The Inspirations For Cyber Security

웹격리 및 강화된 인증기술을 활용한 제로트러스트 구현

2023. 11. 28.

SOFTCAMP

Zero Trust Security

> **Never trust, Always verify.**
> 절대 신뢰하지 말고, 항상 검증하라.

제로 트러스트 주요 원칙

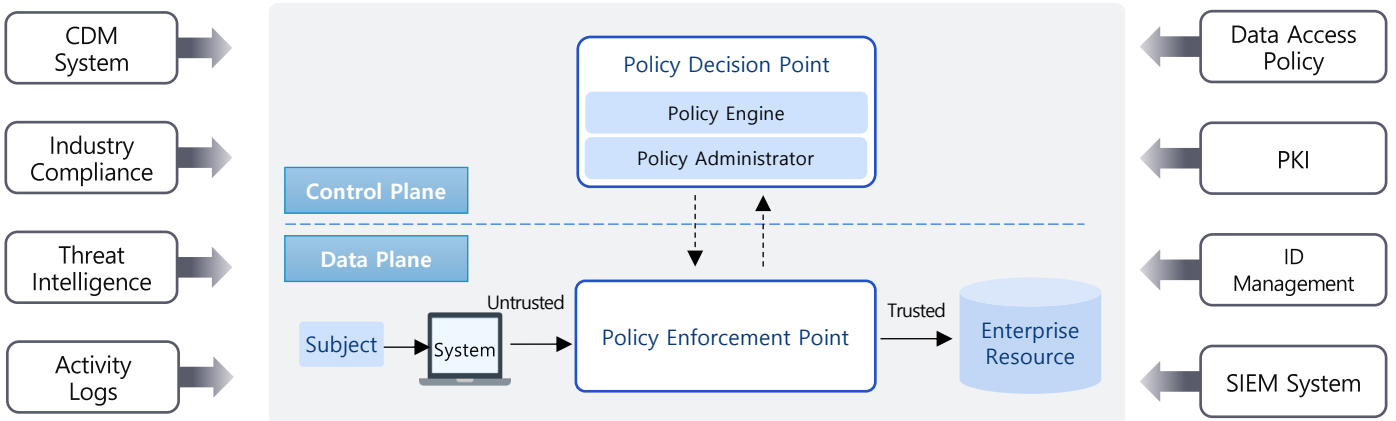
명시적인 확인

최소 권한 액세스 부여

침해 가정

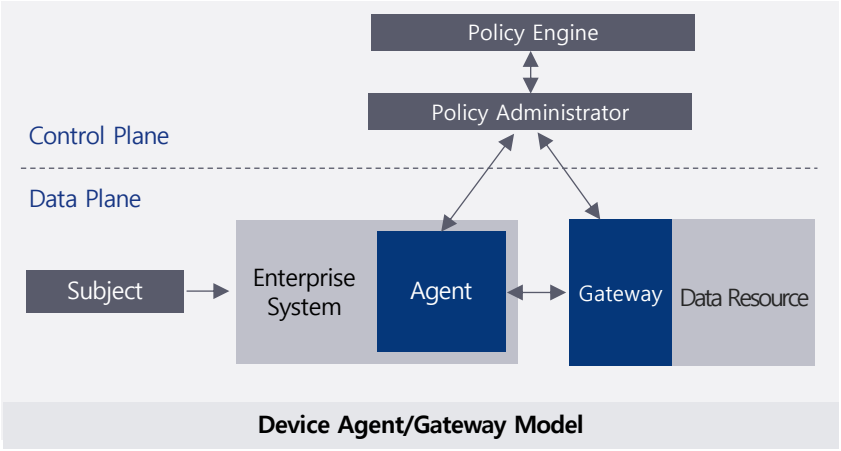
SOFTCAMP

제로트러스트 아키텍처 구성 요소 – NIST



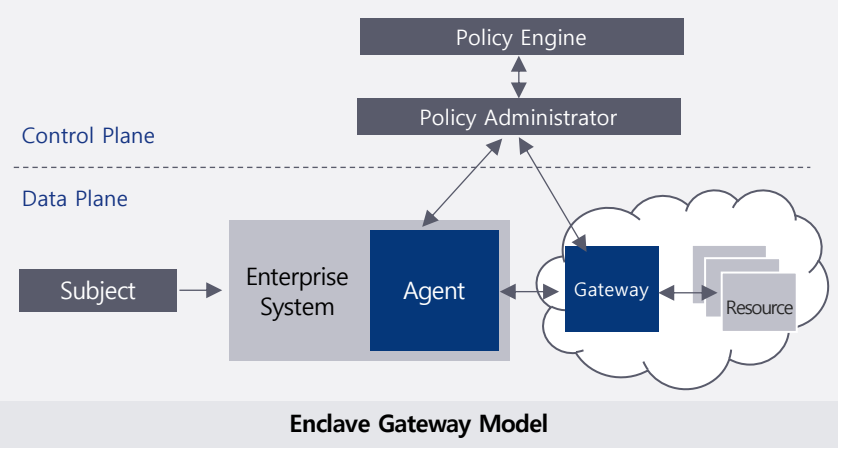
핵심 구성 요소	• Policy Decision Point : 다양한 입력요소를 검토하여 자원에 대한 접근 허용 여부를 결정, Subject와 Resource 사이 통신 경로 관리 • Policy Enforcement Point Subject에게 할당된 정책 실행, 연결 활성화, 모니터링, 종료
입력 요소	• Resource에 대한 접근을 결정하기 위해 사용하는 다양한 요소 (Policy Information Point) • 정책 및 내부 정보 관리 Data Access Policy, CDM(Continuous Diagnostics and Mitigation)System, PKI, ID Management • 외부 법적 규제, 내 외부에서 발생하는 보안 위협 : Industry Compliance, Threat Intelligence • 각종 로그 및 분석결과 : Network and System Activity Logs, SIEM System
NW 구성 요소	• Control Plane : 정책관리를 하기 위한 통신 흐름을 제어하고 관리 • Data Plane : Subject와 Resource 사이의 통신 흐름을 제어하고 관리

제로트러스트 아키텍처 구현 방법 – NIST (1)



Device Agent/Gateway Model

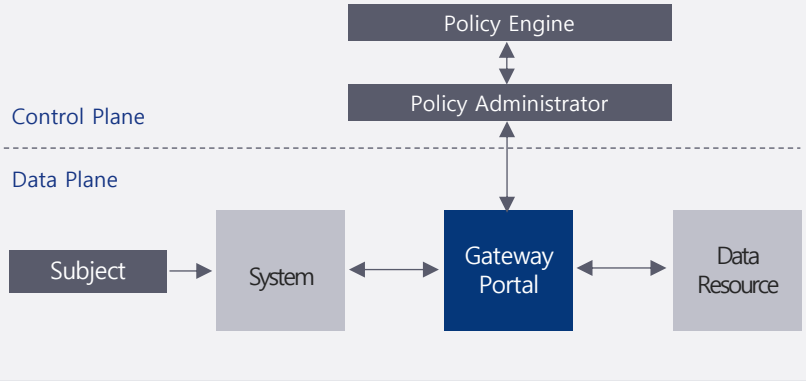
배포 모델	주요 기능	장점	단점
Device Agent / Gateway Model	- 장치에 에이전트를 설치하여 통신 - 게이트웨이를 통해 리소스 접근	- 고도화된 접근 제어 가능 - 분산된 리소스에 대한 일관된 정책 적용	- 에이전트 관리 및 업데이트의 복잡성 - 다양한 장치 유형에 대한 호환성 문제



Enclave Gateway Model

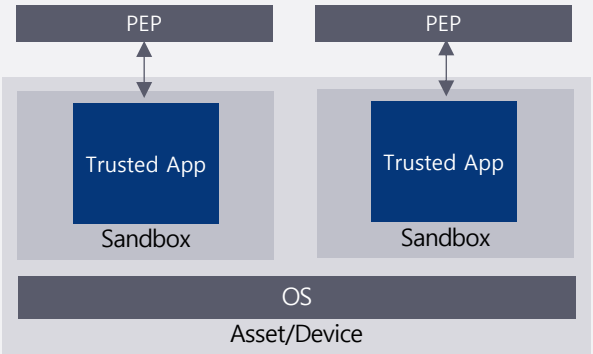
배포 모델	주요 기능	장점	단점
Enclave Gateway Model	- 정의된 보안 영역(enclave) 내의 리소스 접근 - 게이트웨이를 통한 집중적 접근 관리	- 보안 영역 내에서 일관된 보안 정책 적용 - 중앙에서의 관리와 모니터링 용이	- 병목 현상 발생 가능성 - 확장성 및 유연성에 대한 한계

제로트러스트 아키텍처 구현 방법 – NIST (2)



Resource Portal Model

배포 모델	주요 기능	장점	단점
Resource Portal Model	- 사용자가 특정 포털을 통해 필요한 리소스에 접근 - 사용자 중심의 접근 제어	- 사용자 경험 향상 - 리소스별 세분화된 접근 제어 가능	- 포털의 보안 취약점 발생 가능성 - 접속 디바이스의 보안태세를 점검할 수 없음



Application Sandboxes

배포 모델	주요 기능	장점	단점
Application Sandboxes	- 애플리케이션을 격리된 환경(sandbox) 내에서 실행 - 애플리케이션 간의 상호 작용 제한	- 높은 수준의 애플리케이션 보안 - 악성 코드의 피해 범위 제한	- 성능 저하 가능성 - 애플리케이션 호환성 문제

Zero Trust 기반 기술

Zero Trust Architecture의 배치 방법을 실제로 구현할 수 있게 하는 기반 기술은 다음과 같다.

Software Defined Perimeter (SDP)

- SDP는 클라우드 환경과 같은 분산된 IT 환경에서 보안을 강화하기 위한 접근 제어 솔루션입니다. SDP는 모든 사용자와 장치를 초기에 신뢰하지 않는 것으로 간주하며, 검증된 사용자와 장치만 지정된 IT 리소스에 접근할 수 있게 합니다.

Identity Aware Proxy (IAP)

- 사용자의 신원과 콘텍스트를 기반으로 웹 애플리케이션 및 리소스에 대한 접근을 제어하는 프록시 서비스입니다. 전통적인 VPN 대신 사용될 수 있습니다.

Remote Browser Isolation (RBI)

- 사용자의 기기에서 웹 콘텐츠를 직접 렌더링하지 않고 원격 서버에서 웹 콘텐츠를 렌더링하고, 그 결과를 안전하게 사용자의 브라우저에 전달하는 보안 방법입니다.

이들 기술은 기존의 전통적인 통신보안인 VPN의 한계점을 극복하고, 제로트러스트의 원칙인 모든 요청은 검증되어야 하고, 네트워크 내부의 위치와 관계없이 접근 권한이 제한되어야 하는 원칙에 잘 부합하는 기술들입니다.

각 조직의 특정 환경 및 요구 사항에 따라 이러한 기술을 단독으로 사용하거나 혼합하여 사용할 수 있습니다.

SDP (Software Defined Perimeter)

1) 정의

Software Defined Perimeter (SDP)는 전통적인 네트워크 경계 기반의 보안 방식을 대체하는 접근 제어 아키텍처입니다. SDP는 사용자와 장치의 신원에 기반하여 안전한 네트워크 접근을 제공하며, 국내 및 국외의 클라우드 환경에 배포된 애플리케이션 및 서비스에 대한 접근을 보호합니다.

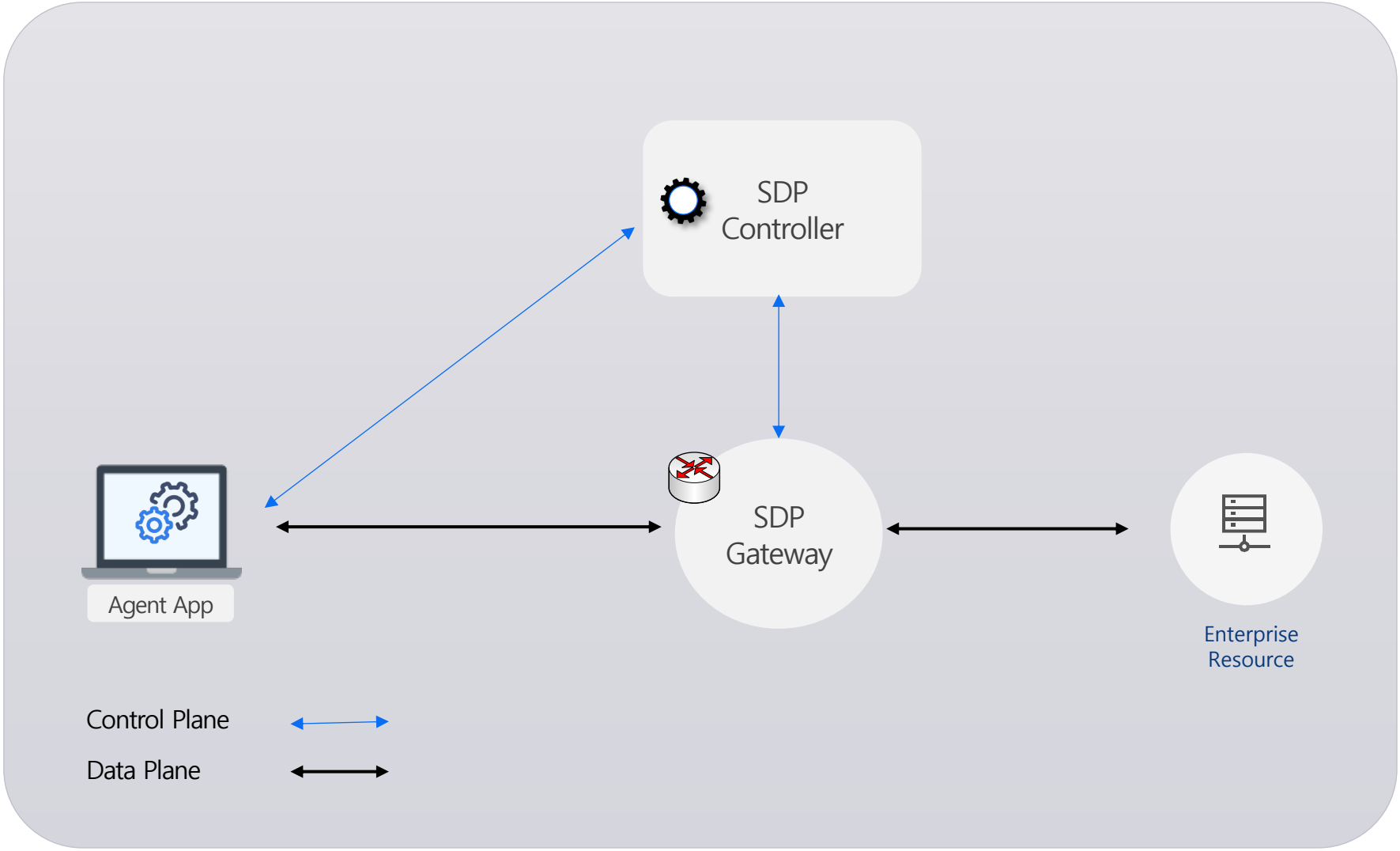
2) 특징

- 불필요한 가시성 감소: 무인가 사용자는 네트워크 자원을 "보지" 못합니다.
- 신원 기반 접근 제어: IP 주소 대신 사용자와 장치의 신원을 중심으로 접근을 제어합니다.
- 다단계 인증: 다양한 인증 메커니즘과 통합됩니다.
- 동적 접근 제어: 상황에 따라 접근 권한을 동적으로 변경합니다.

3) 제로트러스트 보안 관점에서 특징

SDP는 "Zero Trust" 보안 모델의 원칙과 밀접하게 연관됩니다. 이 모델의 기본 원칙은 모든 사용자와 장치를 신뢰하지 않는 것입니다. SDP는 이 원칙을 구현하여 모든 접근 요청에 대한 검증과 인증을 요구합니다.

SDP (Software Defined Perimeter)



IAP (Identity Aware Proxy)

1) 정의

- Identity Aware Proxy (IAP)는 사용자와 장치의 신원 정보를 사용하여 애플리케이션 및 리소스에 대한 보안 액세스를 제공하는 중간 서버 또는 게이트웨이입니다. IAP는 특정 리소스에 대한 사용자 액세스를 동적으로 허용하거나 거부하기 위해 사용자 및 장치의 콘텍스트 및 정책을 평가합니다.

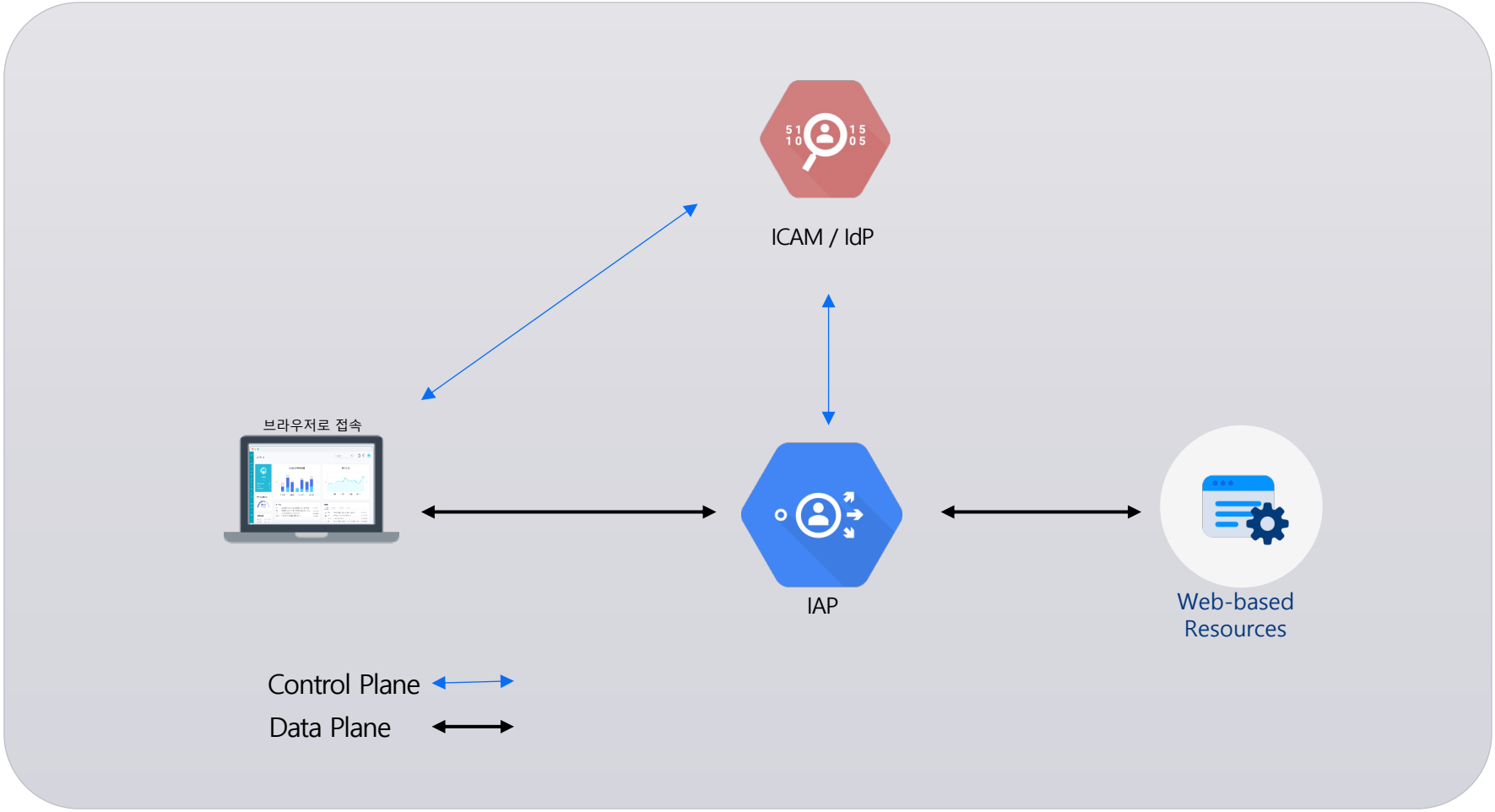
2) 특징

- 신원 중심의 접근 제어: 사용자의 신원 및 콘텍스트에 기반한 동적인 접근 제어가 가능합니다.
- VPN 대체: IAP는 전통적인 VPN을 대체하여 더 간단하고 효율적인 원격 접근을 제공합니다.
- 신원 및 콘텍스트 기반의 정책 평가: 실시간으로 사용자와 장치의 상태를 평가하여 접근 결정을 내립니다.

3) 제로트러스트 보안 관점에서 특징

- IAP는 제로트러스트 보안 모델의 핵심 원칙에 따라 동작합니다. 이러한 원칙에는 내부 네트워크나 외부 네트워크에 있더라도 모든 접근 요청을 신뢰하지 않는 것이 포함됩니다. IAP는 모든 액세스 요청을 검증하고, 사용자의 신원과 콘텍스트에 기반한 동적 접근 제어를 제공하여 제로트러스트 모델을 구현합니다.

IAP (Identity Aware Proxy)



ICAM : Identity Credential Access Management
IdP : Identity Provider

RBI (Remote Browser Isolation)

1) 정의

- Remote Browser Isolation (RBI)은 웹 콘텐츠의 렌더링을 사용자의 로컬 장치에서 원격 서버로 분리하는 보안 기술입니다. 이 방식에서 사용자의 웹 브라우저는 원격 서버에서 실행되며, 사용자 장치에는 렌더링된 결과의 안전한 표현만 전송됩니다. 이로써 위험한 웹 콘텐츠로 인한 직접적인 공격이나 유해한 코드 실행을 방지할 수 있습니다.

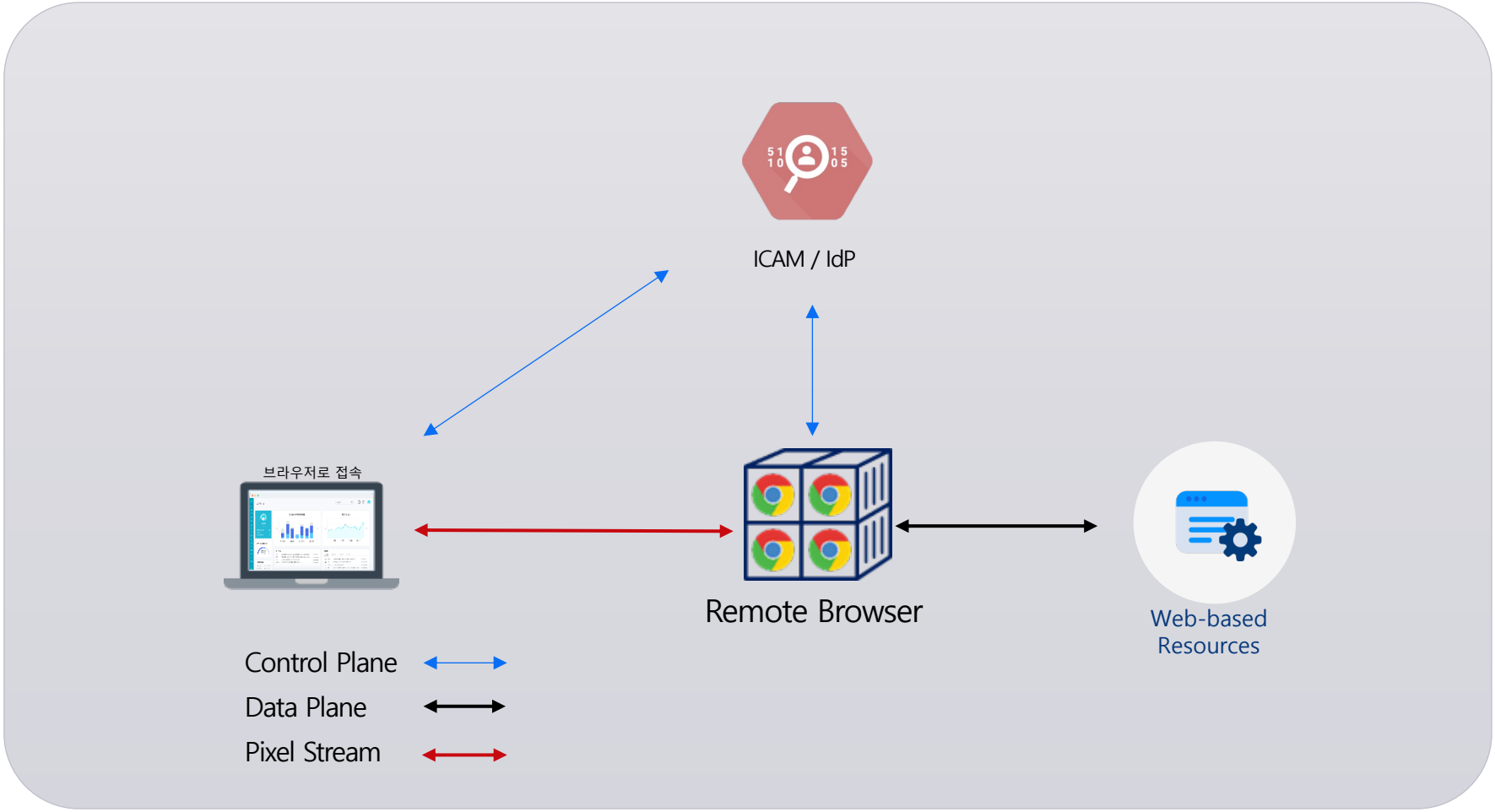
2) 특징

- 원격 실행: 웹 페이지와 관련된 모든 프로세스는 원격 서버에서 실행됩니다.
- 로컬 장치와의 분리: 웹 콘텐츠와 로컬 시스템 사이에 격리된 환경을 제공하여 공격 벡터를 줄입니다.
- 높은 사용자 경험 유지: 원격 렌더링에도 불구하고 사용자에게는 일반적인 웹 브라우징 경험을 제공합니다.

3) 제로트러스트 보안 관점에서 특징

- 모든 웹 콘텐츠는 신뢰할 수 없다고 가정하고, 로컬 장치에서 실행되는 대신 원격 서버에서 격리된 환경에서 실행됩니다. 따라서, 웹 콘텐츠에 대한 "신뢰하지 않기"의 접근 방식을 취합니다.

RBI (Remote Browser Isolation)



ICAM : Identity Credential Access Management
IdP : Identity Provider

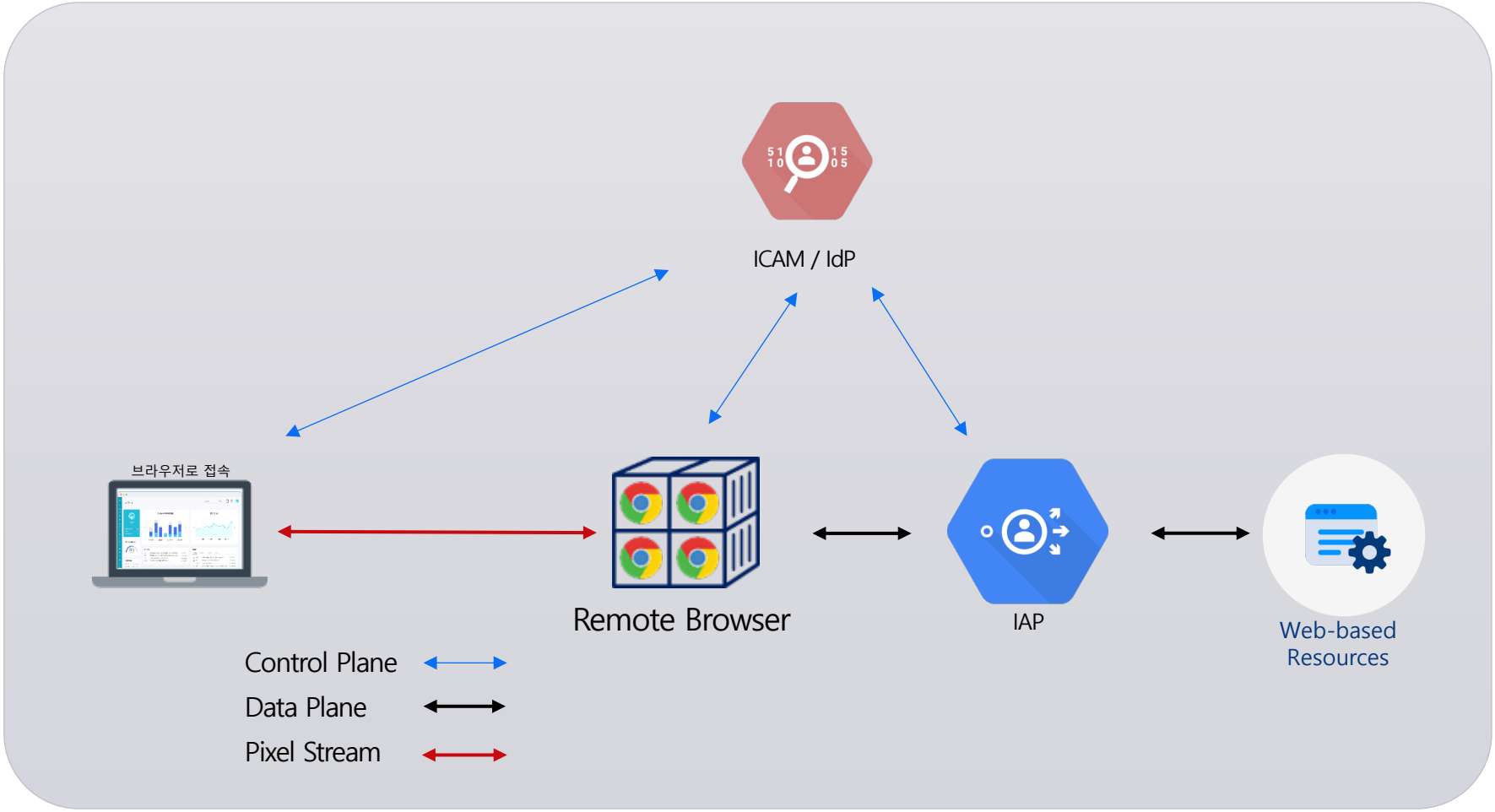
IAP + RBI 의 융합

1) 제로트러스트 보안 관점에서 특징

- 신원 중심의 웹 접근: IAP는 신원 기반의 접근 제어를 제공하므로, 사용자와 장치의 신원 및 상태를 기반으로 웹 리소스에 대한 접근을 동적으로 허용하거나 제한합니다.
- 웹 컨텐츠 격리: RBI는 사용자의 브라우저와 웹 콘텐츠 간의 격리를 통해 웹 콘텐츠로부터의 위협을 차단합니다. 그 결과, 모든 웹 콘텐츠는 신뢰 되지 않는 것으로 간주되고 원격 서버에서 처리됩니다.
- 종합적인 방어: 신원 기반 접근과 웹 컨텐츠의 격리는 사용자와 리소스를 보호하기 위한 두 개의 강력한 방어층을 제공합니다.

› Resource Portal Model의 단점인 접속 디바이스의 보안 설정 모니터링이 불가능하여 발생할 수 있는 취약점과 위협을 격리하여 보다 강력한 보안을 구현합니다.

IAP + RBI 의 융합



ICAM : Identity Credential Access Management
IdP : Identity Provider

주요 Zero Trust 구현 기술 비교 (ChatGPT 생성 비교표)

		SDP	IAP	RBI	IAP+RBI
기본 특성	정의	동적 액세스 제어 프레임워크	사용자 신원과 컨텍스트 기반 프록시	웹 브라우징 활동의 원격 격리	사용자 인증 및 웹 브라우징 활동의 원격 격리
	기본 원칙	"모든 것이 미신뢰"	"신원 기반 접근"	"브라우징 활동의 완전한 격리"	신원 기반 접근 + 브라우징 활동의 격리
인증 및 접근 제어	사용자 인증	중요함	중요함	일반적으로 미지원	중요함
	MFA	지원	지원	외부 솔루션과의 통합 가능	지원
구성 및 관리	구성 복잡성	상대적으로 높음	상대적으로 낮음	중간 수준	상대적으로 높음
	확장성	다양한 환경 적용 가능	클라우드에 최적화	클라우드 또는 온프레미스 환경에 적용	클라우드 환경에 최적화
통신 및 성능	통신 방식	양방향 통신, 보안 강화	양방향 프록시 통신	렌더링 된 결과의 단방향 전송	양방향 프록시 + 렌더링 된 결과의 단방향 전송
	지원 통신	모든 통신(C/S, Web)	Web 만 지원	Web 만 지원	Web 만 지원
안정성 및 보안	안정성	동적 네트워크 변화에 잘 대응	중앙화된 서비스로 안정성 제공	브라우징 세션의 격리로 높은 보안성 제공	중앙화된 서비스 + 브라우징 세션의 격리로 안정성 제공
	데이터 보호	동적 전송 경로 제어로 보호	프록시 중간에서 보호	원격 서버에서 처리되므로 엔드 유저 장치는 보호됨	프록시 및 원격 서버에서의 이중 보호
지원/ 적용 분야	통합성	다양한 보안 도구와의 통합 요구	클라우드 서비스와 잘 통합	웹 게이트웨이 또는 다른 보안 솔루션과의 통합 가능	클라우드 서비스 및 웹 게이트웨이와의 통합
	최적 환경	전체 네트워크에 적용 가능	클라우드 및 웹 애플리케이션에 최적화	웹 브라우징 및 웹 기반 애플리케이션에서의 위협 방지	클라우드 및 웹 기반 애플리케이션에서의 위협 방지 및 인증
관련 제품		Akamai EAA Zscaler Private Access	Google IAP Zscaler Identity Proxy Cloudflare Access F5 BIG-IP Access Policy Manager	SOFTCAMP RemoteBrowser Menlo Security Web Isolation Zscaler Browser Isolation Cloudflare RBI Broadcom Web Isolation	SOFTCAMP SHIELDGate Zscaler Zero Trust Exchange Cloudflare Cloud Platform

ChatGPT에게 제로트러스트 구현 기술 선택을 하게하면....

Zero Trust 보안 모델을 구현하는 데 어떤 기술을 사용할지 결정하는 것은 많은 변수들을 고려해야 합니다.

그러나 주어진 옵션들을 기반으로 개인적인 의견을 제시한다면:

1.목적 및 환경에 따라 선택:

1. 웹 브라우징 활동에 집중된 보안을 원한다면 **RBI**를 사용하거나 **IAP+RBI** 조합을 사용하여 클라우드 환경과 웹 브라우징 활동 모두의 보안을 강화할 수 있습니다.
2. 클라우드 기반의 애플리케이션에 대한 접근을 중심으로 보안을 강화하고자 한다면, **IAP**가 적합합니다.
3. 전체 네트워크에 적용 가능한 보안 모델을 구현하려면 **SDP**가 적합합니다.
4. 전통적인 원격 접속 보안을 원한다면, **VPN**을 사용할 수 있습니다. 그러나 Zero Trust 모델의 기본 원칙에 완전히 부합하지 않을 수 있습니다.

2.통합 및 호환성:

1. 기존의 IT 인프라와의 통합 및 호환성이 중요한 경우, 그러한 요구 사항을 가장 잘 충족하는 솔루션을 선택해야 합니다.

3.비용과 리소스:

1. 각 솔루션의 도입 및 유지보수 비용, 그리고 필요한 리소스를 고려하여 가장 효율적인 선택을 해야 합니다.

› 개인적으로, 현대의 클라우드 중심의 IT 환경에서는 **IAP**나 **IAP+RBI** 조합을 사용하여 사용자 신원 및 컨텍스트 기반의 접근 제어와 웹 브라우징 활동의 보안을 동시에 강화하는 것이 바람직하다고 생각됩니다. 특히 RBI를 통해 웹 기반의 위협으로부터의 보안을 높이는 것은 매우 중요합니다.

› 그러나 결국에는 조직의 특정 요구 사항, 기존 인프라, 예산, 그리고 보안 목표 등을 종합적으로 고려하여 최적의 선택을 해야 합니다.

내부에서 인터넷 사용

내부에서 인터넷 사용시 보안의 한계

- 유해 사이트 차단용 **웹 필터의 한계**(신규 URL 에 대한 구분 어려움)
- Client PC에 백신, EDR, XDR 등을 설치해도 **랜섬웨어 방어**가 어렵다.
- 외부 수신 메일에 대한 **BEC 방어**가 어렵다.(바로가기, 첨부파일)
- 인터넷을 통한 문서 또는 **중요 정보 유출 차단**이 어렵다.
- 인터넷 사용 내역을 **모니터링** 하기 어렵다.

대응 방안들

망 분리 환경에서 인터넷 전용 VDI 운영

- VDI 하드웨어 및 소프트웨어 등 **대규모 투자 필요**.
- 부트스톰(Boot Storm), Disk 병목 등으로 인한 **속도 저하** 발생.
- VDI **내부가 감염** 되는 것을 피할 수 없다.
- VDI 내부에 별도의 **보안 솔루션 구축이 필요**하다.
- 사용자 증감에 따른 **관리가 어렵다**.

인터넷 전용 물리 PC 운영

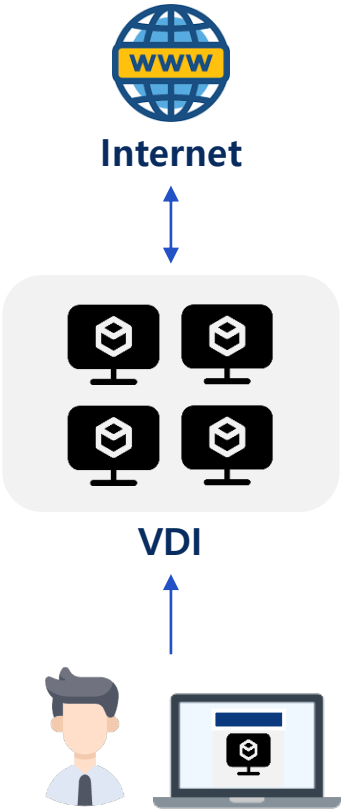
- 2대의 장비를 사용함으로 인한 공간, 구입 등 한계
- 내부망과 **자료 교환이 어려움**
- 보안 솔루션 등 이중 투자 필요

온북 사용

- 노트북 등 **고성능 사양 필요**
- 완벽한 대안이 될 수 없다.(노트북 자체 가상화 기능 활용)
- 성능 저하 및 정보유출, 자체 감염을 피할 수 없다

인터넷 활용 이슈

VDI based Access



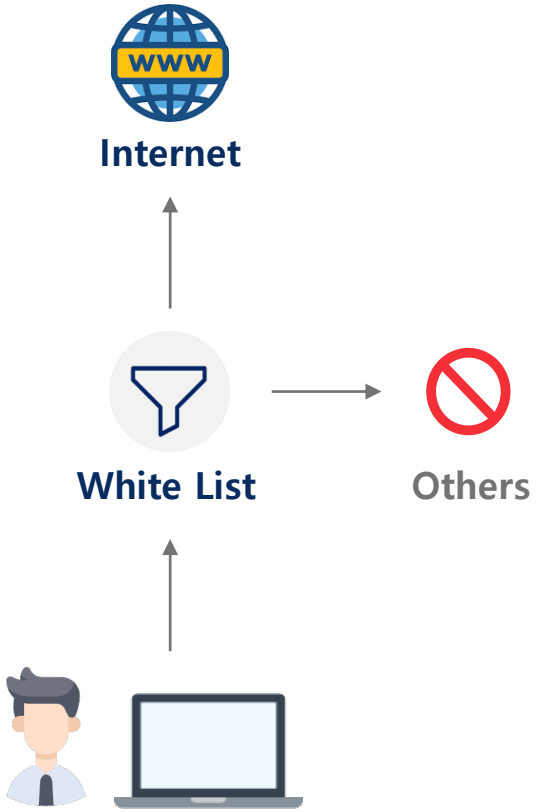
- 인터넷 접속을 VDI를 통해 수행함으로써 보안 효율성 향상
- 최초 로그인 및 사용자 체감에 불만족 및 **고비용 구조**

TCO ↑

관리 부담 ↑

생산성 ↓

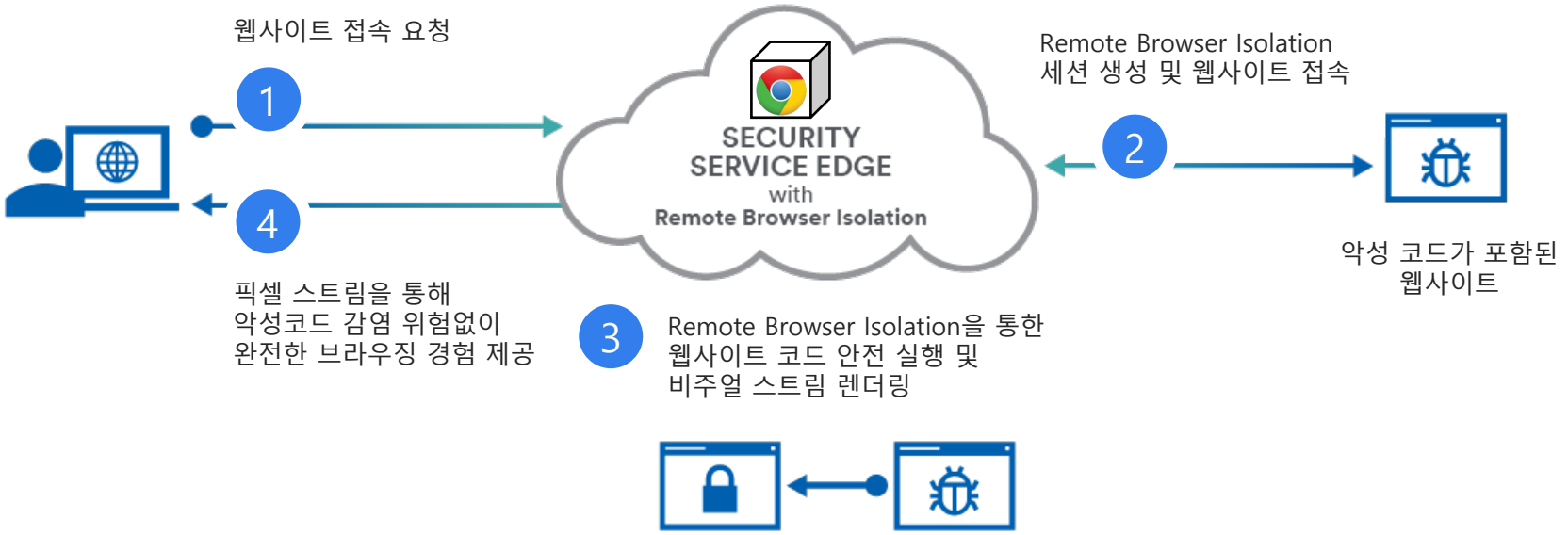
White List Access



- 인터넷으로 접속이 허락된 도메인만 접속 가능
- 도메인 **허용 신청 등 소요시간 증가**로 생산성 저하
- White list 도메인 증가로 관리 부담 가중

RBI 기술을 활용한 인터넷 접속 격리

› **원격 브라우저 격리(RBI)는** 서버 가상 브라우저로 인터넷을 접속하고,
사용자 브라우저에서는 접속한 화면을 픽셀 스트림으로 전송 받는 기술입니다.

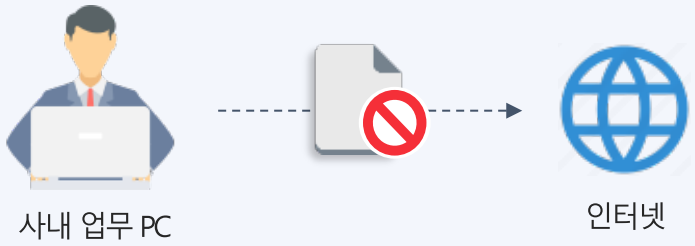


특장점

- 접속하는 사용자의 PC에서 접속한 인터넷 컨텐츠의 (악성코드가 포함된) 어떤 스크립트도 End Point(접속한 PC)에서 실행되지 않음
- 알려지지 않은 인터넷 사이트를 통해 다운로드 받은 파일도 내부 PC에서 안전하게 사용 가능

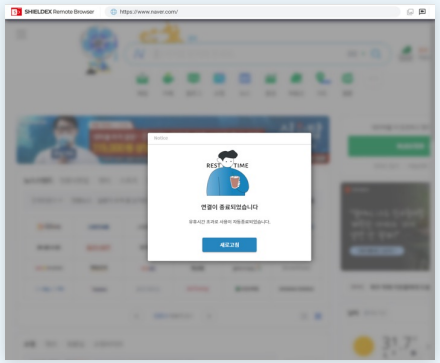
RBI 기술을 활용한 인터넷 접속 격리

› 가상 브라우저를 직접적으로 제어할 수 있으므로, 기존에 구현하지 못했던 각종 보안 기능을 실현합니다.

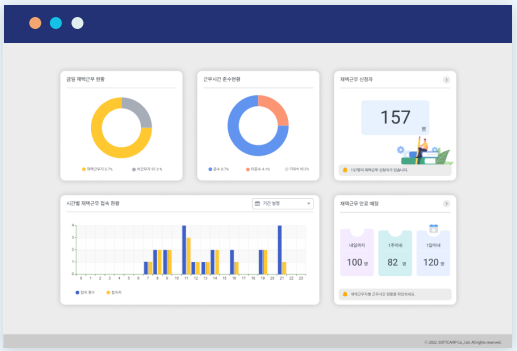


자료 무단 반출 통제

민감 정보 입력 통제



유휴시간 경과시 화면 잠금



인터넷 사용 이력

RBI 기술을 활용한 인터넷 접속 격리

›조건에 따른 다양한 사용 정책 부여(Zero-Trust Conditional Access)

› Zero-Trust Conditional Access 정책에 따라, 사용자의 환경 및 접속 대상 인터넷 컨텐츠를 모두 검사하고 정책을 집행합니다.

조건 판단

- 접속 사용자
- 접속 시간
- 접속 URL, 사이트 분류
- 파일 첨부
- 파일 다운로드
- 양식에 정보 전송

Policy Decision Point

Policy Engine

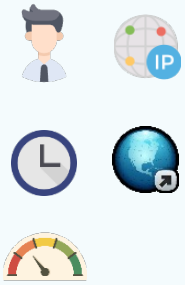
Policy Administrator

정책 판단 및 부여

집행 정책 목록

- 접속 허용/차단
- 키보드 입력 허용/차단
- 파일 첨부 차단
- 다운로드 파일 CDR 처리
- 다운로드 파일 웹디스크 저장
- 양식 입력정보 감사/통제

Subject



System

Policy Enforcement Point

Remote Browser

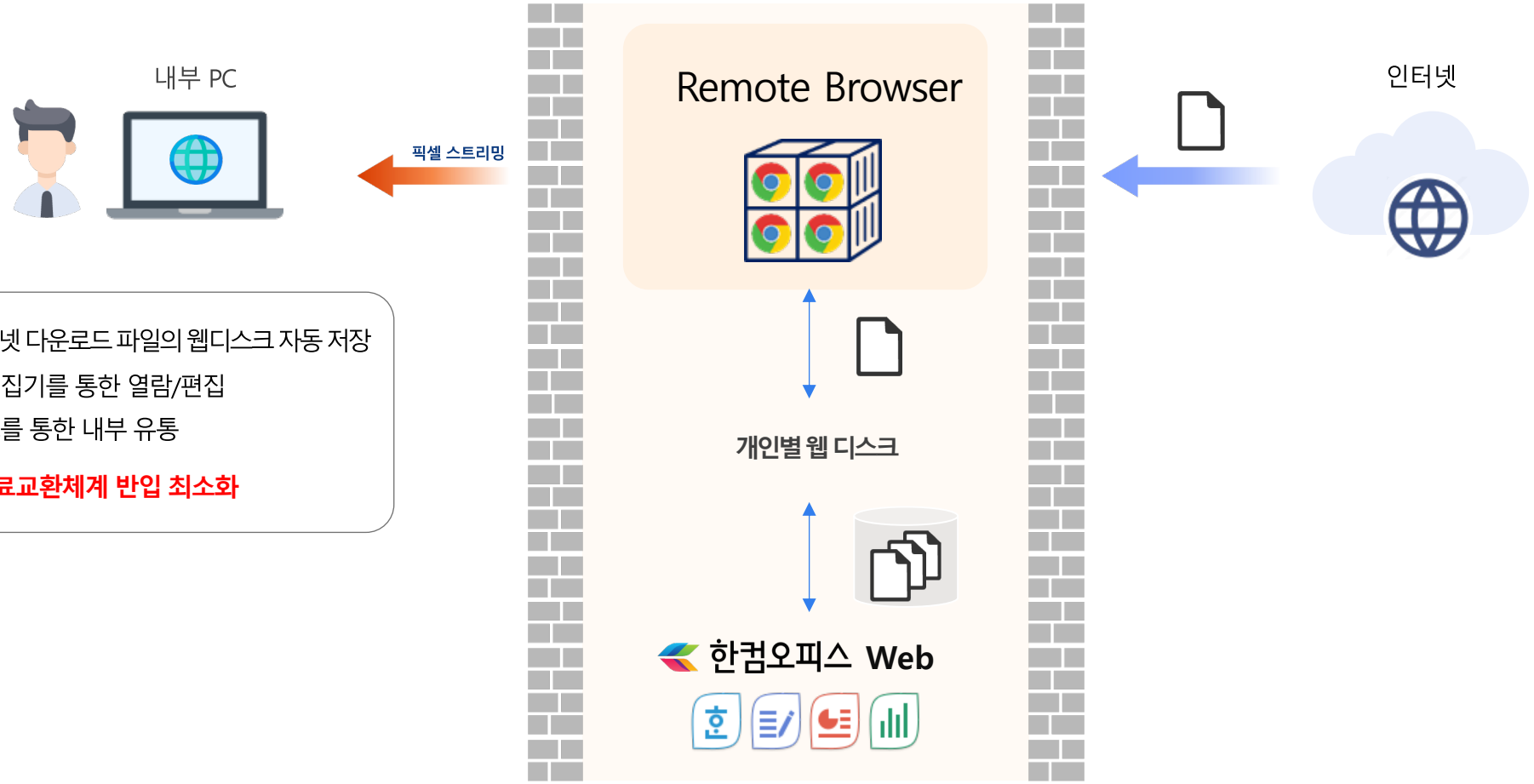
접속 허용/차단
및 정책 집행

Internet

RBI 기술을 활용한 인터넷 접속 격리

적용 사례 : 웹 디스크 / 웹 편집기를 통한 기능 확장

- 웹디스크를 통하여 인터넷 가상 브라우저로 파일 업로드/ 다운로드 / 열람 / 편집
- 인터넷 파일을 자료 교환 체계를 통한 반입 최소화하며 업무 수행



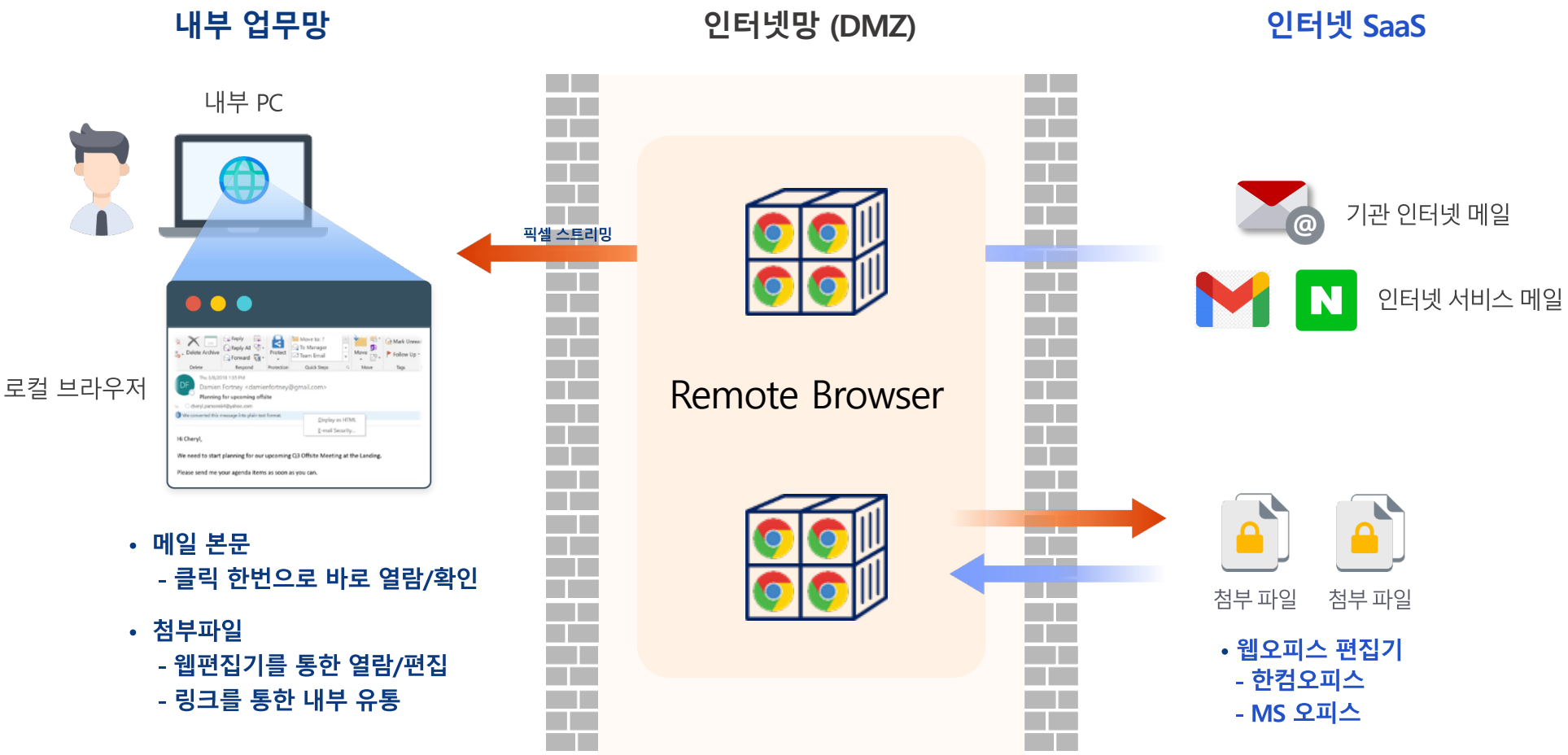
- 인터넷 다운로드 파일의 웹디스크 자동 저장
- 웹편집기를 통한 열람/편집
- 링크를 통한 내부 유통

➔ **자료교환체계 반입 최소화**

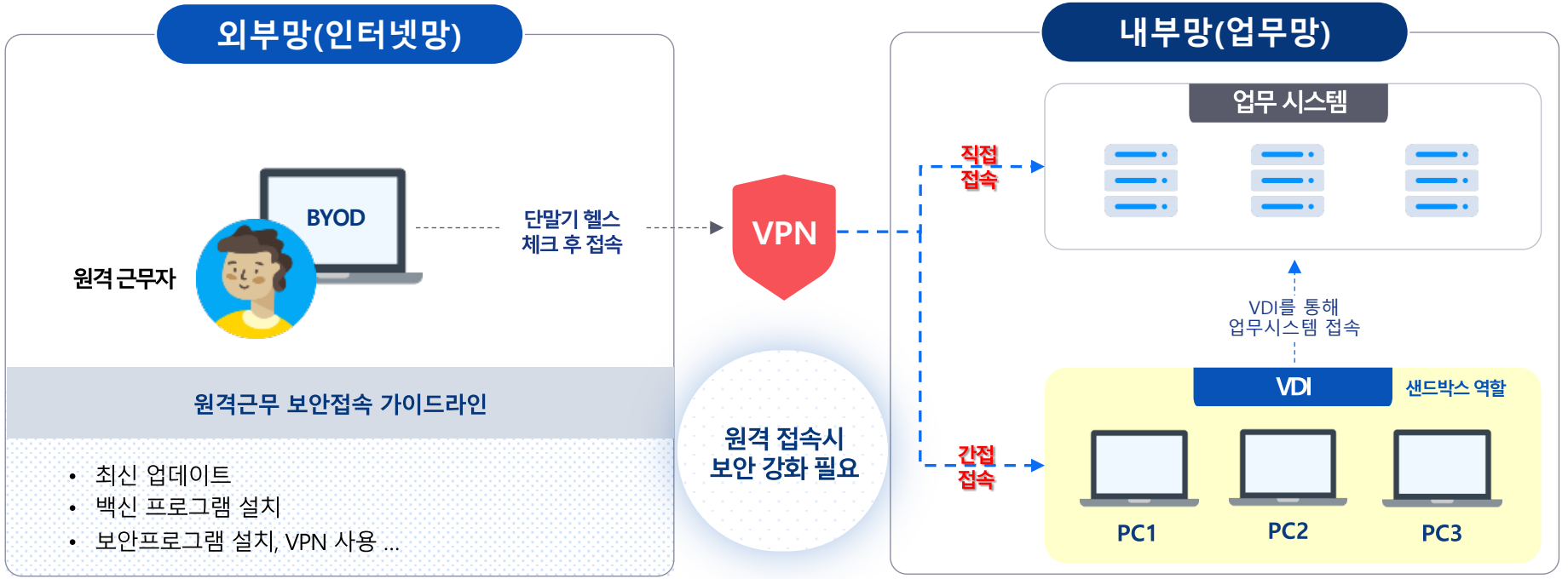
RBI 기술을 활용한 인터넷 접속 격리

적용 사례 : 내부망에서 인터넷 메일 열람

› 웹 격리 솔루션을 통해서 **웹 메일 및 업무를 위한 인터넷사이트를 허용**하여 편의성과 보안성 제공
(내부 업무망에서 인터넷 메일 열람 가능, 망연계 솔루션과 연계한 파일 반출입 승인처리)



현재 원격 접속 이슈(VPN)



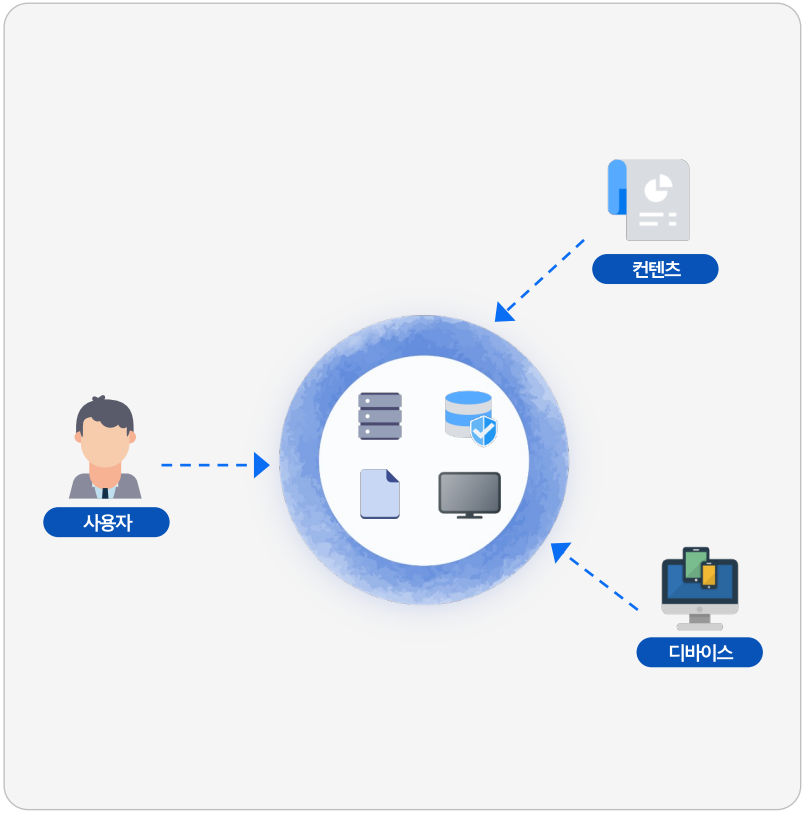
보안 이슈

- 외부 접속 PC에서 내부 시스템으로 **바이러스 등 침투 가능**
- 내부 업무 시스템의 외부 네트워크 노출 및 **자료 유출 가능**
- 내외부에 접속에 따른 조건부 **접근 사용정책 구현 불가**
- 업로드/다운로드 **파일 통제 이슈**
- 기존 업무**시스템 수정의 어려움**
- 외부 사용자 PC에 별도 보안 프로그램 설치 및 **관리 어려움**

제로트러스트 보안 어떻게 할 것인가?

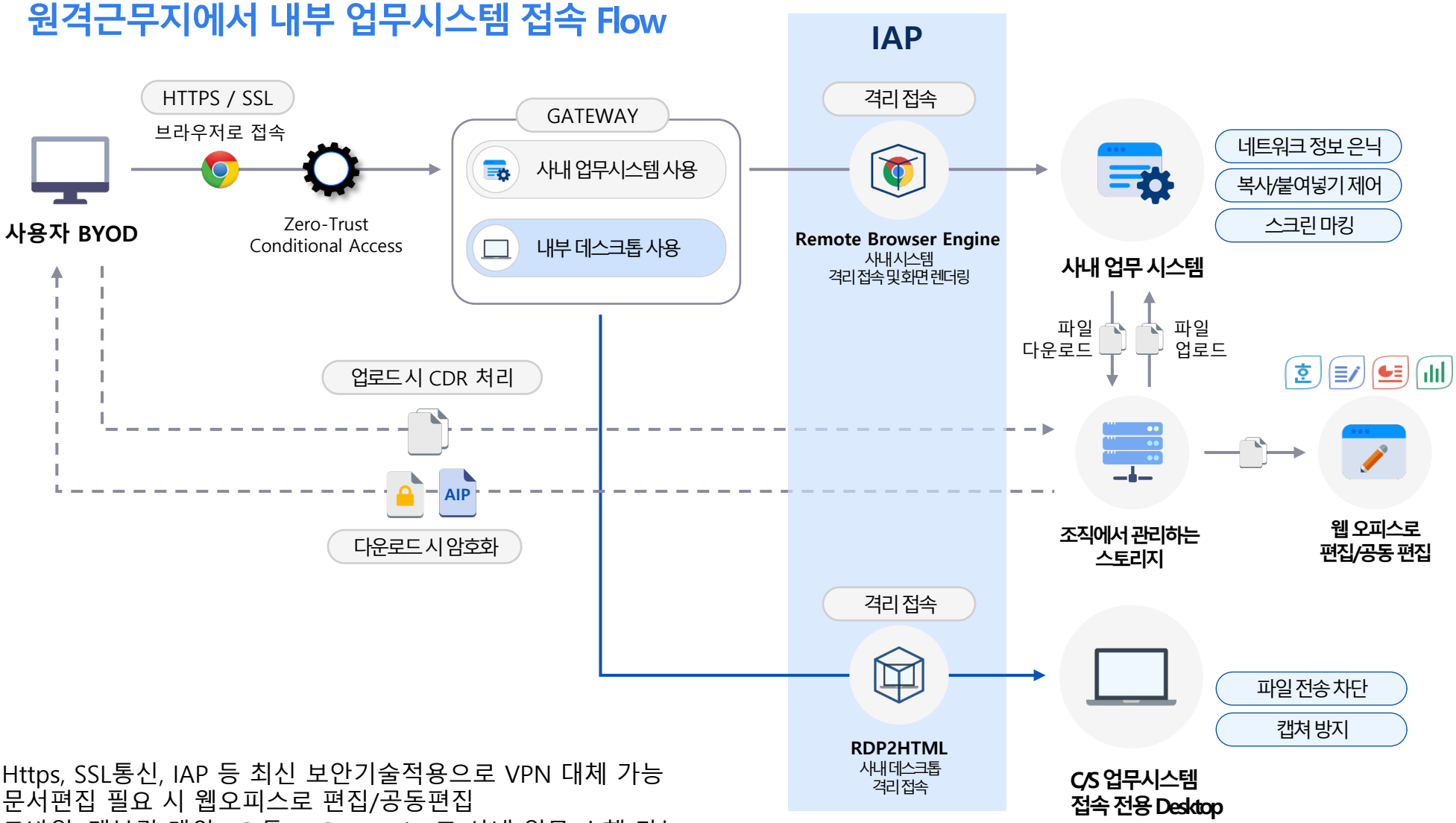
제로트러스트 관점의 보안 이슈

- 접속 후 내부 컨텐츠의 유출 차단
- 신뢰할 수 없는 외부 파일 반입
- 신뢰할 수 없는 디바이스가 내부 접속
- 한번의 판단으로 전부 허용할 것인가?
- 접속 허용 후에도 보안 관리가 필요



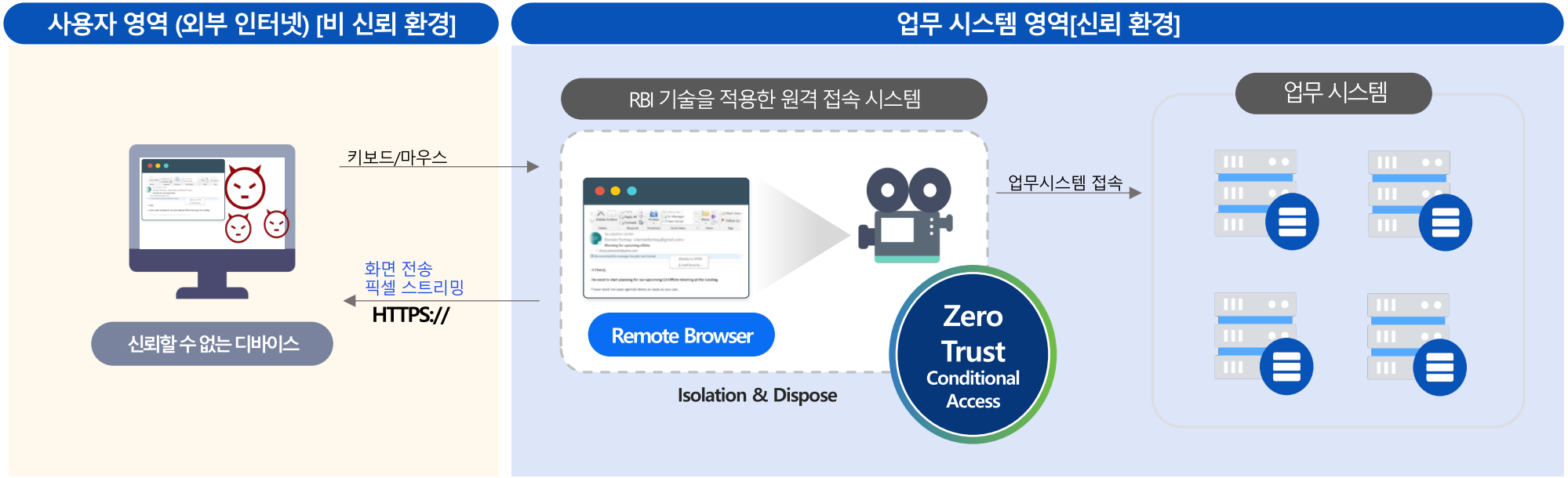
IAP + RBI 융합 기술을 통한 원격근무 제로트러스트 구현

원격근무지에서 내부 업무시스템 접속 Flow



- Https, SSL통신, IAP 등 최신 보안기술적용으로 VPN 대체 가능
- 문서편집 필요 시 웹오피스로 편집/공동편집
- 모바일, 태블릿 개인 PC 등 BYOD Device로 사내 업무 수행 가능

최신 보안 모델 적용



외부 접근 시 별도 프로그램 설치 불필요

- 보안 프로그램 설치 불필요
- 일반 브라우저로 사용(any device, mobile)

조건부 접근/사용 정책 적용

- 추가인증 요구 (OTP, 생체 인식)
- 패스워드 리셋 요구
- 업로드/다운로드 차단
- 스크린 마킹

IP / Network 접속 정보 은닉

업로드/다운로드 파일 컨트롤

- 업로드시 CDR
- 다운로드시 암호화
- 백신 검사
- 개인정보 검사

기존 업무시스템의 수정 없음

웹 보안

- 스크린 마킹
- 캡처 방지
- 임시 파일 삭제
- 소스 보기 차단

최신 보안모델 적용

Remote Browser Isolation [RBI]	Zero-Trust Conditional Access [ZTCA]	Security Service Edge [SSE]
사용자 디바이스 대신 원격 서버에서 사용자의 웹 브라우징 세션을 호스팅하여 온라인 위협 무력화	사용자의 접속 환경에 따른 추가 인증 제공 & 사용권한 제어	업무 시스템의 액세스 제어, 위협 보호, 모니터링 등 통합 관리 기능

Zero Trust – Access

프로그램 설치나 접속 흔적 없이 내부 시스템 액세스

접속 프로그램 설치 없이

브라우저로만 접속

접속 정보 흔적 없이

HTML 임시 파일 없음
쿠키 없음

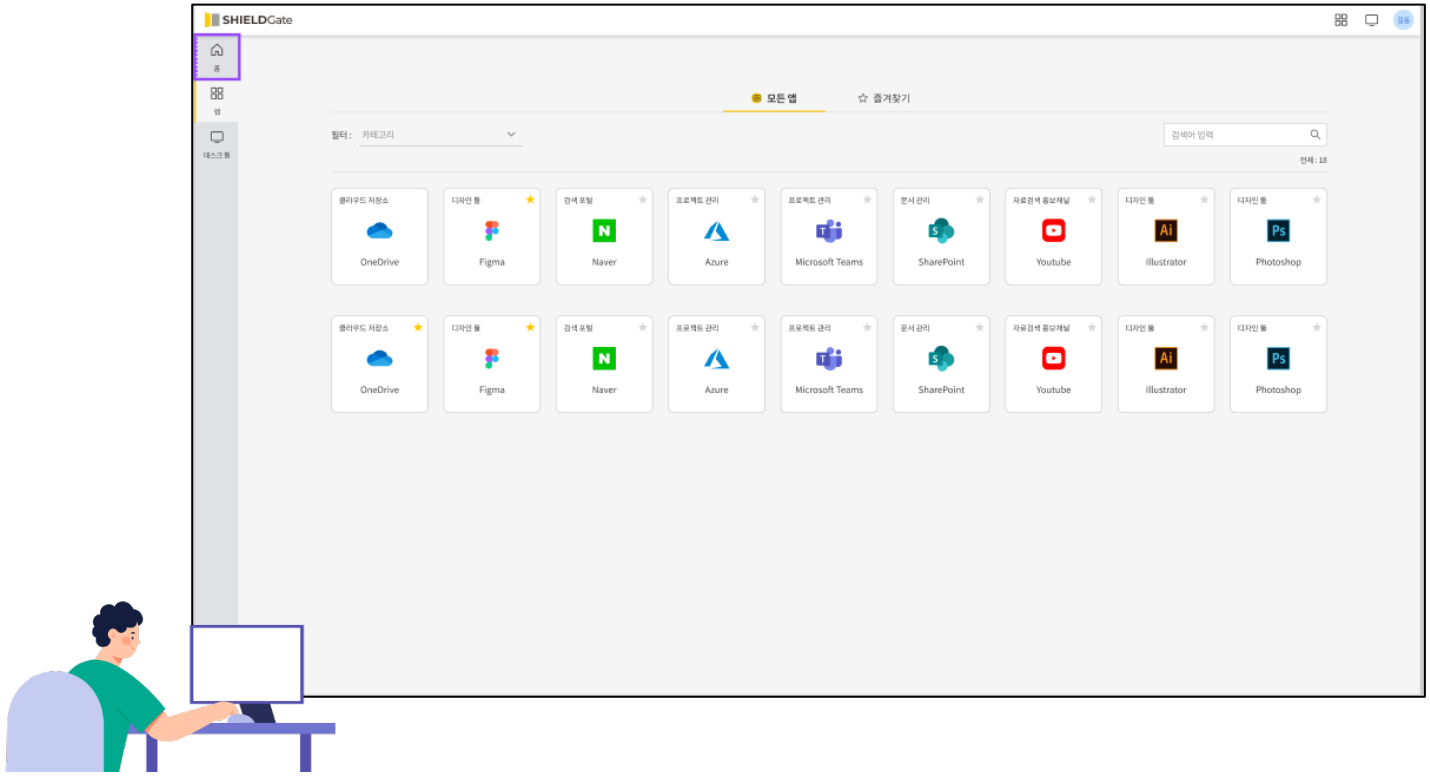
파일 다운로드 없이

웹 편집기로 편집/저장/업로드

개인화 Portal과 적응형 접속관리

Security Service Edge – 업무시스템 포털 액세스 관리

› 사용자가 접속해야 하는 업무시스템(또는 앱)을 관리할 수 있습니다. 사용자는 접속 시 자신에게 할당된 업무시스템(또는 앱) 목록이 나타나고, 이를 통해 접속할 수 있습니다.

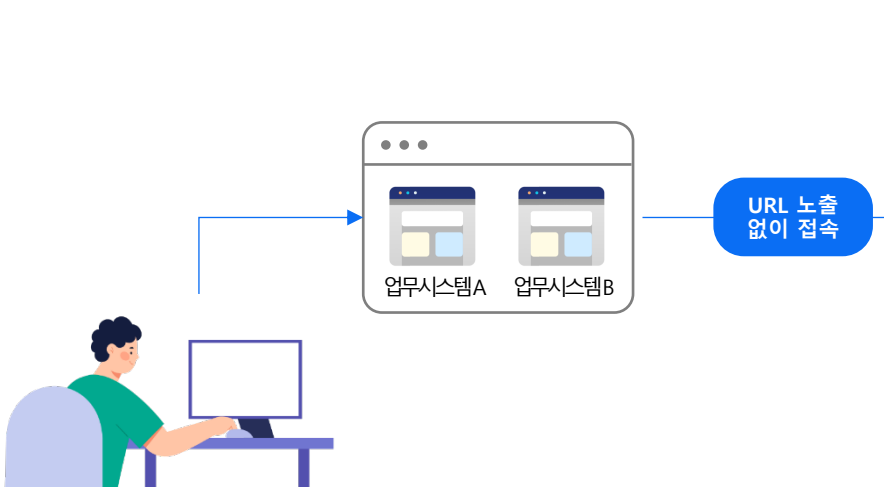


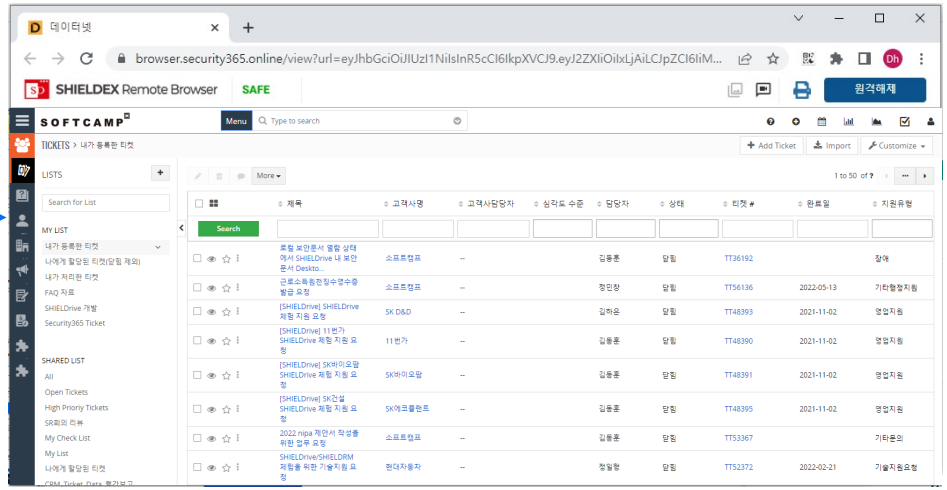
Benefit

- 보안관리자를 통한 업무시스템(또는 앱) 별 접속/사용권한 관리 가능
- 관리범위에 포함되지 않은 Shadow IT도 내부 통제 가능
- 접속 이력 저장(화면 저장, OCR 검색) 및 이상 징후 감지

Security Service Edge – 네트워크 은닉 및 위협 보호

› 사용자에게 업무시스템 접속 시 URL 정보가 노출되지 않습니다. 위험으로 부터 공격표면이 은닉되고, 최소화 됩니다.





[업무시스템 접속 화면]

Benefit

- 사용자 및 노출된 통신 구간에서 업무시스템 정보가 노출되지 않음
- 업무시스템 URL, IP 정보가 노출되지 않음 ➔ 공격 표면 은닉 및 최소화
- 업무시스템 취약점 점검 사항을 대폭 줄임 ➔ 오픈소스 취약점 은닉

www.softcamp.co.kr

THANK YOU

SOFTCAMP

소프트캠프㈜ 경기도 성남시 분당구 성남대로 779번길 6, KT분당빌딩 3, 4층