Genian GPI

제품소개서

2017.01

GeniNet

목 차

Genian GPI 소개

Prologue

Compliance ?

회사 임직원들이 사회적으로 승인된 내·외부 준거 기준(법·규정·회사 사규나 매뉴얼·문화·관습·사회적 책임 등)을 수용하고 이행하는 조직의 문화라고 정의할 수 있다 (Deloitte 2015)

특정 주요정보

PCI DSS COMPLIANT

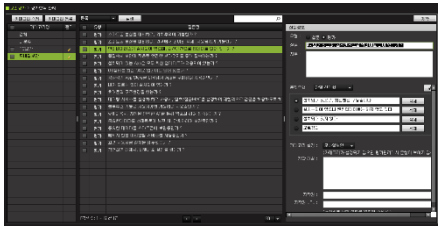
HIPAA COMPLIANCE

우리회사 내부정책

FACILITIES

규제 정책 & 회사의 정책

적용정책의 정립,
적용방안(일정, 평가방법)

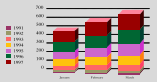


시스템화

Prologue

Awareness 장비 ? :
사용자의 보안의식을 강화하기 위해, 일반사용자에게 보안 규약, 정책을 알림, 교육, 점검을 위한 장비로
사용자가 스스로 단말의 보안을 유지 하기 위한 일련의 행동을 지속적으로 유도/점검함

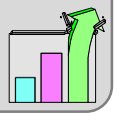
검사/측정
1. 현재의 Status ?



분석
2. 취약점, 요소 찾기

가이드/ 조치 안내
3. 학습/직접수행

지속적 관리 컨텐츠 업데이트
4. 보안의식 상승
& 단말의 보안성 증가

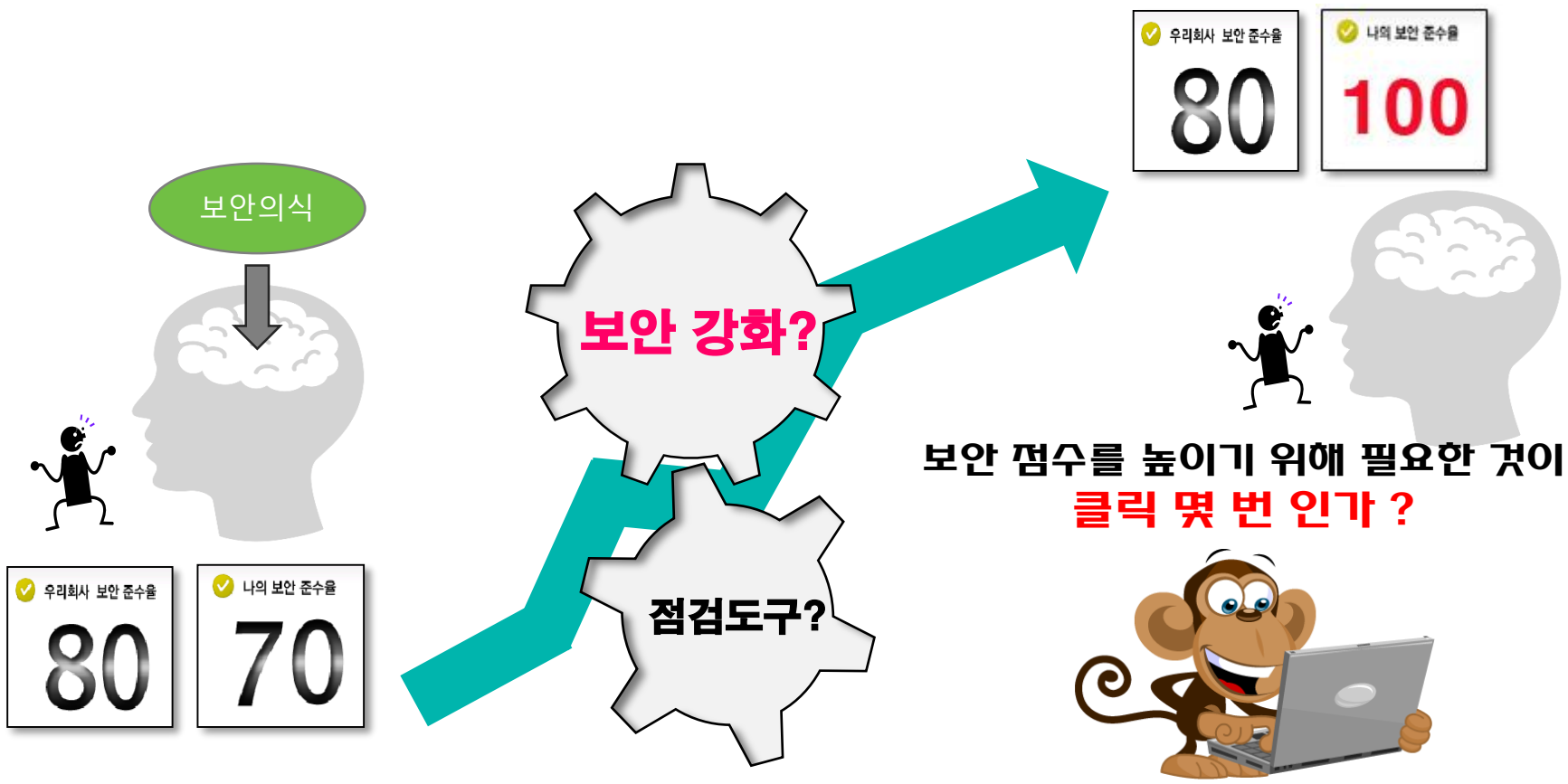


Who are the bad guys ?

출처 : IBM Security intelligence 2015

Why Awareness ?

보안 점검 솔루션의 착각 오류 : 보안의식을 높이기 위해선, 사용자의 직접 참여가 필수 !



Prologue

보안상태에 대한 가시성 제공

보안상태 지수화(가시성)
- 사용자 단말에 대한 보안평가
- 사용자 행동에 대한 보안평가
- 보안의식에 대한 평가

일회성이 아닌 지속적인 관리
- 사용자 보안의식 향상
- 능동적인 보안 문화 형성
- 조직 보안 수준 향상

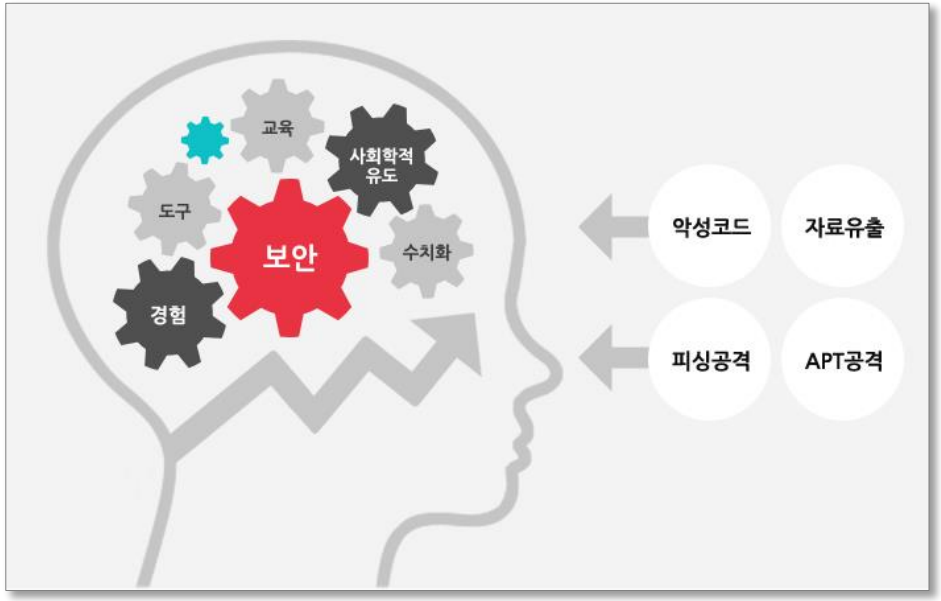
긍정적 착각
대다수의 사람들은
자신이 속한 그룹에서
자신이 평균 이상이라고 생각

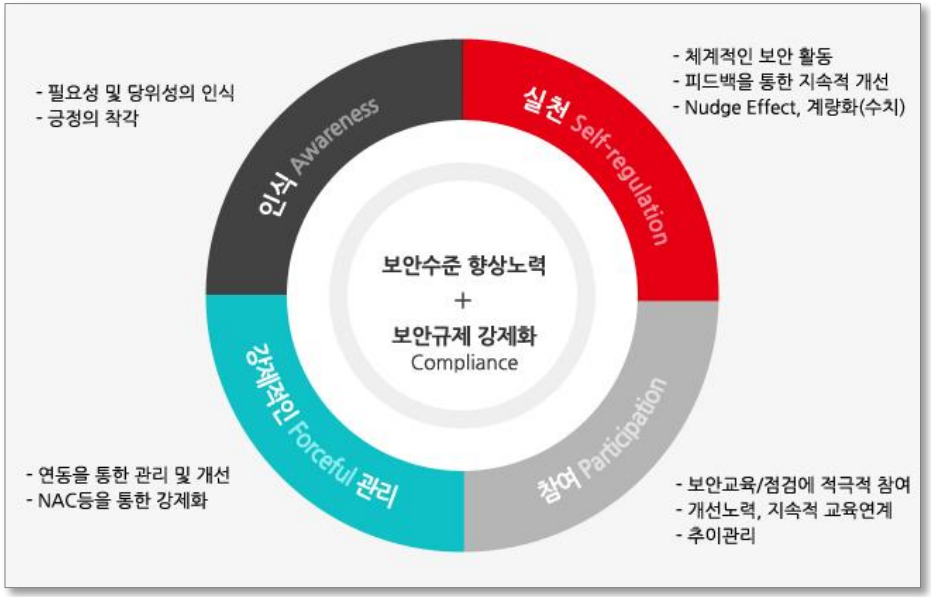
Genian GPI - 필요성

보안 관리 및 인식 개선 필요

네트워크에 아무리 고가의 솔루션을 구입하여 완벽하다고 생각되는 보안체계를 구축해도 보안수준이 낮은 사용자가 많다면 애써 끌어올린 보안수준이 낮아지기 마련입니다. 보안의 시작과 끝은 바로 사람입니다.

Genian GPI 는 고객사 내부 사용자 PC 에 대한 진단과 결과를 개인/부서별 수치화하여 사용자로 하여금 보안 규정을 준수, 조직의 보안수준 향상, 자발적이고 능동적인 보안문화를 조성할 수 있도록 하는 데에 그 목적이 있습니다.



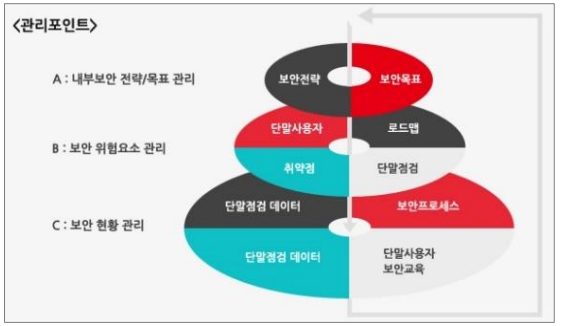


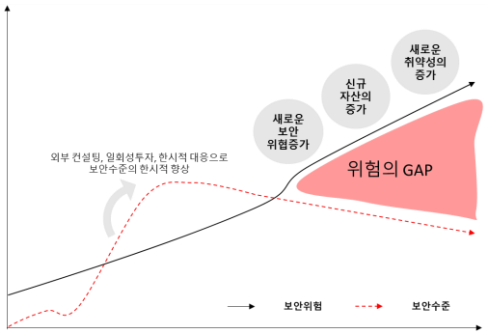
Genian GPI - 기대효과

조직의 보안 수준 개선 및 보안 문화 조성

- **전사적 차원의 보안문화 조성 가능**

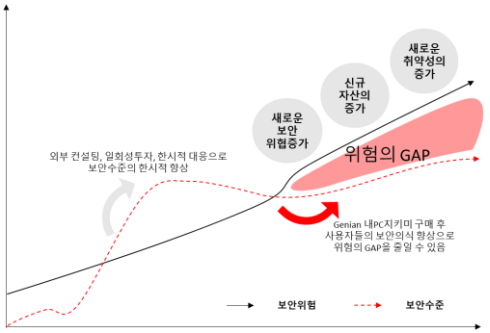
보안에 대한 인식 제고와 실천 등 사용자의 참여를 유도하여 보안 수준을 향상시키고 NAC 솔루션과의 연동을 통한 지속적인 관리와 개선으로 기업 내에 보안 문화를 조성합니다. 또한, 조직 별 보안 전략을 바탕으로 실제 위협 요소를 도출하여 효과적인 보안 관리를 수행합니다





- **보안 위험성 감소**

일회성 보안 수준을 향상시키는 것이 아닌 지속적인 관리를 통해 시간이 지날 수록 낮아질 수 있는 보안 위험성을 줄일 수 있습니다.



- **지속적인 보안 수준 관리를 통한 대규모 보안사고 예방**

사이버 공격의 1차 목표가 되기 쉬운 내부 PC 및 노트북 사용자의 보안수준에 대한 능동적이고 지속적인 보고/조치를 통해 기업의 보안 의식과 수준을 향상시켜 APT, 개인정보유출사고 등 대규모 보안사고를 예방할 수 있습니다.

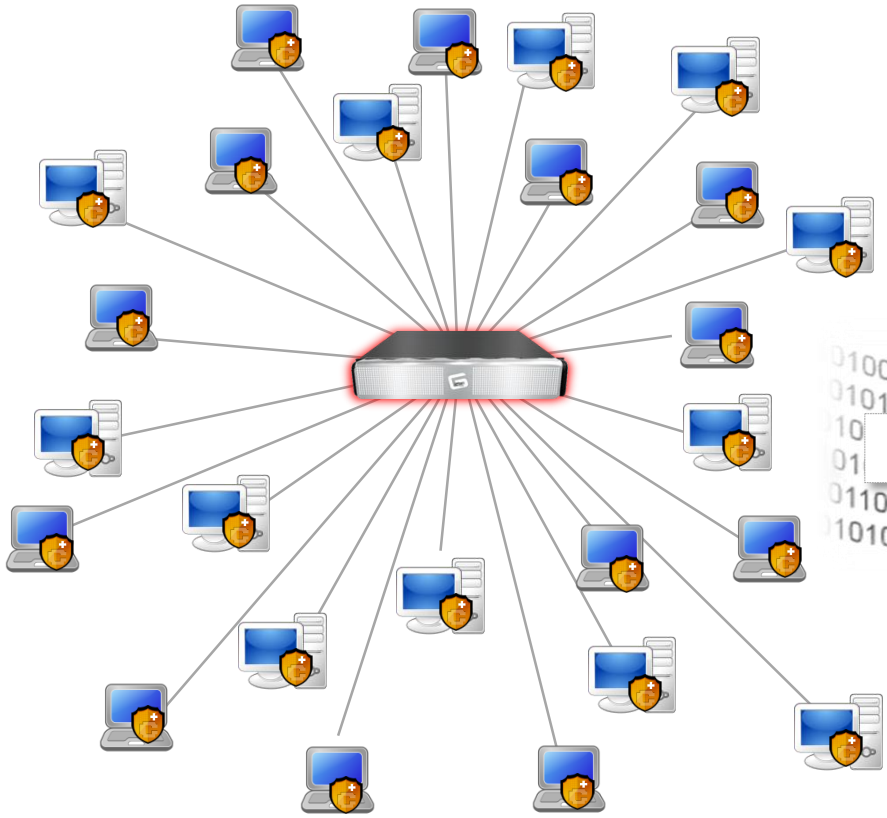
Genian GPI - 특징 및 장점 (지원 규제 정책)

다양한 보안 정책 지원

보안 정책	관련법규 및 규정	대상기관	점검항목 수
사이버보안진단의날	• 국가정보원 국가정보보안 기본지침 • 행정안전부 정보통신보안업무규정	• 국가 공공기관, 공사	• 16개 점검항목
정보통신기반시설 취약점진단(단말)	• 미래창조과학부 정보통신기반 보호법	• 정보통신기반시설 보유 기관	• 20개 점검항목
특정금융거래정보 보안점검	• 금융위원회 공문 (2013.08.13) • 특정금융거래정보(STR, CRT) 보안기준	• 금융위원회 산하 금융기관	• 13개 점검항목
지불카드산업 데이터 보안표준 (PCI-DSS)	• 지불카드정보보안표준위원회 정보보안 표준규격 (PCI 3.0)	• 카드사, VAN, PG사	• 9개 점검항목

Genian GPI - 특징 및 장점 (중앙집중 관리방식)

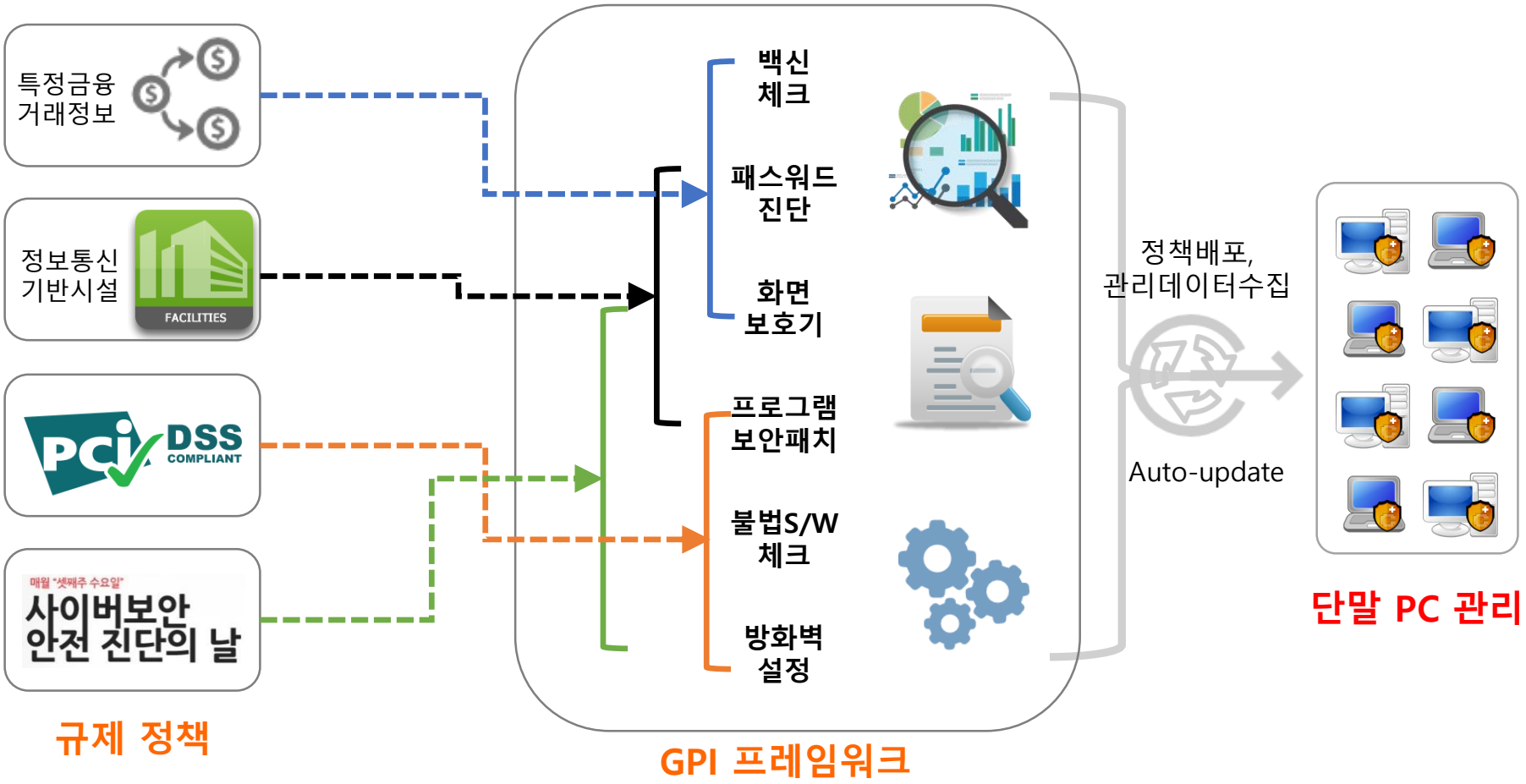
- 중앙집중 방식을 통한 지속적인 관리 및 수준을 개선하고 조치활동이 용이 하도록 구성
- 제한된 비용 및 시간으로 전사적/전수검사 가능 형태 (인력,비용,시간에 자유로움)
- 새로운 점검 및 관리 항목에 대한 손쉬운 확장이 용이



단말 상황 Data

Genian GPI - 특징 및 장점 (정책적용의 유연성)

- 새로운 Compliance 항목 및 단말체크/관리 항목에 유연하게 대처 할 수 있는 프레임워크 구성
- 추가되어진 관리항목을 관리자의 설정으로 단말사용자 개입 없이 정책적용 후 단말체크



Genian GPI - 기능

평가

- 보안규제 정책 지원
  → 사이버보안 진단의 날 등 4개 규제정책 지원
- 4개 규제정책 외 다수의 점검 항목 지원
- 관리자 정의 규제 항목 생성 지원
  → 파일, 프로세스, 레지스트리, Explorer 설정 점검
- 스케줄 설정 기능 지원
- 단말 사용자 보안 평가 및 설문조사 기능 지원

분석(보고)

- 개인별 평가 보고서 제공
- 부서별 평가 보고서 제공
- 대쉬보드 기능 지원
- 중간관리자 기능 지원
- 점검 결과 다운로드 기능 지원

제어(통제)

- 기준 점수 미달, 특정 항목 취약 시 점검 창 닫기 제한 및 주기적 팝업 기능 지원
- Genian NAC 연동 기능
  → 기준 점수 미달자에 대한 네트워크 차단
- 조직 보안포탈 연동 기능 지원

기타

- 점검항목별 도움말 제공 (AGENT)
- 취약 항목에 대한 바로 조치 기능 (AGENT)
- AGENT 자동 패치 기능
- 보안공지 기능
- 인사DB 연동

Genian GPI - 구성 및 역할

- 보안전용 OS를 탑재한 전용센터 장비 (H/W와 S/W 일체형 장비)
- 단말 내 설치를 위한 Non-Driver Based Agent
- Genian NAC와 동시 사용 시 Agent 통합 및 연동 기능 제공

관리자 콘솔

WEB 기반
멀티 브라우저 지원

정책관리 ⟷ 통계,보고서

정책 서버

Management Server	Node Server
DBMS (MySQL)	
TLS, SSLv2	
GNOS (전용OS)	

보안정책 ⟷ 점검결과

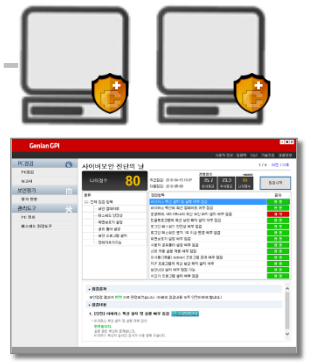
AGENT

Non-Driver Base Agent
Plug-in 기반

적용 단말

- 보안정책 수립
- 보고서 확인

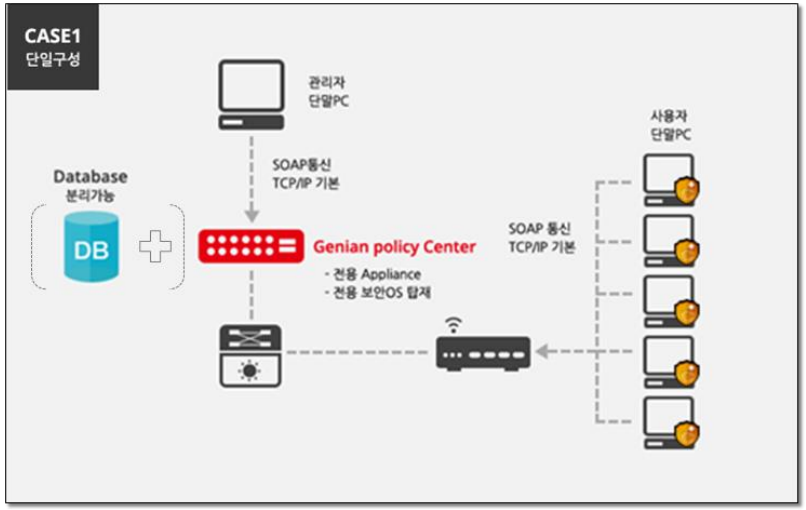
- 노드 관리
- 사용자 정보 저장
- 단말 정보 저장
- 점검결과 저장
- 보고서 생성
- DB 내장



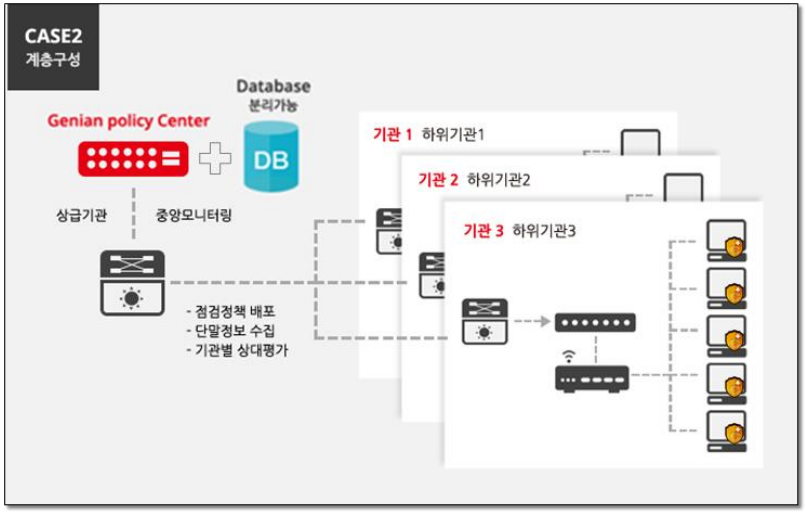
- 보안정책 점검
- 점검결과 전송

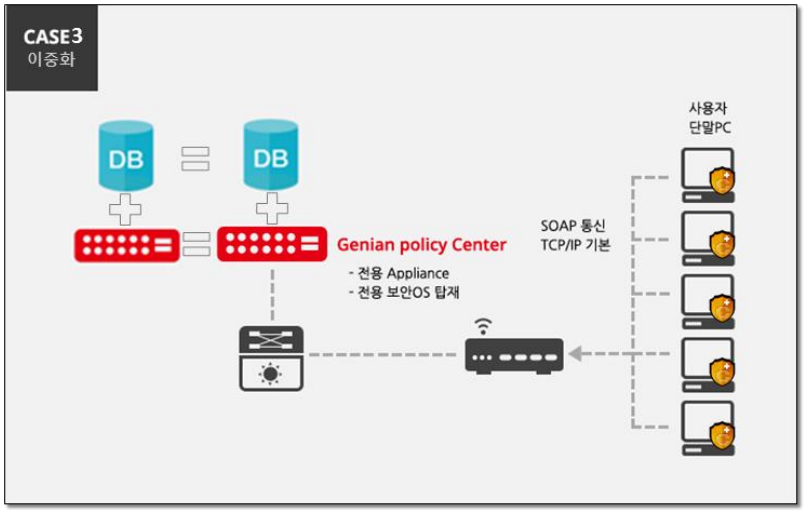
Genian GPI - 구성 방안

- **단일 센터 구성 및 계층적 구성 방법 등 다양한 조건에 알맞도록 구성 가능**



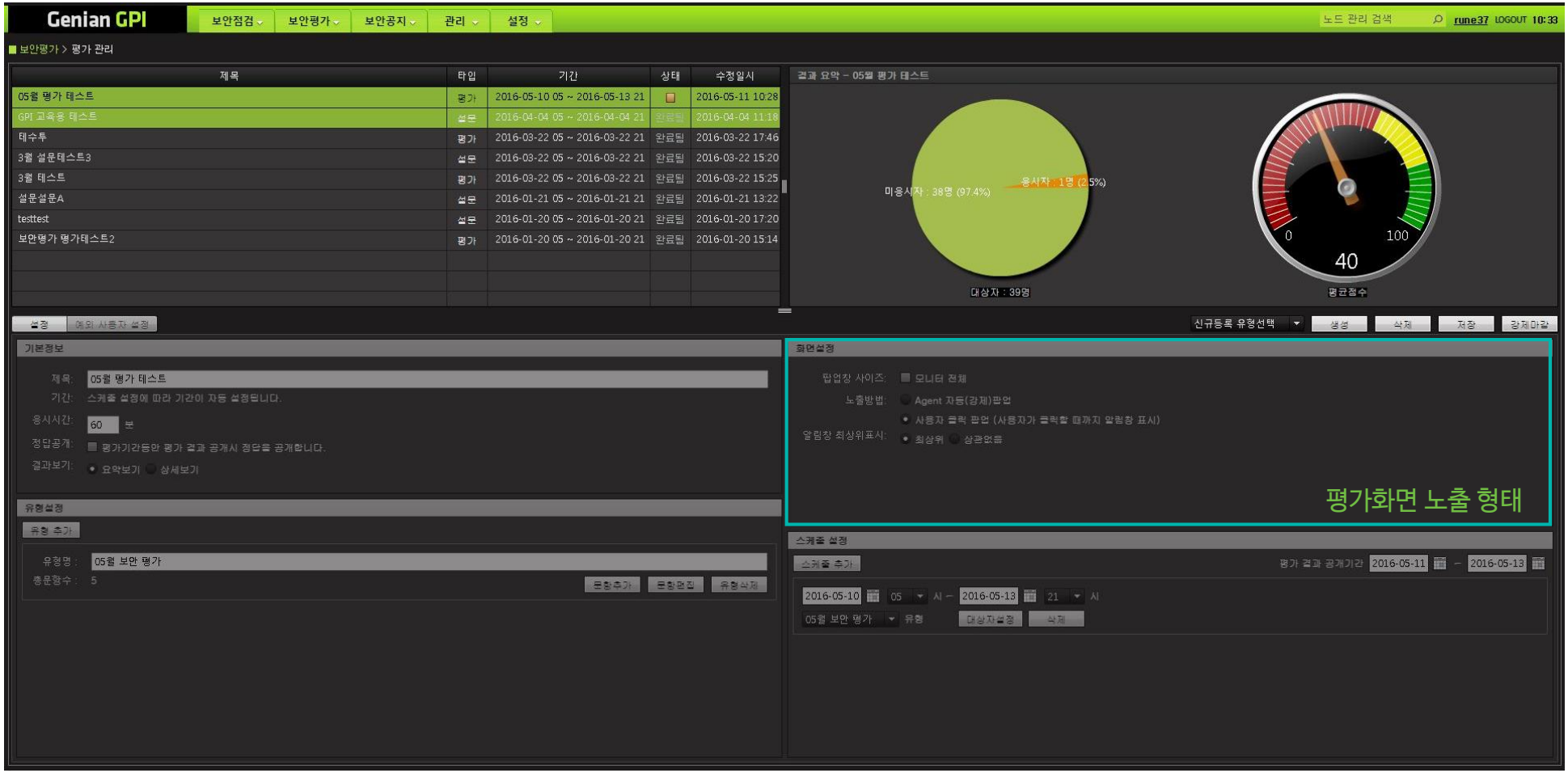
- 정책서버(Genian Policy Center)는 Agent 수량에 맞게 소형/중형/대형으로 구성
- 단일 구성 : 정책서버와 DB 일체형 구성 (일반적 구성이며 DB 분리 가능)
- 계층 구성 : 대규모일 경우 성능 향상을 위한 DB 분리 구성 권장
- 정책서버의 이중화 구성
- 정책 - DB 분리 이중화 구성





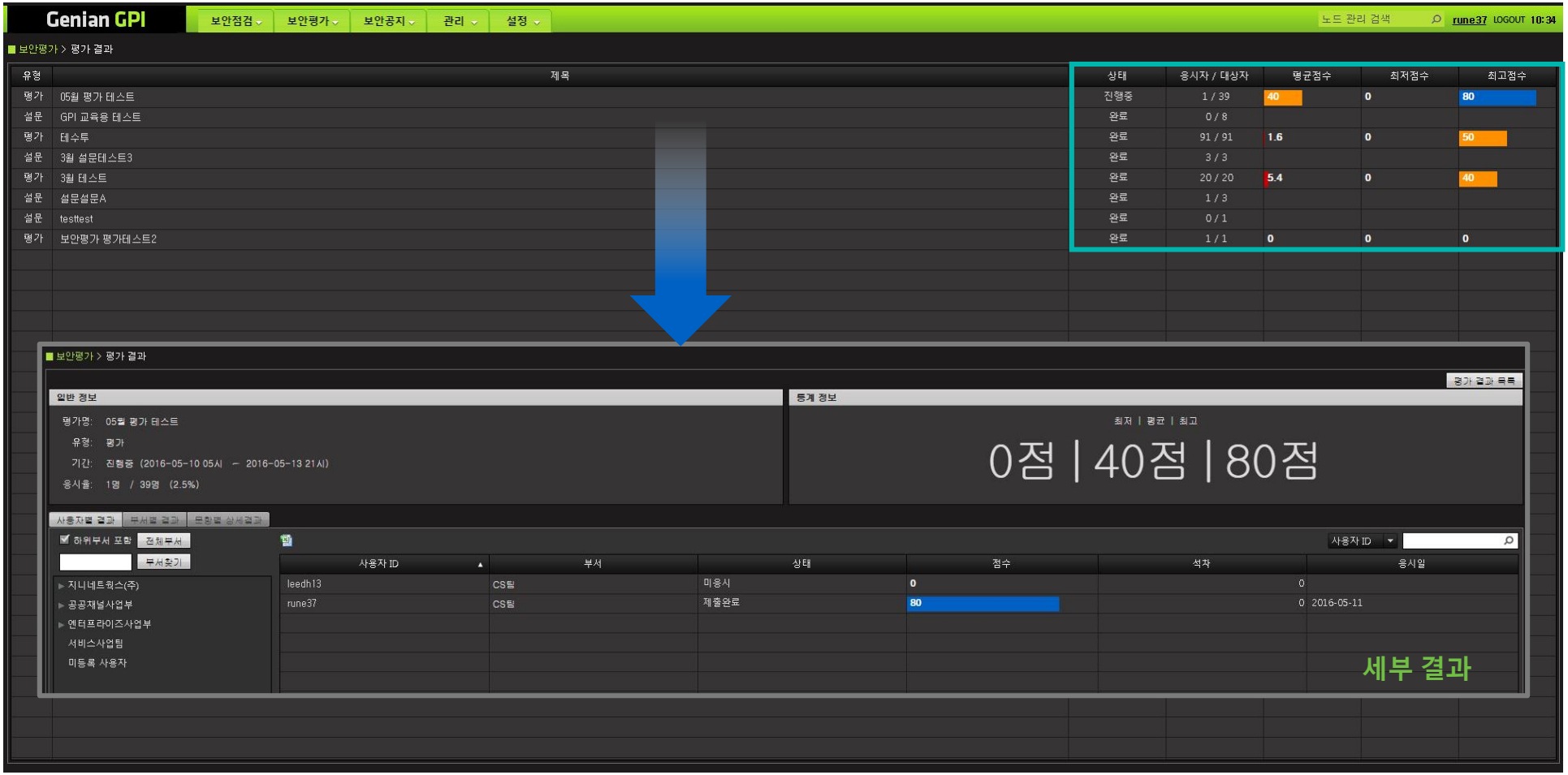
Genian GPI – 평가

- 사용자에 대한 보안 평가 대쉬보드



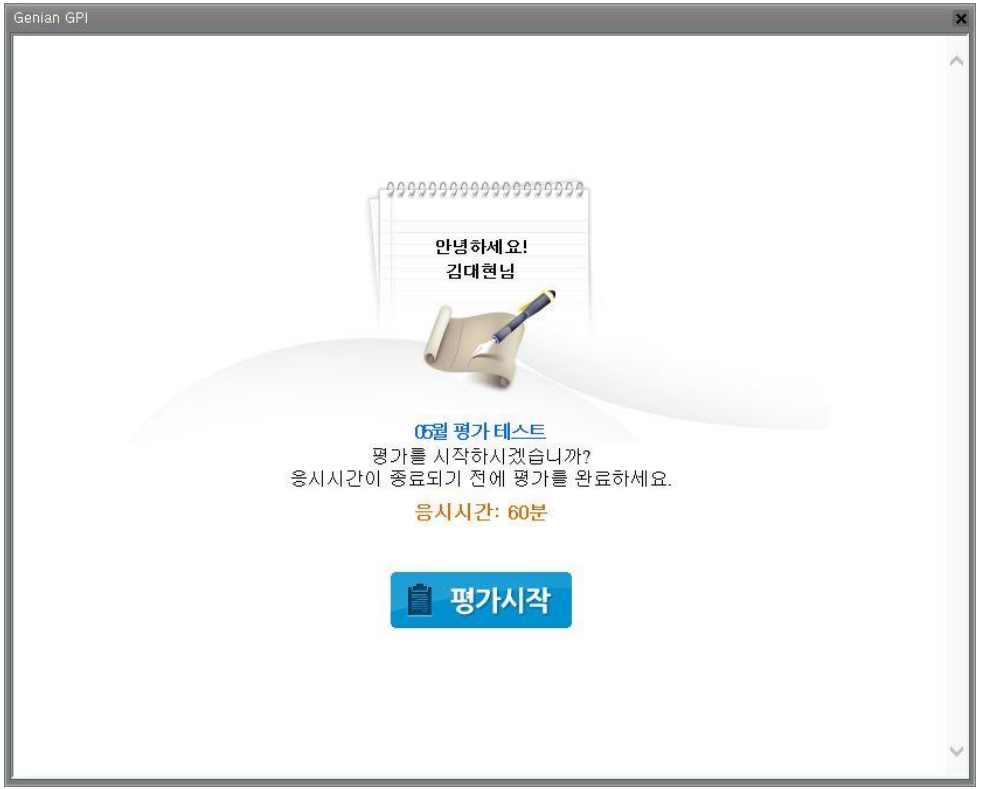
Genian GPI – 평가

- 사용자에 대한 보안 평가 대쉬보드

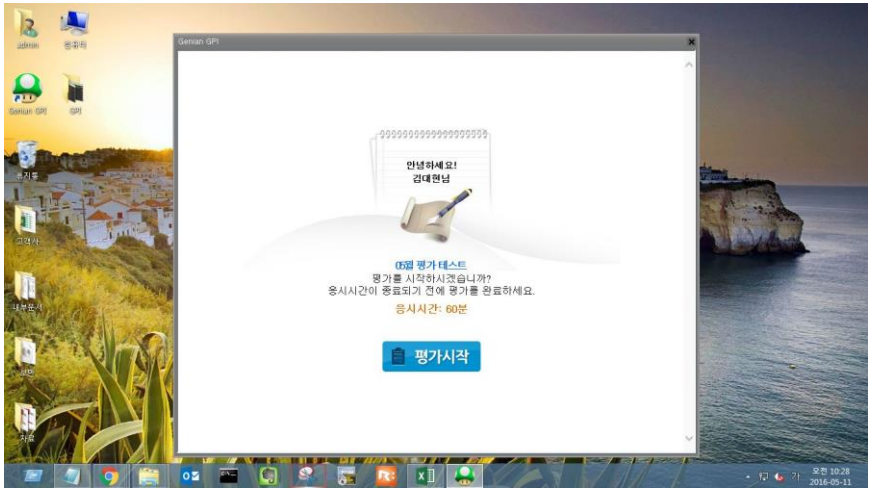


Genian GPI – 평가

- **사용자 평가 화면**



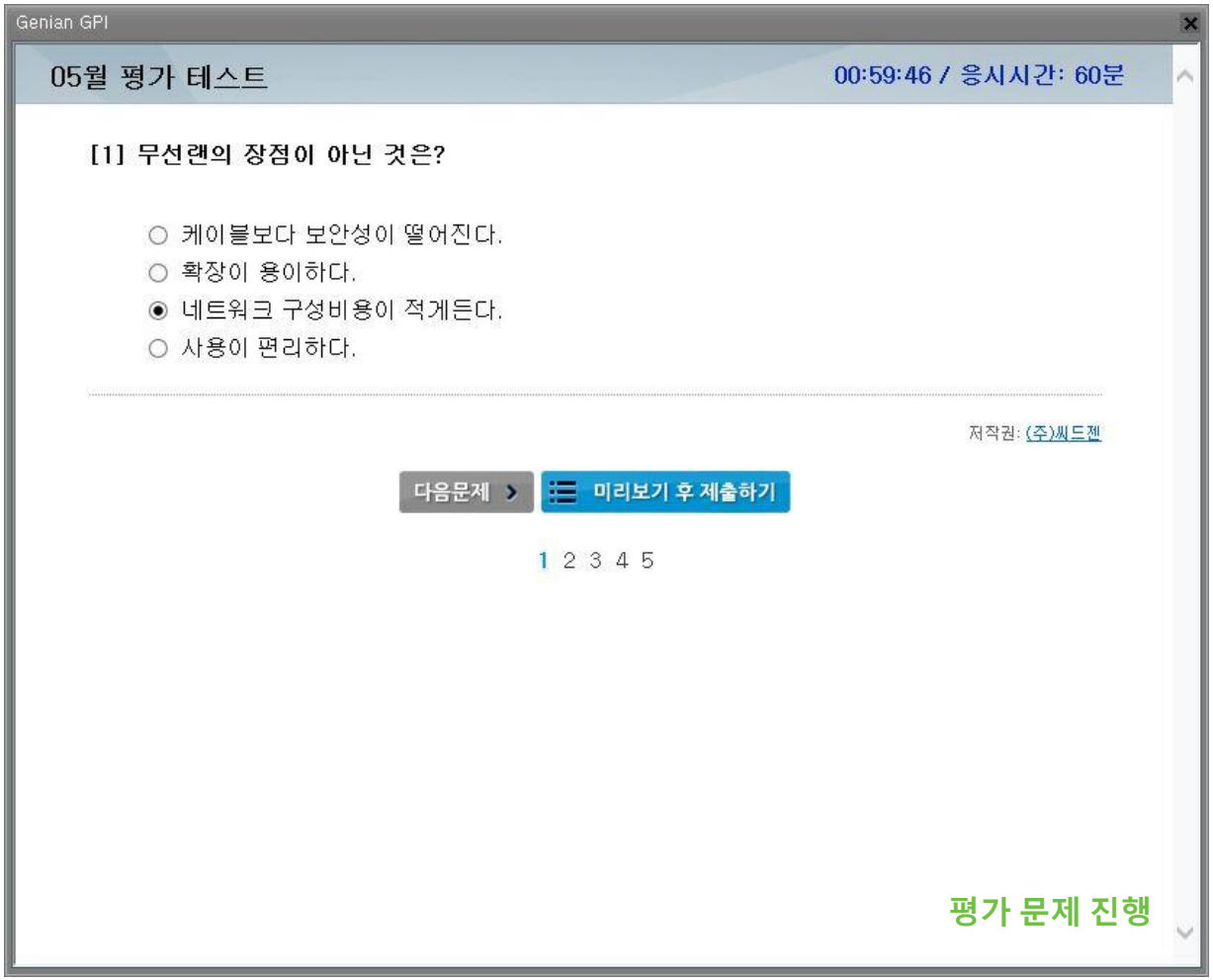
전체 화면



팝업 화면

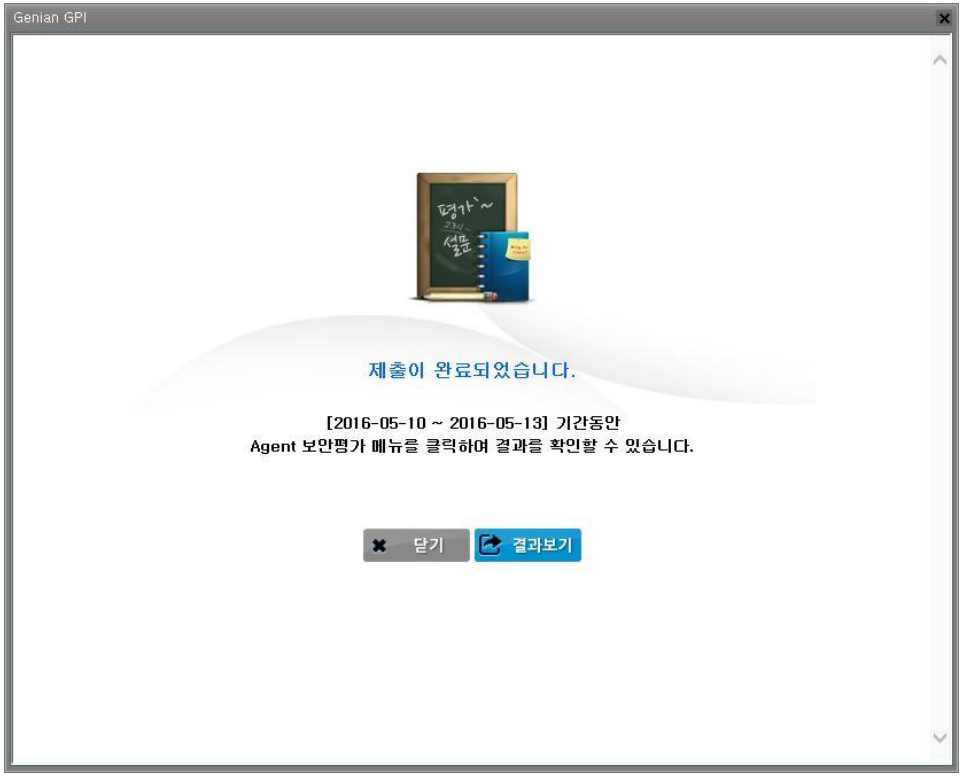
Genian GPI – 평가

- **사용자 평가 화면**



Genian GPI – 평가

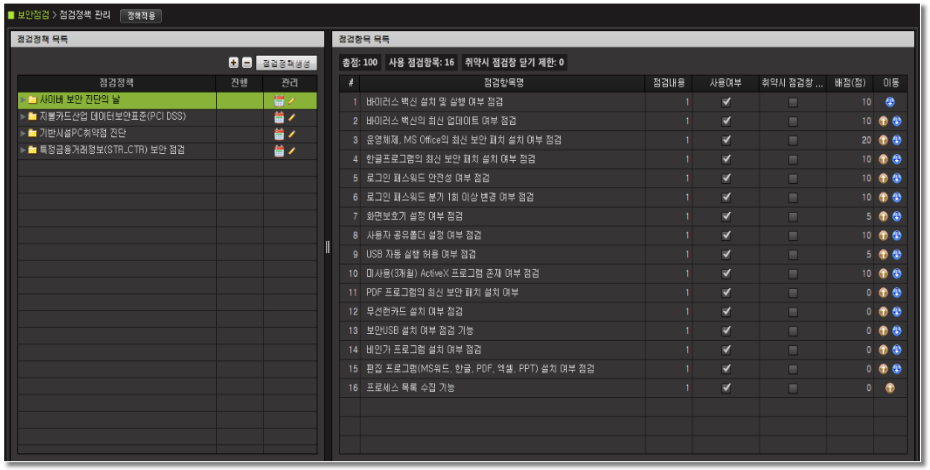
- **사용자 평가 화면**

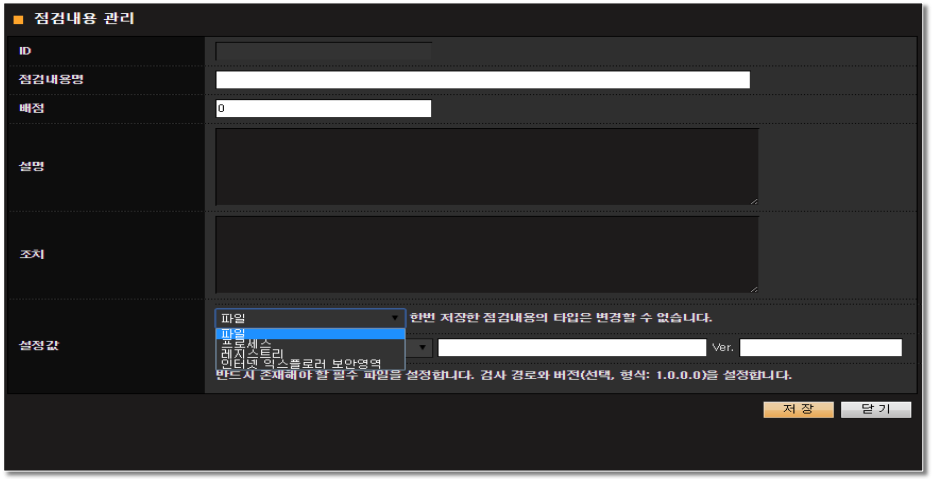


평가 완료 후, 제출 화면

Genian GPI – 평가

▪ 단말 보안 상태 점검

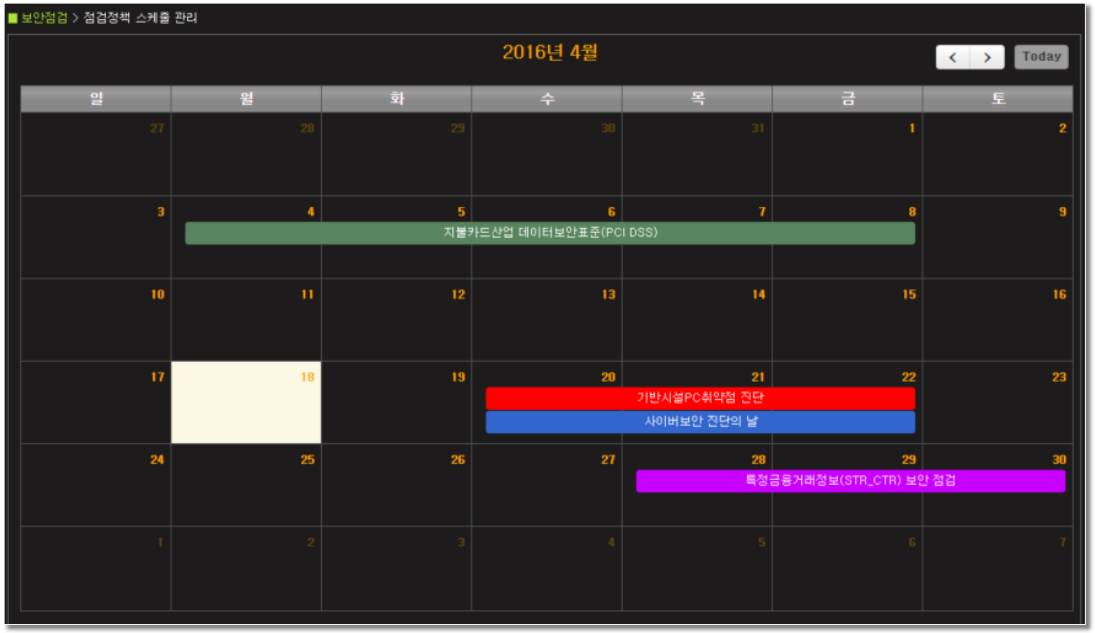




- 국정원 보안기준(사아버보안진단의 날) 16개 점검항목 지원
- 정보통신기반시설 20개 점검항목 지원
- 특정금융거래정보 13개 점검항목 지원
- PCI-DSS 9개 점검항목 지원
- 4개 점검정책의 점검항목 외에 추가 점검 항목 제공
- 관리자 추가 점검항목 생성 기능 제공
- 점검 정책(항목) 생성 기능 제공
- 고객사 별도의 보안 점검 기준 적용 가능
- 정책 수립 후 정책을 자동으로 배포하는 기능 제공

Genian GPI – 평가

▪ 보안점검 스케줄 설정

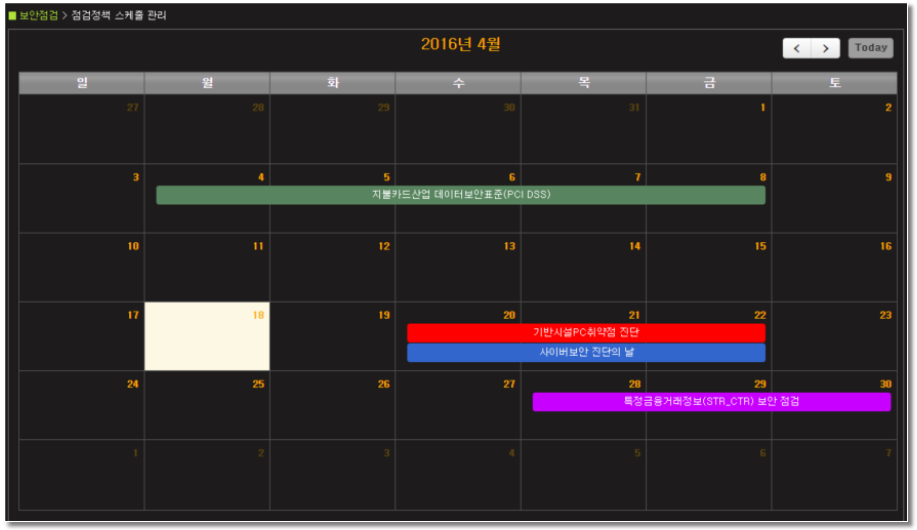


- 각각의 보안점검 스케줄 설정 기능
  - 월별, 주별, 일별 반복 스케줄 기능 지원
  - 일회성 점검 스케줄 기능 지원
- 점검스케줄 즉시실행 및 중단 기능 제공
- 달력 형태의 점검 스케줄 표시 기능 제공

- 각각의 보안점검 스케줄 설정 기능으로 인한 부하 분산

Genian GPI – 평가

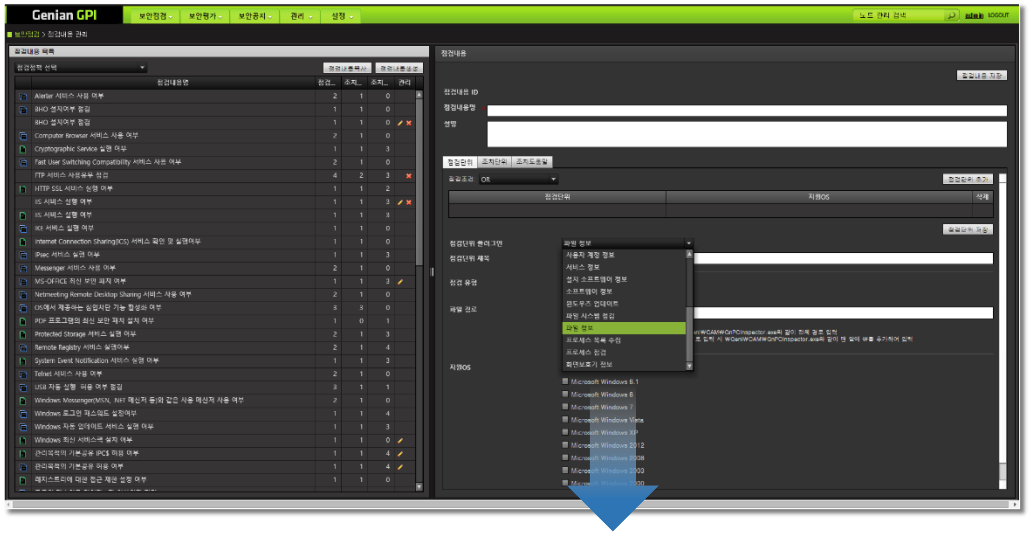
▪ 점검대상자 차등스케줄 설정

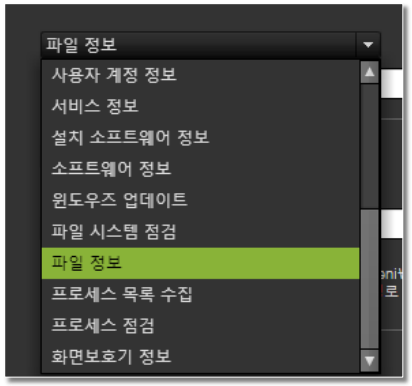


- 하나의 보안정책 내에서 점검 대상자 별로 차등 점검 스케줄 점검 기능 지원
  - 사이버보안점검의 날 자동점검 스케줄이 3일일 경우
  - A지역본부는 첫째날 자동점검 실행
  - B지역본부는 둘째날 자동점검 실행
  - C지역본부는 셋째날 자동점검 실행
- 각각의 보안 점검 스케줄 + 대상자 별 점검 스케줄
- GPI 서버 부한 분산 효과
- 보안업데이트, 한글, PDF 업데이트 트래픽에 대한 부하 분산 효과

Genian GPI – 평가

▪ 관리자 추가 점검내용 생성

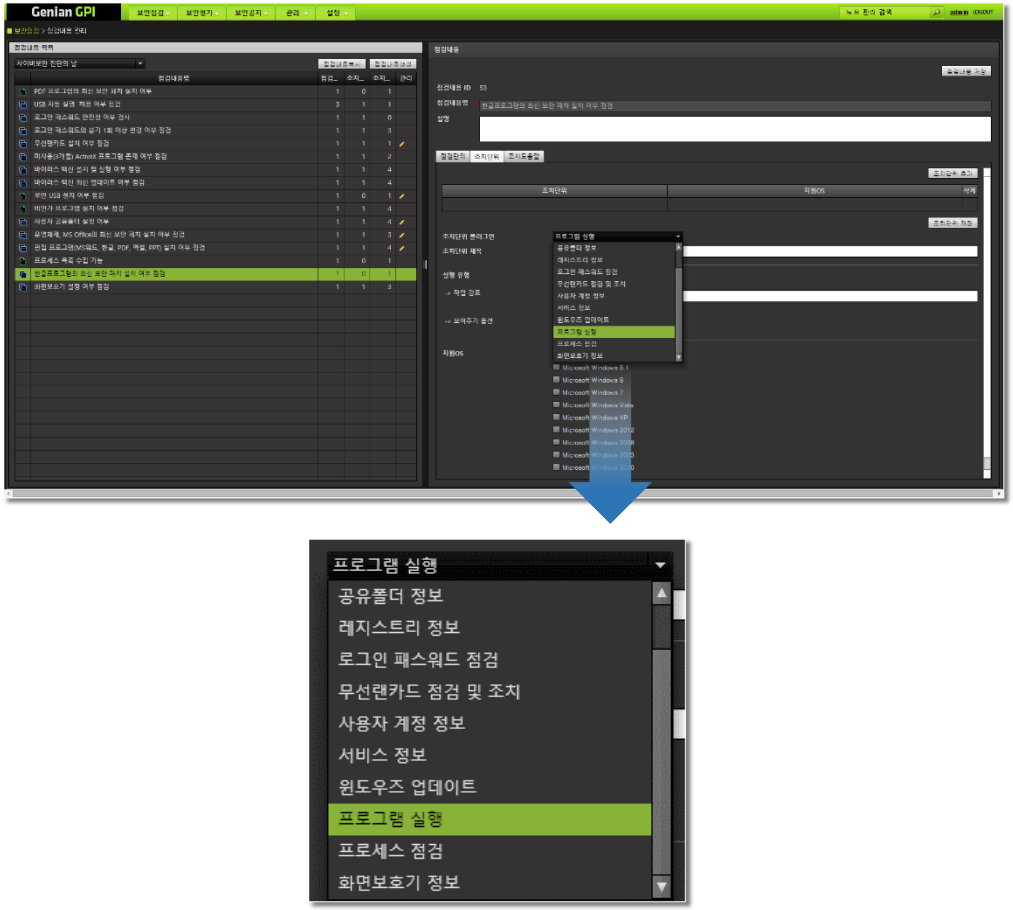




- 관리자가 조직 환경에 적합하게 점검내용 추가 생성 기능 제공
- 18개 PLUG-IN을 이용하여 점검내용 수정 및 생성 가능
  - IE 보안설정
  - IE 추가 기능 정보 (ActiveX 점검)
  - WMI 정보 점검
  - 공유폴더 정보
  - 레지스트리 정보
  - 로그인 패스워드 점검
  - 무선랜카드 점검 및 조치
  - 바이러스 백신 정보
  - 사용자 계정 정보
  - 서비스 정보
  - 설치 소프트웨어 정보
  - 원도우즈 업데이트
  - 파일시스템 점검
  - 파일정보
  - 프로세스 목록 수집
  - 프로세스 점검
  - 화면보호기 정보 등

Genian GPI – 평가

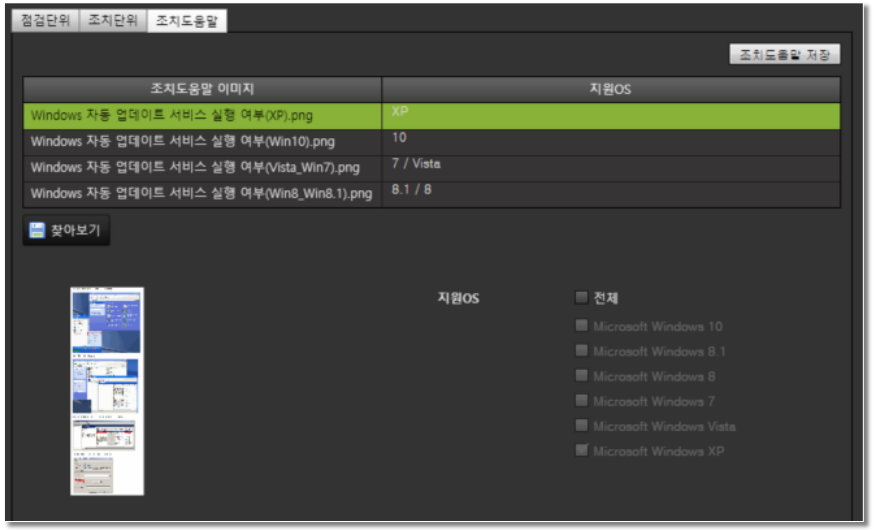
- **점검내용별 조치방법 수정 기능**



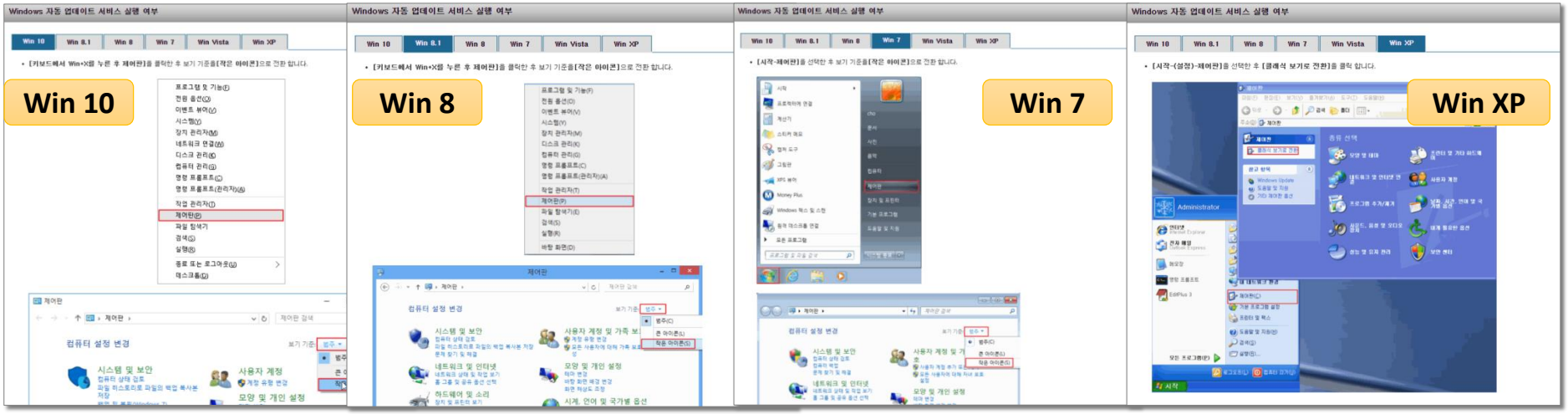
- 점검내용이 취약일 경우 Agent의 바로조치 버튼 선택 시 조치방법에 대한 수정 기능 제공
- 12개 PLUG-IN을 이용하여 조치방법 수정 및 생성 가능
  - IE 보안설정
  - IE 추가 기능 정보 (ActiveX 점검
  - 공유폴더 정보
  - 레지스트리 정보
  - 로그인 패스워드 점검
  - 무선랜카드 점검 및 조치
  - 사용자 계정 정보
  - 서비스 정보
  - 원도우즈 업데이트
  - 프로그램 실행
  - 프로세스 점검
  - 화면보호기 정보
- 바로 조치 클릭 시 특정 프로그램 실행 또는 특정 웹페이지 출력 등의 조치 방법 적용 가능

Genian GPI – 평가

- **조치도움말 수정 기능**



- 동일한 점검항목이라도 조치도움말을 OS별로 다르게 표시 가능
- 기본으로 제공되는 조치도움말이 회사 환경과 맞지 않을 경우 조치도움말 변경 기능 제공
- 원도우 업데이트, 한글프로그램, PDF 업데이트의 경우 MS 업데이트 사이트, 한컴, 어도비 홈페이지가 아닌 회사 내부에 있는 PMS에서 패치 파일을 다운로드 할 수 있게 조치 도움말 수정 가능



Genian GPI – 평가

▪ 점검항목 OS별 차등 적용

- 동일 항목이라도 OS별 점검내용 다르게 점검 기능 제공

- 원도우 방화벽 활성화 여부 점검
- Window OS별로 점검해야 하는 내용이 다르기 때문에 OS별로 차등화된 점검내용 설정 기능 지원

- Internet Connection Sharing 서비스 확인 및 실행 여부
- Window OS별로 점검해야 하는 내용이 다르기 때문에 OS별로 차등화된 점검내용 설정 기능 지원

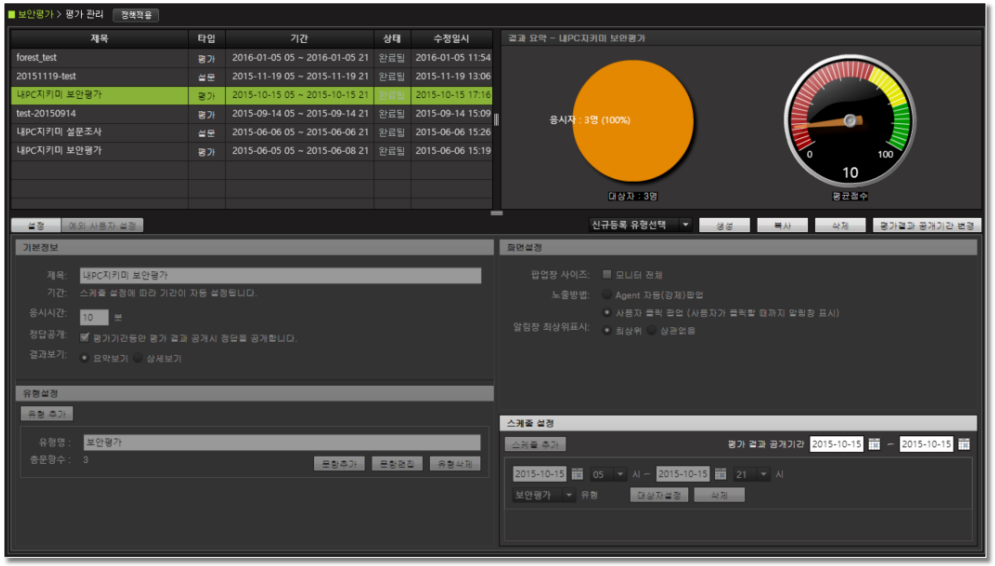
Genian GPI – 평가

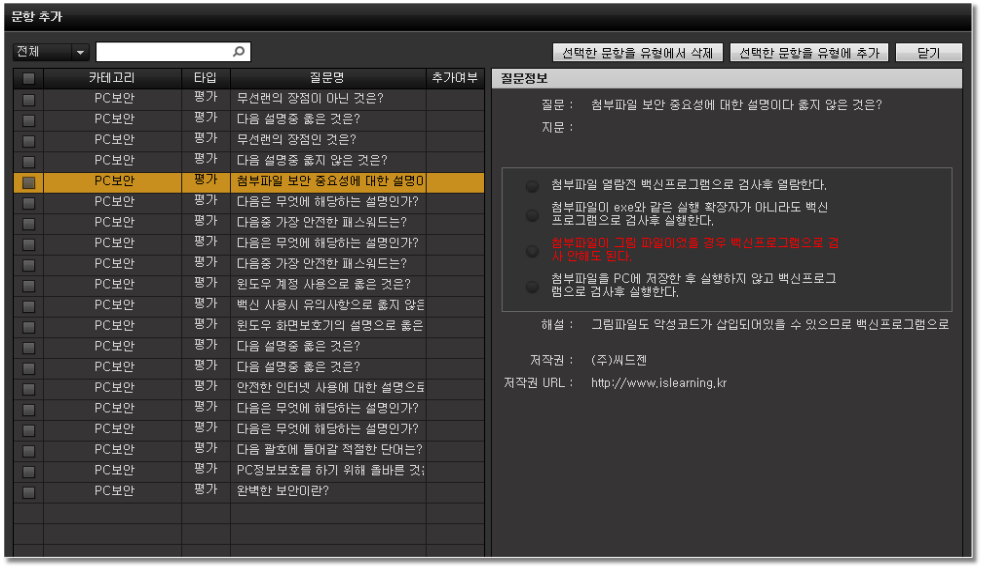
- **Foreground점검, Background 점검 선택가능**

- 고객사의 상황에 따른 다양한 점검방식 선택 기능 지원
- Foreground점검 (점검 팝업창 표시)
  - 점검 안내창 표시 여부 설정
  - 점검 진행상황 표시 여부 설정
- Background 점검 (Stealth Mode)

Genian GPI – 평가

- **단말 사용자의 보안수준 향상을 위한 평가도구**



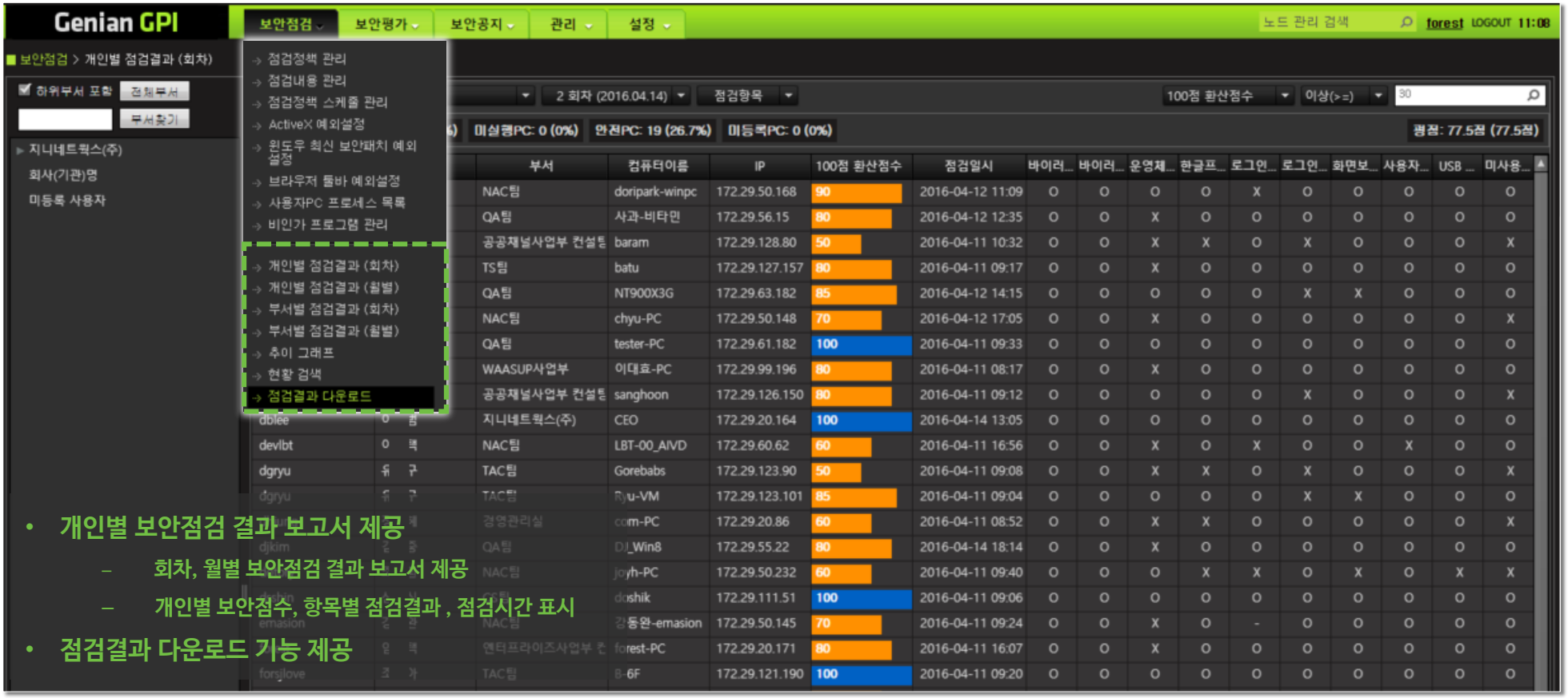


- 보안평가 및 보안설문조사 기능 제공
- 사용자 보안평가를 위한 평가기능 제공
  - 단말 사용자의 보안평가를 위한 스케줄 설정관리 기능
  - 단말 사용자의 보안평가 결과 조회
- 평가 결과 보고서 제공
  - 개인, 및 부서 결과 보고서 제공

- 기본 PC보안에 대한 20개 평가문제 제공
- 관리자에 의한 추가 보안평가 항목 생성 기능
- 4지선다 및 주관식항목 설정 기능

Genian GPI – 분석

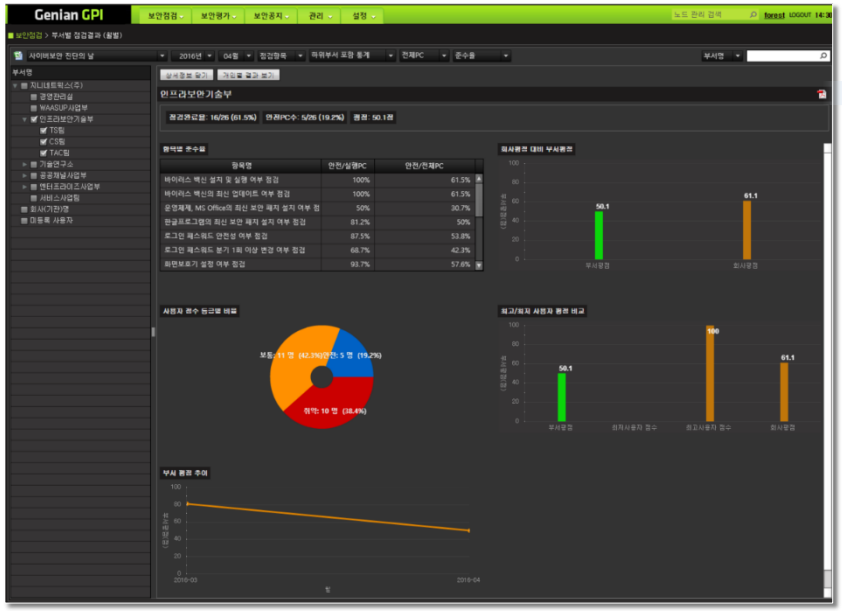
- 점검결과 분석을 위한 개인별 점검결과 보고서 제공



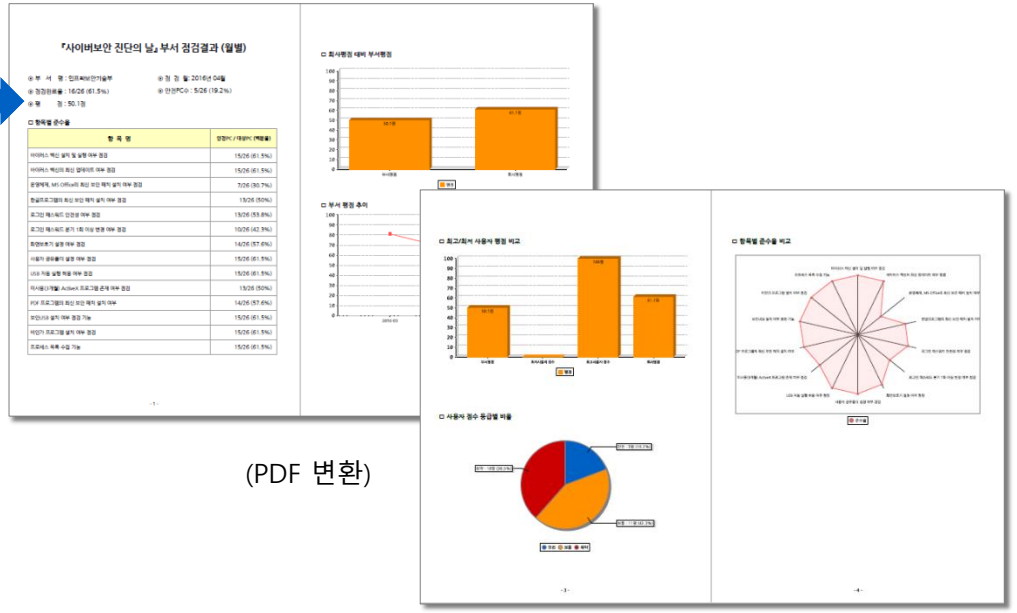
- 개인별 보안점검 결과 보고서 제공
  - 회차, 월별 보안점검 결과 보고서 제공
  - 개인별 보안점수, 항목별 점검결과 , 점검시간 표시
- 점검결과 다운로드 기능 제공

Genian GPI – 분석

- **점검결과 분석을 위한 개인별 점검결과 보고서 제공**



- **부서별 보안점검 결과 보고서 제공**
  - 회차, 월별 보안점검 결과 보고서 제공
  - 부서별 평균점수, 항목별 안전/취약 비율, 점검율 등 표시
  - 부서별 상세보고서 제공
- **점검결과 PDF 변환 및 다운로드 기능 제공**



(PDF 변환)

Genian GPI – 분석

- 보안점검 진행상황 분석을 위한 대쉬보드 제공

진행중인 보안정책
현황 자료 제공

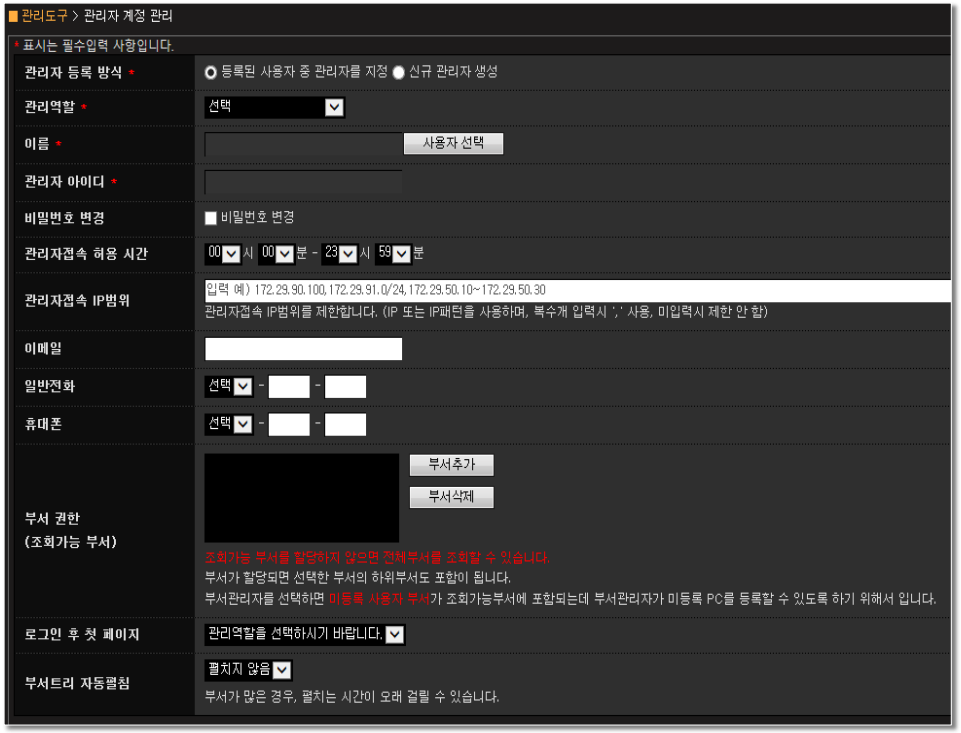
보안 정책 통계

보안정책 별
점검 진행 정보 제공

점검항목 별
점검결과 자료 제공

Genian GPI – 분석

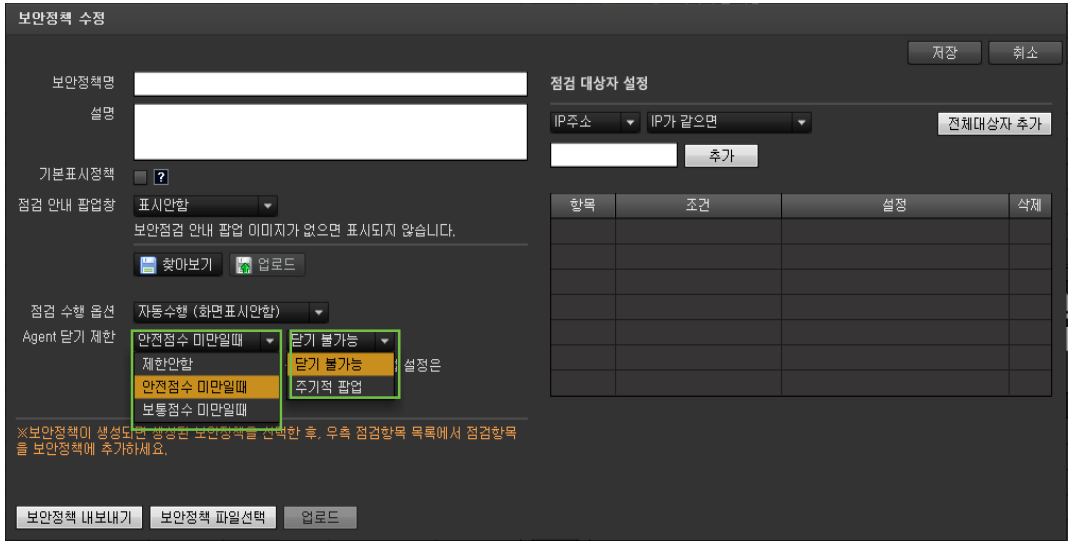
- **중간관리자 / 관리자 계정 상세정보 표시 및 검색 기능**

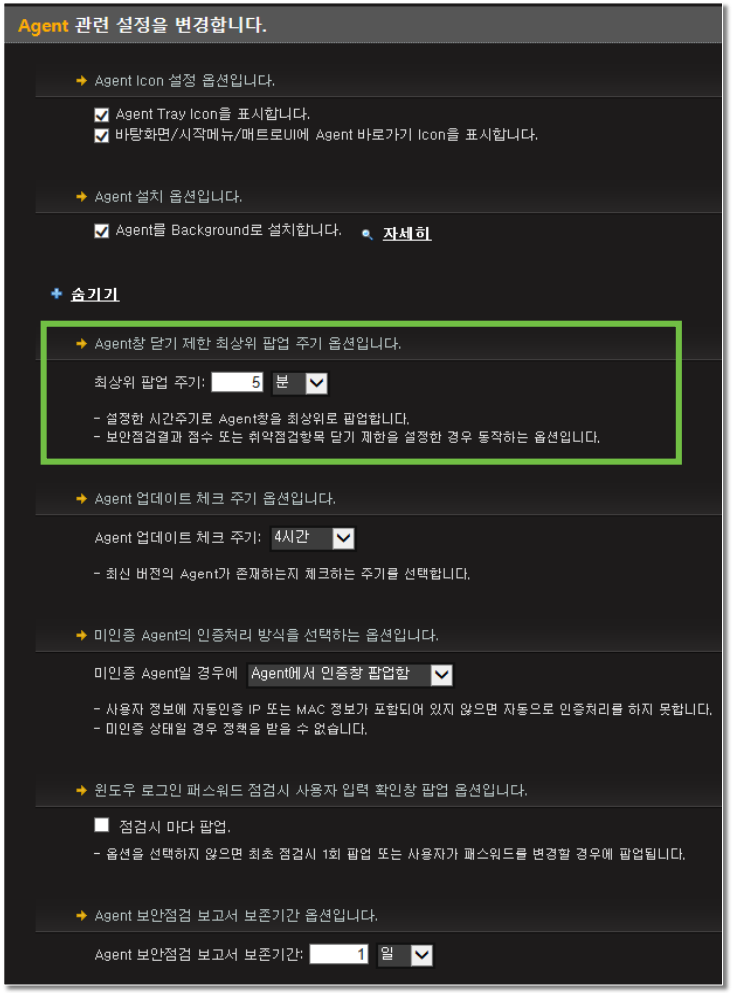


- 관리자 별 차등 권한 부여 기능
- 그룹(부서)별 중간관리자 설정 가능
- 관리자 계정상세정보 표시
- 관리자 이름/아이디/그룹으로 검색가능

Genian GPI – 제어

▪ 설정점수 미달 시 점검 창 닫기 제한 기능

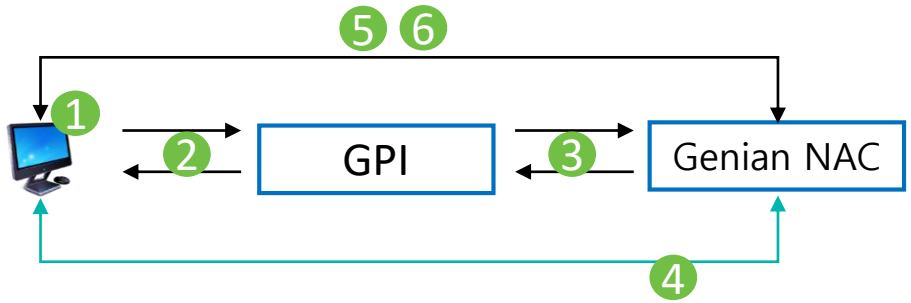




- 설정 점수 미달 시 Agent 점검 창 닫기 불가 및 최상위 팝업(주기 설정기능 제공)
- 취약점검항목에 따라 닫기 제한 설정기능 제공
- 관리자에 따른 선택적 제한 기능 제공

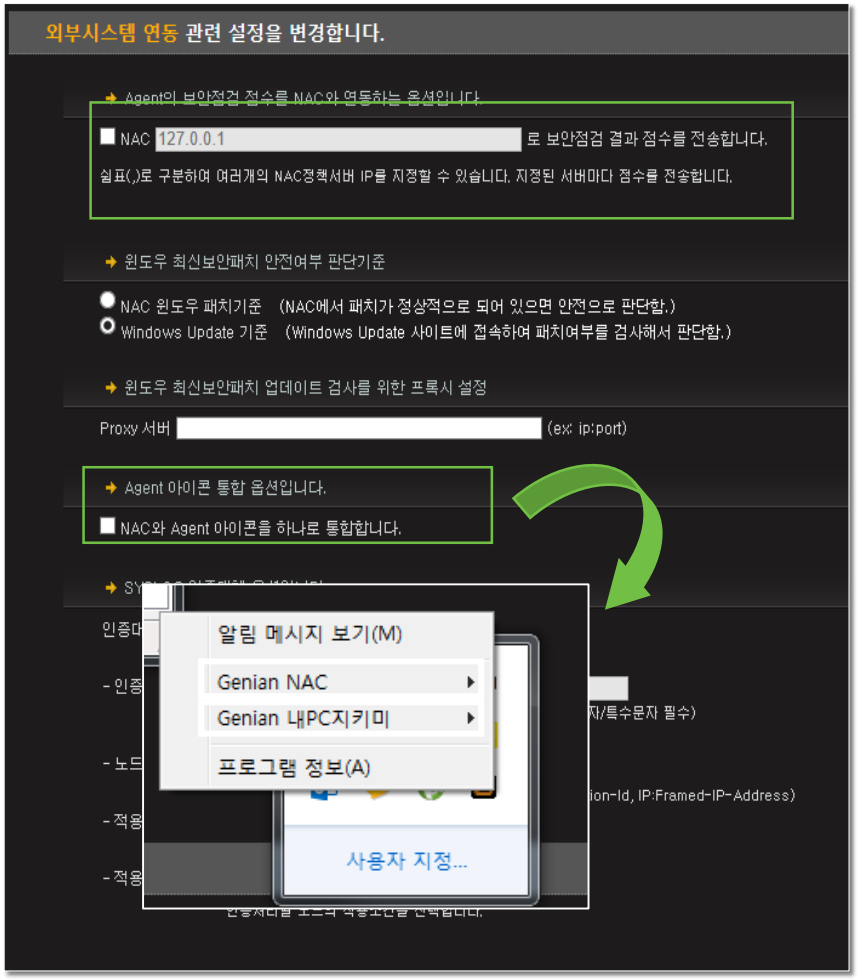
Genian GPI – 제어

▪ Genian NAC 연동 기능



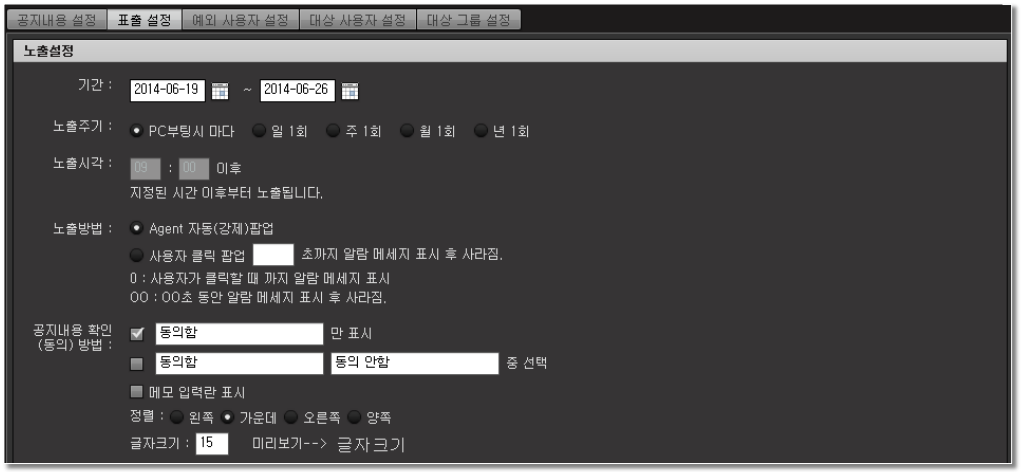
내부 보안진단 수준 (예시)		
등급	GPI(준수율)	NAC 적용 사항
A	90 ~ 100 점	네트워크 전체 허용
B	80 ~ 89 점	업무 허용, 인터넷 차단
C	70 ~ 79 점	업무 허용, 인터넷 차단
D	60 ~ 69 점	업무/인터넷 차단
E	59 점 이하	업무/인터넷 차단

1. GPI 점검수행
2. 점검수행결과 GPI서버 전송
3. 점검수행결과 NAC 전송
4. NAC정책에 따른 조치
   - ✓ 점수 이상 : 정상사용
   - ✓ 점수 이하 : 인터넷 차단 등의 접근제어 수행
5. 재점검을 통해 점수 상승
6. 실시간 NAC로 점수 전송 후 차단 해제



Genian GPI

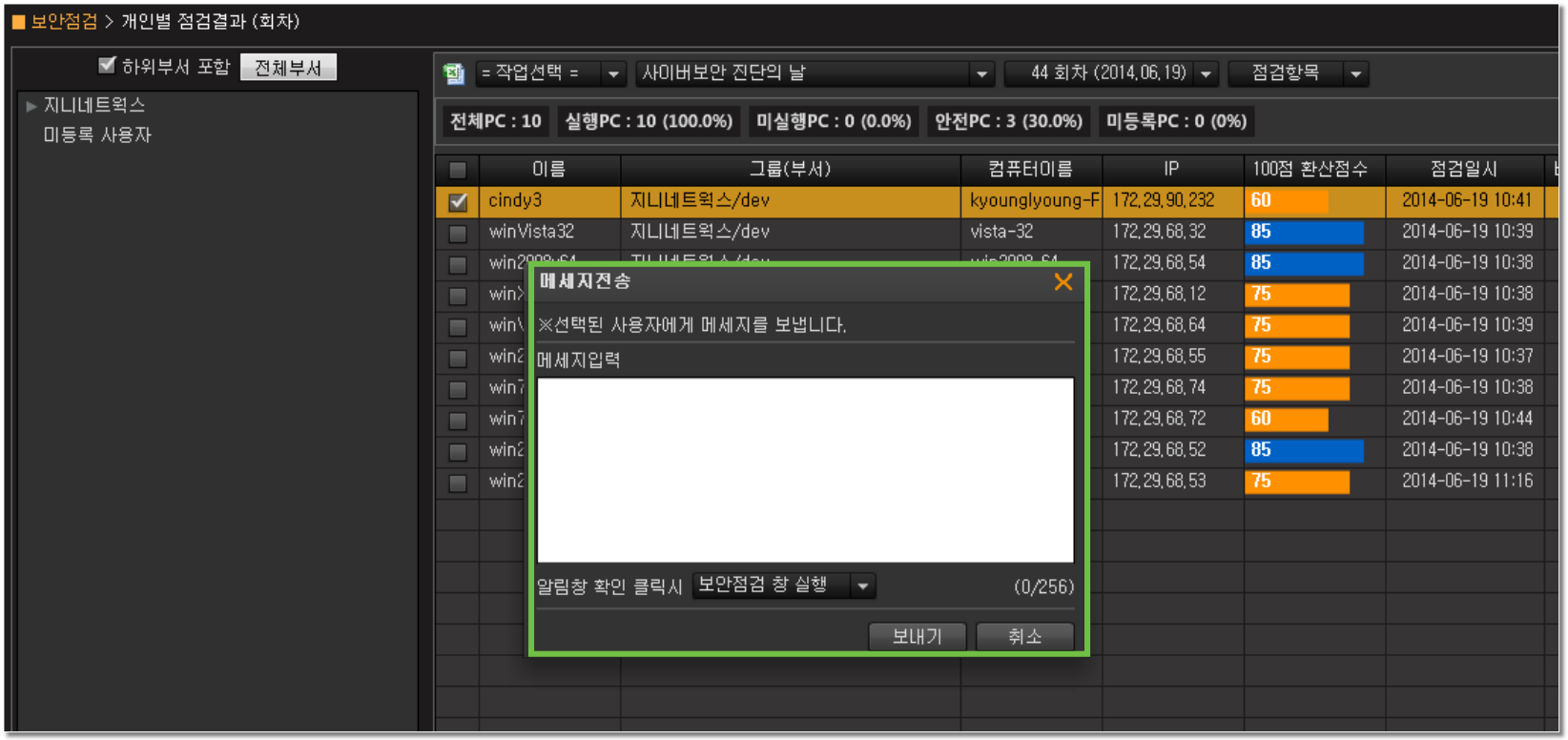
▪ 단말사용자들의 보안사항 알림 기능



- **보안공지기능**
- 화면 팝업 주기 설정 기능 제공
- 공지내용을 PC사용자가 인지하였는지 확인하는 방법 제공
- 팝업창 사이즈 및 모니터 위치 설정 기능 제공
- **사용동의 및 보안정책 전달 기능**
  - 의무사항 동의정보 조회(관리자)
  - 공지 및 동의 대상설정 및 예외 설정 기능

Genian GPI

▪ 메시지 전송 기능



- 미 점검자 및 기준점수 미달 자를 지정하여 메시지 전송 기능
- PC사용자가 알림 창 확인 후 보안점검 창 실행 가능

Genian GPI

▪ 관리자 웹 콘솔 접속 시, 로그인 2단계 인증 기능

✓ OTP 인증 지원 (Google OTP)

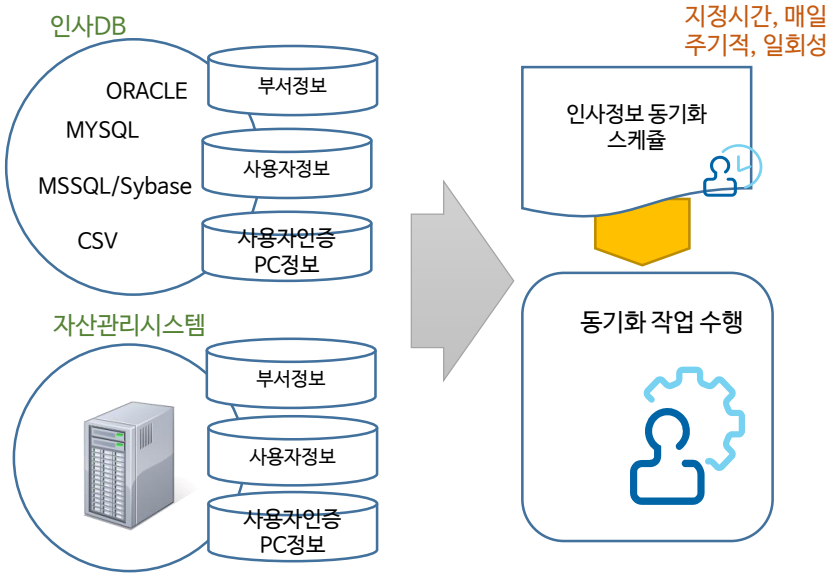
- 관리자는 스마트폰에 Google OTP를 설치
- (재)로그인 시 SECRET KEY를 발급 받은 후 OTP 코드 입력 후 로그인
- ID/PW 인증 + OTP 코드 인증 후 로그인 성공
- Time-Sync 방식

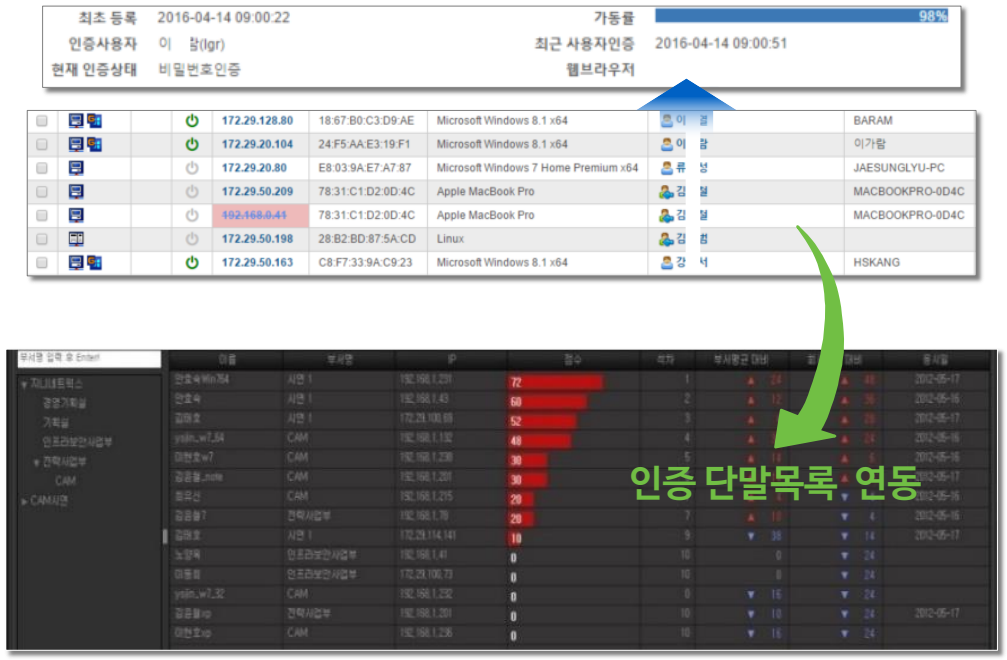
✓ SMS 인증 지원

- ID/PW + SMS 인증번호 입력 후 인증을 통한 로그인 기능
- SMS 서비스₩ 자체 제공 가능(월 500 건)
- 내부 SMS 서버와의 연동을 통한 기능 구현 가능

Genian GPI

▪ 고객사 인사DB연동 기능



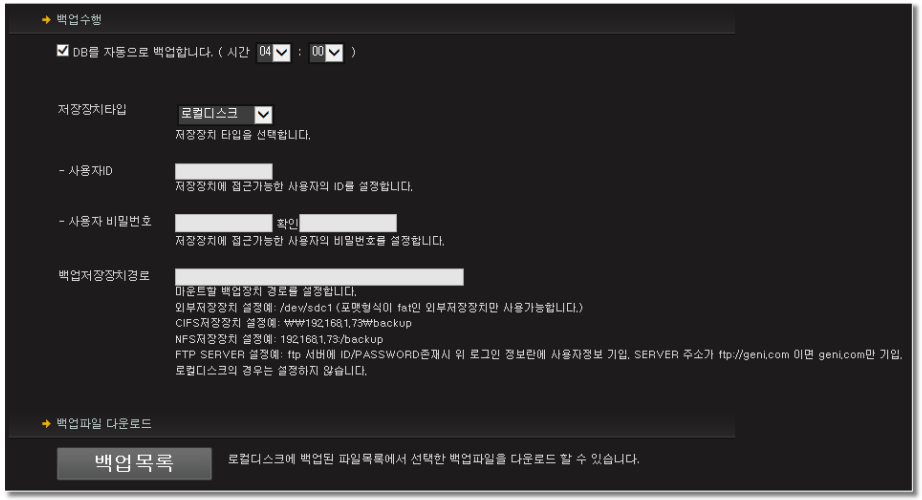


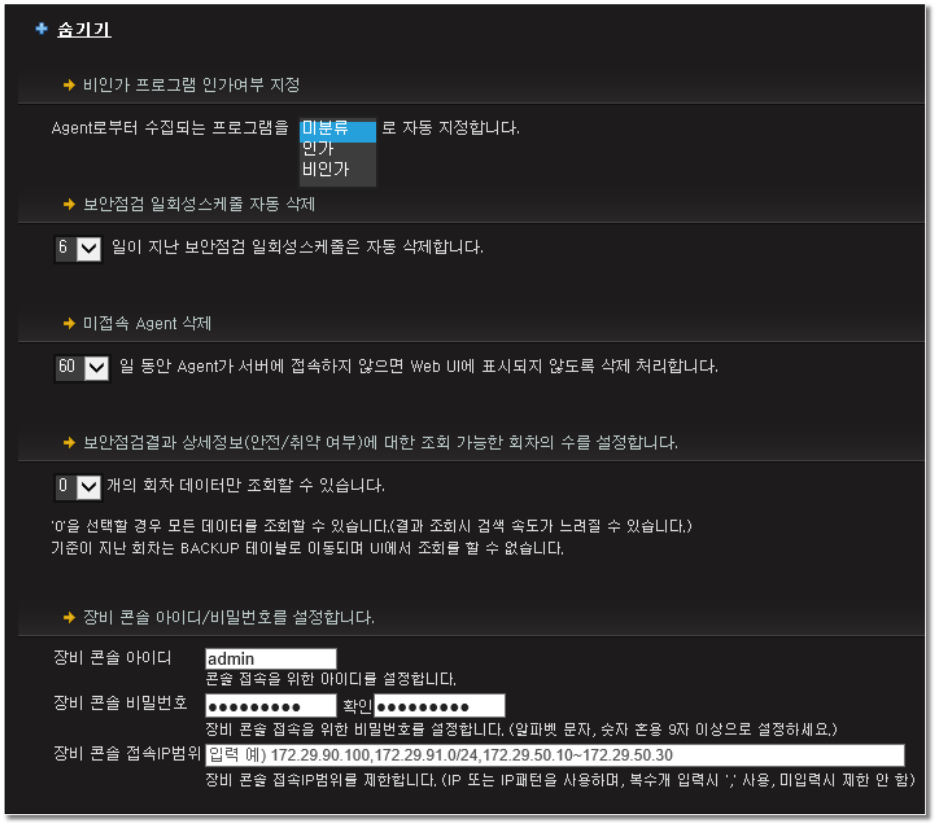
- SSO 인증 기능을 제공하여 단말사용자 업무 효율성을 증대

- 기존구축 된 인사DB시스템 및 자산관리시스템, 정보보안포털서버의 필요정보를 스케쥴에 따라 사용자인증 PC 정보와 동기화 작업 수행
- 사용자 ID 및 PC의 MAC 정보로 개인PC 인증처리, 자산관리시스템과 해당정보 연동

Genian GPI

▪ Genian GPI DB백업 기능

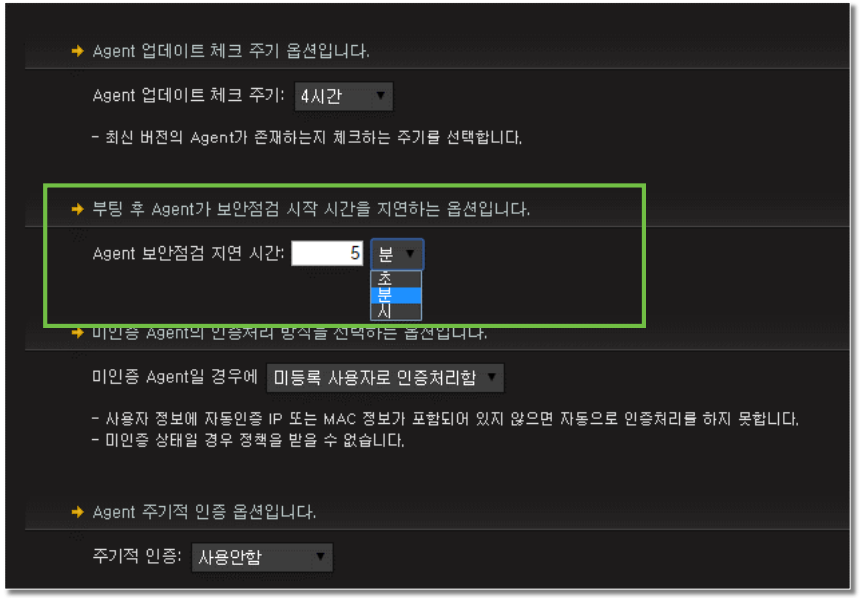




- 로컬디스크,외부저장장치, CIFS저장장치, NFS저장장치,FTP SERVER 등 다양한 저장장치 지원
- 백업시간 설정 가능

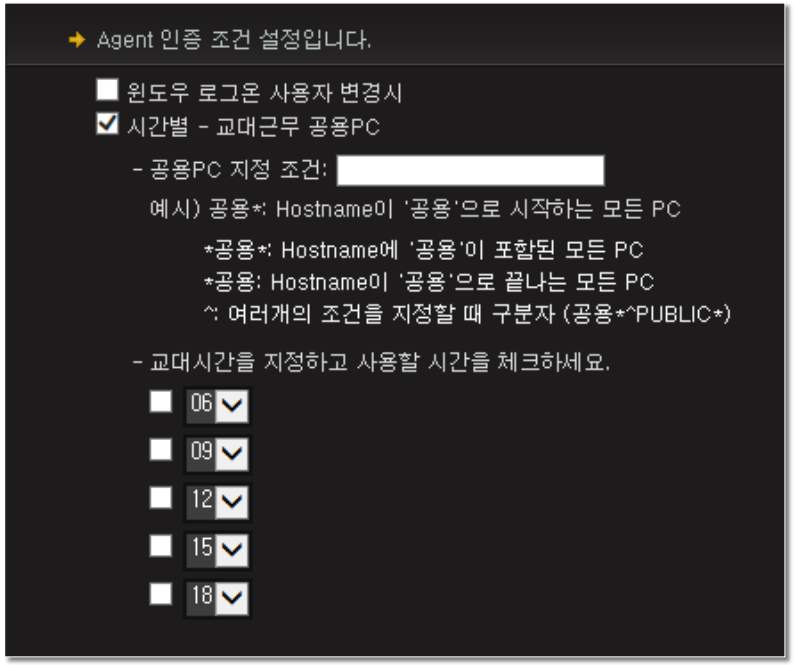
Genian GPI

▪ 부팅 후 보안점검 시작 지연 기능



- 지연 된 시간 후에 점검 시작
- 초/분/시 시간설정 지원
- 사용자 PC에 설정 된 업데이트 진행 후 점검 진행

▪ 교대근무/공용PC 점검기능 지원

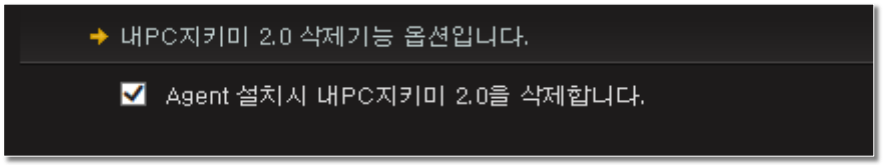


- 교대근무자 및 공용PC 점검기능 지원
- 특정시간(근무교대시간)에 따른 점검 지원

Genian GPI

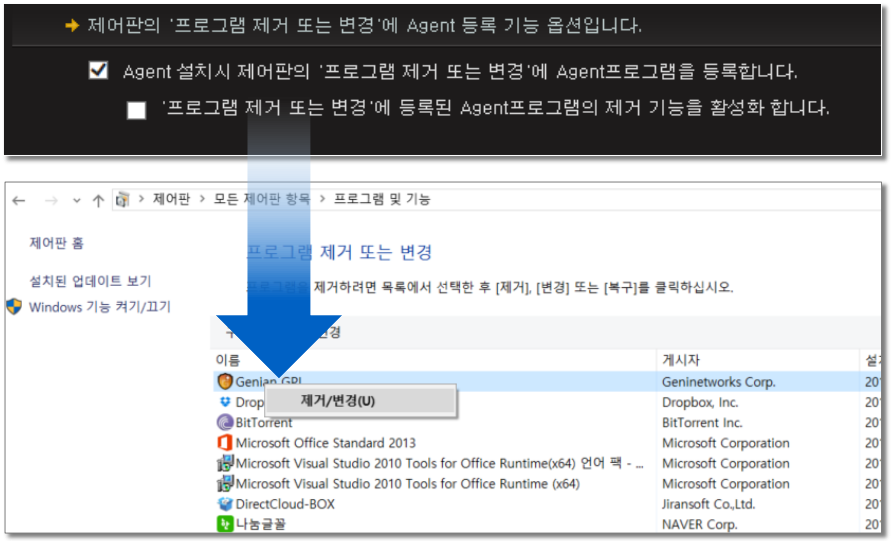
▪ GPI V2.0 자동 삭제 기능

- 기존에 설치된 GPI V2.0 자동삭제 기능을 통해 별도의 삭제 절차 없이 자동 삭제 할 수 있음



▪ Agent 임의 삭제 불가

- 관리자 설정에 의한 사용자 수동 프로그램 삭제 옵션 제공

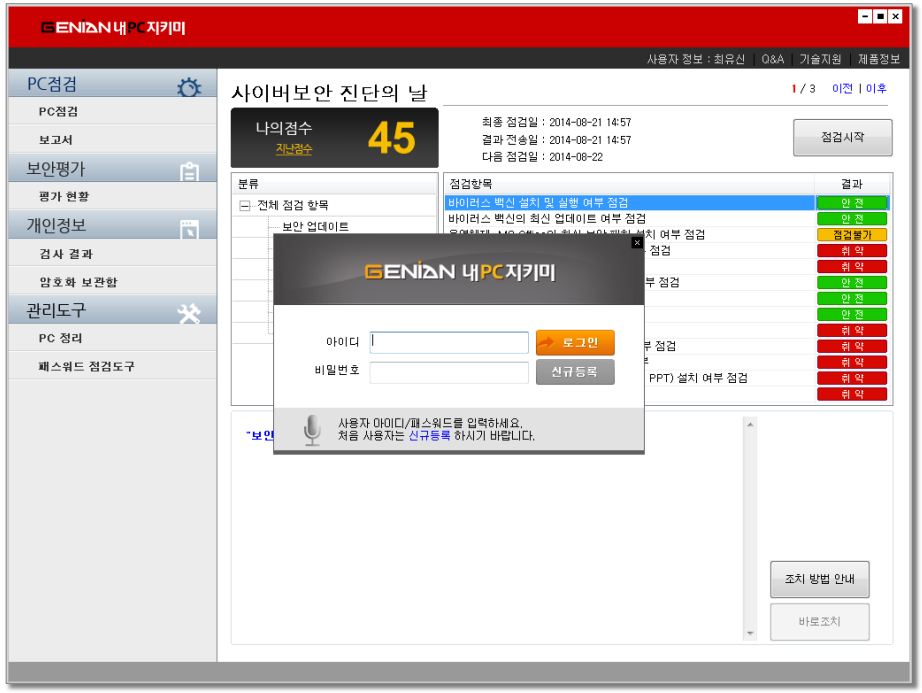


- 삭제 프로그램(클리너)을 통한 Agent 삭제

- 두 가지 삭제 방법 외 사용자 임의 삭제 불가

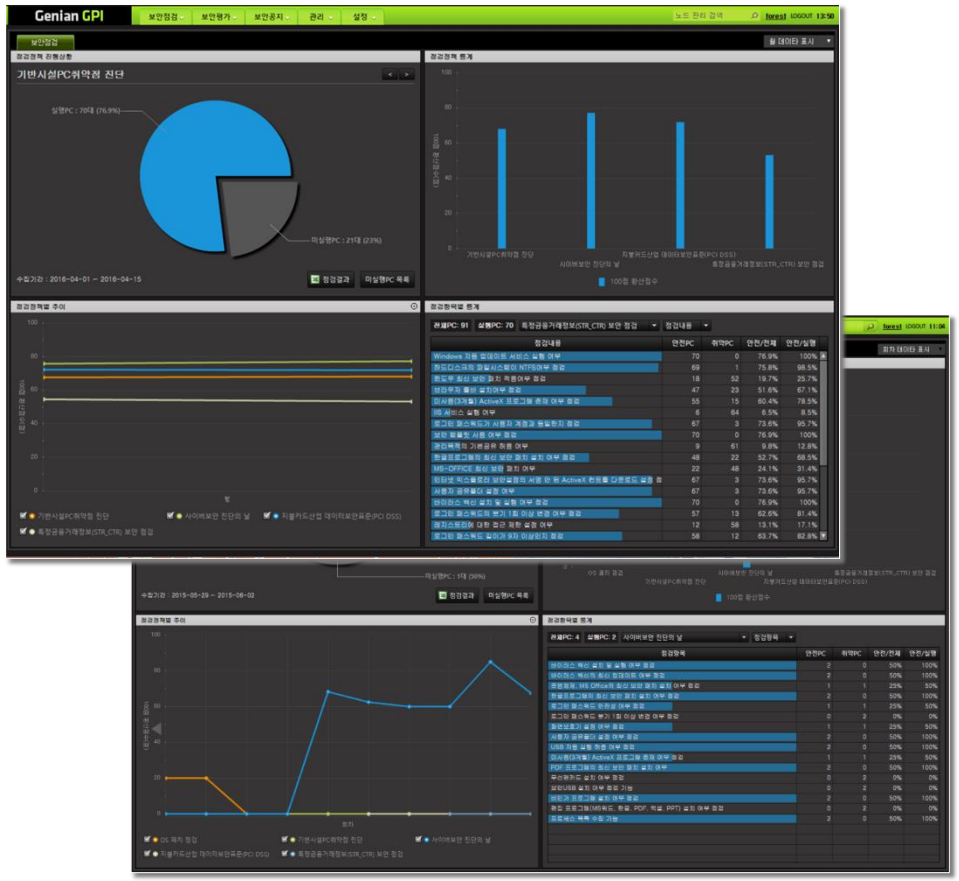
Genian GPI

▪ 사용자 주기적 재 인증 기능



- 보안점검 시 사용자 인증정보를 재확인
- 매월 첫 점검 시/ 매 회차 시 주기적 인증
- 사용자 인증 팝업창으로 인증정보 재확인
- 인증성공 시 보안점검 진행, 실패 시 인증 창 재 팝업

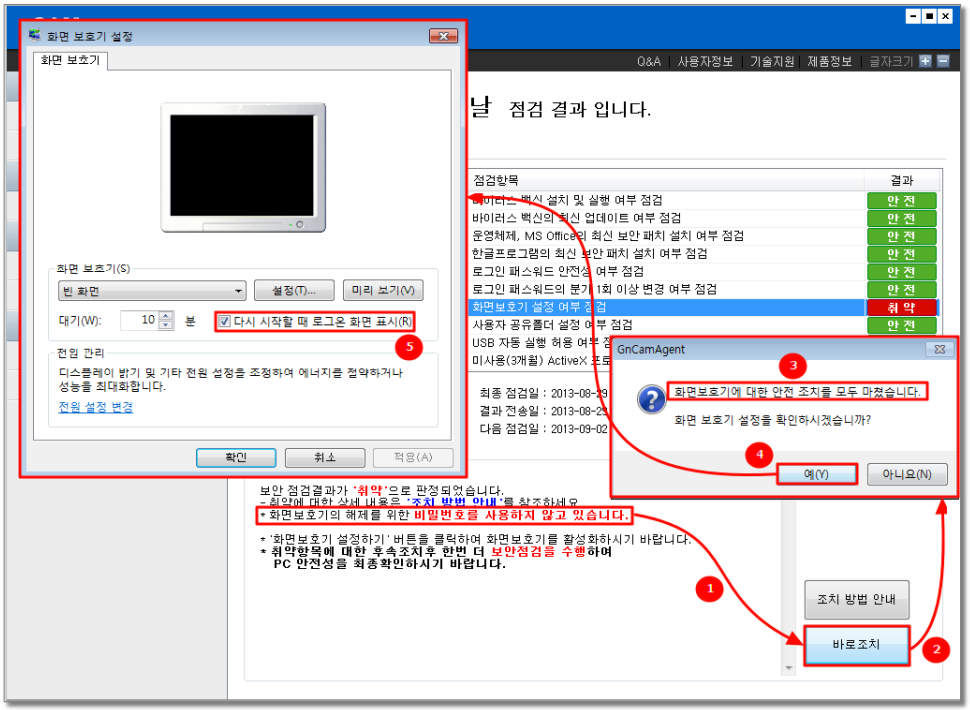
▪ Dashboard

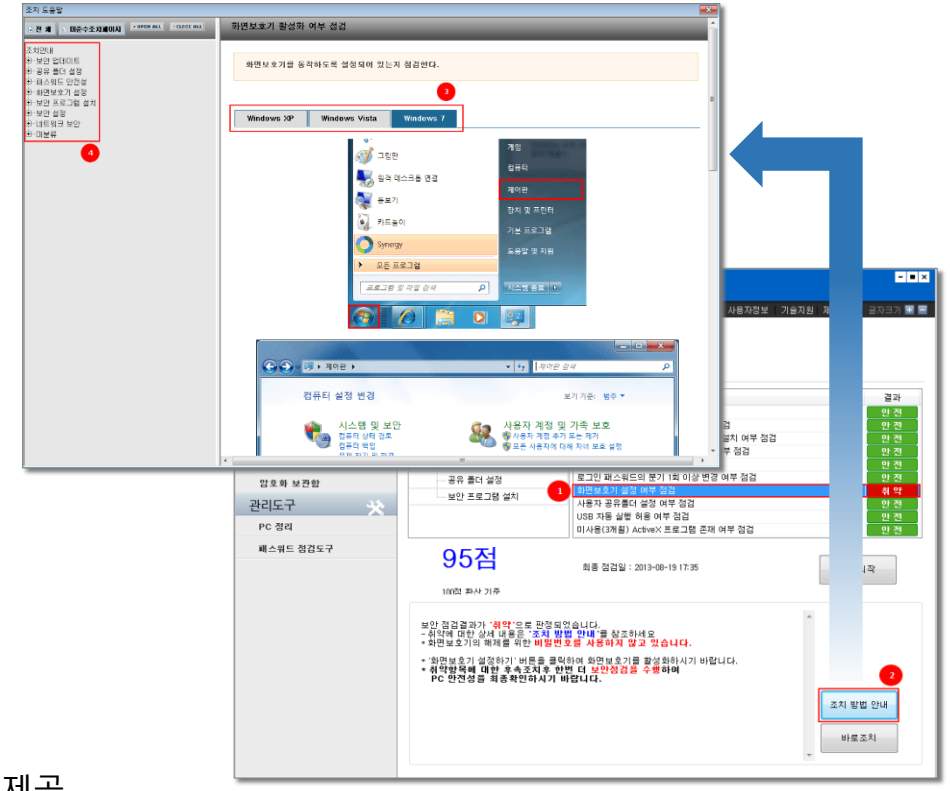


- 회차/월별, 점검 항목 별 통계 화면 제공

Genian GPI - AGENT

- **취약부분 바로 조치 및 조치 방법 안내 가이드 제공**

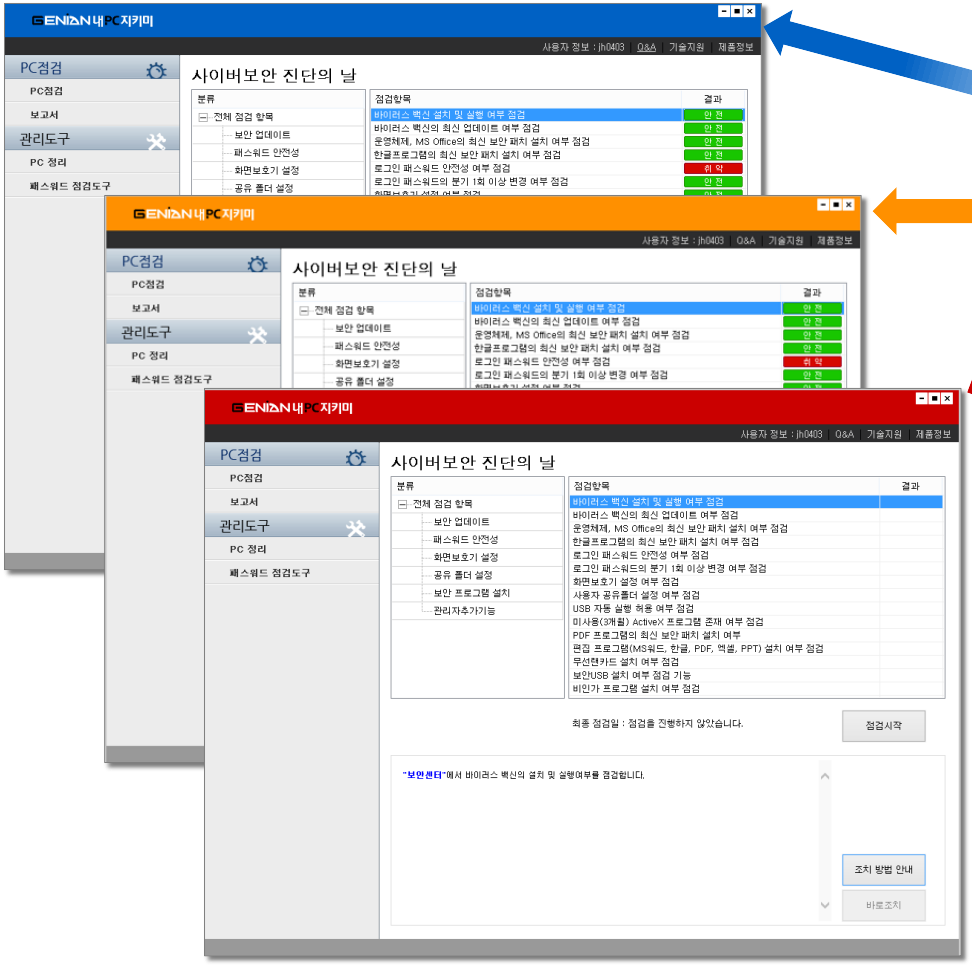




- 사용자PC 점검 결과 취약항목에 대한 설정/ 조치 방법 안내 기능 제공
- 사용자 개개인의 보안의식 고취를 위해 조치방법 안내 팝업창을 통해 직접 취약점 해결을 통한 보안의식 고취
- OS, MS-office 보안패치, 로그인 패스워드 안정성 등 일부 항목의 경우, 바로 조치 기능을 통해 간편히 취약항목 개선 기능 제공

Genian GPI - AGENT

- **보안점수에 따른 상태 바 변경 기능 제공**



- 관리자 설정을 통해 점수에 따라 사용자 PC 점검창의 상태바 색상 변경 기능 제공

GenianNAC + GPI 연동

Genian GPI - Genian NAC Suite 연동모델

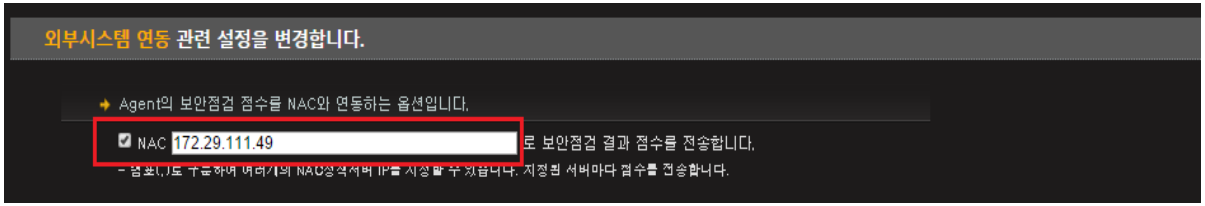
- 기존의 NAC Suite 연동 모델 구축구성 방안

Genian GPI - Genian NAC Suite 연동모델

- **NAC에서 GPI의 평가점수, 검사 여부 등에 의한 관리, 조치 기능 제공**

  - 내 PC지키미의 동작상태/ 검사결과에 따라 NAC의 제어 정책에 의해서 강제수행/ 교정 작업을 수행하도록 각 장비 설정 및 정책 수립

  - 내PC지키미의 NAC 연동 설정 화면



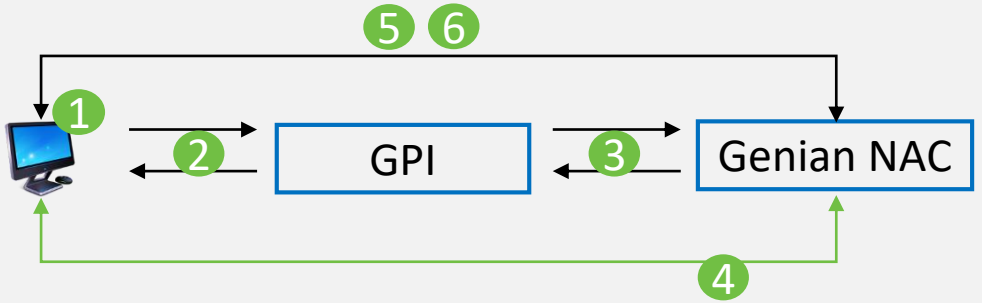
  - NAC의 관리 화면의 내PC지키미 단말의 점수 화면

GPI 점수

규제정책이름	점수	검사시각
"잘못된 인수" 에러 발생 테스트	53	2015-09-24 14:09:32
3.x 점검테스트	37	2015-09-24 14:28:31
NAC 기준 윈도우 보안 패치 연동 테스트	100	2015-09-24 14:09:35
Release Patch Test	63	2015-09-24 14:09:09
기반시설PC취약점 진단	70	2015-09-24 14:08:55
사이버보안 진단의 날	65	2015-09-24 14:10:27
지불카드산업 데이터보안표준(PCI DSS)	55	2015-09-24 14:09:44
특정금융거래정보(STR_CTR) 보안 점검	40	2015-09-24 14:09:03

Genian GPI - Genian NAC Suite 연동모델

- **기준 점수 미달 자에 대한 조치 예시**



① GPI 점검수행
② 점검수행결과 GPI서버 전송
③ 점검수행결과 NAC 전송
④ NAC정책에 따른 조치
- 점수 이상 : 정상사용
- 점수 이하 : 인터넷 차단, 사용자알람 통제 기능 수행

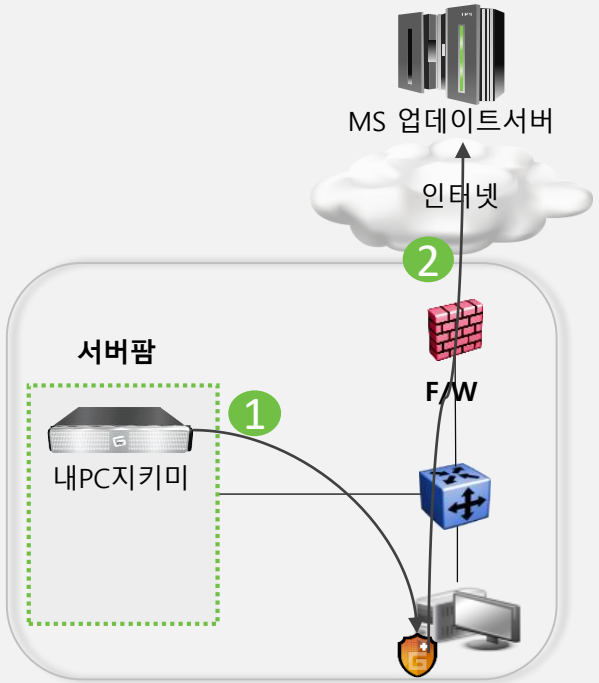
⑤ 재점검을 통해 점수 상승
⑥ 실시간 NAC로 점수 전송 후 차단 해제

내부 보안진단 수준 (예시)		
등급	GPI(준수율)	NAC 적용 사항
A	90 ~ 100 점	네트워크 전체 허용
B	80 ~ 89 점	업무 허용, 인터넷 차단
C	70 ~ 79 점	업무 허용, 인터넷 차단
D	60 ~ 69 점	**업무/인터넷 차단**
E	59 점 이하	**업무/인터넷 차단**

Genian GPI - Genian NAC Suite 연동모델

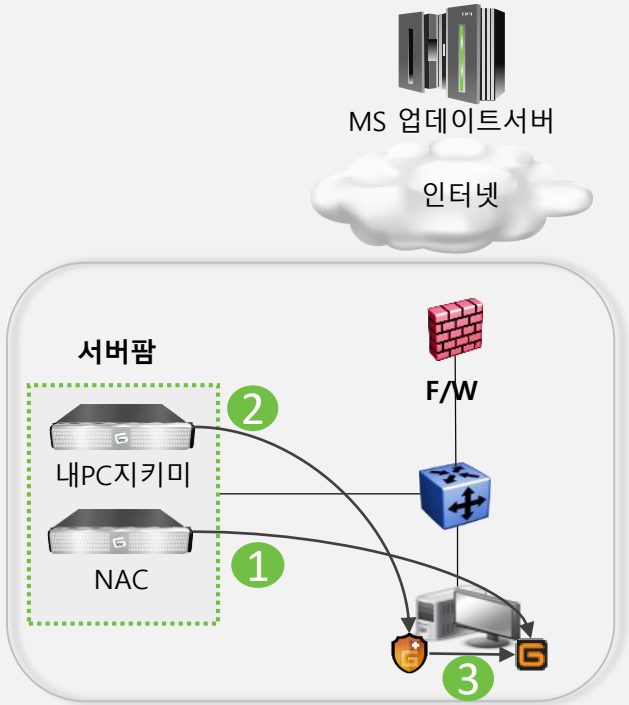
- OS/MS OFFICE 업데이트 점검 항목 연동

MS 업데이트서버를 이용한 OS/MS OFFICE 패치 확인



① 내PC지키미에서 GPI AGENT에게 OS/MS OFFFICE 업데이트 점검 명령
② MS 업데이트서버에서 OS/MS OFFICE 패치 만족 여부 확인

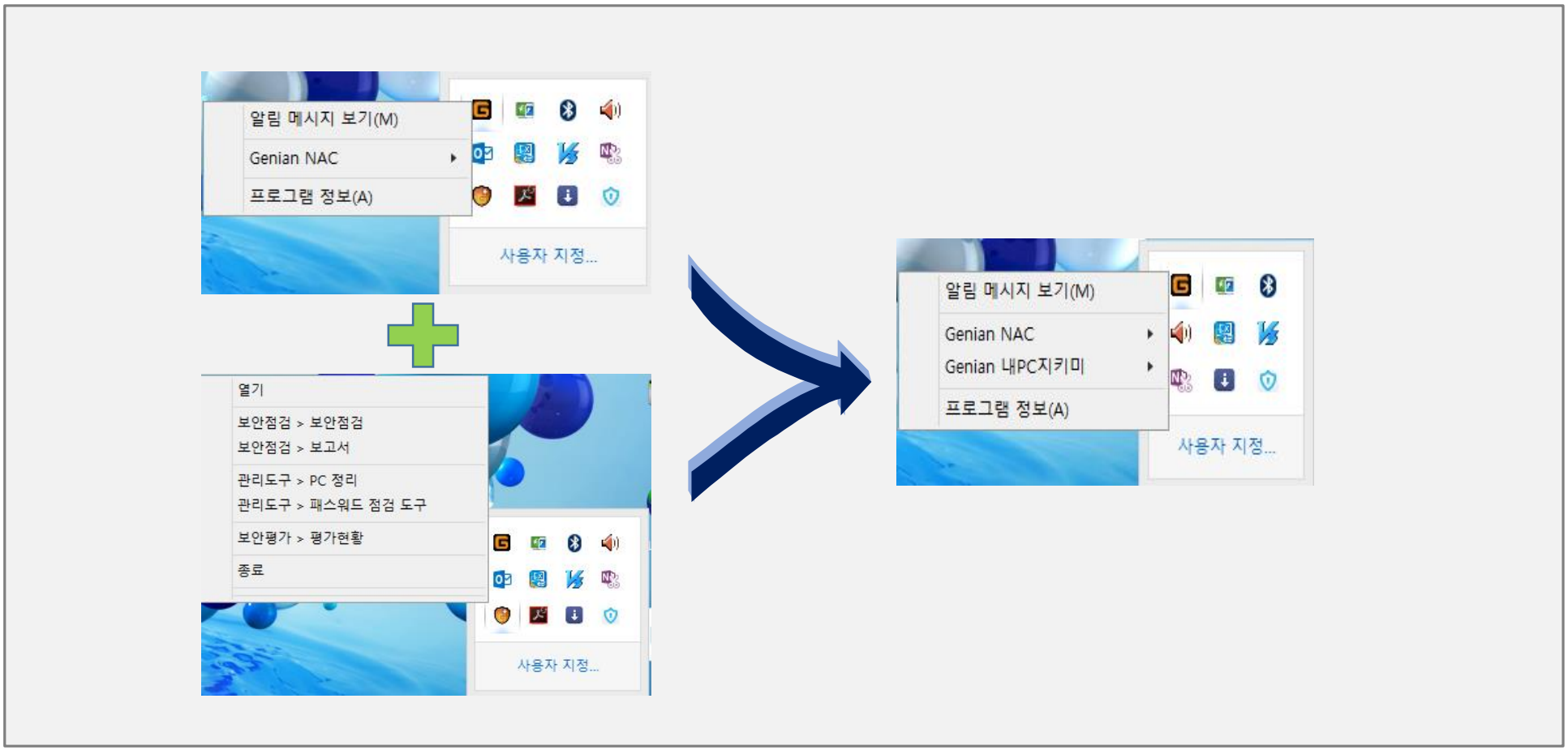
NAC 연동을 이용한 OS/MS OFFICE 패치 확인



① NAC를 이용한 주기적인 OS/MS OFFICE 패치 진행
② 내PC지키미에서 GPI AGENT에게 OS/MS OFFFICE 업데이트 점검 명령
③ NAC AGENT에게 OS/MS OFFICE 패치 만족 여부 확인

Genian GPI - Genian NAC Suite 연동모델

- NAC Agent, GPI Agent 통합 – 사용자 단말에서 하나의 아이콘으로 표시



회사 소개

회사개요

고객과 함께 좋은 가치를 만들어갑니다. 행복한 꿈을 이뤄가는 기업, 지니네트웍스입니다.

GeniNet

회 사 명	지니네트웍스㈜
대표이사	이 동 범
설 립 일	2005년 01월 07일
자 본 금	5억
주요사업	네트워크 보안 솔루션 개발/판매, 보안감사(audit) 솔루션 개발/판매
임직원수	97명 (16년 04월 현재)
협 력 사	론스텍(총판), 대신정보통신(총판) 등 약 30개사
주 소	경기도 안양시 동안구 시민대로 361 에이스평촌타워 803호
홈페이지	http://www.geninetworks.com/

제품소개

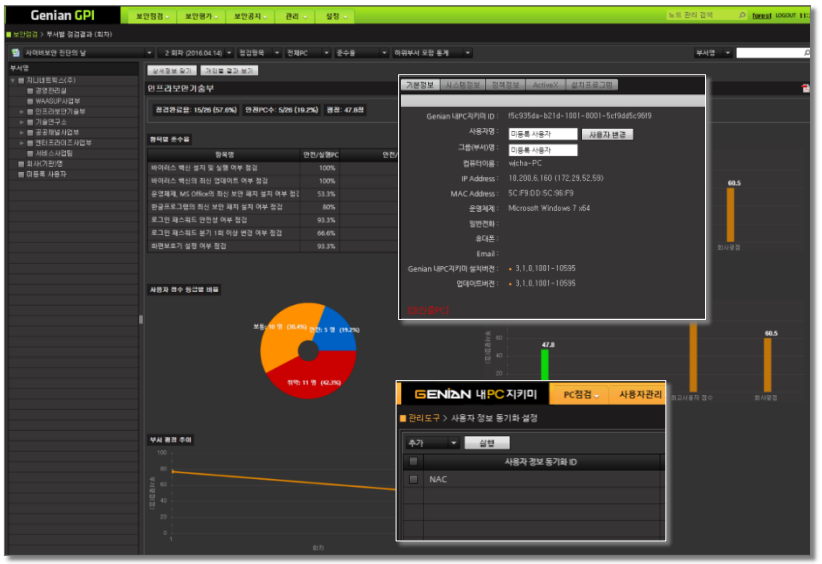
Genian NAC Suite

Genian NAC Suite는 내부 정보보호 체계를 수립하여
내부 자산과 사용자를 보호하고 기업 자원을 안전하게
사용할 수 있도록 지원하는 유무선 내부보안 전문 솔루션

Network Access Control

Genian GPI

Genian GPI는 조직 내부의 보안준수 여부를 빠르게
파악하고, 다면평가를 통해 사용자/조직/
보안정책 별 보안수준을 평가하는 규제준수관리 솔루션



Genian GPI

별 첨

주요고객사

GPI 주요 고객

지원 규제 정책

보안 정책 점검 상세 목록

사이버보안 진단 점검항목

1. 바이러스 백신 설치 및 실행 여부 점검
2. 바이러스 백신의 최신 보안 패치 여부 점검
3. 운영체제, MS Office의 최신 보안 패치 설치 여부 점검
4. 한글 프로그램의 최신 보안 패치 설정 여부 점검
5. 로그인 패스워드 안전성 여부 점검
6. 로그인 패스워드의 분기 1회 이상 변경 여부 점검
7. 화면보호기 설정 여부 점검
8. 사용자 공유 폴더 설정 여부 점검
9. USB 자동 실행 허용 여부 점검
10. 미사용(3개월) ActiveX 프로그램 존재 여부 점검
11. PDF 프로그램의 최신 보안 패치 설치 여부
12. 편집 프로그램(MS워드, 한글, PDF) 설치 여부 점검
13. 무선랜카드 설치 여부 점검 기능
14. 보안USB 설치 여부 점검 기능
15. 비인가 프로그램 설치 여부 점검
16. 사용자PC 프로세스 목록 수집기능

특정금융거래정보(STR CTR) 보안 점검

1. 최신 서비스팩과 보안패치 설치 여부
2. 불필요한 서비스/ 프로그램 사용 여부
3. 불필요한 자원 공유여부
4. 보안 템플릿 사용 여부
5. 계정정책 수립여부
6. 디스크 드라이브 안정적 포맷 여부
7. 바이러스 백신의 최신 업데이트 여부
8. 레지스트리에 대한 접근제한 여부
9. 기타 (OS 에서 제공하는 침입차단 기능, IIS/원격/FTP 실행여부)
10. 바이러스 백신 점검항목
11. 무선랜카드 사용여부 점검
12. 개인정보 암호화 저장 여부 점검
13. 개인정보 출력 복사 시 보호조치, 표시제한 조치

정보통신 기반시설PC 취약점 진단

1. 패스워드의 주기적 변경
2. 패스워드 정책이 해당기관의 보안정책에 적합하게 설정
3. 복구 콘솔 자동 로그온 방지
4. 공유폴더 제거
5. 메신저 사용 제한 여부
6. 불필요한 서비스 제거
7. 파일 시스템 NTFS로 포맷 여부
8. 다른 OS로 멀티부팅 금지
9. 브라우저 종료 시 임시 인터넷 파일 폴더의 내용 삭제
10. HOT FIX 등 최신 보안패치 적용
11. 최신 서비스팩 적용
12. MS-Office, 한글 어도비 아크로뱃 등의 응용 프로그램에 대한 최신 보안 패치 및 벤더 권고사항 적용
13. 바이러스 백신 프로그램 설치 및 주기적 업데이트
14. 바이러스 백신 프로그램에서 제공하는 실시간 감시 기능 활성화
15. OS에서 제공하는 침입차단 기능 활성화
16. 화면보호기 대기 시간을 5~10으로 설정 및 재 시작 시 암호로 보호하도록 설정
17. 이동식 미디어(CD, DVD, USB메모리 등)의 자동실행 방지 설정 여부
18. PC 내부의 미사용(3개월) ActiveX 제거
19. 시스템 부팅 시 Windows Messenger 자동시작 금지
20. 원격 지원을 금지 정책 설정 여부

PCI DSS

1. 개인정보 실행 여부 점검
2. 네트워크 자원 및 고객 데이터에 대한 모니터링
3. 시스템 접속 시 개인별 ID 관리
4. 시스템 및 Appl 의 안전한 개발 유지
5. 백신 사용 및 업데이트
6. 공중망 전송 시 데이터 암호화
7. 저장 데이터 보호
8. 패스워드 및 보안 파라미터의 기본값 사용금지
9. 방화벽의 설치 및 구성 관리

Thank you!

문의 : 031)422-3823,
consulting@geninetworks.com