Upgrade Your Expectations

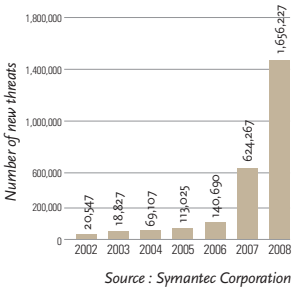
Genian NAC

Network Access Control

geni NETWORKS

1 이제 내부(Internal Network) 보안 관리를 위한 전문 솔루션이 필요 합니다.

Today's Challenge



Source : Symantec Corporation

Threats

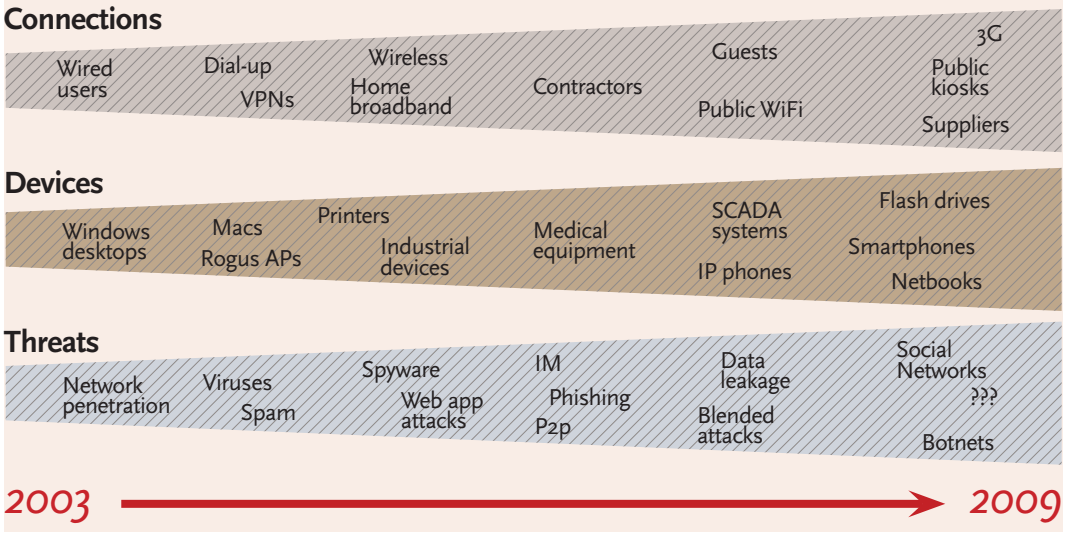
최근 사이버 위협의 주 목적은 금전취득에 있습니다. 서비스거부공격(DoS)과 개인 및 기밀정보를 탈취하기 위한 악성코드(트로이 목마, 웜 등)의 감염 및 확산이 가장 큰 보안위협이 되고 있습니다. 보호의 대상이 사용자 및 내부자원, 콘텐트(Contents)등으로 이동하면서 방화벽, IPS 등의 네트워크보안 제품 및 백신(Vaccine)등을 통한 대응이 한계를 드러내고 있습니다.

Devices

다양한 기기들이 네트워크에 접속을 시도하고 있습니다. 랩톱 컴퓨터를 이용한 업무처리는 점차 사용자들에게 외면 당하고 있으며 넷북 또는 스마트폰이 보편화 되고 있습니다. 이미 기업에서는 많은 직원들이 각자의 영역에서 다양한 기기들을 사용하여 고유의 업무를 수행합니다. 스마트폰, PDA, POS(Point Of Sales) 단말기, VoIP 전화기 등이 네트워크에 접속하여 업무의 생산성을 높여 줍니다. 그러나 비 인가 단말의 증가, 권한 설정 및 적용의 어려움 등으로 보안의 위협 또한 증가하고 있습니다.

Connection

많은 기업의 네트워크는 전용선(Lease Line)과 이더넷(Ethernet)에만 국한되지 않습니다. 이미 AP(Access Point)를 통한 무선(Wireless)네트워크 접속은 보안에 대한 이슈가 정의되기도 전에 보편화 되었고 우리는 Wibro 나 Hot Spot 서비스 등을 이용해서 길거리에서도 손쉽게 네트워크로의 접속이 가능합니다. 이러한 네트워크의 개방은 보다 쉬운 접속(Connection)을 보장하지만 안과 밖이 구별되지 않은 상황에서 우리를 보다 큰 위협에 빠뜨릴 수 도 있습니다.



비인가/장치 제어
- 비인가 저장매체 제어
- 비인가 통신장치 제어
- IP 변경 관리 / 제어
- IP / PC 실명제

역할기반 접근제어
- 단말 보안상태에 따른 접근 제어
- 사용 용도별 접근 제어
- AD, 인사DB연동으로 직무 별 접근 권한 부여

Compliance 준수
- 패치 및 백신 미 설치 사용자 네트워크 통제
- 사용자 인증을 통한 권한 부여
- 유해 트래픽 차단
- 불법무선경로 탐지 및 대응

검증된 솔루션
- 국내 점유율 1위
- 최다 레퍼런스 보유
- Agent / Agentless 지원
- 효율적인 운영/관리

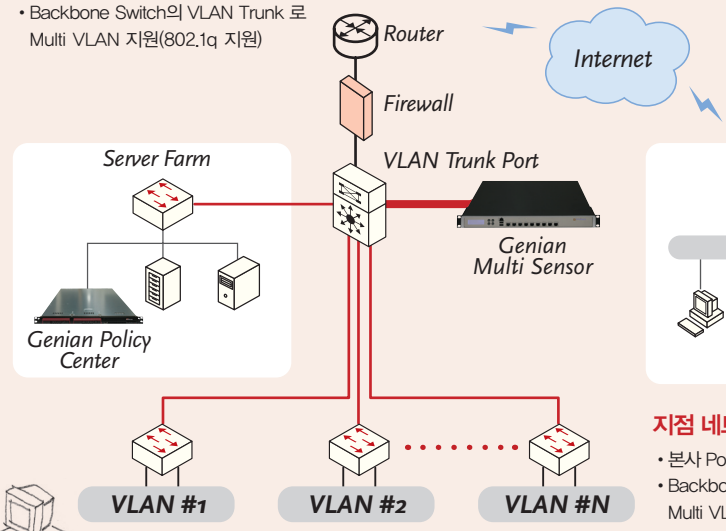
Genian NAC

● Genian NAC는 End Point Security 강화, 내부네트워크 제어 및 통제, 내부정보보호 체계 수립을 위한 가장 강력한 솔루션 입니다.

2 Genian NAC는 내부 보안 관리를 위한 가장 효과적인 솔루션 입니다.

● 단일 및 다(多)지점 환경에서도 기존 네트워크의 변화 없이 적용이 가능합니다.

단일 네트워크 환경
- Policy Center와 Sensor로 구성
- Backbone Switch의 VLAN Trunk 로 Multi VLAN 지원(802.1q 지원)



지점 네트워크 환경
- 본사 Policy Center 및 지점 별 Network Sensor
- Backbone Switch의 VLAN Trunk로 Multi VLAN 지원(802.1q 지원)

3 내부 보안 관리를 위한 가장 효과적인 구성과 기능을 제공합니다

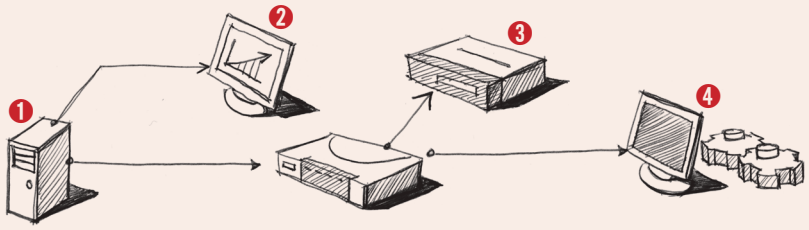
● 센터(Center), 센서(Sensor), 에이전트(Agent)로 구성되어 빈틈없는 보안관리 환경을 구축합니다.

❶ 정책 관리 서버
- NAC 차단서버와 Agent에 대한 정책 및 로그 관리
- PC 보안성태 및 사용자 역할 기반의 정책 수립
- 차단 서버로부터 수집된 정보 분석
- 차단 서버 및 Agent 동작 설정 기능

❷ 관리자 콘솔(Console)
- 웹(Web) 기반 보안정책 설정 및 감사, 모니터링
- 장비 별 CLI(Command line interface) 지원
- Dashboard 제공 및 주요 이벤트 발생 시 알람기능

❸ 차단 서버
- 네트워크 상의 장비 및 사용자 통제 기능 수행
- IP, MAC, OS등 노드 정보 수집 및 자동 분류
- Web 기반의 사용자 인증 기능
- Honey Pot 운영으로 유해 traffic 감지 및 차단

❹ Agent
- 단말(PC)의 보안 정책 준수 여부 점검 및 조치
- 패치자동적용 및 자산관리 기능 수행
- 사용자 PC 취약성 점검 및 정보 확인 기능

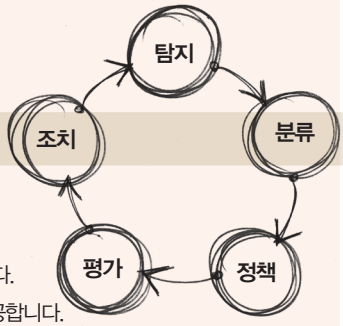


● Genian NAC 사양 및 주요 기능

구분	기능	사양
운영환경	정책관리 서버 (센터) 관리자 콘솔 차단 서버 (센서) 에이전트	• 자체 OS (이중화(HA) 구성 지원) • Windows 2000 이상 • 자체 OS (이중화(HA) 구성 지원) • Windows 2000 이상(Windows 7포함) 및 Windows Mobile 6.0 이상
	동작 방식(센터, 센서) 동작 방식(Agent)	• Out of Band 및 Mirror Mode 지원 • Non Driver, No Control 기반 단말기 정보 수집
네트워크 접근 통제	가상 방화벽	• Agent설치 없이 IP 단말기의 네트워크 접근제어
	IP 관리 기능	• User ID, IP, MAC을 이용한 비 인가 단말 사용 탐지 및 차단 • IP 충돌 방지 기능을 이용한 방화벽, 라우터 등 주요 장비 보호
	보안 정책 운용	• 사용자 정보, 단말기 정보, 네트워크정보를 이용한 보안 정책 수립 • 보안 정책 위반 사용자 및 단말기의 네트워크 사용 통제
	유, 무선 사용자 인증	• 유 · 무선 사용자 대상
자산 보호	AND(Active Network Discovery)	• 네트워크 내의 모든 IP 장비의 자동 검출 및 식별을 통한 관리 환경 구축
	비 인가 장비 및 서비스 탐지	• 주요 네트워크 서비스(DHCP, SMTP, HTTP 등)의 불법 사용 탐지 및 대응
	네트워크 우회 경로 탐지	• 비 인가 네트워크 경로 탐지 및 정보 유출 등 잠재위협 대응
	패치관리기능(PMS)	• OS 및 주요 Application 패치의 중앙관리 (On / Off-Line 지원) • 필수 S/W의 강제 배포 및 설치
	데스크톱 관리기능(DMS)	• 사용자정보, H/W 정보, S/W 정보, 설정 정보의 수집 및 관리(조회 / 설정 / 감사) • 주요 매체(CD-ROM, USB, Wireless 등)의 관리(조회 / 설정 / 감사)
네트워크	악성 트래픽 탐지	• 허니팟(Honey Pot)을 통한 악성 트래피 탐지 및 의심 단말기 통제
	Zero-Day 공격 방어	• 행위(Behavior)기반 탐지를 통한 잠재위협 탐지 및 통제
	감염 단말 통제	• 악성 트래픽 발생 등 감염 추정 단말의 네트워크 격리 • 백신 미 설치(사용) 단말의 네트워크 사용 통제
인증	CC(Common Criteria)	• 국정원 EAL2
	소프트웨어품질인증(Good Software)	• 한국정보통신기술협회(TTA)

Why Genian NAC?

왜 Genian NAC를 선택해야 할까요?



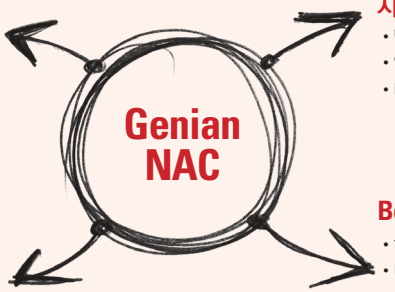
1 완벽한 내부 보안 관리의 완성 입니다.

- 모든 기능은 자동화 되고 상호 보완되어 관리자의 반복 작업을 획기적으로 줄여 줍니다.
- 자원의 검색(탐지)➔분류➔정책적용➔감사, 평가➔조치 의 Full Cycle Mgmt.를 제공합니다.
- 사용자, H/W, S/W, 시간 등 다양한 정보를 이용하여 누락 없는 보안 정책의 운용이 가능합니다

2 내부 보안 관리에 꼭 필요한 기능을 제공합니다.

비용절감
- 네트워크 장비교체 / 구성변경 불필요
- No Single point of failure
- No Network Latency

End-Point Security 강화
- 사용자 PC의 취약 요소 제거
- 필수 S/W 배포 및 업데이트
- 사용자 MS Patch에 대한 강제성 제공
- 최신 MS Patch 업데이트
- 백신 강제화 및 최신업데이트 유지



사용자 별 네트워크 제한
- 단말 / 사용자 역할에 따른 인증 지원
- 인증여부에 따른 사용자 네트워크 제한
- 비인가 사용자 네트워크 차단

Behavior-based 트래픽 제어
- 허니팟을 이용한 악성 트래픽 탐지 및 격리
- 네트워크 이상행위 및 변경사항 탐지

3 다양한 솔루션과의 연동을 통한 완벽한 통합 보안 인프라 구축이 가능해 집니다.

표준

외부 솔루션과 연동을 위한 Syslog, SNMP 지원

백신

AhnLab HAURI

ESM, TMS

SPIDER TM NOWCOM

SSO

KSIGN

기타

eWalker 3

geni NETWORKS

Upgrade Your Expectations

지니네트웍스(주)는 보안분야 최고 전문가 그룹입니다

***최고 기술 보유**
- 관련 특허 5건 및 CC인증, GS 인증 등 보유
- 10년 이상 경험의 네트워크 보안 Sales / R&D / Planning

***최다 구축 실적**
- 2009년 프로젝트 수행 실적 1위
- 우정사업본부, 해군, 공군, 현대카드, 하이마트 등 190여 고객사 확보

***최고 사업 추진**
- 자체 프로젝트 수행 방법론 보유
- 지역 별, 수준 별 파트너 체제 구축을 통한 전국 규모의 프로젝트 진행 및 본사 수준의 지원 역량 보유

파트너

지니네트웍스(주)

www.geninetworks.com

경기도 성남시 수정구 수진동 587번지 성남벤처빌딩 102호

Tel 031-721-3870 **Fax** 031-721-3910