EMPHASIS
INFORMATION TECHNOLOGY

2025 Solution Guidebook for the Security Market

보안솔루션가이드북

엠퍼시스
정보기술

EMPHASIS
INFORMATION TECHNOLOGY

SECURITY CONTENTS

EMPHASIS A Leading Company of Enterprise Solution Provider.

고객의 미래가치를 극대화하는 IT기업

엠퍼시스정보기술

EMPHASIS INFORMATION TECHNOLOGY

회사명	㈜엠퍼시스정보기술	**대표자**	이영호
설립일자	2009년 03월 02일	**임직원**	16명
자산총계	69.27억	**신용등급**	BB+
사업분야	응용소프트웨어 개발 및 공급업		

주요사업

정보보안 사업
(Information Security)

개인정보검출, 접속기록관리, 출력물보안, 백신, EDR, DB보안, 문서중앙화, 개인정보 비식별화,FW, VPN, IPS, Ddos, APT, L2보안스위치, 유해차단, 웹방화벽, WIPS, VDI, 망분리, 망연계, NAC, SSL가시성, 이메일 보안 등의 제품을 제공합니다.

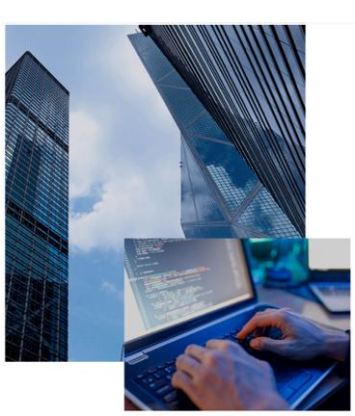
보안관제서비스
(Security Operation Service)

네트워크, 서버, 컴퓨터, 엔드포인트 디바이스, 운영 체제, 애플리케이션 및 데이터베이스에서 사이버 보안 사고의 징후가 있는지 지속적으로 검사하고 24시간 모니터링하여 고객의 정보를 보호합니다.

컨설팅
(Security Consulting)

고객의 요구사항에 따라, 정보보안 솔루션 도입부터 프로젝트 종료 후, 지속적인 고객서비스를 통해 문제점 및 해결 방안을 제시하고 컨설팅 및 교육을 통해 자체적인 운영이 가능하도록 가이드 합니다.

주요연혁



- **2024** 위즈코리아 핵심 파트너 체결
  팔로알토 전략기술 파트너 등록
  위즈베이스 협력파트너 체결
  펜타시큐리티 협력 파트너 체결
  오케스트로 파트너 체결
- **2023** 엑스게이트 플레티넘 파트너 체결
  파이오링크 전략 파트너 체결
- **2022** 아이젝스 전략파트너 체결
  뉴데이소프트 전략 파트너 체결
- **2021** 아토리서치 파트너 체결
- **2020** 이스트 파트너 체결
- **2019** 기업부설연구소 설립
  한싹시스템즈 파트너 체결
- **2018** 이너버스 파트너 체결
  시스코 보안사업부 기술 파트너 체결
- **2017** 조직 개편 및 확장 이전
  연구개발전담부서 IoT개발부 설립
- **2016** 이노티움 채널 체결
- **2015** 파이어아이 채널 체결
- **2014** 넥스지 골드 파트너 체결
  인포블락스 채널 체결
  모두스원 채널 체결
- **2013** 유넷시스템 채널 체결
  미라지웍스 채널 체결
  시큐아이 골드 파트너 체결
- **2012** 펌킨네트웍스 전국 총판 체결
  이지서티 제품공급 채널 체결
  시큐위즈 채널 체결
  DB Inc.(구.동부CNI) 협력사 체결
- **2011** 펌킨네트웍스 제품공급 채널 체결
  소만사 기술전문 채널 체결
  펜타시큐리티 웹방화벽 채널 체결
  LG엔시스 협력사 체결
- **2010** 어울림정보기술 제품 공급 채널 체결
  시스코 파트너 체결
  엑스퍼넷 레드스캔 총판 체결
  대신정보통신 파트너 체결
- **2009** ㈜엠퍼시스정보기술 법인 설립

Main Product

Security Distributor Solution Map

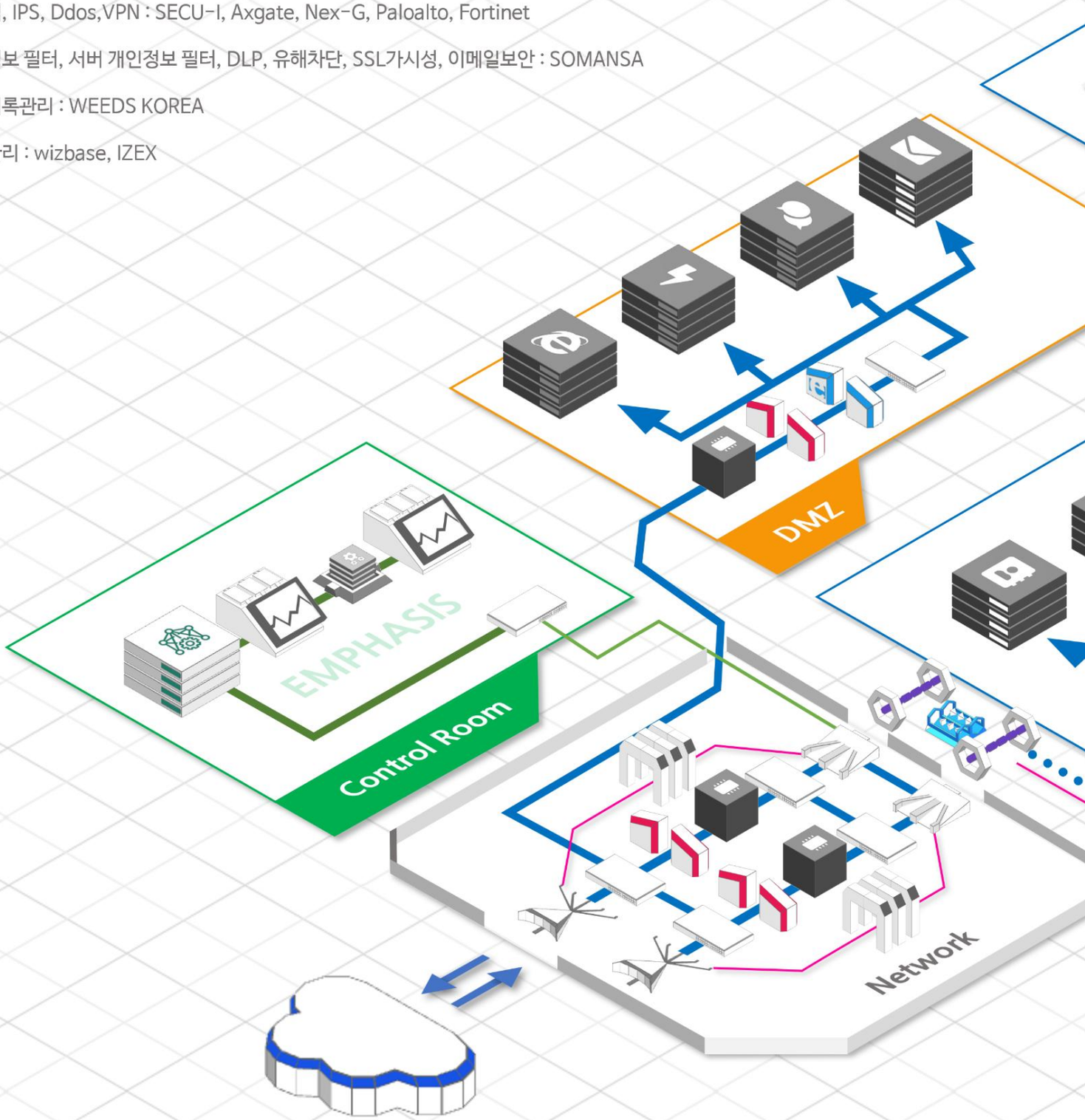
Technical Support Product

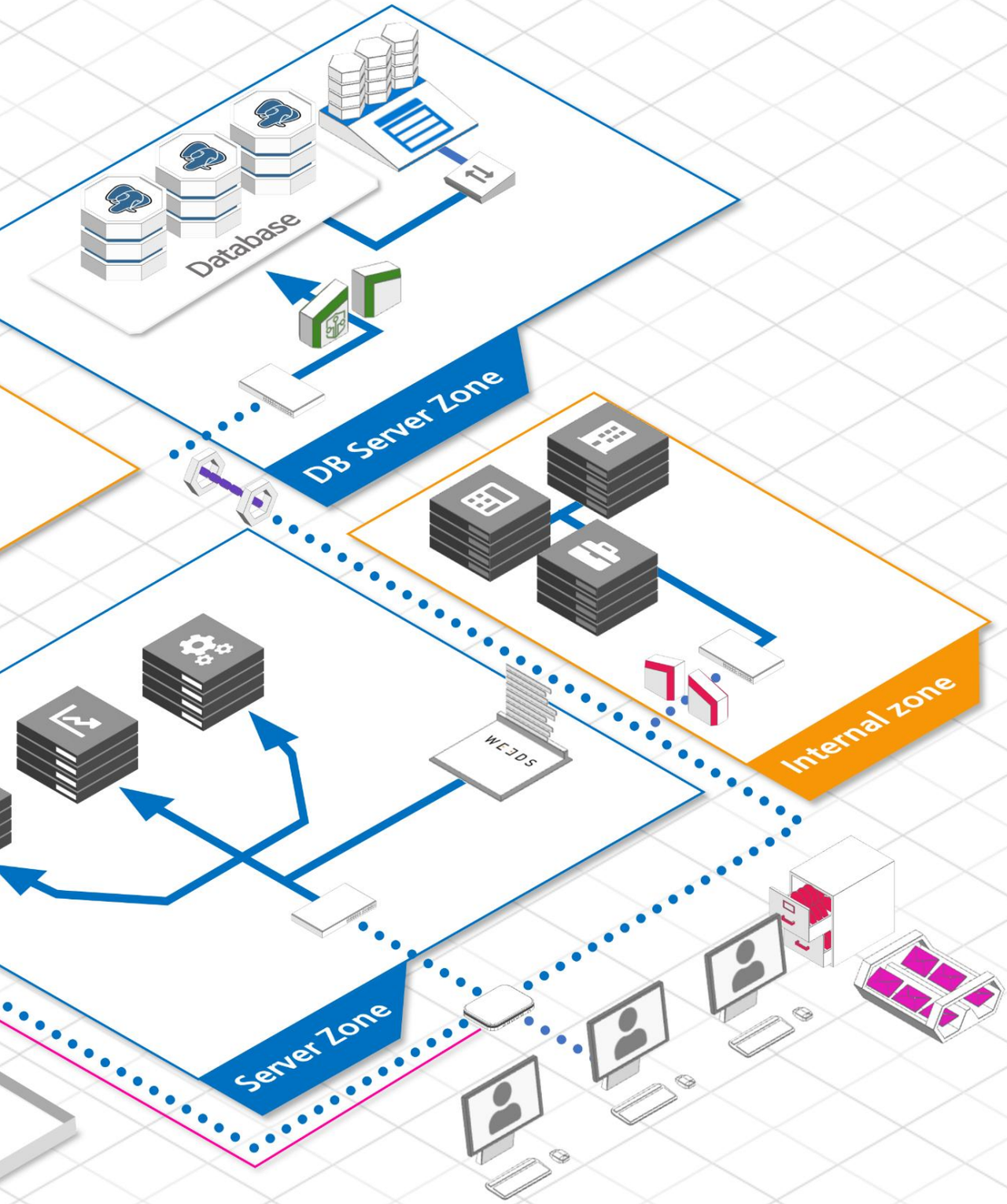
방화벽, IPS, Ddos,VPN : SECU-I, Axgate, Nex-G, Paloalto, Fortinet

개인정보 필터, 서버 개인정보 필터, DLP, 유해차단, SSL가시성, 이메일보안 : SOMANSA

접속기록관리 : WEEDS KOREA

자산관리 : wizbase, IZEX



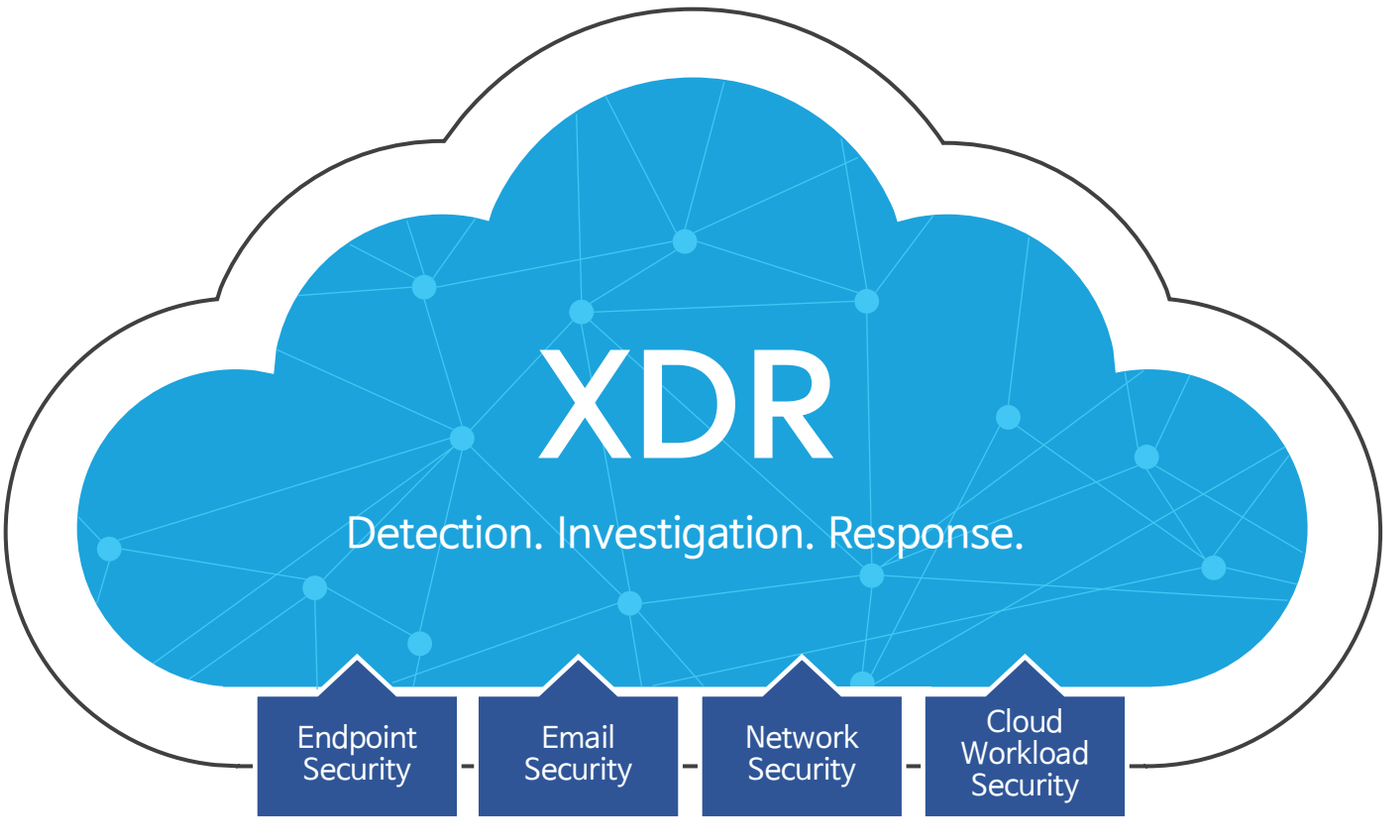


기술문의 02-413-2280
sales@epsis.co.kr
서울 송파구 송파대로 201
테라타워2 A동 1008호
기술문의를 하시면 고객사 별 담당 엔지니어 및 영업지원을 배정하여 안내해 드립니다.
EMPHASIS INFORMATION TECHNOLOGY

XDR

eXtended Detection & Response

확장된 탐지 및 대응, 통합 보안의 정점을 향하다



XDR, EDR, SIEM, SOAR, MDR, SOC 비교

기능	XDR	EDR	SIEM	SOAR	MDR	SOC
실시간 모니터링	O	O	O	O	O	O
위협 탐지	O	O	O	O	O	O
자동화 대응	O	O	X	O	X	X
포렌식 분석	O	O	O	O	O	O
보고 및 알림	O	O	O	O	O	O
데이터 통합	O	X	O	O	X	X
포괄적 분석	O	X	O	O	O	O
보고 및 시각화	O	O	O	O	O	O
데이터 수집	O	X	O	X	X	X
실시간 분석	O	O	X	O	O	X
상관관계분석	O	X	O	O	O	O
인적자원필요	△	△	O	△	O	O
규정 준수 지원	O	X	O	X	O	O
오케스트레이션	O	X	X	O	X	X
인시던트 대응	O	X	X	O	O	O

XDR

확장된 탐지 및 대응(eXtended Detection & Response)은 EDR 솔루션의 진화입니다. XDR은 탐지 범위를 엔드포인트 너머로 확장하여 여러 데이터 소스에서 탐지, 분석 및 대응을 제공합니다. XDR은 모든 IT 계층과 애플리케이션의 동작을 수집하고 분석합니다. 엔드포인트 외에도 여기에는 네트워크 구성 요소와 클라우드 서비스가 포함됩니다. 이런 방식으로 XDR은 IT 보안과 가능한 사이버 위협에 대한 전체적인 관점을 만들어 조사 및 대응 활동을 간소화합니다.

EDR

엔드포인트 탐지 및 대응(Endpoint Detection and Response)은 PC, Labtop 또는 Server와 같은 앤드포인트 디바이스에서 사이버 위협을 탐지하고 조사하도록 설계된 솔루션입니다. 바이러스 백신 소프트웨어와 달리 EDR은 바이러스 서명을 위해 파일을 스캔하여 사이버 위협을 탐지할 뿐만 아니라 엔드포인트 디바이스의 동작을 살펴봅니다. 의심스러운 동작이 탐지되면 이 도구는 IT 보안 팀에 경고하고 수정 조치를 제안합니다. EDR 도구는 엔드포인트 격리와 같은 자동화된 완화 대응도 제공할 수 있습니다.

SIEM

SIEM(보안 정보 및 이벤트 관리, Security Information and Event Management)은 조직이 IT 네트워크에서 데이터를 중앙 집중화, 상관 관계 분석하여 보안 문제를 탐지할 수 있는 솔루션입니다. SIEM의 주요 기능은 로그 관리 및 중앙 집중화, 보안 이벤트 탐지, 보고 및 검색 기능을 포함합니다. 분석가는 로그 및 이벤트 데이터를 검토할 수 있으며, 규정 준수 및 감사 목적으로 보안 데이터를 추적하고 기록할 수도 있습니다.

SOAR

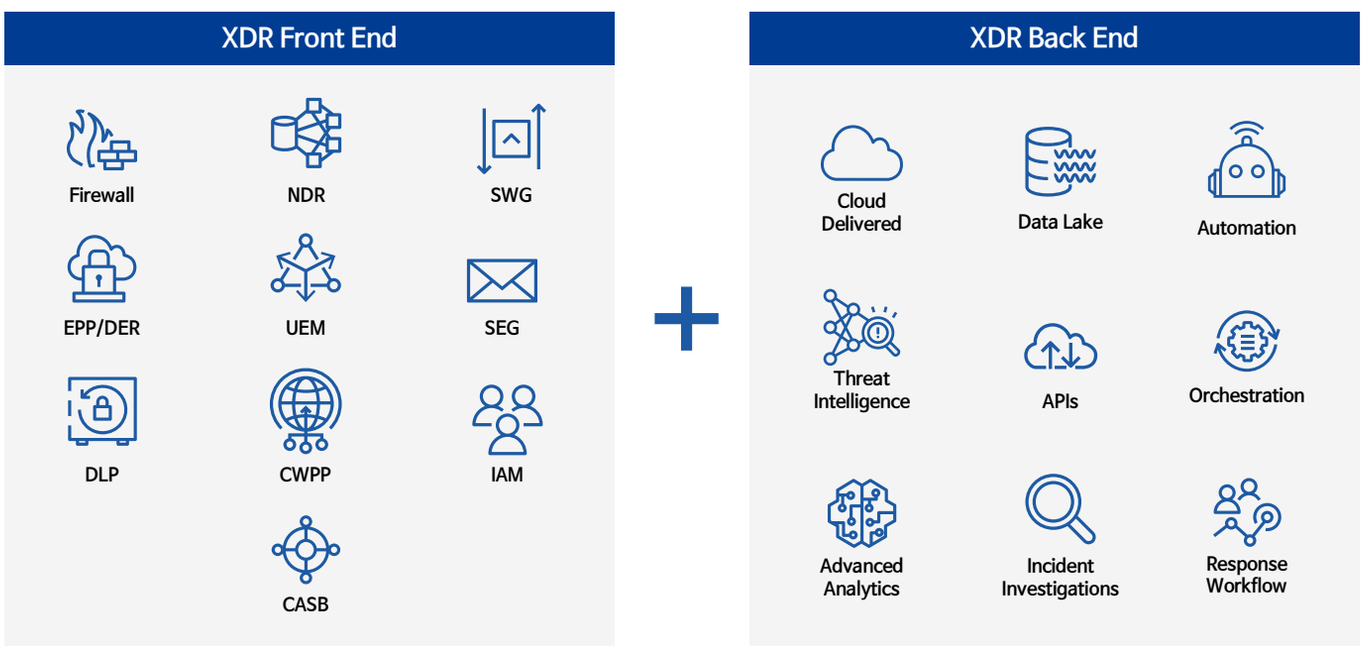
보안 오케스트레이션, 자동화 및 대응(SOAR)은 SIEM 플랫폼을 보완하고 지원하는 솔루션입니다. SOAR는 이벤트 데이터를 풍부하게 하고, 중요한 인시던트의 식별을 간소화하고, 특정 이벤트나 트리거에 대한 대응 조치를 자동화하는 것을 목표로 합니다. 인간의 개입이 필요할 때만 위협을 확대하는 것이 목표입니다.

MDR

MDR(Managed Detection and Response)은 전문 보안 서비스 제공업체가 기업의 사이버 보안 환경을 관리하고, 위협을 탐지하며, 대응하는 서비스입니다. MDR은 기업 내부의 보안 인력이나 자원이 부족한 경우, 외부의 전문 보안 팀을 통해 효과적으로 보안 위협에 대응할 수 있도록 지원합니다.

SOC

보안 운영 센터(SOC) 는 조직의 IT 인프라를 보호하도록 설계된 중앙 제어 센터입니다. SOC는 보안 관련 시스템을 모니터링하는 역할을 합니다. 또한 위협을 분석하고 적격성을 평가하며, 인시던트 대응 조치를 초기화하고 지원합니다. SOC 분석가는 일반적으로 특수 도구를 사용하여 조정된 프로세스에서 다른 분야의 사이버 보안 전문가와 협력합니다.



가트너(Gartner) 보고서에서 XDR의 구성요소를 크게 프론트엔드와 백엔드, 두 가지로 구분하고 있습니다. 보안 벤더의 XDR 구성 역시 크게 다르지 않습니다. 정보수집 대상과 대응을 위한 보안 솔루션 다수가 프론트엔드에 해당됩니다. 솔루션의 제한은 없습니다. 그러나 탐지와 대응에 중점을 두고 협업을 통해 역량을 고도화 할 수 있어야 합니다. 백엔드는 정보수집 방법과 분석을 위한 클라우드, 인공지능(ML), 통합과 자동화 기술 등으로 구성됩니다. 프론트엔드 솔루션을 위한 데이터 통합, 연동 API 제공, 통합 정책관리 등의 기능이 요구됩니다.

SASE

Secure Access Service Edge

도입 장벽을 넘어 영향력을 확대하다

클라우드 보안 서비스

SASE는 광역 네트워킹 및 네트워크 보안 기능을 하나의 통합된 클라우드 제공 네트워크 보안 서비스로 결합하는 네트워크 보안 접근 방식입니다.
최근 4차 산업혁명, 디지털 전환의 가속화로 고객 IT 인프라 환경은 지속적으로 다양화되고 고도화되고 있습니다. 특히 온프레미스뿐만 아니라 클라우드를 활용하는 기업들이 늘어나면서 방어해야 하는 영역은 더 넓어지고 있는 상황입니다. 또한 고객의 정보자산을 노리는 공격자와 보안 위협은 지속적으로 강력해지고 있으며, 전문성을 갖춘 전문가의 신속한 대응이 중요합니다.
SASE와 기존 네트워크 보안의 주요 차이점은 SASE가 보안 정책을 적용하기 위해 모든 트래픽을 데이터 센터로 다시 라우팅하는 대신, 네트워크 엣지에서 사용자와 엔드포인트가 연결되는 위치와 더 가까운 곳에서 보안 기능 및 기타 서비스를 제공한다는 것입니다.

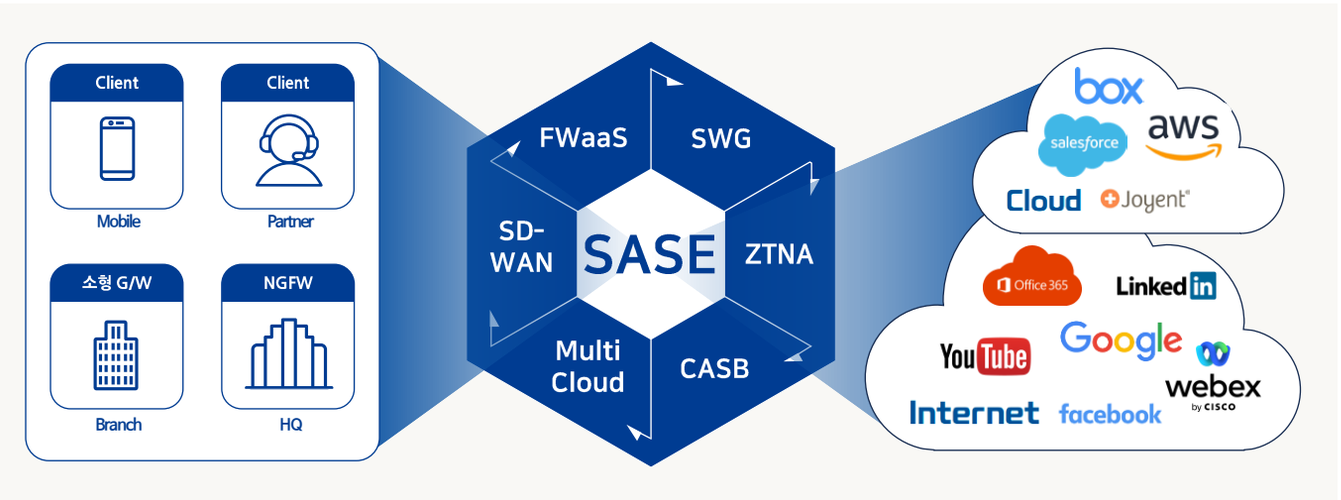
SASE
왜 SASE 인가?

SASE 도입 배경

- 고객들의 자산이 멀티 클라우드 전환
- 비대면 근무, 지점/ 지사 등으로 분산되고 복잡한 IT 환경
- 모바일, PC, IoT 다양한 접속 단말 증가로 보안 복잡도 증가

필요 고객

- 증가하는 지사/ 지점에 따라 빠른 보안 솔루션 구성이 필요한 기업
- 스타트업, 소규모 기업 등 전문적인 보안 담당자 부재한 기업
- 재택 및 출장 등 원격 업무 사용자 많은 고객



SASE
모든 것을 하나로 통합하기

SASE 솔루션은 SD-WAN을 사용하여 네트워크 엣지에서 연결 위치에 있거나 연결 위치에 가까운 사용자, 디바이스 및 기타 엔드포인트에 SSE 보안 서비스를 제공합니다.

특히, SASE 아키텍처는 검사 및 암호화를 위해 모든 트래픽을 중앙 데이터 센터로 다시 보내는 대신 최종 사용자 또는 엔드포인트와 가까운 분산 접속점(PoP)으로 트래픽을 보냅니다. (PoP는 SASE 서비스 제공업체가 소유하거나 타사 공급업체의 데이터 센터에 구축됩니다.) PoP는 클라우드 제공 SSE 서비스를 사용하여 트래픽을 보호한 다음, 사용자 또는 엔드포인트를 퍼블릭 및 프라이빗 클라우드, 서비스형 소프트웨어(SaaS) 애플리케이션, 퍼블릭 인터넷 또는 기타 리소스에 연결합니다.

SASE
특장점 및 구성 요소

SASE 플랫폼은 하나의 인터페이스에서 관리되고 하나의 제어판에서 제공되는 다양한 보안 기능에 서비스형 네트워크(NaaS) 기능을 결합합니다.

구분	상세 내용
Service Portal	• 고객/ 서비스별 운영 현황(이용 추이, 과금 현황 등), 이미지/ 콘텐츠 배포 관리 • 이용 중인 서비스에 대한 정책 설정 및 모니터링 기능 제공(고객사별)
내부 보안 기능 Inline Security Edge	• NGFW의 정책 기반 보안 기능 수행 • SSL 암/복호화, QoS, VPN, NAT 등 네트워킹 기능 수행 • 인증/계정 관리, 과금, 정책 적용 등
외부 보안 기능 Out-Of-Band Security Edge	• AV, 정적/ 동적 분석, AI/ ML 분석을 통한 멀웨어 탐지 • 민감한 정보 및 조직의 주요 정보 유출 검사 및 Compliance 점검 • 시그니처, Blacklist, URL DB, TI 정보 등 위협 관련 정보 제공
로그 관리 기능 DataLake	• Big Data 기반 Security Edge에서 발생한 로그 저장 • 고객/ 서비스별 로그 조회 및 Top 정보 제공 등 • 로그 분석을 통한 이상 행위 탐지 및 고객사별 리포트 생성

SASE
지원 서비스

벤더의 역량에 따라 위의 SASE 구성 요소는 아래에 자세히 설명된 클라우드 이메일 보안, 웹 애플리케이션 및 API 보호(WAAP), DNS 보안 및/또는 보안 서비스 에지(SSE) 기능과 함께 번들로 제공될 수도 있습니다.

구분	상세 내용
FWaaS	기존 방화벽보다 더 깊은 수준에서 데이터를 검사합니다. 예를 들어, NGFW는 애플리케이션 인식 및 제어, 침입 방지, 위협 인텔리전스를 제공하여 정상적으로 보이는 트래픽에 숨어 있을 수 있는 위협을 식별하고 차단할 수 있습니다.
SD-WAN	SASE 아키텍처의 경우 조직에서는 SD-WAN 또는 서비스형 WAN(WANaaS)을 채택하여 사무실, 소매점, 데이터센터 등 원거리에 걸쳐 있는 운영 조직을 연결하고 확장합니다.
SWG	원치 않는 웹 트래픽 콘텐츠를 필터링하고 온라인에서 위험하거나 승인되지 않은 사용자 행동을 차단하여 사이버 위협을 방지하고 데이터를 보호합니다. SWG는 어디에든 배포할 수 있으므로 하이브리드 근무 보안에 이상적입니다.
ZTNA	보안 모델은 위협이 네트워크 내부와 외부에 모두 존재한다고 가정하므로 사람, 앱, 장치가 회사 네트워크의 리소스에 액세스하려고 할 때마다 엄격한 컨텍스트 확인이 필요합니다. Zero Trust 네트워크 액세스(ZTNA)는 Zero Trust 접근 방식을 가능하게 하는 기술로, 사용자와 해당 사용자가 필요로 하는 리소스 간에 일대일 연결을 설정하고 이러한 연결을 주기적으로 재확인 합니다.
CASB	클라우드 및 SaaS 앱을 사용하면 데이터를 비공개로 안전하게 유지하기가 더 어려워집니다. CASB는 이러한 문제에 대한 해결책 중 하나로, 조직의 클라우드 호스팅 서비스 및 애플리케이션에 대한 데이터 보안 제어 및 가시성을 제공합니다.

SASE
지원 벤더사

paloalto NETWORKS | SECUI | FORTINET | netskope | HPE aruba networking

ITAM

IT Asset Management

기업의 성장을 위한 IT자산관리의 방향을 제시하다

자산의 사용 기간은 한정되어 있으며 조직은 ITAM과 선제적 관리를 통해 자산의 가치를 극대화할 수 있습니다. 수명주기의 단계는 일반적으로 계획, 구매, 배포, 유지관리, 폐기, 처분 등으로 구성됩니다.

일반적으로 IT 자산은 하나 이상의 범주(물리적, 소프트웨어, 하드웨어, 모바일, 클라우드)에 속합니다. ITAM은 IT 자산의 성공적인 배포와 지속적인 지원을 보장하도록 설계됩니다. 이와 같이, 이러한 IT 자산 유형 중 하나에 해당합니다.

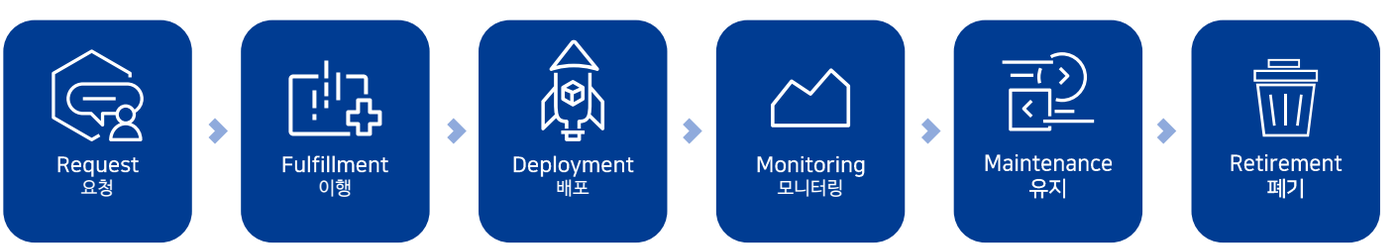
ITAM
IT자산관리 유형

IT 자산 관리의 세 가지 기본 유형은 다음과 같습니다.

구분	상세 내용
소프트웨어	이 유형의 ITAM은 규정 준수 요구 사항, 라이센스, 섀도 IT, IoT 등을 포함하므로 다른 ITAM보다 약간 복잡합니다. 소프트웨어 자산은 지속적으로 모니터링 및 검토되어야 하며, 요구 사항을 따르고 수요와 시장 변화에 부합할 만큼 충분한 유동성이 확보되어야 합니다.
하드웨어	물리적 하드웨어는 조직의 IT 에코시스템 내에서도 중요한 역할을 합니다. 이러한 물리적 자산에는 PC, 프린터, 복사기, 노트북, 모바일 장치, 서버, 그 외 회사 내에서 데이터 관리 목적으로 사용하는 하드웨어가 포함됩니다.
클라우드	ITAM은 SaaS(Software as a Service), IaaS(Infrastructure as a Service), PaaS(Platform as a Service)를 포함한 클라우드 리소스의 비용과 사용량을 추적합니다. 이들은 각각 ITAM 내에서 비용 및 규정 준수를 위해 관리되어야 하는 자산으로 간주됩니다.

ITAM
IT자산관리 프로세스

개별 조직마다 IT 자산 수명주기를 다르게 정의할 수 있지만, 대부분은 다음과 같은 단계를 따릅니다.



ITAM
IT자산관리 필수기능

IT 자산 관리는 단일 작업이 아닙니다. IT 리소스가 가능한 한 효과적으로 사용되도록 보장하는 일련의 전략과 프로세스입니다. 튼튼한 IT 자산 관리 시스템을 구성하는 필수 구성 요소들을 살펴보겠습니다:

구분	내용	주요기능
자산식별	• 사내 모든 IT 유무형 자산 파악과 세부 정보 기록	PC, 노트북,프린터 등 유형자산 현황 자동수집
		사내PC에 설치된 S/W, OS 자동수집
		Shadow IT 식별 및 등록
		변경, 신규, 삭제 등 세부 정보 기록
구매 및 배포	• 구성원이 필요한 기기 및 서비스의 구매 및 배포	개인, 부서별 필요 기기 구매요청 및 배포
		유형자산 등록(바코드 등)기능, 부품모델 자동식별등록
		S/W라이선스 구매 후 Key등록 등 S/W자동 배포기능
		필수 S/W(OS포함), 지정 업데이트 기능
추적 및 모니터링	• 기기 및 서비스의 사용 현황, 상태, 결제 내역 등의 지속적인 추적	HDD 변경 내역 조회
		PC, 노트북 반출현황 및 내역 조회
		임시, 만료라이선스 모니터링
		자산실사(직접, 사용자지정)를 통한 자산변경 상태 모니터링
수명 주기 관리	• 기기 및 서비스의 결함, 서비스 종료 일정 등의 체계적인 관리	퇴사자 PC 재할당 및 설치된 S/W 라이선스 사용권한부여
		TCO 감가상각에 의한 생명주기 관리
		EOS, EOL 라이선스 관리
		유휴, 폐기, 불용 자산 분류
규정 준수 및 관리	• 라이선스 및 계약 조건 준수	사용라이선스 구매 및 배포 유형에 따라 불법 자동 분류
		사내 보유한 라이선스 수량 초과하는 경우 삭제권고
		지정 IP변경 시 알림 및 통제 관리
		라이선스 승인결제 권한 대상자 분류

ITAM
IT자산관리 추천 기업

임직원은 많은데 인사변동이 심해 자산변동이 심한 기업

실시간으로 변하는 **자산이동 상황을 일일이 추적하고 기록하기가 어려울 때** 필수도입

복잡한 IT 업무 처리로 개별관리를 하고 있는 기업

사내 모든 유무형 IT 자산을 하나의 대시보드에서 관리가 필요하다면 필수 도입

불법단속 또는 자산유실이 빈번히 일어나는 기업

유무형자산 구매 후 관리가 되지 않아 유실이 잦다면 필수 도입

ITAM
지원 벤더사

아이젝스 | 위즈베이스 | 제론소프트앤

CASB

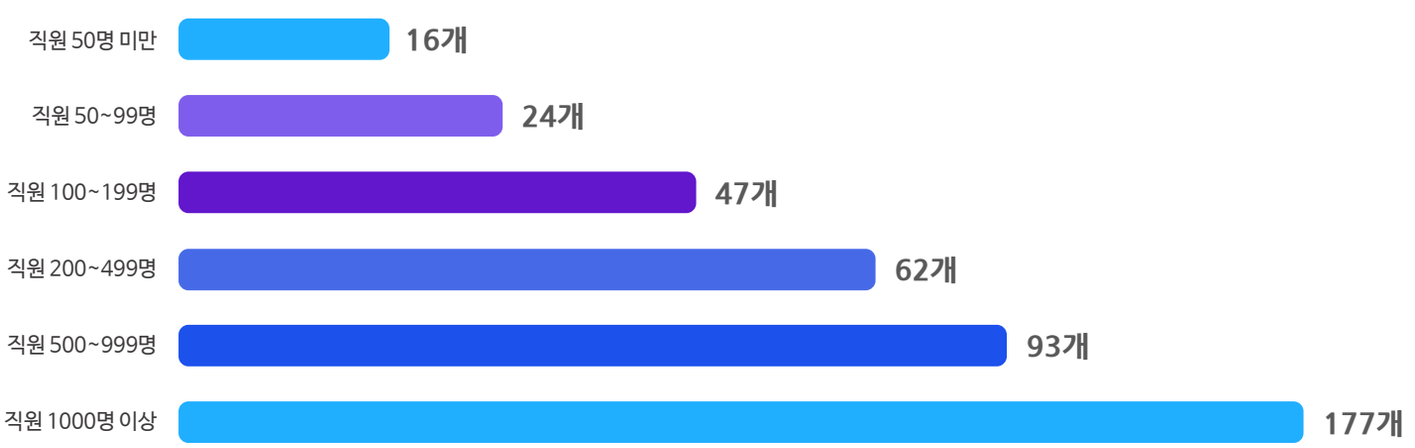
Cloud Access Security Broker

인터넷 연결만으로 어디서든 보안을 강화하다

SaaS(Software as a Service)는 다양한 소프트웨어를 구독 형태로 제공하는 클라우드 비즈니스 모델입니다. SaaS 서비스를 이용하면 인사, 구매 생산관리 등 기업의 주요 업무를 디바이스나 시공간의 제약 없이 처리할 수 있습니다.
하지만 SaaS의 편리함 이면에 새로운 보안 위협도 증가하고 있는데 외부 클라우드에 주요 정보를 저장하다 보니 정보 유출에 대한 우려가 발생하고, 재택근무 환경에서 직원들이 SaaS 서비스를 직접 연결해 사용하면서 유해 사이트를 통한 악성 소프트웨어 유입 사례가 증가했습니다. SaaS를 도입한 기업의 보안 담당자들은 솔루션 사가 제공하는 보안 기능의 생소함과 제약사항, 낮은 보안 가시성으로 어려움을 겪고 있습니다.

CASB
SaaS 서비스 이용현황

기업규모가 클 수록 더 많은 SaaS를 이용합니다.



CASB
장점과 단점

SaaS 서비스는 사용자가 자체 서버에 소프트웨어를 따로 설치하거나 유지 및 관리를 할 필요 없이 최신 기술을 저렴한 비용으로 쉽게 활용할 수 있다는 장점이 있지만 중요데이터를 외부에 저장하기 때문에 보안 규정을 엄격히 준수하여야 합니다.

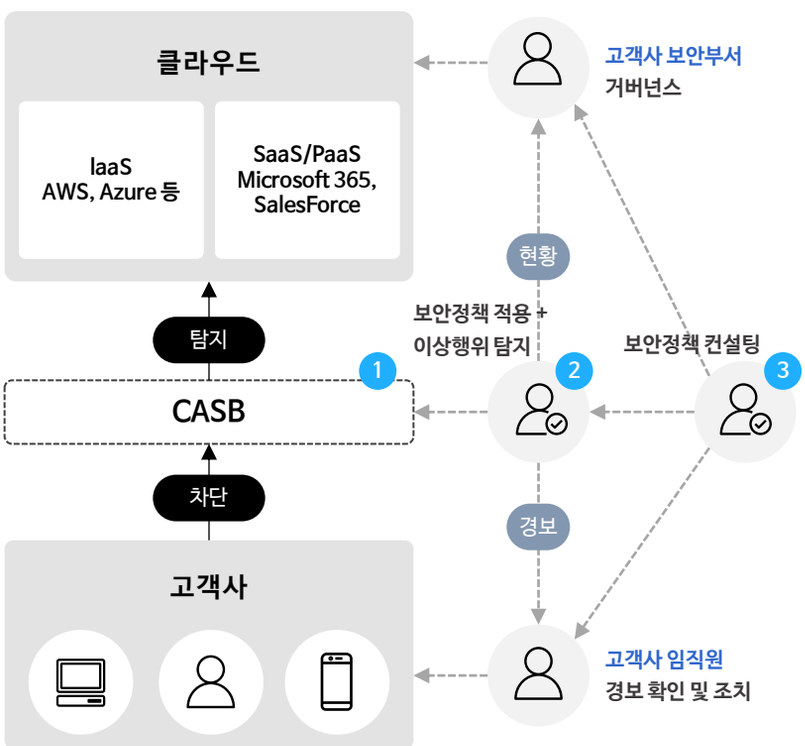
장점	단점
어디서나 아무 장치에서 액세스	강력한 액세스 제어 필요
업데이트나 설치 불필요	벤더종속
비용 절감	**보안 및 규정 준수**

CASB
보안을 위한 기능

서비스형 소프트웨어(SaaS) 보안 솔루션에서 살펴봐야 할 몇 가지 주요 기능은 다음과 같습니다.

구분	상세 내용
PC보안	개인정보 검출
	IT자산의 변경상태 확인
	업무환경 관리
	PC취약점 진단
	이동식 저장매체 차단
	인터넷 파일첨부 차단
	메신저, 원격제어, 웹하드 등 소프트웨어로 반출 차단
	캡처 프로그램, 공유폴더를 활용한 정보 공유 차단
	메일, 클라우드, 웹브라우저 등 인터넷 기반 파일첨부 차단
출력물보안	사용자 출력물 워터마크 삽입
	개인정보 검출 문서는 출력물 통제
	출력이력 기록
암호화	민감정보를 포함한 문서 암호화
	사내 서버 DB암호화
유해차단	웹사이트 접속 제어(차단, 경고, 허용)
백업	중요파일 자동백업
	파일복구
	백업 및 반출현황 관리
관제	24시간 모니터링 및 실시간 대응
백신	랜섬웨어로 인한 파일 훼손 탐지
	원본 파일보호

CASB
CASB 구성 및 적용 사례



CASB(Cloud Access Security Broker)컨설팅

- 고객이 사용중인 SaaS에 최적화된 CASB 선정 및 구축 형태 컨설팅
  → 사전 PoC를 수행한 CASB 모델 적용
  → 모니터링 시 API모드, 차단 필요 시 Proxy모드

※ CASB 종류 추가 및 추후 모드 변경 가능

CASB연동

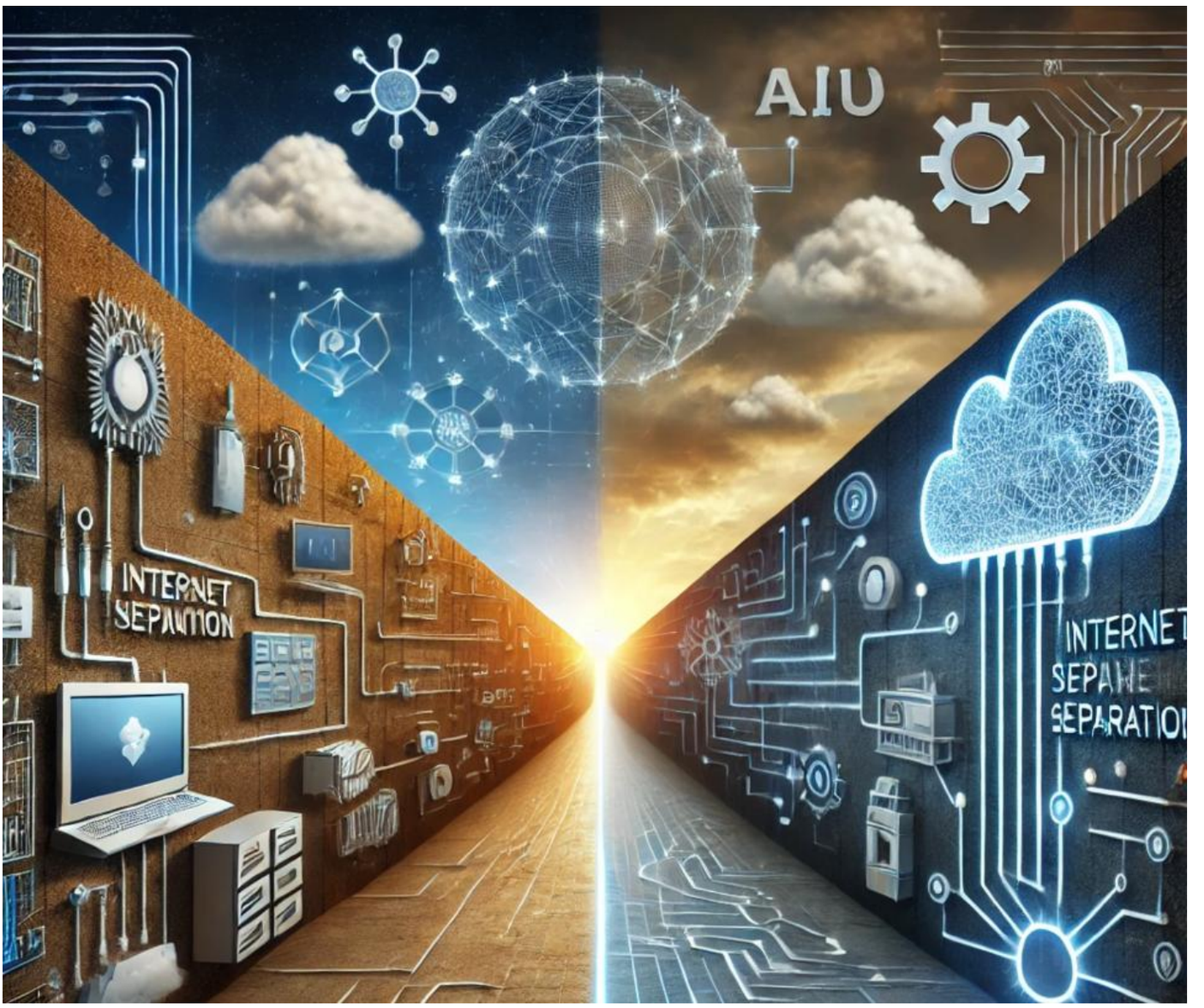
- 고객이 사용 중인 SaaS와 연동 및 구축형태에 따른 IDP, MDM배포

보안정책 및 연락체계 적용

- 고객사 클라우드 보안정책 컨설팅 및 수립된 정책에 기반하여 탐지 및 차단 수행
- 이상행위 발견 시 23x365 상황 전파를 위한 연락체계 정비

망분리
Network Separation

망분리·망연계 규제 개선, 관련 업계에 미치는 영향



망분리 규제 개선의 목적이 망분리 자체를 허무는 것이 아닌, 업무의 효율성과 유연성을 향상시키는 것이며, 예외적 허용이 아닌 보안대책 기술 적용에 따른 명시적 허용인 규제 특례로 비중요 업무의 SaaS 허용이나 생성형 AI의 활용, 그리고 연구개발 단말의 인터넷 접속(보안대책 적용) 등으로 인해 망분리·망연계 솔루션이 신규로 적용되고 있습니다.

망분리
규제 개선방안

망분리 개선의 핵심은 금융회사 등의 망분리 규정을 수정하여 생성형 AI의 활용을 허용하고, 클라우드 서비스(SaaS)의 이용 범위를 대폭 확대하며, 연구·개발 환경을 개선하는 것이 목적입니다.

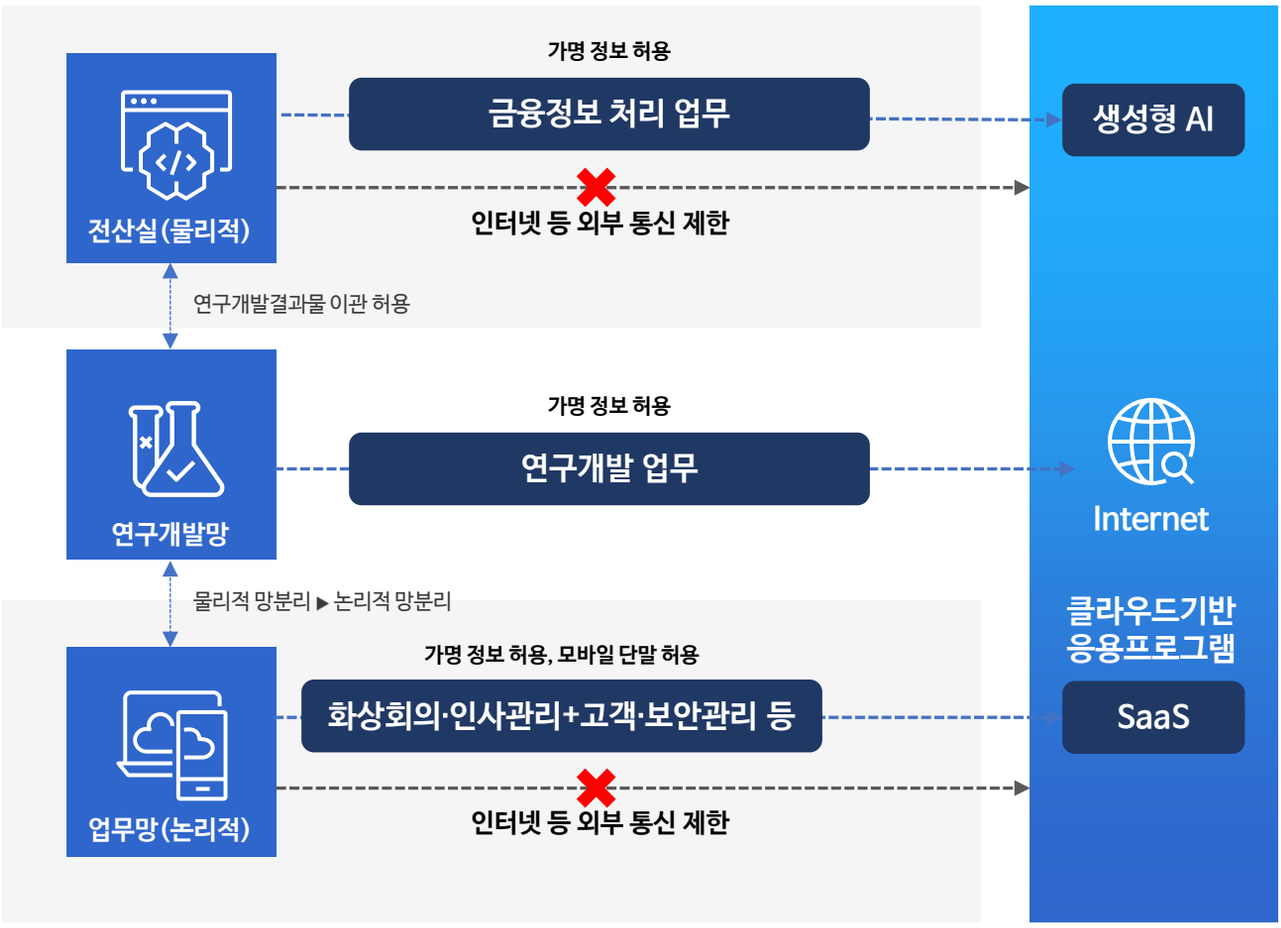
획일적·일률적
물리적 망분리 규제

→

- **개발·테스트 분야 망부리 예외**
- **비전자금융업무, SaaS 망분리 예외**
- **단계적 망분리 완화 추진**

망분리
개선안 구성도

보안사고로 인해 폐쇄적이기만 하던 망분리 시대의 흐름에 따라 변화하며 중요데이터가 아닌 시스템은 클라우드로 이관되고 통제의 범위도 완화되었습니다.



망분리
망분리 솔루션

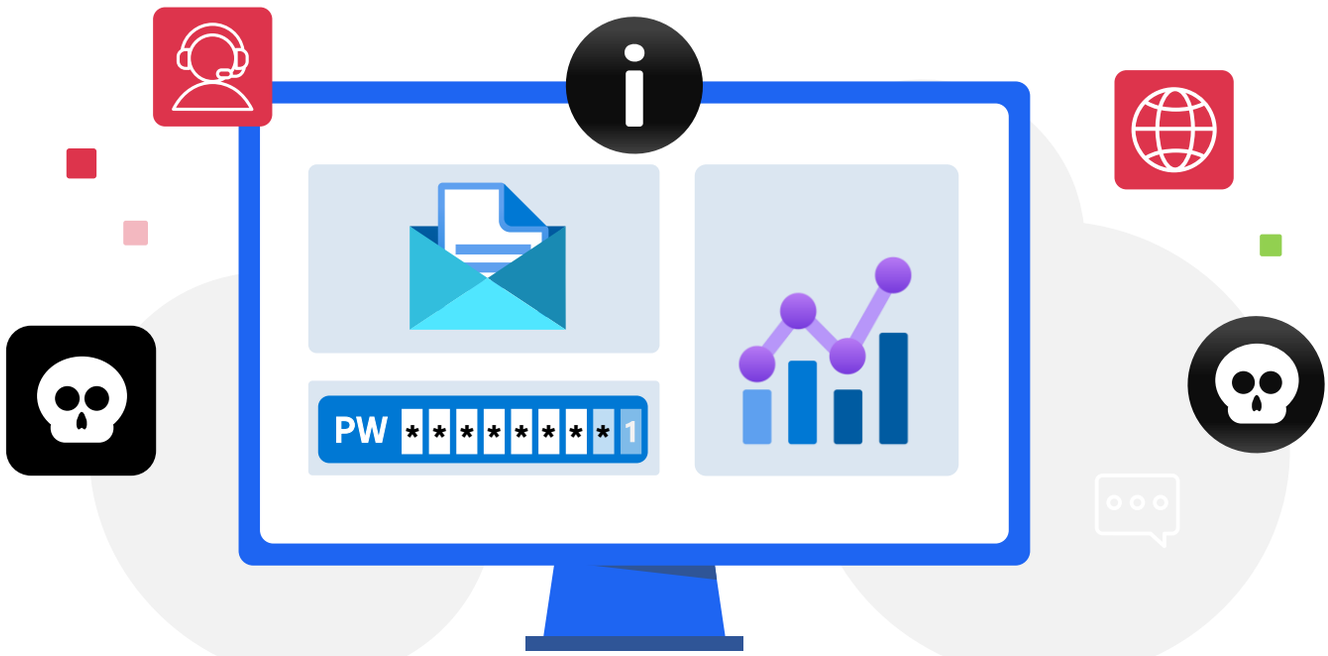
다음은 망분리를 적용하기 위한 최소요건으로 적용 시 장단점에 대한 내용을 안내 드립니다.

망분리 구분	구성 방식	장점	단점	지원사
물리적 망분리	PC 이중화 + KVM 망전환	명확한 망 분리 적용	업무 효율성의 저하	ATEN, TETRA
논리적 망분리	서버기반 컴퓨팅(CBS) Server Base Computing	문서보안성 높음	서버 퍼포먼스 영향 많음	Tilon, Vmware, citrix
	서버기반 컴퓨팅(CBC) Client Base Computing	최저 도입비용, 쉬운설치	H/W 장애 시 사용불가	VMSolution
공통	망연계 솔루션	기존 보안USB보다 편리	망분리 시스템 보안의 홀	Hanssak
	방화벽	시스템 진입점 통제 가능	시스템 내 공격에 취약	SECUI, Paloalto, Fortinet, Nexg Axgate
	스위치	데이터 전송속도 개선	제한된 제어 및 취약점	Juniper, HDN(HanDreamnet)
	NAC	허가되지 않은 기기의 무단 반입 차단	사내 보안정책 우회 가능	Genians, Netman, HUNESION
	DLP(EDLP, NDLP)	외부자료유출 방지	사용자의 불편함	SOMANSA, WISBASE
	백신	악성코드 실시간 검사	Zeroday 공격 대응 불가	EstSecurity
	PMS	보안성, 편의성, 가시성	패치 위변조시 문제 심각	

SOC

Security Operations Center

차세대 보안관제센터(SOC)로의 전환을 위한 핵심 기술



보안관제 서비스는 기업의 정보자산을 노리는 다양한 사이버 보안 위협에 대응하여 전문적이고 체계적으로 24시간 365일 빈틈없이 기업의 정보를 보호하는 서비스 입니다.
보안관제 서비스는 보안관리 체계 개선을 통하여 보안사고를 미리 예방·대응하는 체계를 갖추고, 나아가 외부 사이버 보안 위협 및 내부 정보유출에 신속히 대응하여 정보자산에 대한 선진 수준의 보안 역량 및 기업의 서비스 신뢰도를 확보할 수 있습니다.

SOC

보안관제 서비스 종류

고객의 인프라 환경 및 정보 자산의 특성에 따라 원격·클라우드·파견·하이브리드 형태의 보안관제 서비스를 제공하고 있습니다.

원격 보안관제

On-Premise 환경의 고객 정보 자산을 보호하기 위해 자사 보안관제센터의 침해사고 대응 전문인력이 보안장비 구축 · 운영 및 사이버 위협 분석 · 대응하는 보안관제 서비스

클라우드 보안관제

Cloud 환경에서 운영되고 있는 고객 정보 자산을 보호하기 위해 클라우드 정보보안 전문인력이 SECaaS 및 사이버 위협 분석 · 대응하는 보안관제 서비스

파견 보안관제

고객사 사이버안전센터(SOC)에 정보보안 및 침해사고 대응 전문 인력이 상주하여 고객 요구사항을 반영한 현장 맞춤형으로 제공되는 보안관제 서비스

하이브리드 보안관제

고객사 사이버안전센터와 자사 보안관제센터 간 협력을 기반으로 제공되는 보안관제 서비스 (원격 · On-Premise · Cloud 환경의 다양한 하이브리드 서비스 제공)

SOC
보안관제 서비스 역할

보안관제 서비스는 "예방 → 모니터링 → 분석 → 대응"의 보안관제 방법론에 따라 보안 장비 구축 · 임대 · 운용 및 사이버 위협 분석 · 대응의 전문화된 통합 보안관제 서비스로 고객의 비즈니스 연속성을 보장합니다.

구 분	상세내용
보안관제	• 예방 → 모니터링 → 분석 → 대응 • (예방) 신규 취약점 동향 모니터링 및 분석, 탐지 패턴 생성 · 검증 · 최적화 • (모니터링) IT 자원 및 보안 시스템 실시간 모니터링 (방화벽, IPS/IDS, WAF, Anti-DDoS, Anti-Web shell 등) • (분석) 공격 이벤트 초동 분석, 공격 이벤트 심화 분석(재현 분석, 영향도 분석) • (대응) 침해 원인 분석, 침해사고 복구 지원, 침해사고 재발방지 대책 수립
보안장비 구축 · 운영 (임대 포함)	• SIEM 구축 · 임대 · 운영 · 유지보수 • 다양한 벤더의 보안 장비 구축 · 임대 · 운영 · 유지보수 • 보안장비 상태, 성능 등 리소스 모니터링 • 보안장비 정기 점검 · 패치 · 패턴 업데이트 및 장애 지원 • 보안장비 정책 최적화 및 유효성 검증 • 보안 이벤트(로그) 관리 및 백업
품질관리	• NIST의 SOC-CMM 기반 품질점검 • 품질점검 기반 보안관제 매뉴얼 및 프로세스 개선 • ISO27001 인증 심사원 등 품질관리 전담 조직 운영, 현장 방문 품질점검 및 개선활동
보고서	• 일별/주별/월별 보안관제 정기보고서 • 동향분석, 탐지이벤트 분석, 침해사고 분석 등 비정기 보고서

SOC
부가서비스

보안관제 서비스 외에 취약점 점검 · 시나리오 기반 모의해킹 · 사이버 위협 대응 모의훈련 등 다양한 사이버 위협 대응 예방활동을 강화하여 고객의 정보자산을 안전하게 지켜드립니다.

Cyber Threat Intelligence

취약점
진단 서비스

모의훈련 서비스

침해사고 분석

보안관제 컨설팅

SOC
보안관제 특장점

엔드포인트부터 네트워크, 클라우드 관제까지 고객의 IT 자원 및 보안 시스템을 24시간 모니터링 및 분석하여 안전하게 지켜드립니다.
빅데이터, AI 기반 통합보안관제 시스템으로 고객군에 특화된 원격 및 파견 관제 서비스를 제공하며, **보안관제뿐만 아니라 취약점 진단, 보안장비 임대 및 위탁 운용 등** 통합보안관제서비스를 제공합니다.

빅데이터·인공지능 기반
통합보안관제시스템

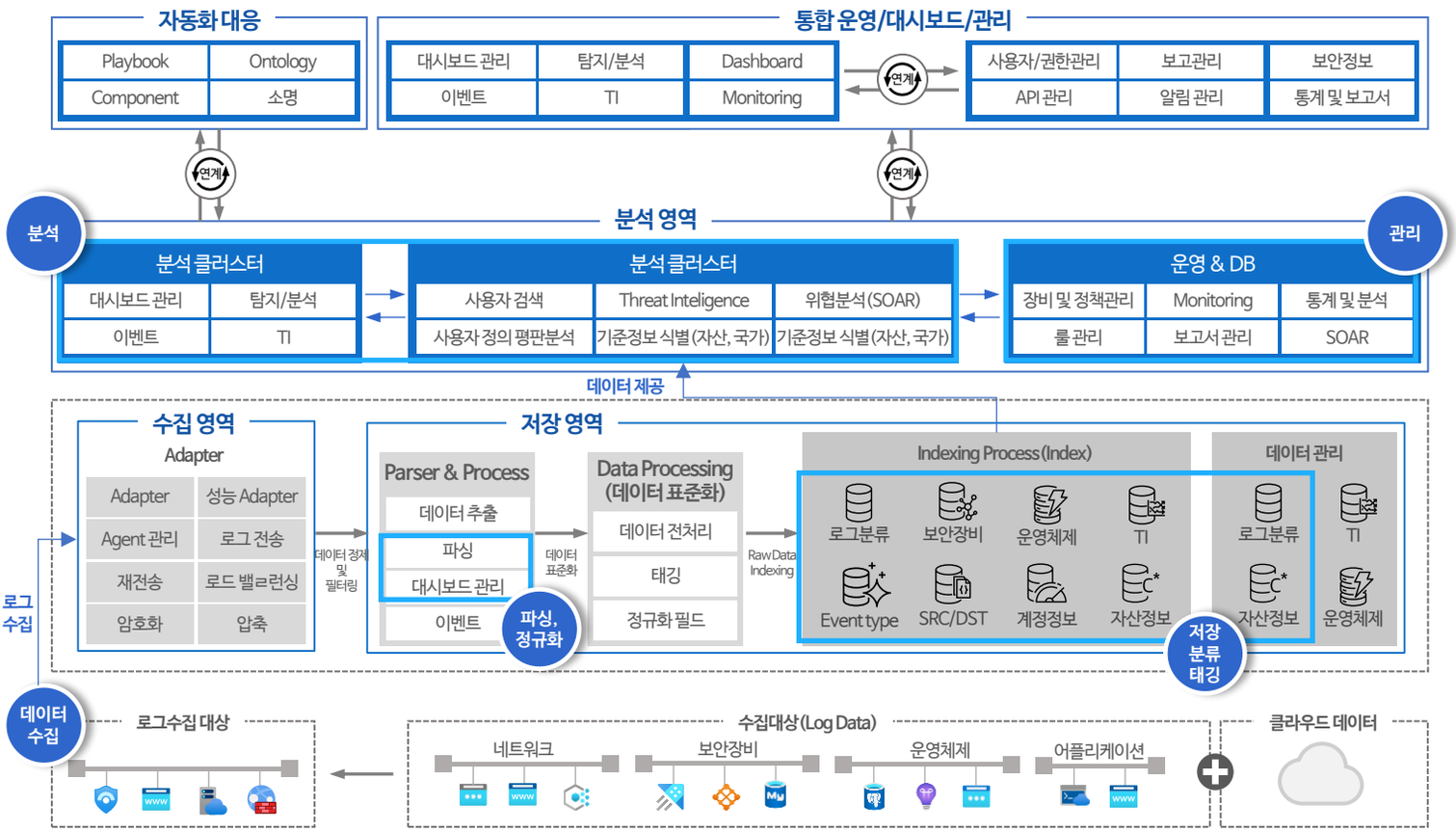
게임, 결제, 공공 등
높은 수준 보안 요구 만족

AWS, NHN 등
클라우드 보안관제

SOAR
Security Orchestration, Automation and Response
SOAR, 피할 수 없는 길! 지능적 자동화로 대응한다.

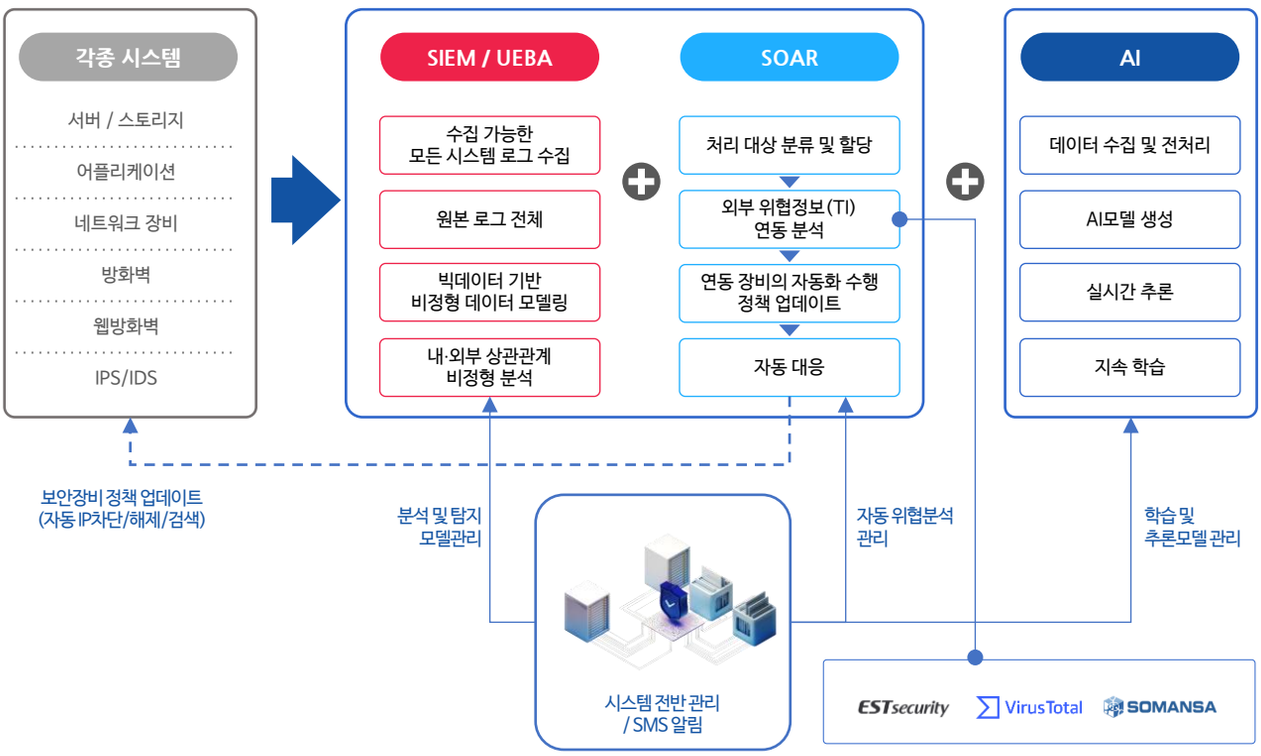
2015년 가트너에서 처음 사용한 용어로 SOAR를 통해 사람(People), 기술(Technology) 그리고 프로세스(Process)를 조율하고 자동화함으로써 조직에서 사고 대응 효율성과 일관성을 개선할 수 있도록 도와주기 때문에 다양한 사이버 위협에 대해, 대응 수준을 자동(Automation) 으로 분류함으로서 보안 팀은 사이버 공격 및 사고에 대한 조직의 대응을 표준화하고 간소화할 수 있습니다.

SOAR 아키텍처



SOAR
오케스트레이션

보안 오케스트레이션은 작업을 중앙 집중화하고 전파할 수 있도록 서로 다른 보안 도구를 상호 연결하는 수단입니다. 이를 통해 보안 팀은 프로세스를 간소화하고 사고 대응 프로세스를 가속화할 수 있습니다. SOAR은 SOC 프로세스를 표준화하여 일관된 조사와 대응을 보장하는 동시에 모든 경험 수준의 보안 분석가의 기술을 향상시킵니다.



SOAR
도입효과

SOAR은 효율성을 높여 SOC의 시간과 노력을 크게 절약하고, 사이버 보안 팀이 사람의 개입을 줄여 보안 운영을 간소화할 수 있도록 지원합니다.덕분에, 분석가들은 인간의 창의성과 직관을 필요로 하는 긴급한 문제에 집중할 수 있게 됩니다. 기타 이점은 다음과 같습니다.

더 짧은 시간에 더 많은 경고 처리

SOC는 매일 수백 또는 수천 개의 보안 경고를 처리해야 할 수 있습니다. 이러한 경고는 피로함으로 이어질 수 있으며 분석가는 이로 인해 위협 활동의 중요한 징후를 놓칠 수 있습니다. SOAR은 보안 데이터를 중앙 집중화하고, 이벤트를 강화하고, 대응을 자동화하여 경고를 보다 쉽게 관리할 수 있도록 합니다. 결과적으로 SOC는 응답 시간을 단축하면서 더 많은 경고를 처리할 수 있습니다.

보다 일관된 인시던트 대응 계획

SOC는 SOAR 플레이북을 사용하여 일반적인 위협에 대한 확장 가능한 표준 인시던트 대응 워크플로를 정의할 수 있습니다. 보안 분석가는 사례별로 위협을 처리하는 대신 효과적인 문제 해결을 위한 적절한 플레이북을 트리거할 수 있습니

향상된 SOC 의사 결정

SOC는 SOAR 대시보드를 사용하여 네트워크와 직면한 위협에 대한 인사이트를 얻을 수 있습니다. 이 정보는 SOC가 오탐을 찾아내고, 경고의 우선순위를 더 잘 지정하고, 올바른 대응 프로세스를 선택하는 데 도움이 될 수 있습니다.

SOC 협업 개선

SOAR는 보안 데이터와 인시던트 대응 프로세스를 중앙 집중화하여 분석가가 함께 조사를 수행할 수 있도록 합니다. 또한 SOAR를 통해 SOC는 HR, 법률 및 법 집행 기관과 같은 외부 당사자와 보안 메트릭을 공유할 수 있습니다.

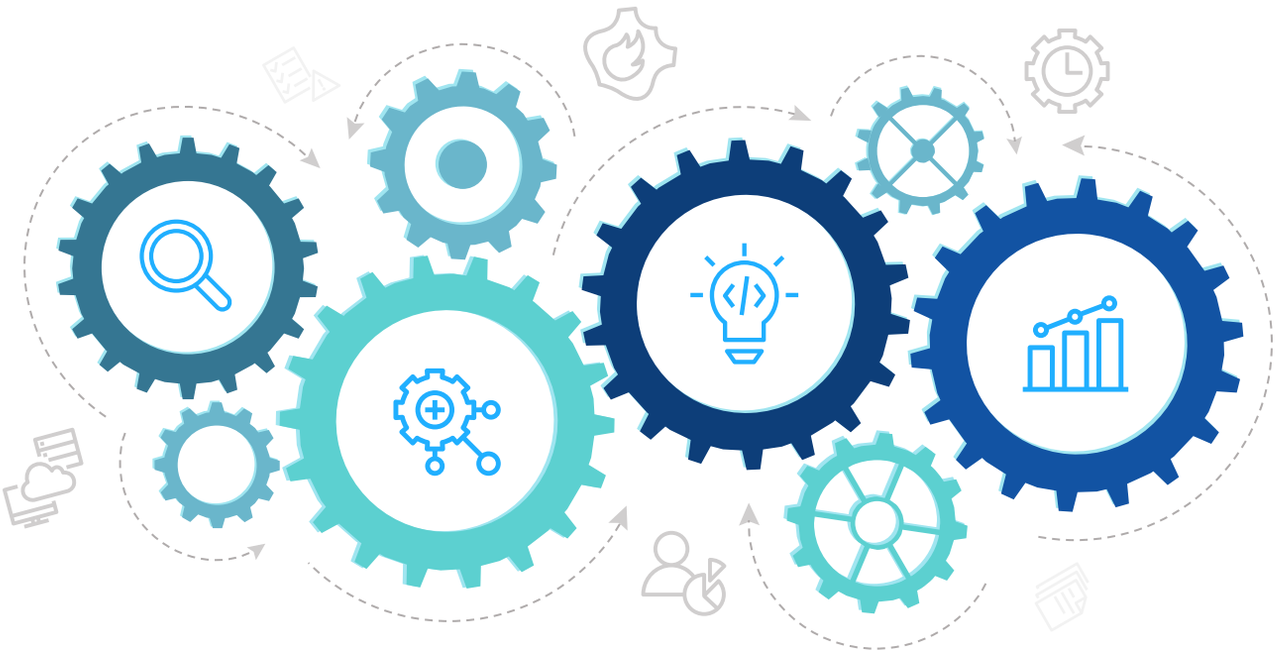
SOAR
지원사

SecuLayer	LOGPRESSO	AhnLab	splunk>
시큐레이어	이글루시큐리티	안랩	스플렁크

IMS

Integration Maintenance Service

비용은 줄이고 운영 효율은 높이는 최고의 선택



다양한 전산장비와 시스템환경에 대하여 각 Vendor사와 서비스 Partner 계약을 체결하고 자체 전문인력 및 협력사를 통한 체계적인 통합 유지보수 서비스로 시스템 성능관리, 장애관리, 네트워크관리, 데이터 백업관리, 소프트웨어 버전관리 등을 통해 급변하는 IT환경 변화에 유연하게 대처함으로써 고객사 전산시스템의 효율적인 운영과 가용성 보장이 가능하여 고객사의 안정적이고 효율적인 시스템 운영을 지원합니다.

IMS
유지보수 정책

IT 통합유지보수는 IT 인프라의 구성 관리, 성능관리, 장애관리, 보안관리, 운영보고 및 모니터링 등 통합유지보수를 위한 A to Z의 One-Stop 관리를 지향하고 있습니다.

긴급유지보수	예방정비	고정장비	고객센터 운영
비상시 신속한 장애처리를 위한 비상연락망을 구축하고 원격 및 현장대응	무고장/무수리 원칙을 준수하기 위해 월 1회 통신장비 및 운영상태의 정기적인 점검을 실시	장애 발생시 해당하는 시스템으로부터 분리하여 전체적인 운용에 미치는 영향을 최소화한 후 복구작업을 실시	체계적인 장애접수는 차후 유지보수관리의 편리성 추구

IMS
특장점

통합 유지보수는 다양한 IT 장비와 업무관리를 위한 유지보수 서비스를 단일창구로 통합한 서비스입니다. IT 인프라의 구성, 변경, 성능, 장애, 보안 등을 관리하여 시스템이 안정적으로 운영되도록 지원합니다.

1. 기술 지원 및 지속적 모니터링

오류 및 이슈 로깅	시스템에서 발생하는 오류 및 이슈를 지속적으로 로깅하고 모니터링합니다. 로그 데이터를 분석하여 문제의 근본 원인을 식별하고 조치를 취하여 시스템 안정성을 유지합니다.
보안 모니터링	지속적인 보안 모니터링은 잠재적인 보안 위협을 감지하고 방지하기 위해 필수적입니다. 로그 및 이벤트 데이터를 모니터링하고 이상 징후를 조기에 식별하여 보안 조치를 취합니다. 새로운 보안 업데이트 및 취약점에 대한 대응도 지속적으로 검토합니다.
24x365 상시 지원	24x365 무중단 운영서비스 지원

2. 시스템 효율성 향상

시스템 효율성 측면

- IT 운영 시스템 **성능 최적화**
- IT 운영 시스템 **성능 고도화**
- IT 운영 시스템 **안정화**
- 고객사 만족도 및 **성능 최적화**

3. 비용절감

자원 중복 제고	여러 시스템이나 서비스 간의 기능 중복이 발생하는 경우, 중복된 사항들을 제거하고 단일화된 솔루션을 도입함으로써 관리 및 유지보수 비용을 절감할 수 있습니다.
라이선스 통합	통합된 시스템을 사용함에 따라 라이선스 및 계약 관리가 효율적으로 이루어질 수 있으며, 이를 통해 비용을 절감 할 수 있습니다.
프로세스 표준화	통합된 시스템을 통해 표준화된 프로세스와 일관성 있는 환경을 구축함으로써 관리 및 유지보수 비용을 절감할 수 있습니다.
자동화 및 스크립트	반복적인 작업들을 자동화하고 스크립트를 활용함으로써 인력 비용을 절감할 수 있으며, 자동화된 프로세스는 더 신속하게 실행되어 휴먼에러를 줄일 수 있습니다.

Webshell

a program or script for controlling a device through commands

웹쉘을 이용한 공격 패러다임 변화 및 대응전략

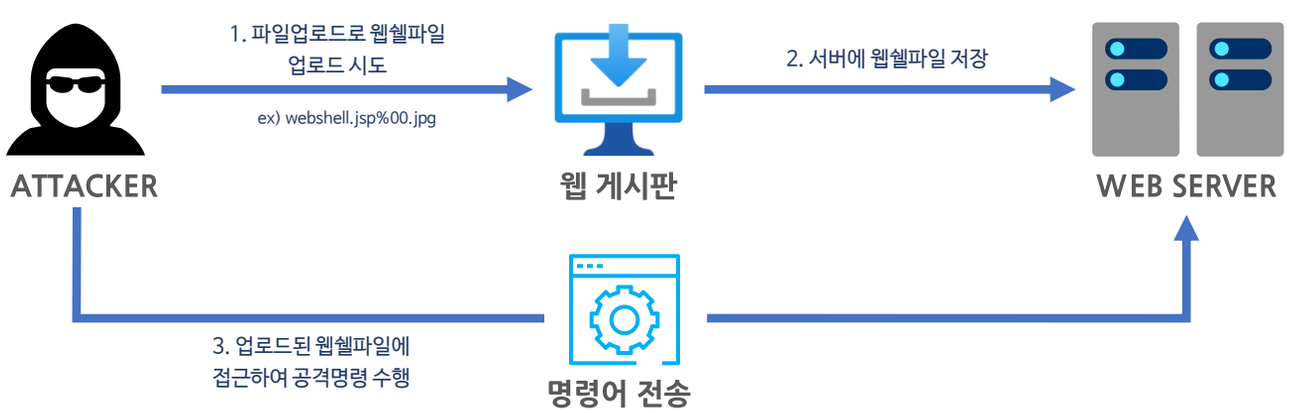
웹쉘은 웹 서비스를 구동하기 위한 웹서버 환경에서 지원 가능한 웹 애플리케이션 언어를 기반으로 동작되는 파일을 의미하여, PHP, JSP, ASP, ASP.NET 과 같은 확장자 파일을 이용해 정상 비정상적인 접근 경로로 접근하여 서버 정보 및 권한을 탈취하는 기능을 수행하게 됩니다.웹쉘은 주로 외부망에 있는 공격자가 시스템 내부에 명령 수행을 하기 위한 목적으로 사용되기 때문에 시스템 명령을 사용할 수 있는 함수를 포함하고 있거나, 업로드된 웹쉘 파일을 숨기거나 기능 분석을 저해하기 위한 목적으로 암호화나 압축을 수행하게 됩니다.

구분	함수 종류
시스템 명령어	system, passthru, shell_exec, exec, popen, proc_open
암호화 및 압축	eval, assert, call_user_func,base64_decode, gzinflate, gzuncompress, gzdecode, str_rot13
파일 생성 또는 내용 포함 함수	require, require_once, include, include_once, file_get_contents, file_put_contents, fputs, fwrite

대표적인 웹쉘 사용 함수 목록

Webshell
웹쉘 유입경로

웹쉘은 시스템 제어 및 장악을 통한 시스템 가용성 저해나 데이터 탈취 등을 목적으로 하고 있기 때문에 단발적인 공격으로 그치지 않고 다수 접속하여 시스템을 제어하는 데 사용됩니다.



Webshell
공격대응 방안

웹쉘 공격에 대한 대응은 예방, 감지, 대응 세 가지 단계로 나뉩니다.

예방

웹 애플리케이션 및 웹 서버의 보안을 강화하여 공격을 예방합니다. 이는 취약점을 패치하고 , 파일 업로드 및 다운로드 기능에 대한 보안을 강화하며, 웹 애플리케이션 방화벽(WAF) 등의 보안도구를 사용함으로써 이루어집니다.

감지

서버 로그를 정기적으로 분석하거나 IDS(Intrustion Detection System) 같은 시스템을 이용해 웹쉘 공격을 감지합니다. 또한, 파일 무결성 체크 등을 통해 변경된 파일을 감지할 수 있습니다.

대응

웹쉘 공격이 발견되면 즉시 대응해야 합니다. 웹쉘 코드를 제거하고, 시스템을 복구하며, 취약점을 패치하는 등의 대응이 필요합니다. 또한, 공격의 원인과 경로를 분석하여 재발 방지 대책을 마련해야 합니다.

Webshell
탐지솔루션 핵심 기능

웹서버의 안전한 운영을 위해서는 웹셸 탐지 및 방어 솔루션이 필수적입니다. 이러한 웹쉘 탐지 솔루션은 기존 웹방화벽 도입 이전에 유입됐거나 웹방화벽을 우회해서 들어온 웹셸의 탐지와 차단, 웹셸의 실행 방지 등의 기능외 아래의 기능요건을 충족하는지 검토해 보아야 합니다.

구분	상세 내용
행위 기반 실시간 웹쉘 탐지	웹 서버 내에서 발생하는 각종 데이터를 실시간으로 분석하여 웹쉘 행위를 실시간으로 판단
알려지지 않은 웹쉘 탐지	웹쉘 파일 수정(함수 명, 인자 값 등), 패킷 암호화, SSL 적용 환경 등에서 탐지하기 어려운 새로운 웹쉘 탐지 가능
웹쉘 의심 행위 정보 및 이력 관리	웹쉘이 탐지된 서버, 시간, 실행한 명령어, 웹쉘 경로, 공격자 IP 등 정보 제공 제공받은 정보를 참고하여 세밀한 대응 전략 수립 가능 대응 방법 등 관련 정보 및 이력 관리 가능
파일 격리/복구	웹쉘 의심 파일을 격리하거나 복구 가능
웹쉘 의심 파일 목록 제공	웹쉘 의심 파일 목록을 제공하여 웹쉘 행위 탐지 시 신속한 대응 가능 웹쉘 의심 파일 관련 생성 시간, 파일 권한, 소유자, 그룹, 파일 경로, 사이즈 등 부가 정보 제공
공격자 의심 IP 목록 제공	공격자가 시도한 행위 분석 및 IP 차단 등의 조치에 참고할 수 있는 의심 IP 및 국가 정보 제공
다양한 OS환경 제공	Linux, Windows, Ubuntu, Oracle Linux, Red Hat 등 다양한 환경의 웹서버 OS환경을 지원

Webshell
지원사

S³I [주] 에스큐브아이

에스큐브아이

기술문의 02-413-2280 | sales@epsis.co.kr | 서울 송파구 송파대로 201 테라타워2 A동 1008호

기술문의를 하시면 고객사 별 담당 엔지니어 및 영업지원을 배정하여 안내해 드립니다.

EMPHASIS INFORMATION TECHNOLOGY

파트너/고객사
Partner & Customers

엠퍼시스와 함께한 고객사 및 파트너

파트너/고객사
파트너사

제조사

SECUI | AXGATE Security and Beyond | KX NexG | paloalto NETWORKS | FORTINET
WEDS | NEWDAYSOFT | PIOLINK | KTNF KOREA TECHNOLOGY AND FUTURE | SOMANSA
SecuLayer | LOGPRESSO | GeniNet | NetMan | SECU LETTER
OKESTRO | Penta SECURITY | wizbase | IZEX | ZERONSOFT N
ESTsecurity | CUBE THE MOMENT (주)큐브더모먼트 | SGN | Progress | VMSolution
SANDS Lab | SNAPTAG | CISCO | JUNIPER NETWORKS | Sparrow
HANSSAK | sga | BANDI SNC SYSTEM & CLOUD INNOVATION | WINS | KSIGN
S3I [주]에스큐브아이 System, Security, Service & Integration | Ahranta, Inc. | INITECH | Skyhigh Security | SecuWiz

총판사

DB Inc. | SysOne | uniPoint | ETEVERS | 대신정보통신(주)
SCIENS | 에스원 | SK networks | SK쉴더스 | LG CNS

파트너사

SECUWIN Security Winner | NANUMUNITECH (주)나눔유니텍 | Sanbit | bellock | Vinetech
T&DSOFT Think&Do | FXCONSULTING | 롯데정보통신 | KYOBO 교보정보통신 | SPHERES
i-Cloud | AEGISECU Easy ISMS Companion | CUDO COMMUNICATION | SD secuDAim | HYUNDAI AutoEver
CJ OLIVENETWORKS | Metanet Tplatform | SEJONG NETWORKS | FINEVT | QUARRY SYSTEMS

파트너/고객사
고객사

공공기관

한국도로공사 | 한국환경공단 Korea Environment Corporation | KARI 한국항공우주연구원 | 한국교육개발원 KOREAN EDUCATIONAL DEVELOPMENT INSTITUTE
인천광역시 Incheon Metropolitan City | 김포시 | Yangju | PAJU | 연천군
서초 SEOCHO | 은평구 Eunpyeong | 가평군 GAPYEONG | Incheon Airport 인천국제공항공사 | 천안도시공사 CHEONAN URBAN CORPORATION
KIPHRD 한국발전인재개발원 | 식품안전정보원 NATIONAL FOOD SAFETY INFORMATION SERVICE | 국립암센터 NATIONAL CANCER CENTER | 경기도환경교육센터 Gyeonggi-Do Environmental Education Center | 초록우산 어린이재단
ktl 한국산업기술시험원 Korea Testing Laboratory | 성남문화재단 | 화재보험협회 | KITECH 한국생산기술연구원 | GKL Grand Korea Leisure

금융기관

SGI서울보증계열 SGI신용정보 | KB신용정보 | KB손해사정 | 미래신용정보 | AIG 손해보험
KakaoPay | pay 손해보험 | MIRAE ASSET 미래에셋캐피탈 | MIRAE ASSET 미래에셋생명 | NH농협손해보험
금융결제원 | 신한EZ손해보험 | 한국성장금융 K-Growth | NICE페이먼츠 | KORE ASSET 코리아에셋투자증권
KVIC 한국벤처투자 | 광주은행nk | 우리금융캐피탈 | 현대하이카손해사정(주) | KYOBO 교보자산신탁
한국증권금융 Korea Securities Finance Corp. | 한국금융솔루션 | toss | IBK기업은행 금융그룹 IBK투자증권 | 한국은행

일반기업

GS칼텍스 | GS에코메탈 | GS EPS | GS에너지 | GS바이오
GS칼텍스 예울마루 | HYUNDAI MOTOR GROUP | HYUNDAI MOBIS | 해양에너지 | Huvitz
kakao | KG 모빌리언스 | DAELIM | EUGENE 유진기업 | EUGENE 유진IT서비스
kakaomobility | Hanbitco | ㈜엔지켐생명과학 ENZYCHEM LIFESCIENCES | HYUNDAI 현대이지웰 | TOYO ENGINEERING
Metanet Mplatform | 주식회사 오뚜기 | PAGODA | ID HOSPITAL 아이디병원 | BGF리테일
Daewon 대원제약 | 고려대학교 KOREA UNIVERSITY | 롯데렌탈 | OKmall | 동서식품주식회사
Dongwon 동원엔터프라이즈 | MetaM | NICE정보통신 | SHINSEGAE CHOSUN HOTEL | TP
quantec | 프론티어 | SK디스커버리 | 면사랑 | UBcare | SJ 상지해운주식회사

(주)엠퍼시스정보기술

EMPHASIS INFORMATION TECHNOLOGY

서울시 송파구 송파대로 201 테라타워2 A동 1008호

02-413-2280 sales@epsis.co.kr www.epsis.co.kr