Think Secure!

아스트론시큐리티 표준 소개서

ASTRON SECURITY

Rev. 2023-09-01

회사 소개

Chapter 1

Think Secure!

ASTRON SECURITY

회사 소개

No.1
클라우드 보안 기업
아스트론시큐리티

아스트론시큐리티는 AI 기반 클라우드 보안을 제공하는 국내 최초 클라우드 보안 기업입니다.

회사 소개

회사 명 ㈜아스트론시큐리티	대표자 조근석
주소 서울 강남구 봉은사로 115 노벨테크 6F	사업 분야 클라우드 보안, AI 보안
설립연도 2019. 03	직원 수 63명

기업 특징

01 국내 최초 클라우드 보안 기업

02 CNAPP 기반 통합 보안 기술 보유

03 국내 유일 클라우드 이벤트 기반 AI 보안 기술 보유

주요 투자사

NAVER CLOUD PLATFORM, AhnLab, KDB산업은행, KB Investment, LIGHTHOUSE, IBK기업은행, HYUNDAI, 아주IB투자, kibo 기술보증기금

누적 투자 금액
100억+

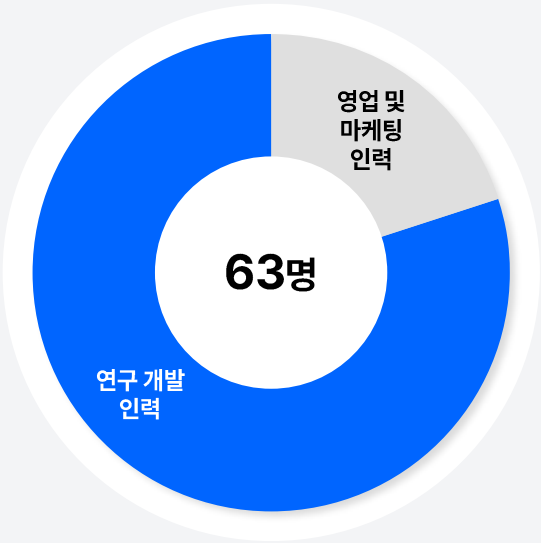
아스트론시큐리티 사업 분야

클라우드 보안	AI 보안	연구개발(R&D)
ASTRON-CWS (설치형 클라우드 보안)	AI-GUARDIAN (SaaS형 AI 보안)	클라우드 보안 관리를 위한 시스템 구축
ASTRON-GUARD (SaaS형 클라우드 보안)		클라우드 해킹 연구소 운영

조직 및 인력 현황

연구 개발 및 기술 인력
80%

영업 및 마케팅 인력
20%



회사 소개

No.1
클라우드 보안 기업
아스트론시큐리티

아스트론시큐리티는 클라우드 보안 선두 기술력을 기반으로 CNAPP 통합 보안 솔루션을 제공하고 있습니다.

특허 등록 및 출원 건수

총 12건	총 6건	총 8건	총 12건
국내	글로벌	AI 보안	클라우드 보안

인증 내역


KSM 등록 기업 확인서


CSAP 인증서


기업부설연구소


GS 인증서

수상 내역

넥스트라이즈
Innovation Prize

과기정통부장관상

중기부장관상


시큐리티어워드
코리아2021대상


시큐리티어워드
코리아2022 대상

아스트론시큐리티 보안 솔루션

설치형

ASTRON CWS

CSPM, CWPP, CIEM, CNS의 기능을
통합적으로 지원하는 CNAPP 기반
설치형 클라우드 보안 솔루션

주요 기능	
클라우드 자산 식별 및 시각화	컨테이너 현황 감시
취약점 진단 및 탐지	호스트 보안
계정 및 권한 시각화	클라우드 네트워크 시각화
최소 권한 관리	방화벽 정책 관리

SaaS형

ASTRON GUARD

CSPM 및 CIEM의 핵심 기능을 지원하는
SaaS형 클라우드 보안 솔루션

주요 기능	
클라우드 자산 식별 및 시각화	클라우드 네트워크 시각화
취약점 진단 및 탐지	계정 및 권한 시각화
VM 감시	

SaaS형

AI GUARDIAN

클라우드 내 이상 행위 탐지 및 대응을
지원하는 SaaS형 AI 보안 솔루션

주요 기능	
클라우드 이상 행위 탐지	MITRE ATT&CK 기반 이벤트 로그 관리
TI 기반 악성 IP 탐지	클라우드 이벤트 사전
쿼리 기반 커스텀 데이터 검색	

제품 소개

No.1
클라우드 보안 기업
아스트론시큐리티

아스트론시큐리티는 클라우드 보안의 핵심 기능을 하나의 솔루션에서 모두 제공합니다.

CSPM
- 자산 식별 및 시각화
- 컴플라이언스 취약점 진단 및 탐지
- 조치 가이드 제공

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

CIEM
- 계정 및 권한 시각화
- 최소 권한 관리

CNS
- 클라우드 네트워크 시각화
- 방화벽 정책 관리
- 정책 시뮬레이션 시각화

CDR
- 이상 행위 탐지
- 이벤트 로그 분석
- 악성 IP 탐지

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

클라우드 보안 시장 환경

Chapter 2

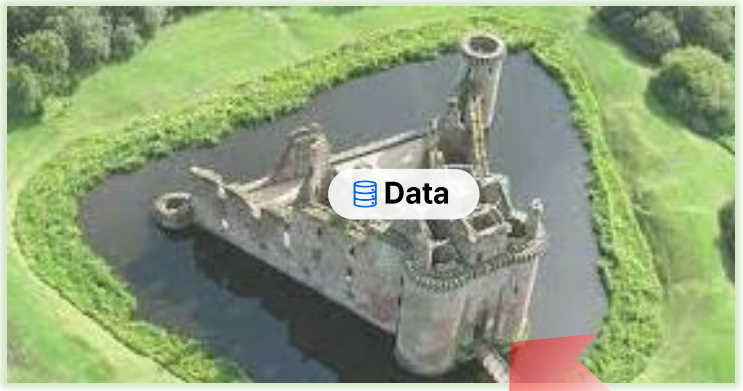
Think Secure!

ASTRON SECURITY

클라우드 보안 환경의 변화

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

전통적 IT 환경



- 개별 보안 관리 모델
- 경계선 보안

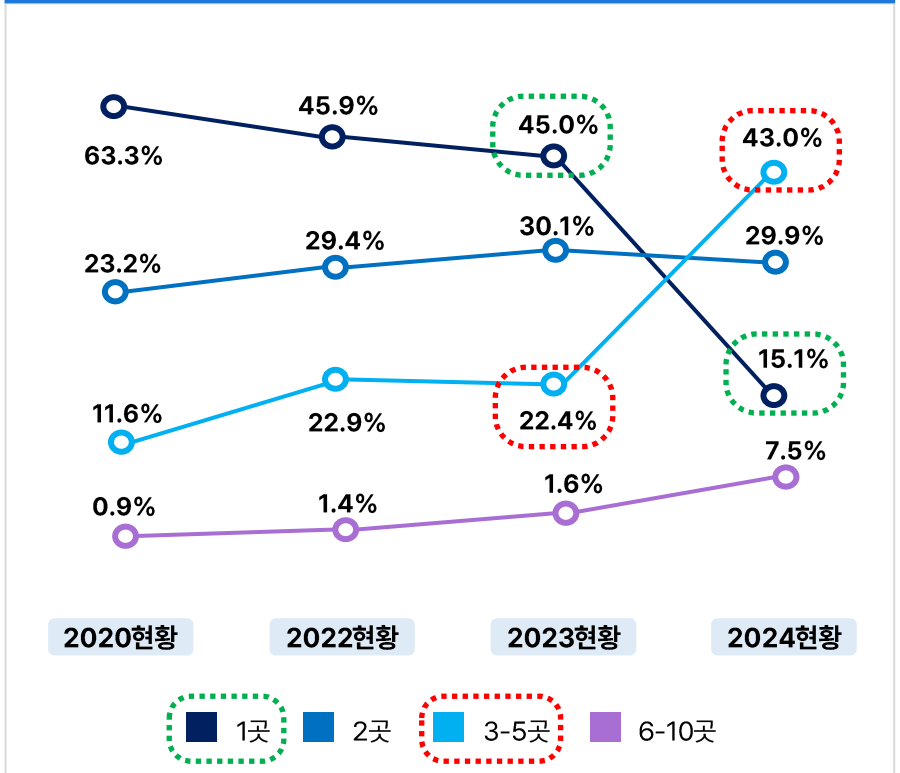
새로운 클라우드 환경

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

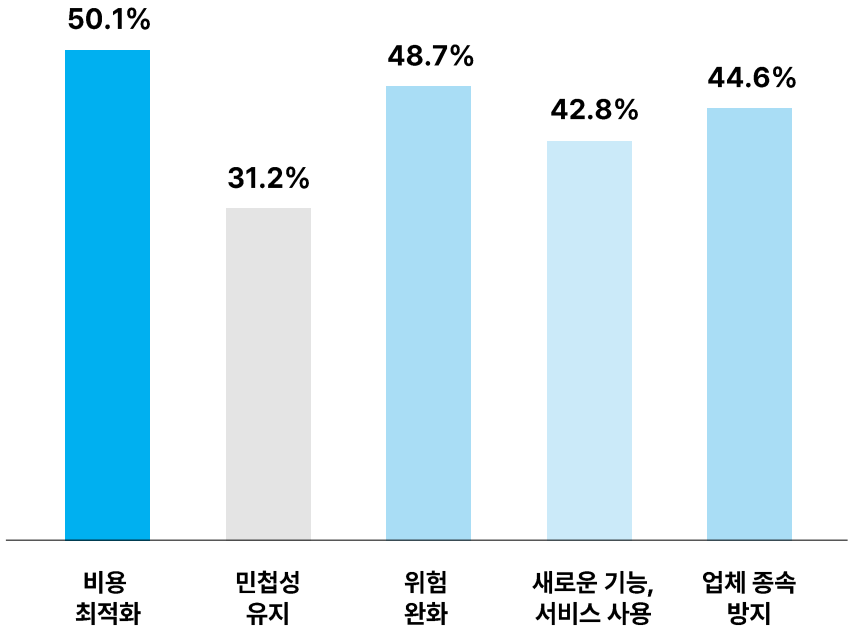
멀티 클라우드 도입 트렌드

멀티 클라우드를 이용하는 기업은 지속해서 증가 중이며, 특히 비용 최적화 및 위험 완화 측면에서 멀티 클라우드를 지향하고 있습니다.

기업별 멀티 클라우드 도입 전망



멀티 클라우드를 도입하는 이유

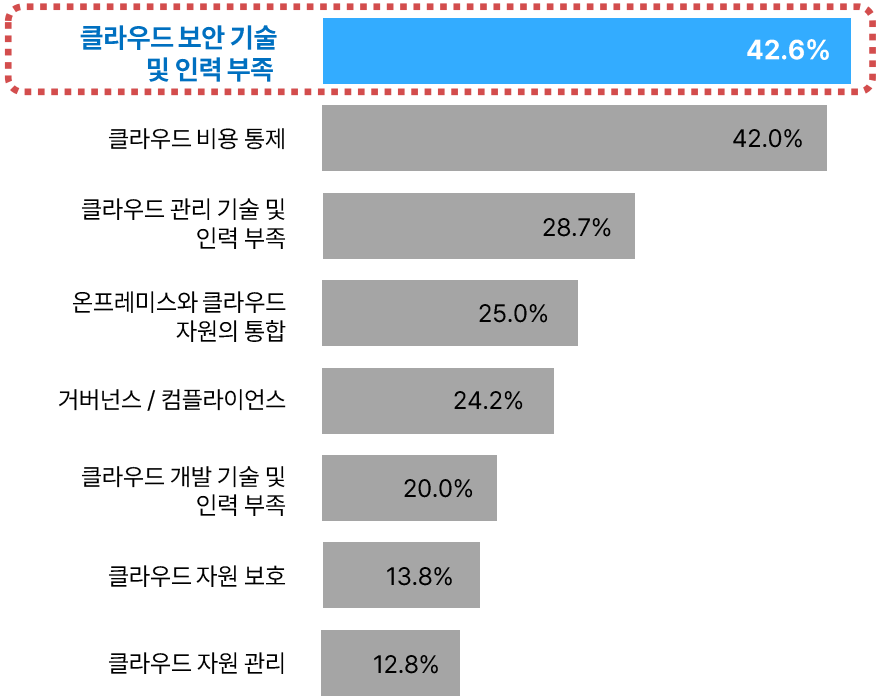


출처: 2023년 국내 클라우드 컴퓨팅 현황과 전망 IT World CIO

클라우드 환경의 보안적 문제점

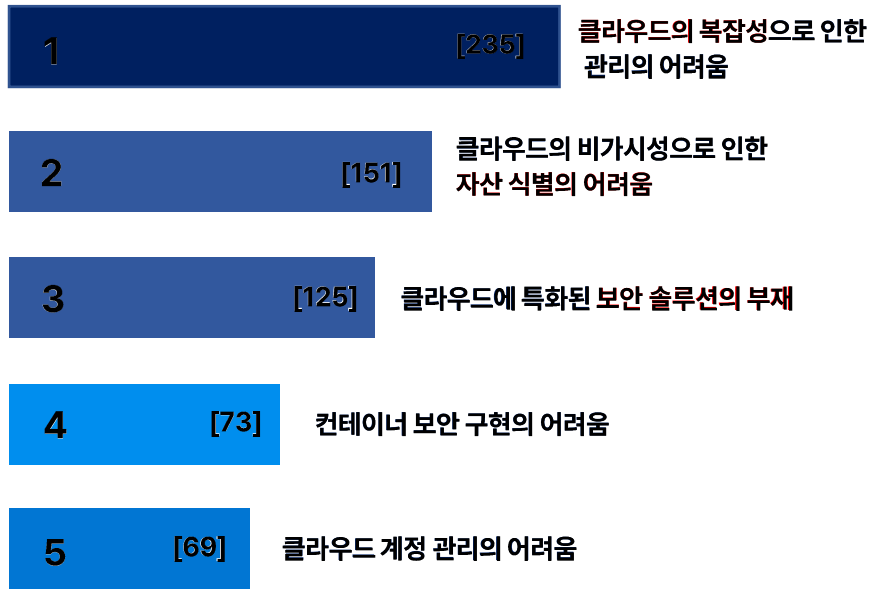
클라우드 도입을 저해하는 요인으로는 보안 기술 및 인력 부족 등을 꼽았으며 클라우드 환경의 가장 큰 보안적 문제점으로 복잡성으로 인한 관리의 어려움, 비가시성으로 인한 자산 식별의 어려움을 꼽았습니다.

Q1.클라우드 도입 및 활용 과정의 어려움은?



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

Q2.온프레미스 대비 클라우드 환경에서의 가장 큰 보안적 문제점은?



출처: 국제보안전시회 기업고객 설문조사, 총 475명 응답

클라우드 보안 사고 주요 원인

클라우드 보안 사고의 가장 큰 원인은 계정 탈취, 내부자 위협, 사용자 설정 오류 등이며 고도화된 보안을 적용하지 않을 경우 막대한 해킹 피해로 이어져 기업의 생존을 위협받을 수 있습니다.

클라우드 보안 위협 7가지

데이터 유출

계정 탈취

내부자 위협

사용자 설정 오류

클라우드 보안 아키텍처 도입 미흡

불안정한 인터페이스 및 API

신원, 엑세스 관리 미흡

클라우드 해킹에 의한 피해

출처 : IBM, 2022

중요 데이터 유출로 인한 피해 **기업당 평균 43억원**

웹사이트 무력화를 통한 **서비스 중지**

내부 시스템 다운으로 인한 **업무 마비**

내부 자원을 활용한 **채굴**

정부기관의 클라우드 네이티브 전환 추진

정부의 클라우드 네이티브 전환이 본격화됨에 따라 클라우드 네이티브 보안의 필요성이 증대되고 있습니다.

전자신문

2023.07.23. 오후 2:17 기사원문

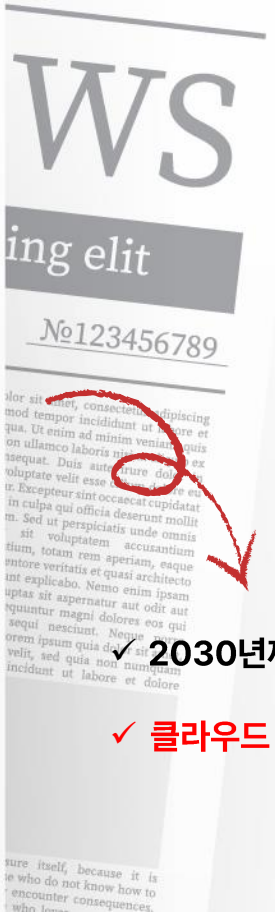
공공 클라우드 네이티브 전환 본격화 한다...부처, 지자체 등 준비 착수

주요 부처와 지방자치단체가 클라우드 네이티브 전환에 속도를 낸다. 연내 주요 계획·방향 등을 수립하고 내년부터 전환을 본격화한다는 방침이다.
21일 업계에 따르면 과학기술정보통신부, 관세청, 지자체 등이 클라우드 네이티브 전환 대응을 시작했다.

업계 관계자는 "주요 부처와 지자체에서 클라우드 네이티브 전환 컨설팅 등 문의가 최근 급증했다"라며 "올해 주요 계획을 마련하고 예산이 집행되는 내년부터 실제 사업이 발주 날 것"이라고 말했다.

클라우드 네이티브는 서버나 스토리지 등 인프라뿐만 아니라 아키텍처, 애플리케이션, 개발 환경까지 클라우드에 최적화한 상태로 구현하는 것을 의미한다.
개발자 생산성 향상은 물론 시스템 운용 시 민첩성, 가용성 등을 높일 수 있는 클라우드 성숙도 최고 단계다.

과기정통부는 부처뿐만 아니라 소속·산하기관 전반에 클라우드 네이티브 도입·확산을 위한 중단기 추진방안을 연내 도출한다.
공공부문 클라우드 네이티브 전환 방법부터 운영방법·운영비용 등 실무에 필요한 사항을 정리한다.
앞으로 7년간(2024년~2030년) 클라우드 네이티브 도입 관련 적용 방안을 마련한다.
△마이크로서비스 △컨테이너 △데브옵스 등 클라우드 네이티브 주요 구성요소별 단계적 도입 방안도 수립한다.

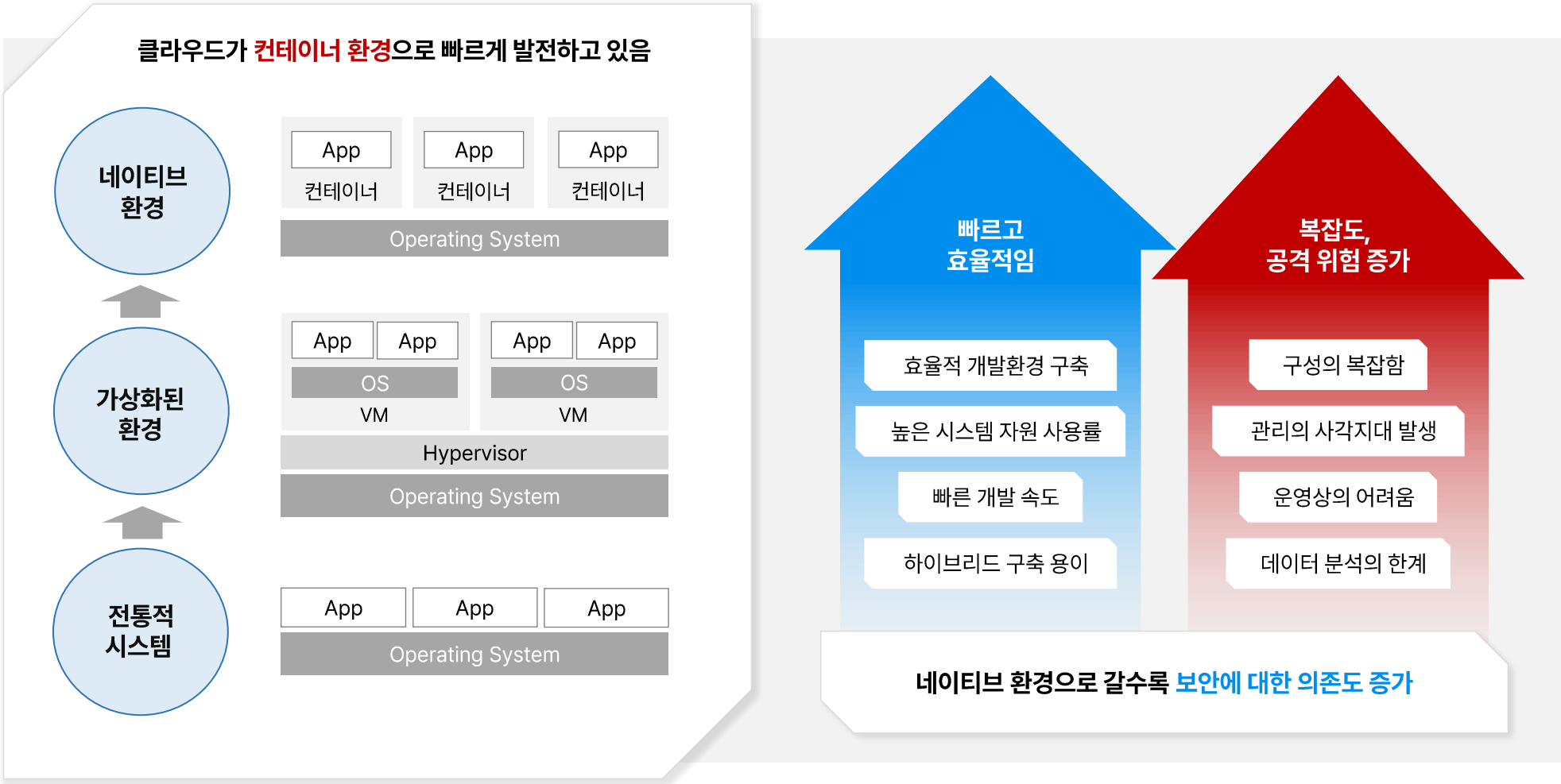


✓ 2030년까지 공공 기관의 **컨테이너 환경 전환 70% 목표**

✓ **클라우드 네이티브 보안 필요성 증대**

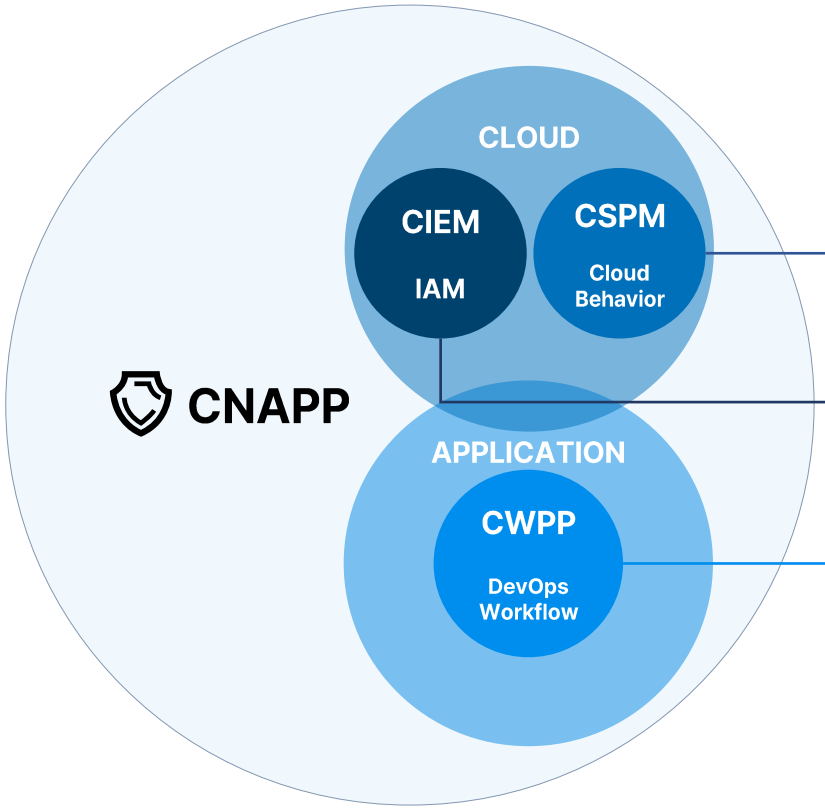
클라우드 네이티브 보안의 필요성

클라우드 네이티브 환경은 운영 효율이 좋아지는 반면 복잡성과 공격 위험도가 증가하여 보안의 사각지대가 발생합니다.



클라우드 보안 트렌드

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



출처: Gartner

CNAPP
(Cloud Native Application Protection Platform)

CSPM

자산 식별 및 시각화, 컴플라이언스에 따른 클라우드 인프라의 취약점 탐지, 조치 가이드 제공

CIEM

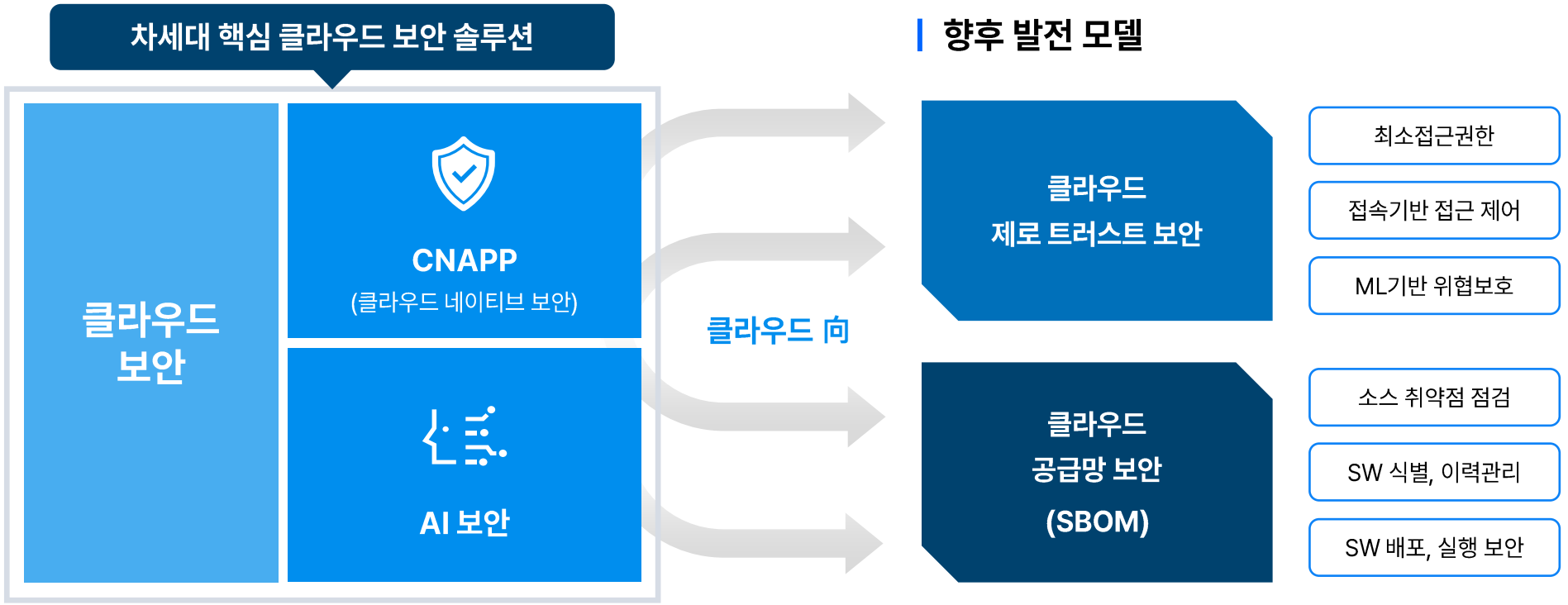
계정 및 권한 대한 관리, 시각화 / 최소권한 관리
지속적 모니터링을 통한 위협 탐지 및 보호

CWPP

개발부터 운영까지 클라우드 워크로드 보호
호스트 보안, 컨테이너 보안 등의 기능 지원

향후 클라우드 보안 발전 모델

**차세대 핵심 클라우드 보안 솔루션으로 CNAPP와 AI를 결합한 보안 솔루션이 주목받고 있으며,
최소 권한 관리를 기반으로 한 제로 트러스트 보안 및 SBOM 중심의 공급망 보안이 강화될 것으로 보입니다.**



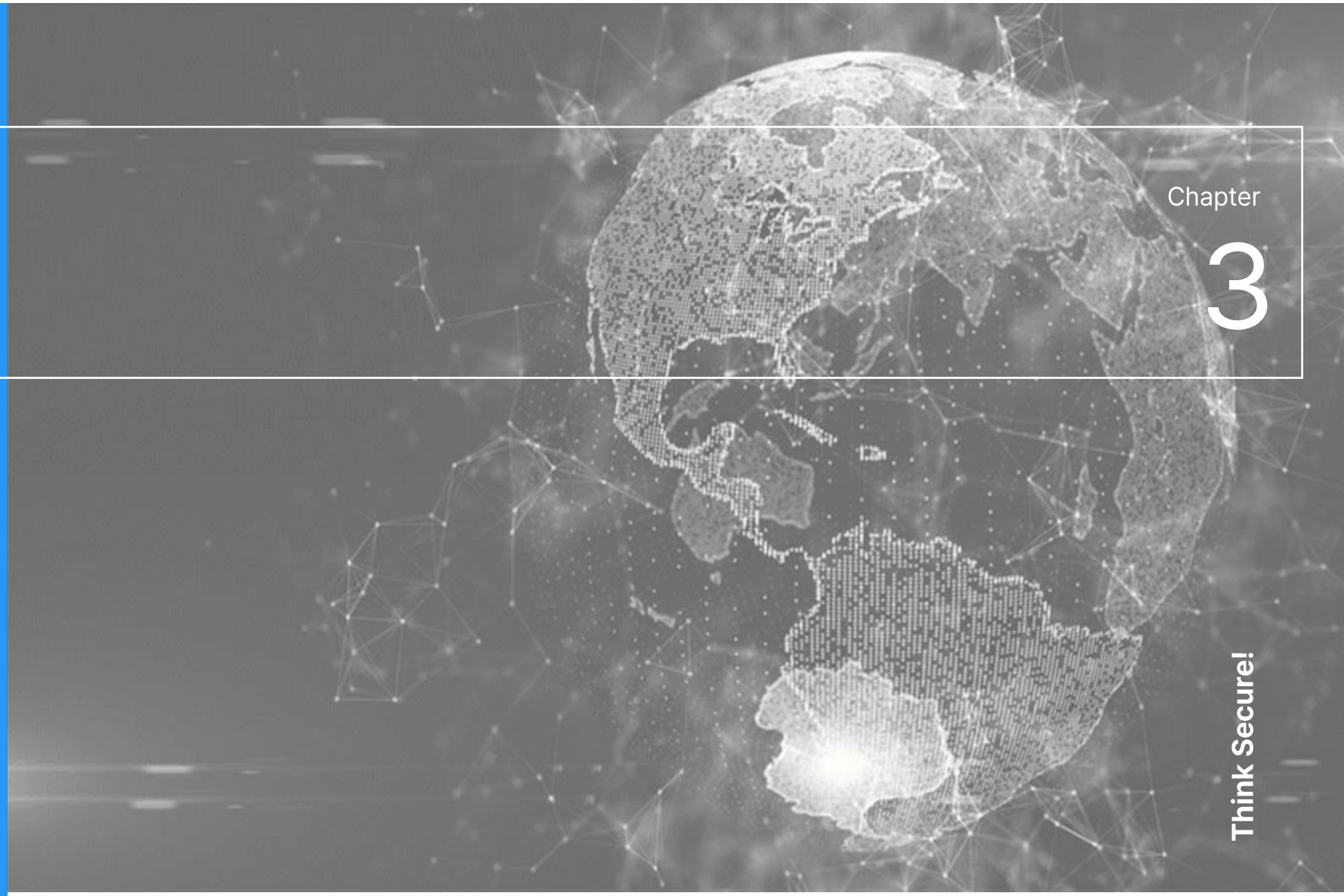
* CNAPP(Cloud Native Application Protection Platform)은
IaaS 보안, PaaS 보안, 컨테이너 보안을 모두 포함한 개념임

- SBOM (Software Bill Of Materials)
  최종 고객이 사용하는 소프트웨어 혹은 서비스를 완성하기 위해 활용되는 모든 소프트웨어 정보를 담고 있는 명세서

솔루션 특장점

Chapter

3



Think Secure!

ASTRON SECURITY

솔루션 특장점(1)

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

클라우드 보안의 단계별 필수 기능

CSPM 01

- **클라우드 시각화**
  실시간 데이터 현행화
- **토폴로지 시각화**
  보안 연결상태 확인
- **자산 자동 식별**
  호스트, 컨테이너, APP
- **변동 내역 관리**
  현황, 구성, 상태 등
- **취약점 점검 및 실시간 진단**
  조치 이행 관리
- **컴플라이언스 관리**
  Best Practice 및 커스텀 기능 지원

CIEM 02

- **계정 권한 시각화**
  계정, 접근 권한, 구성 시각화
- **최소 권한 관리**
  권한 변경, 상승, 미사용 계정 탐지

CWPP 03

- **호스트 보호**
  서비스 감시
  상태 감시
  애플리케이션 감시
- KSPM(쿠버네티스 보안 형상 관리) → **쿠버네티스, 컨테이너 보호**

CNS 04

- **클라우드 네트워크 시각화**
  마이크로세그멘테이션 기반
  네트워크 시각화
- **클라우드 네이티브 방화벽 관리**
  정책 변경 감시

CDR 05

- **AI 기반 이상행위 탐지**
- **이벤트 로그 관리**
- **TI 기반 악성 IP 탐지**

솔루션 특장점(2)

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

솔루션 특장점(3)

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

지원 컴플라이언스

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

솔루션 주요 기능

ASTRON SECURITY

ASTRON-CWS 01

CSPM

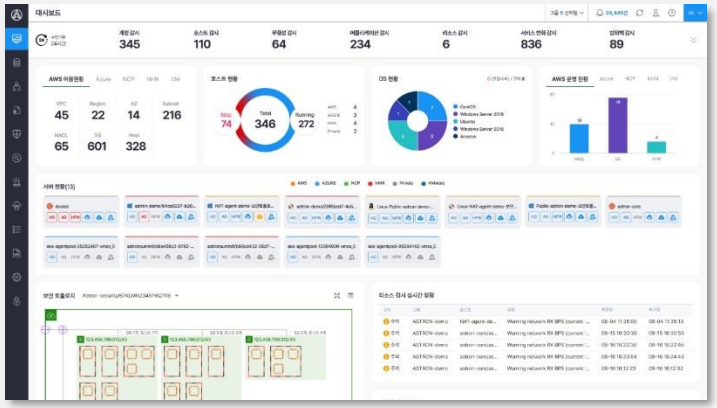
클라우드 환경이 복잡해짐에 따라 보안 사고로 이어지는 설정 오류를 미리 탐지하고 예방하는 것은 점점 더 어려워지고 있습니다.

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

01. CSPM

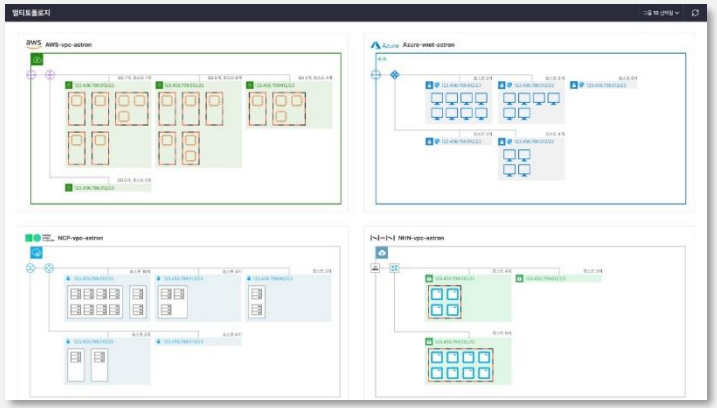
정교한 클라우드 시각화를 통해 리소스 변동 현황을 한눈에 파악하고 관리합니다.

멀티 클라우드 시각화



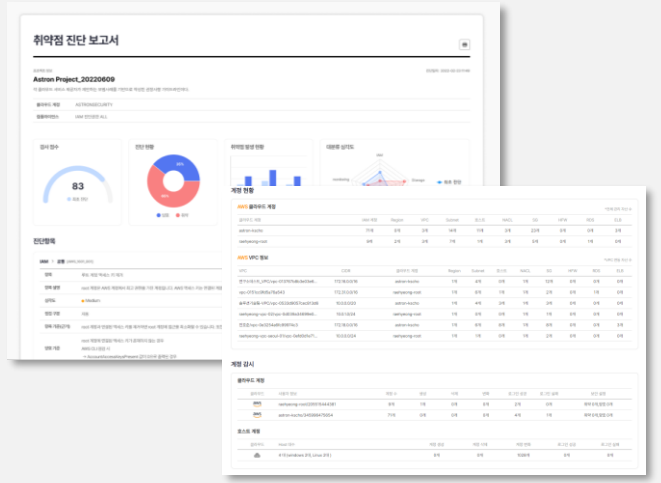
국내·외 주요 멀티 클라우드 환경을 지원하여 클라우드 보안 및 운영 상태를 통합적으로 관리합니다.

멀티 토폴로지



호스트, 에이전트, 방화벽에 대한 연결 상태를 클라우드 별로 확인합니다.

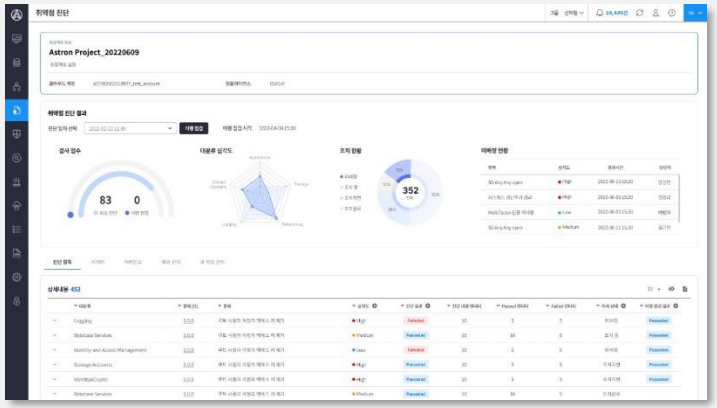
자산 및 취약점 진단 보고서



컴플라이언스 진단 보고서, 클라우드 자산 현황 보고서 등 다양한 형태의 보안 점검 보고서를 커스텀 방식으로 제공합니다.

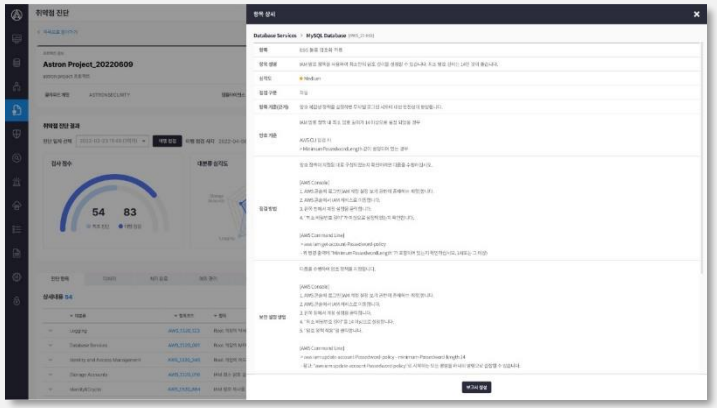
실시간으로 컴플라이언스 취약점을 탐지하고 조치 가이드를 제공하여 클라우드 보안 상태를 지속적으로 점검합니다.

실시간 취약점 탐지 및 자동 진단



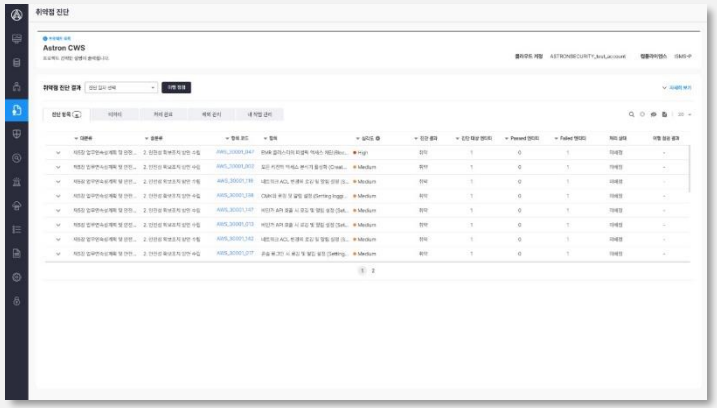
실시간으로 컴플라이언스 취약점을 탐지하고 설정 주기에 따라 자동화된 진단을 시행하여 클라우드 위험을 지속적으로 관리합니다.

조치 가이드



발생한 컴플라이언스 취약점에 대한 조치 가이드를 제공하여 보안 위협을 원활하게 관리합니다.

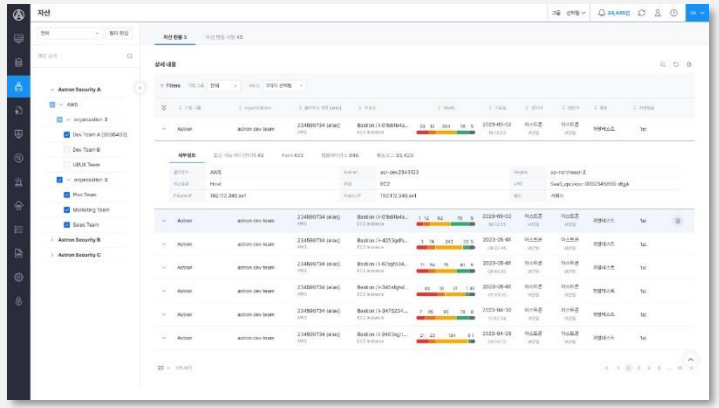
담당자별 이행점검



점검 결과에 따른 담당자 지정 및 이행 점검을 통해 취약점에 대한 조치 결과를 확인할 수 있습니다.

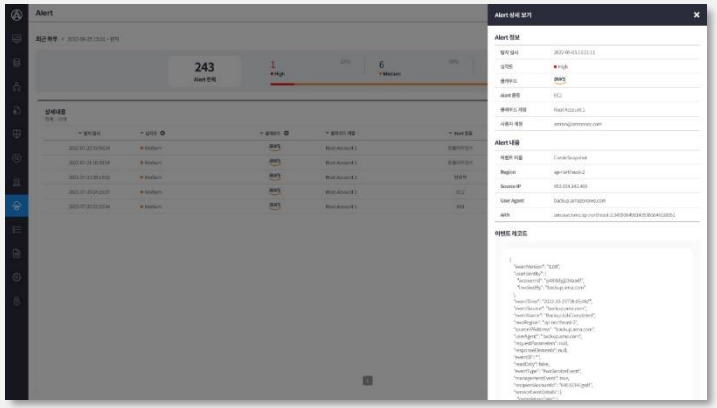
다양한 클라우드 자산을 식별하고 변동 상황에 따라 얼럿을 제공하여 클라우드 위협을 사전에 방지합니다.

클라우드 자산 식별



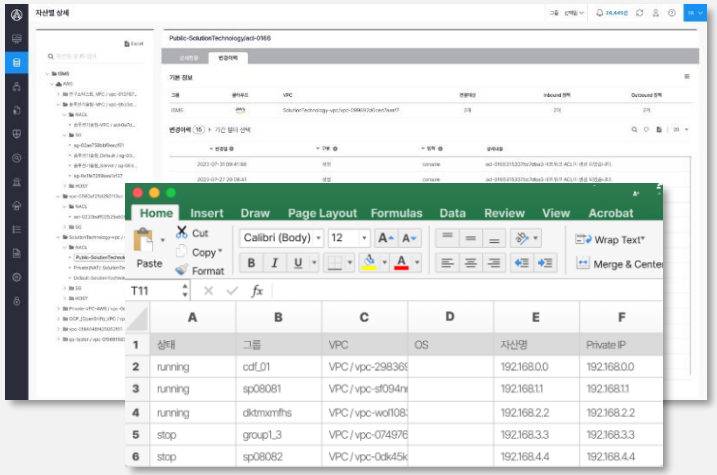
약 40여개의 AWS 주요 자산에 대한 상세 정보 및 변동 사항을 제공합니다.

변동 상황에 대한 얼럿 제공



취약점 자동 점검 및 자산의 생성·변경·삭제에 대한 현황을 얼럿으로 제공하여 변동 사항을 식별합니다.

자산 변경에 대한 로그 제공



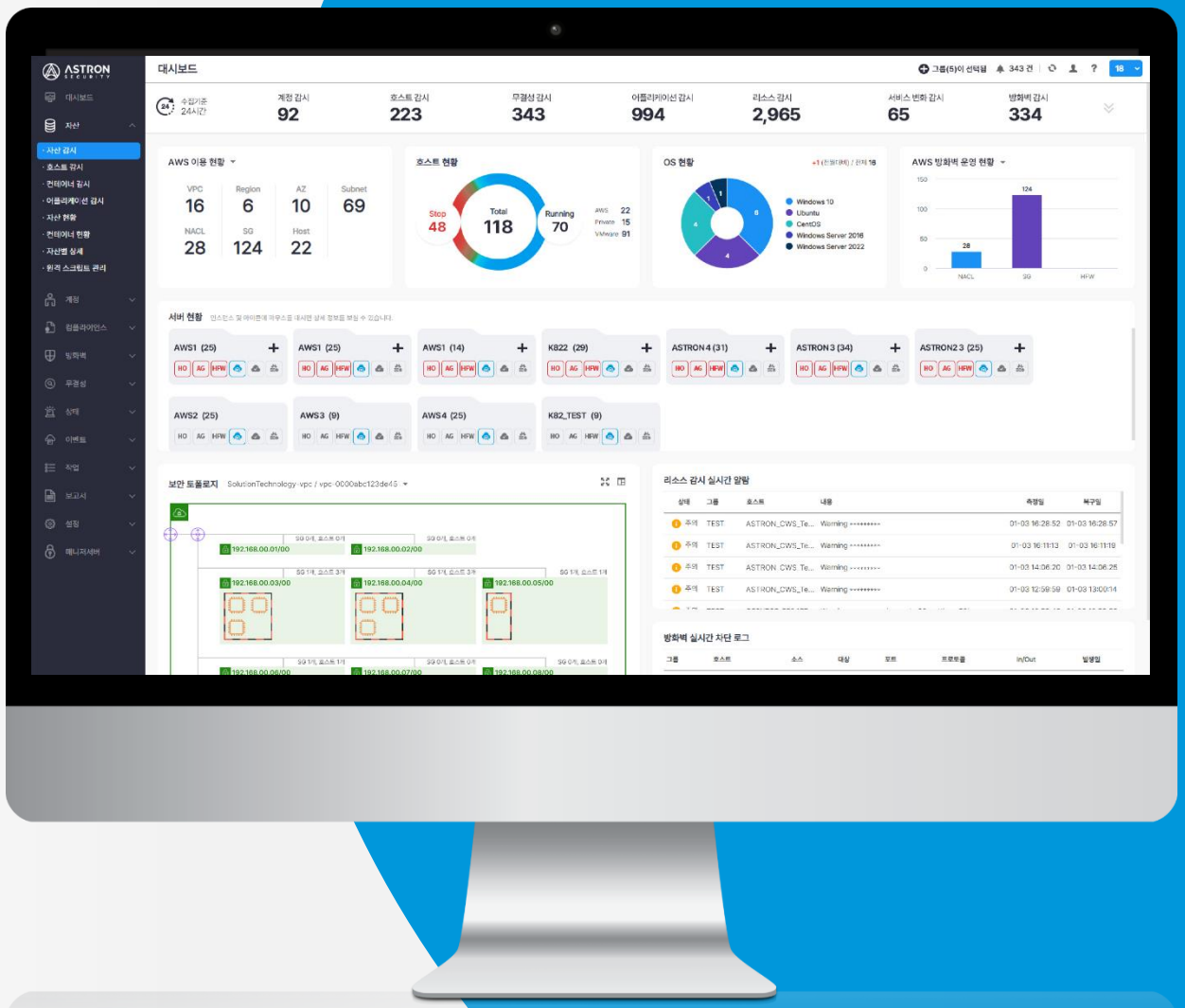
자산의 변동 내역에 대한 로그를 제공하고 이를 엑셀 및 보고서 형태로 다운로드할 수 있습니다.

ASTRON-CWS 02

CWPP

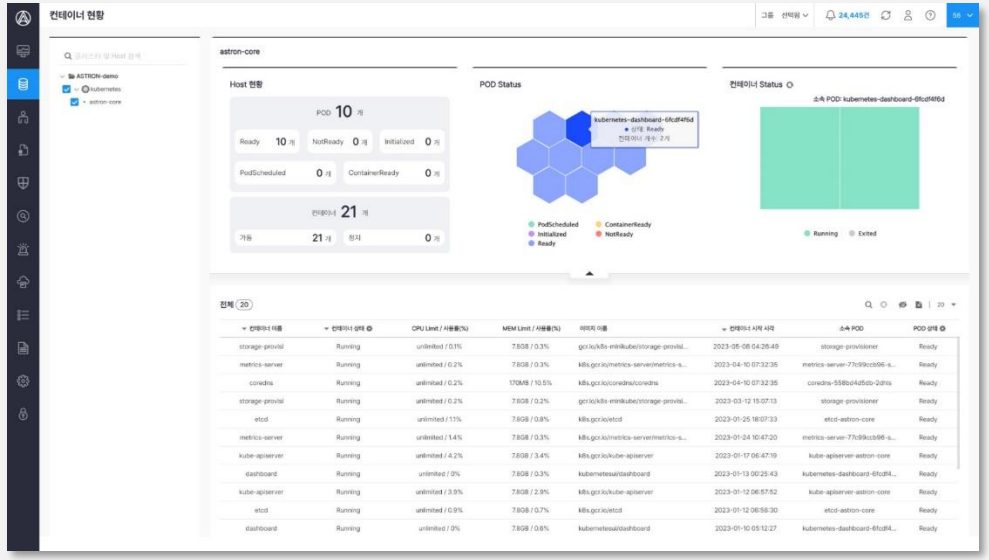
컨테이너 네이티브 환경으로 인해 워크로드별 보안 요구 사항이 다양해짐에 따라 일관된 보안 관리가 어려워지고 있습니다.

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



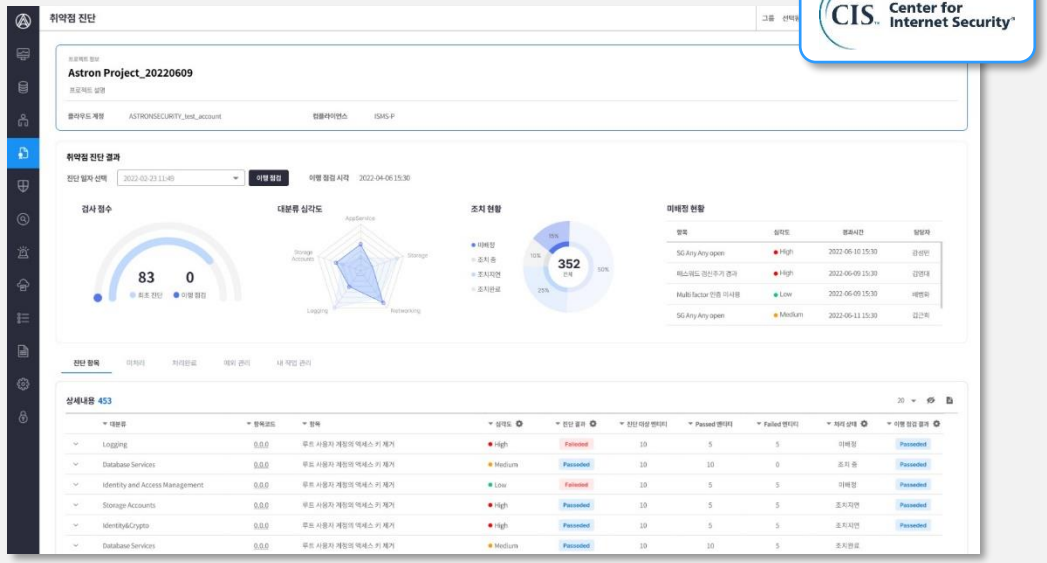
컨테이너 현황을 실시간으로 시각화하고 쿠버네티스용 컴플라이언스에 따라 취약점을 점검합니다.

컨테이너 시각화



클러스터 내 호스트 및 POD를 시각화하고 컨테이너 상태 및 현황에 대한 정보를 제공합니다.

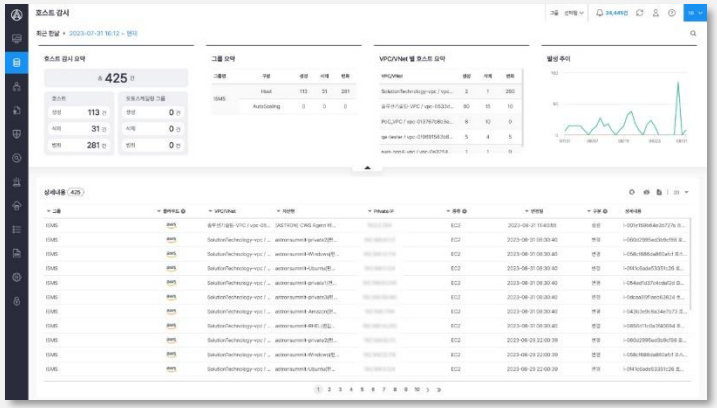
쿠버네티스 취약점 진단 및 탐지



CIS Kubernetes Benchmark에 따라 쿠버네티스 취약점을 실시간으로 탐지하고 기업별 보안 정책에 맞춰 커스텀 컴플라이언스를 생성합니다.

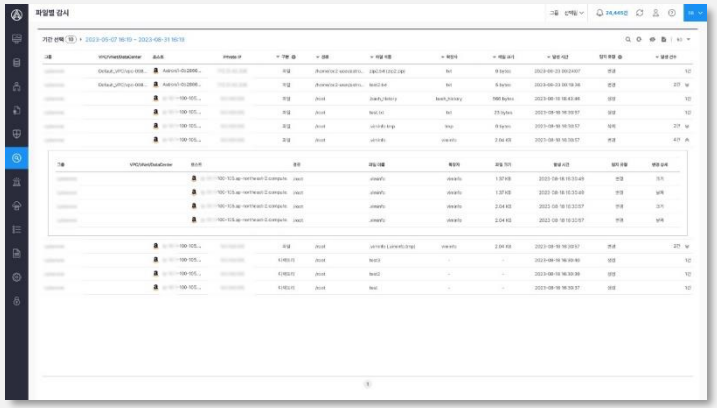
호스트 자산 및 계정 변동 현황에 대한 상세 정보를 제공하고 실시간으로 파일 무결성을 감시합니다.

호스트 변동사항 식별



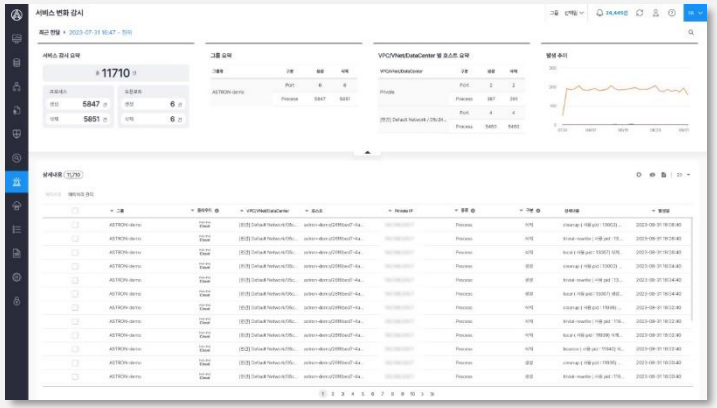
VM에서 생성된 호스트 및 애플리케이션에 대한 생성, 수정, 삭제 및 상세정보를 확인할 수 있습니다.

무결성 감시



실시간으로 파일 및 디렉토리의 요약 정보를 확인하고 변동사항을 모니터링합니다.

상태 감시



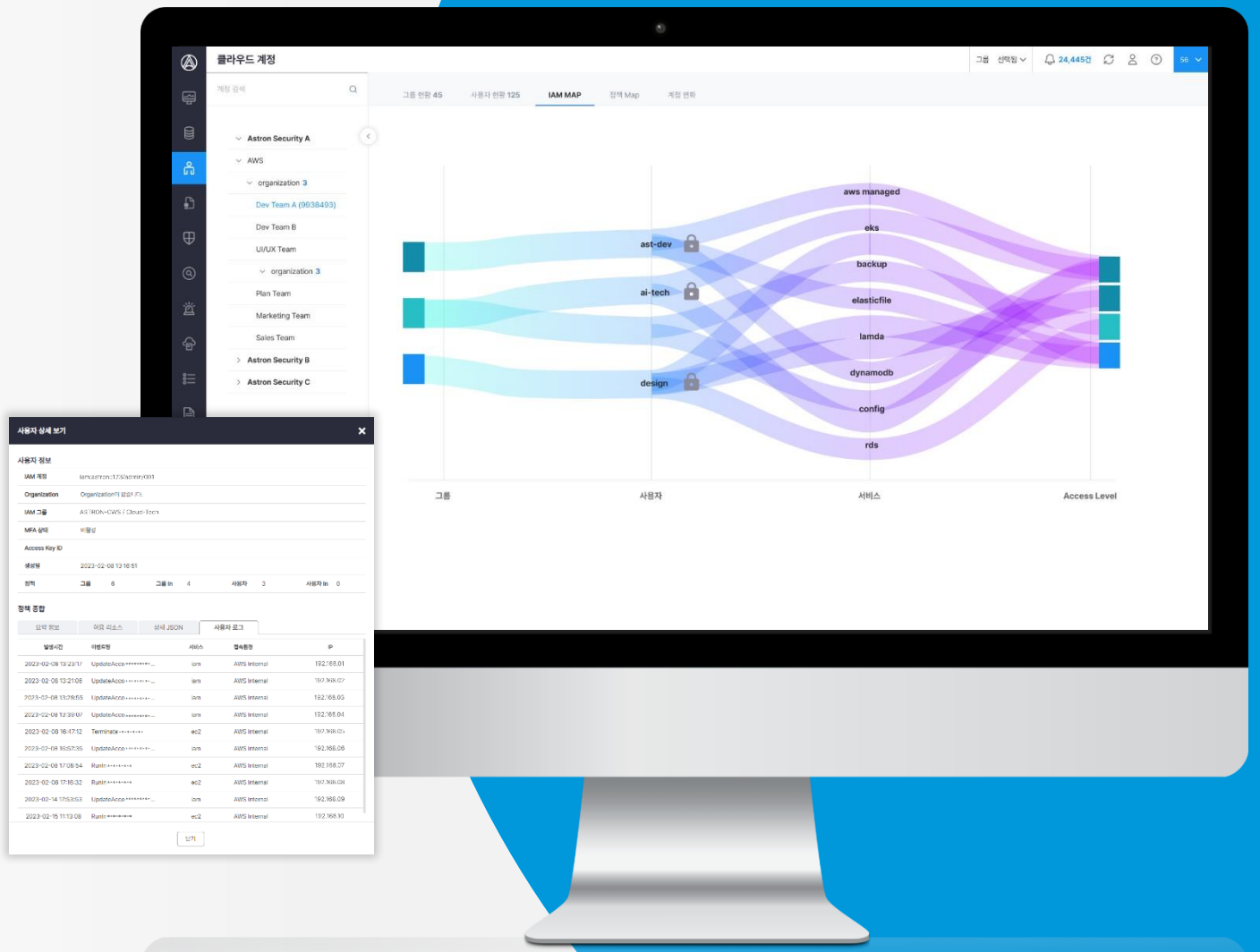
호스트 내 포트 및 프로세스에 대한 모니터링 기능을 제공합니다.

ASTRON-CWS 03

CIEM

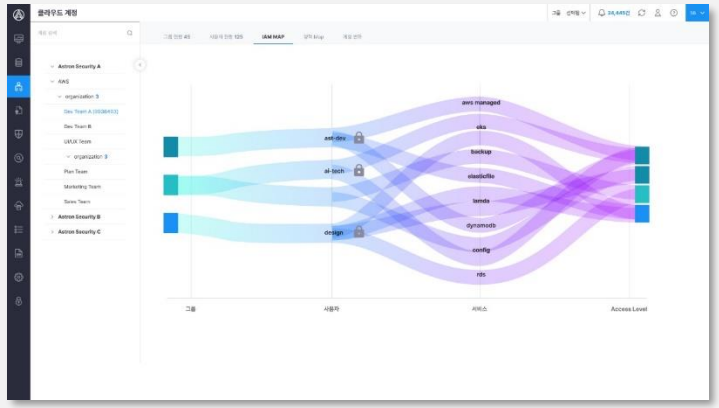
클라우드 인프라의 가장 큰 위험은 기업 '밖'이 아닌 '안'에 있습니다. 기업을 노리는 해커들은 민감한 데이터에 접근하기 위해 IAM 권한을 악용합니다.

ASTRON-CIEM은 클라우드 계정 및 권한에 대한 위협을
실시간으로 탐지하여 과도한 권한 및 설정 오류를 신속하게 파악하고
최소한의 권한으로 계정을 관리할 수 있습니다.



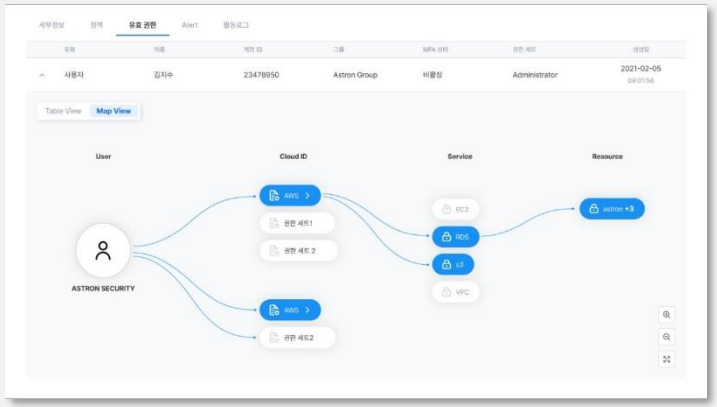
IAM, Identity Center, Organizations 현황을 분석하여 계정 및 권한을 시각화합니다.

IAM



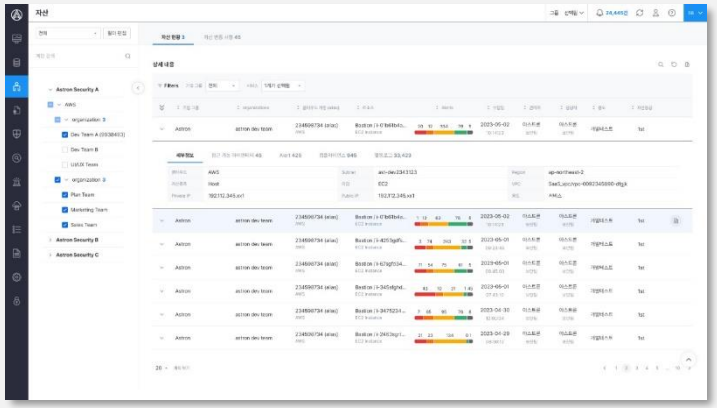
그룹, 사용자, 정책, Access Level에 따른
유효 권한을 시각화합니다.

Identity Center



IAM Identity Center의 유효 권한을 Map 및
테이블 형태로 시각화합니다.

Organizations

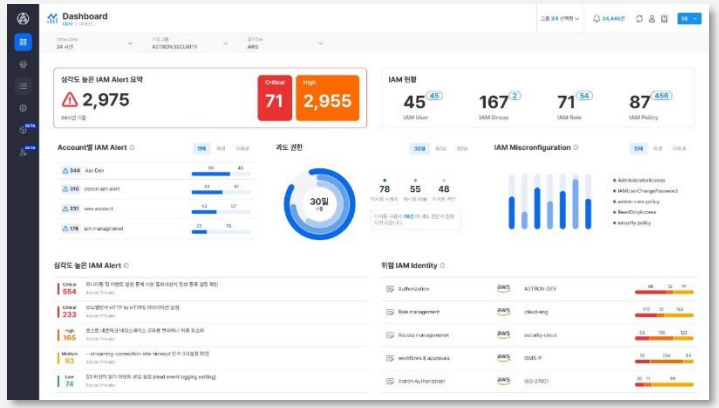


Organizations 구조에 따른 클라우드 계정별 리소스
목록을 시각화합니다.

03. CIEM

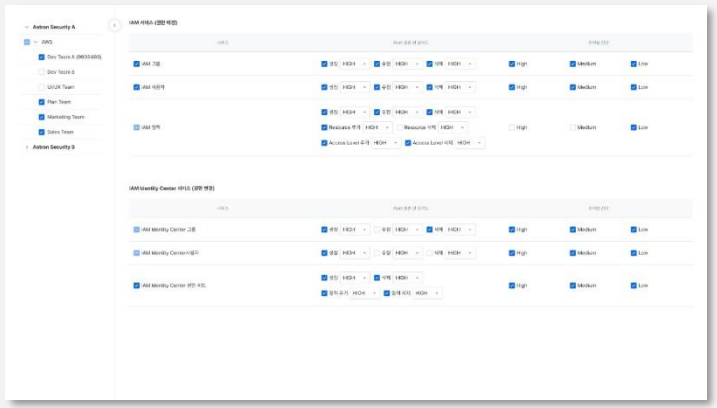
미사용 계정 및 권한 상승 계정을 실시간으로 탐지하고 위험 계정에 대한 얼럿을 제공하여 권한에 대한 위협을 파악합니다.

CIEM 통합 대시보드



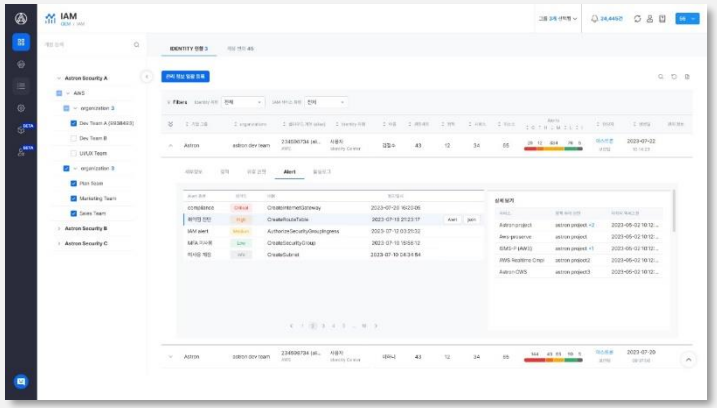
CIEM 전용 대시보드를 제공하여 계정 및 권한 위협을 한눈에 파악하고 관리합니다.

Identity Center 현황 변동 시 얼럿 제공



IAM Identity Center의 그룹 및 사용자 권한 세트의 생성, 수정, 삭제 시 얼럿을 제공합니다.

IAM 심각도에 따른 얼럿 제공



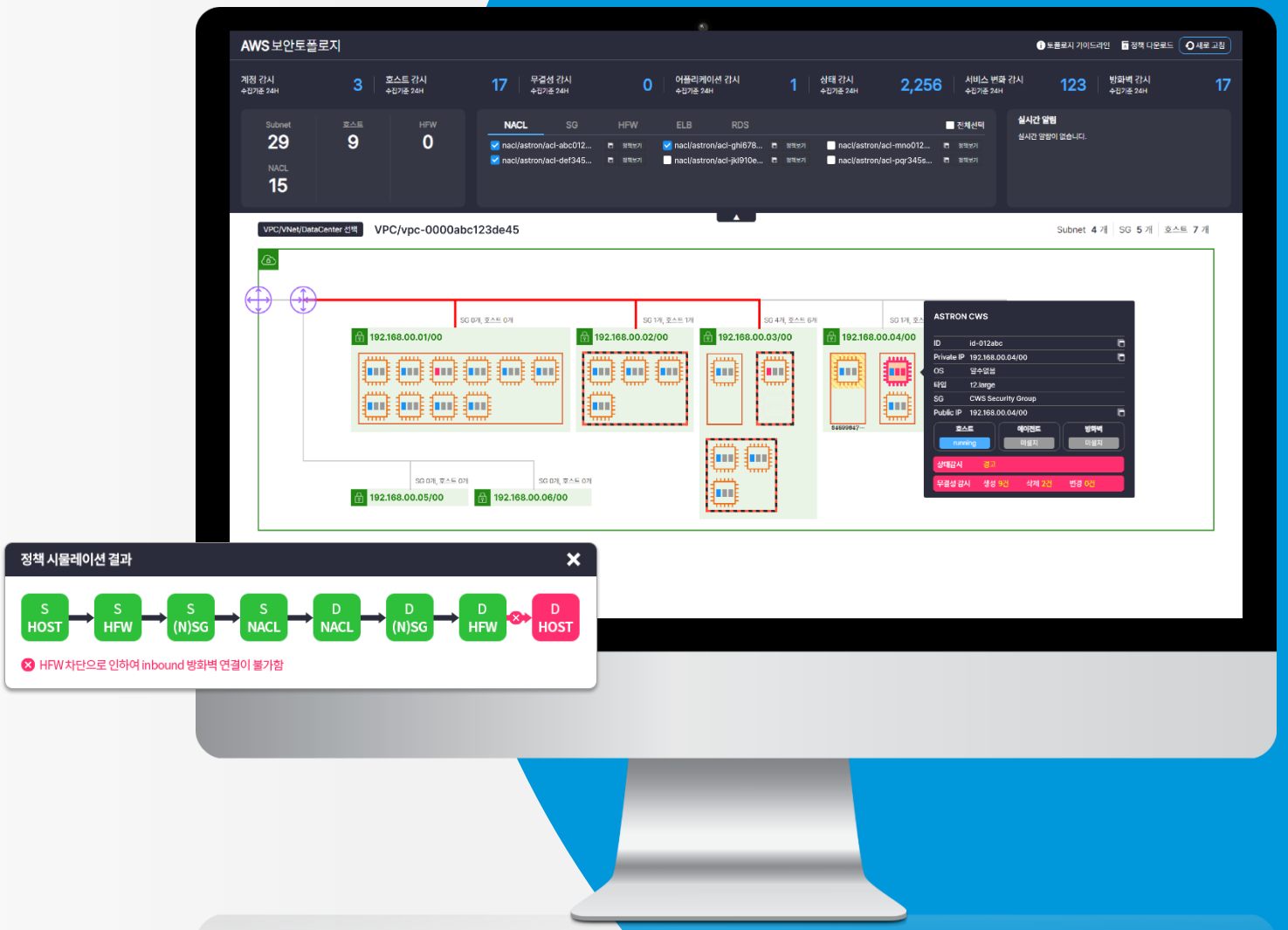
IAM 심각도에 따라 얼럿 현황을 제공하고 위험 계정에 대한 상세 정보를 확인합니다.

ASTRON-CWS 04

CNS

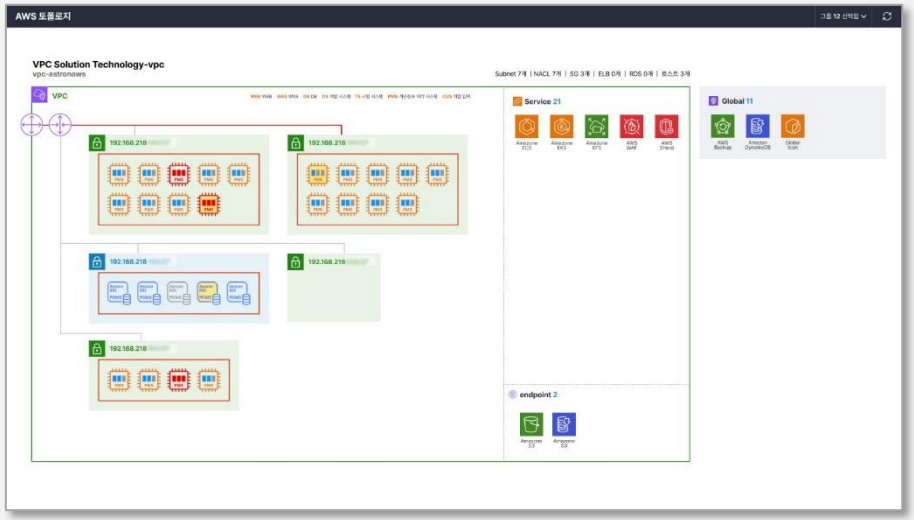
빠르게 변화하는 클라우드 환경에서 네트워크 위협을 효과적으로 탐지하고 보호하는 것은 매우 어렵습니다.

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



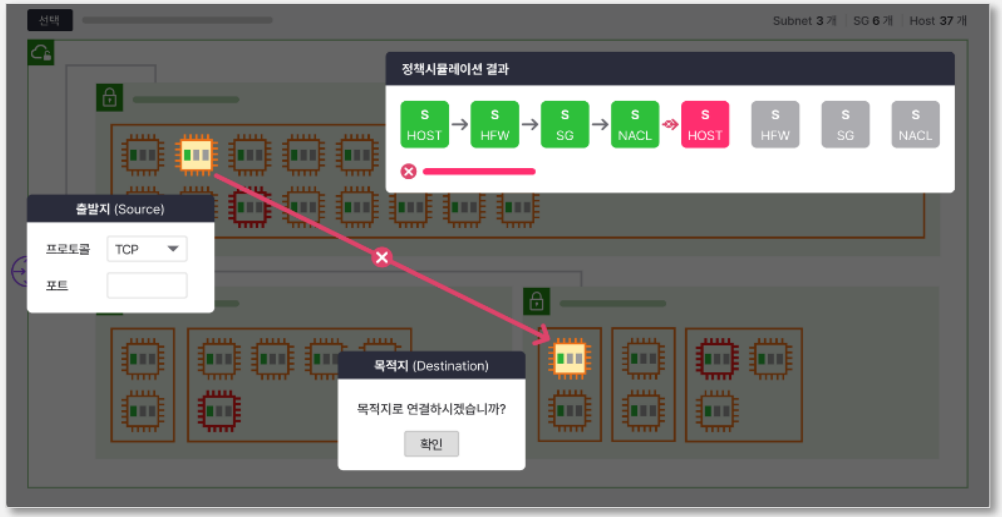
마이크로세그멘테이션 기반 네트워크 시각화를 통해 클라우드 내부의 위협을 탐지합니다.

마이크로세그멘테이션 기반 네트워크 시각화



마이크로세그멘테이션 기반 East-West 트래픽에 대한 가시성을 확보하고
클라우드 네트워크 계층 구조를 실시간으로 파악할 수 있습니다.

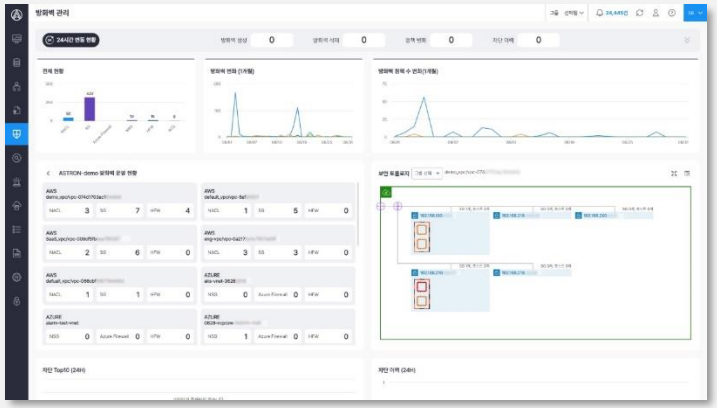
방화벽 정책 시뮬레이션



정책 시뮬레이션을 통해 호스트 간 방화벽 연결 가능 여부를 미리 파악하고
부적합할 시 수정할 수 있습니다.

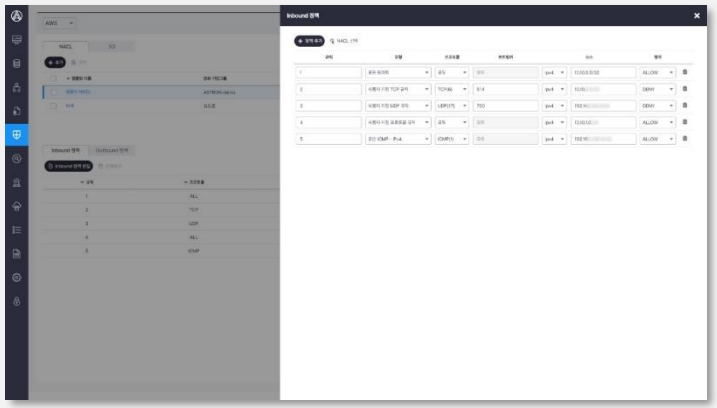
다양한 방화벽 정책 편집 기능과 얼럿 제공을 통해 효율적으로 방화벽 정책을 관리할 수 있습니다.

방화벽 정책 관리



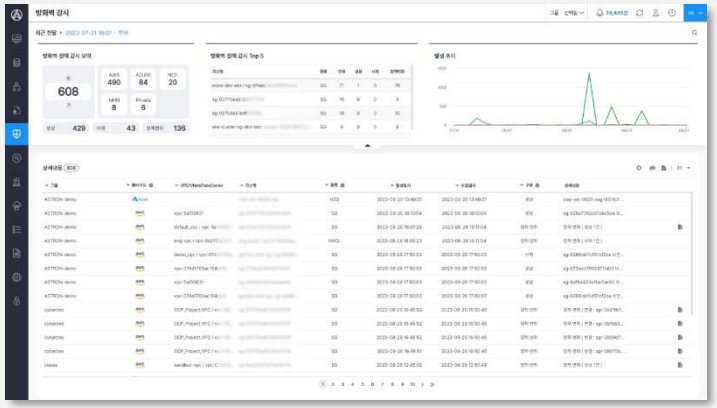
방화벽 정책 변동 현황을 한눈에 확인하고
정책의 생성,수정,삭제를 통해
효율적으로 정책을 관리할 수 있습니다.

방화벽 정책 템플릿



정책 템플릿을 미리 작성하여
방화벽 정책 설정 시 쉽게 적용할 수
있습니다.

방화벽 알림 및 로그



방화벽 정책이 변동될때마다 알람을 제공하고
방화벽에 대한 차단 및 허용 로그를 수집하여
변동 내역을 확인합니다.

ASTRON-CWS 05

ISMS

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

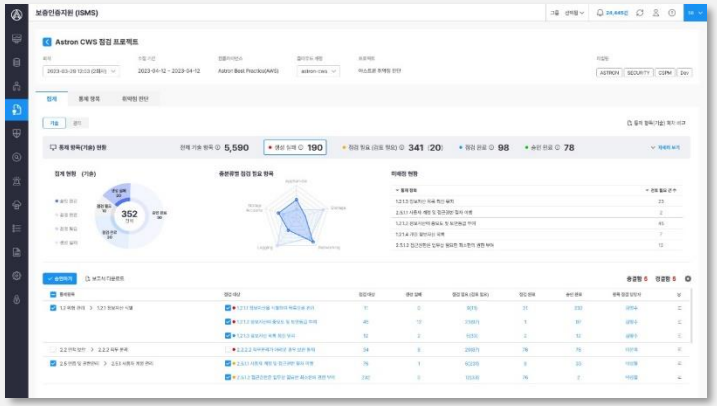
ASTRON-ISMS는 정책 자동 점검 및 조치 가이드 제공을 통해
클라우드 환경에서의 ISMS 인증을 자동화하여
보안 담당자의 인증 관련 시간과 비용을 절감시킵니다.

05. ISMS

기술적 영역 | 관리적 영역

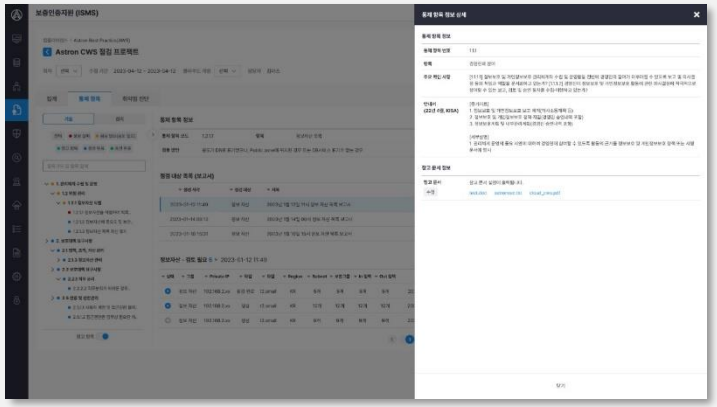
기술적·관리적 영역에 대한 ISMS 인증 지원 기능을 통해 체계적인 인증 관리 프로세스를 수립할 수 있습니다.

정책 자동 점검



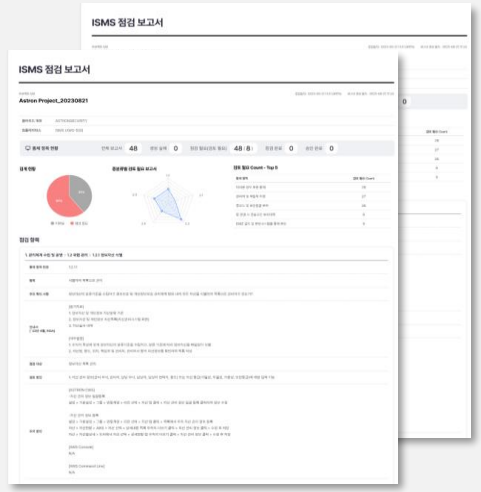
약 300여개의 ISMS 인증 항목 관련 정책을 자동으로 점검합니다.

조치 가이드 제공



ISMS 통제 항목에 대한 정책을 자동으로 점검하고 부적합할 시 조치 가이드를 제공합니다.

커스텀 보고서 지원



ISMS 통제 항목 점검 보고서를 회차별로 제공하고 보고서 열람 대상 및 진단 항목에 따라 커스텀 보고서를 제공합니다.

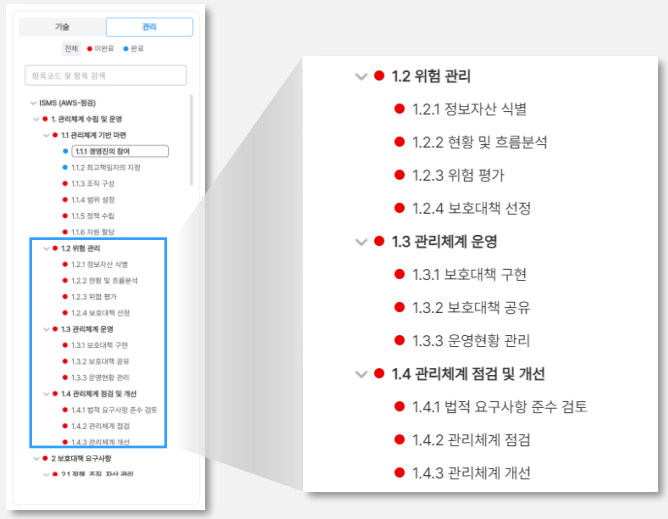
05. ISMS

기술적 영역

관리적 영역

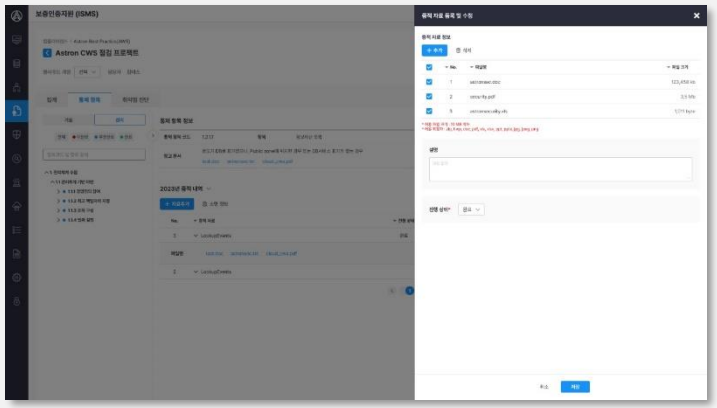
기술적·관리적 영역에 대한 ISMS 인증 지원 기능을 통해 체계적인 인증 관리 프로세스를 수립할 수 있습니다.

관리 통제항목 지원



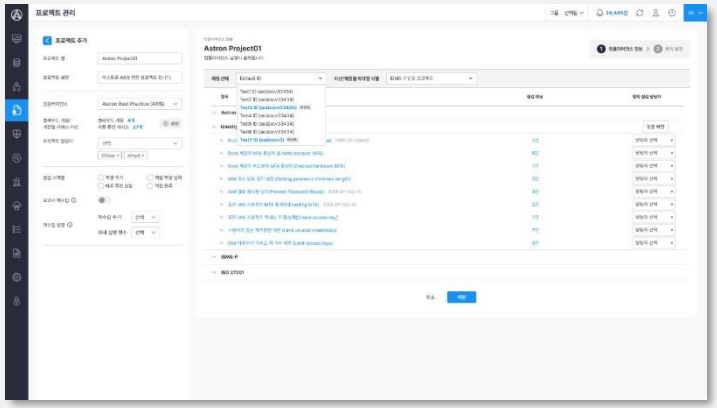
ISMS 관리적 통제항목을 모두 지원합니다.

문서 관리



관리 통제항목에 관한 문서를 별도로 업로드하여 관리합니다.

담당자별 점검 이력 관리

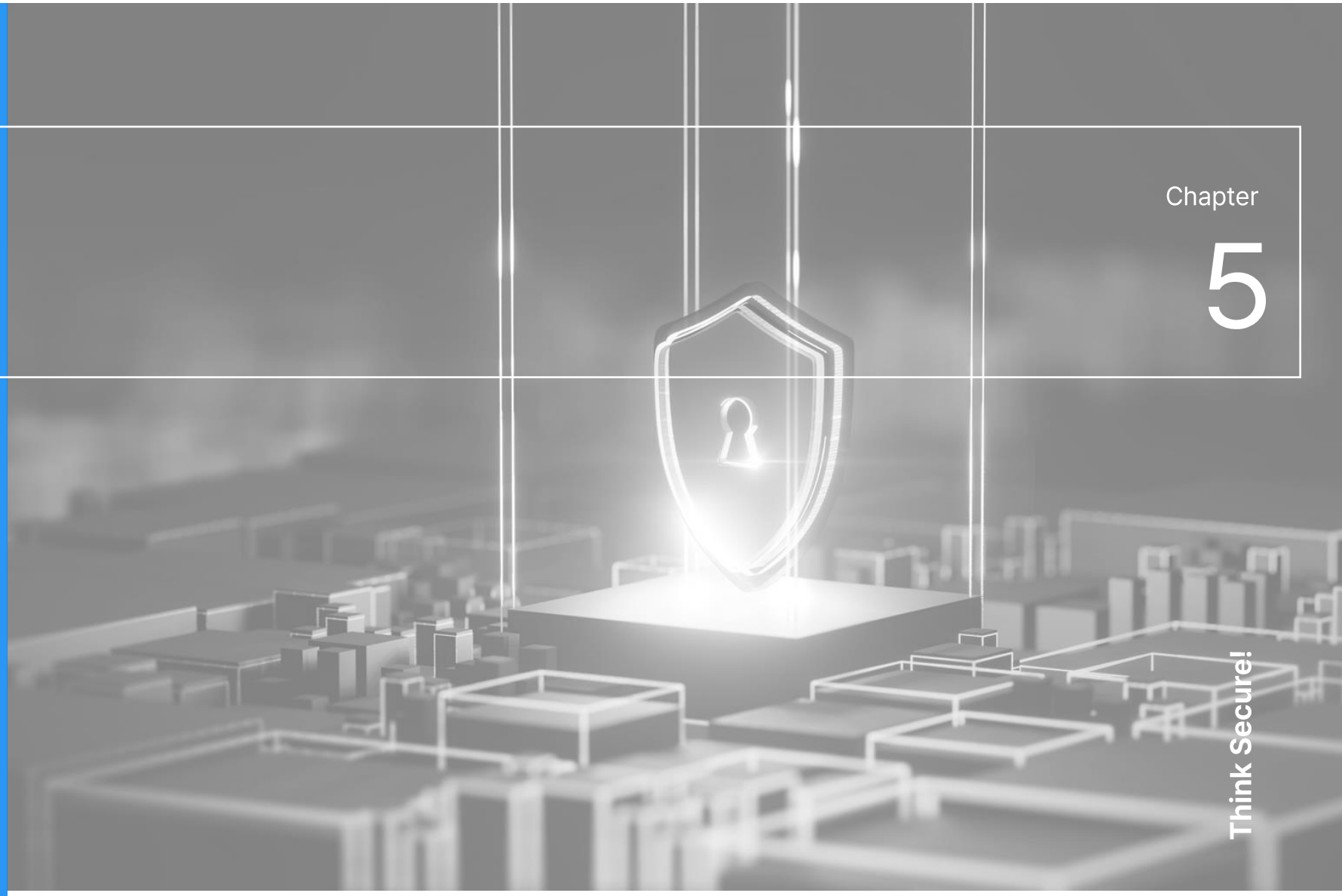


ISMS 인증 시 담당자별 이력 관리가 가능하여 정보 보호 담당자 변경 시에도 원활한 업무 수행이 가능합니다.

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

보안 구축 사례 – C 은행

"C 은행은 성공적인 클라우드 보안통제 솔루션 구축을 통한 안전한 클라우드 서비스 환경을 구현하였습니다"

Industry : 금융
기업 규모 : 은행

- AWS 클라우드를 이용 중이며 멀티 클라우드로 확대 예정
- 클라우드 내부 보안 강화 및 서버리스 서비스에 대한 보안 확보 필요

Challenges

- 클라우드 보안 위협에 대한 사전 예방 필요
- 리소스의 취약한 설정에 대한 오류 점검을 통해 침해 사고 발생 방지 필요

Solution

- 클라우드 자산 식별 및 실시간 취약점 탐지
- 계정 및 권한 시각화, 최소 권한 관리를 통한 실시간 위협 탐지
- 컴플라이언스 점검 결과에 대한 조치관리 기능으로 효율적인 취약점 통제
- 클라우드 운영환경에 최적화된 자산 및 SW 수집으로 보안 강화
- CNAPP 기반 통합 보안 적용

솔루션 구축 절차

Chapter

6

Think Secure!

ASTRON SECURITY

솔루션 구축 절차

SaaS형

회원 가입 → 1달 무료 Trial → 솔루션 구독 신청 → 클라우드 계정 연동 → 솔루션 이용 → 솔루션 도입 시간 5분

설치형

POC 시행 (1-2주) → 데모 계정 생성 및 테스트 (1일) → 계약 (3일 이내) → 클라우드 계정 연동 (1시간) → 솔루션 이용 → 솔루션 도입 시간 2주 이내

Why Astron Security?

No.1
클라우드 보안 기업
아스트론시큐리티

CNAPP 기반 통합 보안 관리 실현

CSPM, CWPP, CIEM 등의 기능을 통합적으로 제공

멀티 및 하이브리드 환경 지원

AWS, Azure, NHN Cloud, NCP, VMware 등 다양한 멀티 클라우드 환경 지원

국내 특화 보안 솔루션

고객사별 커스터마이징 제공,
국내 주요 컴플라이언스 지원

합리적 가격

기업 규모에 따라
다양한 플랜별 가격 제공

다양한 솔루션 형태 제공

SaaS(구독형)및
설치형 제공

Think Secure!

'Astron SaaS', a powerful solution that combines AI security and cloud security, offering robust protection. It ensures comprehensive safeguarding for your cloud infrastructure. Experience simple and swift cloud security with Astron SaaS, the ultimate choice for your enterprise!

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

계정 및 권한 시각화, 최소 권한 관리를 통해 과도하게 권한이 부여된 계정 탐지!

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

약어표

약어	원어	한국어	뜻
CSPM	Cloud Security Posture Management	1) 클라우드 보안 형상 관리 2) 클라우드 보안 태세 관리	컴플라이언스 취약점을 진단, 탐지하고 조치 가이드를 제공하여 클라우드 위험을 지속적으로 관리하는 솔루션
CWPP	Cloud Workload Protection Platform	클라우드 워크로드 보호 플랫폼	물리적 서버, VM, 컨테이너 등 모든 유형의 클라우드 워크로드에 대한 보안을 제공하는 솔루션으로 컨테이너 및 호스트 보안을 통해 개발부터 운영에 걸쳐 클라우드 라이프사이클에 최적화된 보안을 지원하는 솔루션
CIEM	Cloud Infrastructure Entitlement Management	클라우드 인프라 권한 관리	클라우드 계정 및 서비스에 대한 권한과 활동을 시각화하여 나타내고 과도한 권한에 대한 지속적 탐지를 통해 최소 권한으로 관리하는 솔루션
CNS	Cloud Network Security	클라우드 네트워크 보안	클라우드 네트워크 환경에서의 악의적 공격을 탐지하고 보호하는 솔루션
CNAPP	Cloud Native Application Protection Platform	클라우드 네이티브 보호 플랫폼	클라우드 네이티브 애플리케이션의 개발과 운영 전반을 안전하게 보호하도록 설계된 솔루션으로 CSPM,CWPP, CIEM 등의 기능을 통합하여 제공
ISMS	Information Security Management System	정보보호 관리체계 인증	정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원 또는 인증기관이 증명하는 제도
ISMS-P	Information Security Management System Personal Information	정보보호 및 개인정보보호 관리체계 인증	정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 제도
CI/CD	Continuous Integration Continuous Development	지속적 통합/지속적 배포	솔루션 개발 시 빌드 및 배포를 자동화하여 효율적인 개발 파이프라인을 구축하는 애자일 개발 방식