Cyber Security Conference 2021

SAMSUNG SDS

차세대방화벽을 이용한

안전한 원격근무 환경 구성

조원용 이사 시큐아이

AGENDA

1. 배경
2. 원격 근무 확산에 따른 보안 관리자의 고민
3. Zero Trust Network 란 ?
4. 차세대 방화벽을 이용한
   Zero Trust Network 구성 방안
5. 차세대 방화벽을 이용한 안심 재택 구축 방안

배경

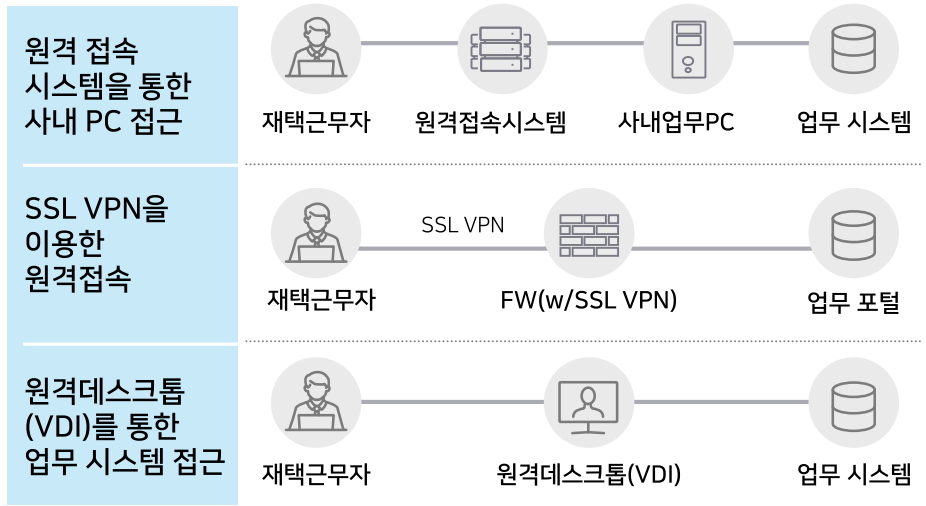
COVID-19 확산에 따른 외부에서의 업무의 연속성을 보장할 수 있는 환경 구축 필요

'19년 대비 '21년 원격 근무 41% 증가 예상
(Gartner Forecast Analysis, 2021.1.5)

원격 근무 확산에 따른 보안 영역의 확대	원격 근무자에 대한 위협 증가	모바일 환경을 통한 업무 이동성 증가
✔ 장소와 환경에 제약 없이 업무 연속성 보장 필요	✔ 외부 접속 단말에 대한 보안성 확보 필요	✔ 업무 이동에 따른 정책 적용 시간 최소화 필요

문제점 및 보안 이슈 사항

재택근무 구성 형태



1 외부 단말기의 물리적 통제 미흡

단말기의 분실·도난이나 타인의 정보 훔쳐보기 시, 단말기내 데이터가 유출·노출

2 안전하지 않은 네트워크 사용

공용 네트워크 사용에 따른 도청, 중간자 공격(MITM)으로 중요 정보 유출

3 악성코드 감염에 따른 네트워크 침해

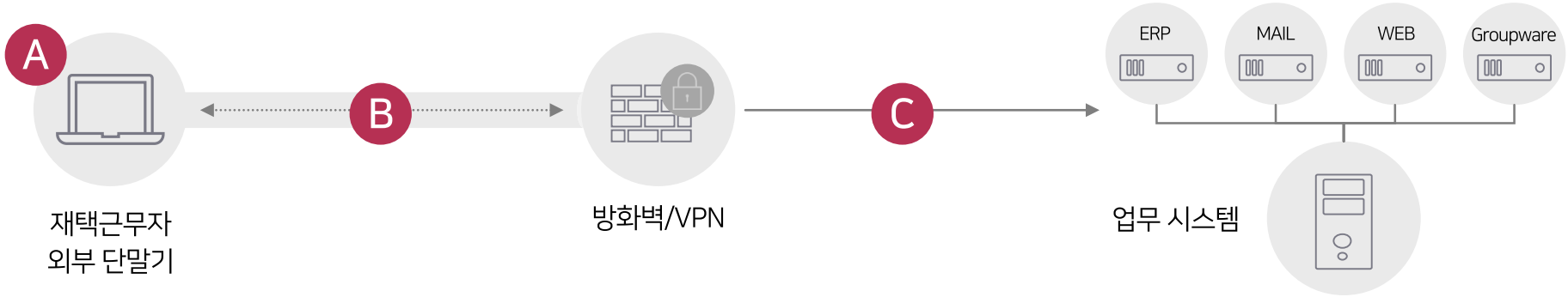
악성코드에 감염된 외부 단말기로 내부 네트워크 연결 시 시스템 침해 가능

4 내부 자원에 대한 원격접근 위협

내부 자원에 대한 외부에서의 비인가 접근 등 보안 위협

배경

원격 근무 확산에 따른 보안 고려 사항



구분	A 외부 단말기 보안관리	B 인증 및 통신회선	C 내부망 접근 통제
고려 사항	**단말 보안 설정, 정보 유출 방지 적용** • 백신 설치, 최신 운영체제/패치 적용 • 로그인 비밀번호 및 화면보호기 설정 • 화면/출력물 등에 대한 정보 유출 방지 적용 **추가 보안통제 적용을 통한 보안성 향상** • 취약/비인가 S/W 사용 금지, 파일 송/수신 차단, 보안설정 임의 변경 차단, 내부 자료 암호화 적용, 외부 저장장치 사용 금지 등	**Multi-Factor 인증 및 인증 실패 조치** • 다중 인증을 통한 사용자 인증 강화 1차 인증 (ID/PW) + 2차 인증 (OTP) + 3차 인증 (인증서) • 일정 회수 이상 인증 실패 시 접속 차단 **가상사설망(VPN)의 통신 보안 수준 확보** • 통신구간 암호화, 내부망 접속 시 인터넷 연결 차단, 접속 유효 기간 설정 등	**최소한의 연결 허용** • 필요 시스템 접근 IP/Port만 허용 **원격 접속 기록 저장** • 원격 접속 사용자 정보, 접속 일시, 접속 시스템 정보 기록/관리 **원격 접속 시 사전 보안 검사** • 접속 단말의 정보보호 필수 통제 사항 적용 여부 등에 대한 확인

※ "금감원 재택근무 보안 안내서" 주요 내용

원격 근무 확산에 따른 보안 관리자의 고민

보안 영역 확대에 따른 보안 체계는 어떻게 하는 게 좋을까 ?

인가된 사용자에 의한 접근인가 ?
인사정보 연동, 다중 인증 필요

보안 적용에 따른 업무 지연은 없을까 ?
수동 방식이 아닌 내부 시스템 연계 정책 관리 필요
(인사 정보와 사용자 연계를 통한 정책 연동 등)

사용 단말은 안전한가 ?
안전한 단말에 대해서만 접근 허용 필요

정보 유출은 어떻게 방어하지 ?
PC통제 및 문서 보안 적용을 통한 사전 대응 필요
(매체제어, DRM, 캡처 방지, 출력 통제 등)

업무용 트래픽만 허용하고 있나 ?
IP/Port 기반이 아닌 애플리케이션 기반 제어 필요

새로운 보안 모델 필요

사용자, 단말 정보 기반 최소한의 접근 허용 ***Zero Trust Network***

Zero Trust Network 란 ?

기존 방화벽의 한계

Zero Trust
관점 방화벽
제품 요구 사항

신원 확인

- **단순 ID/PW 기반 사용자 인증**
  - ID/PW 도용에 따른 접근 허용 가능
- **IP 기반 정책**
  - 사용자 IP변경에 따른 정책 변경 필요 (IP ≠ 사용자)

※ 인사 정보와 연계한 사용자 기반 접근제어 정책 지원 필요 (w/Multi-Factor 인증)

디바이스 신뢰성 확인

- **단말 상태 확인 불가**
  - 악성코드에 감염된 단말로 인한 내부 전파 위험
- **필요 시 별도 단말 보안 솔루션 필요**
- **이원화에 따른 불편함 발생**
  - 단말 관리와 방화벽 정책 이원화에 따른 불편함 발생

※ 단말의 상태 정보와 연계한 접근제어 정책 지원 필요 (w/단말 상태 수집 클라이언트)

최소 접근 권한 관리

- **IP/Port 기반 접근 제어**
  - 동일 포트/포트 변경을 통한 접근 가능 (Port ≠ 애플리케이션)
  - 사용자 IP변경에 따른 정책 변경 필요 (IP ≠ 사용자)

※ 업무에 필요한 사용자 및 업무용 애플리케이션에 대한 접근 허용 필요

차세대 방화벽을 이용한 Zero Trust Network 구성 방안

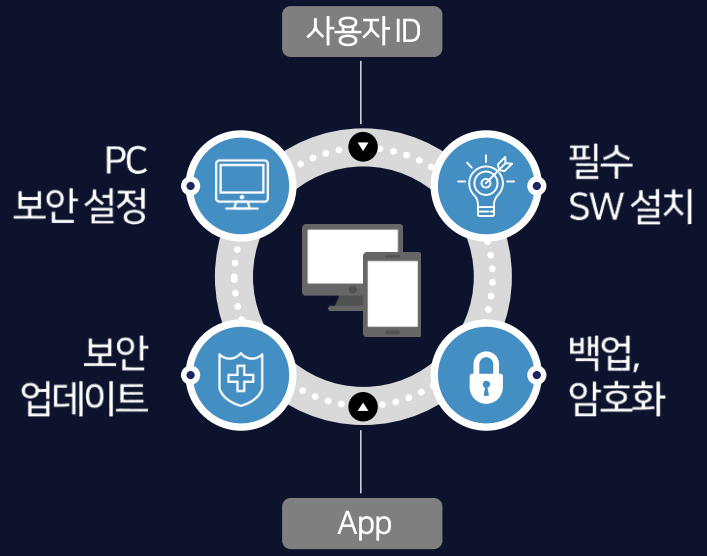
차세대 방화벽과 클라이언트 연동을 통해

Zero Trust Network 환경 지원 가능

* 차세대방화벽(NGFW) : 사용자, 애플리케이션, 디바이스 상태 정보 기반 접근제어 지원

클라이언트

Device 환경, 트래픽 정보 분석



차세대 방화벽

사용자 ID, Device, App 제어

사용자 ID 인증, 연동

\+

DEVICE COMPLIANCE

\+

Application 분석, 제어

DMZ 구간

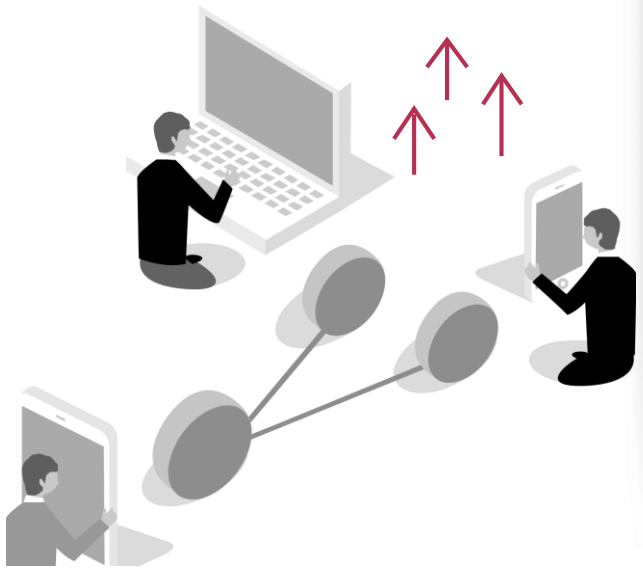
클라우드

사내 업무 시스템

차세대 방화벽을 이용한 안심 재택 구축 방안

검증된 단말/사용자의
업무용 트래픽에 대해서만

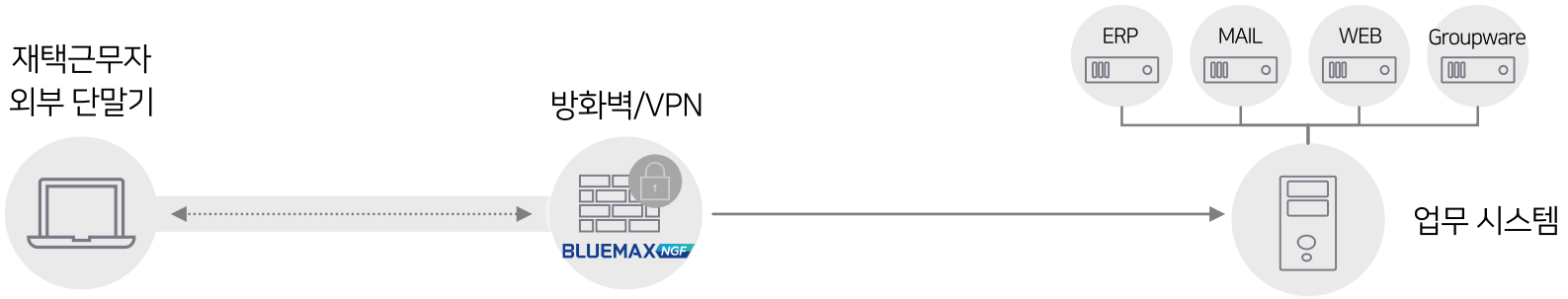
접근 허용



사전 점검	사용 단말 상태 사전 점검을 통해 안전성 유/무 판단
신원 확인 및 암호 통신	인사 정보 연동, Multi-Factor 인증을 통해 확인된 사용자만 허용
디바이스 신뢰성 확인	단말의 보안 상태/레벨에 따른 차별화된 내부 자원 접근 제어
최소 접근 권한 관리	사용자/애플리케이션 기반 업무용 트래픽에 대해서만 접근 허용

차세대 방화벽을 이용한 안심 재택 구축 방안

1단계 : 사전 점검 - 디바이스 신뢰성 점검 결과를 토대로 원격 연결 허용



사전 점검을 통한 원격 연결 여부 판단

상태 점검을 통한 원격 연결 지속 여부 판단

01 사전 점검을 통한 원격 연결 여부 판단

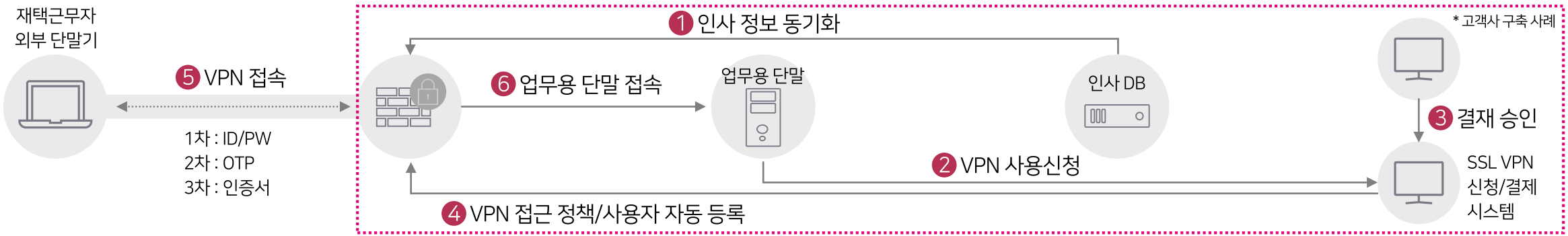
- 원격 연결(SSL VPN)을 하기 전에 단말의 상태 점검을 통해 안전성 유무 판단
- 지원 항목
  - 안전하지 않은 운영체제 사용 여부, 로그인 패스워드 및 화면보호기 설정 여부, PC 방화벽 설정 여부, 백신 프로그램 설치 여부 및 백신 구동을 통한 검사 진행 등

02 상태 점검을 통한 원격 연결 지속 여부 판단

- 정보 유출 및 악성코드 내부 유입을 방지 하기 위한 단말 기능 비활성화 및 연결 해제 진행
- 지원 항목
  - 외부 인터넷 연결 차단, 네트워크 드라이브 연결 차단, 공유 폴더 차단, 클립보드 기능 비활성화(윈도우 원격 터미널 접속 시)
  - 마우스/키보드 유휴 상태 지속 시 원격 연결(SSL VPN) 종료

차세대 방화벽을 이용한 안심 재택 구축 방안

2단계 : 신원 확인 - 인사 정보와 연계한 사용자 검증 및 Multi-Factor 인증



1 고객사 인사 DB 동기화 (SSL VPN 사용자 정보)

- 고객사 인사 DB 연동으로 SSL VPN 사용자 정보 자동 갱신 (비활성화 상태 동기화)

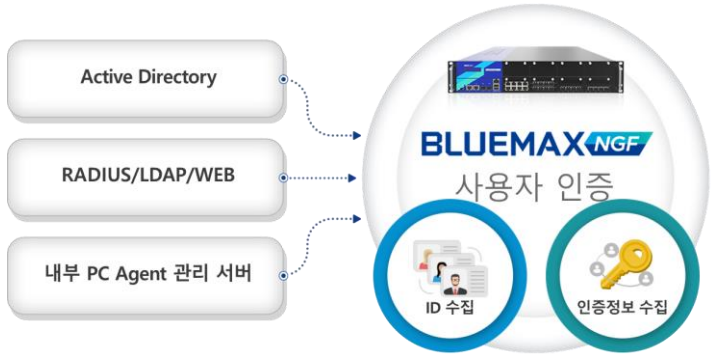
2 SSL VPN 전자 결재 시스템 연동을 통한 SSL VPN 사용자 활성화

- REST API로 고객사 SSL VPN 전자 결재 시스템과 연동
- SSL VPN 신청/승인 → REST API를 통해 정보 전송 (접속 정보, 이용 기간 등을 포함한 사용자 자동 활성화)

3 Multi-Factor 인증을 통한 SSL VPN 연결

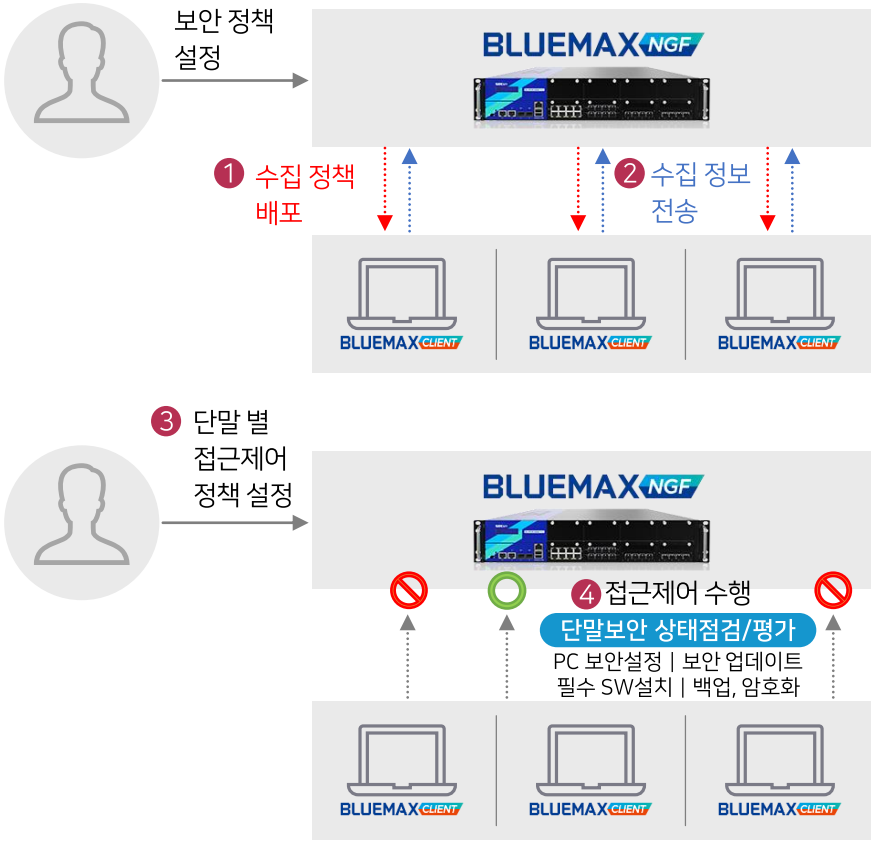
- ID/PW 인증 및 OTP 인증을 통한 사용자 확인 진행 후 연결 허용

다양한 방식의 사용자 인증 지원



차세대 방화벽을 이용한 안심 재택 구축 방안

3단계 : 디바이스 신뢰성 확인 - 디바이스 보안 상태에 따른 접근 제어 (방화벽 정책 연동)



1 방화벽에서 단말 보안 정보 수집 정책 설정/배포

- OS 정보 : OS 종류 및 버전 정보 수집
- Security : 백신, 백업, 최신 패치, 방화벽, 화면 잠금 등 보안 관련 사용 정보 수집
- Program : 사전 정의된 40여 종 프로그램 사용 정보 수집
- Custom : 사용자가 임의 정의한 프로그램 사용 정보 수집

2 Client에서 설정된 정책 기반 단말 정보 수집 및 전송

- 방화벽에서 설정된 단말 정보 수집 정책에 따른 단말의 정보를 수집하여 방화벽으로 전송

3 단말의 수집 정보 기반 접근 제어 정책 설정

- 디바이스 상태에 따른 허용/차단 방화벽 정책 수립
- 그룹 보안 정책 설정을 통해 다양한 조건 지정 가능

4 수집된 정보를 기반으로 정책과 매칭하여 접근제어 수행

- 최신 보안 패치 미적용, 필수 SW 미설치 단말에 대한 주요 업무 서버 접근 차단 등

※ 방화벽 정책과 연계하여 단말의 보안 상태에 따른 세분화된 접근제어 정책 적용 가능

차세대 방화벽을 이용한 안심 재택 구축 방안

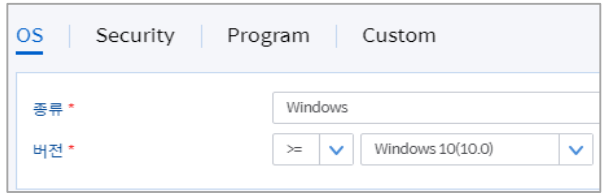
3단계 : 디바이스 신뢰성 확인 - 방화벽 정책 연동 화면

1 재택근무자

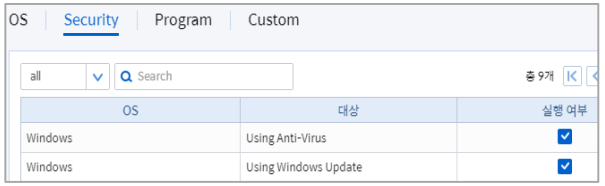
인증 대상
hugh.kim1
tyjeong
jongdeok74.kim
yoingkyu45.kim
jungsu.kim
taeyoune.jeong

2 보안 정책

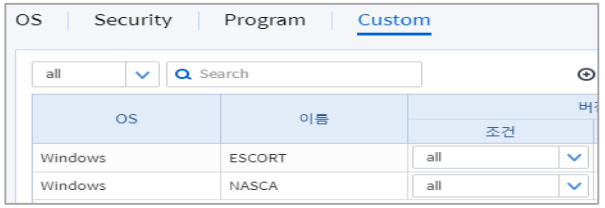
- Windows 10이상



- AntiVirus 사용, Windows update 사용



- 필수 보안 S/W 사용 (예 : NASCA, ESCORT)



3 접근 통제

그룹에 속한 객체 이름	IP 주소
ERP서버	11.4.8.23
메일서버	168.128.121.11
SPMS	192.168.230.20
QNA_SERVER	192.168.230.21

차세대 방화벽을 이용한 안심 재택 구축 방안

4단계 : 최소 접근 권한 관리 – 업무용 애플리케이션에 대해서만 접근 허용

- **업무용 애플리케이션만 접근 허용 (IP/Port ≠ 애플리케이션)**
  - 제조사 배포 인지룰을 통한 애플리케이션 인지 지원
  - 애플리케이션 별 세부 행위 인지 및 제어

  ※주기적인 애플리케이션 인지룰 업데이트 및 사용자 정의 등록을 통한 내부 애플리케이션 인지 지원

- **비인가 애플리케이션 인지 및 차단**
  - 애플리케이션 사용 포트 현황 및 사용자 별 애플리케이션 사용 현황 정보 등

  ※허가되지 않은 포트를 사용하는 애플리케이션, 인가되지 않은 사용자 식별 가능

Thank you

SAMSUNG SDS