Think Secure!

아스트론시큐리티 회사소개서

ASTRON SECURITY

회사 소개

Chapter 1

Think Secure!

ASTRON SECURITY

회사 소개 (1)

아스트론시큐리티는 누적 100억원 이상의 투자를 받은 국내 선두 기술력의 '클라우드 보안 전문 기업'입니다.

회사소개

회사명
아스트론시큐리티

설립일
2019.03.26

주소
서울 강남구 봉은사로 115
노벨테크 6F (신논현역)

자본금
7억원

특징

누적 투자금 100억
직원의 80% R&D 인력

주요 투자사

NAVER CLOUD PLATFORM
IBK기업은행
KDB산업은행
KB Investment
LIGHTHOUSE COMBINED INVESTMENT
HYUNDAI GBFMS CO., LTD.
AhnLab
아주IB투자
KIBO 기술보증기금

인증 및 특허

5 건	1 건	11 건
국내 특허 등록	글로벌 특허 등록	국내 및 글로벌 특허 출원

KSM 등록 기업 확인서

CSAP 인증서

기업부설연구소

GS 인증서

회사소개 (2)

2019년 설립 이래 클라우드 보안 기술력을 인정 받아 아기유니콘 기업 선정 및 다수의 국가 기관에서 상장을 수여받았습니다.

수상 이력

넥스트라이즈
Innovation Prize

과기정통부 장관상

중기부 장관상

시큐리티어워드 코리아
2021대상

시큐리티어워드 코리아
2022대상

2022
아기유니콘
기업 선정

제품 소개

아스트론시큐리티는 ASTRON-CWS를 통해 클라우드 보안의 핵심 기능을 하나의 솔루션에서 모두 제공합니다.

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

CWPP
- 컨테이너 시각화
- 쿠버네티스 취약점 진단 및 탐지
- 파일 무결성 감시
- 호스트 현황 모니터링

CIEM
- IAM 권한 시각화
- 권한 상승 계정 탐지
- IAM 권한 변경 관리

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

CDR
- 이상 행위 탐지
- 이상 징후 탐지
- 이벤트 로그 분석

ASTRON CWS

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

클라우드 보안 시장 환경

Chapter 2

Think Secure!

ASTRON SECURITY

클라우드 보안 환경의 변화 (1)

전통적 IT 환경 대비 클라우드 환경으로 갈수록 보안의 취약성 및 복잡성이 증가합니다.

전통적 IT 환경

- 데이터센터 중심의 설계 (통제 가능)
- 개별 보안 관리 모델
- 경계선 보안
- 비교적 안전한 보안

새로운 클라우드 환경

- 멀티 클라우드 기반의 복잡한 설계
- 제로트러스트 보안
- 보안 위험도 증가
- 통합 보안 관리 모델

클라우드 보안 환경의 변화 (2)

전통적인 IT 환경에서의 보안은 위협 방지 및 차단을 목표로 하지만, 클라우드 환경은 신속하게 피해를 최소화하는데 맞춰져 있습니다.

전통적인 위협 관리 조치
(SIEM)

- 로그 정보 (Discrete)
- 자동화된 보안 관리
- 알려진 위협에 대한 관리

위협 방지 및 차단

침투 불가능한 시스템
Prevention

클라우드 위협 헌팅
(Cloud Threat Huntiong)

- 클라우드 이벤트 로그, 행위 정보 관리
- 자동화된 변동사항 식별 관리
- AI의한 알려지지 않는 위협 탐지

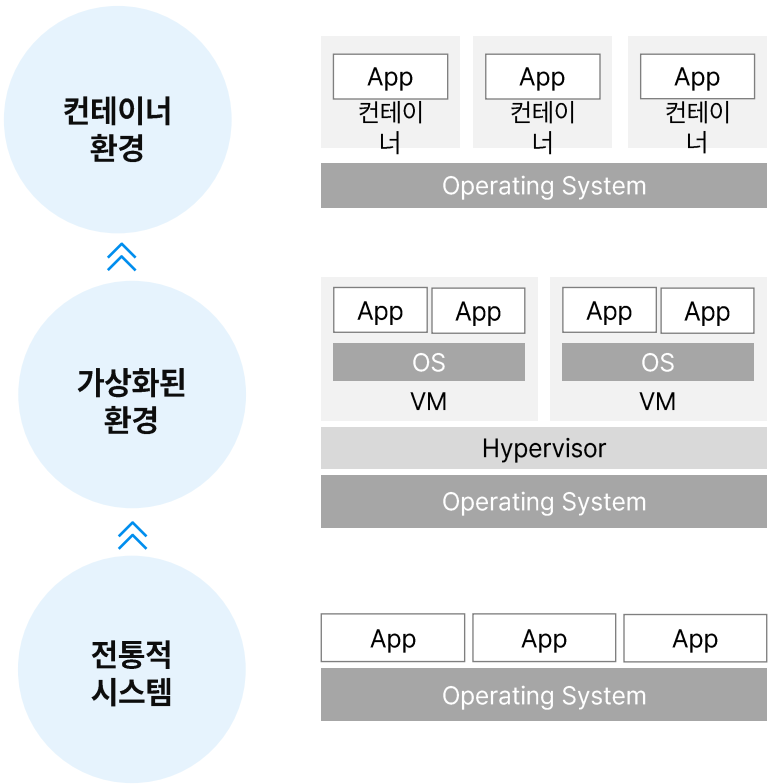
신속한 피해 최소화

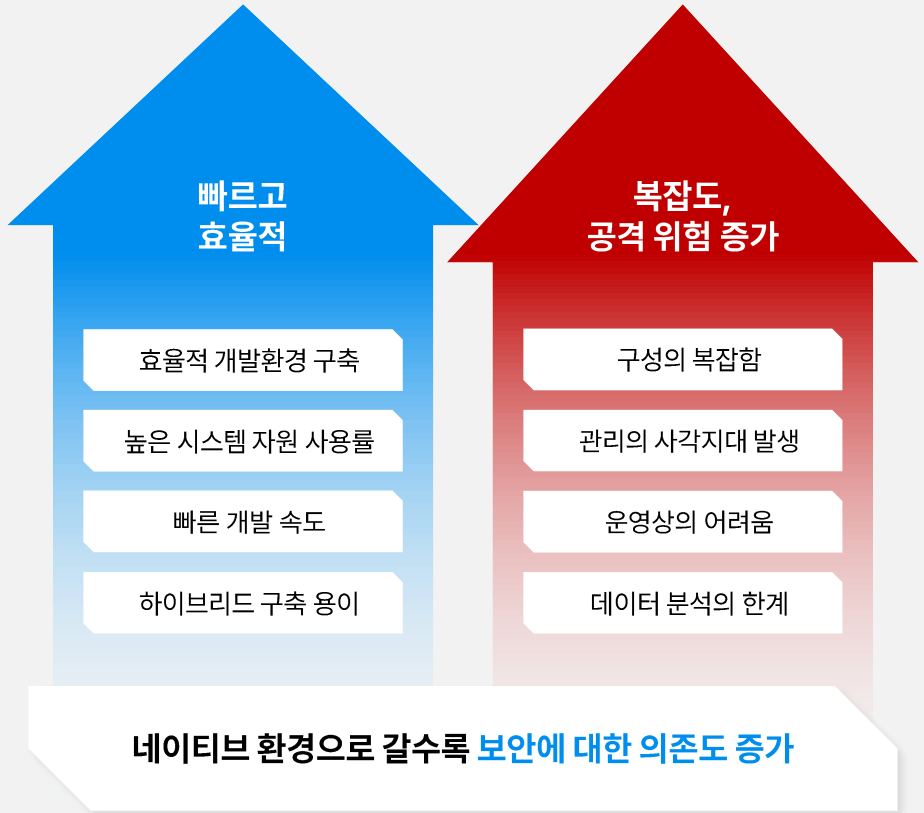
탄력적인 적응형 시스템
Detection & Response

클라우드 네이티브 환경에서의 보안

컨테이너 환경은 운영 효율이 좋아지는 반면 복잡성과 공격 위험도가 빠르게 증가하여 보안의 사각지대가 발생합니다.

클라우드가 네이티브 환경으로 빠르게 발전하고 있음





네이티브 환경으로 갈수록 보안에 대한 의존도 증가

클라우드 보안 사고 주요 원인

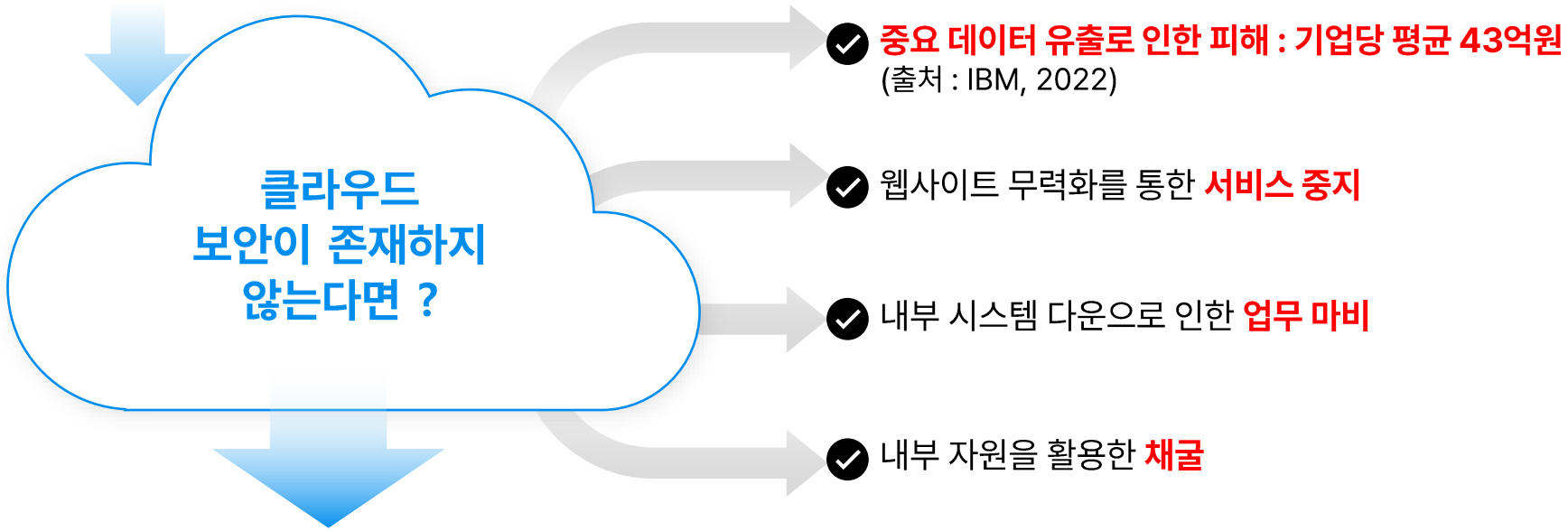
클라우드 환경은 내 · 외부에 다양한 위협 요소가 존재하며 다음 7가지 사항이 클라우드에서 보안 사고를 일으키는 핵심적인 원인입니다.

클라우드 보안 사고의 7가지 원인

1. 데이터 유출
2. 계정 탈취
3. 내부자 위협
4. 사용자 설정 오류
5. 클라우드 보안 아키텍처 미흡
6. 불안정한 인터페이스 및 API
7. 신원,액세스 관리 미흡

클라우드 보안의 중요성

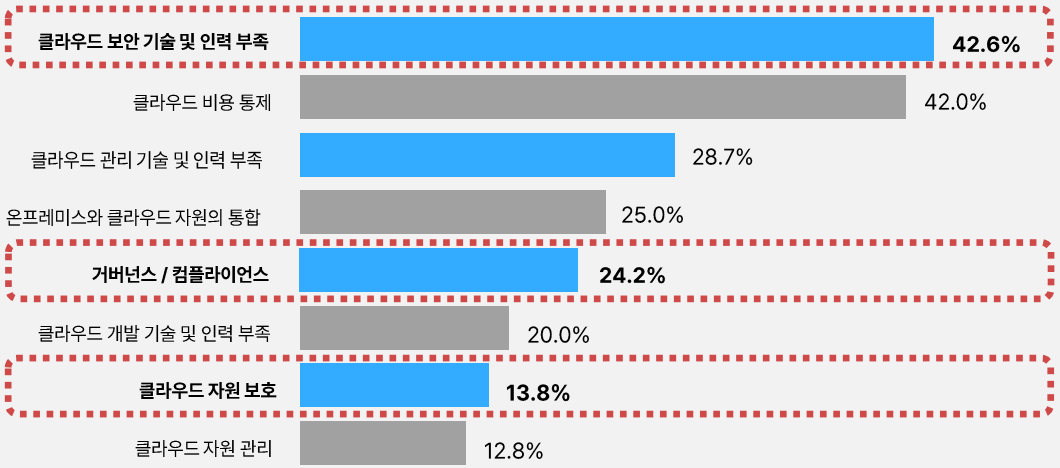
고도화된 클라우드 보안이 필요함에도 기본 보안만 적용할 경우 막대한 해킹 피해로 이어져 기업의 생존을 위협 받을 수 있습니다.



클라우드 도입 저해 요인

클라우드 도입을 저해하는 요인으로는 보안적 이슈가 가장 많은 부분을 차지하고 있었으며, 클라우드 보안 솔루션 도입 시 가장 중요하다고 생각하는 기능으로는 **클라우드 취약점 진단 및 탐지, 시각화** 등을 꼽았습니다.

"클라우드 도입 및 활용 과정의 어려움은?"



출처: 2023년 국내 클라우드 컴퓨팅 현황과 전망 IT World CIO

"클라우드 보안 솔루션 도입 시 중요하다고 생각하는 기능은?"

1. 클라우드 취약점 진단 및 탐지 — 45%
2. 클라우드 자산 식별 및 시각화 — 37%
3. 클라우드 계정 및 권한 보안 — 33%

보안 관련 전문가 475명 대상, 자체 설문 조사 진행

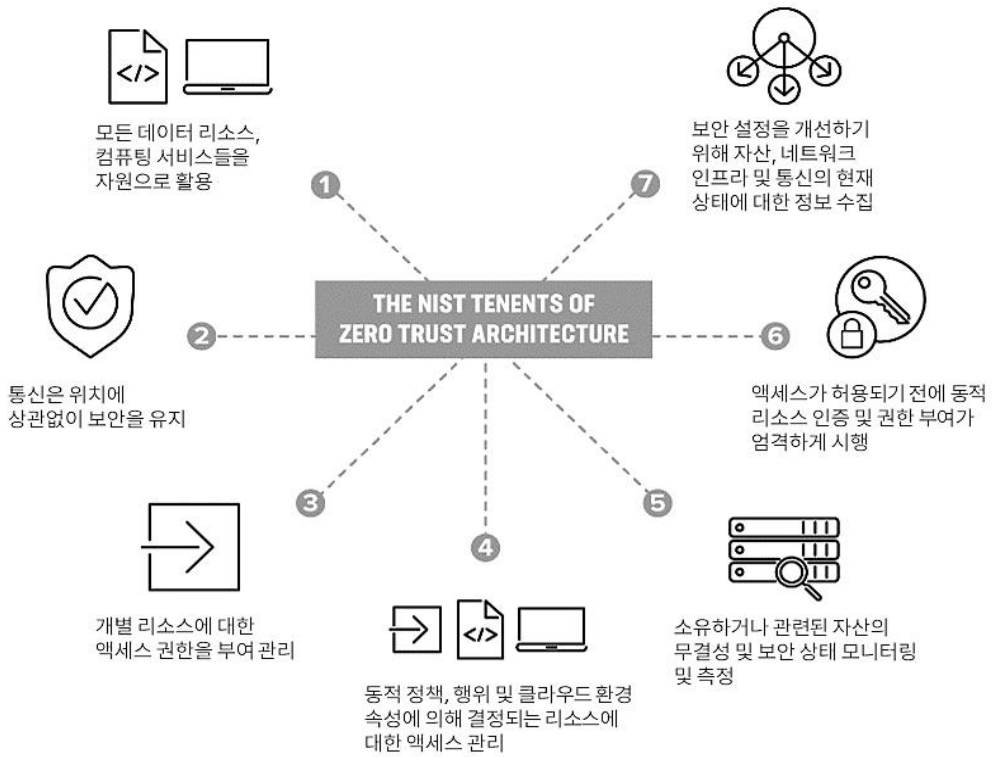
제로 트러스트 환경

미국 바이든 행정부는 국립표준기술연구소(NIST)의 규정 800-207에 의거 사이버 영역에서 제로 트러스트 보안을 강화하도록 행정명령으로 지시하고 있습니다.

미국 행정부 클라우드 컴퓨팅 제로트러스트 보안 규정

- 미국은 NIST 800-207에 의거 제로 트러스트 보안에 대해 규정
  → 클라우드컴퓨팅 보안에 적용

1) 계정 도용, 내부자 위협 대비
2) 주체 및 소유 자산 식별
   - "섀도우 IT" 식별
3) 핵심 프로세스 식별 및 위협 평가



[미국 NIST 800-207 제로트러스트 기본 원칙]

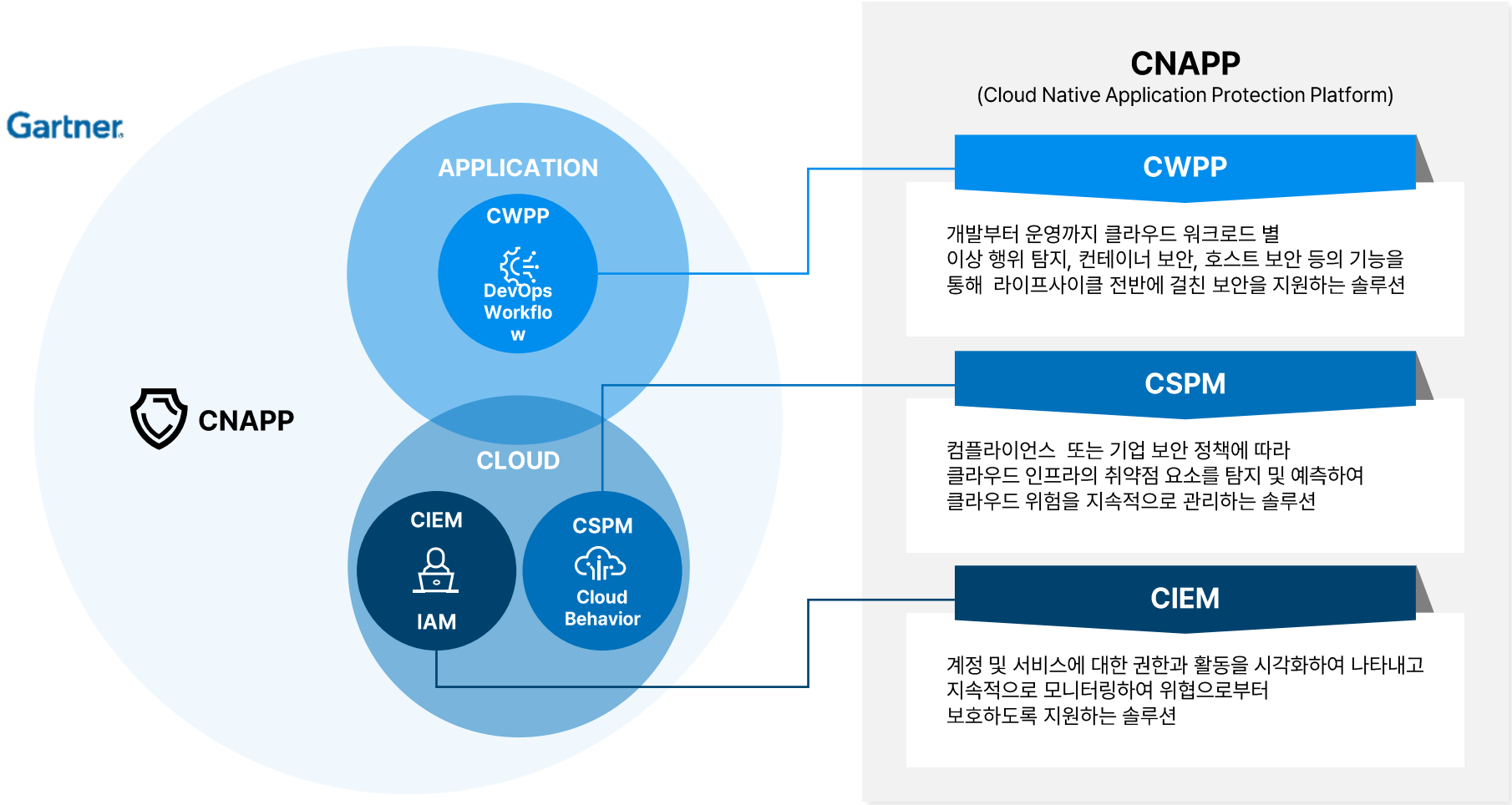
클라우드컴퓨팅 환경에 대한 제로트러스트 보안

클라우드 네이티브 환경까지 통합화된 보안체계 CNAPP 도입 운용중임

- CSPM & KSPM
- CIEM
- CWPP
- \+
- 지능화

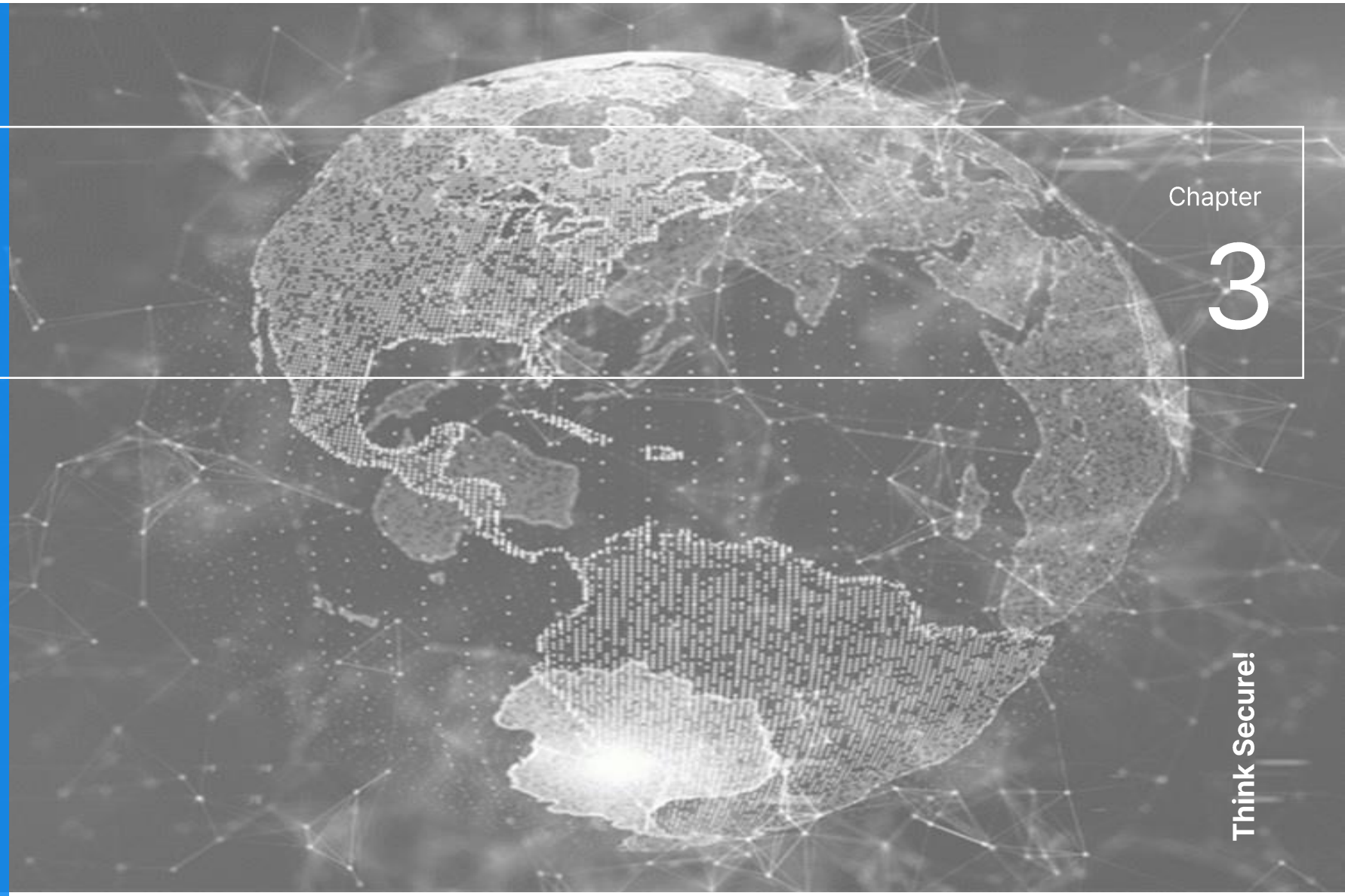
클라우드 보안 트렌드

가트너는 CSPM, CWPP, CIEM을 통합한 CNAPP를 차세대 클라우드 보안 솔루션으로 권장하고 있습니다.



제품 개요 및 주요 기능

Chapter 3



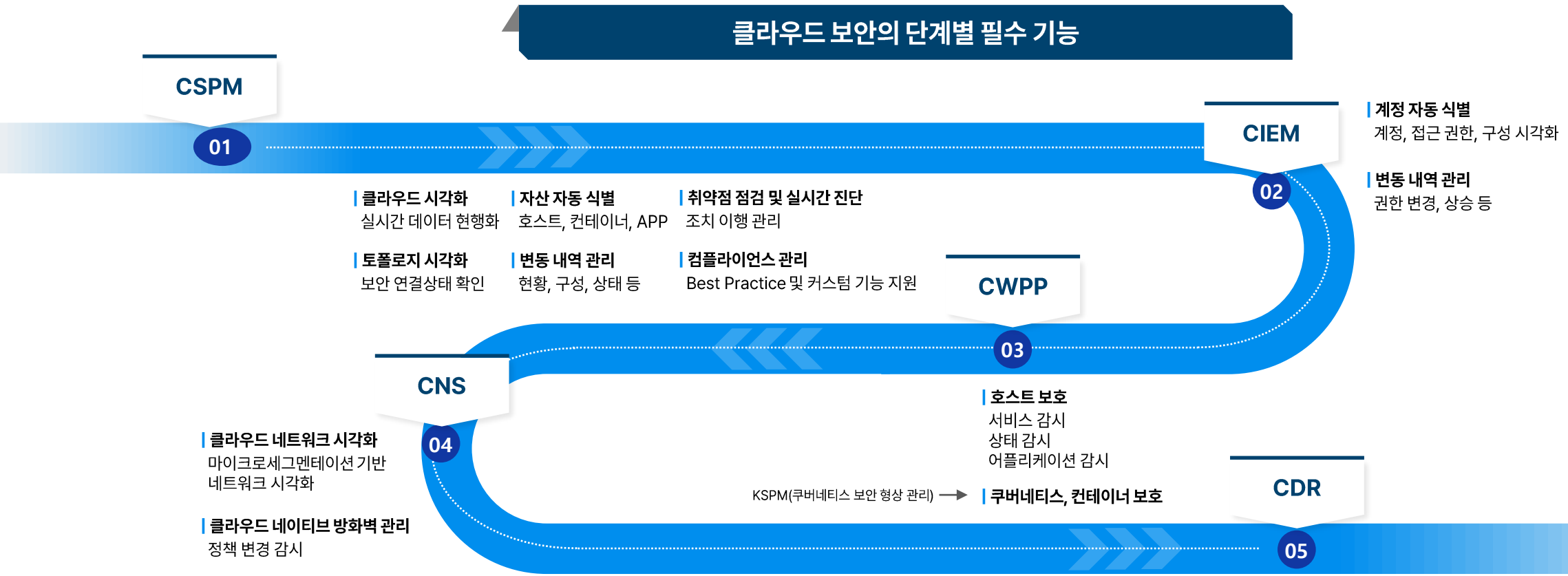
Think Secure!

ASTRON SECURITY

제품 개요 (1)

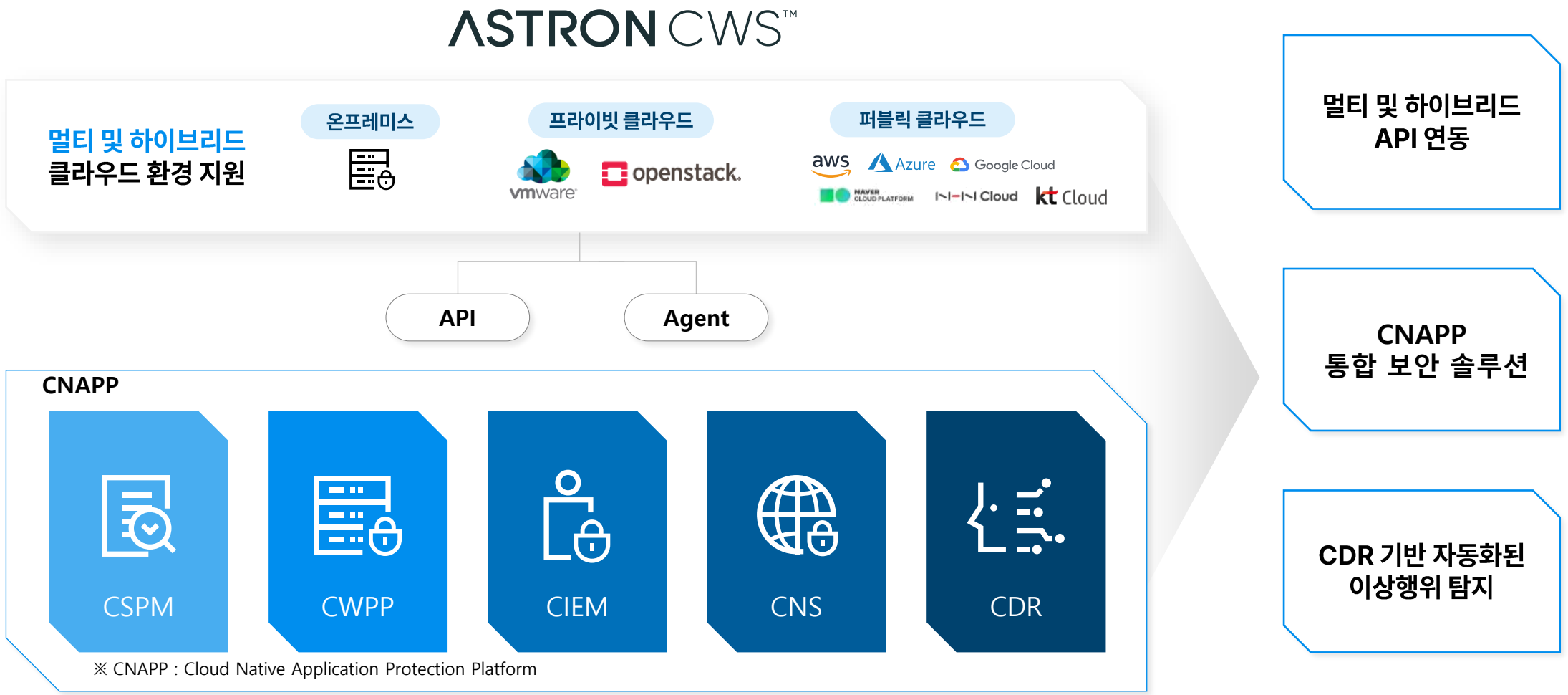
ASTRON-CWS는 멀티 및 하이브리드 클라우드를 보호하는 All-In-One 클라우드 보안 솔루션입니다.

클라우드 보안의 단계별 필수 기능



제품 개요 (2)

멀티 클라우드 API 연동, 자산 식별, 시각화 등의 핵심 모듈과 AI 기반의 CDR 기술을 결합하여 K-Cloud 보안을 구현합니다.



ASTRON-CWS 01

CSPM

클라우드 환경이 복잡해짐에 따라 보안 사고로 이어지는 설정 오류를 미리 탐지하고 예방하는 것은 점점 더 어려워지고 있습니다.

ASTRON-CSPM은 자산 식별 및 변동 관리, 컴플라이언스 관리, 클라우드 시각화를 통해 멀티 클라우드 자산을 안전하게 보호하고 사용자의 설정 오류를 방지합니다.

ASTRON-CWS 01

CSPM의 주요기능

실시간 취약점 탐지

실시간으로 클라우드 환경의 취약점을 탐지하고
자동으로 조치 결과를 점검하여 빠르게 대응

주기적인 취약점 진단

주기적으로 클라우드 환경의 취약점을 진단하고 조치
가이드를 제공하여 보안 담당자의 리소스 축소

자동 컴플라이언스 관리

다양한 국내 외 컴플라이언스 및 커스텀 컴플라이언스를
생성하여 기업별 맞춤 보안 관리

자산 식별 및 변동 관리

국내·외 퍼블릭 및 프라이빗 클라우드에 대한 API 연동을 통해
복잡한 클라우드 환경을 손쉽게 관리

클라우드 시각화

클라우드 내 모든 자산에 대한 가시성을 실시간으로
확보하여 클라우드 보안을 지속적으로 점검

보안 토폴로지

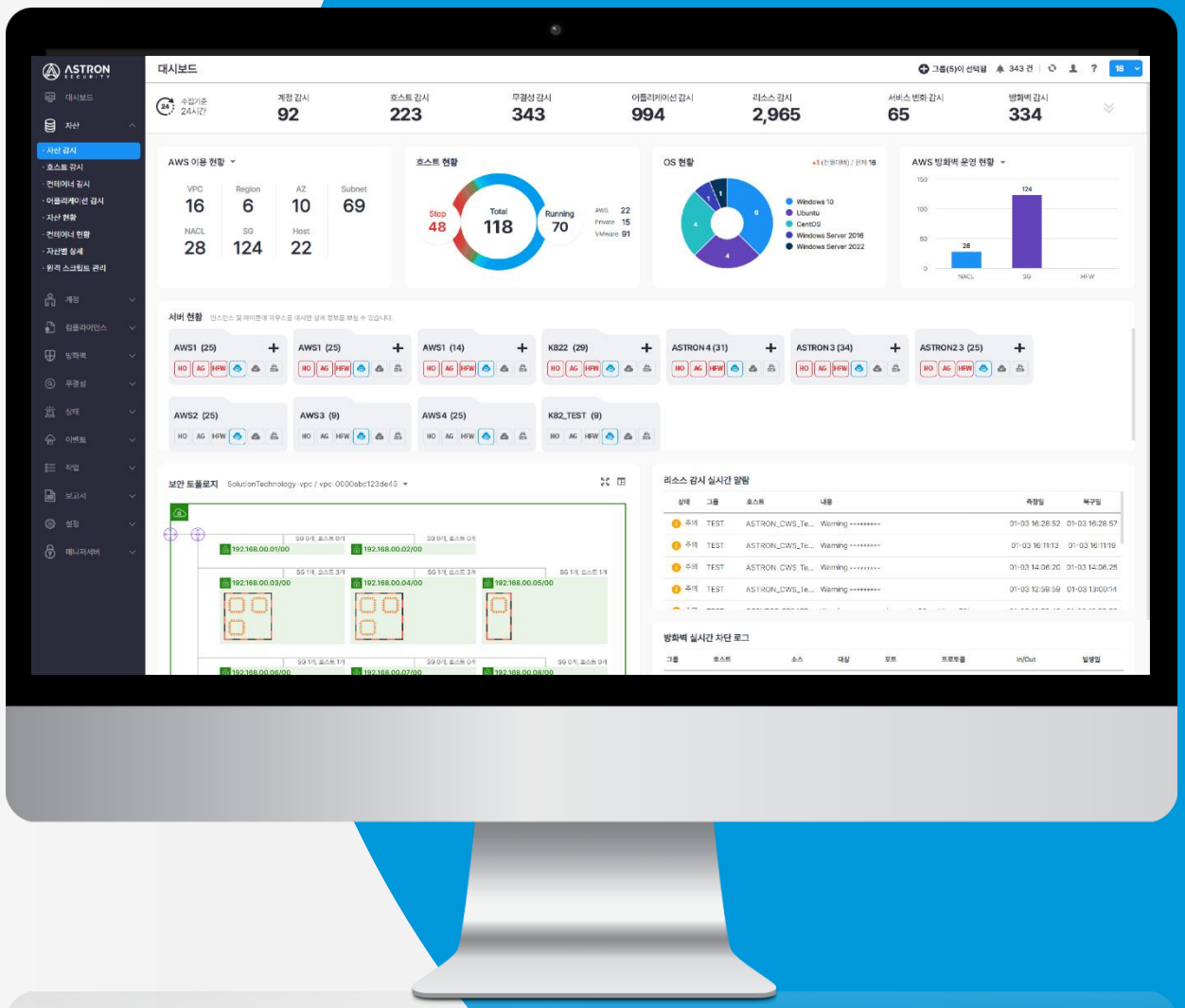
클라우드 운영 및 보안 상태를 한눈에 파악할 수 있는
최적의 네트워크 아키텍처를 제공하여 보안 가시성 확보

ASTRON-CWS 02

CWPP

컨테이너 네이티브 환경으로 인해 워크로드별 보안 요구 사항이 다양해짐에 따라 일관된 보안 관리가 어려워지고 있습니다.

ASTRON-CWP는 개발부터 배포, 운영에 이르기까지
라이프사이클 전반에 걸쳐 클라우드 워크로드 위협을
신속하게 탐지하여 워크로드별 보안 요구사항을 지원합니다.



ASTRON-CWS 02

CWPP의 주요기능

호스트 계정 및 자산 관리

VM에서 생성된 호스트의 생성, 수정, 삭제, 변경
내역 등을 확인하고 호스트 자산 및 계정 현황 파악

무결성 감시

실시간으로 파일 및 디렉토리의 변경사항을
확인하고 파일 위변조 여부 파악

상태 감시

호스트의 리소스 현황 및 알람 제공, 서비스
변화감시, 프로세스, 포트 현황 제공

쿠버네티스 컴플라이언스 관리

CIS Kubernetes Benchmark에 따른 취약점 진단을
제공하고 커스텀 기능을 통해 커스텀 컴플라이언스 생성

컨테이너 및 쿠버네티스 시각화

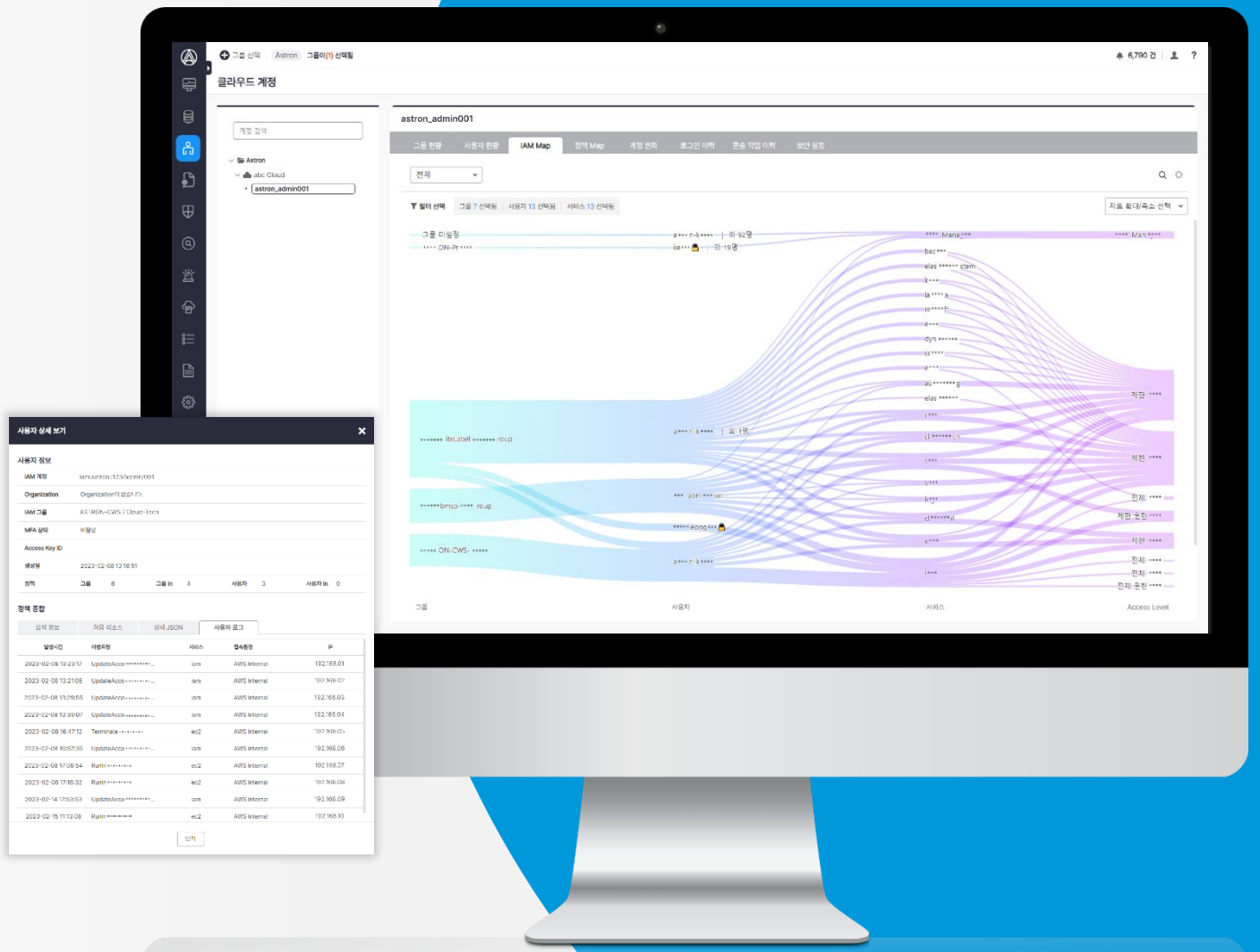
클러스터 내 호스트, POD, 컨테이너의 상태를 시각화하여
컨테이너 및 쿠버네티스 정보를 쉽게 파악

ASTRON-CWS 03

CIEM

클라우드 인프라의 가장 큰 위험은 기업 '밖'이 아닌 '안'에 있습니다. 기업을 노리는 해커들은 민감한 데이터에 접근하기 위해 IAM 권한을 악용합니다.

ASTRON-CIEM은 클라우드 내 IAM 시각화 및
권한 상승 계정 탐지를 통해 최소한의 권한으로 계정을
관리할 수 있습니다.



ASTRON-CWS 03

CIEM의 주요기능

IAM 서비스의 다양한 항목 지원 및 시각화

그룹, 사용자, 정책, 액세스 레벨 등의 권한을 확인하고
데이터를 실시간으로 수집하여 각 항목들의 관계를
시각화하여 제공

정책 MAP

조직, 그룹, 사용자 정책 별로 MAP을 제공하여
정책에 따른 액세스 레벨 확인

실시간 IAM 권한 탐지

계정의 생성, 수정, 삭제를 실시간으로 업데이트하여
사용자별 권한 범위를 손쉽게 파악

IAM MAP 시각화

그룹과 사용자 계정에 관한 MAP을 제공하여
계정에 대한 권한 구조 및 MFA 보안 설정 확인 가능

IAM 권한 변경 관리

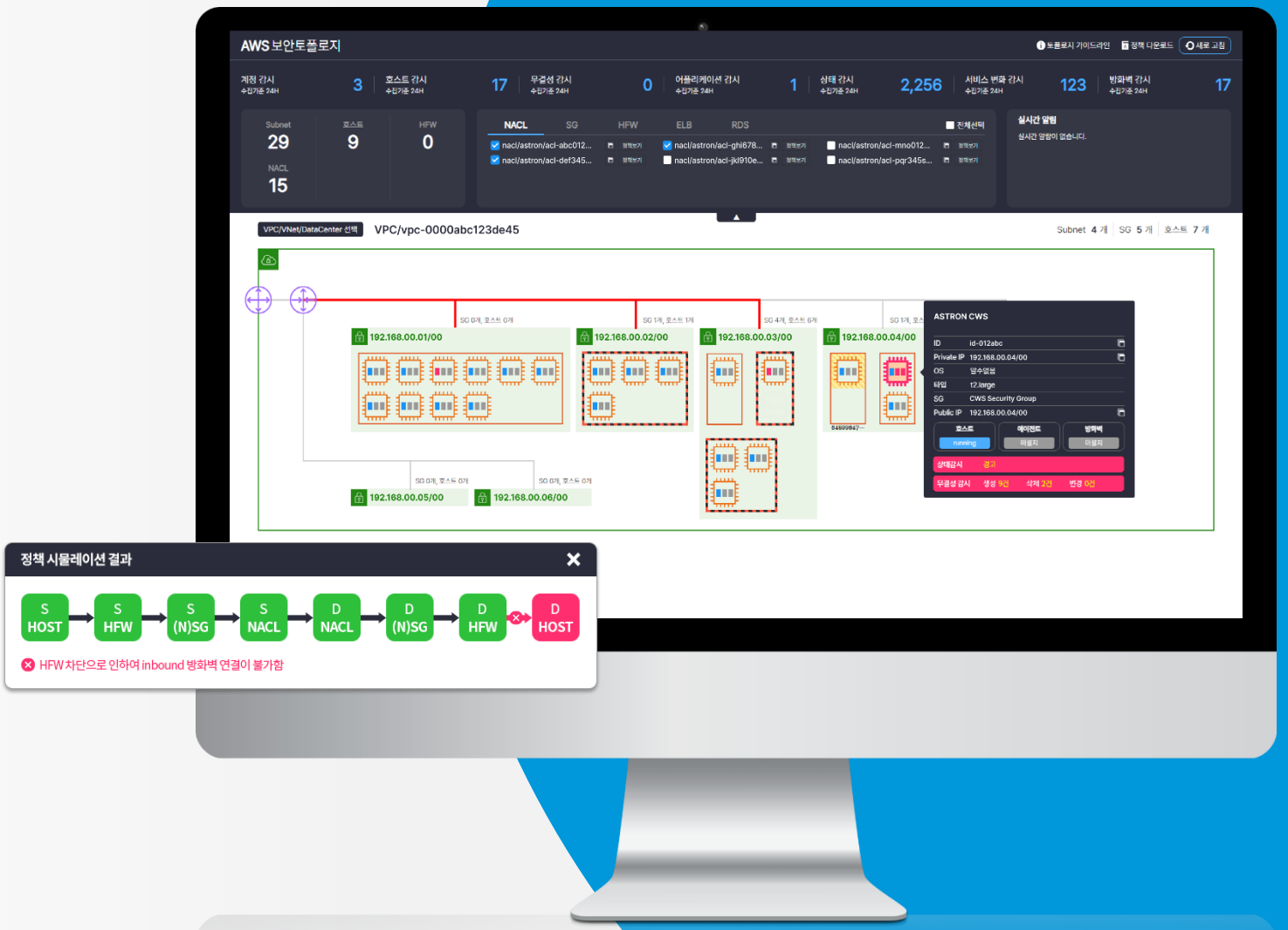
신규 생성 계정, 미사용 계정, 권한 상승 계정을
MAP으로 확인 가능

ASTRON-CWS 04

CNS

빠르게 변화하는 클라우드 환경에서 네트워크 위협을 효과적으로 탐지하고 보호하는 것은 매우 어렵습니다.

ASTRON-CNS는 클라우드 네트워크 환경에 대한
가시성을 제공하고 보안 토폴로지 및 내부 방화벽 정책 제어를 통해
지속적으로 위협을 탐지하여 대응합니다.



ASTRON-CWS 04

CNS의 주요기능

클라우드 네트워크 시각화

클라우드 네트워크 계층 구조를 파악하는 토폴로지 제공

마이크로세그멘테이션

마이크로세그먼테이션을 통해 East-West 트래픽에 대한
가시성을 확보하고 클라우드 내부에서 발생하는 네트워크
위협을 탐지

방화벽 시각화

호스트 간 방화벽 연결 상태를 시각화하여 한눈에 확인하고
정책 시뮬레이션을 시각화하여 사전에 정책의 적합성 판단

방화벽 정책 관리

방화벽 정책의 생성, 수정, 삭제를 통해 정책을 관리하고
인바운드 및 아웃바운드 정책을 탬플릿으로 미리 작성하여 사용

방화벽 알람 및 로그

방화벽 정책이 변동될때마다 실시간으로 알람 제공,
방화벽에 대한 모든 차단 및 허용 로그 수집

ASTRON-CWS 05

ISMS

클라우드 환경에서의 ISMS 인증을 위해선 인증 취득을 위해 매년 비용과 시간을 투자해야 합니다.

ASTRON-ISMS는 정책 자동 점검 및 조치 가이드 제공을 통해
클라우드 환경에서의 ISMS 인증을 자동화하여 보안 담당자의 인증 관련
시간과 비용을 절감시킵니다.

ASTRON-CWS 05

ISMS의 주요기능

정책 자동 점검

300여개의 ISMS 인증 항목에 대한 정책을
자동으로 점검

조치 가이드 제공

인증 기준에 부적합할 시 자동 조치가이드 제공

증적 자료 제공

ISMS 인증 항목에 따른 증적을 제공하여
관리의 연속성 보장

결과 보고서 지원

인증 항목 점검에 따른 결과 보고서 및
엑셀 다운로드 기능 지원

담당자별 점검 이력 관리

ISMS 인증 시 담당자별 이력관리가 가능하여
정보보호 담당자 변경 시에도 원활한 업무 수행 가능

중요도에 따른 자산 관리

중요도 및 특이사항에 따라 자산을 관리하여
보안 담당자의 업무 리소스 절감

제품 특장점

Chapter

4

Think Secure!

ASTRON SECURITY

제품 특장점 – 컴플라이언스 관리 (1)

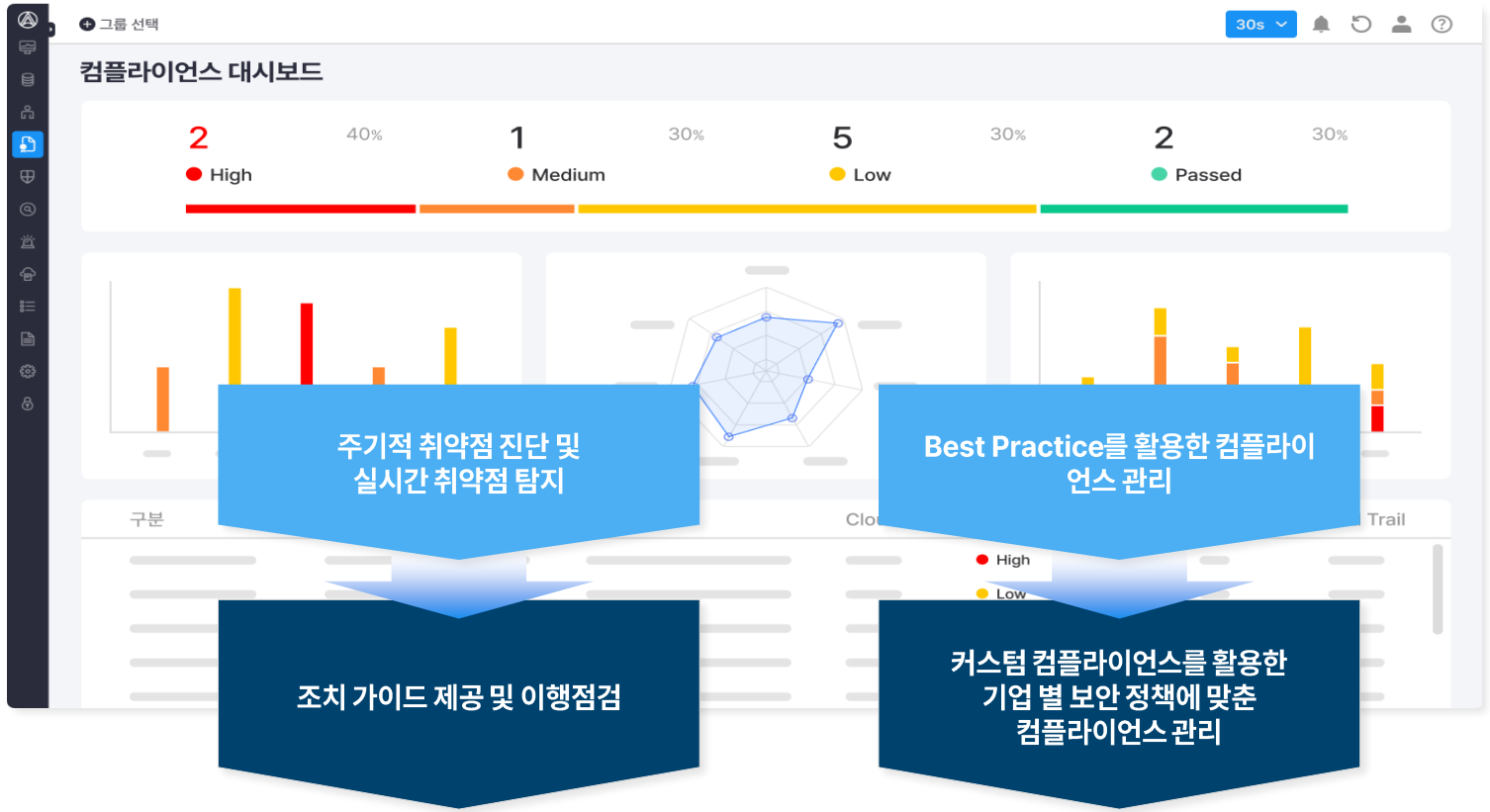
취약점 탐지 및 진단 · Best Practice 및 커스텀 기능을 통해 컴플라이언스 관리를 최적화합니다.

ASTRON CSPM 현황

10,000+
CSPM 취약점 진단 횟수

300+
컴플라이언스 진단 항목

1+
국내 유일
실시간 취약점 탐지



"효과적이고 편리한 컴플라이언스 관리 환경 구축"

제품 특장점 – 컴플라이언스 관리 (2)

기업 보안에 필수적인 ISMS-P, ISO 27001 등 다양한 국내 · 외 표준 컴플라이언스에 맞춰 취약점 점검 및 관리를 할 수 있습니다.

국내 및 글로벌 표준 컴플라이언스에 최적화하여

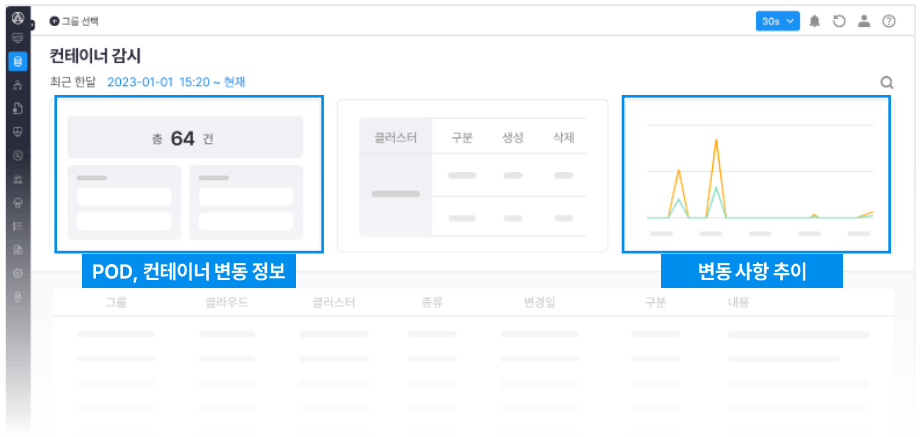
컴플라이언스 관리 → **취약점 진단 및 실시간 탐지**

- ISMS-P
- ISO 27001
- CSAP
- NIST 800-53
- CIS Benchmark / Kubernetes CIS Benchmark
- GDPR
- PCI-DSS
- HIPAA

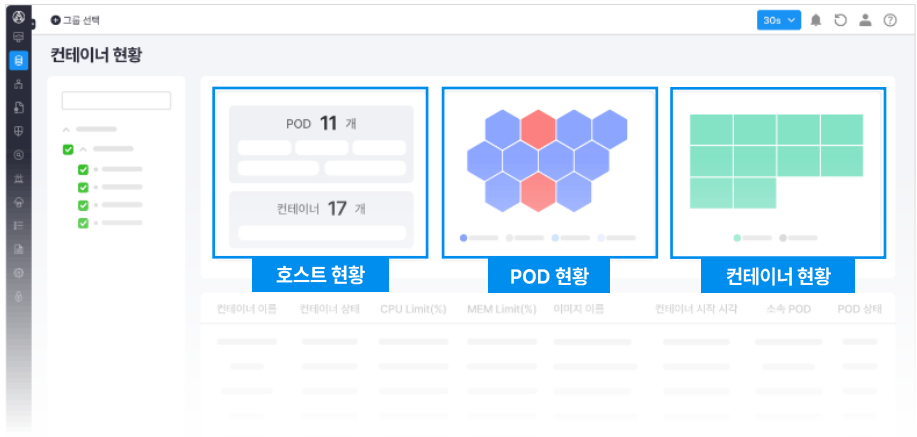
제품 특장점 – 컨테이너 보안

쿠버네티스 및 컨테이너 시각화, 취약점 진단을 통해 애플리케이션을 안전하게 보호합니다.

컨테이너 감시 화면



컨테이너 현황 화면



1 쿠버네티스 및 컨테이너 시각화

호스트, POD, 컨테이너의 상태를
시각화하여 쿠버네티스 정보를 쉽게 파악

2 쿠버네티스 및 컨테이너 취약점 진단

자동화된 컴플라이언스 관리,
쿠버네티스 취약점 진단 및 실시간 탐지를 통해
보안팀이 정책 중심의 관리체계를
수립할 수 있도록 지원

3 취약점 조치 가이드 및 이행 점검 제공

쿠버네티스 취약점 발견 시 조치 가이드를 제공
하여 담당자가 대응할 수 있도록 하며
이행 점검을 통해 취약점에 대한
처리 결과 관리

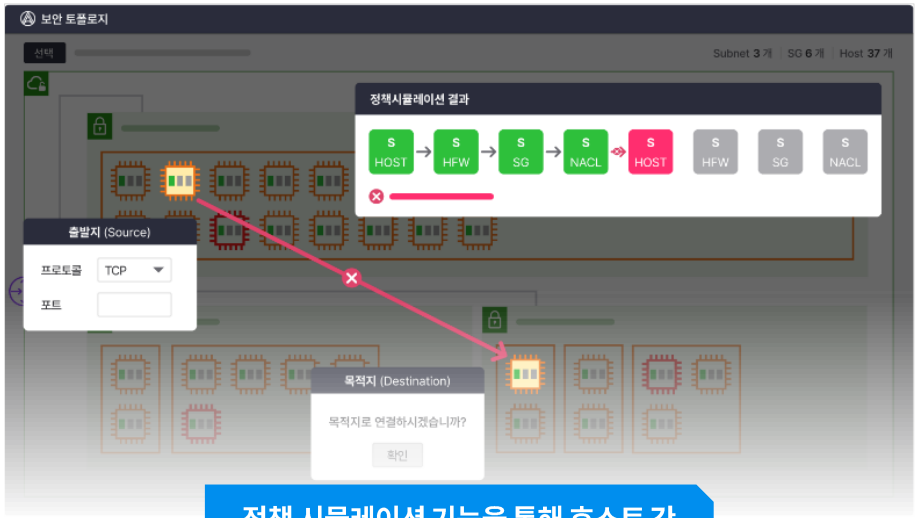
제품 특장점 – 네트워크 시각화

클라우드 네트워크 상태를 한눈에 파악할 수 있는 보안 토폴로지를 제공하고 East-West 트래픽에 대한 가시성을 확보하여 네트워크 위협을 탐지합니다.

멀티 토폴로지 화면

한 화면에서 멀티 토폴로지 관리

토폴로지 정책 시뮬레이션



정책 시뮬레이션 기능을 통해 호스트 간 방화벽 연결 가능 여부 미리 파악

1. 클라우드 네트워크 시각화를 통해 클라우드 계층 구조 파악
2. 호스트 간 방화벽 연결 상태를 시각화하여 한눈에 확인
3. East-West 트래픽에 대한 가시성을 확보하여 네트워크 관리

제품 특장점 – IAM 시각화

실시간 IAM Map을 통해 효과적인 계정 및 접근 권한 식별이 가능합니다.

IAM Map 화면

신규 계정, 미사용 계정, 권한 상승 계정에 대해 Map을 통해 직관적으로 파악

액세스 레벨에 따른 사용자 현황 및 권한을 효과적으로 식별하여
최소한의 권한으로 계정 관리

사용자 정책, 권한 상세보기

- 해당 사용자의 정책, 권한 정보 제공
- 최종 권한의 서비스 리소스 이름(ARN) 제공
- 사용자 정책에 대한 상세 데이터 교환 형식(JSON) 제공
- 사용자 활동 로그 제공

제품 특장점- ISMS 인증

약 30여개의 AWS 자산에 대한 관리적 / 기술적 영역에 대한 증적 자료를 통합적으로 제공하여 관리의 연속성을 보장하고 취약점 진단, 통제항목 점검 등 다양한 기능을 통해 ISMS 인증 프로세스를 쉽게 관리할 수 있습니다.

항목	기능 요건	설명
관리 통제항목	증적 관리	• 문서 관리, 진도 관리, 결함 관리 등
기술 통제항목	취약점 진단	• 설정에 대한 기술적 취약점 진단 • 진단에 따른 조치 가이드 제공
	통제항목 점검	• 정책 자동 점검 • 중요도에 따른 정보 자산 관리 • 접근 통제 관리 • 보안시스템 정책 관리 • 이상행위 분석 및 모니터링
	증적 관리	• 현황, 로그 보고서, 점검 기능 등

AWS 자산 리스트

- ✓ EC2
- ✓ Lambda
- ✓ ECS
- ✓ ECK
- ✓ ECR
- ✓ S3
- ✓ Backup
- ✓ S3 Glacier
- ✓ EFS
- ✓ RDS **외 20개**

보안 구축 사례

Chapter

5

Think Secure!

ASTRON SECURITY

보안 구축 사례 – A 대기업

"A 기업은 멀티 클라우드 환경의 최적화를 통해 클라우드 통합 보안 관리 체계 구축에 성공하였습니다."

Industry : IT 서비스
기업 규모 : 대기업

aws Azure vmware

- VMware 및 AWS, Azure 등의 하이브리드 클라우드 이용 중
- 향후 국내 외 퍼블릭 클라우드 추가 확장 계획
- 소수 인력으로 대량 시스템 이용 중

Challenges

- 수 백대에 이르는 워크로드 보안 관리의 어려움 호소
- 멀티 클라우드 보안 가시성 확보 솔루션의 부재
- 효과적인 클라우드 취약점 점검 솔루션 필요
- 컨테이너 환경에 최적화된 보안 솔루션 도입 니즈 증가

Solution

- 멀티 클라우드 환경에 대한 통합적 관리 (운영, 보안, 장애관리, 로그 등)
- 실시간 취약점 탐지 및 주기적 진단, 조치 사항 제공을 통한 취약점 점검 프로세스 수립
- 멀티 클라우드 API 연동을 통한 자산 가시성 확보
- 컨테이너 취약점 진단 및 탐지, 시각화를 통한 보안 강화

보안 구축 사례 – B 광역지자체

"B 광역지자체는 N사의 클라우드를 대규모로 이용함에 있어 자산 식별 및 취약점 탐지, 계정관리 이상행위 탐지 등의 기능을 통해 클라우드 내부 보안을 강화하였습니다."

Industry : 공공기관

기업 규모 : 광역지자체

- 국내 선두권 N사 클라우드 공공존 이용 중
- 클라우드 내부 보안 강화 및 증적자료 확보 필요

Challenges

- 공공서비스의 발전과 도민 서비스 향상을 위해 국내 선두 N사의 클라우드 공공 존을 안전하게 이용하고자 하는 니즈 보유

Solution

- 클라우드 자산의 생성/수정/삭제, 정책 변경 등을 실시간으로 감시
- 보안 토폴로지 기반 네트워크 시각화 및 마이크로세그멘테이션 구현
- 클라우드 상의 취약점 점검 및 실시간 탐지
- 계정 및 권한 관리, 사용자의 이상행위 탐지
- 클라우드 보안 강화

복잡했던 클라우드 보안,
이제는 달라진 To-Be를 경험할 때입니다.

01

자동화된 취약점 탐지 및 진단으로 클라우드 설정 오류 방지!

02

식별하기 어려웠던 멀티 클라우드 자산, 한눈에 식별!

03

실시간 컨테이너 현황 감시를 통해 효과적인 컨테이너 보안 실현!

04

IAM 권한 시각화를 통해 과도하게 권한이 부여된 계정 탐지!

사각지대 없는 클라우드 보안,
ASTRON-CWS로 실현하세요!

클라우드 보안의 필수 기능을 하나의 솔루션으로 완성할 수 있습니다.

CNAPP 솔루션
CSPM, CWPP, CIEM 솔루션
기능을 통합적으로 제공하여 클라우드
보안을 다양하게 지원합니다.

CDR
AI 기반 이상행위를 탐지하고
예측하여 위협으로부터
클라우드 환경을 보호합니다.

컨테이너 보안
컨테이너 시각화, 쿠버네티스 취약점
진단 및 실시간 탐지를 통해 컨테이너
환경을 보호합니다.

클라우드 시각화
클라우드의 모든 자산에 대한
가시성을 확보합니다.

컴플라이언스 관리
국내 외 주요 컴플라이언스를 지원하고
Best Practice 및 커스텀 기능을 활용해
기업 별 보안 정책에 맞춰 컴플라이언스
를 관리합니다.

멀티 클라우드 API 연동
국내 외 퍼블릭 및 프라이빗
클라우드에 대한 API 연동을 통해
멀티 클라우드 환경을 관리합니다.

클라우드 보안 테크 기업 아스트론시큐리티와
함께 멀티 클라우드 환경에 맞는 보안을 구축하고
디지털 혁신을 경험하세요!

Think Secure!

ASTRON SECURITY

연락처 02-6930-5920
이메일 sales@astronsec.com
웹사이트 http://www.astronsec.com
주소 서울특별시 강남구 봉은사로 115 노벨테크 6F, 8F