종합 정보보호 전문 기업

SOOSAN INT

COMPANY INTRODUCTION

SOOSAN INT

SOOSAN GROUP

ENERGY GROUP

수산인더스트리
플랜트 전문건설
발전설비정비, 전기공사, 플랜트건설

수산이앤에스
발전소 계측정비, 시공
원전/화력 정비, 플랜트, MMIS

SH POWER
신재생 에너지 사업

ICT GROUP

수산아이앤티
네트워크 보안솔루션 개발
ISP형 서비스, 인터넷 접속관리 솔루션
보안 컨설팅 서비스
(과기부 지정 정보보호 전문 서비스 기업)

수산홈텍
가스안전기기 전문 제조
가스센서, 누설경보기, 가스차단장치

HEAVY INDUSTRY GROUP

수산세보틱스
건설중장비 생산
유압브레이커, 유압드릴, 크레인,
카고식 크레인, 특수목적용 차량

비나모터
트레일러, 특수목적용 차량 생산

SOOSAN INT

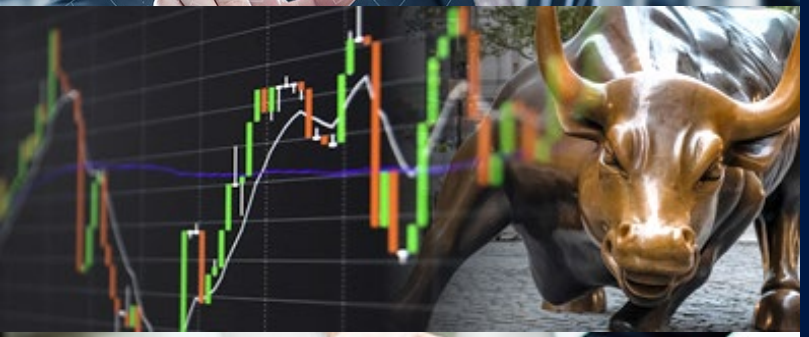
A LeadingGlobal Network Security Solution Provider

회 사 명	㈜수산아이앤티
대표이사	정 은 아
설립일자	1998년 3월 4일
자 본 금	33.7억 원
사업분야	소프트웨어 개발 및 공급업
	(네트워크 접속관리 솔루션 외)
회사주소	06367 서울특별시 강남구 밤고개로 5길 13 수산빌딩
연 락 처	+82-2-750-0843
	ask@soosan.co.kr / www.soosanint.com

Credit Rating A+

KOSDAQ LISTED COMPANY

연 혁



2025 ~

- 악성메일 모의훈련 '제로피쉬(ZeroPhish)' 서비스 출시
- ePrism SSL VA '2025년 우수 정보보호 기술' 과기정통부 장관상 수상
- 과기정통부 '정보보호 전문서비스 기업' 지정 (보안 컨설팅 사업 확장)
- 생성형AI 모니터링 시스템 개발
- 'eWalker SSE'로 제로트러스트 기반 통합 보안 플랫폼 구현
- Keysight Tech Partner 등록 및 아시아·태평양 파트너사 대상 글로벌 파트너십 체결
- 정보보호 해외진출 전문가 협의체, 정보보호기업 자율보안 협의체 참가
- 유해사이트 차단 및 SSL 가시성 솔루션, 네트워크 DLP, 웹방화벽, SSL VPN 다수 공급 (300여 곳)

2024 ~

- 업무용 SaaS 이용 보안 통제 솔루션 eWalker SSG 출시
- 제로트러스트 도입 시범사업 수주
- WAF SECaaS 서비스 시작
- 독일 보안 기업과 ODM 수출 계약 체결

2022 ~

- 웹방화벽 솔루션 eWalker WAF V10 CC인증 EAL4 획득
- 한국교육학술정보원 4세대 나이스 전국 교육청 SSL 가시성 솔루션 공급
- 'eWalker SWG V9' 'K-ICT 신SW상품대상' 과학기술정보통신부 장관상 수상
- 한국에너지공단과 탄소중립 및 외부사업 활성화 MoU 체결
- eWalker WAF V9, eWalker SSL VPN 출시

2016 ~

- eWalker SWG V9 출시
- ePrism SSL VA 출시
- ㈜수산아이앤티로 사명 변경 및 코스닥 상장 (2016~)
- 통신 3사 추가단말서비스 시작 (2012~)
- 벤처기업대상 대통령표창 수상

1998 ~

- 기업용 인터넷 사용관리 솔루션 eWalker 3 출시
- 개인용 인터넷 유해정보차단 S/W 수호천사 1.0 출시
- 플러스기술㈜ 설립 (1998~)

수산아이앤티의 경쟁력

1,700

네트워크 보안 솔루션
1,700여 고객사에 제공

3 통신사 제휴

10년 이상 통신사 플랫폼 기반 서비스
(KT, SK, LG U+)
국내 최다 트래픽 분석 노하우

80%

전체 인력 중 기술개발 인력 80%
인재 경영 추구

133 건

특허경영으로 사업 안정성과
기술 경쟁력 확보

FIRST

인터넷 트래픽 필터링 솔루션 개발
SSL 복호화 솔루션 개발
네트워크 방식 유해차단 서비스 제공

ONLY

통신사와 공유단말 서비스 공급
전국 단위 트래픽 분석 서비스 제공

HAVE

전국 단위 네트워크 분석 역량
고성능 엔진 기반 트래픽 분석 기술
공공기관 및 기업 등 다양한 네트워크 구축 노하우

네트워크 보안솔루션

랜섬웨어 / APT 공격 / 웹서비스 위협 / 내부정보 유출방지를 위한 차세대 보안 기술 기반

Walker SWG

유해사이트 차단 / 인터넷 접속 관리

- 유해사이트 및 악성코드 사이트 차단
- 트래픽 접속 관리를 통한 네트워크 보안 솔루션
- HTTPS 사이트 접속제한 가능
- 국내 최대 URL DB 제공

Walker DLP

정보유출 방지 / 악성코드 사이트 차단

- 이메일, 메신저를 통한 중요정보 유출 방지
- 외부 유출 자료에 대한 로깅
- 메일, 메신저, 클라우드 서비스에 대한 패턴 제공
- 감사로그 제공

Walker SSG

업무용 SaaS 이용 보안 통제 체계

- 허용된 서비스에 대한 사용자 인증
- 비 허용된 서비스에 대한 접속 통제 – 탐지 및 차단 기능
- 개인정보 필터링/유출방지
- 다양한 프로토콜 로깅 및 차단
- SSL 암호화 트래픽에 대한 가시성 제공

Prism SSL VA

SSL 트래픽 가시성 확보

- SSL 가시성 제공 솔루션
- 타 네트워크 장비의 교체, 수정없이 연동 가능
- 모든 포트의 SSL 트래픽 가시성 확보
- 비대칭 라우팅 환경 제공

Walker WAF

웹 공격 탐지 및 방어 / 개인정보 유출 차단

- 안전한 웹서비스를 구현할 수 있는 웹 방화벽 솔루션
- 실시간 모니터링 및 경고 대응 제공
- 잠재적 해킹 공격 보호
- 웹 애플리케이션 트래픽 분석 제공

SafeAI

생성형 AI 게이트웨이

- 다양한 LLM을 한 화면에서 자유롭게 사용
- 프롬프트, 첨부파일 내 민감정보 실시간 저장/탐지/차단
- 사용자/팀 단위 사용량 임계치 설정 – AI 예산 관리
- 실시간 AI 사용 현황 대시보드 제공
- 개인/조직 단위 계정 관리 및 모델 사용 권한 제어

Walker SSL VPN

원격/재택에 최적화, 초고속 속도, 안정적 보안

- 초고속 SSL VPN 솔루션
- 원격/재택 SSL VPN 통신환경 지원
- 빠른 속도와 안정적 보안 채널 제공
- SSL VPN 업계 유일의 자체 OTP 솔루션 탑재

Walker CLOUD

클라우드 환경에서 보안서비스 제공

- 복호화 트래픽 미러 기능 (외부 보안서비스 확장 연동)
- 클라우드 환경에서 웹 보안 서비스 제공 (SECaaS)
- 기업 내부 정보, 사용자 및 서버 보안 (SASE)
- 트래픽 부하에 따른 인스턴스 자동 확장 및 축소

Walker SWG 유해사이트 차단 솔루션

HTTPS를 포함한 비업무 사이트 통제, 유해사이트 접속 차단 기능을 제공하는 통합 인터넷 접속관리 솔루션
업무효율 향상, 보안 위협 예방

도입 필요성

비업무 사이트 사용 → 업무 집중도 저하

업무 특성에 따라 허용/비허용 사이트 구분하여 **업무 집중도 향상**

악성코드 사이트 접속 경로 다양화

유해사이트 차단 솔루션 도입을 통해 **1차 보안 가능**

주요 기능

비업무·유해사이트 통제/차단

웹사이트 카테고리별 제어
인사 DB에 따른 정책 지원
악성코드·우회접속 사이트 차단

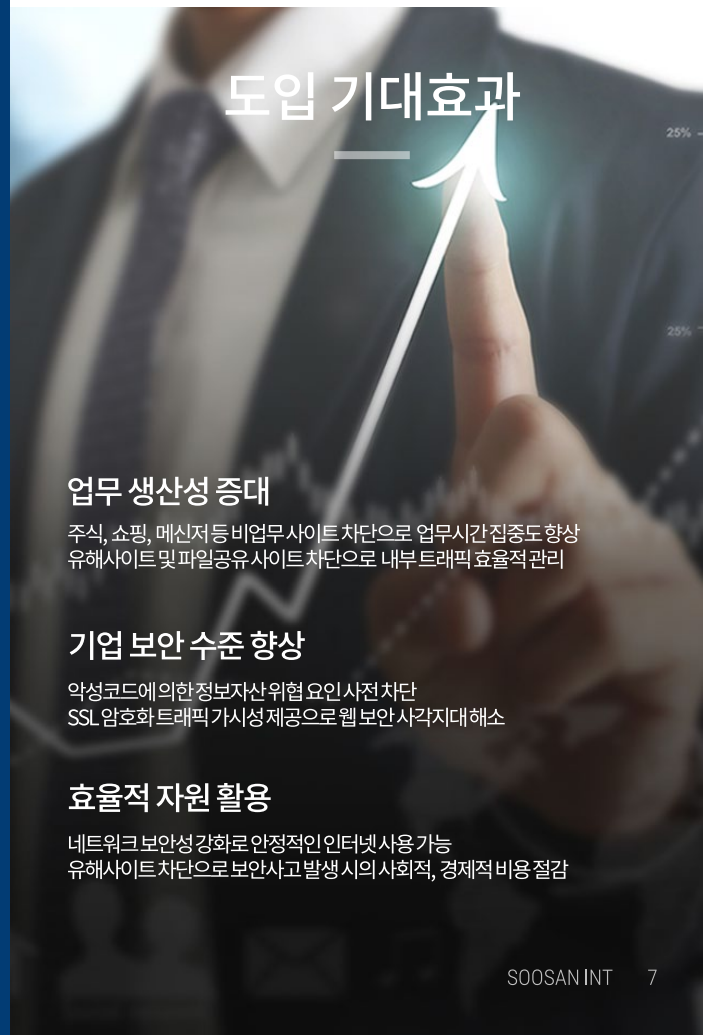
생성형 AI 분석 가능

생성형 AI 접속 제어 지원
ChatGPT, DeepSeek 등

SSL트래픽 가시성 제공

모든 포트 트래픽 가시성
SSL 인증서 설치/관리 지원

도입 기대효과



업무 생산성 증대

주식, 쇼핑, 메신저 등 비업무 사이트 차단으로 업무시간 집중도 향상
유해사이트 및 파일공유 사이트 차단으로 내부 트래픽 효율적 관리

기업 보안 수준 향상

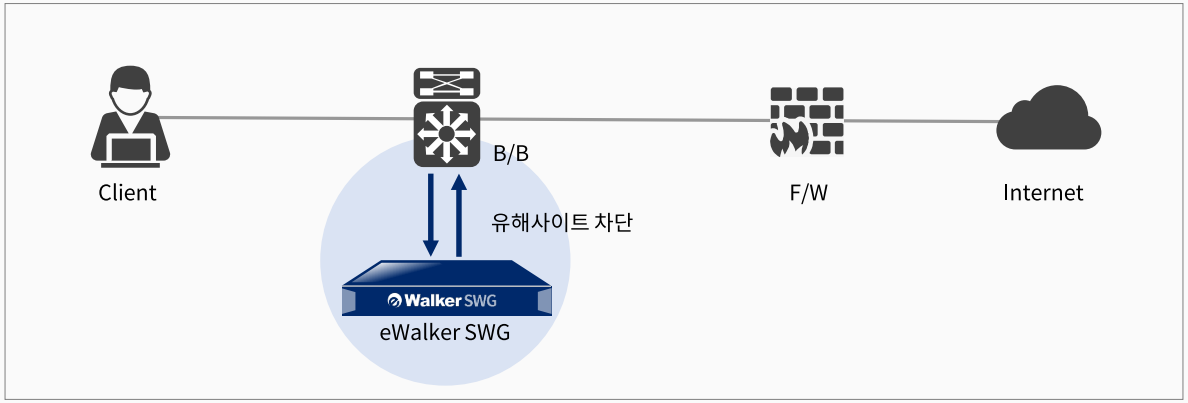
악성코드에 의한 정보자산 위협 요인 사전 차단
SSL 암호화 트래픽 가시성 제공으로 웹 보안 사각지대 해소

효율적 자원 활용

네트워크 보안성 강화로 안정적인 인터넷 사용 가능
유해사이트 차단으로 보안사고 발생 시의 사회적, 경제적 비용 절감

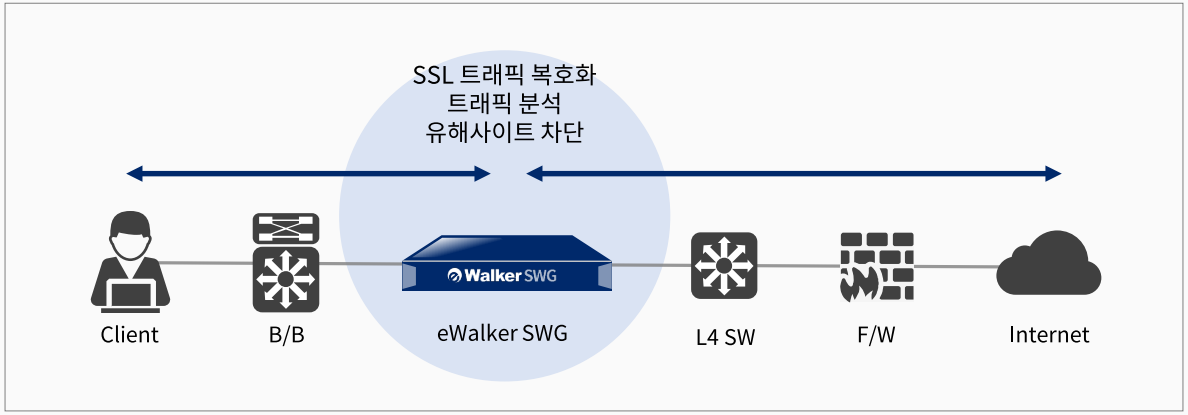
Walker SWG 유해사이트 차단 솔루션

HTTPS를 포함한 비업무 사이트 통제, 유해사이트 접속 차단 기능을 제공하는 통합 인터넷 접속관리 솔루션
업무효율 향상, 보안 위협 예방



Mirror Mode

- 네트워크 영향 없는 구성 지원
- SSL 트래픽 복호화 기능 사용 불가
- DNS 선별 차단 기능을 통하여 HTTPS 및 유해사이트 제어
- 사용자 PC의 인터넷 접속 트래픽을 Mirror Port를 통해 수신
- B/B와 연결된 차단 Port를 통해서 차단 Packet을 사용자 PC에 전송



Inline Mode

- 네트워크 경로상에 eWalker SWG 제품 설치 (Transparency)
- 모든 트래픽 감시 및 SSL 트래픽 선별적 복호화 수행
- 유해사이트 접속 시 Bridge 인터페이스를 통해서 차단 Packet 전송
- 웹 메일 수/발신 차단, 구글 서비스 선별 차단, SNS 계정별 차단 등 HTTPS 사이트에 대한 세부 차단 가능

Prism SSL VA

SSL 암호화 트래픽 복호화 솔루션

TST(TCP Session Transparency) 고성능 엔진을 기반으로 모든 트래픽을 투명하게 감시하며,
네트워크 구성 변경없이 운영 가능한 SSL 가시성 솔루션으로 기존 보안 장비들이 제 기능을 발휘할 수 있도록 보완해 줍니다.

도입 필요성

인터넷 트래픽 90%는 SSL 암호화 트래픽

기존 네트워크 보안장비들은 암호화 트래픽 정보를 확인할 수 없음

기존 장비가 대응하지 못하는 SSL 암호화

ePrism SSL VA는 모든 포트와 트래픽을 감시
기존 보안장비가 분석하지 못하는 SSL 암호화 트래픽에 대한
가시성 확보

주요 기능

SSL 트래픽 복호화

TLS/SSL 프로토콜만 선별적 분리
모든 암호화 트래픽 복호화

세션 투명성 유지

5 Tuple 세션 투명성 유지

우회접속 프로그램 제어

트래픽 세션 분석
각종 우회경로 패턴 차단

도입 기대효과

SSL 가시성 제공으로 N/W 보안 강화

기존 보안장비들에게 복호화된 트래픽을 전달, 분석 지원
SSL 암호화 트래픽을 악용한 악성코드, 랜섬웨어 감염 예방

내부정보 유출 방지

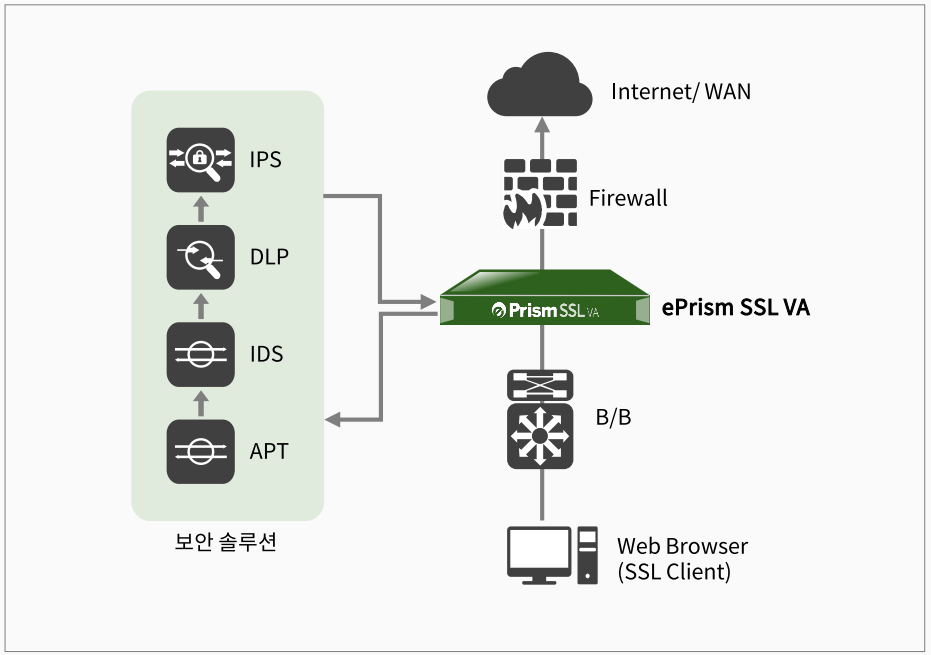
각종 우회경로 프로토콜을 포함한 L7프로토콜을 분류
우회접속 프로그램 분석 및 차단으로 내부정보 유출 방지

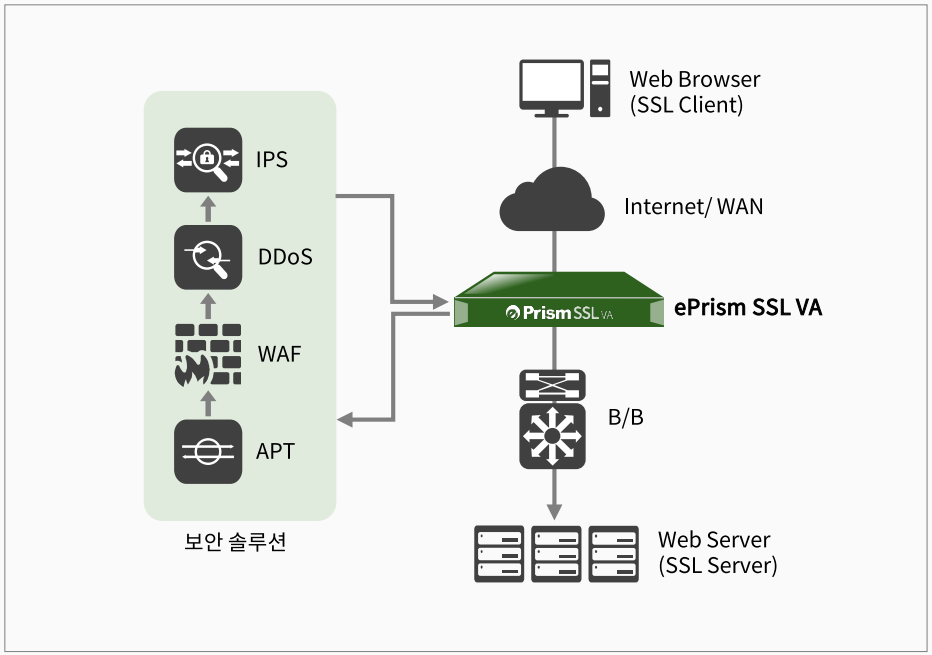
안정적 네트워크 운영 가능

기존 네트워크 환경에 최적화된 호환성 제공
바이패스 기능으로 안정적인 네트워크 운영 가능

Prism SSL VA SSL 암호화 트래픽 복호화 솔루션

TST(TCP Session Transparency) 고성능 엔진을 기반으로 모든 트래픽을 투명하게 감시하며,
네트워크 구성 변경없이 운영 가능한 SSL 가시성 솔루션으로 기존 보안 장비들이 제 기능을 발휘할 수 있도록 보완해 줍니다.





Forward Proxy

- 내부 ➔ 외부
- 내부 사용자의 외부 접속 시 가시성 제공
- 다양한 보안 장비에 연동 기능 제공 (IPS / APT / DLP 등)
- 내부 정보 유출 방지를 위한 SSL 보안성 강화

Reverse Proxy

- 외부 ➔ 내부
- 외부 사용자의 내부 접속 시 가시성 제공
- 다양한 보안 장비에 SSL 가시성 제공 (WAF / IPS 등)
- 대외 서비스에 대한 SSL 보안성 강화

Walker DLP 네트워크 정보유출 방지 솔루션

웹메일 및 메신저 발송 로깅을 통해 정보유출 분석 및 차단을 지원하며, 클라우드 환경 지원으로 확대되는 정보유출 사고 예방

도입 필요성

내부정보 유출 94%, 직원의 메일을 통해

내부정보의 94%는 내부직원/협력업체 직원의 메일을 통해 유출
개인정보 및 회사기밀 유출은 기업 보안의 가장 큰 위협

내부정보 유출 사전 방지 가능

웹메일, 메신저, 웹하드, 클라우드 서비스 등 유출 경로 다양화
외부와 수/발신되는 내용들을 점검, 개인정보/내부정보 유출 방지

주요 기능

웹메일 발신 로깅

개인정보 및 중요 정보의 불법 유출에 대한
발신 모니터링

메신저 수/발신 로깅

개인정보 및 중요정보 채팅 및 첨부파일
모니터링

생성형 AI 분석 가능

생성형 AI(질의·응답) 분석
ChatGPT, DeepSeek 등

클라우드 업로드 로깅

Cloud/SaaS 서비스로 유출되는 파일 모니터링

도입 기대효과

강화된 보안 컴플라이언스 준수

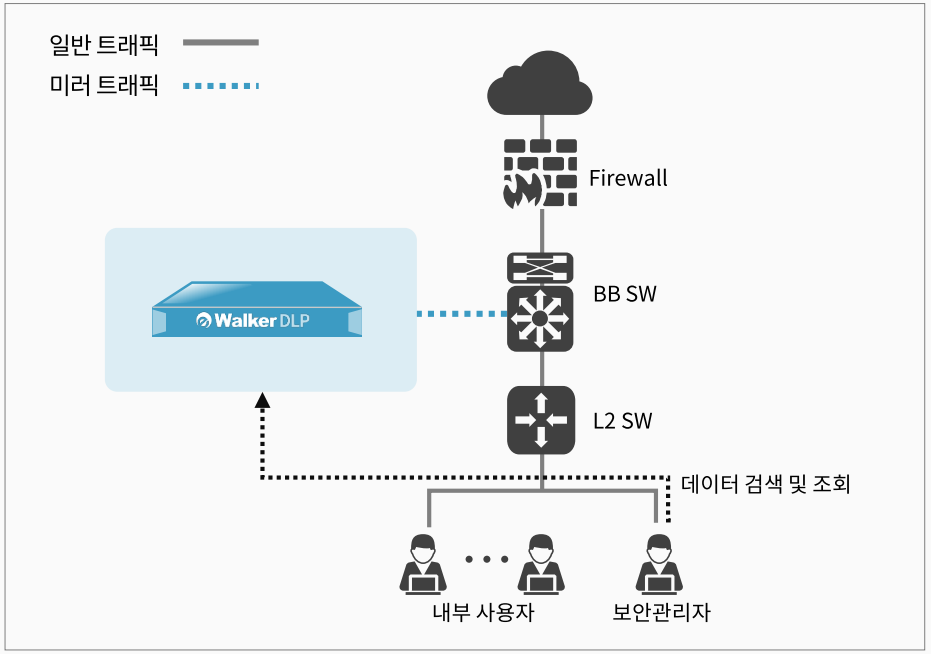
개인정보보호법은 개인정보가 공개 및 유출되지 않도록
조치해야 한다고 명시
DLP는 정보보호법을 지키기 위한 기본 솔루션

정보유출에 의한 경제적 피해 최소화

기업의 신뢰도, 손해배상 및 경영진 처벌 등
기업의 데이터 자산 보호를 못함으로써 발생하는 피해 예방

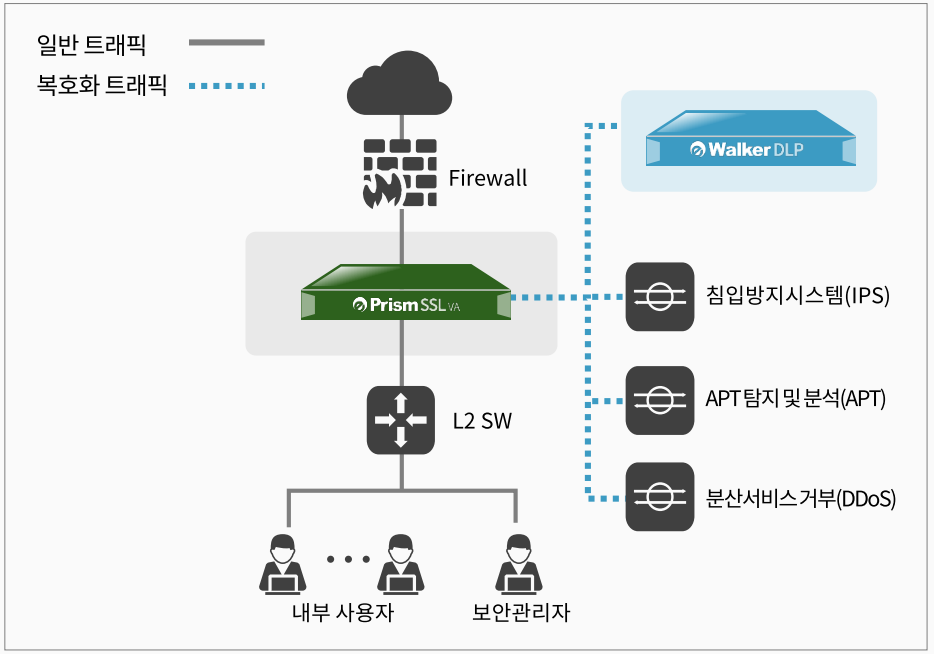
Walker DLP 네트워크 정보유출 방지 솔루션

웹메일 및 메신저 발송 로깅을 통해 정보유출 분석 및 차단을 지원하며, 클라우드 환경 지원으로 확대되는 정보유출 사고 예방



일반 구성

- 특징: 기존 네트워크 영향없음, 간단한 구성
- 개인정보(주민등록번호, 카드 정보 등) 및 내부정보(키워드, 사이즈 등)가 포함된 메일, 메신저, SNS, 파일 전송에 대한 모니터링 가능
- HTTPS 트래픽에 대한 로깅은 ePrism SSL VA 제품과 연동 필요
- 인라인 구성 가능 (네트워크 가용성 보장을 위한 Bypass card 포함)



SSL 복호화 및 필터 구성

- 특징: 원 제조사 제품으로 SSL 가시화, 유해사이트 차단 및 내부정보(개인정보 포함) 유출 탐지 및 차단할 수 있는 통합 구성
- SSL 가시화 및 HTTPS 유해사이트 차단
- 개인정보 (주민등록번호, 카드 번호 등) 및 내부정보 (키워드, 사이즈 등)가 포함된 메일, 메신저, SNS, 파일 전송에 대한 모니터링 및 차단 가능
- 다양한 보안 장비에 SSL 가시화(복호화) 트래픽 전송 가능
- ePrism SSL VA 추가 구매 필요

Walker WAF 차세대 웹방화벽

Real time white URL 기술을 적용, 오탐률과 처리 시간을 획기적으로 줄여 안전하게 웹 서비스 구현/악성코드 능동적 방어

도입 필요성

서비스에 대한 공격/보안 사고 발생 증가

웹 서버의 잠재적 취약점 공격 시
기존의 IPS, IDS, 방화벽 등 네트워크 보안솔루션 탐지 불가

안전한 웹 서비스 구현

다양한 웹 서비스에 대한 트래픽 분석을 통해
웹 공격 방어, 서버 보호 ➔ 안전한 웹 서비스 구현

주요 기능

웹공격 탐지 및 방어

자동화/지능화된 최신 웹공격 대응
HTTP(S) 무차별 대입 및 HTTP2.0 웹공격 대응

개인정보 유출 차단

의도적/비의도적으로 시행되는 개인정보 유출
자동차단 및 비식별화

Anti Web DoS

HTTP Get Flood 등 실시간 감지 및 차단

도입 기대효과

안전한 웹 서비스 운영

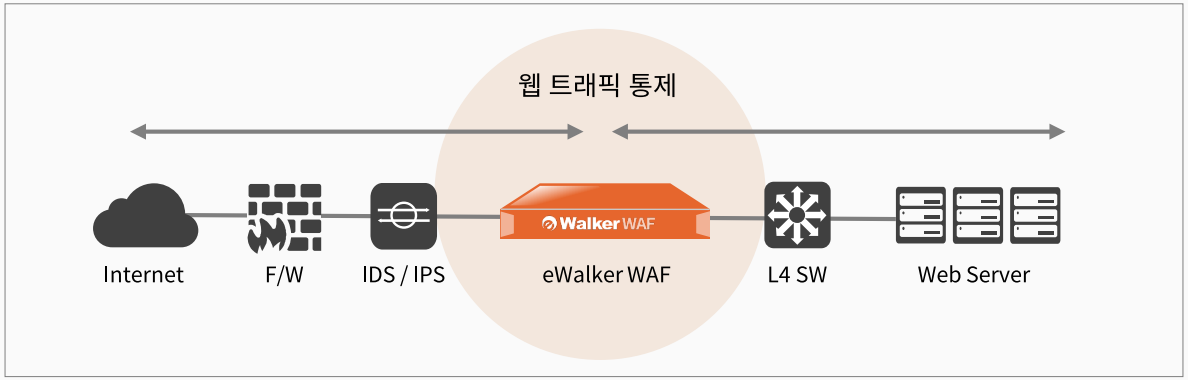
정상적인 웹 서비스 요청은 허용하고 웹 서버에 대한 공격은
탐지 및 차단하여 안전하게 운영

편리한 보안관리로 높은 보안성 확보

어려운 보안관리가 편리하도록 다양한 지원 기능을 제공
실시간 모니터링, 정책 설정 등 사용자 편의성 제공
최신 웹 공격 및 신종 Dos 공격 등 보안위협에 대한 보안성 향상
OWASP, SANS, 국가정보관리국 등 취약점을 분석 반영

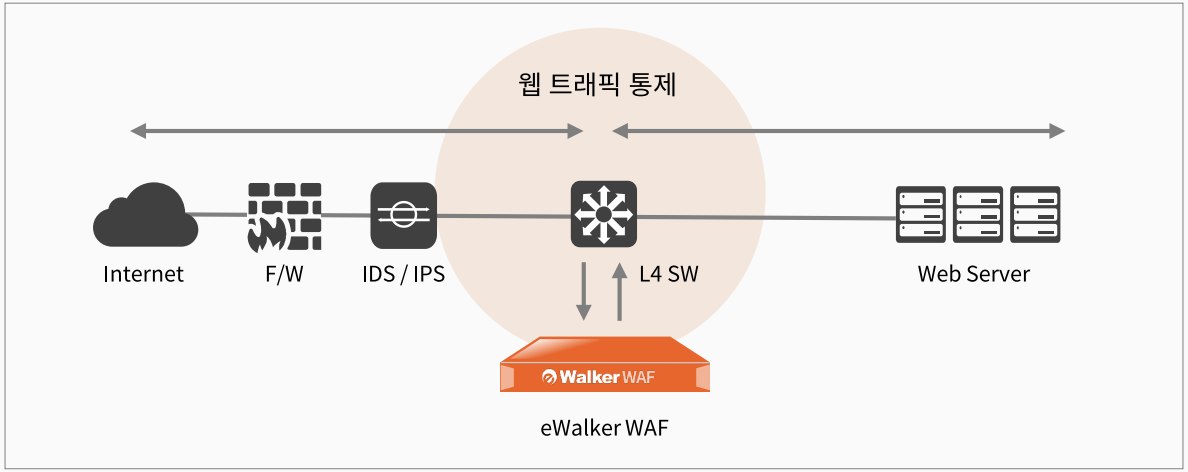
Walker WAF 차세대 웹방화벽

Real time white URL 기술을 적용, 오탐률과 처리 시간을 획기적으로 줄여 안전하게 웹 서비스 구현/악성코드 능동적 방어



In-line Mode

- 이중화 구성 설치 지원 (A-S, A-A 비동기 트래픽 처리)
- SSL 트래픽 암/복호화 수행
- 웹 트래픽 감시 및 웹 공격 시 차단 Packet 전송
- 네트워크 구성 변경없이 운영 장애 시 Bypass 기능을 통해 안정적인 웹 서비스 제공



Out-of-Path Mode

- 네트워크 장비의 Port Redirection 기능 필요
- SSL 트래픽 암/복호화 수행
- 웹 트래픽 감시 및 웹 공격 시 차단 Packet 전송
- 네트워크 장애 시 L4 SW Bypass 기능을 통해 안정적인 웹 서비스 제공

Walker SSL VPN 고성능 가상사설망 솔루션

원격접속자가 내부 시스템 접속 시 강력한 보안 경로를 제공해 주는 고성능 SSL VPN 전용 네트워크 보안 솔루션
기존 네트워크 구성의 변경/단절없이 안전하고 편리한 설치 가능

도입 필요성

원격/재택근무 확산 → SSL VPN 적용 확대

재택근무, 원격수업, IoT, M2M 서비스 등
SSL VPN이 적용되며 중요성 부각

철저한 보안 제공

개인정보보호를 위한 자체 OTP 솔루션 탑재, 실시간 모니터링,
5가지 이상의 멀티인증 과정으로 철저한 보안 제공

주요 기능

원격/재택 SSL VPN 통신환경 지원

다양한 사용자 OS 환경 지원
서버별 IP/Port에 대한 접근 제어

SSL VPN 전문 솔루션

자체 OTP 솔루션 탑재
강력한 5가지 이상의 멀티 인증 과정 지원

빠른 속도, 안정적 보안 채널

초고속 SSL VPN
사용자/그룹별 접근 설정
기간별 사용자 접속 제한 기능 제공

도입 기대효과

안전한 기업 네트워크 보안 강화

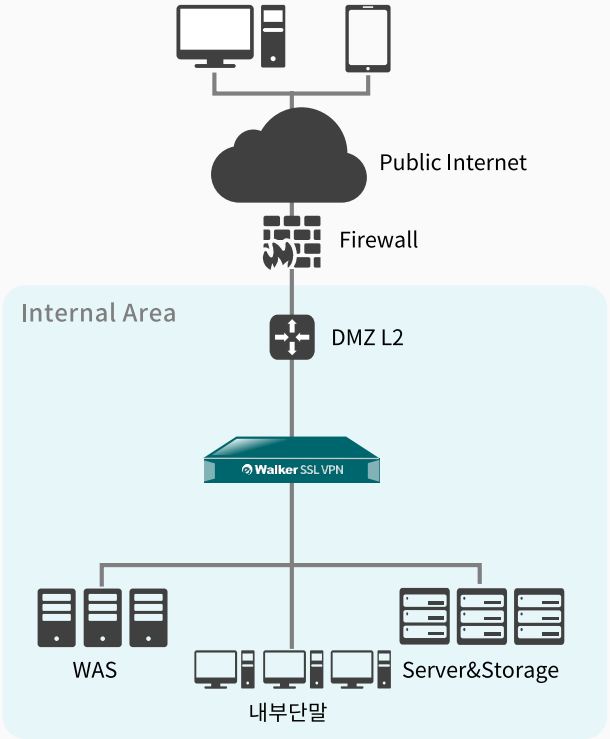
회사 외부에서도 암호화를 통한 내부 인프라 사용
인증 절차 강화로 철저한 기업 네트워크 보안 구축
암호화된 원격지 데이터 수집

클릭 한 번으로 비용 절감과 편리한 구축

기존 IPSec 방식의 VPN 대체 (SSL 방식 사용)
VPN TCO 절감
손쉬운 VPN 확장 제공

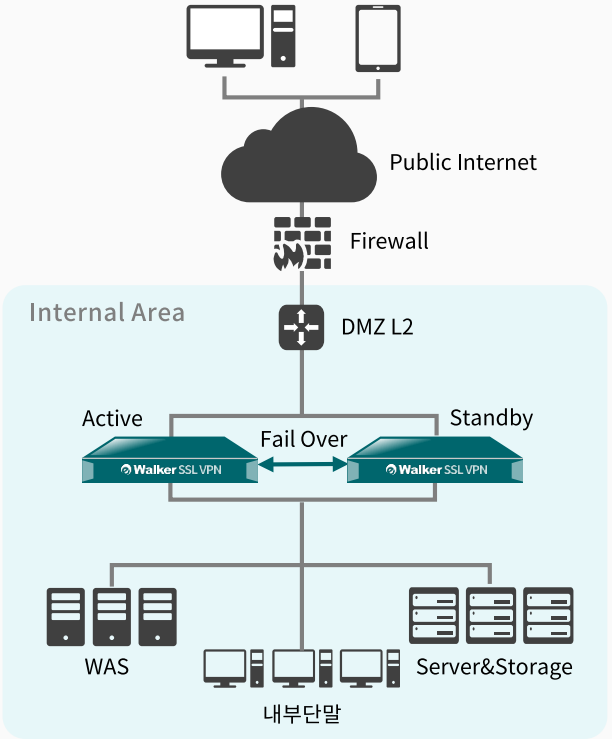
Walker SSL VPN 고성능 가상사설망 솔루션

원격접속자가 내부 시스템 접속 시 강력한 보안 경로를 제공해 주는 고성능 SSL VPN 전용 네트워크 보안 솔루션
기존 네트워크 구성의 변경/단절없이 안전하고 편리한 설치 가능



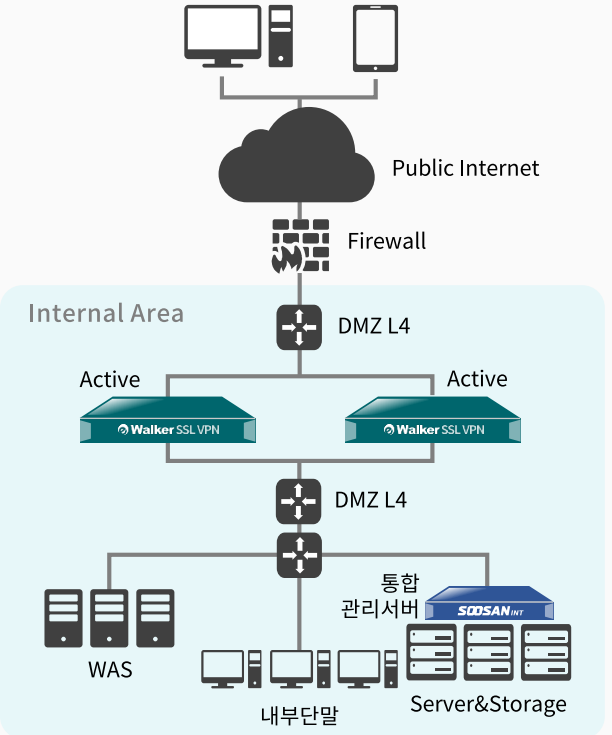
일반 구성 (Single)

- 방화벽 DMZ 위치 (불필요한 트래픽 제어)
- 방화벽 보안정책 설정을 통한 보안 등급 강화
- 방화벽에서 SSL VPN Service port만 허용



이중화 구성 (Active-Standby)

- 솔루션 2대로 HA를 구성하여 장애 발생 시 Fail over 형태로 실시간 적용
- 이중화 구성 내/외부에 각각 VRRP로 적용



이중화 구성 (Active-Active)

- 내부 L4 스위치 존재 시 Load Balancing으로 트래픽 부하 분산
- Policy Server를 통한 사용자 계정 관리, VPN 정책 설정, 통합 모니터링, 통계 리포트 제공

Walker SSG 업무용 SaaS 이용 보안통제 솔루션

폐쇄망에서(업무용 PC) SaaS 서비스를 사용할 수 있도록 개발한 업무용 SaaS 이용 보안통제 솔루션으로
사용자 인증을 통해 내부 사용자임을 확인하고, 부여된 권한에 따라 SaaS 서비스 이용이 가능하도록 제공

도입 필요성

IT 환경 변화

코로나 이후 원격 근무, 클라우드 사용 증가
LLM, sLLM, 생성형 AI 사용 증가
VPN, NAC을 이용한 이용자/단말만 통제
이용자가 실제 사용하는 애플리케이션 통제 불가

국가 망 보안체계(N2SF) 대응

IT 환경 변화에 맞는 필요 보안 대책 마련 (AI, SaaS, 원격)
클라우드 서비스 이용 시, 데이터 보호를 위한 사용자 액세스를 관리
애플리케이션에 대한 데이터 보호 및 통제

주요 기능

개인·내부정보 유출 차단

· 서비스 정책(메일, 메신저, SNS 등)과 웹 정책을 설정해 사용자 관리·첨부파일 타입 기반 탐지/차단
· 정책은 감시, 허용, 미 감시, 차단으로 구성되어 우선순위에 따라 적용
· 개인정보 및 키워드 등의 정책별 세부 조건도 추가/삭제 편집 기능을 제공

인터넷 접속관리·SSL 암복호화

· 업무, 비업무, 유해사이트 등 Rule 기반 통합 인터넷 접속관리
· 화이트리스트 기반 SaaS 접근 URL 필터링 악성코드 탐지
· 수산아이앤티 인증서 설치 유도 및 배포
· SSL 트래픽 암복호화

감사기록 및 사용자 인증

· DLP 필터링, URL 필터링 등에 대한 감사기록
· SaaS 접근 시 웹페이지에서 IP/PASSWD 인증
※ SaaS 접속을 위한 사용자 인증은 SaaS에서 별도 수행

도입 기대효과

사용자들의 업무 효율성 제고

망 분리 제도를 완화하여 외부 연결이 불가했던 업무용 PC에서 생성형 AI 서비스, 외부 클라우드 협업도구(SaaS) 등을 활용할 수 있도록 업무 환경 개선

비용 절감과 기업 네트워크 보안 강화

[사용자 인증·SaaS 접근 통제·SSL 가시성·내부정보 유출 방지] 통합 제공으로 비용 절감 효과
SaaS 서비스 보안 및 시스템 실시간 트래픽 분석을 통한 기업 네트워크 보안 강화

Walker SSG 업무용 SaaS 이용 보안통제 솔루션

폐쇄망에서 (업무용 PC) SaaS 서비스를 사용할 수 있도록 개발한 업무용 SaaS 이용 보안통제 솔루션으로
사용자 인증을 통해 내부 사용자임을 확인하고, 부여된 권한에 따라 SaaS 서비스 이용이 가능하도록 제공

네트워크 구성

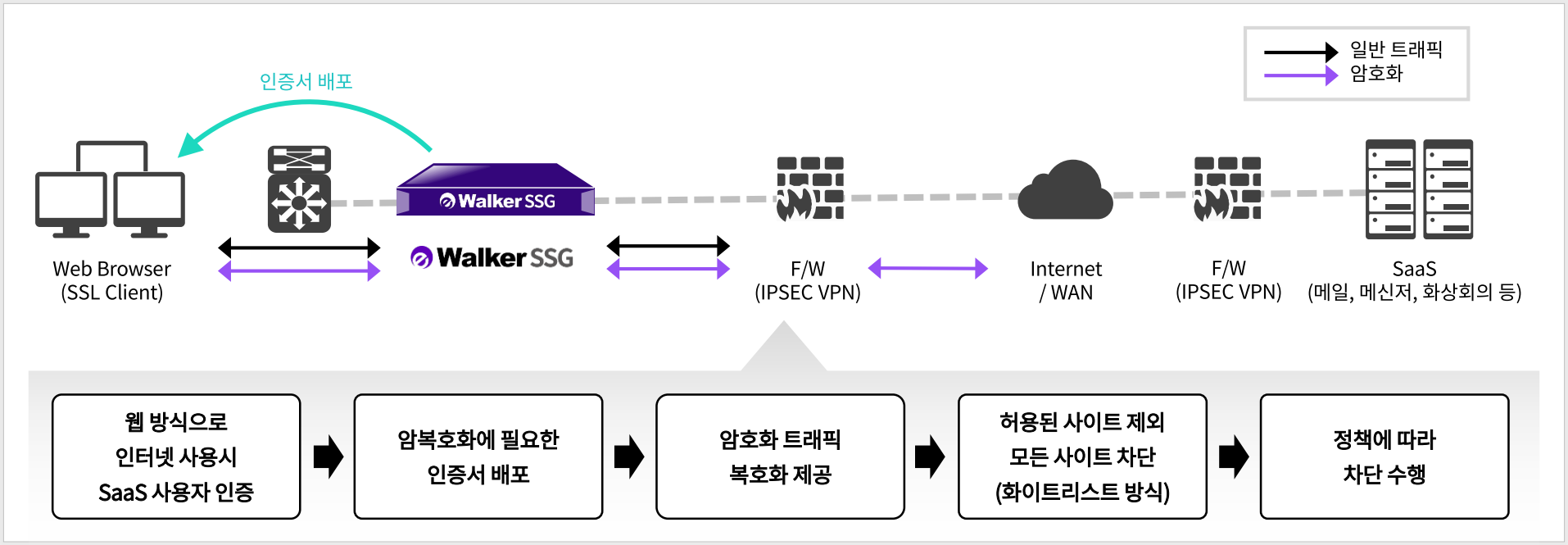
기관 업무 망에서 클라우드 업무용 SaaS 접속 방안

논리적 프록시 체인 구성

- SaaS Secure Gateway는 프록시 체인(리얼 인라인) 모드가 내부에서 논리적으로 구성
- 네트워크 트래픽의 SWG와 DLP를 통과하여, 보안 정책이 실시간으로 적용

접근 제어

화이트 리스트
모두 차단, 특정 항목만 허용
보안성 ⬆



SafeAI 생성형 AI 게이트웨이 솔루션

안전한 생성형 AI 서비스만 사용할 수 있도록 관리하고, N2SF 가이드라인을 준수하여 생성형 AI 사용 과정에서
발생할 수 있는 민감정보 유출을 실시간으로 저장/탐지/차단하는 AI 업무혁신 전문 솔루션

도입 필요성

생성형 AI 사용 증가에 따른 보안 위협 증가

민감정보 프롬프트 입력, 기밀파일 업로드, 비인가 AI 도구 사용 등
생성형 AI 도입으로 인한 새로운 데이터 반출 경로 형성

국가 망 보안체계(N2SF) 정책 변화

최신 보안 정책 변화 가이드라인에 따라 생성형 AI 서비스 이용 시
'보안 대책 마련' 필수

주요 기능

멀티 LLM 사용 편의성

다양한 LLM을 한 화면에서 자유롭게 사용
원클릭 모델 전환 / 복수 LLM 동시 사용 및 응답 비교
수백 종의 LLM 손쉬운 연동 지원

데이터 보안

민감정보 자동 탐지 및 마스킹
LLM으로 프롬프트 전송 전 검증
정책 위반 데이터 차단 / 사용자별 직접 접근 차단
프롬프트 내용 및 첨부파일까지 모두 로깅

AI 사용 예산 관리

실시간 AI 활용 현황 및 비용 모니터링
총 사용량 임계치 설정
사용자/팀 단위 사용량 제한
예산 설정 및 알림

도입 기대효과

보안 강화

개인/기밀/민감 정보 유출 원천 차단
생성형 AI 사용 제어 및 Shadow AI 통제

컴플라이언스 준수

AI 기본법(2026.01) 준수 및 국가 망 보안체계(N2SF) 신속 대응
개인정보보호법, ISMS-P 감사 대응 체계 확보

AI 사용 비용 최적화

사용량 가시화로 AI 사용 예산 절감
사용자/부서별 임계치 조정 및 토큰/비용 실시간 모니터링 및 추적

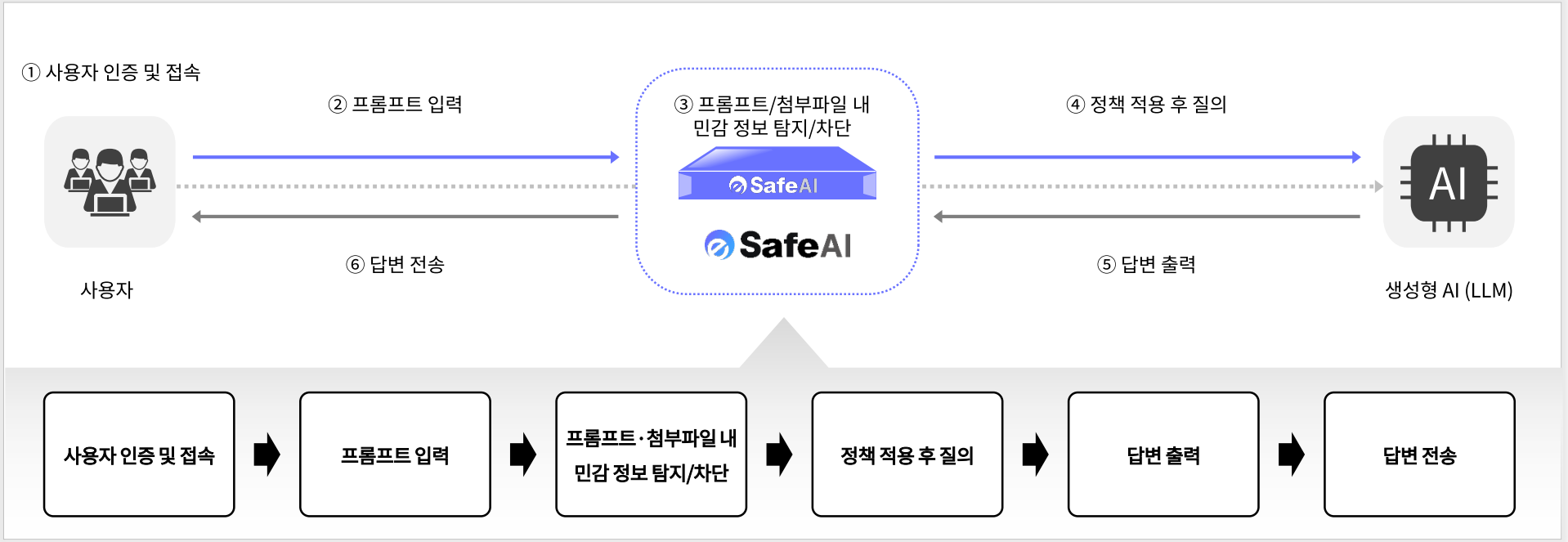
SafeAI 생성형 AI 게이트웨이 솔루션

안전한 생성형 AI 서비스만 사용할 수 있도록 관리하고, N2SF 가이드라인을 준수하여 생성형 AI 사용 과정에서
발생할 수 있는 민감정보 유출을 실시간으로 저장/탐지/차단하는 AI 업무혁신 전문 솔루션

시스템 구성도

별도의 설치 없이 간편한 서비스 도입

- AI-DLP 및 가이드라인 기반 민감 정보 차단, 프롬프트 위협을 실시간 모니터링하는 직관적인 대시보드 제공
- 공공·금융기관의 보안성 검토와 N2SF 요건에 최적화된 화면 제공



보안컨설팅 서비스

수산아이앤티는 과학기술정보통신부 지정 정보보호 전문서비스 기업으로, 고객의 정보자산을 안전하게 보호하기 위한 전문 컨설팅 서비스를 제공합니다.

서비스 특장점

정보보호 전문서비스 기업

- 과기정통부 지정 정보보호 전문서비스 기업
- 공공·금융기관 대상 인증 컨설팅 다수 수행

전문 컨설턴트 수행

- 고객 요구에 최적화된 맞춤형 대응
- 다수 컨설팅 경험의 보안 전문가 구성

검증된 방법론

- 독자적 방법론(SMART) 적용
- 기술·경험을 접목한 체계적 마스터 플랜

최신 보안 정보 반영

- IT 신기술 및 컴플라이언스 변화 신속 대응
- 보안 트렌드 및 업계 사례 기반 환경 분석

서비스 제공 항목

구분	제공 항목	주요 내용
01	정보보호 종합 컨설팅	기업 전반의 보안 수준 진단부터 전략 수립까지 전사적 대응 체계 수립
02	주요정보통신기반시설 취약점 분석·평가	국가 기반시설 대상 보안 취약점 분석 및 평가 후 대응 전략 제시
03	기술적 취약점 점검 및 모의해킹	실전 침투 테스트를 기반으로 한 시스템 진단
04	클라우드 보안·인증 컨설팅	Public Cloud(AWS) 환경 보안 진단 및 정보보호 관리 체계 인증 지원
05	개인정보보호 컨설팅	개인정보 흐름 분석과 유출 방지 대응 전략 수립
06	정보보호 및 개인정보보호 인증 지원	ISMS, ISMS-P, ISO27001 등 인증 획득을 위한 전문 컨설팅 제공

통신사 플랫폼 서비스

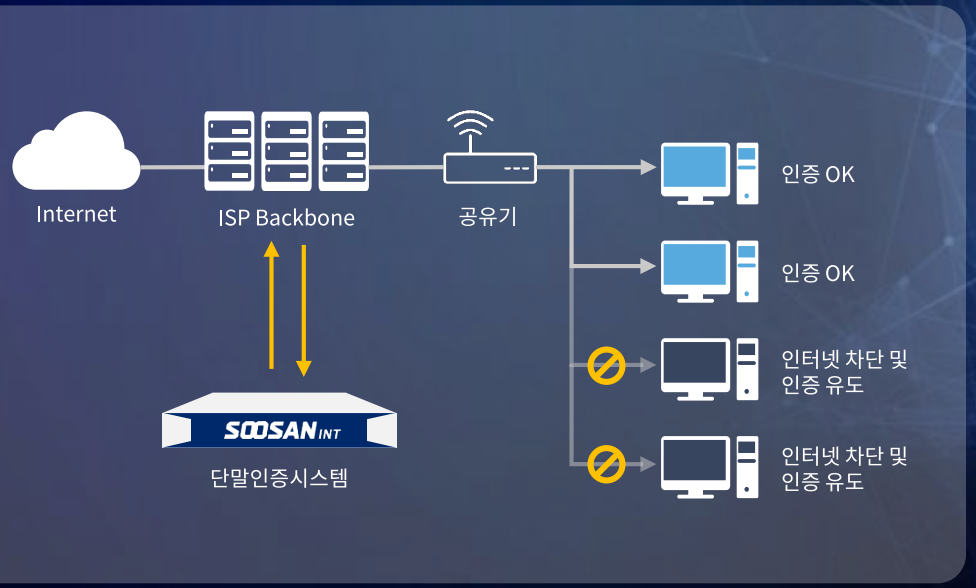
통신사의 새로운 부가서비스를 창출한 전국 규모의 백본 인프라 서비스로서 '단말식별기술'을 기반으로 한 국내외 최초 부가서비스 모델

다수단말 사용 고객을 위한 초고속 인터넷 부가서비스

10년 이상 서비스 진행

통신 3사 서비스 제공

전국 단위 서비스 운영



주요 고객사

기업

- SAMSUNG
- kt
- HYUNDAI
- LG U+
- posco
- KIA
- SK E&S
- SK 브로드밴드
- CJ ENM
- KUMHO TIRE
- 현대건설
- NC
- 롯데이노베이트
- MBC

금융

- 한국은행
- 금융결제원
- 한국수출입은행
- 신한은행
- toss
- kakaobank
- 비씨카드
- Hyundai Capital
- KB증권
- 한화투자증권
- KDB생명
- 현대해상화재보험
- NEXTRADE
- 금융투자협회

공공

- 국가인권위원회
- 방송통신위원회
- 금융위원회
- 법제처
- 교육부
- 외교부
- 통일부
- 법무부
- 보건복지부
- 국세청
- 경찰청
- 검찰
- 대법원
- LH 한국토지주택공사

의료/교육

- 서울아산병원 Asan Medical Center
- 강릉아산병원 GangNeung Asan Hospital
- 세브란스병원 SEVERANCE HOSPITAL
- 국민건강보험공단 일산병원
- 한일병원 HANIL GENERAL HOSPITAL
- 울산대학교병원 ULSAN UNIVERSITY HOSPITAL
- KNUH 경북대학교병원
- 중앙대학교병원
- 경상북도교육청
- 경상남도교육청
- 인천광역시교육청
- 제주특별자치도교육청
- 대전광역시교육청
- 울산광역시교육청

주요 수상 및 인증

수상 내역

최우수 중소기업상 인터넷기반 네트워크 SW 부문 (2000)
정보문화상 국무총리상 (2002)
인텔리전스대상 지능형응용부문 우수상 (2010)
벤처창업진흥 공로 대통령 표창장 (2011)
한국발명진흥회 발명진흥 표창장(2011)
전자 IT산업 특허경영대상 한국라이센싱협회장상 (2012)
ICT 중소 벤처기업 발전공로 표창장 (2014)
전자 ICT 산업 특허경영대상 동상 (2014)
신 SW 상품대상 우수상 (2019)
신SW상품대상 과기정통부 장관상 (2021)
과기정통부 우수 정보보호 기술 선정 (2025)

인증 내역

CC인증 (Common Criteria)
eWalker SWG V10, eWalker SSL VPN V10, eWalker WAF V9
GS인증 (Good Software)
eWalker DLP V9, eWalker SWG V9, eWalker SWG V10,
ePrism SSL VA V10, eWalker DLP V10, eWalker WAF V9

궁금하신 점은 아래 대표번호로 연락 주시면 상세히 안내해 드리겠습니다.

1,700여 개 고객사에 인정받은 27년 노하우로 여러분의 네트워크 보안을 책임집니다.

① 보안솔루션

- N2SF 맞춤형 SaaS 통제 솔루션
- 유해사이트 차단 솔루션
- SSL 복호화 솔루션
- 내부정보 유출방지 솔루션
- 웹방화벽 솔루션
- 가상사설망 솔루션
- 클라우드 보안 솔루션
- 생성형 AI 게이트웨이 솔루션

② 보안컨설팅

- 정보보호 종합 컨설팅
- 주요정보통신기반시설 취약점 분석·평가
- 기술적 취약점 점검 및 모의해킹
- 클라우드 보안·인증 컨설팅
- 개인정보보호 컨설팅
- 정보보호 및 개인정보보호 인증 지원

③ 서비스

- 공유단말접속관리
- 수호천사 모바일
- 악성메일 모의훈련
- 침해사고 분석 서비스

www.soosanint.com ask@soosan.co.kr
서울특별시 강남구 밤고개로 5길 13 수산빌딩, 06367