Contribution

Marathon

Innovation

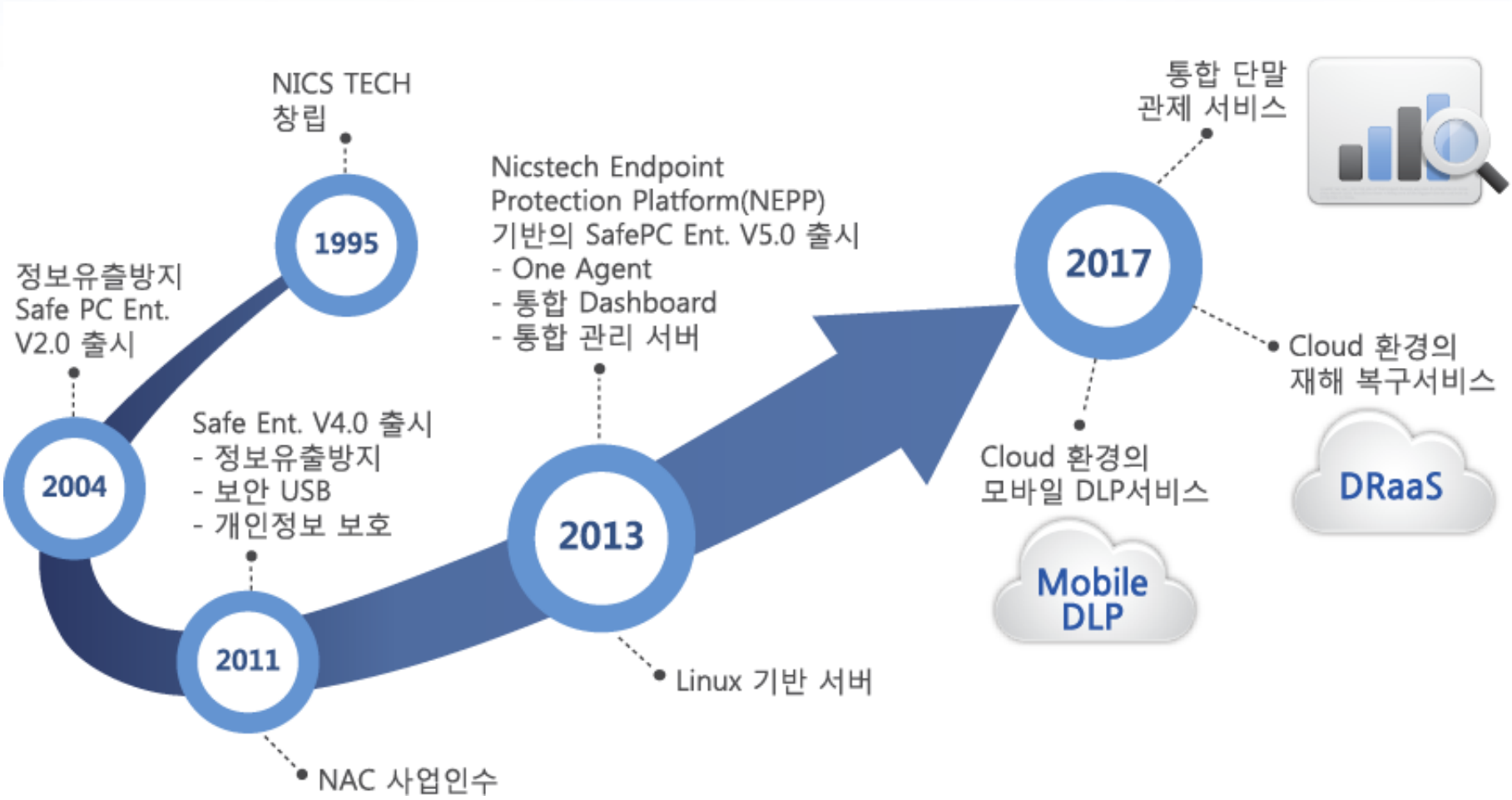
효과적인 엔드포인트 보안 전략

하나의 작은 움직임이 큰 기적을.

Smart Security & Service

NICS TECH

닉스테크 성장


NICS TECH
창립
1995
정보유출방지
Safe PC Ent.
V2.0 출시
2004
Safe Ent. V4.0 출시
- 정보유출방지
- 보안 USB
- 개인정보 보호
2011
NAC 사업인수
Nicstech Endpoint
Protection Platform(NEPP)
기반의 SafePC Ent. V5.0 출시
- One Agent
- 통합 Dashboard
- 통합 관리 서버
2013
Linux 기반 서버
통합 단말
관제 서비스
2017
Cloud 환경의
재해 복구서비스
DRaaS
Cloud 환경의
모바일 DLP서비스
Mobile
DLP

닉스테크 사업부

서비스 사업

네트워크 보안사업

클라이언트 보안사업

우리은행 · 하나은행 · KYOBO 교보문고

힘찬병원 HIMCHAN HOSPITAL · KB · MIRAE ASSET 미래에셋 · Megapass

영동세브란스병원 YONGDONG SEVERANCE HOSPITAL · SK telecom · 군인공제회

smart KPX 전기의 미래를 열어가는 전력거래소 · 신한은행 SHINHAN BANK · 신한 DAMOA · kt · 문화체육관광부

1,400+
Sites and Services

대법원 · 농협 · LG TeleCom

KEB 외환은행

성신여자대학교 · 지식경제부 · woongjin · 기획예산처 · kr

목 차 |

보안 사고 들여다보기

1 보안 사고

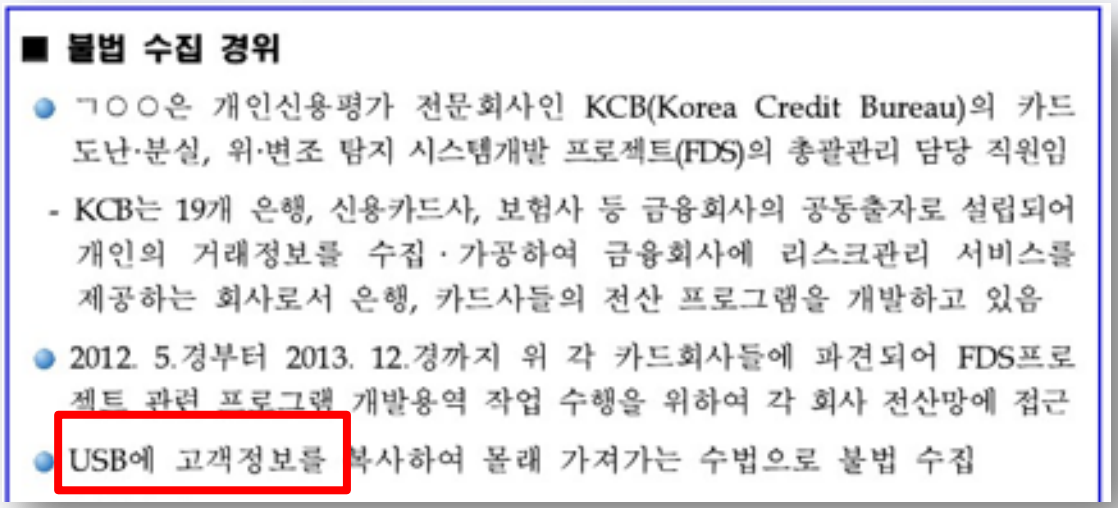
2 사고 원인

3 선제적 대응 방안

1.1 보안 사고

사이버 공격 증가	•개인정보 유출 사고 증가 •해킹 공격 등 사이버 테러 증가
내부자 자료 유출 사고 증가	•내부자 자료 유출 사고 35% 이상 •스마트폰 기기에 의한 내부 보안 침해 가능성 증가
공격 방식의 지능화	• 업무용 취약점 이용한 침해 • 침해 스펙트럼의 다양화 (단말 악성 코드 → DDoS 공격)

1.2 사고 원인



■ 불법 수집 경위

- ㄱㅇㅇ은 개인신용평가 전문회사인 KCB(Korea Credit Bureau)의 카드 도난·분실, 위·변조 탐지 시스템개발 프로젝트(FDS)의 총괄관리 담당 직원임
  - KCB는 19개 은행, 신용카드사, 보험사 등 금융회사의 공동출자로 설립되어 개인의 거래정보를 수집·가공하여 금융회사에 리스크관리 서비스를 제공하는 회사로서 은행, 카드사들의 전산 프로그램을 개발하고 있음
- 2012. 5.경부터 2013. 12.경까지 위 각 카드회사들에 파견되어 FDS프로젝트 관련 프로그램 개발용역 작업 수행을 위하여 각 회사 전산망에 접근
- USB에 고객정보를 복사하여 몰래 가져가는 수법으로 불법 수집

위협 주체

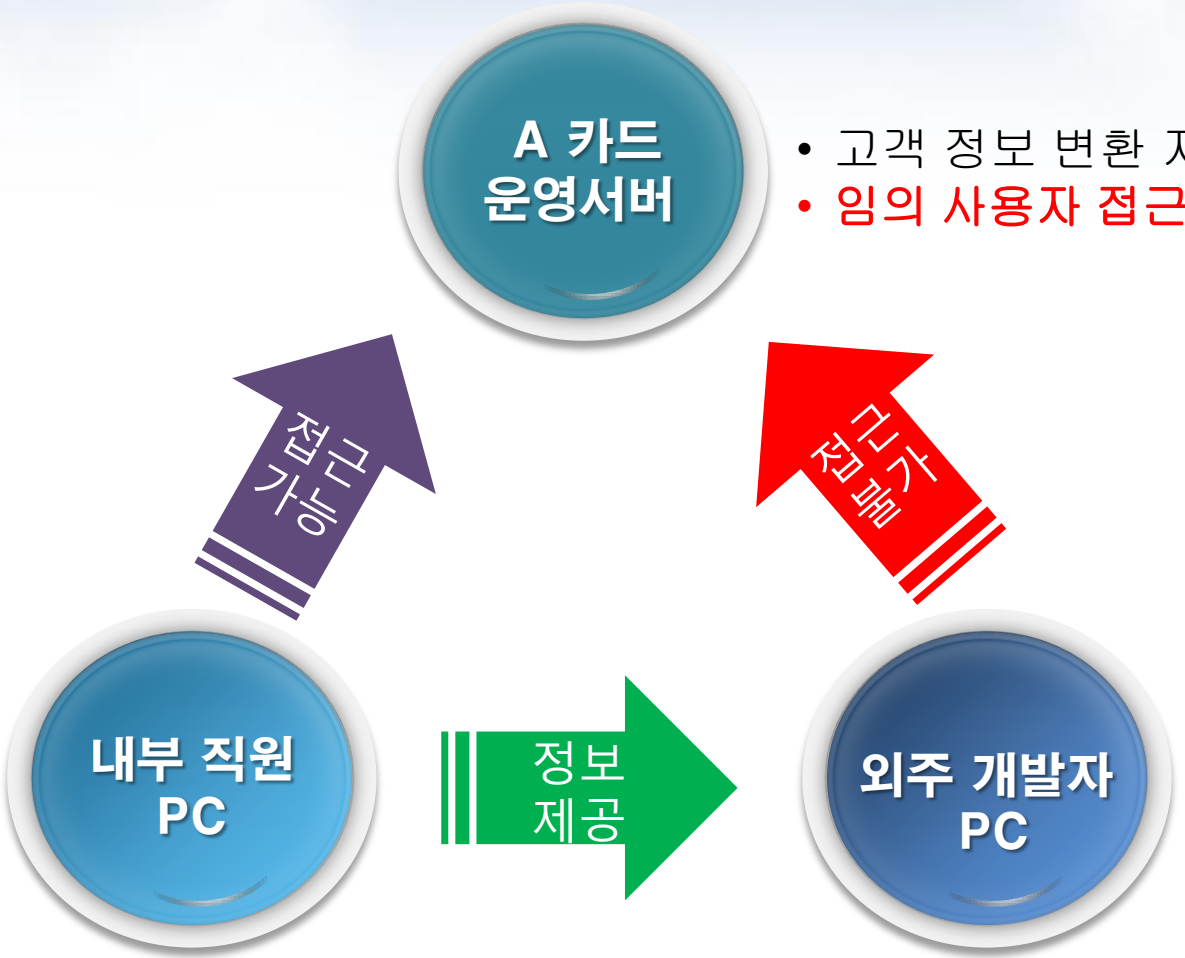
내부

- 불만을 품은 직원
- 계약사원
- 외주 인력
- 비즈니스 파트너 / 벤더

외부

- 산업스파이
- 사이버테러리스트
- 사기꾼
- 사회공학자
- Script kiddies

1.3 선제적 대응 방안


A 카드
운영서버
• 고객 정보 변환 저장
• 임의 사용자 접근 통제
접근
권한
접근
권한
내부 직원
PC
정보
제공
외주 개발자
PC
• PC 보안 설치
• 승인된 고객 정보 암호화 전달
• PC 보안 설치
• USB/메일 통한 데이터 유출 차단

계층적 보안 방안 |

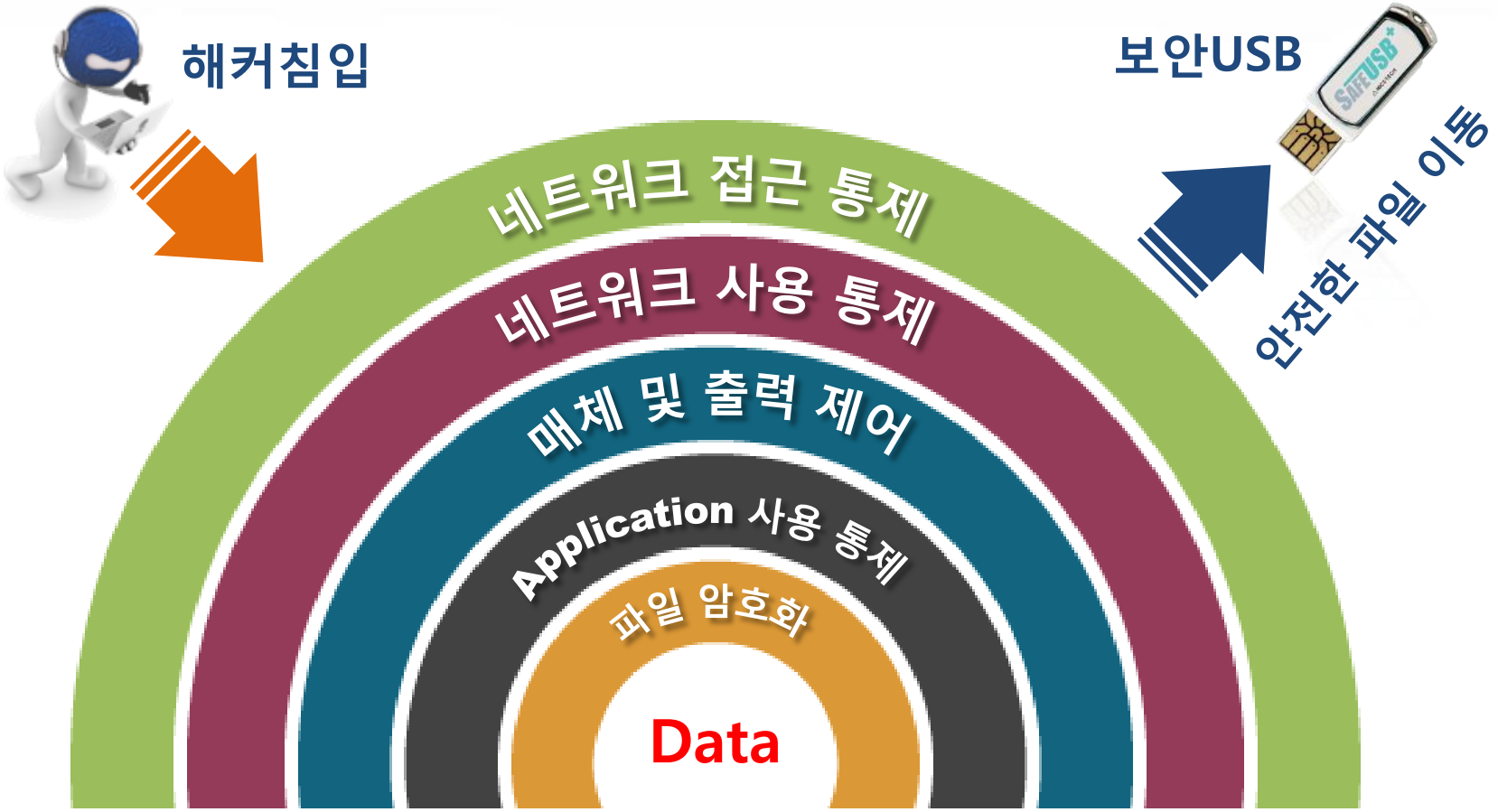
1 계층적 보안

2 보안의 가시성

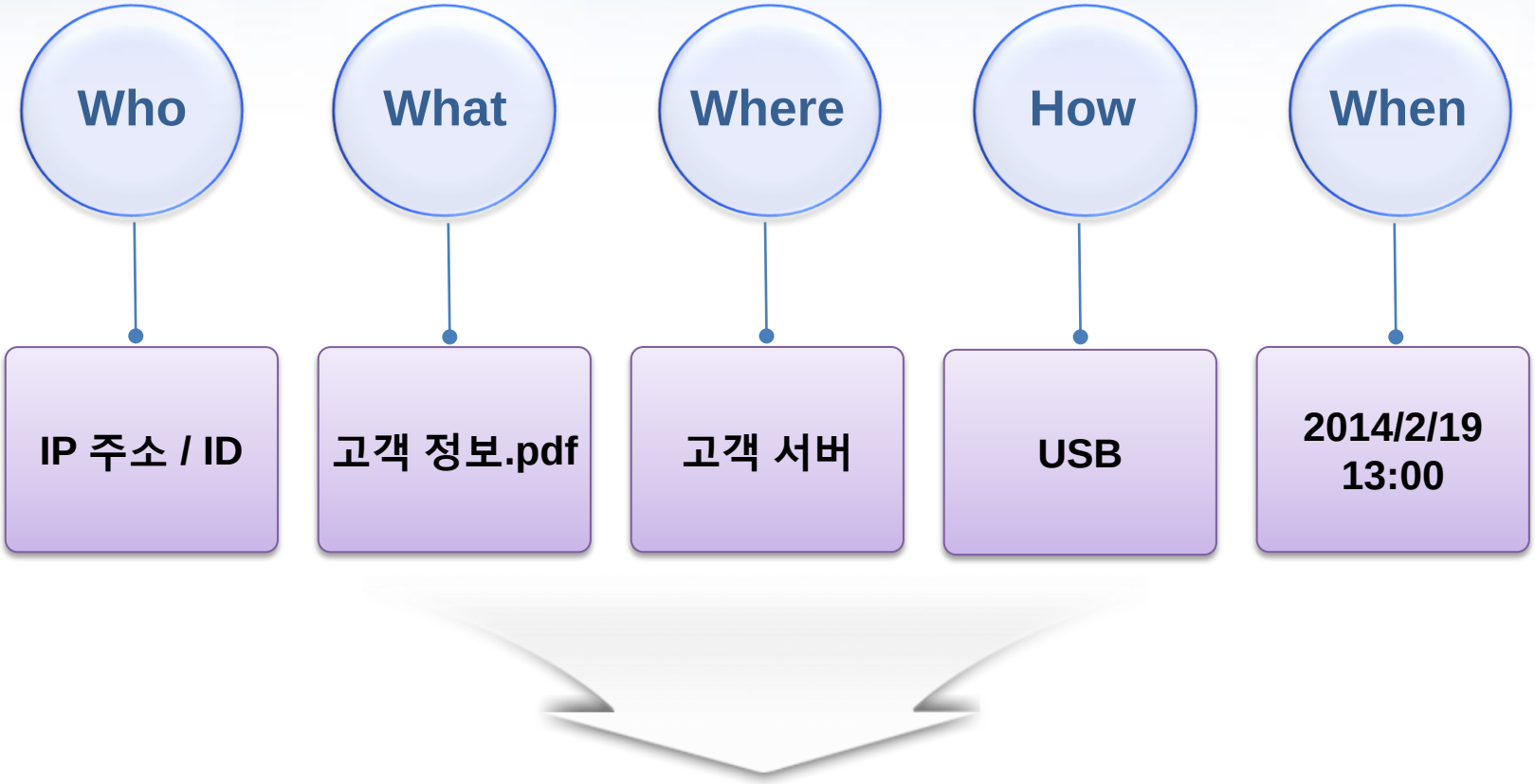
3 계층적 단말 보안

2.1 계층적 보안 (Defense in Depth)

하나의 솔루션에 의존하지 말라

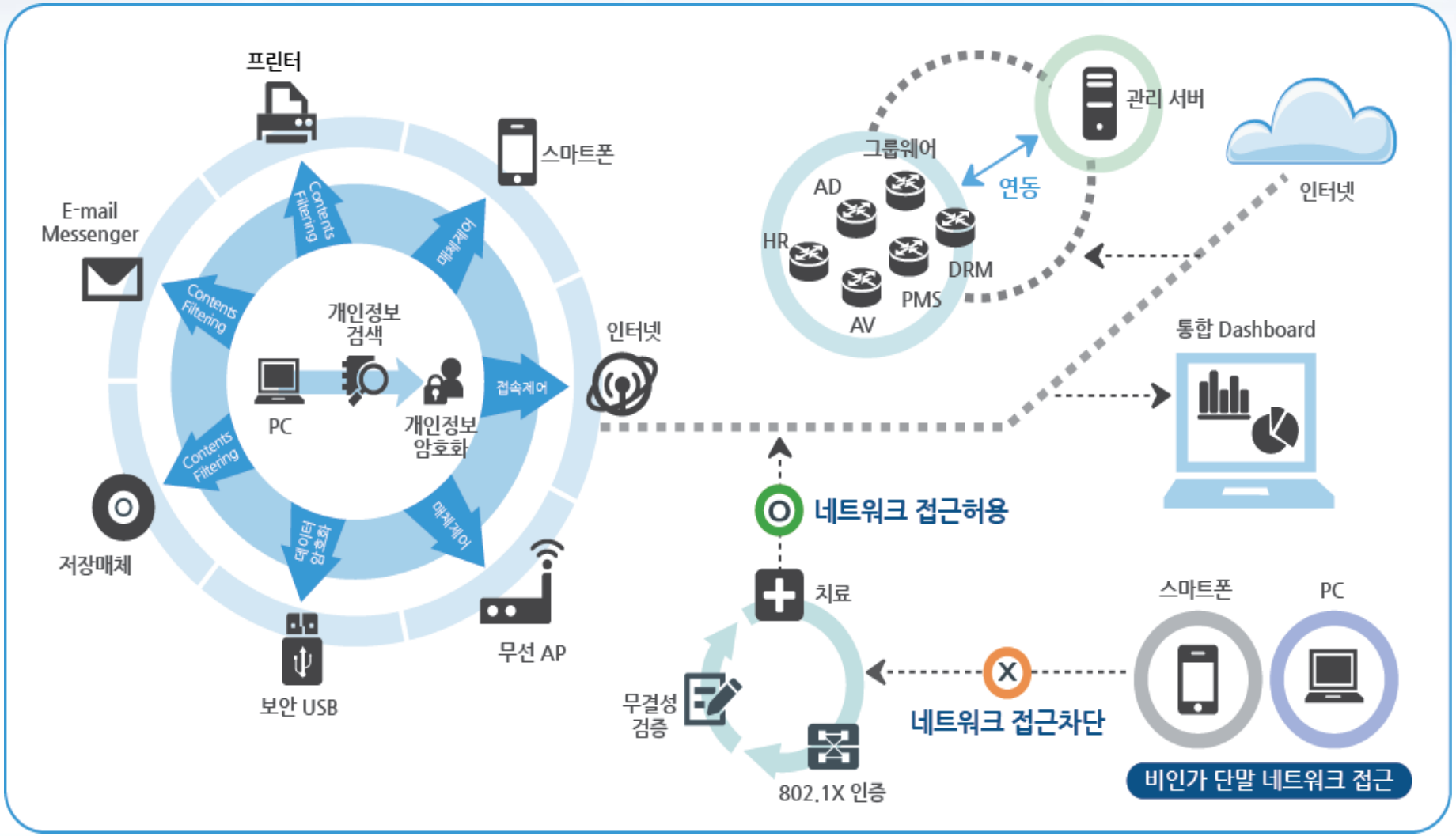


2.2 보안의 가시성

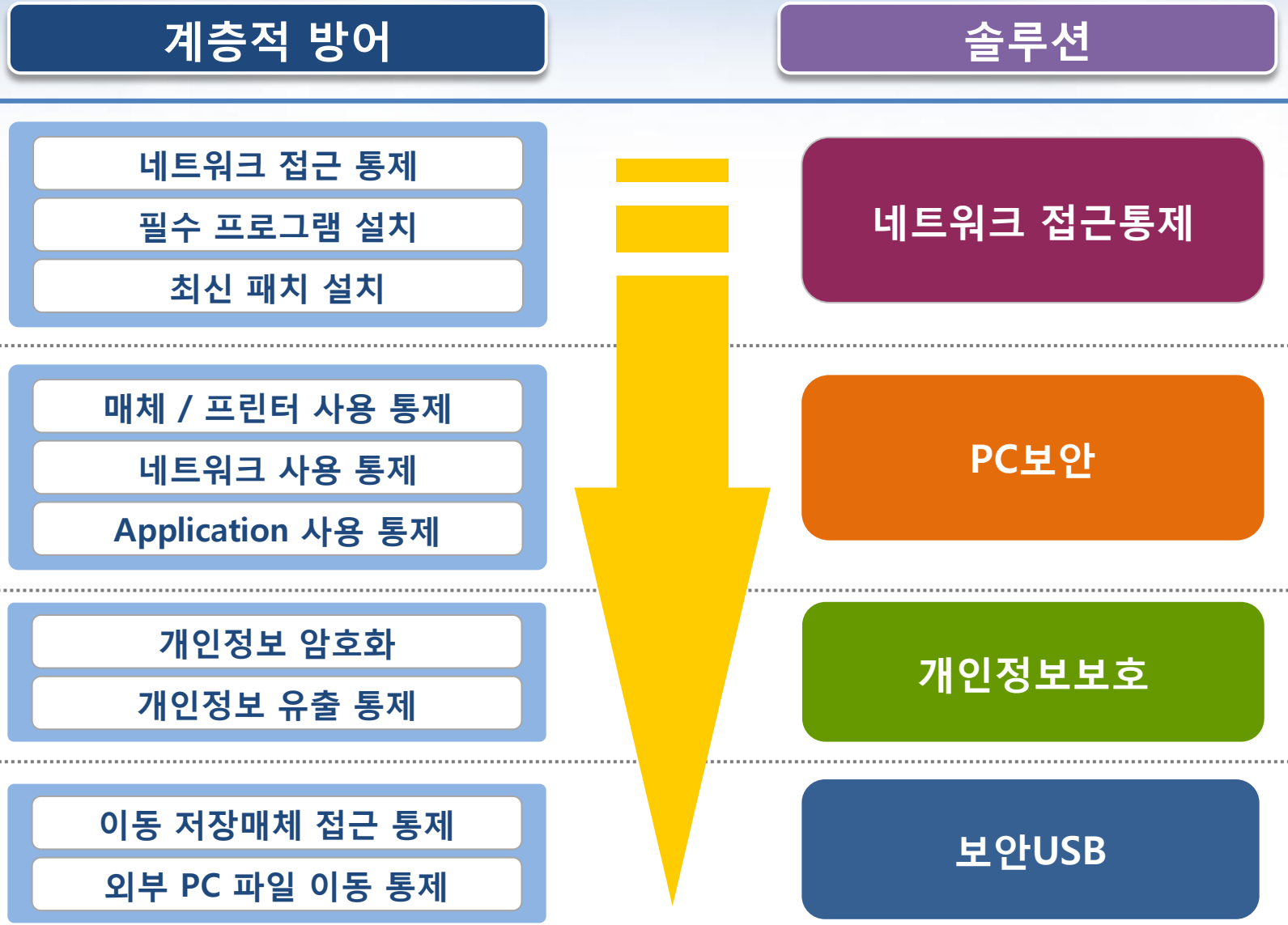


보안의 가시성 확보

2.3 계층적 단말 보안


프린터
스마트폰
E-mail
Messenger
Contents Filtering
매체제어
Contents Filtering
개인정보 검색
PC
개인정보 암호화
접속제어
Contents Filtering
데이터 암호화
매체제어
저장매체
보안 USB
무선 AP
인터넷
관리 서버
그룹웨어
연동
AD
HR
DRM
PMS
AV
인터넷
통합 Dashboard
네트워크 접근허용
치료
무결성 검증
802.1X 인증
네트워크 접근차단
스마트폰
PC
비인가 단말 네트워크 접근

2.3 계층적 단말 보안 (계속)



2.3 계층적 단말 보안 (계속)

- ✓ 네트워크 접근 통제
- 필수 프로그램 설치
- 최신 패치 설치
- 매체/프린터 사용 통제
- 네트워크 사용 통제
- Application 사용 통제
- 개인정보 암호화
- 개인정보 유출 통제
- 이동 저장매체 접근 통제
- 외부 PC 파일 이동 통제

❖ 유/무선 네트워크 접근 통제

- 엔드포인트의 내부망 접근 시도 시, 접근이 가능한 자에 대한 사전 정의를 통해 접근 통제

❖ 인증 방법

- 사용자 ID/PW/IP/MAC/HDD size
- 국제 표준 IEEE 802.1x

2.3 계층적 단말 보안 (계속)

- 네트워크 접근 통제
- ✓ 필수 프로그램 설치
- ✓ 최신 패치 설치
- 매체/프린터 사용 통제
- 네트워크 사용 통제
- Application 사용 통제
- 개인정보 암호화
- 개인정보 유출 통제
- 이동 저장매체 접근 통제
- 외부 PC 파일 이동 통제

❖ 보안 취약자 접근 통제 및 치료

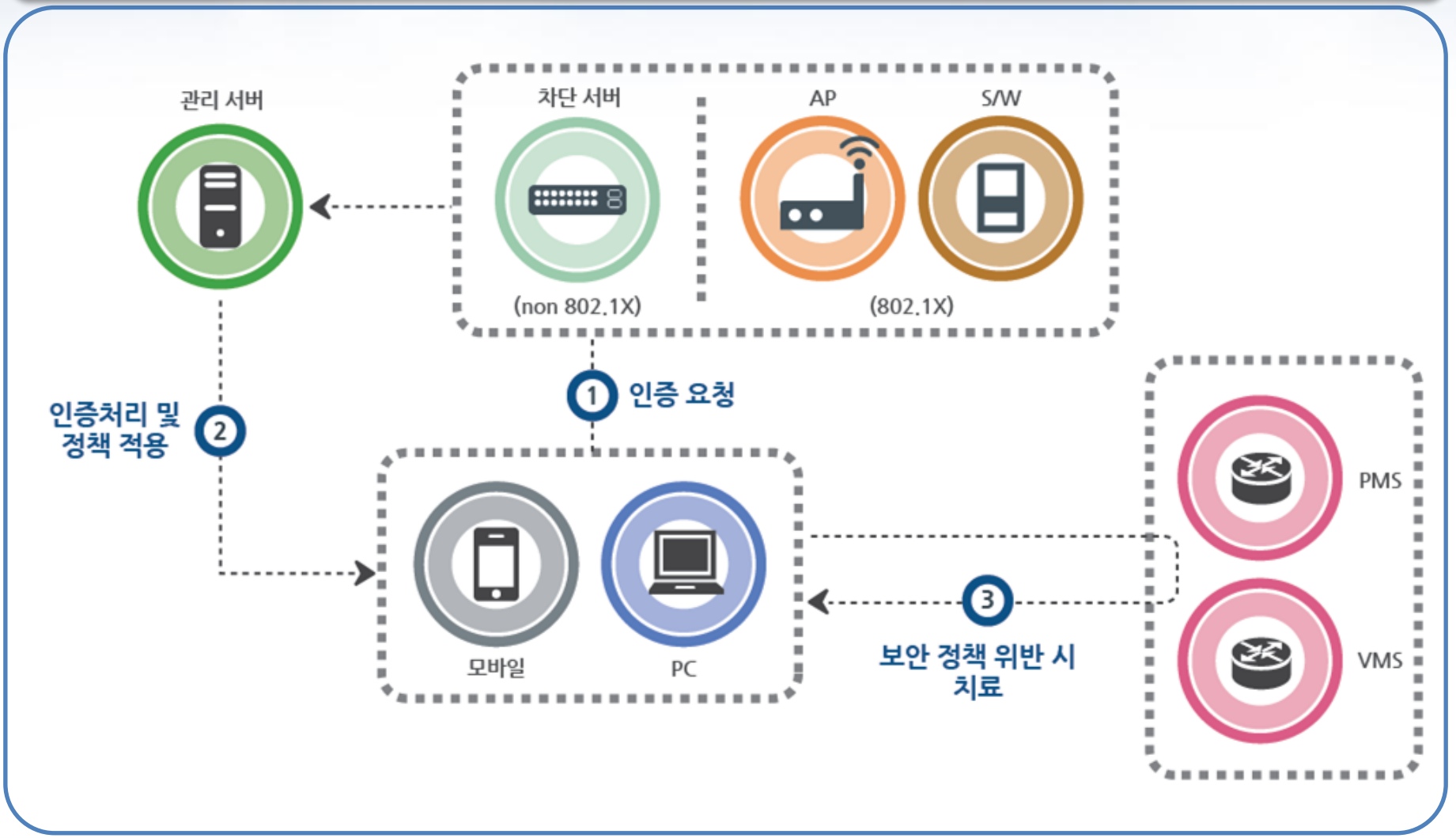
- 엔드포인트 보안상태 적절성 및 위협 방어 솔루션 운영 여부 점검 후 패치

❖ 보안 정책 준수 여부 체크

- 바이러스 감염 등으로 접근 거부된 엔드포인트 단말은 치료 후 접근 허용

2.3 계층적 단말 보안 (계속)

네트워크 접근 통제 프로세스



2.3 계층적 단말 보안 (계속)

- 네트워크 접근 통제
- 필수 프로그램 설치
- 최신 패치 설치
- ✓ 매체/프린터 사용 통제
- ✓ 네트워크 사용 통제
- ✓ Application 사용 통제
- 개인정보 암호화
- 개인정보 유출 통제
- 이동 저장매체 접근 통제
- 외부 PC 파일 이동 통제

❖ 매체 / 프린터 사용 통제

- 허용되지 않은 모든 매체 사용 통제.
- 스마트폰, USB 저장매체, Wi-Fi, CD/RW
- 출력물 워터마킹
- 출력 로깅 및 원문 저장

❖ 네트워크 유출 통제

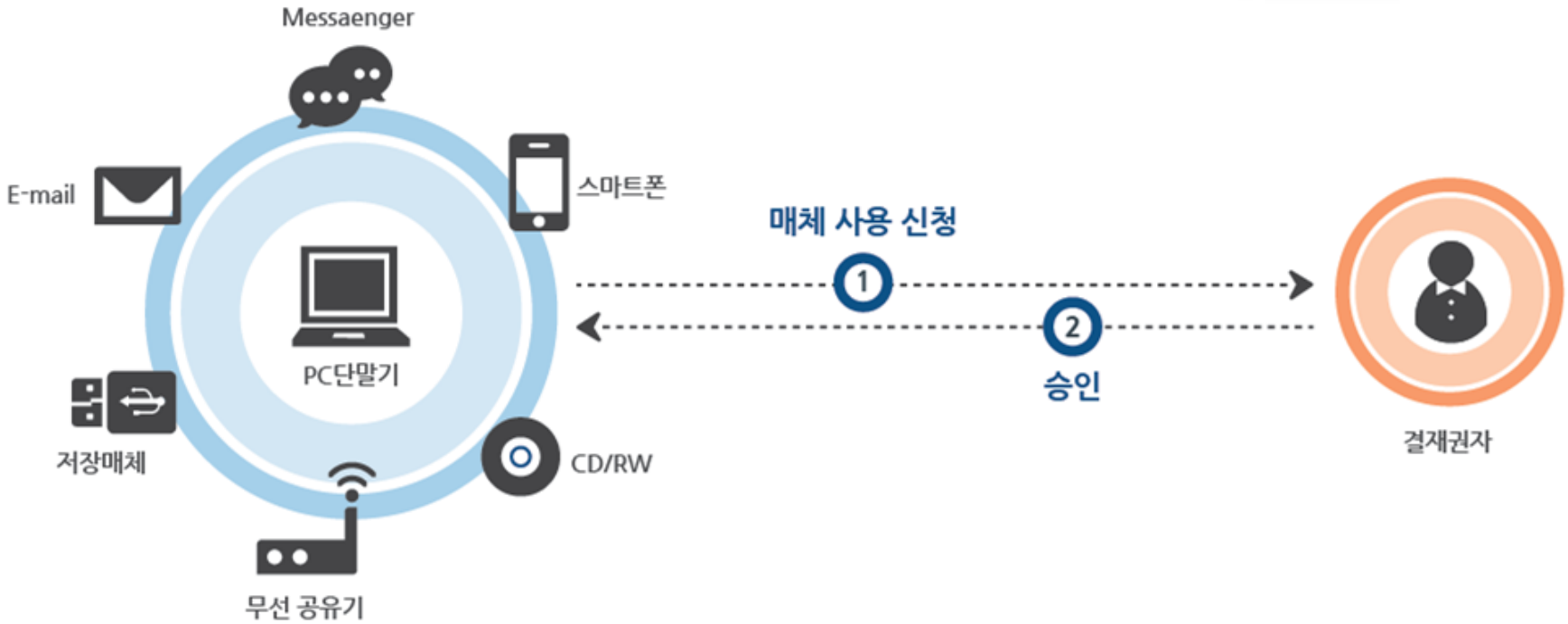
- 비업무 사이트 접속 차단
- E-mail 통한 파일 유출 차단

❖ Application 사용 통제

- 비업무/불법 Application 사용 제어

2.3 계층적 단말 보안 (계속)

매체 및 웹사이트(E-mail) 접근 통제 프로세스



2.3 계층적 단말 보안 (계속)

- 네트워크 접근 통제
- 필수 프로그램 설치
- 최신 패치 설치
- 매체/프린터 사용 통제
- 네트워크 사용 통제
- Application 사용 통제
- ✓ 개인정보 암호화
- ✓ 개인정보 유출 통제
- 이동 저장매체 접근 통제
- 외부 PC 파일 이동 통제

❖ 개인정보 암호화

- 내용 기반 개인정보 검색
- 개인정보 암호화 및 중앙 통제

❖ 내용 기반 유출 경로 통제

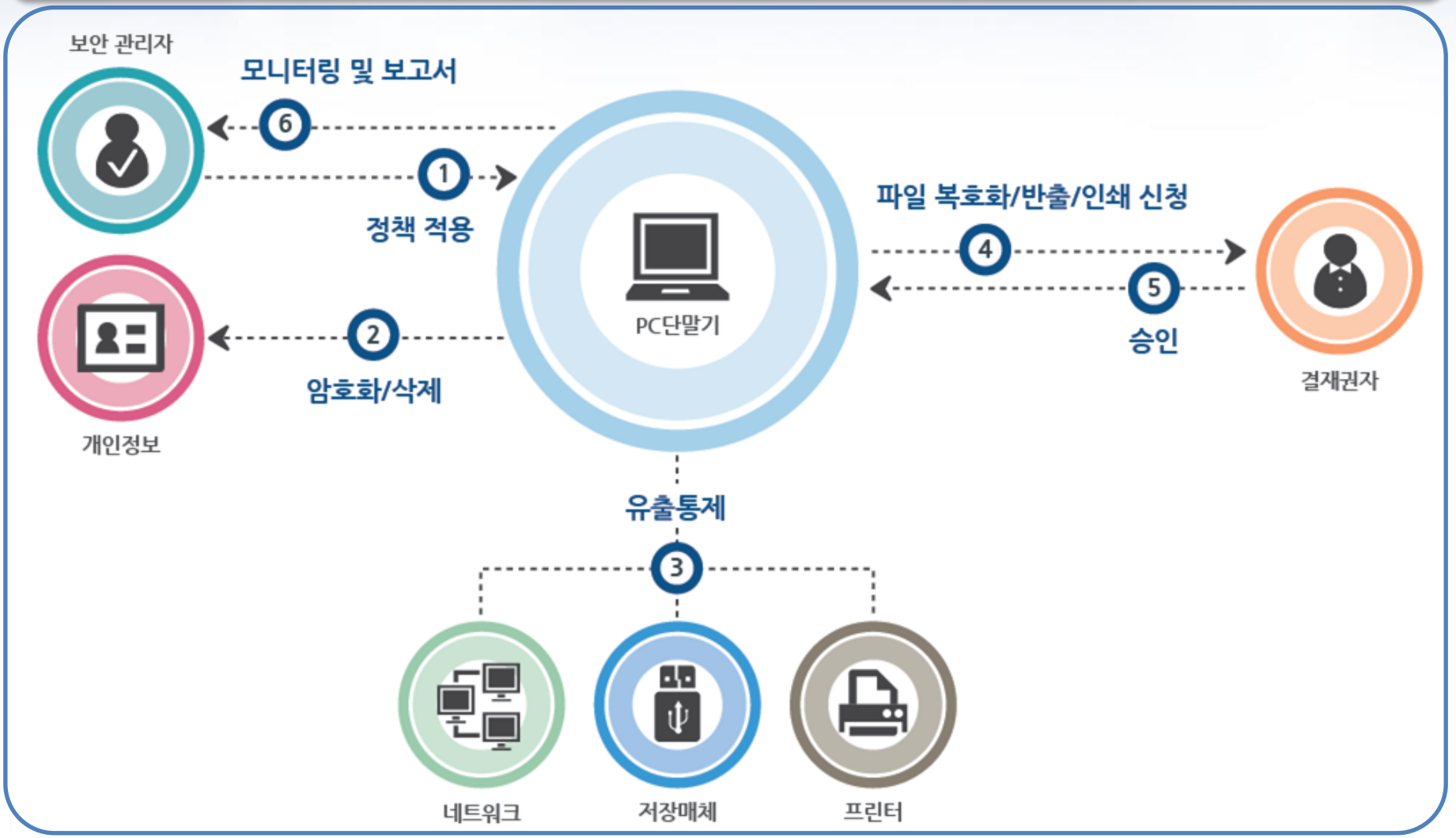
- USB 저장 매체/E-mail/프린트 유출 통제

❖ 파일 반출 승인 프로세스

- 승인된 암호화 파일에 대해서만
  외부 반출 통제 및 반출 파일 원문 저장

2.3 계층적 단말 보안 (계속)

개인정보 유출 통제 프로세스



2.3 계층적 단말 보안 (계속)

- 네트워크 접근 통제
- 필수 프로그램 설치
- 최신 패치 설치
- 매체/프린터 사용 통제
- 네트워크 사용 통제
- Application 사용 통제
- 개인정보 암호화
- 개인정보 유출 통제
- ✓ 이동 저장매체 접근 통제
- ✓ 외부PC 파일 이동 통제

❖ 보안USB 접근 인증

- USB 저장매체 접근 시, 인증 요구
- 인증 실패 시 USB 접근 통제

❖ 데이터 자동 암호화

- **PC → USB** 파일 이동 시, 자동 암호화

❖ USB 분실 조치

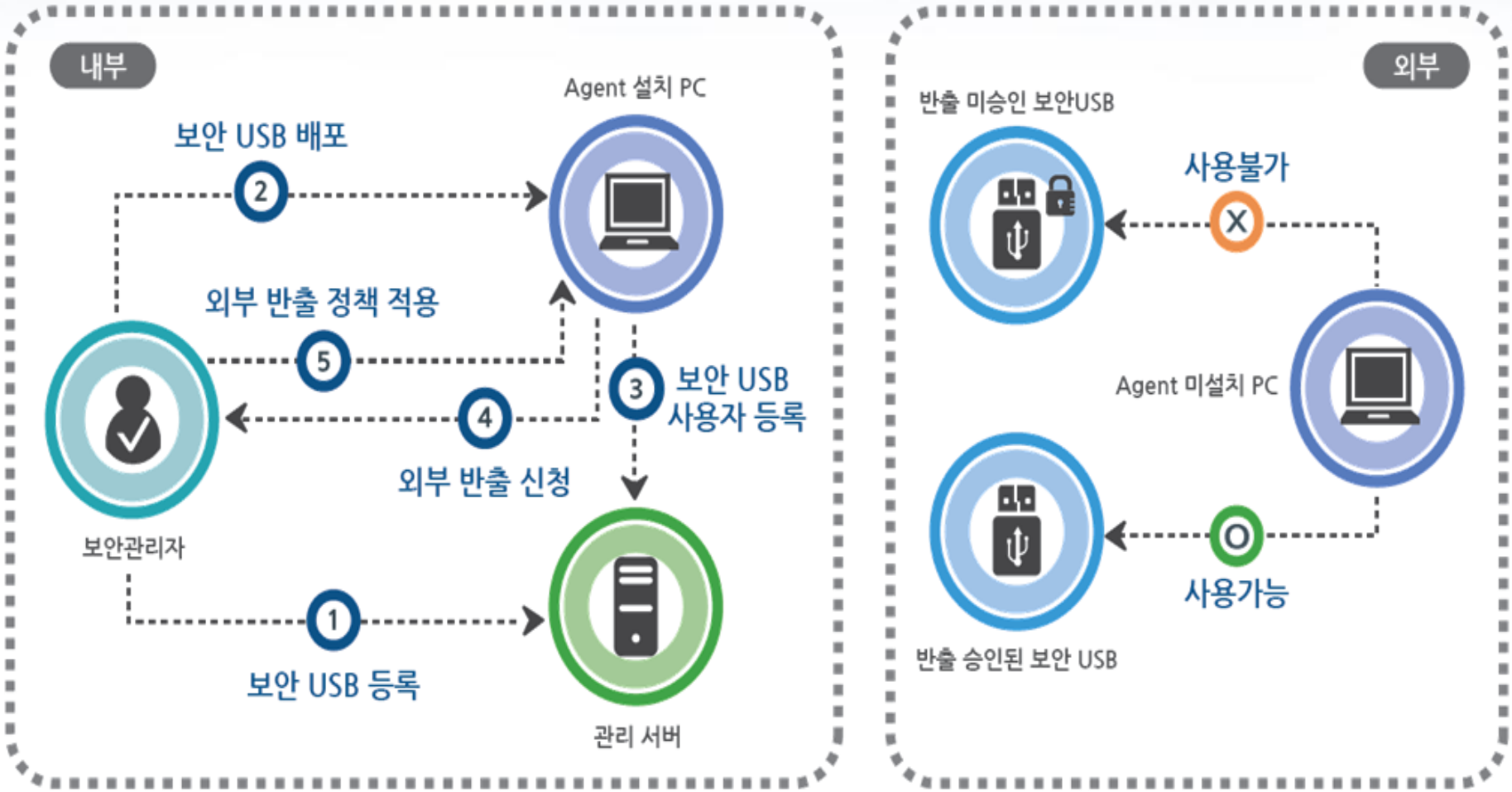
- 데이터 완전 삭제 및 **USB** 접근 통제

❖ 외부 PC 파일 이동 통제

- **USB** 외부 반출 승인 프로세스
- 파일 읽기 및 외부 복사 통제

2.3 계층적 단말 보안 (계속)

보안USB 운영 프로세스



안전한 데이터 이동 방안 |

1 파일의 안전한 이동

2 정보 유출 통제

3 파일 승인 이동

4 망분리 환경의 파일 이동

3.1 파일의 안전한 이동

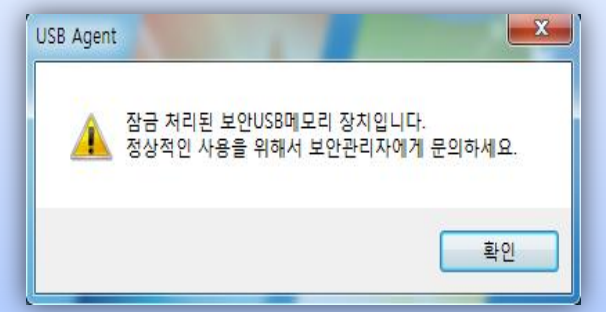
[보안USB 내부 구성]

- 하드웨어 암호화

- PC 연결 시, 장치 인증 Password 요구

장치
인증

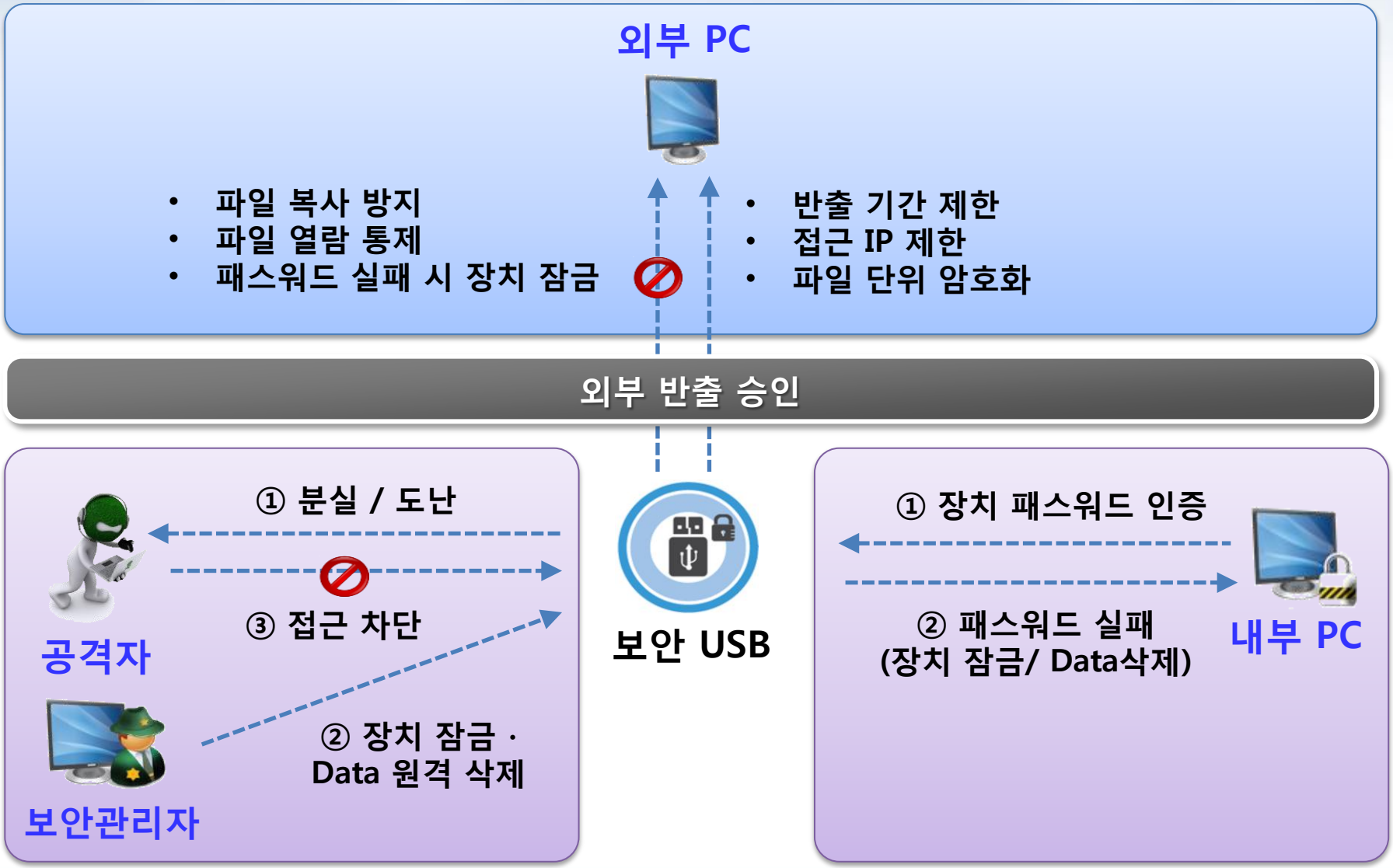
[외부 반출 통제]



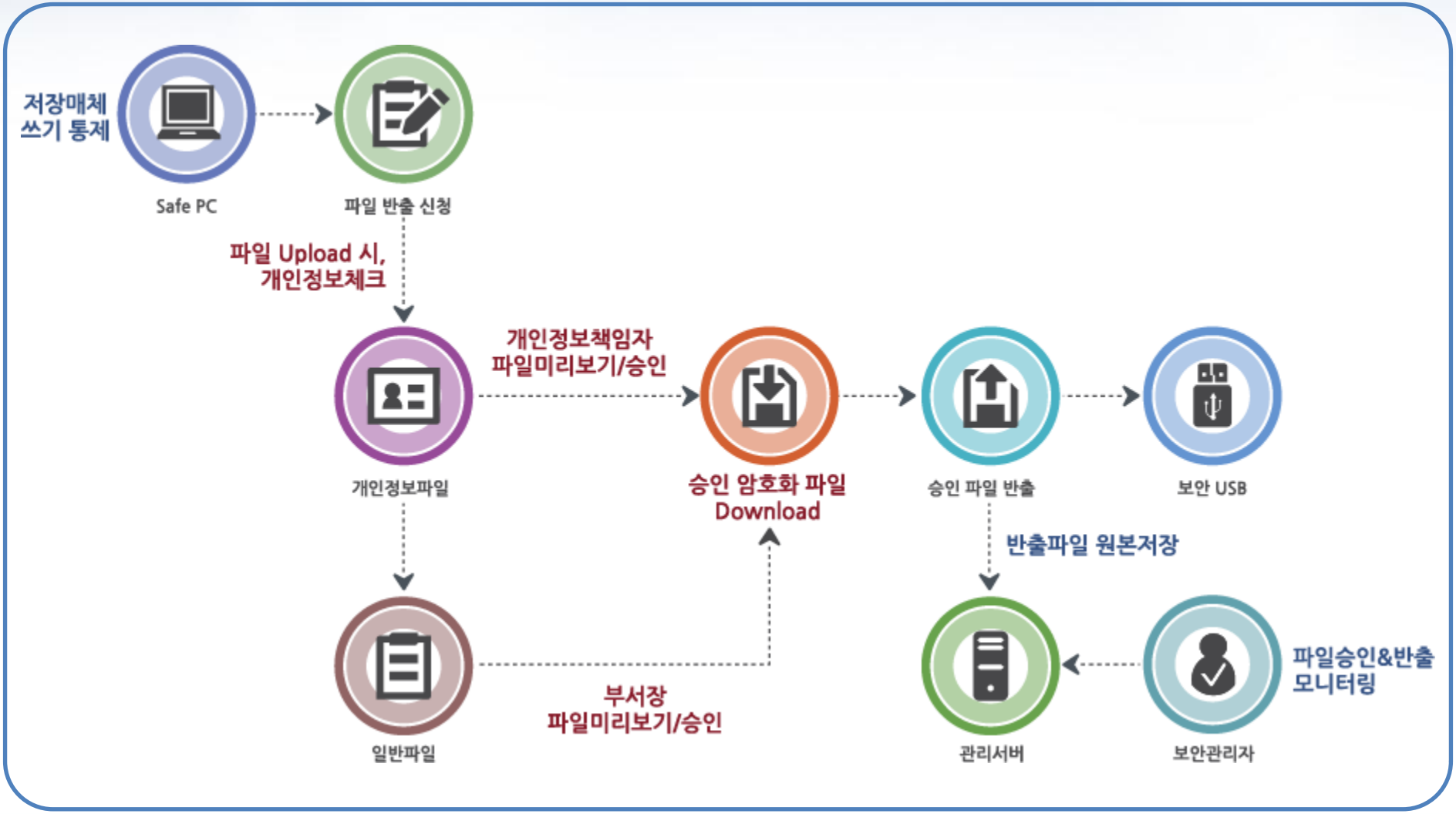
- 외부 파일 복사 통제

- 보안 영역 활성화
- 파일 자동 암·복호화

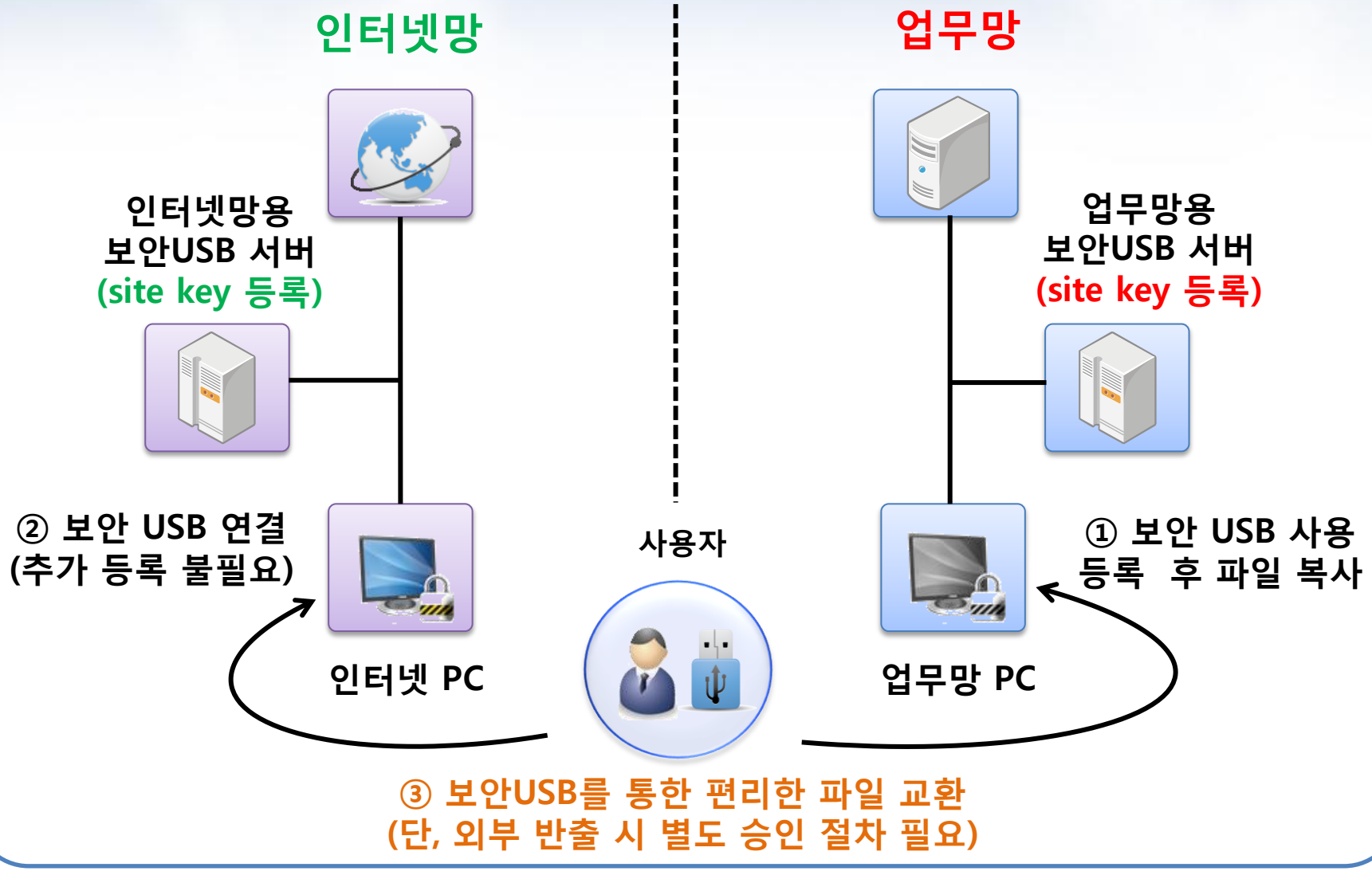
3.2 정보 유출 통제


외부 PC
• 파일 복사 방지
• 파일 열람 통제
• 패스워드 실패 시 장치 잠금
• 반출 기간 제한
• 접근 IP 제한
• 파일 단위 암호화
외부 반출 승인
① 분실 / 도난
③ 접근 차단
공격자
② 장치 잠금 · Data 원격 삭제
보안관리자
보안 USB
① 장치 패스워드 인증
② 패스워드 실패 (장치 잠금/ Data삭제)
내부 PC

3.3 파일 승인 이동


저장매체
쓰기 통제
Safe PC
파일 반출 신청
파일 Upload 시,
개인정보체크
개인정보파일
개인정보책임자
파일미리보기/승인
승인 암호화 파일
Download
승인 파일 반출
보안 USB
반출파일 원본저장
일반파일
부서장
파일미리보기/승인
관리서버
보안관리자
파일승인&반출
모니터링

3.4 망분리 환경의 파일 이동



관리적 보안 방안 |

1 정보 보안 프레임워크

2 통합 단말 Platform

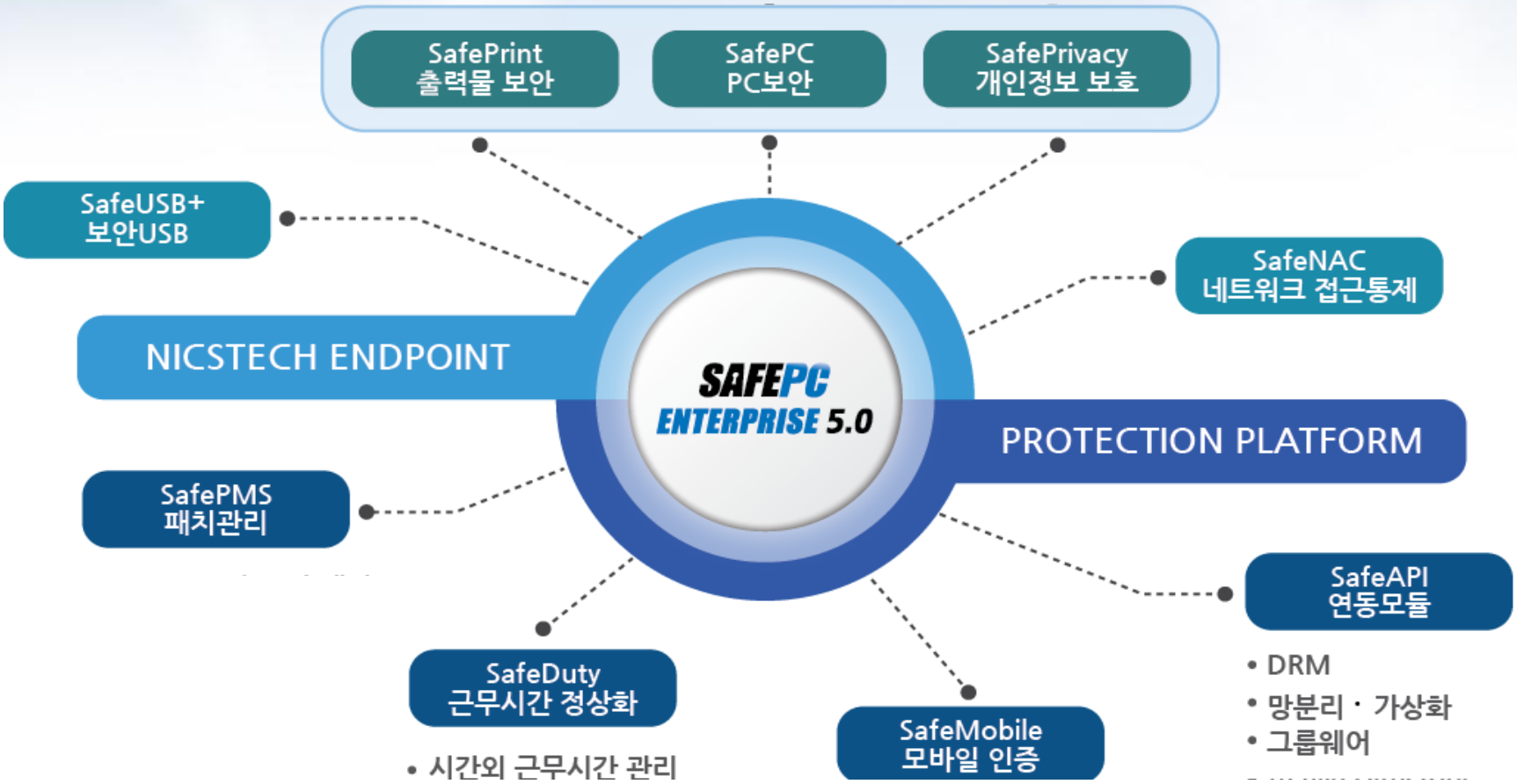
3 통합 관리 콘솔

4 통합 관리 서버

4.1 정보 보안 프레임워크

보안 정책 수립이 최우선 과제

4.2 통합 단말 Platform

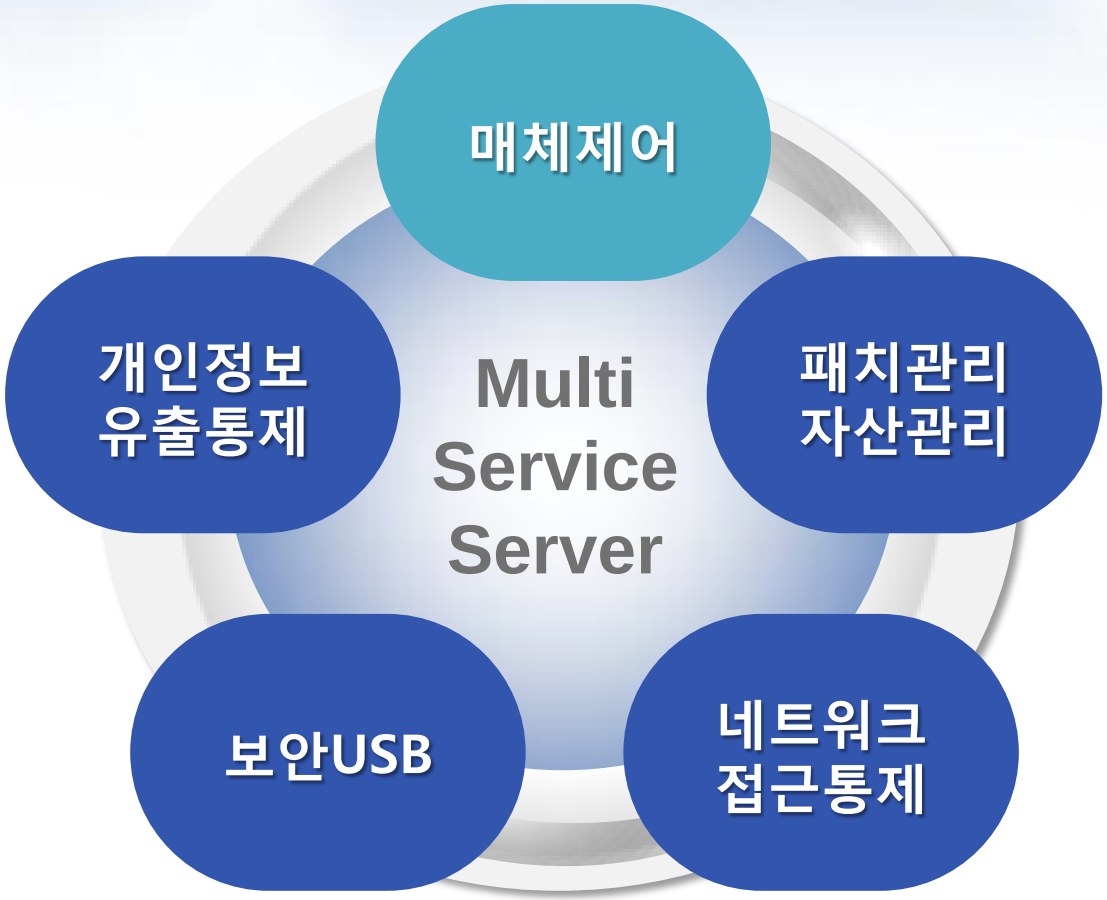


- **손쉬운 단말 보안 확장** (One-step Installation)
- **보안의 시너지 효과**
- **보안 솔루션간 충돌 이슈 제거**
- **보안 정책의 일원화**

4.3 통합 관리 콘솔

- **통합** Dashboard **단말 가시성 극대화**
- **정확하고 편리한** Reporting / **보안 감사**
- **통합된 관리자 권한 관리**
- **일관된 보안 정책**

4.4 통합 관리 서버



- 개발 Code 레벨의 기능 통합화 지원
- 서버 관리 및 유지보수 비용 절감
- 비즈니스 가용성 극대화
- One License Package

Contribution

Marathon

Innovation

닉스테크㈜

Network Integrated computing Service Provider

감사합니다

- Tel. : 02-3497-8900
- Email : jangjh@nicstech.com

하나의 작은 움직임이 큰 기적을.

Smart Security & Service
NICS TECH