



# Genian GPI 제품 소개서

---

지니언스



# 목 차

- 
- Genian GPI 소개
  - Genian NAC와 GPI 연동
  - 별첨
-

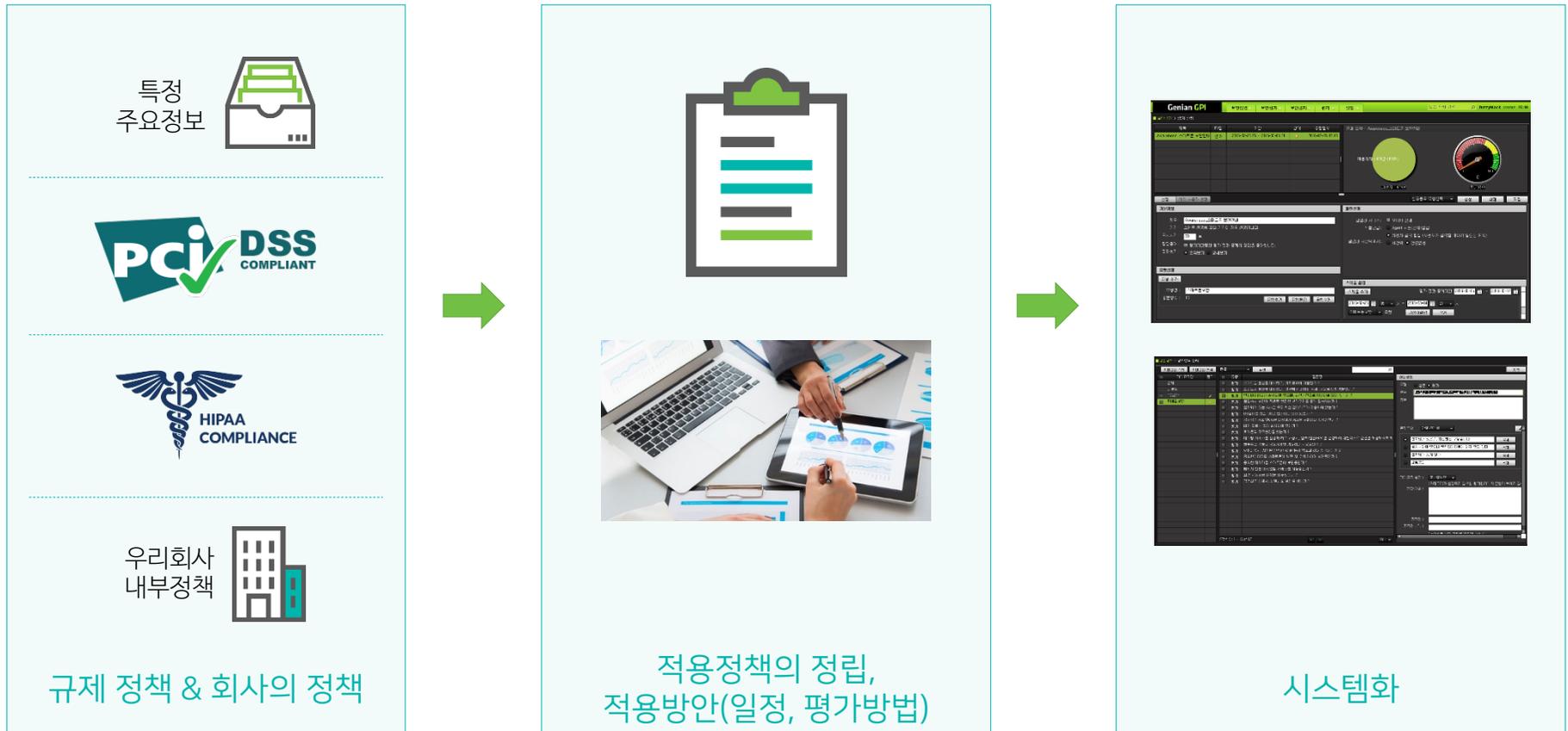
# Part1, Genian GPI 소개



# Prologue

## Compliance ?

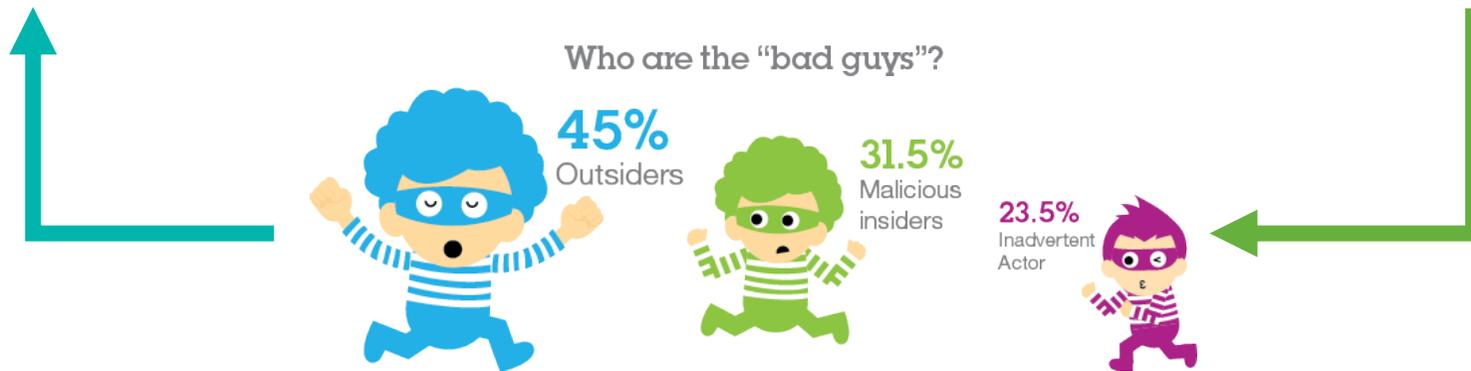
회사 임직원들이 사회적으로 승인된 내·외부 준거 기준(법·규정·회사 사규나 매뉴얼·문화·관습·사회적 책임 등)을 수용하고 이행하는 조직의 문화라고 정의할 수 있다 (Deloitte 2015)



# Prologue

## Awareness 장비?

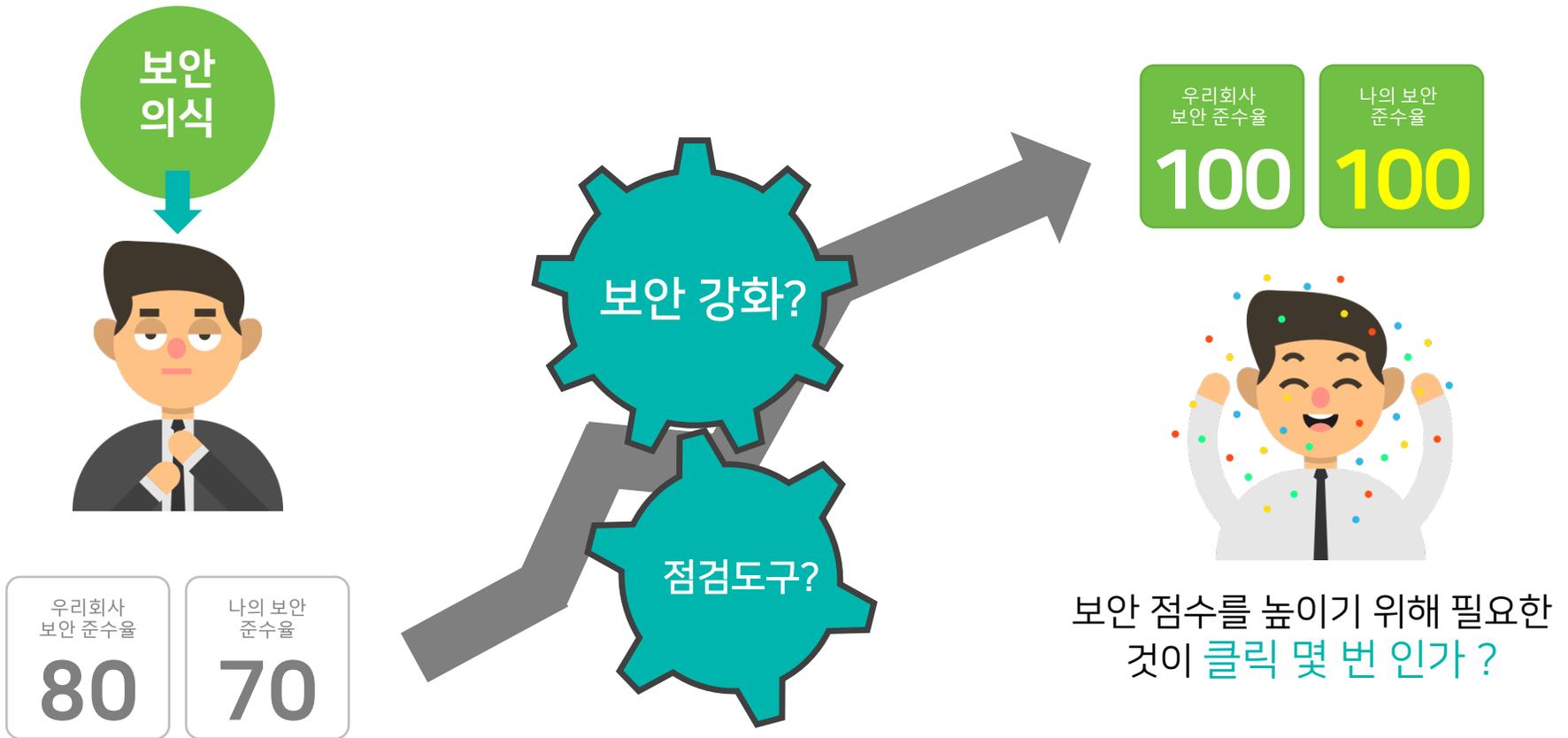
사용자의 보안의식을 강화하기 위해, 일반사용자에게 보안 규약, 정책을 알림, 교육, 점검을 위한 장비로 사용자가 스스로 단말의 보안을 유지 하기 위한 일련의 행동을 지속적으로 유도/점검함



출처 : IBM Security intelligence 2015

# Why Awareness ?

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



# Prologue

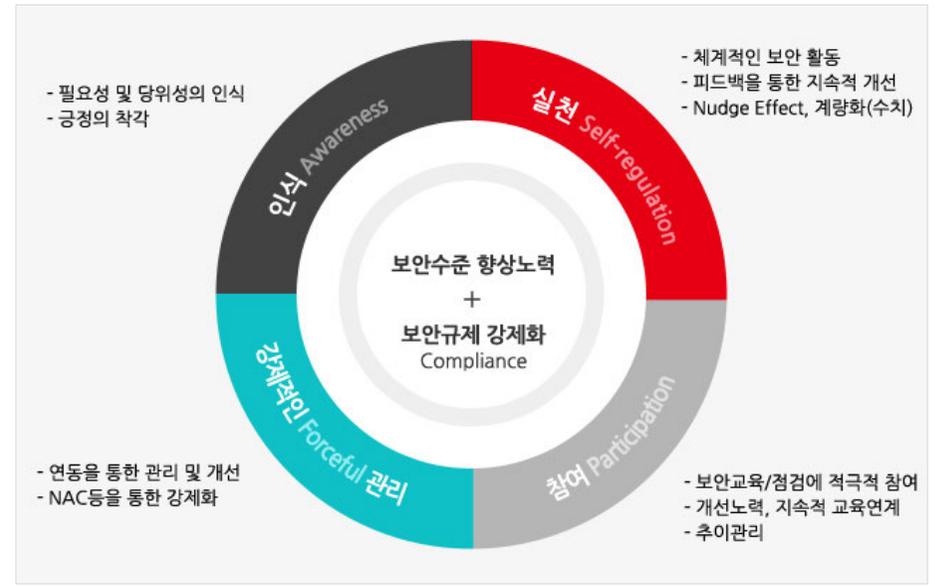
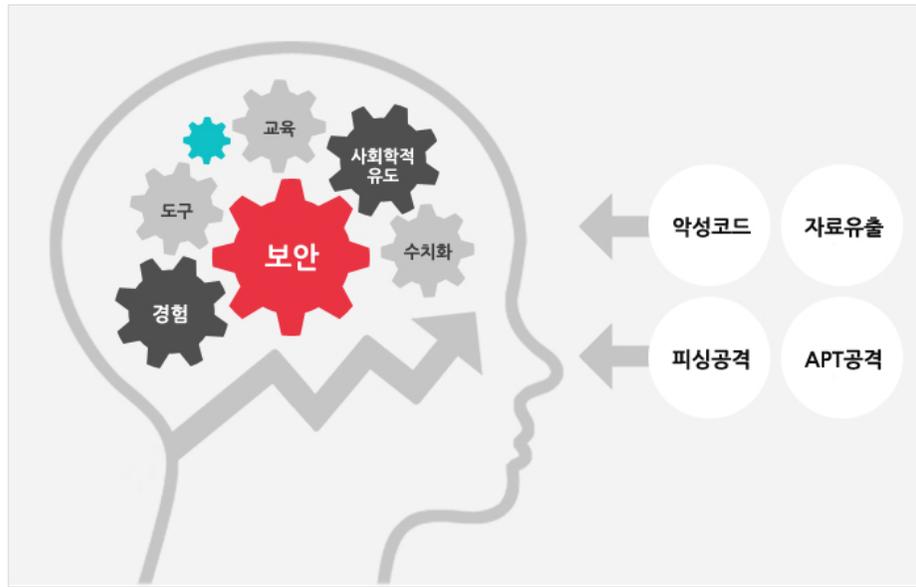


# Genian GPI - 필요성

## 보안 관리 및 인식 개선 필요

네트워크에 아무리 고가의 솔루션을 구입하여 완벽하다고 생각되는 보안체계를 구축해도 보안수준이 낮은 사용자가 많다면 애써 끌어올린 보안 수준이 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.

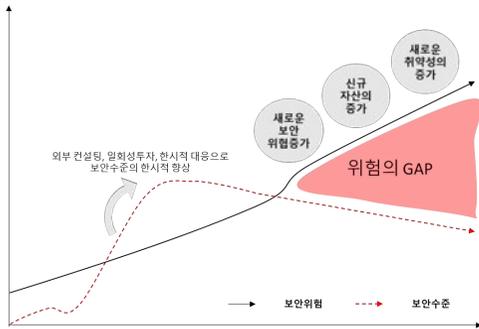
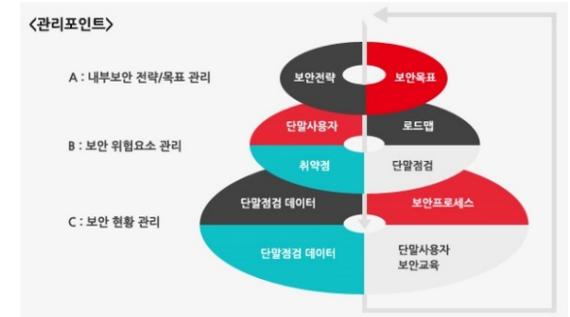


# Genian GPI - 기대효과

## 조직의 보안 수준 개선 및 보안 문화 조성

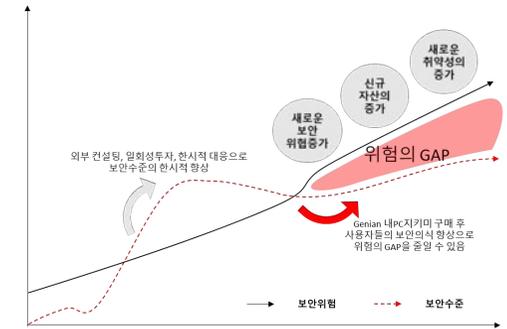
### • 전사적 차원의 보안문화 조성 가능

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.



보안 의식/수준

### 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.

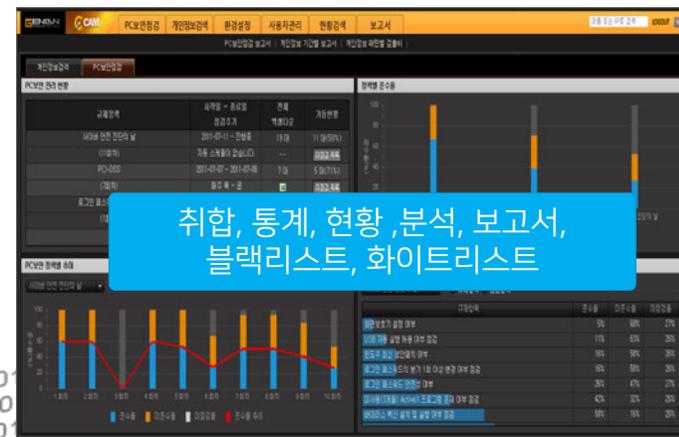
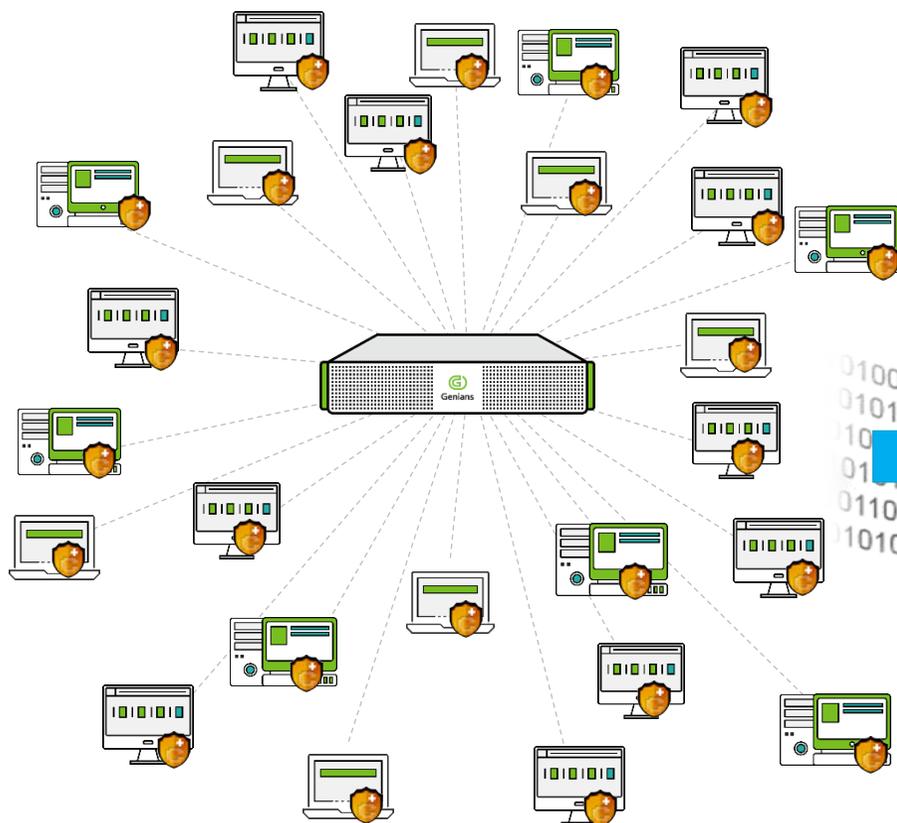
# Genian GPI - 특징 및 장점 ( 지원 규제 정책 )

## 다양한 보안 정책 지원

보안 정책	관련법규 및 규정	대상기관	점검항목 수
사이버보안진단의날	<ul style="list-style-type: none"> <li>국가정보원 국가정보보안 기본지침</li> <li>행정안전부 정보통신보안업무규정</li> </ul>	<ul style="list-style-type: none"> <li>국가 공공기관, 공사</li> </ul>	<ul style="list-style-type: none"> <li>16개 점검항목</li> </ul> 
정보통신기반시설 취약점진단(단말)	<ul style="list-style-type: none"> <li>미래창조과학부 정보통신기반 보호법</li> </ul>	<ul style="list-style-type: none"> <li>정보통신기반시설 보유 기관</li> </ul>	<ul style="list-style-type: none"> <li>20개 점검항목</li> </ul> 
특정금융거래정보 보안점검	<ul style="list-style-type: none"> <li>금융위원회 공문 ( 2013.08.13 )</li> <li>특정금융거래정보(STR, CRT) 보안기준</li> </ul>	<ul style="list-style-type: none"> <li>금융위원회 산하 금융기관</li> </ul>	<ul style="list-style-type: none"> <li>13개 점검항목</li> </ul> 
지불카드산업 데이터 보안표준 (PCI-DSS)	<ul style="list-style-type: none"> <li>지불카드정보보안표준위원회 정보보안 표준규격 ( PCI 3.0 )</li> </ul>	<ul style="list-style-type: none"> <li>카드사, VAN, PG사</li> </ul>	<ul style="list-style-type: none"> <li>9개 점검항목</li> </ul> 

# 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

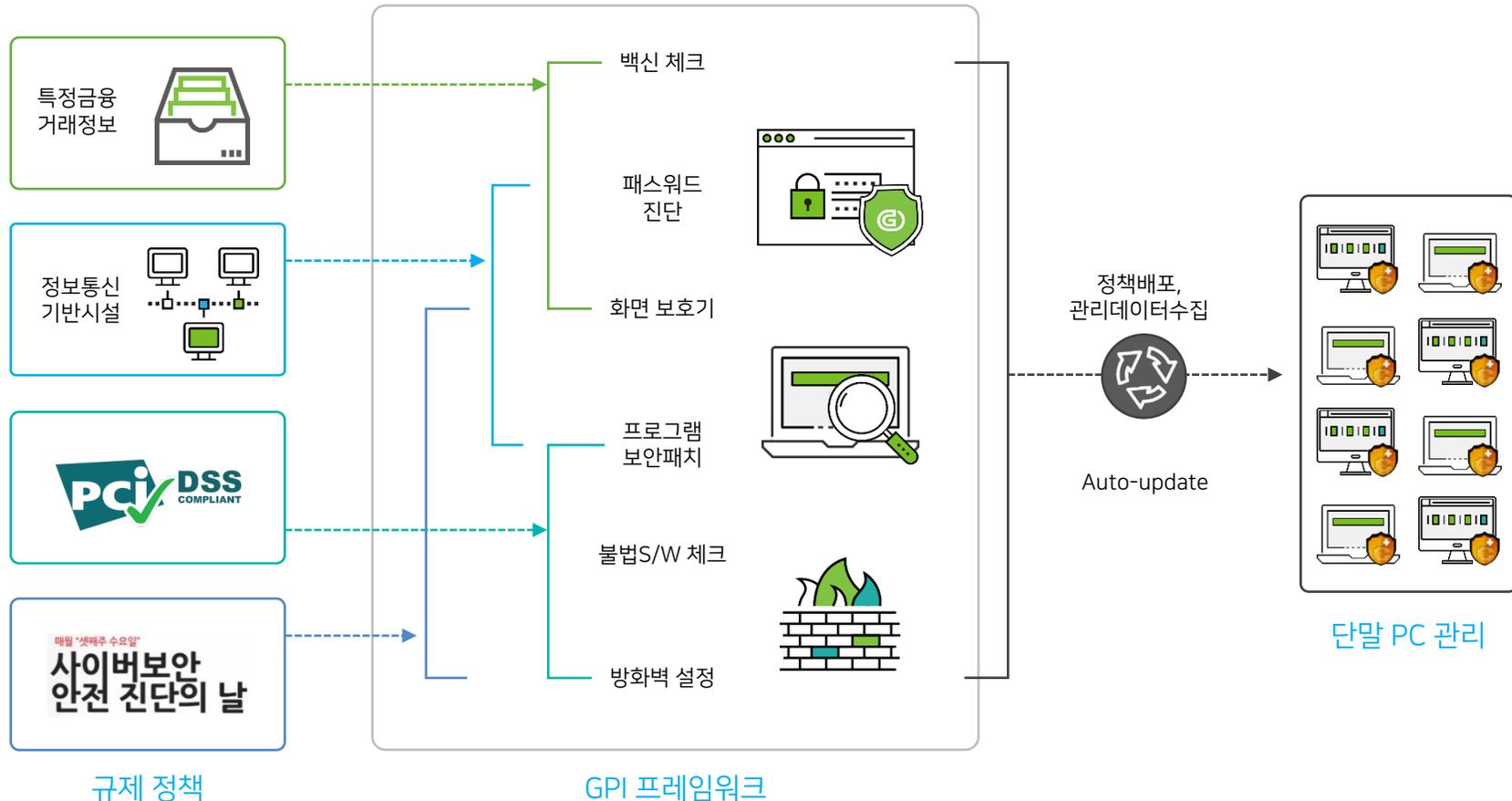


단말 상황 Data



# 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
- 대시보드 기능 지원
- 중간관리자 기능 지
- 점검 결과 다운로드 기능 지원

## 제어(통제)

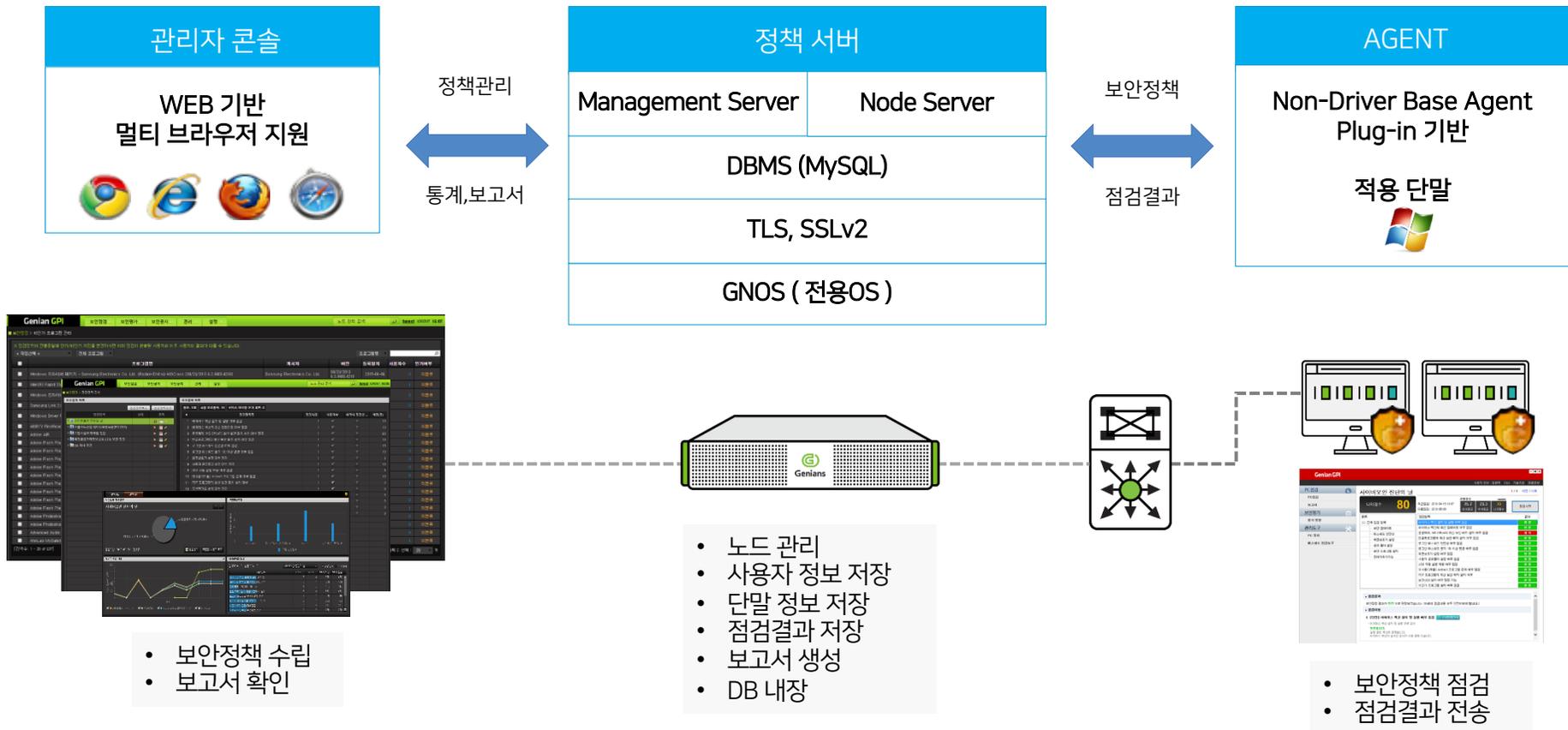
- 기준 점수 미달, 특정 항목 취약 시 점검 창 닫기 제한 및 주기적 팝업 기능 지원
- Genian NAC 연동 기능
  - 기준 점수 미달자에 대한 네트워크 차단
- 조직 보안포탈 연동 기능 지원

## 기타

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

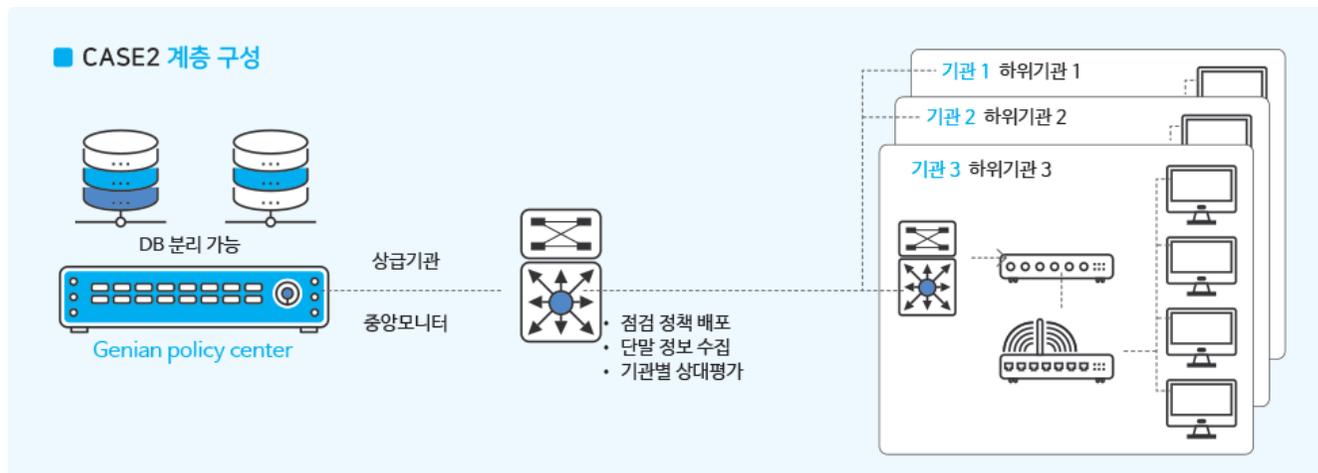
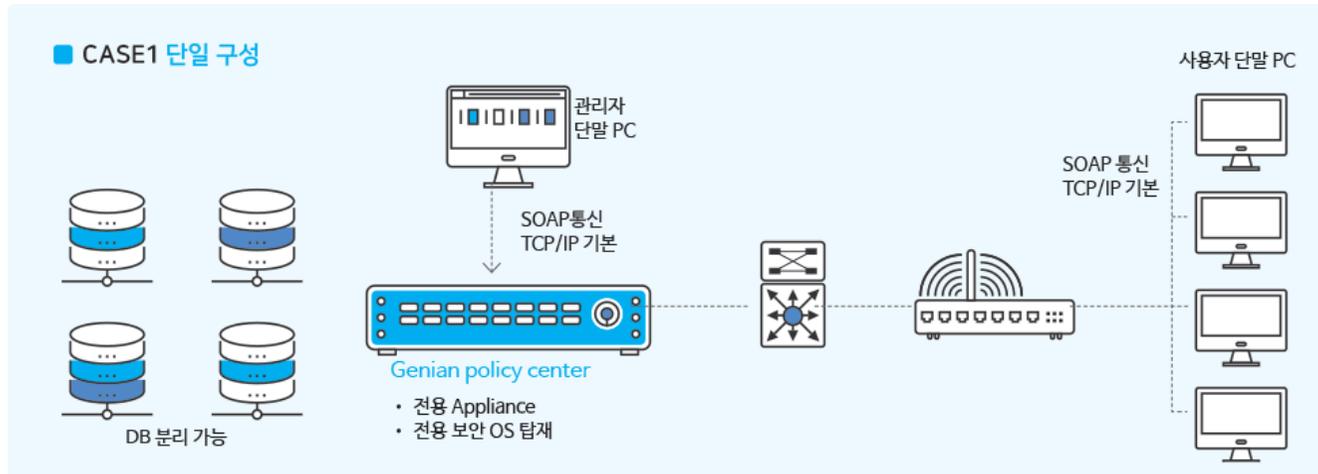
# Genian GPI - 구성 및 역할

- 보안 전용 OS를 탑재한 전용 센터 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



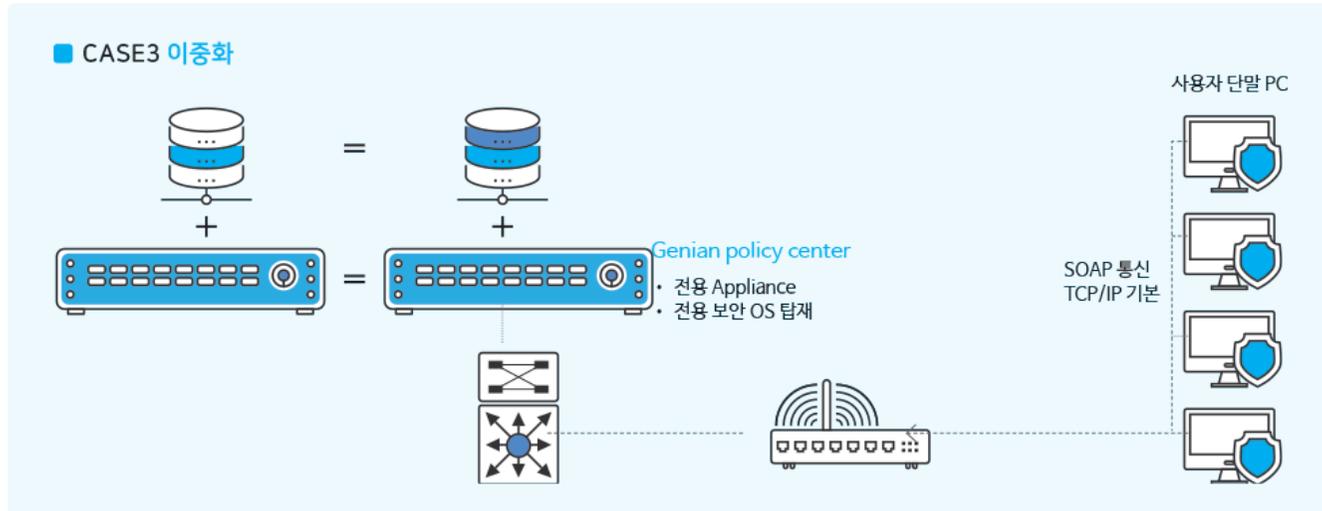
# Genian GPI - 구성 방안

- 단일 센터 구성 및 계층적 구성 방법 등 다양한 조건에 알맞도록 구성 가능\_단일 구성, 계층 구성



# Genian GPI - 구성 방안

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



- 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

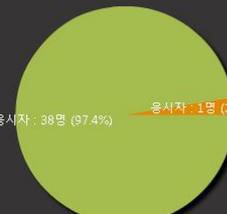
## ■ 사용자에게 대한 보안 평가 관리 대시보드

**Genian GPI**
노드 관리 검색 rune37 LOGOUT 10:33

[보안점검](#)
[보안평가](#)
[보안공지](#)
[관리](#)
[설정](#)

제목	타입	기간	상태	수정일시
05월 평가 테스트	평가	2016-05-10 05 ~ 2016-05-13 21	<span style="color: red;">■</span>	2016-05-11 10:28
GPI 교육용 테스트	실험	2016-04-04 05 ~ 2016-04-04 21	완료됨	2016-04-04 11:18
테수투	평가	2016-03-22 05 ~ 2016-03-22 21	완료됨	2016-03-22 17:46
3월 설문테스트3	실험	2016-03-22 05 ~ 2016-03-22 21	완료됨	2016-03-22 15:20
3월 테스트	평가	2016-03-22 05 ~ 2016-03-22 21	완료됨	2016-03-22 15:25
설문설문A	실험	2016-01-21 05 ~ 2016-01-21 21	완료됨	2016-01-21 13:22
testtest	실험	2016-01-20 05 ~ 2016-01-20 21	완료됨	2016-01-20 17:20
보안평가 평가테스트2	평가	2016-01-20 05 ~ 2016-01-20 21	완료됨	2016-01-20 15:14

결과 요약 - 05월 평가 테스트



대상자 : 39명



평균점수

**기본정보**

제목: 05월 평가 테스트

기간: 스케줄 설정에 따라 기간이 자동 설정됩니다.

응시시간: 60 분

정답공개:  평가기간동안 평가 결과 공개시 경합을 공개합니다.

결과보기:  요약보기  상세보기

**유형설정**

유형명: 05월 보안 평가

종문장수: 5

**화면설정**

팝업창 사이즈:  모니터 전체

노출방법:  Agent 자동(강제)팝업

알림창 최상위표시:  사용자 클릭 팝업 (사용자가 클릭할 때까지 알림창 표시)

알림창 최상위표시:  최상위  상관없음

평가화면 노출 형태

**스케줄 설정**

스케줄 추가

평가 결과 공개기간 2016-05-11 ~ 2016-05-13

2016-05-10 05 시 ~ 2016-05-13 21 시

05월 보안 평가 유형

지니언스(주)



# Genian GPI - 평가

## ■ 사용자에게 대한 보안 평가 결과 대시보드

**Genian GPI** | 보안점검 | 보안평가 | 보안공지 | 관리 | 설정 | 노드 관리 검색 | rune37 LOGOUT 10:34

■ 보안평가 > 평가 결과

유형	제목	상태	응시자 / 대상자	평균점수	최저점수	최고점수
평가	05월 평가 테스트	진행중	1 / 39	40	0	80
설문	GPI 교육용 테스트	완료	0 / 8			
평가	테수투	완료	91 / 91	1.6	0	50
설문	3월 설문테스트3	완료	3 / 3			
평가	3월 테스트	완료	20 / 20	5.4	0	40
설문	설문설문A	완료	1 / 3			
설문	testtest	완료	0 / 1			
평가	보안평가 평가테스트2	완료	1 / 1	0	0	0

■ 보안평가 > 평가 결과

**평가 정보**

평가명: 05월 평가 테스트  
 유형: 평가  
 기간: 진행중 (2016-05-10 05시 - 2016-05-13 21시)  
 응시율: 1명 / 39명 (2.5%)

**통계 정보** | 최자 | 평균 | 최고

0점 | 40점 | 80점

평가 결과 목록

사용자별 결과 | 부서별 결과 | 문항별 상세결과

하위부서 포함 |  전체부서

부서찾기

사용자 ID	부서	상태	점수	석차	응시일
leadh13	CS팀	미응시	0	0	
rune37	CS팀	제출완료	80	0	2016-05-11

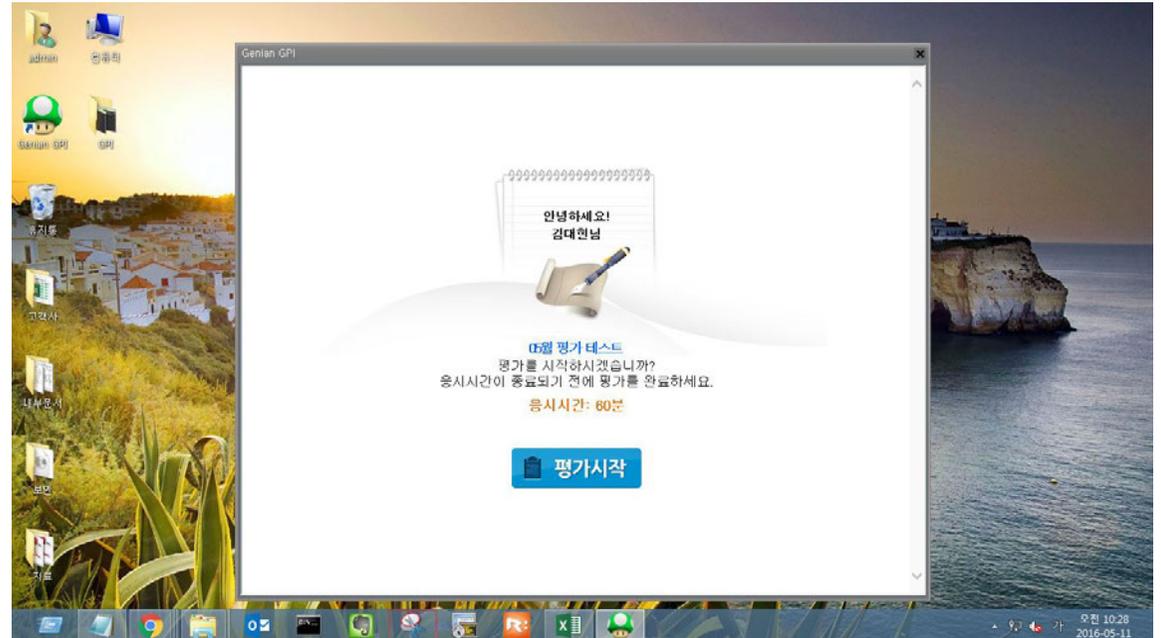
세부 결과

# Genian GPI - 평가

## ■ 사용자 평가 시작 화면



Full Screen



Popup Screen

# Genian GPI - 평가

## ■ 사용자 평가 테스트 화면

Genian GPI

05월 평가 테스트 00:59:46 / 응시시간: 60분

[1] 무선랜의 장점이 아닌 것은?

- 케이블보다 보안성이 떨어진다.
- 확장이 용이하다.
- 네트워크 구성비용이 적게 든다.
- 사용이 편리하다.

저작권: (주)씨드젠

다음문제 > 미리보기 후 제출하기

1 2 3 4 5

# Genian GPI - 평가

## ■ 사용자 평가 완료 후 제출 화면

Genian GPI

[4] 다음 설명중 옳지 않은 것은?

**이동**

- 정보반출이 허용된 사용자가 외부로 유출하는 것은 막을 수 없다.
- 문서보안이란 정보의 생성에서 사용, 공유, 폐기에 이르기까지 전 라이프 사이클에서 디지털 정보의 불법적인 또는 무분별한 사용 및 변경, 유출을 차단하는 것을 뜻한다.
- 문서보안에서의 문서란 업무상 생성되는 모든 전자정보이다.
- 문서보안 기술을 쓰면 유출을 100% 막을 수 있다.

저작권: (주)씨드젠

웹 페이지 메시지

제출하시겠습니까?  
제출이 완료되면 다시 수정할 수 없습니다.

**확인** **취소**

[5] 첨부파일 보안 중요:

**이동**

- 첨부파일 열람전 백신프로그램으로 검사후 열람한다.
- 첨부파일이 exe와 같은 실행 확장자가 아니라도 백신프로그램으로 검사후 실행한다.
- 첨부파일이 그림 파일이었을 경우 백신프로그램으로 검사 안해도 된다.
- 첨부파일을 PC에 저장한 후 실행하지 않고 백신프로그램으로 검사후 실행한다.

저작권: (주)씨드젠

**처음으로**  **제출하기**

Genian GPI

제출이 완료되었습니다.

[2016-05-10 ~ 2016-05-13] 기간동안  
Agent 보안평가 메뉴를 클릭하여 결과를 확인할 수 있습니다.

**닫기** **결과보기**

# Genian GPI - 평가

## ■ 단말 보안 상태 점검

#	점검항목명	점검내용	사용여부	위약시 점검항...	배점(점)	이동
1	비버리온 백신 설치 및 실행 여부 점검	1	✓		10	
2	비버리온 백신의 최신 업데이트 여부 점검	1	✓		10	
3	운영체제, MS Office의 최신 보안 패치 설치 여부 점검	1	✓		20	
4	한글프로그램의 최신 보안 패치 설치 여부 점검	1	✓		10	
5	로그인 패스워드 안전성 여부 점검	1	✓		10	
6	로그인 패스워드 분기 1회 이상 변경 여부 점검	1	✓		10	
7	화면보호기 설정 여부 점검	1	✓		5	
8	사용자 응용프로그램 설정 여부 점검	1	✓		10	
9	USB 자동 실행 허용 여부 점검	1	✓		5	
10	미사용(3개월) ActiveX 프로그램 존재 여부 점검	1	✓		10	
11	PDF 프로그램의 최신 보안 패치 설치 여부	1	✓		0	
12	무선랜카드 설치 여부 점검	1	✓		0	
13	보안USB 설치 여부 점검 가능	1	✓		0	
14	비인가 프로그램 설치 여부 점검	1	✓		0	
15	편집 프로그램(MSWord, 한글, PDF, 엑셀, PPT) 설치 여부 점검	1	✓		0	
16	프록시주소 목록 수집 가능	1	✓		0	

점검내용 관리

ID: [input field]

점검내용명: [input field]

배점: [input field]

설명: [input field]

조치: [input field]

설명값: [input field]

한번 저장한 점검내용의 타입은 변경할 수 없습니다.

Ver. [input field]

저장 | 닫기

- 국정원 보안기준(사이버보안진단의 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

**사이버보안 진단의 날**

달력에 표시되는 식  
#3366CC

**반복 스케줄 설정**

- 반복 스케줄 사용안함
- 요일단위설정(월당)
  - 2 주차 ~ 2 주차
  - 매 주 일 ~ 일
- 날짜단위설정(월당)
  - 매달
  - 예) 시작일-종료일 (5-8, 12-15) : 구분, 최대 4개까지 설정 가능
  - 매일 (토, 일은 제외됨.)

**일회성 스케줄 설정**

일회성은 오늘 ~ 60일까지만 설정할 수 있습니다. 반복 스케줄과 연계성이 없으며 독립적으로 동작합니다. 달력버튼을 선택하시기 바랍니다. [추가](#)

2016-04-27 ~ 2016-04-27 [삭제](#)

보안점검 > 점검정력 스케줄 관리

2016년 4월

일	월	화	수	목	금	토
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
1	2	3	4	5	6	7

- 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

점검 대상자 설정

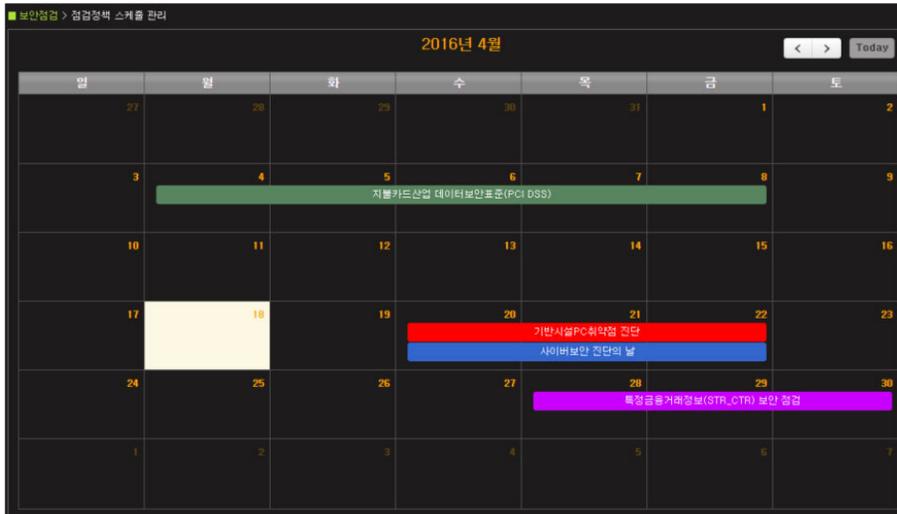
IP주소  IP가 같으면

실 정:

점검일시: 2 일후 00 시 00 분 부터

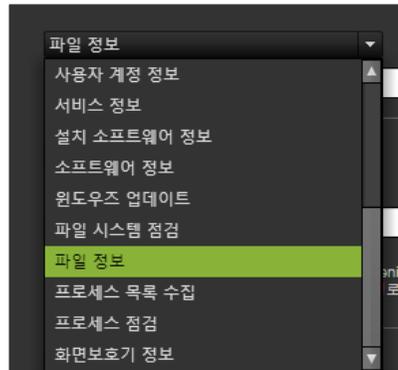
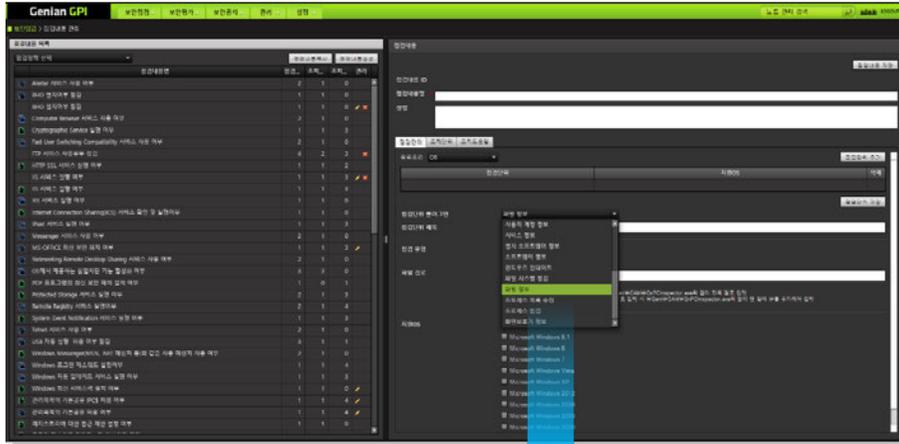
항목	조건	설정	점검일시	관리
사용자 추가정보1	같으면	A지역본부	0일후 00:00부터	🔧 ✖
사용자 추가정보1	같으면	B지역본부	1일후 00:00부터	🔧 ✖
사용자 추가정보1	같으면	C지역본부	2일후 00:00부터	🔧 ✖

- 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 부하 분산 효과
- 보안업데이트, 한글, PDF 업데이트 트래픽에 대한 부하 분산 효과



# Genian GPI - 평가

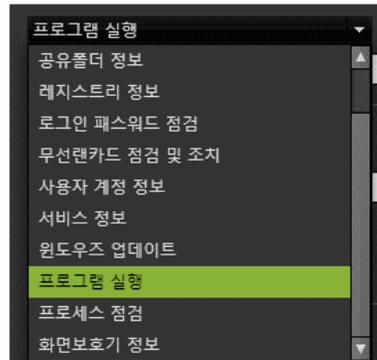
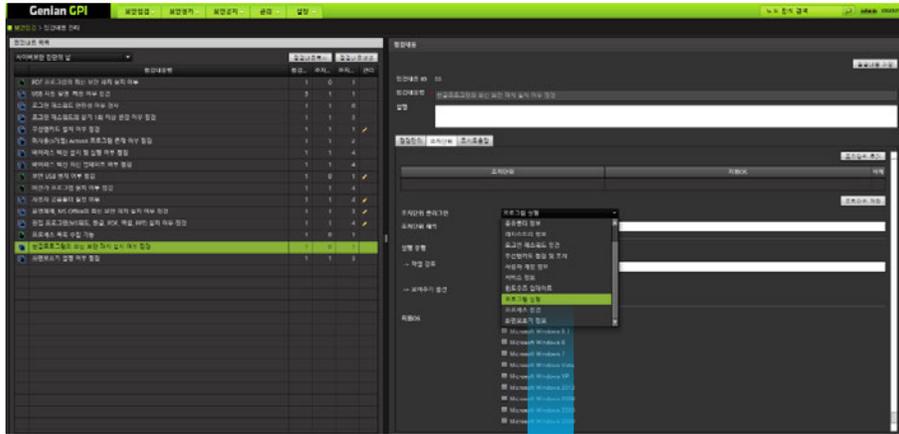
## 관리자 추가 점검내용 생성



- 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
  - 윈도우즈 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
- 윈도우즈 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

## ■ 점검항목 OS별 차등 적용

The screenshot shows the configuration interface for a security check item. The '점검조건' (Check Condition) is set to 'OR'. The table below lists the check items and their supported OS versions:

점검단위	지원OS
윈도우 방화벽 활성화되어 있으면 안전	XP / 2003 / 2000
윈도우 기본 방화벽 활성화되어 있으면 안전	8.1 / 8 / 7 / Vista / 2012 / 2008
윈도우 공용 방화벽 활성화되어 있으면 안전	8.1 / 8 / 7 / Vista / 2012 / 2008

Below the table, the '점검단위 플러그인' (Check Item Plugin) is set to '레지스트리 정보' (Registry Information). The '점검단위 제목' (Check Item Title) is '윈도우 방화벽 활성화되어 있으면 안전'. The '점검 유형' (Check Type) is '존재하면' (If Present), and the 'Registry Key' is 'SYSTEM#CurrentControlSet#Services#SharedAccess#Parameters#FirewallPolicy#StandardP...'. The '점검 유형을 선택합니다.' (Select Check Type) dropdown is set to 'HKEY\_LOCAL\_MACHINE'.

The screenshot shows the configuration interface for a security check item. The '점검조건' (Check Condition) is set to 'AND'. The table below lists the check items and their supported OS versions:

점검단위	지원OS
Internet Connection Sharing(ICS) 서비스 실행중이면 안전	XP / 2003 / 2000
Internet Connection Sharing(ICS) 서비스 동작하지 않으면 안전	10 / 8.1 / 8 / 7 / Vista / 2012 / 2008

Below the table, the '점검단위 플러그인' (Check Item Plugin) is set to '서비스 정보' (Service Information). The '점검단위 제목' (Check Item Title) is 'Internet Connection Sharing(ICS) 서비스 동작하지 않으면 안전'. The '점검 유형' (Check Type) is '동작하지 않으면' (If Not Running), and the '서비스 명' (Service Name) is 'SharedAccess'. The '서비스 유형을 선택합니다.' (Select Service Type) dropdown is set to 'SharedAccess'.

- 동일 항목이라도 OS별 점검내용 다르게 점검 기능 제공
- 윈도우 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

보안정책 수정

보안정책명: 사이버보안 진단의 날

점검 안내 팝업창: 포시할 (취소불가) [이름] [미리보기] [X]

점검 수행 옵션: 자동수행 (화면포시할)

Agent 닫기 제한: 제한안함

항목	조건	설정	삭제
IP주소	서브넷에 속하면	0.0.0.0/0.0.0.0	X

보안정책 수정

보안정책명: 사이버보안 진단의 날

점검 안내 팝업창: 보안점검 안내 팝업 이미지가 없으면 표시되지 않습니다. [찾아보기] [업로드] [미리보기] [X]

점검 수행 옵션: 자동수행 (화면포시할)

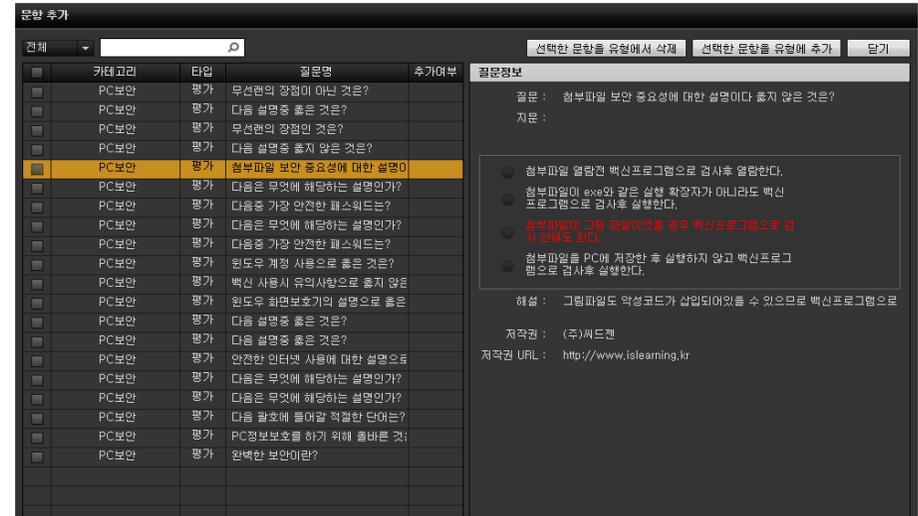
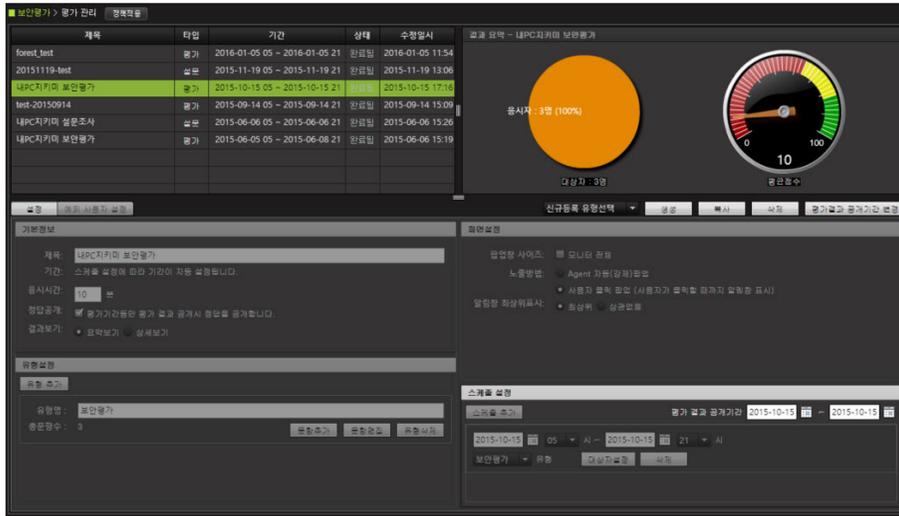
Agent 닫기 제한: 자동수행 (결과만 표시)

항목	조건	설정	삭제
IP주소	서브넷에 속하면	0.0.0.0/0.0.0.0	X

- 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

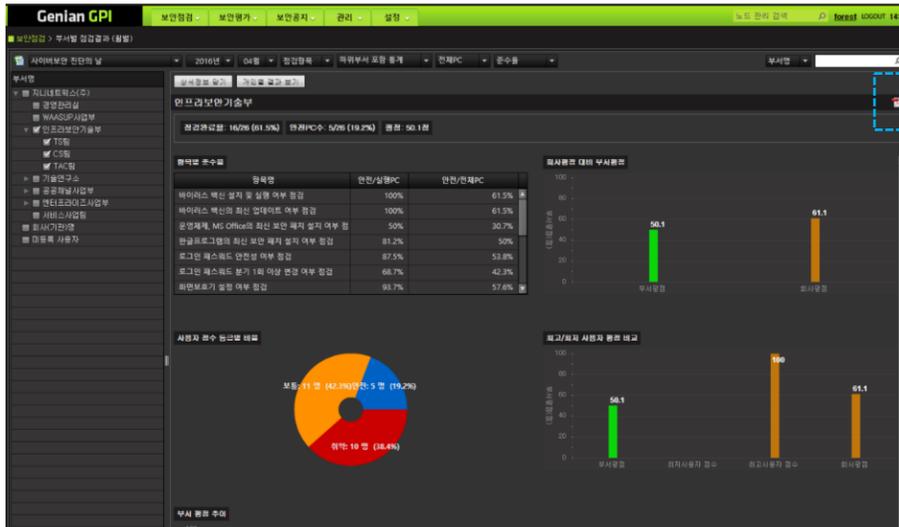


# Genian GPI - 분석

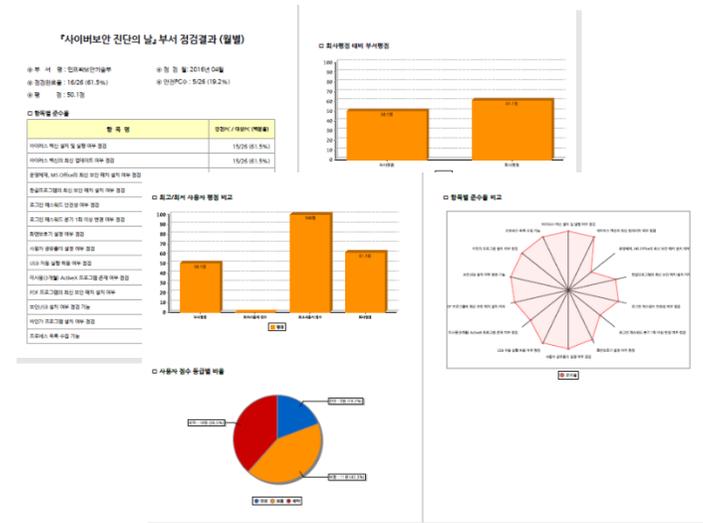
## ■ 점검결과 분석을 위한 개인별 점검결과 보고서 제공

부서명	실검	전제	완료율	부서평점	바이러스	바이러스	운영체제	한글프로
지니네트웍스(주)	72	91	79.1%	61.1	79.1%	79.1%	31.8%	56%
경영관리실	7	8	87.5%	55.6	87.5%	87.5%	12.5%	37.5%
WAASUP사업부	7	9	77.7%	56.1	77.7%	77.7%	11.1%	44.4%
인프라보안기술부	16	26	61.5%	50.1	61.5%	61.5%	30.7%	50%
TS팀	8	14	57.1%	45	57.1%	57.1%	21.4%	42.8%
CS팀	2	4	50%	40	50%	50%	25%	50%
TAC팀	5	7	71.4%	62.1	71.4%	71.4%	57.1%	57.1%
기술연구소	23	27	85.1%	71.2	85.1%	85.1%	48.1%	74%
공공채널사업부	8	8	100%	77.5	100%	100%	50%	50%
엔터프라이즈사업부	6	8	75%	53.1	75%	75%	12.5%	50%
서비스사업팀	3	3	100%	63.3	100%	100%	0%	66.6%
회사(기관)명	0	0	0%	0	0%	0%	0%	0%
미등록 사용자	0	0	0%	0	0%	0%	0%	0%

- 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

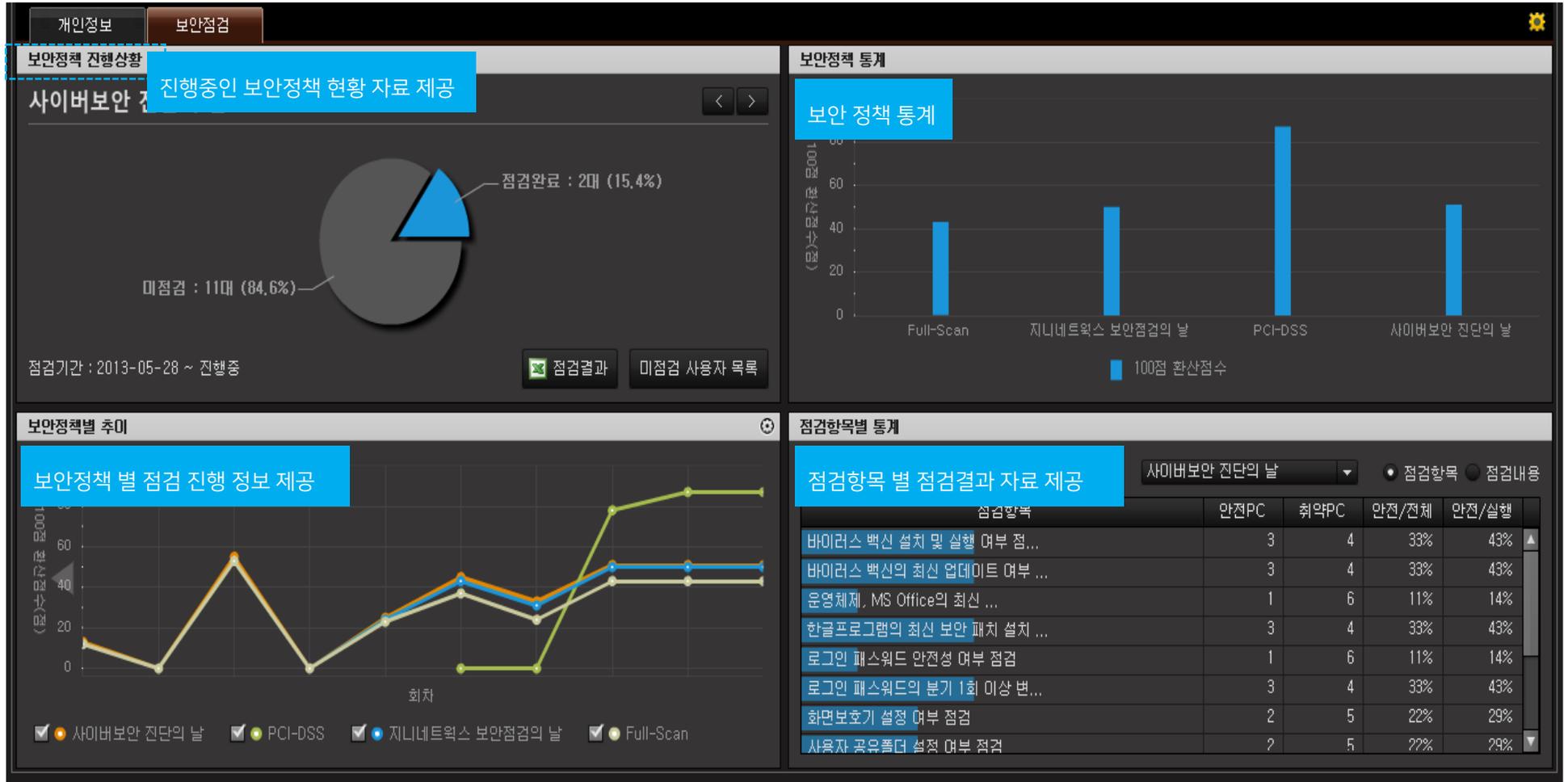


PDF 변환



# Genian GPI - 분석

- 보안점검 진행상황 분석을 위한 대시보드 제공



# Genian GPI - 분석

## ■ 중간관리자 / 관리자 계정 상세정보 표시 및 검색 기능

관리도구 > 관리자 권한 설정

작업선택

관리역할	관리역할 ID	적용된 관리자
슈퍼관리자	ROLE_ADMIN	admin (admin) admin1 (admin1) admin12 (admin12) admin32 (admin32) admin51 (admin51) admin52 (admin52) admin53 (admin53) admin54 (admin54)
PC점검 관리자	ROLE_SECURITY_ADMIN	pc점검관리자 (security)
부서관리자(조회전용)	ROLE_VIEW_ADMIN	부서조회 (view)
부서관리자	ROLE_VIEW_USER_MANAGE_ADMIN	부서관리자 (viewuser)

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

관리도구 > 관리자 계정 관리

표시는 필수입력 사항입니다.

관리자 등록 방식  등록된 사용자 중 관리자를 지정  신규 관리자 생성

관리역할

이름

관리자 아이디

비밀번호 변경  비밀번호 변경

관리자접속 허용 시간 00 시 00 분 - 23 시 59 분

관리자접속 IP범위   
관리자접속 IP범위를 제한합니다. (IP 또는 IP패턴을 사용하며, 복수개 입력시 ; 사용, 미입력시 제한 안 함)

이메일

일반전화  -  -

휴대폰  -  -

부서 권한 (조회가능 부서)

조회가능 부서를 할당하지 않으면 전체부서를 조회할 수 있습니다.  
부서가 할당되면 선택한 부서의 하위부서도 포함이 됩니다.  
부서관리자를 선택하면 **미등록 사용자 부서**가 조회가능부서에 포함되는데 부서관리자가 미등록 PC를 등록할 수 있도록 하기 위해서 입니다.

로그인 후 첫 페이지

부서트리 자동펼침  펼치지 않음  
부서가 많은 경우, 펼치는 시간이 오래 걸릴 수 있습니다.

# Genian GPI - 제어

## ■ 설정점수 미달 시 점검 창 닫기 제한 기능

보안정책 수정

보안정책명: [ ] 설명: [ ]

기본표시정책: [ ? ]

점검 안내 팝업창: 표시안함

점검 수행 옵션: 자동수행 (화면표시안함)

Agent 닫기 제한: 안전점수 미만일때 (닫기 불가능) [설정은]

항목	조건	설정	삭제

※보안정책이 생성되면 생성된 보안정책을 선택한 후, 우측 점검항목 목록에서 점검항목을 보안정책에 추가하세요.

Agent 관련 설정을 변경합니다.

Agent Icon 설정 옵션입니다.

Agent Tray Icon을 표시합니다.

바탕화면/시작메뉴/매토리비에 Agent 바로가기 Icon을 표시합니다.

Agent 설치 옵션입니다.

Agent를 Background로 설치합니다. [자세히](#)

숨기기

Agent창 닫기 제한 최상위 팝업 주기 옵션입니다.

최상위 팝업 주기: 5 분

- 설정한 시간주기로 Agent창을 최상위로 팝업합니다.

- 보안점검결과 점수 또는 취약점검항목 닫기 제한을 설정한 경우 동작하는 옵션입니다.

Agent 업데이트 체크 주기 옵션입니다.

Agent 업데이트 체크 주기: 4시간

- 최신 버전의 Agent가 존재하는지 체크하는 주기를 선택합니다.

미인증 Agent의 인증처리 방식을 선택하는 옵션입니다.

미인증 Agent일 경우에 Agent에서 인증창 팝업함

- 사용자 정보에 자동인증 IP 또는 MAC 정보가 포함되어 있지 않으면 자동으로 인증처리를 하지 못합니다.

- 미인증 상태일 경우 정책을 받을 수 없습니다.

윈도우 로그인 패스워드 점검시 사용자 입력 확인창 팝업 옵션입니다.

점검시 마다 팝업.

- 옵션을 선택하지 않으면 최초 점검시 1회 팝업 또는 사용자가 패스워드를 변경할 경우에 팝업됩니다.

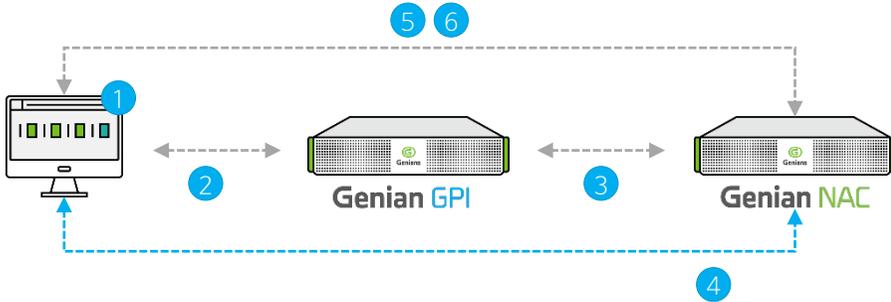
Agent 보안점검 보고서 보존기간 옵션입니다.

Agent 보안점검 보고서 보존기간: 1 일

- 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



1. GPI 점검수행
2. 점검수행결과 GPI서버 전송
3. 점검수행결과 NAC 전송
4. NAC정책에 따른 조치
  - 점수 이상 : 정상이용
  - 점수 이하 : 인터넷 차단 등의 접근제어 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	네트워크전체 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

외부시스템 연동 관련 설정을 변경합니다.

Agent 보안점검 점수를 NAC와 연동하는 옵션입니다.

NAC 127.0.0.1 로 보안점검 결과 점수를 전송합니다. 실패()로 구분하여 여러개의 NAC정책서버 IP를 지정할 수 있습니다. 지정된 서버마다 점수를 전송합니다.

원도우 최신보안패치 안전여부 판단기준

- NAC 윈도우 패치기준 (NAC에서 패치가 정상적으로 되어 있으면 안전으로 판단함.)
- Windows Update 기준 (Windows Update 사이트에 접속하여 패치여부를 검사해서 판단함.)

원도우 최신보안패치 업데이트 검사를 위한 프록시 설정

Proxy 서버  (ex: ip:port)

Agent 아이콘 통합 옵션입니다.

NAC와 Agent 아이콘을 하나로 통합합니다.

알림 메시지 보기(M)

- Genian NAC
- Genian 내PC지킴이
- 프로그램 정보(A)

사용자 지정...

## ▪ 단말사용자들의 보안사항 알림 기능

공지내용 설정 | **표준 설정** | 예외 사용자 설정 | 대상 사용자 설정 | 대상 그룹 설정

### 공지사항 설정

기간 : 2014-06-19 ~ 2014-06-26

노출주기 :  PC부팅시 마다  일 1회  주 1회  월 1회  년 1회

노출시각 :  :  이후  
지정된 시간 이후부터 노출됩니다.

노출방법 :  Agent 자동(강제)팝업  
 사용자 클릭 팝업  초까지 알람 메시지 표시 후 사라짐.  
0 : 사용자가 클릭할 때 까지 알람 메시지 표시  
00 : 00초 동안 알람 메시지 표시 후 사라짐.

공지내용 확인 (동의) 방법 :  동의함  만 표시  
 동의함  동의 안함  중 선택  
 메모 입력란 표시

정렬 :  왼쪽  가운데  오른쪽  양쪽

글자크기 :  15 미리보기-> 글자 크기

보안공지 삭제 | 보안공지 등록 | 보안공지 저장

### 팝업창 설정

팝업창 사이즈 :  모니터 전체  
 이미지 크기에 맞게 자동조절  
 사용자정의 크기

듀얼모니터 옵션 :  Dual 모니터 양쪽 전체  
 Master 모니터 전체  
 Slave 모니터 전체

팝업창 위치 :  중앙  
 사용자정의 위치

최상위 표시 :  최상위  상관없음

프로세스 강제종료 :  프로세스 강제 종료 불가능

확인 버튼 표시 시간 : 공지내용 팝업 후 확인 버튼 표시 시간 (초단위)  
 0 초 후 확인 버튼이 표시됩니다.

- 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

## ▪ 메시지 전송 기능

The screenshot displays the Genian GPI security management interface. On the left, there is a sidebar with a tree view showing '지니네트웍스' and '미등록 사용자'. The main area shows a summary of scan results: '전체PC : 10', '실행PC : 10 (100.0%)', '미실행PC : 0 (0.0%)', '안전PC : 3 (30.0%)', and '미등록PC : 0 (0%)'. Below this is a table of scan results with columns for '이름', '그룹(부서)', '컴퓨터이름', 'IP', '100점 환산점수', and '점검일시'. A dialog box titled '메시지전송' is overlaid on the table, containing the text '※선택된 사용자에게 메시지를 보냅니다.' and a '메세지입력' field. The dialog also has '알림창 확인 클릭시 보안점검 창 실행' and '보내기' and '취소' buttons.

이름	그룹(부서)	컴퓨터이름	IP	100점 환산점수	점검일시
<input checked="" type="checkbox"/> cindy3	지니네트웍스/dev	kyoungyoung-F	172,29,90,232	60	2014-06-19 10:41
<input type="checkbox"/> winVista32	지니네트웍스/dev	vista-32	172,29,68,32	85	2014-06-19 10:39
<input type="checkbox"/> win2000-64	지니네트웍스/dev	win2000-64	172,29,68,54	85	2014-06-19 10:38
<input type="checkbox"/> win2			172,29,68,12	75	2014-06-19 10:38
<input type="checkbox"/> win2			172,29,68,64	75	2014-06-19 10:39
<input type="checkbox"/> win2			172,29,68,55	75	2014-06-19 10:37
<input type="checkbox"/> win7			172,29,68,74	75	2014-06-19 10:38
<input type="checkbox"/> win7			172,29,68,72	60	2014-06-19 10:44
<input type="checkbox"/> win2			172,29,68,52	85	2014-06-19 10:38
<input type="checkbox"/> win2			172,29,68,53	75	2014-06-19 11:16

- 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)

관리도구 > 관리자 계정 관리

\* 표시는 필수입력 사항입니다.

관리역할 + 슈퍼관리자

이름 + 이창수

관리자 ID + test

비밀번호 변경  비밀번호 변경

로그인시 비밀번호 변경  로그인시 비밀번호 변경

Agent 인증가능 여부  Agent 인증가능

2단계 인증  OTP

'설정 > 환경설정 > WEB 콘솔 > 2단계 인증 사용여부' 항목에서 관련설정이 활성화 되어야 합니다.

관리자접속 허용 시간 00 시 00 분 - 23 시 59 분

관리자접속 IP범위 입력 예) 172.29.90.100,172.29.91.0/24,172.29.50.10~172.29.50.30  
관리자접속 IP범위를 제한합니다. (IP 또는 IP패턴을 사용하며, 복수개 입력시 ',' 사용, 미입력시 제한 안 함)

이메일

- 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

관리도구 > 관리자 계정 관리

\* 표시는 필수입력 사항입니다.

관리역할 + 슈퍼관리자

이름 + 이창수

관리자 ID + test

비밀번호 변경  비밀번호 변경

로그인시 비밀번호 변경  로그인시 비밀번호 변경

Agent 인증가능 여부  Agent 인증가능

2단계 인증  SMS

'설정 > 환경설정 > WEB 콘솔 > 2단계 인증 사용여부' 항목에서 관련설정이 활성화 되어야 합니다.

관리자접속 허용 시간 00 시 00 분 - 23 시 59 분

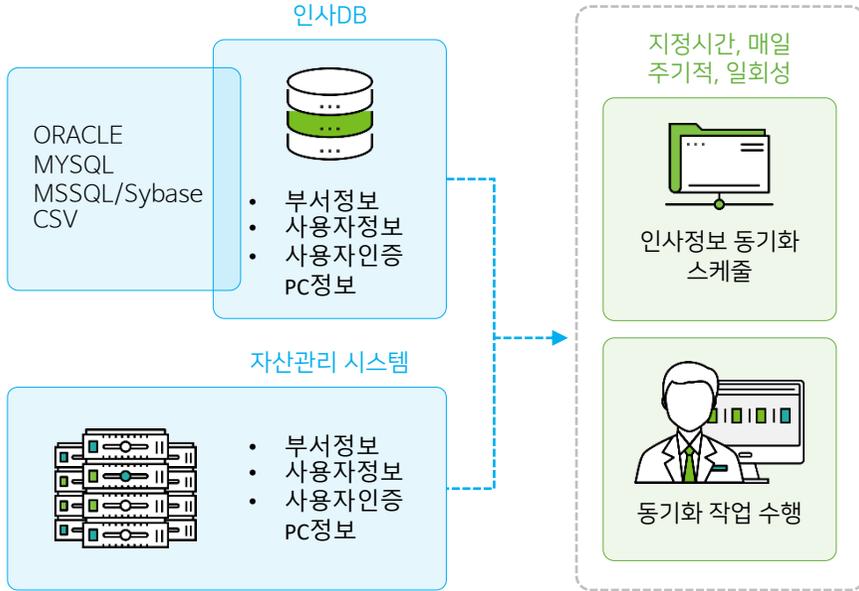
관리자접속 IP범위 입력 예) 172.29.90.100,172.29.91.0/24,172.29.50.10~172.29.50.30  
관리자접속 IP범위를 제한합니다. (IP 또는 IP패턴을 사용하며, 복수개 입력시 ',' 사용, 미입력시 제한 안 함)

이메일

- 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



최초 등록 2016-04-14 09:00:22      가동률 98%

인증사용자 이철(igr)      최근 사용자인증 2016-04-14 09:00:51

현재 인증상태 비활번호인증      웹브라우저

이름	부서명	IP	접수	역자	부서명교 대비	접수명교 대비	동시성
안호국 Win7	사면 1	192.168.1.231	72	1	▲ 24	▲ 16	2012-05-17
안호국	사면 1	192.168.1.43	60	2	▲ 17	▲ 16	2012-05-16
김태호	사면 1	172.29.100.69	52	3	▲ 1	▲ 16	2012-05-17
이현호 w7	CAM	192.168.1.132	48	4	▲ 32	▲ 24	2012-05-16
이현호 w7	CAM	192.168.1.238	30				2-05-16
김윤영_jeon	CAM	192.168.1.201	30				2-05-17
김유진	CAM	192.168.1.215	29				2-05-16
김윤영7	전략사업부	192.168.1.78	26	7	▲ 10	▼ 4	2012-05-16
김태호	사면 1	172.29.114.141	19	9	▼ 39	▼ 14	2012-05-17
노영재	인프라보안사업부	192.168.1.41	0	10	0	▼ 24	
이종희	인프라보안사업부	172.29.100.73	0	10	0	▼ 24	
yhm_w7_32	CAM	192.168.1.232	0	8	▼ 15	▼ 24	
김윤영_je	전략사업부	192.168.1.201	0	10	▼ 10	▼ 24	2012-05-17
이현호 w7	CAM	192.168.1.236	0	10	▼ 15	▼ 24	

부서명 입력 후 Enter

이름	부서명	IP	접수	역자	부서명교 대비	접수명교 대비	동시성
안호국 Win7	사면 1	192.168.1.231	72	1	▲ 24	▲ 16	2012-05-17
안호국	사면 1	192.168.1.43	60	2	▲ 17	▲ 16	2012-05-16
김태호	사면 1	172.29.100.69	52	3	▲ 1	▲ 16	2012-05-17
이현호 w7	CAM	192.168.1.132	48	4	▲ 32	▲ 24	2012-05-16
이현호 w7	CAM	192.168.1.238	30				2-05-16
김윤영_jeon	CAM	192.168.1.201	30				2-05-17
김유진	CAM	192.168.1.215	29				2-05-16
김윤영7	전략사업부	192.168.1.78	26	7	▲ 10	▼ 4	2012-05-16
김태호	사면 1	172.29.114.141	19	9	▼ 39	▼ 14	2012-05-17
노영재	인프라보안사업부	192.168.1.41	0	10	0	▼ 24	
이종희	인프라보안사업부	172.29.100.73	0	10	0	▼ 24	
yhm_w7_32	CAM	192.168.1.232	0	8	▼ 15	▼ 24	
김윤영_je	전략사업부	192.168.1.201	0	10	▼ 10	▼ 24	2012-05-17
이현호 w7	CAM	192.168.1.236	0	10	▼ 15	▼ 24	

인증 단말목록 연동

- SSO 인증 기능을 제공하여 단말 사용자 업무 효율성을 증대
- 기존 구축된 인사 DB 시스템 및 자산관리시스템, 정보 보안포털 서버의 필요정보를 스케줄에 따라 사용자 인증 PC 정보와 동기화 작업 수행
- 사용자 ID 및 PC의 MAC 정보로 개인 PC 인증처리, 자산관리시스템과 해당 정보 연동

## ■ Genian GPI DB백업 기능

→ 백업수행

DB를 자동으로 백업합니다. (시간 04 : 00 )

저장장치타입 **로컬디스크**   
저장장치 타입을 선택합니다.

- 사용자ID   
저장장치에 접근가능한 사용자의 ID를 설정합니다.

- 사용자 비밀번호  확인   
저장장치에 접근가능한 사용자의 비밀번호를 설정합니다.

백업저장장치경로   
마운트할 백업장치 경로를 설정합니다.  
외부저장장치 설정예: /dev/sdc1 (포맷형식이 fat인 외부저장장치만 사용가능합니다.)  
CIFS저장장치 설정예: \\\*\\192.168.1.73\\backup  
NFS저장장치 설정예: 192.168.1.73/backup  
FTP SERVER 설정예: ftp 서버에 ID/PASSWORD은제시 위 로그인 정보란에 사용자정보 기입, SERVER 주소가 ftp://gen.com 이면 gen.com만 기입, 로컬디스크의 경우는 설정하지 않습니다.

→ 백업파일 다운로드

**백업 목록** 로컬디스크에 백업된 파일목록에서 선택한 백업파일을 다운로드 할 수 있습니다.

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

+ **속이기**

→ 비인가 프로그램 인가여부 지정

Agent로부터 수집되는 프로그램을 **미분류**로 자동 지정합니다.  
인가  
비인가

→ 보안점검 일회성스케줄 자동 삭제

6  일 이전 보안점검 일회성스케줄은 자동 삭제합니다.

→ 미접속 Agent 삭제

60  일 동안 Agent가 서버에 접속하지 않으면 Web UI에 표시되지 않도록 삭제 처리합니다.

→ 보안점검결과 상세정보(안전/취약 여부)에 대한 조회 가능한 회차의 수를 설정합니다.

0  개의 회차 데이터만 조회할 수 있습니다.  
'0'을 선택할 경우 모든 데이터를 조회할 수 있습니다.(결과 조회시 검색 속도가 느려질 수 있습니다.)  
기준이 지난 회차는 BACKUP 테이블로 이동되며 UI에서 조회를 할 수 없습니다.

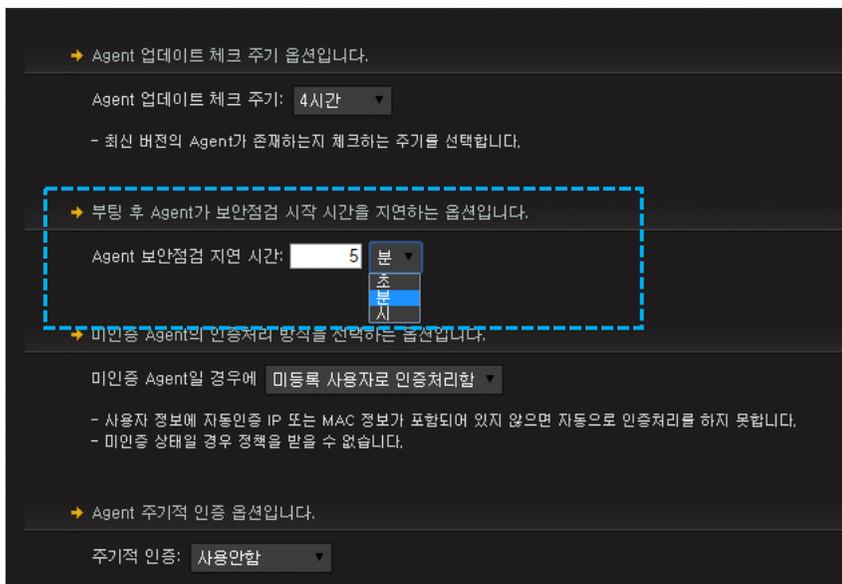
→ 장비 콘솔 아이디/비밀번호를 설정합니다.

장비 콘솔 아이디 **admin**  
콘솔 접속을 위한 아이디를 설정합니다.

장비 콘솔 비밀번호  확인   
장비 콘솔 접속을 위한 비밀번호를 설정합니다. (알파벳 문자, 숫자 혼용 9자 이상으로 설정하세요.)

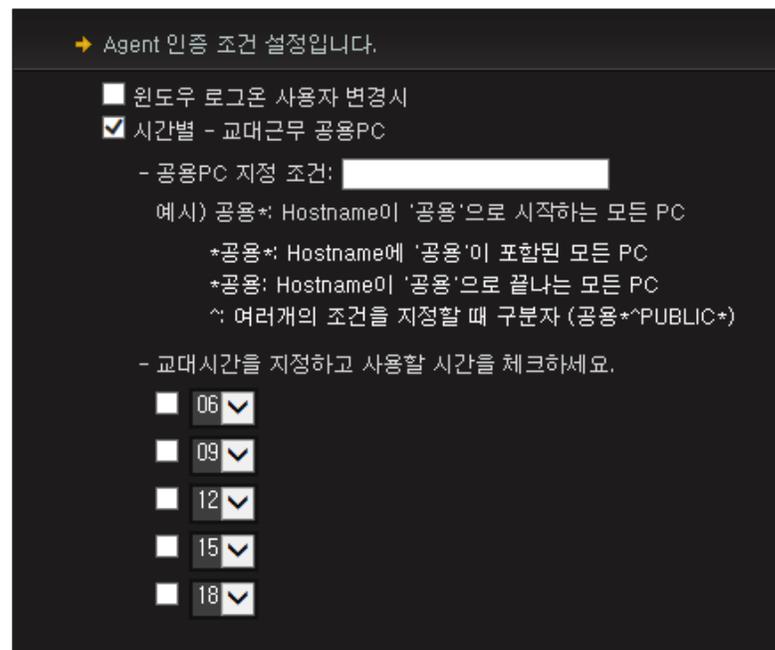
장비 콘솔 접속IP범위 **입력 예) 172.29.90.100,172.29.91.0/24,172.29.50.10~172.29.50.30**  
장비 콘솔 접속IP범위를 제한합니다. (IP 또는 IP패턴을 사용하며, 복수개 입력시 ; 사용, 미입력시 제한 안 함)

## ▪ 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

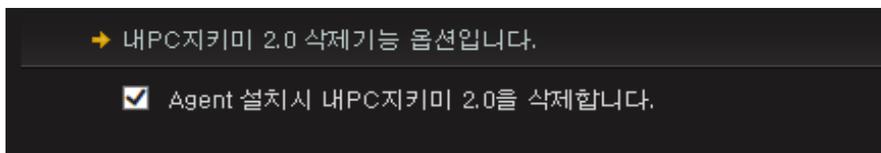


- 교대근무자 및 공용PC 점검기능 지원
- 특정시간(근무교대시간)에 따른 점검 지원

# Genian GPI

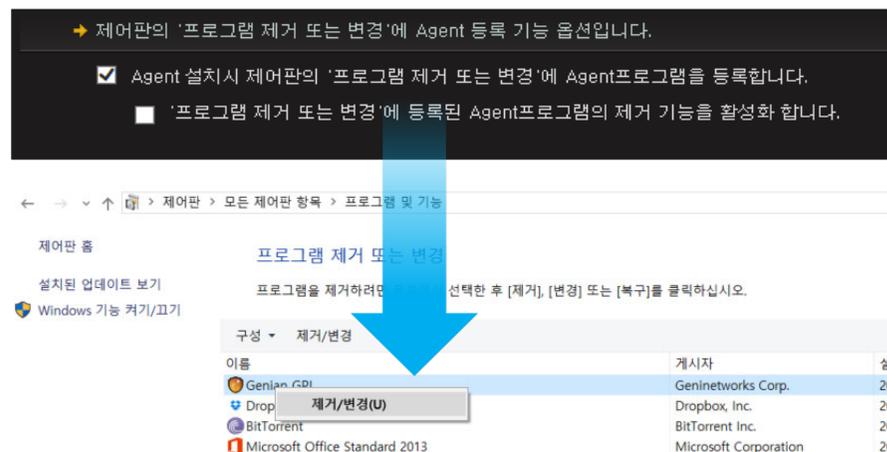
## ▪ GPI V2.0 자동 삭제 기능

기존에 설치된 GPI V2.0 자동삭제 기능을 통해 별도의 삭제 절차없이 자동 삭제 할 수 있음



## ▪ Agent 임의 삭제 불가

1. 관리자 설정에 의한 사용자 수동 프로그램 삭제 옵션 제공

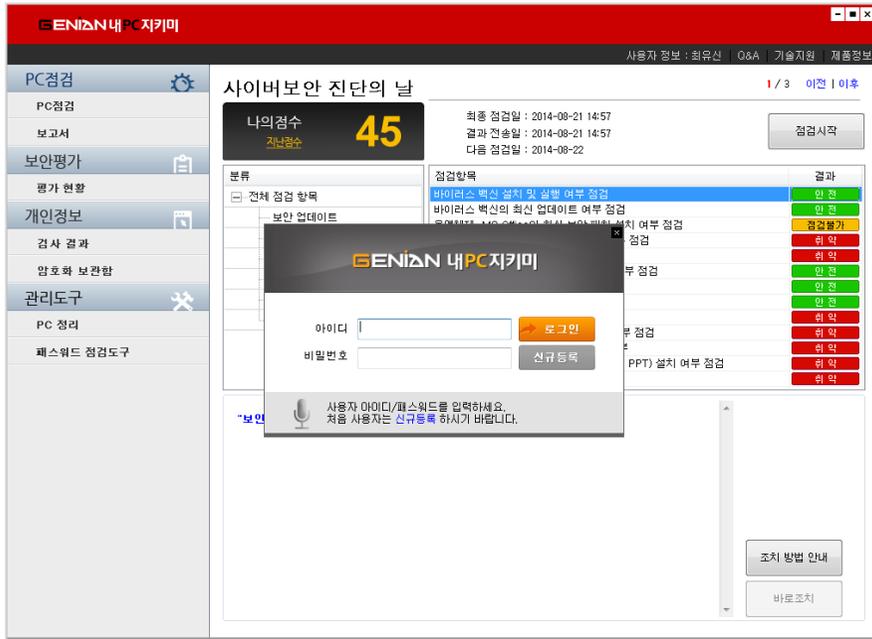


2. 삭제 프로그램(클리너)을 통한 Agent 삭제



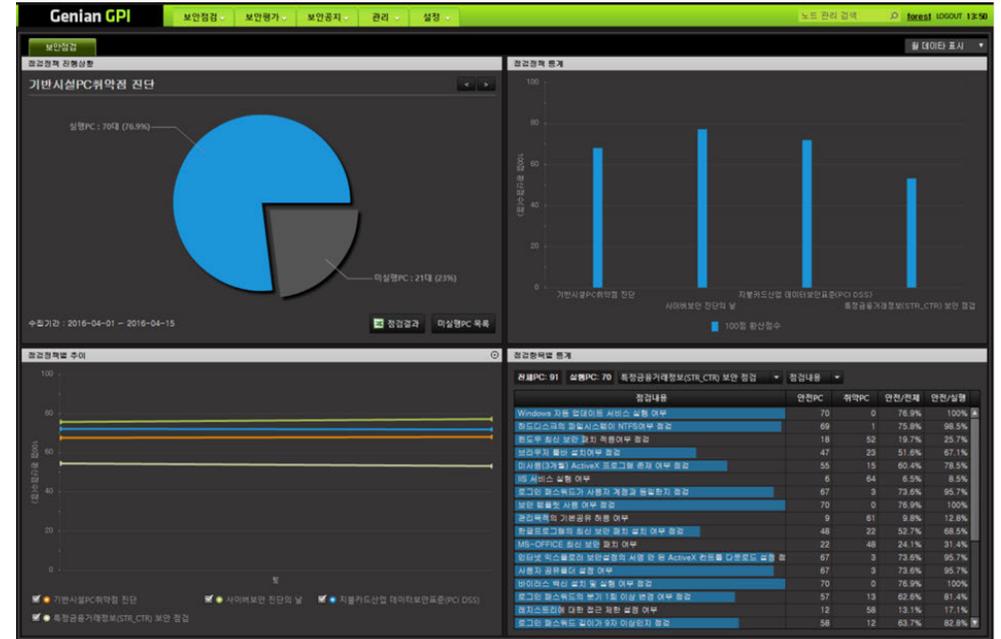
3. 두 가지 삭제 방법 외 사용자 임의 삭제 불가

## ■ 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

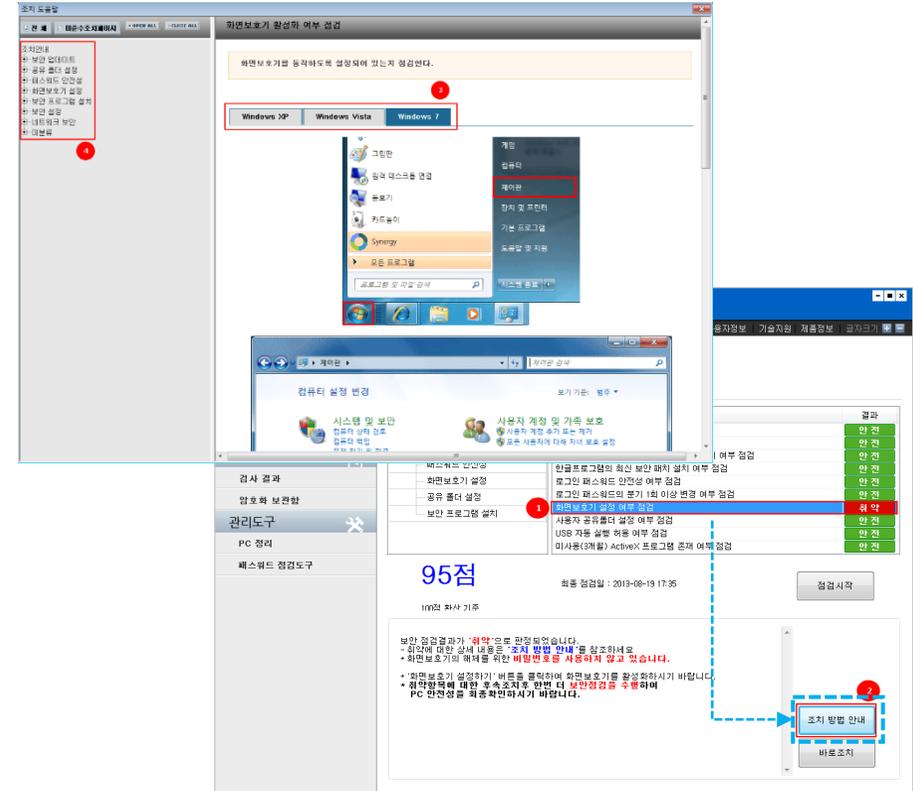
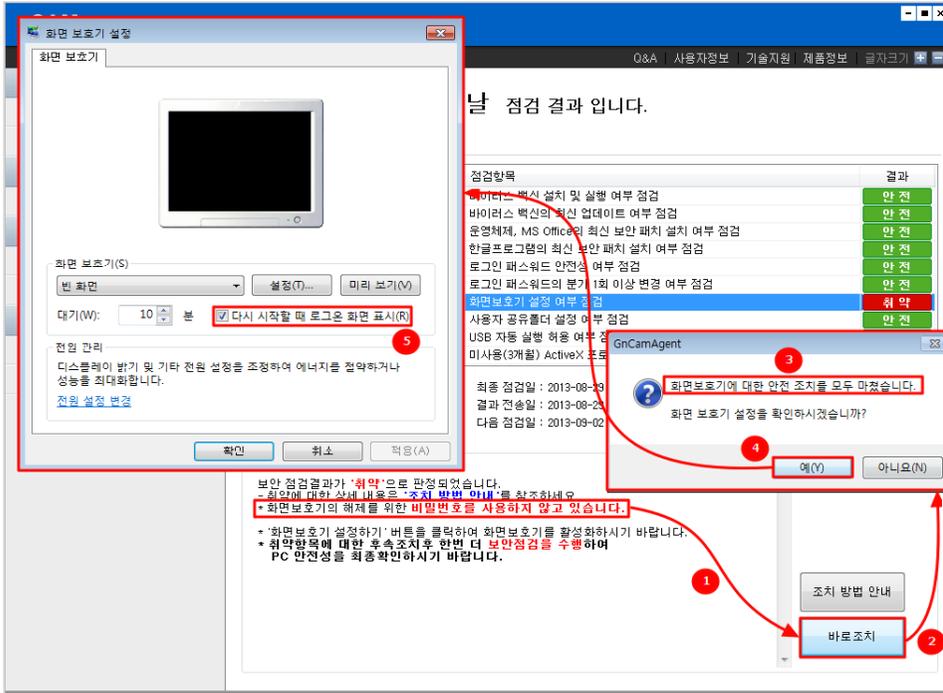
## ■ 대시보드



- 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

The image displays three overlapping screenshots of the Genian GPI interface. The top screenshot shows a security check result table with a blue header bar. The middle screenshot shows the same interface with an orange header bar. The bottom screenshot shows the interface with a red header bar. A separate window titled 'Web UI 관련 설정을 변경합니다.' (Change Web UI related settings) is shown on the right, containing a table for setting score thresholds for different security states.

상태	점수	설정
안전	0061c4	80 점 이상
보통	ff9000	50 점 이상
취약	cb0000	보통에 설정된 점수 미만

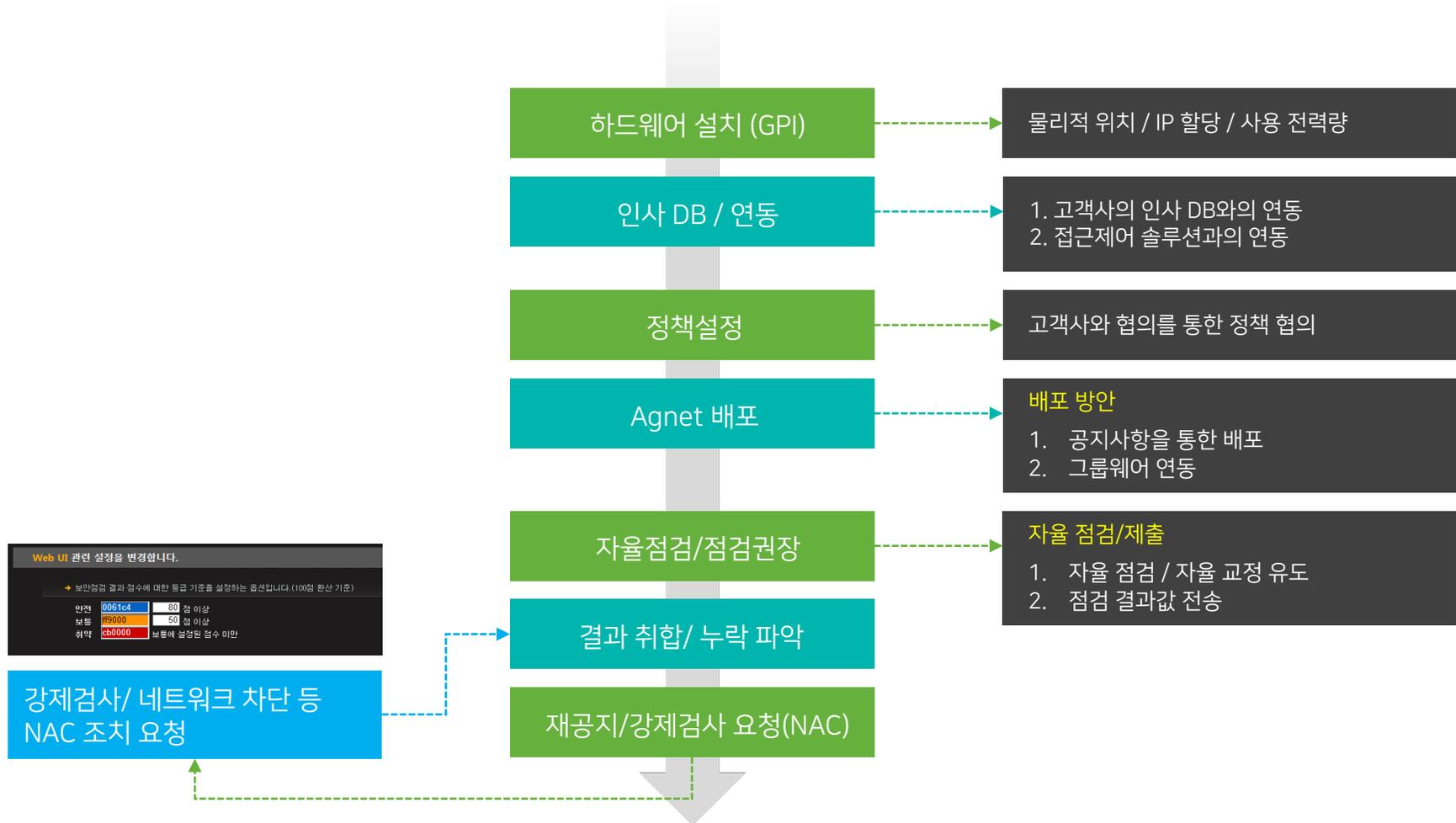
• 관리자 설정을 통해 점수에 따라 사용자 PC 점검창의 상태바 색상 변경 기능 제공

Part2,  
Genian NAC와  
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

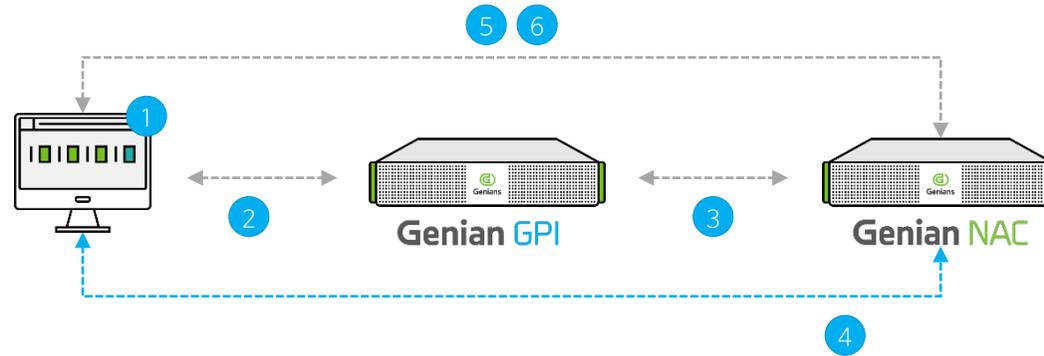


## • NAC의 관리 화면의 내PC지키미 단말의 점수 화면

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



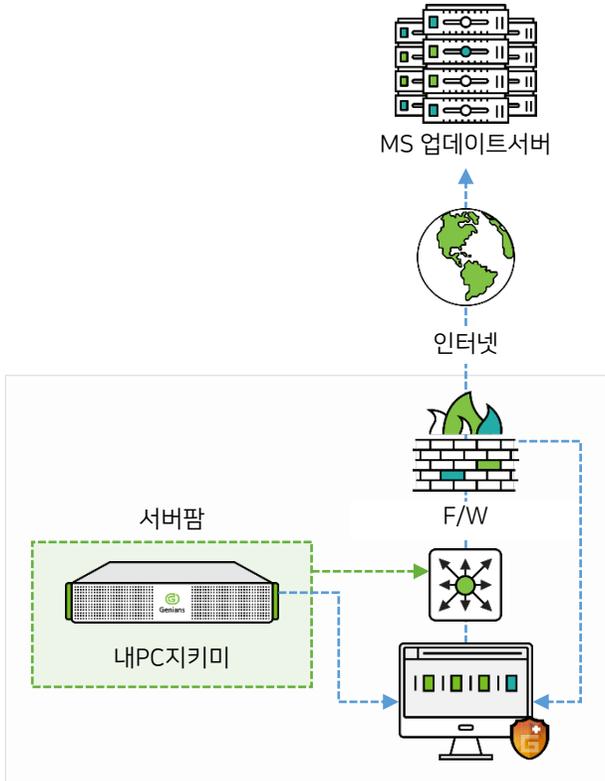
- ① GPI 점검수행
- ② 점검수행결과 GPI서버 전송
- ③ 점검수행결과 NAC 전송
- ④ NAC정책에 따른 조치
  - 점수 이상 : 정상사용
  - 점수 이하 : 인터넷 차단, 사용자 알람 통제 기능 수행
- ⑤ 재점검을 통해 점수 상승
- ⑥ 실시간 NAC로 점수 전송 후 차단 해제

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

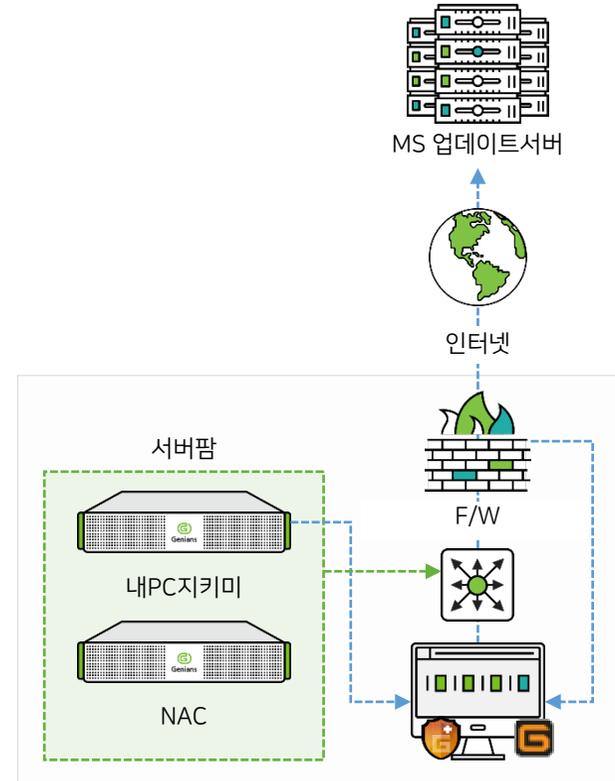
## OS/MS OFFICE 업데이트 점검 항목 연동

MS 업데이트서버를 이용한 OS/MS OFFICE 패치 확인



- ① 내PC지키미에서 GPI AGENT에게 OS/MS OFFICE 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 OFFICE 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



# Part3, 별첨



# 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 가능
14. 보안USB 설치 여부 점검 가능
15. 비인가 프로그램 설치 여부 점검
16. 사용자PC 프로세스 목록 수집가능

### 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 로그인 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 아크로벳 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)8084-9770

[sales@genians.com](mailto:sales@genians.com)