CUDO COMMUNICATION

Cybersecurity Solutions

통합 보안 솔루션 제공

- 클라우드 보안 솔루션
- 디지털전환 보안 솔루션

회사 소개 및 인력 구성

회사 소개

CUDO COMMUNICATION

=

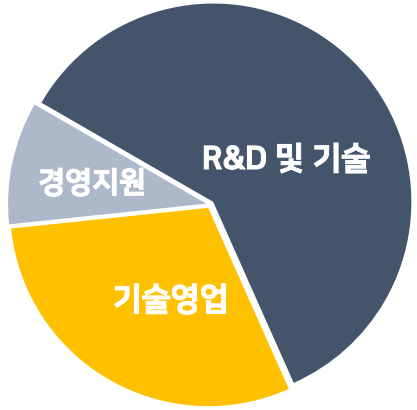
COULD + DO

우리는 많은 것을 해냈고
이를 바탕으로 더 크게 발전할 것입니다.

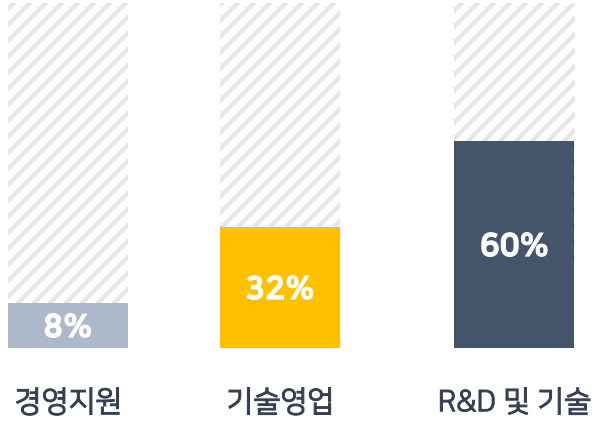
회 사 명	쿠도커뮤니케이션㈜
대표이사	김용식
회사주소	본사_ 서울시 서초구 효령로 171, 용상빌딩 302호 방배사무실_ 서울시 서초구 효령로 34길 4, 프린스효령빌딩 4층, 5층 서울시 서초구 방배로 84, 유성빌딩 4층 서울시 서초구 방배로 18길 5, BH빌딩 7층, 8층 공장_ 경기도 의왕시 성고개로 53 에이스청계타워 401,402,414호
설 립 일	2000년 10월 25일
홈페이지	www.cudo.co.kr
사 업 부	글로벌사업부, 솔루션사업부, 더미디어사업부, 시큐리티사업부, 정보보안사업부, LED사업부
자 본 금	23.7억원 (2022년)
매출규모	962억원 (2022년)
임직원 수	약 240명 (2023년 현재)
신용평가	A- (2023년 평가기준)
인증현황	이노비즈기술신형기업, 가족친화인증기업, 청년친화강소기업, 소프트웨어사업자, 정보통신공사업, 옥외광고사업, 직접생산증명서(영상감시장치 등), Q마크, K마크, GS인증, 우수제품지정증서 G-PASS인증, ISO9001
수상경력	2005.11 300만불 수출의 탑 (한국무역협회) 2006.11 500만불 수출의 탑 (한국무역협회) 2008.07 벤처대상(제조/서비스 부문)[지식경제부장관] 2008.11 1,000만불 수출의 탑 (한국무역협회) 2012.05 표창장(IPTV활성화공로)[방송통신위원회위원장] 2015.12 표창장(국내위성산업발전기여) [미래창조과학부장관] 2016.05 대통령 표창장 2022.05 대통령 산업포장

인력 구성

R&D 등 기술인력 중심의
Man Power



인력 비율



회사 연혁

2000년
10월 회사설립

2001년
11월 100만불 수출의 탑 수상

2002년
8월 기업부설연구소 설립

2003년
6월 위성DMB Uplink 시스템 구축

2004년
1월 벤처기업등록

2005년
11월 300만불 수출의 탑 수상

2006년
7월 기숙혁신형 중소기업 (INNO-BIZ) 선정

11월 500만불 수출의 탑 수상

2008년
1월 TL9000 인증

2월 Software AG와 웹메소드솔루션 총판 계약

7월 매경우수벤처기업대상 대상 수상

11월 1,000만불 수출의 탑 수상

2009년
7월 디지털 방송 개발과제 수행 (KEIT)

2010년
5월 특허등록"범용메모리장치 및 데이터 처리방법

10월 G20 정상회담 지능형 CCTV 구축

2012년
5월 방송통신위원장 표창

11월 GS인증

2013년
6월 Q마크/K마크 등록

8월 지능형 CCTV 우수제품지정(조달청)

2014년
5월 진주지청, 울산지검의 지능형 CCTV 구축

6월 김포시 통합관제 지능형 CCTV 구축

2015년
8월 한강교량 영상감시 출동 시스템 구축

10월 삼성SDS Value Added Reseller 계약 체결

11월 해외조달시장 진출기업 G-PASS 기업 지정

2016년
5월 대통령상 표창

6월 Palo Alto Networks 총판 체결

2017년
3월 INFINIFLUX 총판 체결

4월 Forescout 총판 체결

6월 지능형영상분석 마케팅 협약 체결(한화테크윈)

9월 WSCW 스마트 공공서비스 최우수상 수상

2018년
2월 덕성가족기업 인증

4월 파이어몬 총판 체결

4월 평창올림픽 CCTV 보안관제센터 구축

11월 Kaspersky 총판 체결

11월 가족친화인증기업 선정

2019년
1월 특허등록"객체이미지인식기반 CCTV영상분석장치 "

1월 특허등록"궤적서비스제공장치 및 구동방법 "

2월 상표등록"컴퓨터 프로그래밍 외9건 "

3월 특허등록"궤적서비스제공장치 및 데이터 구축방법 "

8월 조달청 우수제품지정

9월 특허등록"실시간 IPTV 발송 채널전환 시스템"

2020년
6월 부천/화성/양주시 AI 선별관제 시스템

8월 상표등록 "미국,중국,일본 3개국"

8월 금천구 2020 CCTV관제 시스템 구축

9월 IBK 베스트 파트너 선정

12월 '정보통신기술부문' 매경미디어그룹 회장상 수상

2021년
1월 특허등록"멀티 LED유닛 설치장치"

1월 특허등록"무중단 병렬전원 전광판 및 그 전광판의 구동방법"

1월 특허등록"높이조절식 LED 디스플레이장치"

3월 Claroty 총판 체결

3월 K쇼핑 녹화 스튜디오 국내 최대 커브형 LED미디어월 구축

10월 특허등록"LED 전광판 및 그 전광판의 구동방법"

11월 과천사옥 신축공사 착공식

11월 항포구 고성능 CCTV 구축사업 단일 사업최대규모 235억 수주

2022년
5월 대통령 산업포장 수상

7월 구로구 우수기부자 구로구청장 표창 수상

11월 SMTechnology 구독형 총판 체결

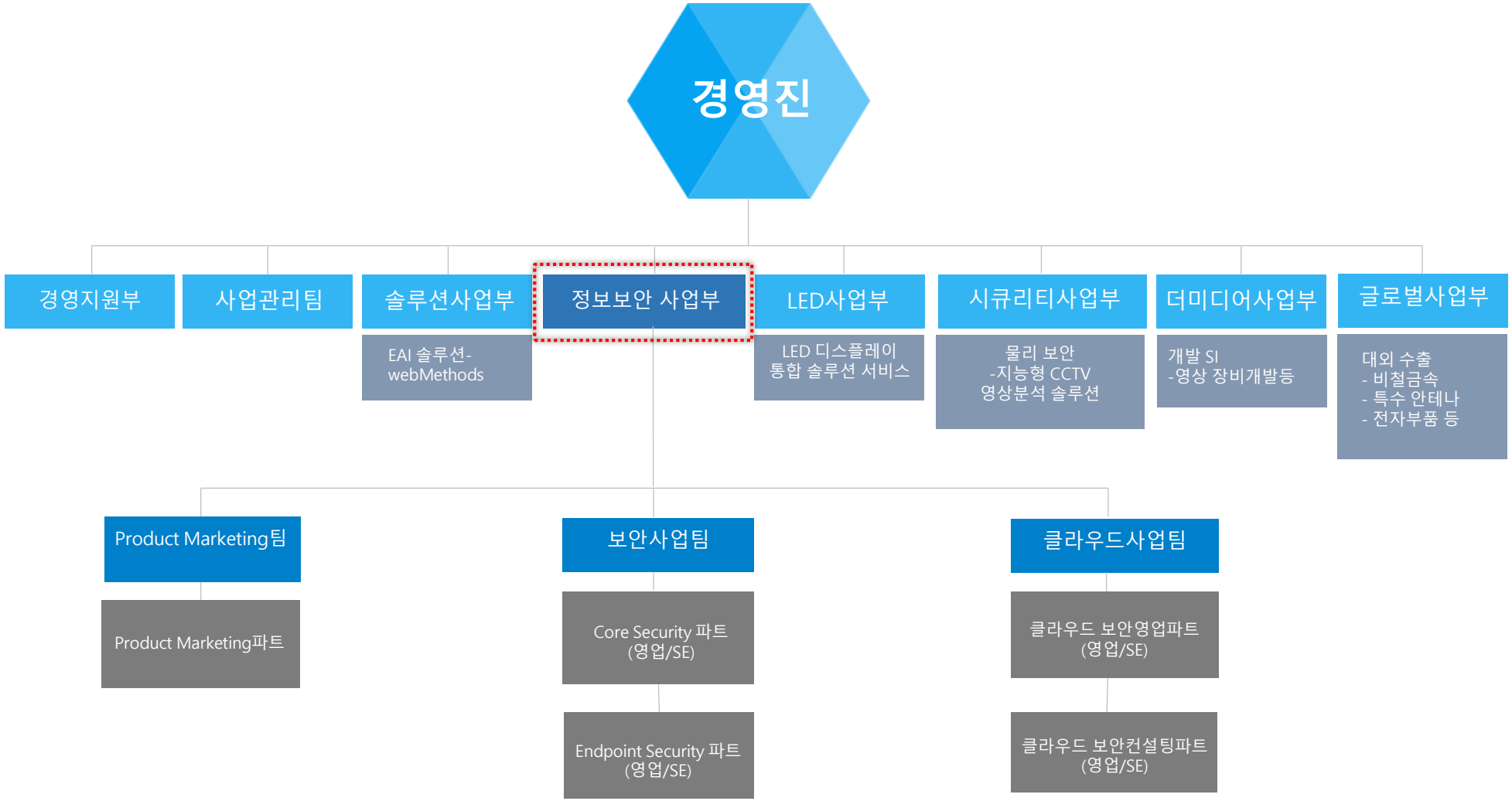
12월 AWS 보안 협의체 선정, Major 등급 보유

2023년
4월 SECUI 총판 체결

5월 Astron 총판 체결

5월 AWS MSA 파트너 체결

조직도


경영진
경영지원부
사업관리팀
솔루션사업부
EAI 솔루션-
webMethods
정보보안 사업부
LED사업부
LED 디스플레이
통합 솔루션 서비스
시큐리티사업부
물리 보안
-지능형 CCTV
영상분석 솔루션
더미디어사업부
개발 SI
-영상 장비개발등
글로벌사업부
대외 수출
- 비철금속
- 특수 안테나
- 전자부품 등
Product Marketing팀
Product Marketing파트
보안사업팀
Core Security 파트
(영업/SE)
Endpoint Security 파트
(영업/SE)
클라우드사업팀
클라우드 보안영업파트
(영업/SE)
클라우드 보안컨설팅파트
(영업/SE)

사이버 보안, 사물 인터넷 보안, 클라우드 보안 컨설팅 영역까지 …

“ Total Security Solution Company ”

쿠도커뮤니케이션㈜ 정보보안사업부는

네트워크 보안 및 엔드포인트 보안과 클라우드 보안 컨설팅까지 **고객 맞춤형으로 설계된 종합 보안 컨설팅 및 서비스를 제공**합니다

디지털 전환 & 클라우드 보안 솔루션

CUDO COMMUNICATION
We COULD Secure, You DO Safer.

SECUI

11년 연속 국내 네트워크 보안 시장 점유율 1위

- 통합네트워크 보안 제품
- 정보보호 컨설팅 서비스
- AI 기반 보안관제 서비스

kaspersky

글로벌 4대 통합 엔드 포인트 보안 솔루션

- 엔드 포인트 보안
- EDR/Sandbox
- 클라우드 보안
- OT 보안 (KICS)

FORESCOUT

글로벌 1위 네트워크 접근제어(NAC)

- 클라우드 환경 지원
- OT & IoT 기반 통제
- 글로벌 제조사 연동을 통한 제로 트러스트 구현

aws

클라우드 보안 컨설팅 'All in ONE' 서비스

- 클라우드 ECSA / ISMS-P 인증심사 컨설팅
- 보안 제품(3rd Party) 제안
- 클라우드 및 인프라 고도화
- 컨테이너 보안 컨설팅

ASTRON SECURITY

클라우드 ISMS 인증 관리 솔루션

- 클라우드 ISMS 인증 지원
- CSPM(클라우드 보안형상관리)
- 클라우드 컴플라이언스 관리

CUDO CLONE PARTENRSHIP 이란 ?

디지털 전환이 가속화 됨에 따라 고객의 IT 인프라 환경은 고도화되고, 고객 보안 자산은 기업 내부망을 넘어 클라우드 환경까지 지속적으로 확장되고 복잡해졌습니다
쿠도커뮤니케이션은 **보안 전문 컨설팅 회사**로서의 오랜 경험과 기술력을 바탕으로 파트너 및 고객사 여러분의 **분신(CLONE)**이 되어 비즈니스 환경에 완벽한 보안 기능과 서비스를 제공하겠습니다

소개 및 주요 서비스

국내 시장 점유율 1위, SECUI

11년 연속 국내 네트워크 보안 시장 점유율 1 위에 빛나는 시큐아이는 업계 최고의 기술력과 전문 인력을 기반으로 보안 솔루션을 개발, 네트워크 · 가상화 · 엔드 포인트 등 보안 전 분야에 걸쳐 차별화된 제품 및 서비스를 제공합니다.

해외 시장
51개국

누적 판매
134,000대

1위

국내 네트워크 보안 11년 연속 1위
11 years
Frost & Sullivan기준

방화벽 국내 점유율
54.1%
나라장터 국가종합전자조달 기준

Network

통합 네트워크 보안 제품

· 네트워크 보안 솔루션 분야 최고 품질의 제품

BLUEMAX NGF
BLUEMAX IPS
BLUEMAX WIPS
BLUEMAX TAMS
BLUEMAX CLIENT
SECUI MF2 SECUI MFI SECUI MFD

Consulting

정보보호 컨설팅 서비스

· 풍부한 경험을 가진 컨설팅 전문가의 고객 지향 정보보호 서비스

AI

AI 기반 보안 관제 서비스

· 최신 보안 위협을 고려한 다양한 환경에 대해 보안 관제 서비스 설계, 구축

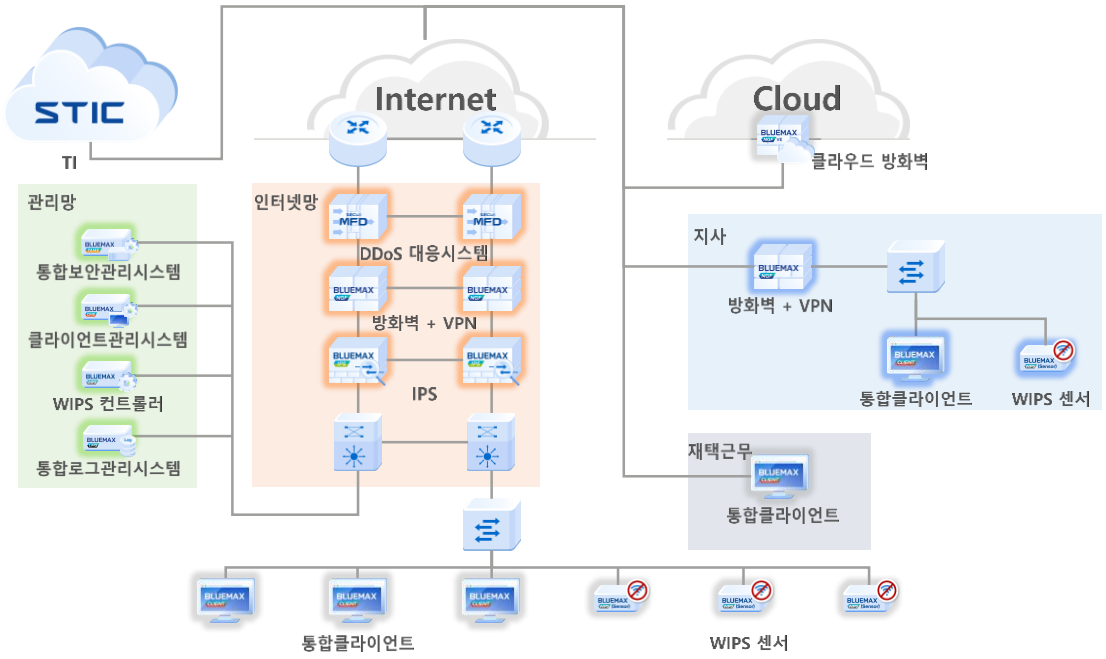
제품군

22년 의 보안 노하우와 기술력이 응집된 글로벌 수준의 시큐아이 보안 솔루션

네트워크 보안 솔루션 분야 최고 품질의 제품을 개발, 생산하고 있습니다. 유무선 IT 인프라 환경의 모든 위협 요소를 탐지 차단하는 통합 보안 플랫폼을 제공합니다

전 보안 영역에 걸친 차세대 보안 솔루션으로 보안의 새로운 패러다임 제시

국내 최초 차세대 방화벽을 시작으로, 차세대 침입 방지 시스템, 무선 침입 방지시스템을 넘어 클라우드 환경에서도 고객의 자산을 안전하게 지키고 있습니다



방화벽	BLUEMAX NGF BLUEMAX NGF VE SECUI MF2	국내 네트워크 보안을 위한 차세대 방화벽 국내 가상 환경을 위한 차세대 방화벽
IPS	BLUEMAX IPS SECUI MFI	최신 보안 위협에 능동적으로 대응하는 선제적 위협 대응 차세대 IPS
DDoS대응시스템	SECUI MFD	진화하는 DDoS 공격에 대응하는 고성능 Anti DDoS 시스템
통합보안관리	BLUEMAX TAMS	BLUEMAX 제품 통합 관리 시스템
단말보안/ 취약점점검	BLUEMAX CMS BLUEMAX CLIENT	통합 보안 취약점 진단 솔루션
무선침입방지시스템	BLUEMAX WIPS	차세대 지능형 무선 위협 대응 시스템
통합로그관리	BLUEMAX LMS	대용량 로그를 효율적으로 관리 · 분석하는 빅데이터 기반 통합 로그 플랫폼

소개

Kaspersky Lab

전 세계 사용자
4억 명 이상

전체 직원 중 30% 이상
R&D 전문가

글로벌성능평가
종합 1위

- 1997년 Chairman & CEO 유진 카스퍼스키에 의해 설립
- Kaspersky Lab 기술로 보호받는 사용자는 전 세계 4억 명 이상
- 직원 수 약 4,000 여명: 전체 직원 중 약 1/3이 R&D 전문가
- 전 세계에서 4번째로 큰 엔드 포인트 보안 벤더

포트폴리오

엔드포인트 보안

- 기계 학습을 통한 다계층 보호로 악성 코드 차단
- 글로벌 인텔리전스 네트워크 활용(KSN)
- 중앙 관리 및 엔드포인트 제어

EDR & KATA

- 네트워크 기반 지능형 위협 탐지
- 엔드포인트 레벨에서 위협 탐지 및 대응
- 위협 활동에 대한 가시성 확보

IoT & 임베디드 보안

- IoT 시스템 및 임베디드 디바이스 전용
- 저사양 하드웨어 지원
- 중앙 관리 및 매체 제어 가능

하이브리드 클라우드 보안

- 물리적 환경, 가상 환경 및 클라우드 환경을 모두 아우르는 차세대 보안
- 리소스 효율성이 우수한 하이브리드 클라우드 보안
- 통합 관리 및 운영

Industrial Cyber Security

- IoT 시스템 및 임베디드 디바이스 전용
- 저사양 하드웨어 지원
- 중앙 관리 및 매체 제어 가능

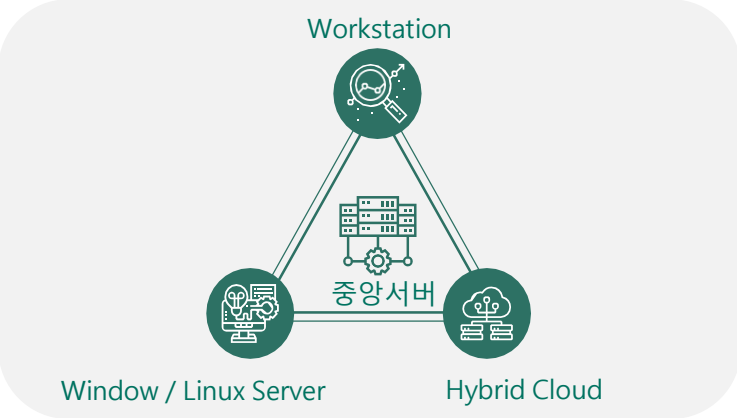
위협 인텔리전스 서비스

- 지능형 지속 공격 APT에 대한 대응 수단
- 가장 광범위한 범위의 우협 가시성 제공
- 사고 관리 전반에 걸쳐 풍부한 전후 맥락 제공

주요제품

Kaspersky Endpoint Security

다중화 된 보안 기능 및 엔드 포인트 제어를 통해 기업 네트워크를 안전하게 보호



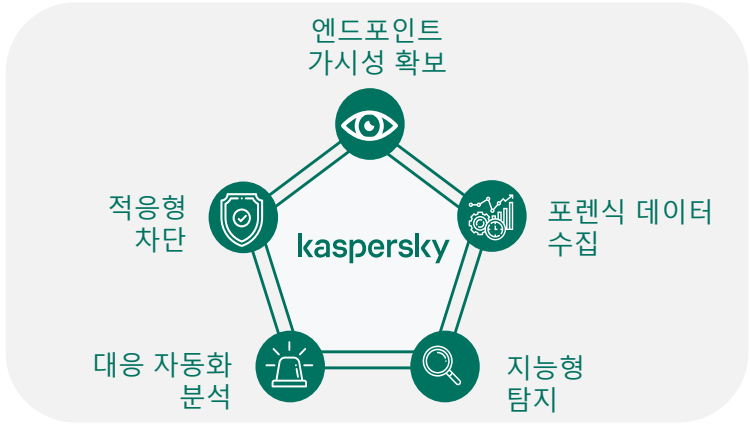
- 방대한 시그니처 및 휴리스틱, 평판기반을 통한 **다중화 된 보호**를 제공
- 기업 내 정보 보호 및 유출을 방지하기 위한 **웹, 매체, 애플리케이션 제어**를 제공
- 클라우드 기반의 Kaspersky Security Network(KSN) 을 통하여 **실시간**으로 보호
- 애플리케이션 권한 제어 및 시스템 감시기를 활용하여 기업 내 유입되는 **랜섬 웨어에 대한 보호 강화**

Kaspersky Endpoint Security 지원 운영체제

- Microsoft Windows Workstation / Server
- Linux 32bit / 64bit
- Macintosh
- Virtualization 환경 지원

Kaspersky Endpoint Detection and Response(EDR)

에이전트 기반 탐지 및 대응 솔루션

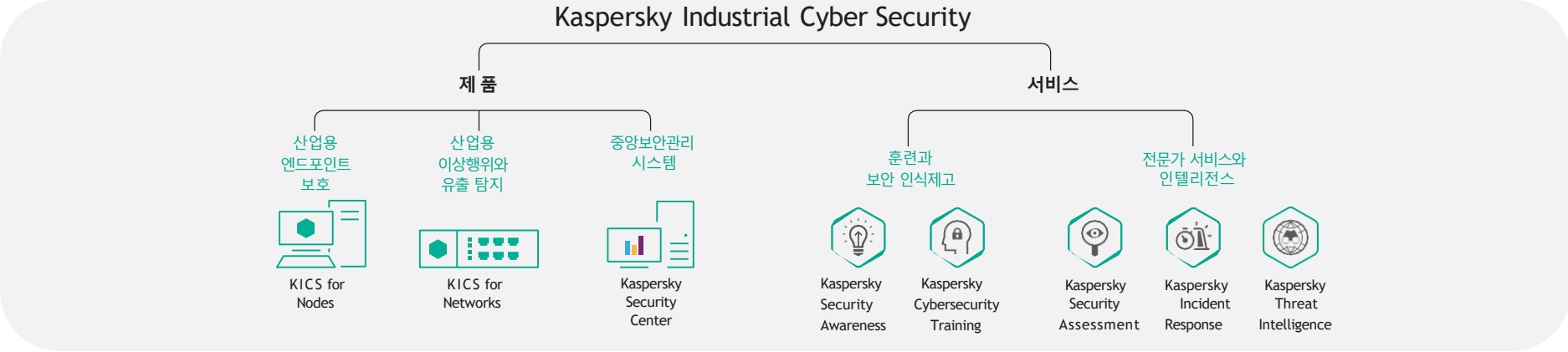


- 보안 사건 대응 업무를 **자동화**
- 엔드포인트 효율적 관리 확인
- **포렌식 기능**을 제공
- **가시성** : 중앙 집중식으로 모든 엔드 포인트의 이벤트 기록 및 조사
- 수작업을 자동화(위협 선별) 및 **보안 프로세스 통합 차단**
- 삭제, 중지, 파일 격리, 파일 실행 차단, 명령 실행, PC 격리
- **지능형 탐지 기능** (표적공격분석기 등)
- 위협 사냥 : 실시간으로 전체 네트워크에 대한 침입 증거 및 IoC(침해 지표) 사전 검색, 이벤트 검색

주요제품

Kaspersky Industrial Cyber Security

최고 수준의 IT·OT 보안 전문성 기반 통합 서비스 제공



Kaspersky Threat Intelligence

조직에 실시간 사이버 위협 정보를 제공하여 보안 전략 강화

- **즉각적인 위협 탐지**로 비즈니스 운영 중단 방지
- 보안 사건으로 인한 **금융 손실 가능성 최소화**
- 기업 대상 위협에 대한 시기 적절한 정보를 기반으로 최적의 인력을 구성하고 특정 기술에 대해 **비용 효율적인 투자 보장**
- 경쟁업체가 지적 재산 반출을 통해 **불공정한 경쟁 우위를 확보하지 못하도록 방지**
- **조정 가능한 선제적 방어 기능 구축** 지원

소개

FORESCOUT Platform & Module

FORESCOUT는 장치의 식별, 인증, 보안 정책 적용, 위협 탐지 및 대응 등을 효과적으로 수행하여 IT/IoT/ IoMT 환경의 고객 자산을 안전하게 보호합니다

자산탐지 및 통합 관리

내부 네트워크의 모든 단말을 탐지하고
자동 자산 분류

3rd party 및 통합 관리

고객만의 커스텀 에코시스템
구축지원

사용자 인증

인증 서버와 연동 또는 자체인증
DB를 통해 사용자 인증 제공

단일 장비 구성

단일 Appliance로 모든 보안정책 구현이 가능하고
Out-of-Band(미러링) 방식으로 기존 네트워크에
영향을 주지 않는 구성

접근 제어

사용자 및 분류에 따른 구간별 네트워크 접근제어

다양한 운영체제 지원

다양한 운영체제(Windows, Linux, Mac 등)에 대해
Agent / Agentless 방식으로 선택적 정책 운영 지원

제품군

eyeSight

네트워크에 연결된 단말 탐지 및
자산분류, 평가

eyeControl

eyeSight가 탐지해 분류한 단말
통제, 차단, 관리

eyeSegment

제로 트러스트 네트워크를 세분화
및 구현 가속화

eyeInspect

OT/ICS 장치를 지속적으로
검색, 분류, 모니터링

eyeExtend

단말 컴플라이언스 강화,
운영 생산성 향상

eyeExtend connect

사용자 지정 관리시스템과
Forescout 플랫폼의 커스텀 연동

eyeManage

다수의 Forescout 장비
중앙집중관리

eyeRecover

단일 또는 다중 사이트 배포에서
Forescout 서비스의 연속성 보장

주요 기능 | Network Access Control (eyeSight & eyeControl) – 통합 네트워크 접근 제어 시스템

- Network Access Control(NAC) 글로벌 1위 제품으로, Agentless/Agent 방식을 모두 지원하며 기업 네트워크의 모든 단말을 식별 및 분류하고 내부 네트워크를 보호합니다
- 최첨단 디바이스 식별 및 분류, 다중 차원의 접근 제어, 실시간 취약점 탐지 및 대응, 게스트 네트워크 관리 등을 통해 보안 위협에 대한 예방 및 대응 능력을 극대화합니다

가시성

· Agentless 방식으로 네트워크에 연결된 모든 장치를 실시간 탐지 및 분류
· 장치의 정확한 프로파일링을 통해 선제적 보안 컴플라이언스 구축
· 실시간 보안 설정 및 컴플라이언스 준수 여부 확인
· 탐색, 분류, 평가의 과정을 통해 기업의 보안 정책 수립 및 관리

탐지

·네트워크 연결 즉시 장치 식별
·네트워크 장치의 상태 변화 지속 모니터링
·사각지대 없이 실시간 자산 인벤토리 확보

분류

·다양한 유형의 IT, IoT 및 OT 장치 식별
·Forescout Device Cloud 활용
·자동 분류, 적용 범위, 탐지 속도 향상

평가

·보안 위험도 감소 및 컴플라이언스 상태 식별
·내외부 규정 준수 여부 평가
·운영 위험 요소 확인

컨트롤

· 외부 위협으로부터 민감한 데이터 보호
· 취약한 장치에 대한 멀웨어 확산 및 감염 방지
· 직원, 관계사, 협력사, 방문자별 네트워크 접근제어
· 개별 상황에 적절한 조치를 제공하는 제어 기능 자동화

알림

·네트워크 관리자 및 기타 IT/보안 시스템
·호스트 또는 최종 사용자

제어

·네트워크 및 호스트 기반 제어 기능을 통해 리스크 완화
·보안 미준수 사용자에 대한 컴플라이언스 개선

통제

·고위험, 감염 및 악의적인 엔드포인트 검역 또는 차단
·위험성이 높은 Compliance 미준수 엔드포인트 차단

개요

AWS ECSA 보안 진단 컨설팅 개요

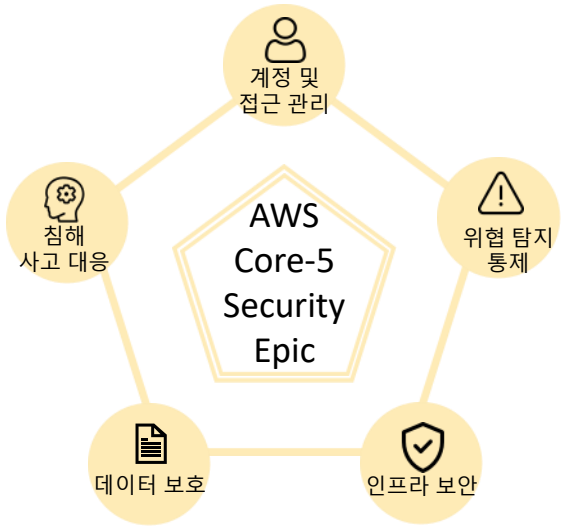
고객의 AWS 환경을 현재의 클라우드 보안 트렌드를 기준으로 진단, 파악하고 AWS 모범 사례기반으로 고객 환경에 최적화 된 대응 방안과 방향성을 제시합니다

AWS ECSA
보안진단컨설팅

ECSA : **E**nhanced **C**loud **S**ecurity **A**ssessment
(클라우드 보안 고도화 및 위험 평가)

도입	구성	보안 · 인증	개인정보보호
클라우드 도입에 관한 고민 해결	기존 환경과 최적의 구성 마련	컨테이너 구성 취약점 문제 해결	ISMS/ISMS-P 인증 준비

보안 진단 범위



1. 계정 및 접근 관리
AWS에서 사용 하는 모든 계정에 대한 권한 및 접근관리에 진단을 통해 최적의 설정 가이드

2. 위협 탐지 통제
AWS 자원에서 사용 되는 EC2, S3, RDS 등 각종 컨텐츠의 로그 및 보안 레벨 진단, 자동화를 통해 위협에 대응 가능한 설정 가이드

3. 인프라 보안
NACL, WAF, VPC 등 내부 인프라를 점검하고 비용절감 및 보안 설정 등에 대한 부분을 보완하여 효율적인 관리 방법 가이드

4. 데이터 보호
KMS, DB 암호화 등 각종 중요 데이터에 암호화 설정 및 키 관리 점검으로 취약한 부분을 보강할 수 있는 방법 가이드

5. 침해 사고 대응
중요 컨텐츠(EC2, RDS 등) 내 이상 행위 발생 시 알람 및 자동화 프로세스 설정 점검 및 취약점 가이드

컨설팅 고도화 단계

1 단계 ECSA

ECSA 수행 (4주간)

1 주차 : 실무자 인터뷰
2 주차 : 오픈소스 점검 툴 연동
3 주차 : 상용화 점검 툴 연동
4 주차 : 결과 정리 및 보고& 도출과제 제출

2 단계 보안 서비스 구조 고도화

네트워크 & 보안 고도화(2개월~3개월)

AWS 네트워크 방화벽 도입 설계
GWLB + APN 솔루션 존 설계
→ 방화벽 정책 설정 가이드
보안 솔루션 선정 가이드
통합 연동 구조 설계

DB 연결 제어

현재 환경 분석/향후 모델 설계
→ AWS 네이티브 서비스 구현
상용화 솔루션 통합 설계

3 단계 보안 서비스 구조 확장

AWS 네이티브 보안 & APN 솔루션 통합 확장(3~4개월)

컨테이너 보안 서비스 설계
침투 테스트 및 사고 대응 흐름 설계
IoT 보안 설계
시큐어 코딩(소스 코드 보안) & 애플리케이션 보안 설계
→ AWS 네이티브 서비스 & 오픈소스 / CWPP
보안 관제 서비스 고도화 : SOAR 솔루션 도입을 통한 자동화 대응 플랫폼 구성
APN 보안 존을 통한 IoT 단말에 최적화된 보안 정책 수립
APN 보안 존을 통한 설계 및 정책 수립

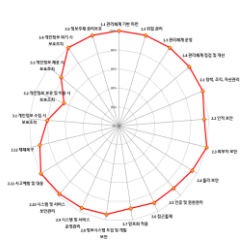
Cloud ISMS/ISMS-P 인증심사 지원

1 년차 ECSA + ISMS - P

오픈소스 진단 툴 점검
결함 조치 및 개선 사항 시스템 적용
ISMS-P 인증 심사 컨설팅 지원
개선 대책 수립 인증 지원 및 사후 관리

→ CIS 벤치마크 기준 취약점 확인
보호대책 요구사항에 해당하는 기술적 보호 대책 확보
1.관리체계 운영 수립
2.보호대책 요구사항
3.개인정보 처리단계별 요구사항
ISMS- P 인증서 획득
클라우드 보안 고도화 로드맵 수립

[진단 결과]



통제 항목	통제 분야	전체	부	Y	P	N/A	보안
1. 관리체계 수립 및 운영	1.1 관리체계 기반 마련	6	17	17	0	0	100%
	1.2 위험 관리	4	13	13	0	0	100%
	1.3 관리체계 운영	3	6	6	0	0	100%
	1.4 관리체계 점검 및 개선	3	6	6	0	0	100%
2. 보호대책 요구사항	2.1 정책, 조직, 자산관리	3	9	9	0	0	100%
	2.2 인적 보안	6	19	17	2	0	95%
	2.3 외부자 보안	4	10	10	0	0	100%
	2.4 물리 보안	7	16	15	0	1	94%
	2.5 인증 및 권한 관리	6	14	11	3	0	89%
	2.6 접근 통제	7	24	20	3	0	90%
	2.7 암호화 적용	2	4	3	1	0	88%
	2.8 정보시스템 도입 및 개발 보안	6	17	16	0	1	94%
	2.9 시스템 및 서비스 운영관리	7	23	21	2	0	96%
	2.10 시스템 및 서비스 보안관리	9	36	34	2	0	97%
	2.11 사고예방 및 대응	5	15	15	0	0	100%
	2.12 재해복구	2	5	4	1	0	90%
3. 개인정보 처리단계별 요구사항	3.1 개인정보 수집 시 보호 조치	7	30	24	0	6	80%
	3.2 개인정보 이용 시 보호조치	5	19	12	1	5	66%
	3.3 개인정보 제공 시 보호 조치	4	14	11	1	2	82%
	3.4 개인정보 파기 시 보고 조치	3	12	12	0	0	100%
	3.5 정보주체 권리보호	3	13	13	0	0	100%
계		102	322	289	16	15	92%

2~3 년차 사후 심사

오픈소스 진단 툴 점검
변경 사항 점검
결함 조치 및 개선
개선 대책 점검
사후 심사 지원

소개

클라우드 환경의 쉽고 편한 ISMS 인증 관리 지원

ASTRON-ISMS는 정책 자동 점검 및 조치 가이드 제공을 통해 클라우드 환경에서의 ISMS 인증을 자동화하여 보안 담당자의 업무를 절감합니다

ASTRON SECURITY

CSPM
- 자산 식별 및 변동 관리
- 자동 컴플라이언스 관리
- 클라우드 취약점 탐지 및 진단
- 클라우드 시각화

CWPP
- 컨테이너 시각화
- 쿠버네티스 취약점 탐지 및 진단
- 컨테이너 현황 감시
- 호스트 보안

CIEM
- IAM 권한 시각화
- 실시간 IAM 권한 탐지
- IAM 권한 변경 관리

CNS
- 클라우드 네트워크 시각화
- 방화벽 정책 관리
- 실시간 보안 토폴로지
- 정책 시뮬레이션 시각화

ISMS
- 정책 자동 점검
- 조치 가이드 제공
- 증적 자료 제공
- 보고서 지원

주요 서비스

ASTRON-ISMS 주요 기능

정책 자동 점검
300여개의 ISMS 인증 항목에 대한 정책을 자동으로 점검

조치 가이드 제공
인증 기준에 부적합할 시 자동으로 조치 가이드 제공

증적 자료 제공
ISMS 인증 항목에 따른 증적을 제공하여 관리의 연속성 보장

담당자별 점검 이력 관리
인증 시 담당자별 점검 이력관리가 가능하여 정보보호 담당자 변경 시에도 원활한 업무 수행 가능

점검 결과 보고서 지원
인증 항목 점검에 따른 결과 보고서 및 엑셀 다운로드 기능 지원

중요도에 따른 효율적 자산 관리
중요도에 따라 자산을 관리하여 보안 담당자의 업무 리소스 절감

감사합니다

We COULD Secure,
You DO Safer.

CUDO COMMUNICATION

쿠도커뮤니케이션㈜

02-525-0481 | secure@cudo.co.kr
www.cudo.co.kr | secure.cudo.co.kr | blog.naver.com/cudo_cybersecurity