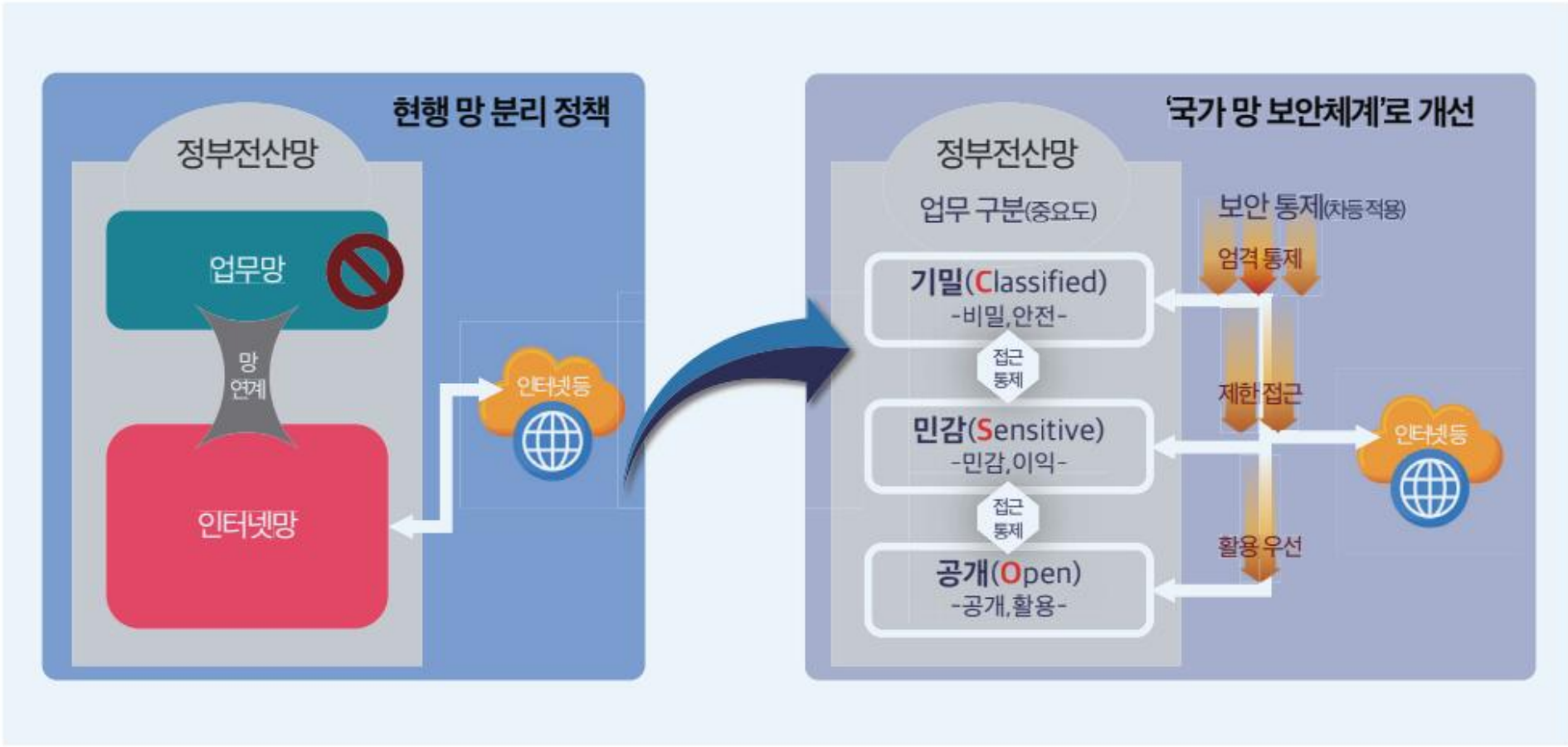
망분리 환경과

안전한 웹 브라우징

AIRCODE

차례

획일적 망분리에서 업무 중요도별 보안 체계

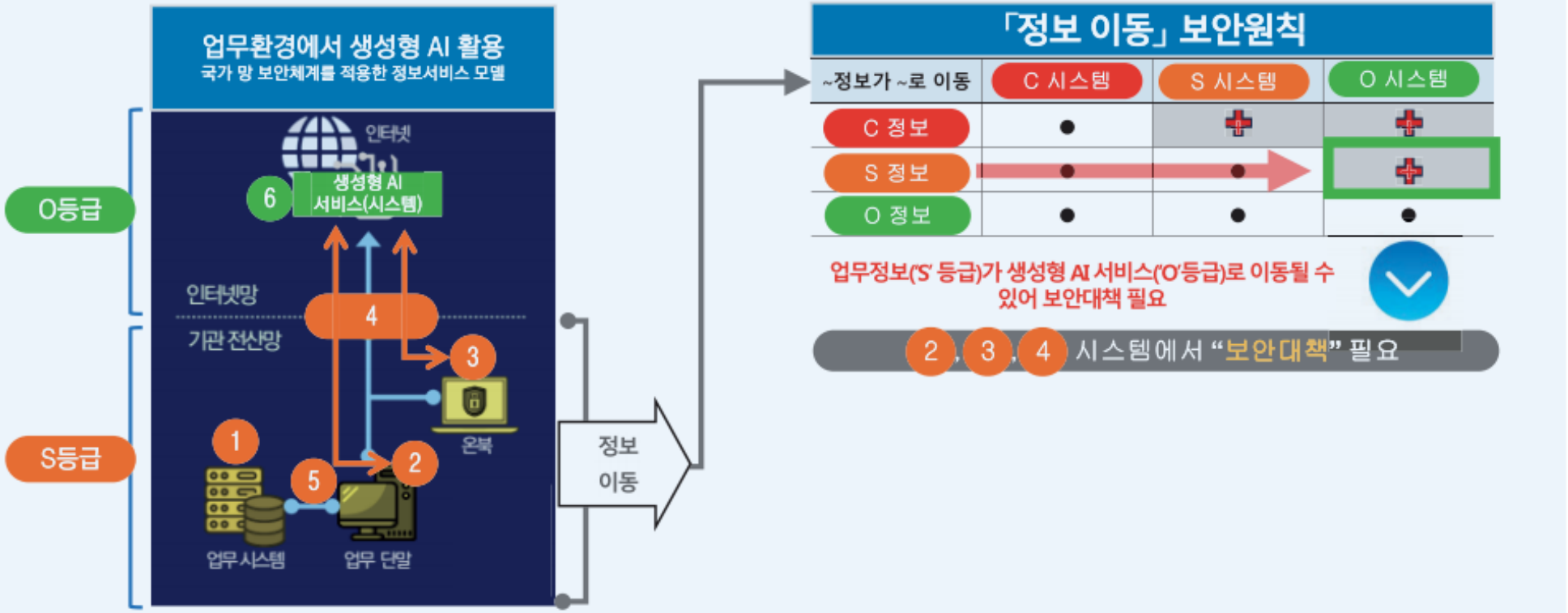


국가 망 보안체계 보안 가이드라인(Draft)

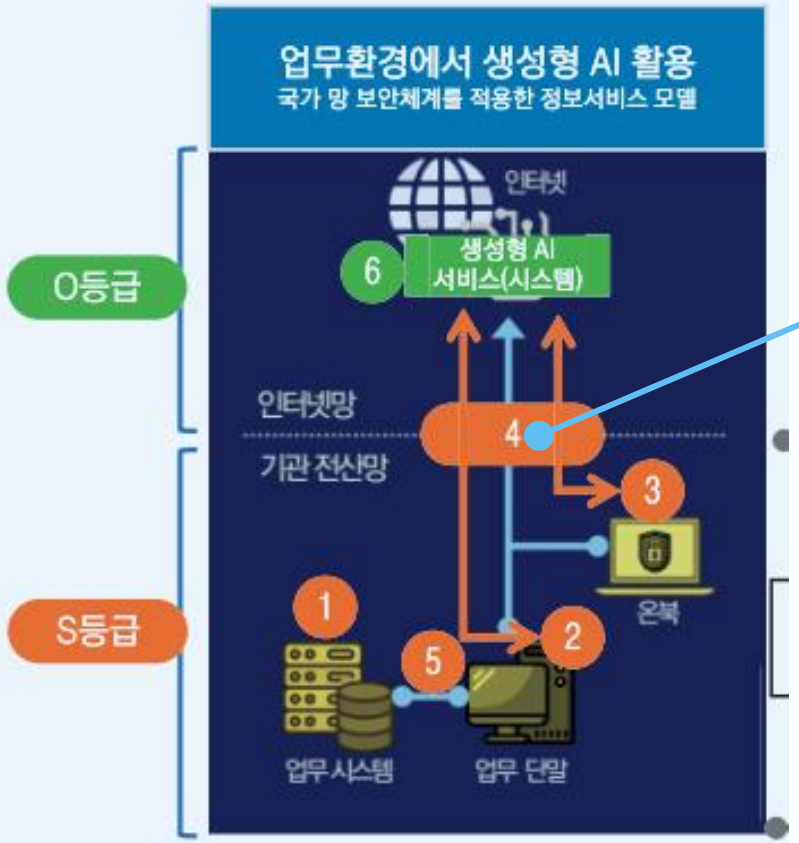
N²SF에서 웹 브라우징

AirRBI
Zero Trust Browsing

그림 3-15 「정보 이동」 보안원칙을 적용한 위협식별 및 보안대책 적용지점 판단



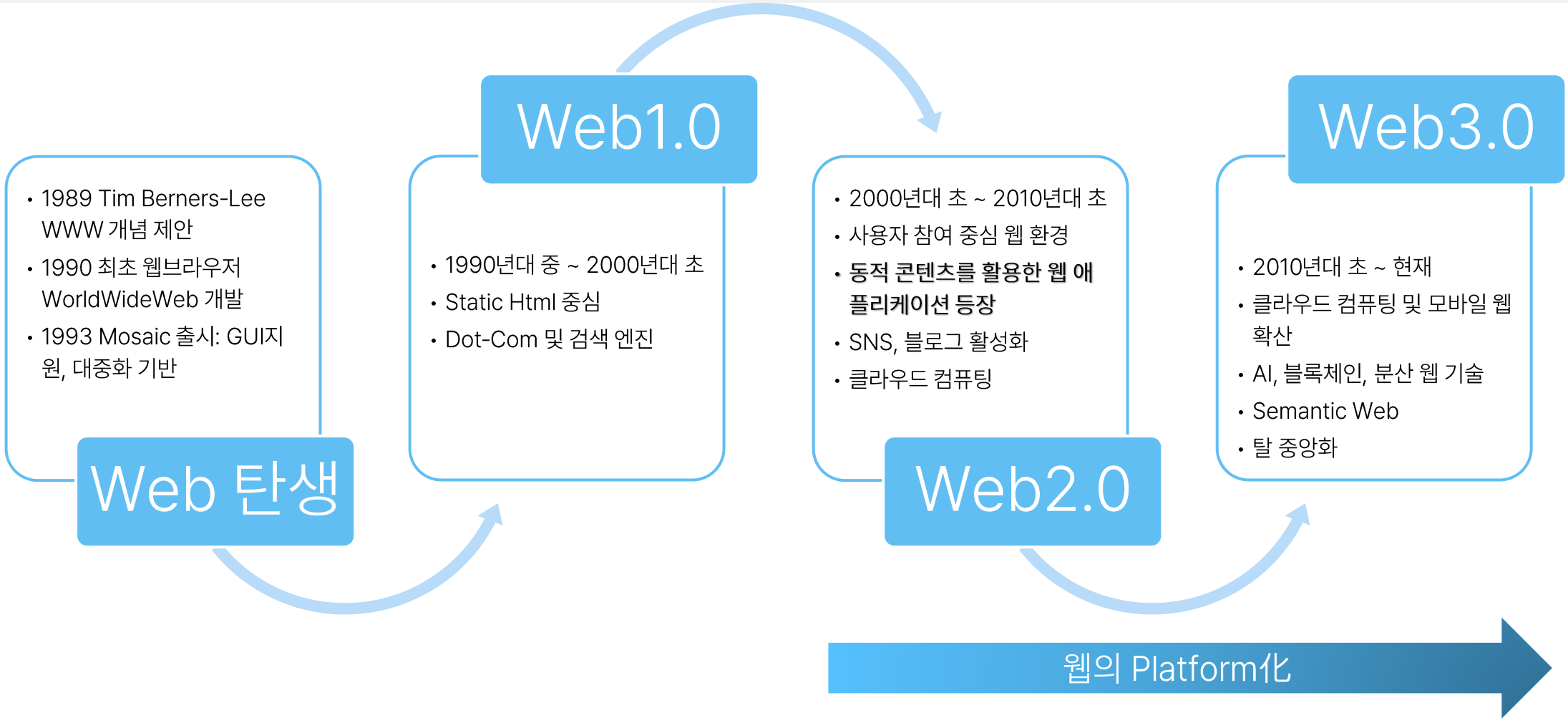
N²SF에서 웹 브라우징



구분	PC	특징	적용
인터넷 전용 PC + 내부망 PC	2대	• 가장 보안성이 높음 • 사용자 불편 • 장비 도입 및 유지보수 증가	• 가장 높은 보안이 필요
VDI	1대	• 비용 절감 가능, • 성능 이슈 가능 • 중앙 통제 용이	• 관리용이성/비용 • 웹 이외의 인터넷 사용
RBI	1대	• 보안 유지와 편의성 제공 • 중앙 통제 용이 • 웹만 가능	• **웹 브라우징 위주 인터넷 사용**

Web 보안의 중요성: Web의 플랫폼化

웹의 발전


Web 탄생
• 1989 Tim Berners-Lee WWW 개념 제안
• 1990 최초 웹브라우저 WorldWideWeb 개발
• 1993 Mosaic 출시: GUI지원, 대중화 기반
Web1.0
• 1990년대 중 ~ 2000년대 초
• Static Html 중심
• Dot-Com 및 검색 엔진
Web2.0
• 2000년대 초 ~ 2010년대 초
• 사용자 참여 중심 웹 환경
• 동적 콘텐츠를 활용한 웹 애플리케이션 등장
• SNS, 블로그 활성화
• 클라우드 컴퓨팅
Web3.0
• 2010년대 초 ~ 현재
• 클라우드 컴퓨팅 및 모바일 웹 확산
• AI, 블록체인, 분산 웹 기술
• Semantic Web
• 탈 중앙화
웹의 Platform化

Web을 통한 공격 증가

AirRBI
Zero Trust Browsing

악성 코드 감염의 주요 경로 중 하나가 웹 브라우징

- 2023년 한국 발생한 웹 기반 사이버 위협 건수가 총 983만 7841건
- 국내 사용자의 21%가 웹 기반 공격의 대상됨(Kaspersky Security Network)

브라우저는 신뢰할 수 없는 코드와 데이터를 실행하는 환경임

- JavaScript, WebAssembly, 동적 콘텐츠(iframe, AJAX 등)
- 사용자가 직접 클릭하지 않아도 자동 실행되는 악성 코드(Drive-by Download)가 로컬에서 실행 가능

브라우저는 가장 많이 사용되는 소프트웨어임

- 브라우저 자체의 보안 취약 존재
- 제로데이 공격 표적

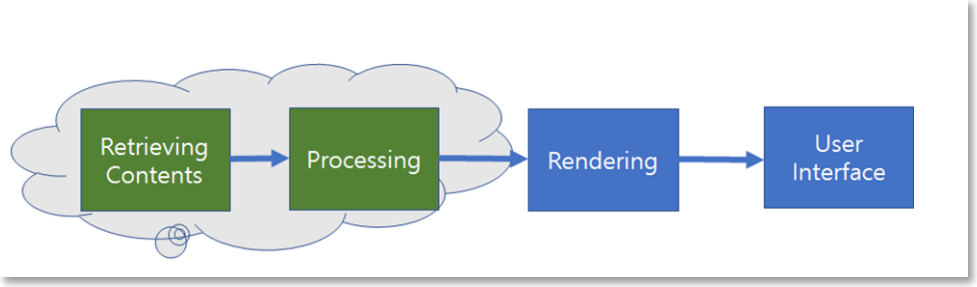
웹 브라우저 공격과 보안 솔루션

RBI를 포함한 다중 계층 방어(Defense-in-Depth) 모델을 구축 필요

보안 솔루션	웹 브라우저 공격 차단	한계점
방화벽(Firewall)	불가능	웹 트래픽(HTTPS)은 대부분 허용됨
웹 애플리케이션 방화벽(WAF)	일부 가능	서버 측 웹 공격(SQL Injection, XSS 등) 방어 가능하지만, 클라이언트(브라우저) 내 공격은 방어 불가
IDS/IPS (침입 탐지/방지 시스템)	일부 가능	패턴 기반 탐지는 가능하지만, HTTPS 트래픽 내부의 공격은 탐지 어려움
엔드포인트 보안(EDR, XDR)	가능	브라우저 내 악성 코드 실행 감지는 가능하지만, 탐지 후 대응에 한계가 있음
SWG(Secure Web Gateway)	가능	Zero-day 위협 존재
EDR	가능	악성 코드 실행 후 탐지 및 대응

AirRBI 주요 기능

격리된 공간에서 브라우징



사용자 환경과 웹 사이 물리적 분리 제공

- 웹 브라우징 중 유해 요소 침해가 가능한 Retrieving과 Processing을 원격 브라우저에서 실시
- 안전한 렌더링 정보를 사용자의 디바이스로 전송
- 단말에서는 렌더링 정보를 활용하여 화면을 구성하고
- 사용자 입력 처리

추가적인 단말 설치가 불필요

- 범용적인 브라우저(Chrome, Edge 등)을 사용
- 추가적인 단말 설치 불필요
- 업그레이드 등 관리가 용이
- 단말 어플리케이션 간 충돌 원천 배제, 단말 리소스 보장

AirRBI 주요 기능

격리된 공간에서 브라우징

제로 트러스트 철학에 부합

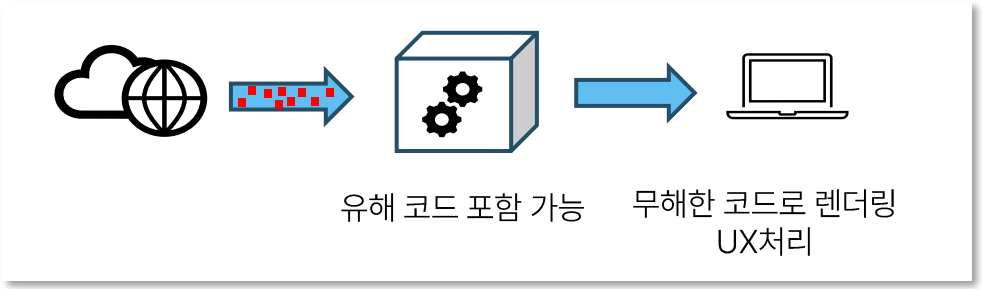
- 모든 콘텐츠를 신뢰하지 않고 모는 잠재적 위협을 차단

웹을 통한 알려지지 않은 위협 방어

- 제로데이 위협에 대한 보호 제공
- 알려지지 않은 악성 코드 (benign-looking malware)에 대한 완전한 보호 제공
- 브라우저 취약점 이용 공격(예: XSS, 드라이브 바이 다운로드) 차단

애플리케이션 계층 위협에 대해 뛰어난 보호

- 웹과 브라우저를 통한 위협 제거



제로트러스트와 AirRBI

AirRBI
Zero Trust Browsing

최소 권한 원칙

- 사용자가 꼭 필요한 리소스에만 접근
- 웹 브라우저는 기본적으로 외부 콘텐츠를 로컬 환경에서 실행하는 특성
- AirRBI는 웹 콘텐츠를 원격에서 실행, 사용자가 사용하기 위한 최소한의 콘텐츠만 단말에서 실행

모든 것을 의심

- AriRBI는 웹 콘텐츠를 격리된 환경에서 렌더링하여 단말에는 안전한 픽셀 스트림(또는 SVG)만 전달

내부 네트워크 보호

- 네트워크 내부로 악성 코드가 침투할 가능성을 최소화해야
- RBI를 사용하면 브라우징 트래픽이 네트워크와 단절된 별도의 환경에서 처리
  내부 네트워크로의 전파를 차단

AirRBI 특장점

높은 HTML 호환성 보장 – 일반 웹 브라우저와 동일한 사용자 경험 제공

사용 거부감 최소화

- 빠른 처리 속도
- 일반 웹 브라우저와 동일한 UX

빠른 처리 속도

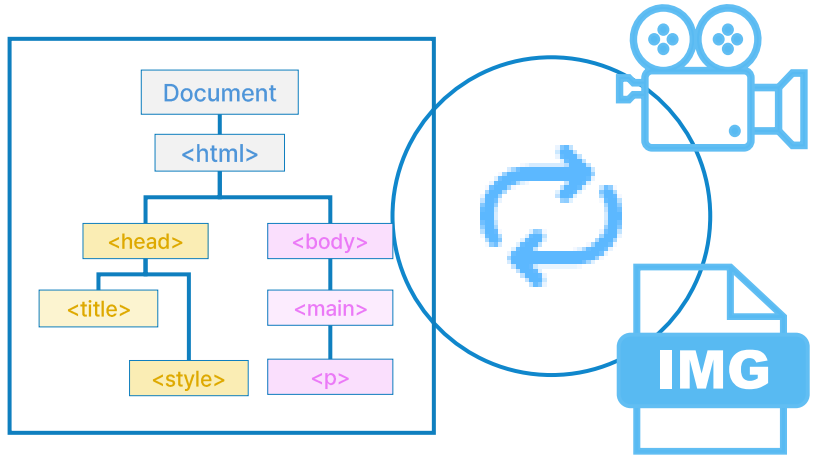
- Hybrid Streaming
- 최적화된 이미지 처리
- 다양한 Level에서 동영상 재 전송

일반 웹 브라우저와 동일한 사용자 경험

- 최신 Chromium 엔진 채택
- 다양한 사용자 인터페이스 제공

AirRBI 주요 기능

Hybrid Streaming



보안 정책과 사이트 특성에 따른 적절한 Streaming 방식 채택

- 이미지 Streaming, 돔(텍스트) Streaming, Video Streaming 지원
- 3가지 스트리밍 방식 중 관리자가 사이트 성격, 사용자(그룹)에 따라 설정
- 일반적으로 돔 트리가 복잡할수록 돔을 처리하기 위한 단말 부하는 증가
- 이미지 혹은 동영상 스트리밍 경우 단말 성능에 따른 처리 속도 차이는 미미

하나의 페이지에서 다양한 스트리밍 적용

- 이미지 스트리밍의 경우 동영상이나 복잡한 애니메이션을 처리하는 데 많은 자원을 사용
- AirRBI는 하나의 페이지 내에서 동영상 혹은 복잡한 애니메이션 요소를 동영상으로 스트리밍하고 그 외 요소는 이미지 혹은 돔 객체로 전송하는 하이브리드 기술을 채택

서버 리소스 사용 및 처리 속도를 최적화

AirRBI 주요 기능

정보 유출 방지

외부 웹 페이지 사용 시

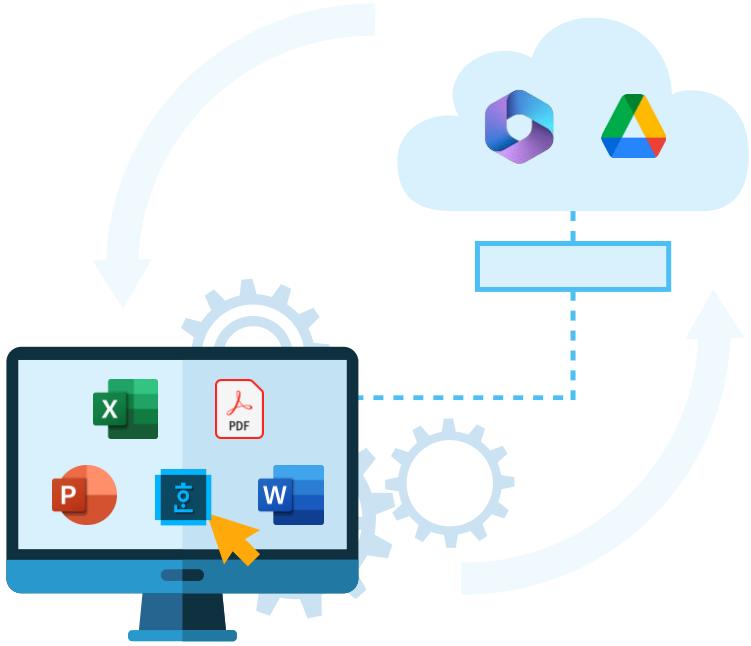
- 사용자별, 그룹별, 사이트 별 클립보드 사용 설정
- 사용자별, 그룹별, 사이트 별 파일 업로드 기능 설정
- 사이트별, 사용자별, 그룹별 사용자 입력 방지 설정
- 3rd Parties DLP 연동 제공(Option)

내부 업무용 웹 페이지/어플리케이션 사용 시

- 사용자별, 그룹별, 사이트 별 클립보드 사용 설정
- 사용자별, 그룹별, 사이트 별 파일 다운로드 기능 설정
- 사용자별, 그룹별, 사이트 별 인쇄 사용 설정
- Watermark 설정

AirRBI 주요 기능

첨부 파일에 의한 위해 요소 방지



사용자 단말과 물리적으로 분리된 환경에서 문서 확인/수정

- 문서 감염에 의한 단말 및 네트워크 감염 원천 차단
- 파일 미리 보기 기능 제공
  - ㄴ MS 오피스 문서(워드, 엑셀, 파워포인트), HWP, PDF
- Microsoft 365, Google Docs를 지원
  - ㄴ 원격에서 격리된 웹 환경에서 문서 작업

파일 다운로드 제어

- 사용자별, 그룹별, 사이트 별 파일 다운로드 기능 설정
- 안전하지 못한 사이트에서 파일 다운로드 원천 차단

3rd Parties 연동을 통한 파일/문서 유해 판단 및 제거(Option)

- 사용자 단말과 격리된 샌드박스 활용
- Virus Checker, CDR 등

AirRBI 주요 기능

정책 탬플릿을 활용한 정책 설정

다양한 정책 항목에 대한 설정 묶음을 템플릿으로 관리/적용, 설정된 템플릿을 사이트와 사용자(혹은 그룹) 조합으로 적용

템플릿

- 격리 방식
  - 격리, 차단, 우회
- 스트리밍 방식
  - 이미지, 돔, 동영상
- 파일 다운로드
- 파일 업로드
- 클립보드 사용
- 읽기 전용
- 인쇄
- 워터마크
  - 간격, 투명도, 글자크기

+

사이트

- 정책이 적용될 Target URL을 정의
  - 도메인 단위(aircode.com)
  - 사이트 단위(www.aircode.com)

사용자

- 정책이 적용될 사용자를 정의
  - 개별 사용자
  - 사용자 그룹별

AirRBI 주요 기능

안정적인 설치 및 지원

자동화 설치 지원

- 고객사이트와 버전마다 설치 디스크 자동 만들기
- 고객사 현장에서 설치 환경 진단
- 고객사 현장에서 설치 자동화를 위한 마법사 지원
- 고객사 현장에서 네트워크 및 서비스 연결 검사
- 고객사 현장에서 DB 문제를 진단하고 해결 지원

기대 효과

- 설치에 필요한 시간과 리소스 최소화
- 설치자 실수에 의한 설치 실패 및 비정상적 동작 최소화
- 제3자(대리점/관리자 등) 엔지니어에 의한 설치 가능

설치 디스크 자동화

- 발행 서버에서 고객사와 솔루션 버전마다 자동으로 설치 디스크를 생성과 라이선스 설치

현장에서 설치 자동화

- 고객사 서버에 설치 디스크를 자동 설치
- 고객사 서버에서 솔루션 자동 설치

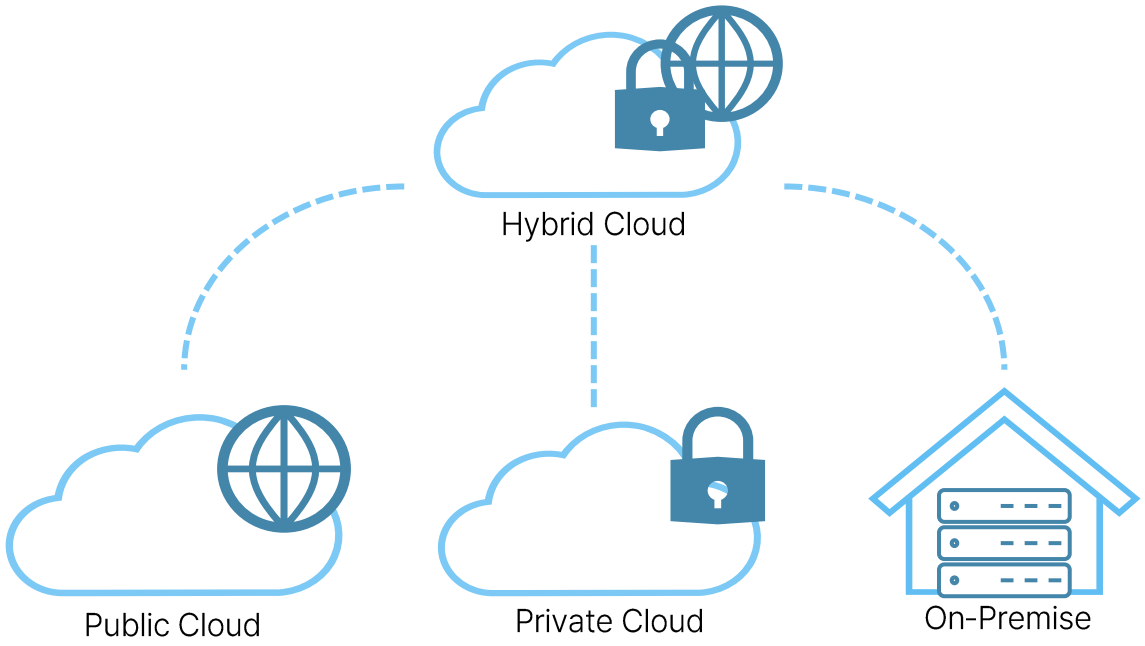
현장 점검과 검사 및 문제 해결

- 계정 검사, 권한 검사, 인증서 점검, 실행상태 점검 등
- 네트워크 선로 및 방화벽 검사, 서비스 연결 검사 등

대리점/총판 엔지니어를 위한 기술지원

- 대리점, 사이트별, 버전별 형상관리 체계 지원
- 설치 디스크 및 설치 프로그램의 다운로드 지원

다양한 배포 및 고객 맞춤형 기술 지원



다양한 배포 옵션

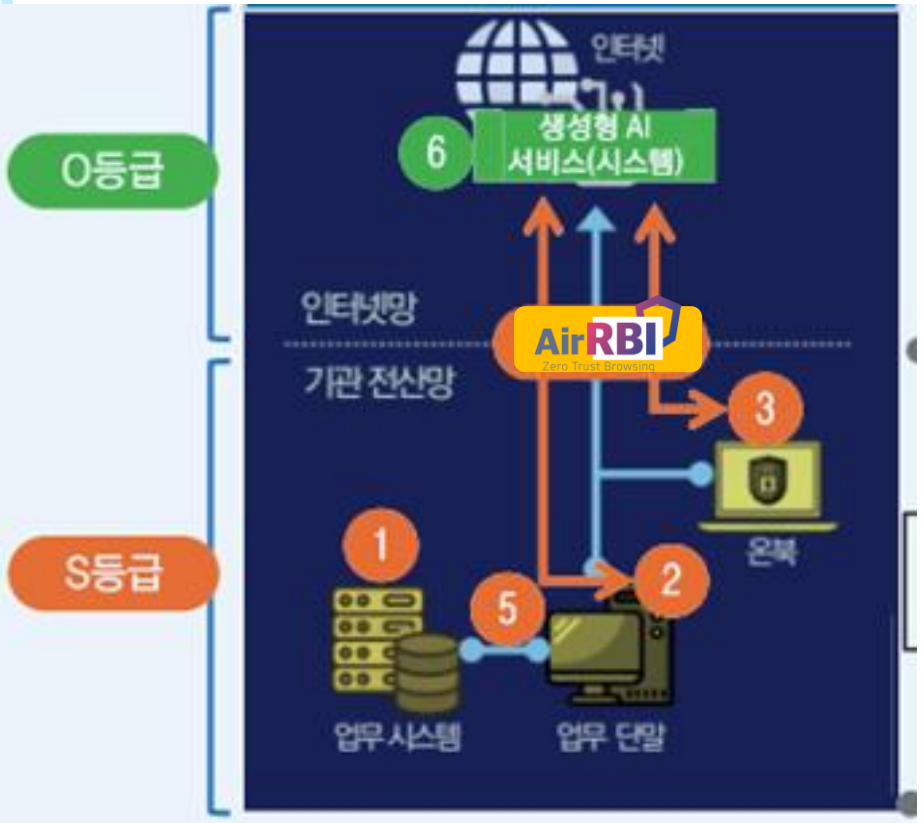
- 기업 내부 On-Prem 과 Public Cloud 모두 설치 가능
- On-Prem 과 Public Cloud 연결하여 scale In/Out 위한 하이브리드 설치 가능

Customizing

- 고객의 요구에 따라 필요한 기능 혹은 제3자 어플리케이션과의 API 연동 기능 제공
  - 주요 SSO 연동
  - CDR 연동
  - DLP 연동
  - SWG 연동 ....

N2SF와 AirRBI

외부 인터넷을 웹으로 이용할 경우 최상의 선택



경제적 솔루션

- OS 등 다양한 라이선스 감소
- 리소스 감소
- 단순한 관리/유지 보수

제로트러스트 철학에 부합

원격 근무와 AirRBI

원격 근무자에게 안전한 웹 브라우징 환경 제공

원격 근무자의 브라우징 안전성 향상

- 원격 근무자는 상대적으로 안전한 회사 네트워크 밖에서 위치하므로, 다양한 보안 위험에 직면
- 악성 사이트나 스크립트가 사용자의 시스템에 접근하는 것을 방지
- 악성 다운로드와 실행 차단
  - 파일을 다운로드할 때 격리된 환경에서 악성 여부를 확인
  - 악성 코드 포함 시 파일이 실제 장치에 다운로드 되거나 실행되지 않도록 차단

기업 데이터 보호

- 민감한 데이터 노출 방지:
  - 원격 근무자는 클라우드 기반 문서나 애플리케이션에 접속할 때 중요한 기업 데이터를 처리
  - RBI는 격리된 환경에서만 이 데이터를 처리, 데이터 유출이나 악성 코드 감염을 방지

네트워크 및 시스템 성능 최적화

- VPN 부하 감소
- RBI를 적용하면 VPN 없이도 안전한 인터넷 브라우징이 가능하므로 VPN 사용량을 줄이고 성능을 개선

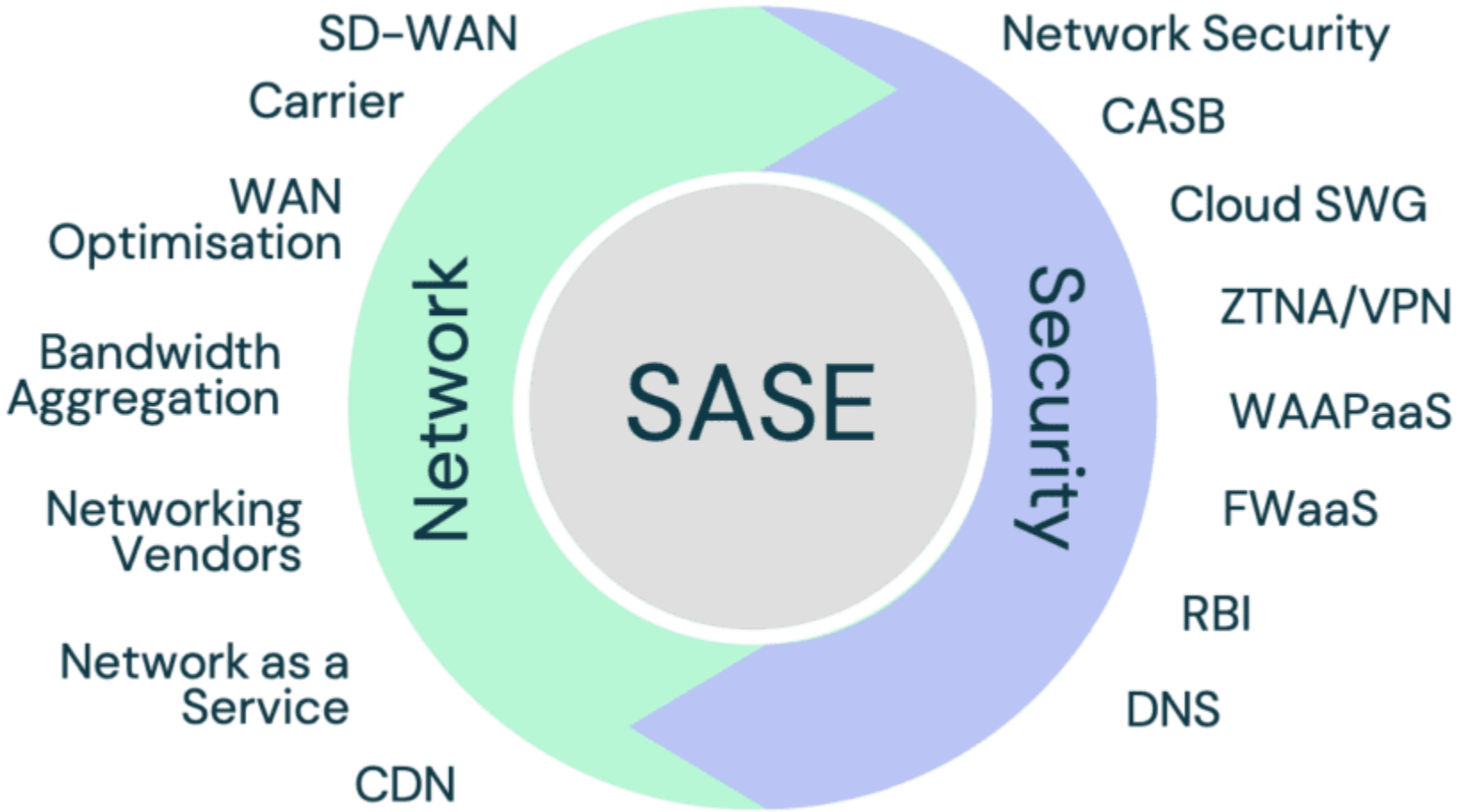
로컬 리소스 소모 최소화

- 스크립트나 광고, 트래킹 요소를 로컬 장치에서 실행하지 않고 클라우드에서 처리
- CPU, 메모리, 배터리 소모 절약

효율적 보안 관리:

- 중앙에서 브라우징 활동을 관리

RBI를 포함한 다중 계층 방어(Defense-in-Depth) 모델을 구축 필요



감사합니다