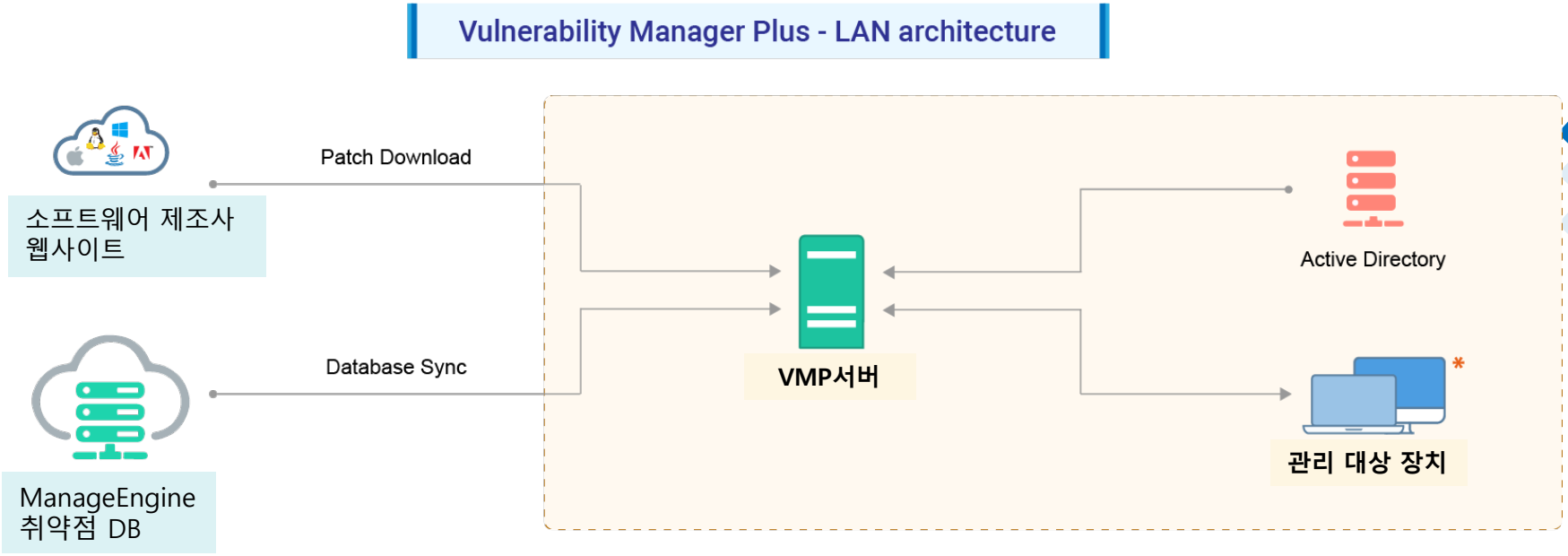
900조원

- Expected foregone revenue cumulative over the next 5 years. Calculations over a sample of 4,700 global public companies
  Source: Accenture Research

효과적인 취약성 관리를 방해하는 장애물

- 다양한 위험 요소가 있는 너무 많은 취약점
- 이기종 분산 네트워크에 분산되어 있는 취약점을 지속적으로 파악할 수 있는 시간, 리소스 및 중앙 집중식 수단의 부족
- 취약점 평가 및 패치 관리를 위한 여러 도구를 이리 저리 섞어서 사용하여 단편적이고 비효율적인 업무의 흐름 생성
- 잘못된 구성과 보안 허점을 추적하고 수정할 수 없음
- 간헐적인 스캔으로 보안 의 공백 발생, 실패로 이어짐

Vulnerability Manager Plus 구조 (LAN 환경)

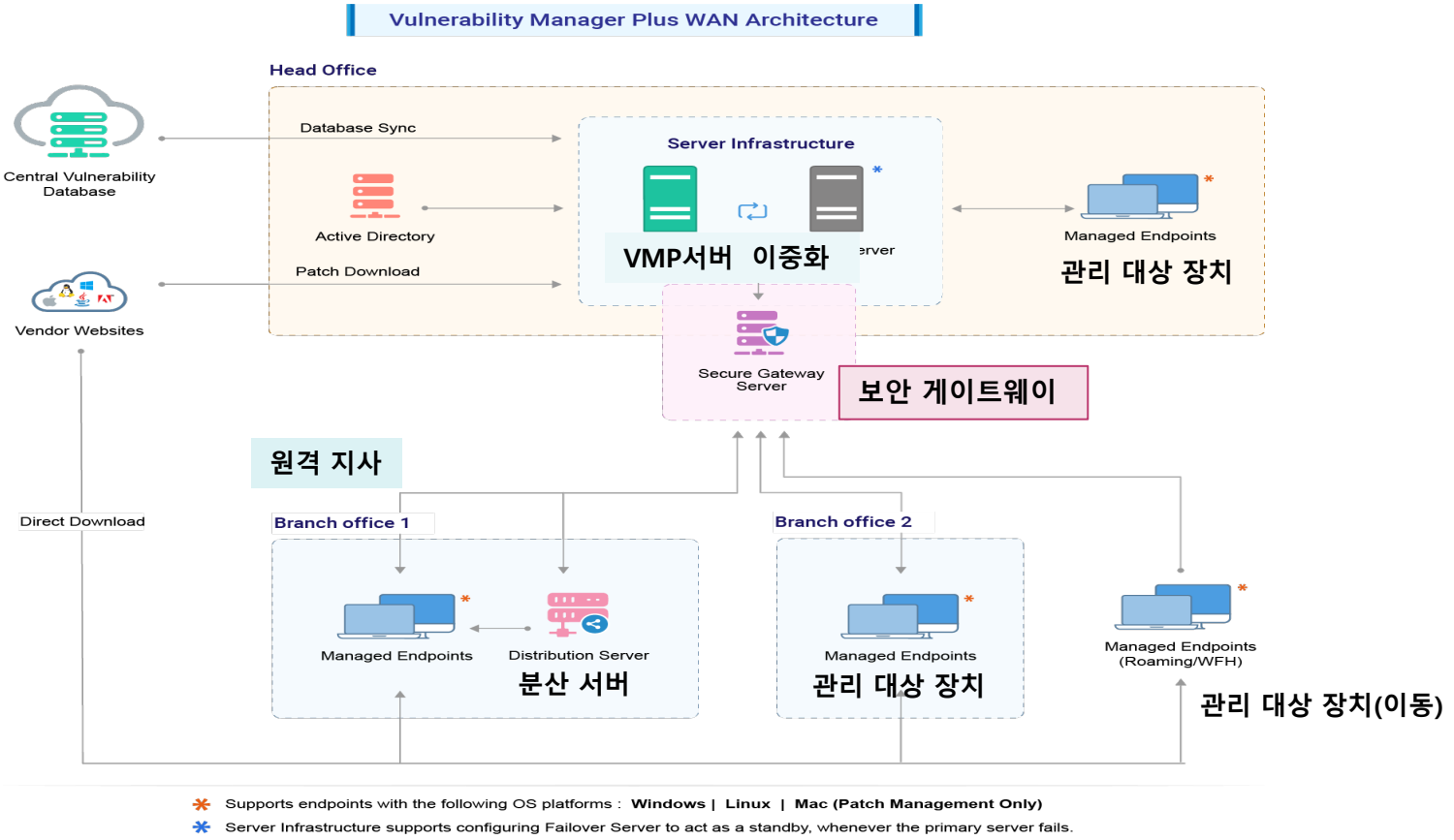


* Supports endpoints with the following OS platforms : **Windows | Linux | Mac (Patch Management Only)**

Vulnerability Manager Plus 구조 (WAN 환경)

ManageEngine 취약점 DB

소프트웨어 제조사 웹사이트



취약점 관리 3 단계 프로세스

스캔 (감사)

로밍 장치뿐만 아니라 모든 로컬 및 원격 사무실 엔드포인트의 노출된 영역을 스캔하고 발견합니다.

평가

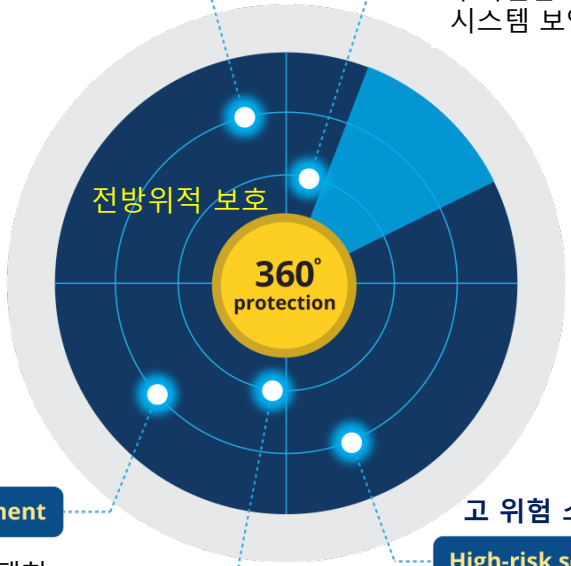
공격자 기반 분석을 활용하고 공격자가 악용할 가능성이 높은 영역의 우선순위를 지정합니다.

관리

네트워크에 존재하는 보안 허점의 악용을 완화하고 더 이상의 허점이 발전하는 것을 방지합니다..

기능: Sneak peek

(몰래 들여다보기)



취약점 평가

Vulnerability assessment

공격자 기반 분석을 활용하고 공격자가 악용할 가능성이 더 큰 취약점의 우선 순위를 지정합니다.

보안 구성 관리

Security configuration management

부적절한 보안 설정을 제거하고 시스템 보안을 강화합니다.

패치 관리

Patch management

패치할 대상, 패치 시기 및 패치 방법을 결정합니다.
더 중요한 것은 자동화입니다.

고 위험 소프트웨어 감사

High-risk software audit

네트워크에서 인증되지 않은 지원되지 않는 소프트웨어를 감사하고, 단 한번의 버튼 클릭으로 제거할 수 있습니다.

웹 서버 강화

Web server hardening

XSS, Clickjacking 등과 같은 다양한 공격으로부터 인터넷을 사용하는 서버를 보호합니다.

포괄적인 취약점 평가를 통해 패치할 항목 우선 순위 지정

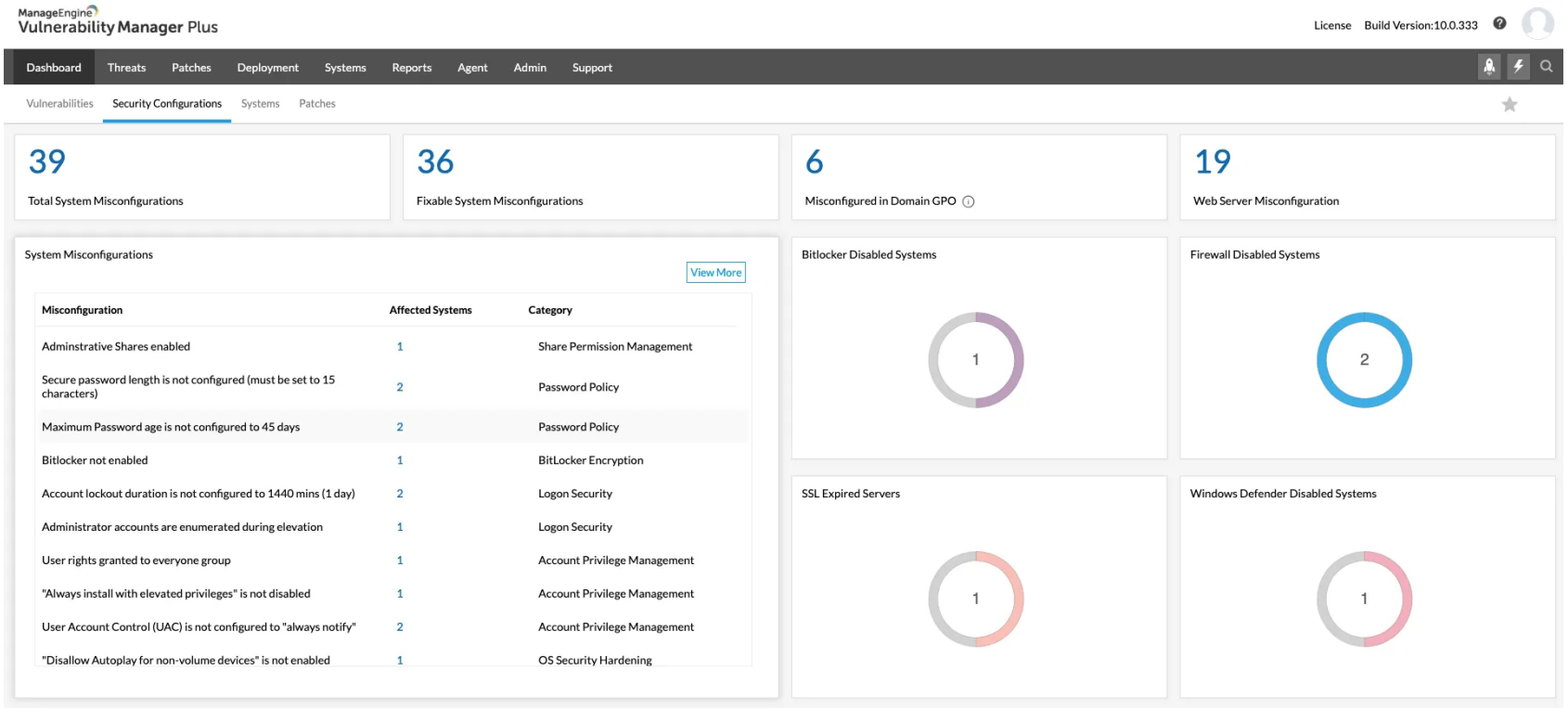
- CVSS 및 심각도 점수와 같은 컨텍스트와 함께 취약점을 식별하여 우선 순위, 긴급성 및 영향을 확인
- 각 취약점에 대해 취약점 코드가 공개적으로 공개되었는지 여부 확인
- 취약점이 네트워크에 있는 기간 동안 계속 감시
- 영향 유형 및 패치 가용성에 따라 취약점을 분류 확인
- 위의 위험 요소들을 기반으로 수집한 높은 취약점에 대한 권장 사항 가져오기
- 공개된 취약점 및 제로 데이 취약점에 대한 전용 탭을 활용하고 해결 방법을 활용하여 수정 사항이 도착하기 전에 영향을 완화
- 중요한 데이터를 보관하고 중요한 비즈니스 운영을 수행하는 데이터베이스 및 웹 서버와 같은 중요 자산에서 취약점을 격리하고 식별

취약점 평가 유튜브 ➔ https://youtu.be/QfzFLQXNxiA

보안 구성 관리를 통한 보안 기반 구축

- 운영 체제, 애플리케이션 및 브라우저에서 잘못된 구성을 식별하고 다시 규정 준수 상태로 전환
- 방화벽, 바이러스 백신 및 BitLocker 상태 감사
- 복잡한 암호, 계정 잠금 및 보안 로그온 정책을 적용하여 무차별 시도 방지
- 구조화된 예외 처리 덮어쓰기 방지, 데이터 실행 방지 및 주소 공간 레이아웃 임의 추출과 같은 메모리 보호 설정 사용
- 이익보다 위험이 큰 레거시 프로토콜 폐지
- 공유 권한 관리, 사용자 계정 컨트롤 수정 및 레거시 프로토콜 비활성화로 공격 표면 감소
- 중요한 배포 경고를 통해 비즈니스 운영을 중단하지 않고 보안 구성을 안전하게 변경

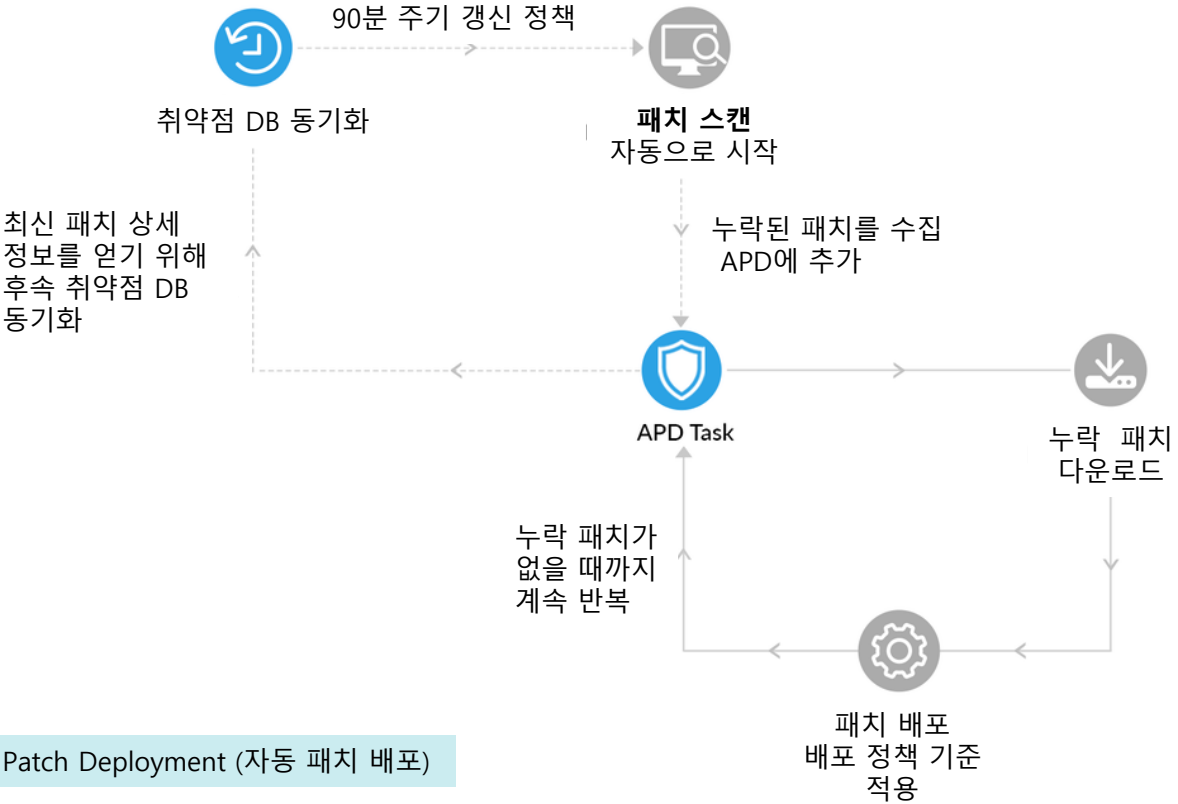
Vulnerability Manager Plus 로 쉽게
Security configuration management (SCM: **보안 구성 관리) 구축**



자동화된 패치 관리

- 수집된 취약점 정보를 패치 관리와 자동으로 연계하여 적용
- Windows, macOS, Linux 및 300개 이상의 타사 응용 프로그램에 대한 자동 패치
- 번거롭지 않은 배포를 위한 배포 정책 사용자 지정
- 패치를 프로덕션 시스템에 배포하기 전에 테스트 및 승인
- 특정 그룹에 대한 패치 거부

자동 패치 배포 작업 워크플로

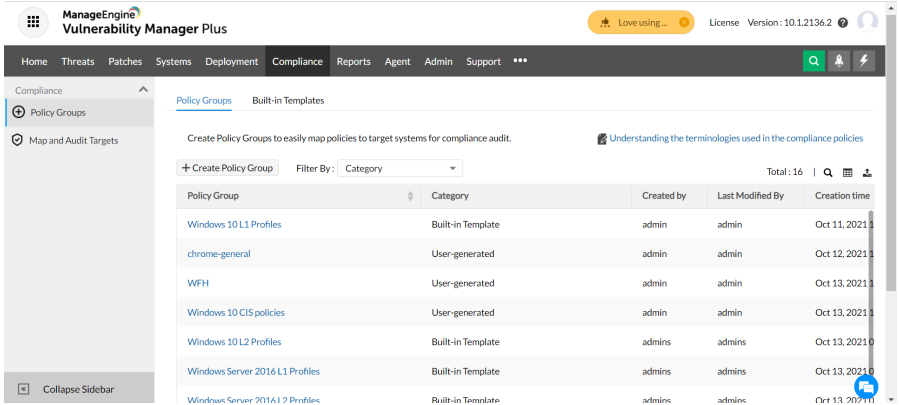


APD: Automate Patch Deployment (자동 패치 배포)

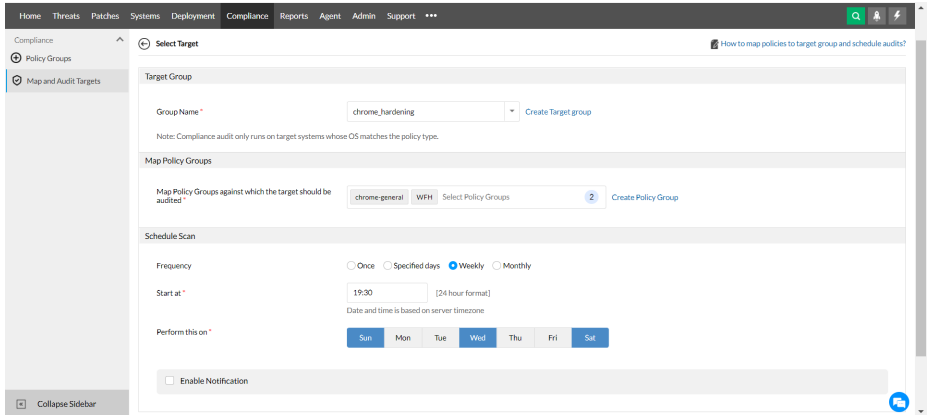
CIS benchmarks 의 규정 준수

- 75개 이상의 CIS 벤치마크에 대한 감사 및 규정 준수를 지원
- 여러 CIS 벤치마크에 대해 한 번에 여러 자산에 대한 감사 자동화
- 모든 위반 사항에 대한 자세한 수정 사항을 확보

신속한 그룹 정책 적용

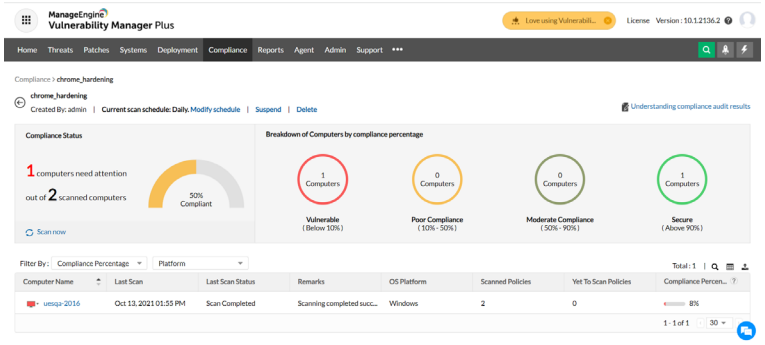


대상 장치를 일정 감사(스캔)에 적용

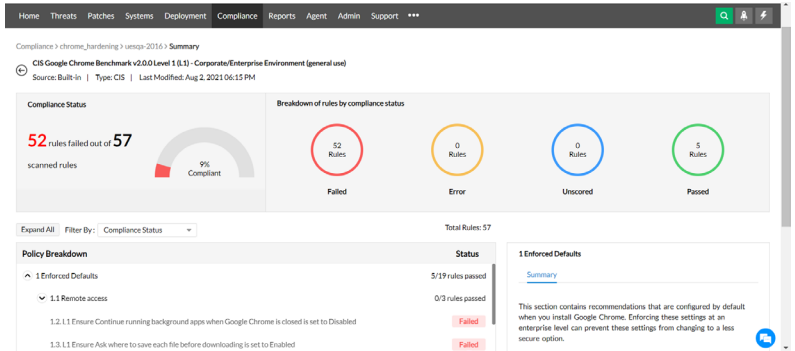


감사 기능을 통한 규정 준수 개선

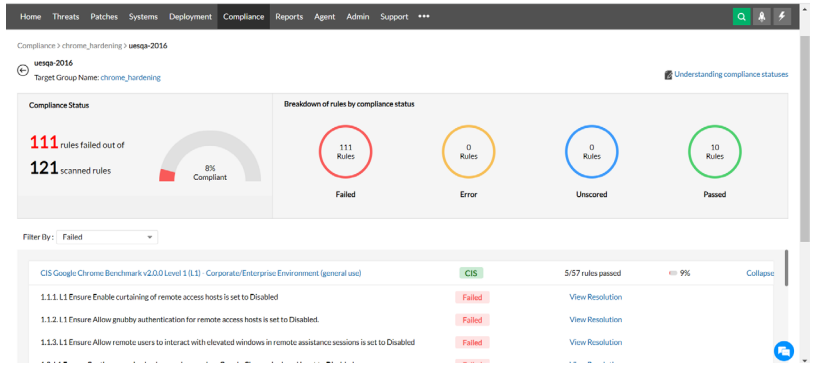
대상 장치 그룹 보기



CIS 정책 보기



대상 장치 그룹 규정 준수 상태 보기



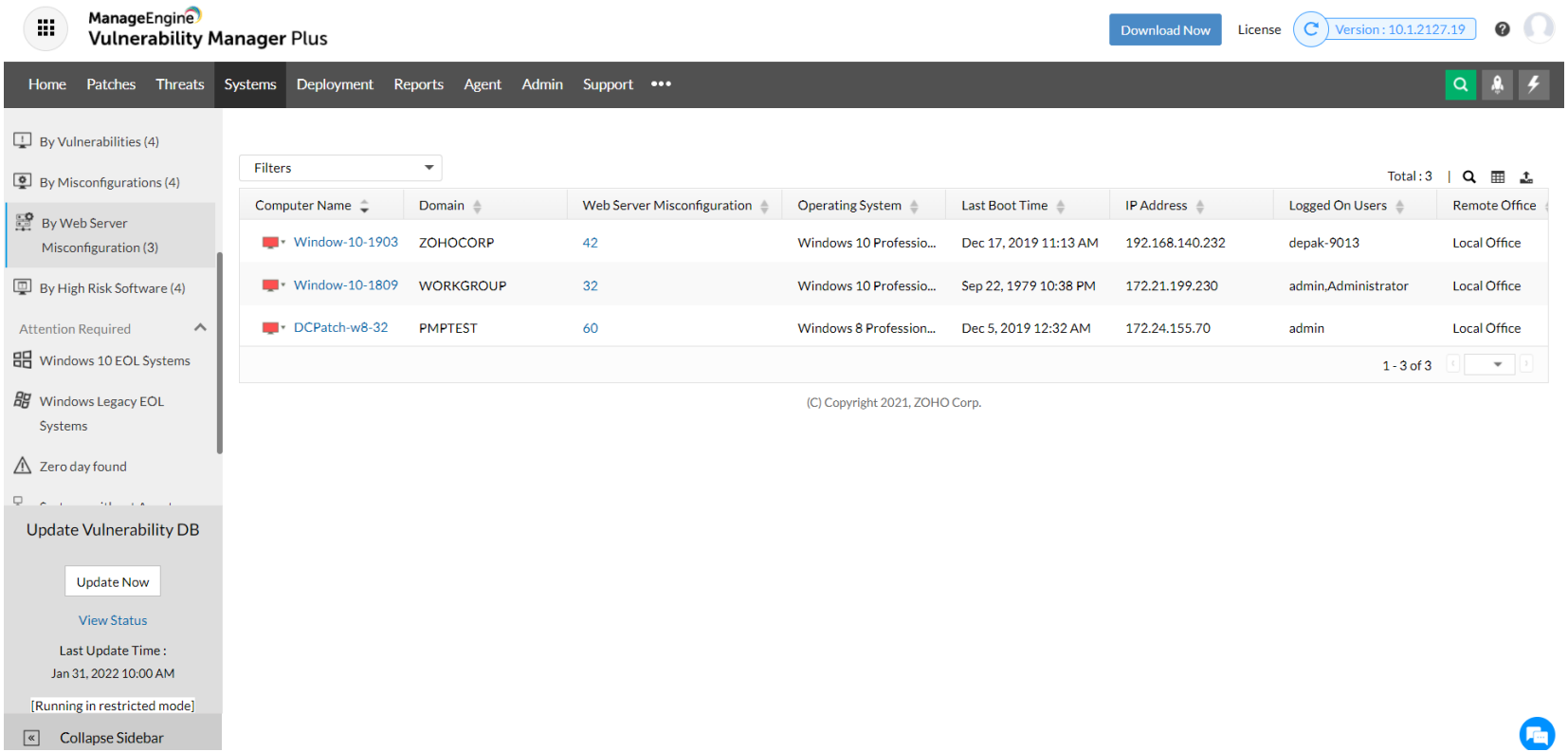
Intelligent 보고서

- 통합 요약 보고서
  - 자산 요약
  - 취약점 요약
  - 패치 요약
  - 위협 우선 순위 보고서
- 준비된 10 가지 종류의 보고서: PDF, CSV, XLSX 형식
- 예약 보고서
- 사용자 정의 쿼리 보고서

Web server 강화

- 웹 서버에서 기본 상태의 구성과 안전하지 않은 구성을 지속적으로 모니터링
- 상황 분석에 따라 웹 서버의 잘못된 구성을 분석하고 보안 권장 사항 확보
- 클라이언트와 서버 간의 통신을 보호하기 위해 SSL 인증서가 구성되어 있고 HTTPS가 활성화되어 있는지 확인
- 무단 액세스를 방지하기 위해 서버 루트 디렉터리 권한이 제한되어 있는지 확인

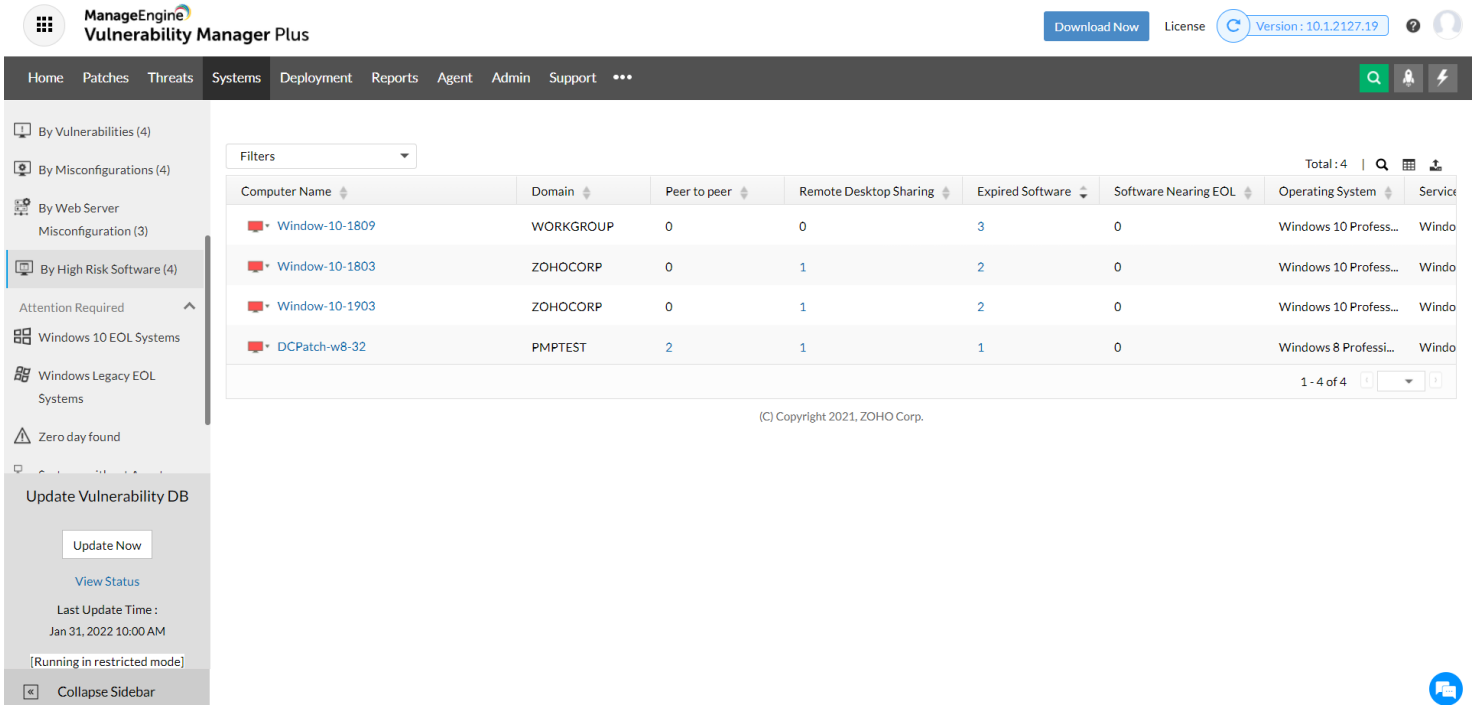
웹 서버 상태 현황


ManageEngine
Vulnerability Manager Plus
Download Now
License
Version : 10.1.2127.19
Home
Patches
Threats
Systems
Deployment
Reports
Agent
Admin
Support
By Vulnerabilities (4)
By Misconfigurations (4)
By Web Server Misconfiguration (3)
By High Risk Software (4)
Attention Required
Windows 10 EOL Systems
Windows Legacy EOL Systems
Zero day found
Update Vulnerability DB
Update Now
View Status
Last Update Time :
Jan 31, 2022 10:00 AM
[Running in restricted mode]
Collapse Sidebar
Filters
Total : 3
Computer Name
Domain
Web Server Misconfiguration
Operating System
Last Boot Time
IP Address
Logged On Users
Remote Office
Window-10-1903
ZOHOCORP
42
Windows 10 Professio...
Dec 17, 2019 11:13 AM
192.168.140.232
depak-9013
Local Office
Window-10-1809
WORKGROUP
32
Windows 10 Professio...
Sep 22, 1979 10:38 PM
172.21.199.230
admin,Administrator
Local Office
DCPatch-w8-32
PMPTEST
60
Windows 8 Profession...
Dec 5, 2019 12:32 AM
172.24.155.70
admin
Local Office
1 - 3 of 3
(C) Copyright 2021, ZOHO Corp.

고위험 소프트웨어와 활성 포트 감사

- 수명이 다했거나 거의 만료될 레거시 소프트웨어에 경계 유지
- 안전하지 않은 것으로 간주되는 P2P소프트웨어 및 원격 공유 도구에 대한 실시간 정보를 얻고, 원 클릭 버튼으로 제거
- 시스템의 활성 포트에 대한 지속적인 가시성을 확보하고 악성 실행 파일에 의해 포트가 활성화된 인스턴스를 탐지

악성 소프트웨어 현황


ManageEngine
Vulnerability Manager Plus
Download Now
License
Version : 10.1.2127.19
Home
Patches
Threats
Systems
Deployment
Reports
Agent
Admin
Support
By Vulnerabilities (4)
By Misconfigurations (4)
By Web Server Misconfiguration (3)
By High Risk Software (4)
Attention Required
Windows 10 EOL Systems
Windows Legacy EOL Systems
Zero day found
Update Vulnerability DB
Update Now
View Status
Last Update Time :
Jan 31, 2022 10:00 AM
[Running in restricted mode]
Collapse Sidebar
Filters
Total : 4
Computer Name
Domain
Peer to peer
Remote Desktop Sharing
Expired Software
Software Nearing EOL
Operating System
Service
Window-10-1809
WORKGROUP
0
0
3
0
Windows 10 Profess...
Windo
Window-10-1803
ZOHOCORP
0
1
2
0
Windows 10 Profess...
Windo
Window-10-1903
ZOHOCORP
0
1
2
0
Windows 10 Profess...
Windo
DCPatch-w8-32
PMPTEST
2
1
1
0
Windows 8 Professi...
Windo
1 - 4 of 4
(C) Copyright 2021, ZOHO Corp.

Vulnerability Manager Plus 의 사용 장점

- 사용자가 거의 개입할 수 없는 즉각적인 공격 가능한 위협 조기 식별
- 중앙 콘솔과 통찰력 있는 대시보드로 취약성 관리에 소요되는 노력 대폭 감소
- 별도의 패치 관리 도구에 대한 투자 필요성 제거
- 사이버 보안 규정 준수 및 규정 준수로 막대한 손실 방지
- 유연하고 사용하기 쉬운 제품

Vulnerability Manager Plus 설치 옵션

자체 플랫폼

공공 클라우드:

aws

kt Cloud

Microsoft Azure

Awards and recognition

Available in 3 editions

01

Free Edition

Up to 25 computers

- Suitable for SMBs
- Fully functional
- Up to 25 computers

02

Professional

suitable for computers in LAN

- Vulnerability scanning and assessment
- System misconfiguration detection
- High-risk software detection
- Detection and resolution of server misconfigurations
- Vulnerability reports

03

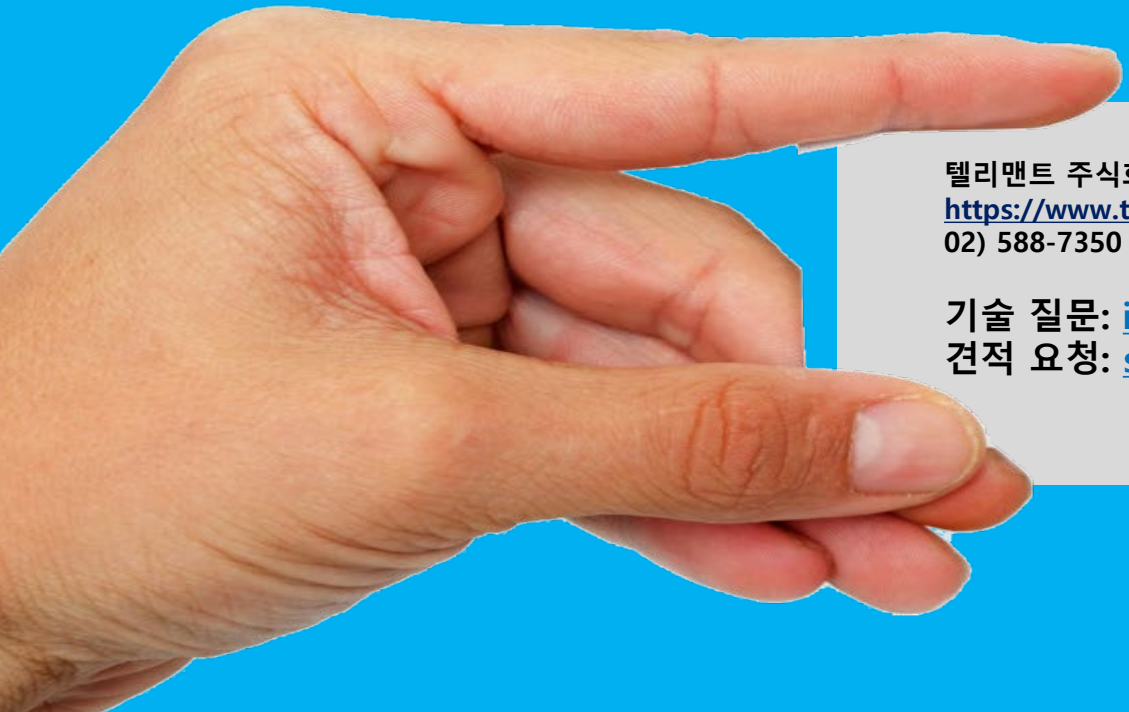
Enterprise

suitable for computers in WAN

Professional Edition features +

- Secure configuration deployment
- Compliance
- Automated Patch deployment
- Test and approve patches
- High-risk software uninstallation
- Zero-day vulnerability mitigation

Thank You



텔리맨트 주식회사
https://www.tmn.co.kr
02) 588-7350

기술 질문: inforeq@tmn.co.kr
견적 요청: sales-info@tmn.co.kr