공공 대상
국가 클라우드 컴퓨팅 보안 가이드라인 적용 방안

-조근석 대표-

ASTRON SECURITY

클라우드 네이티브 환경이 전 세계 표준으로 자리잡고 있습니다.

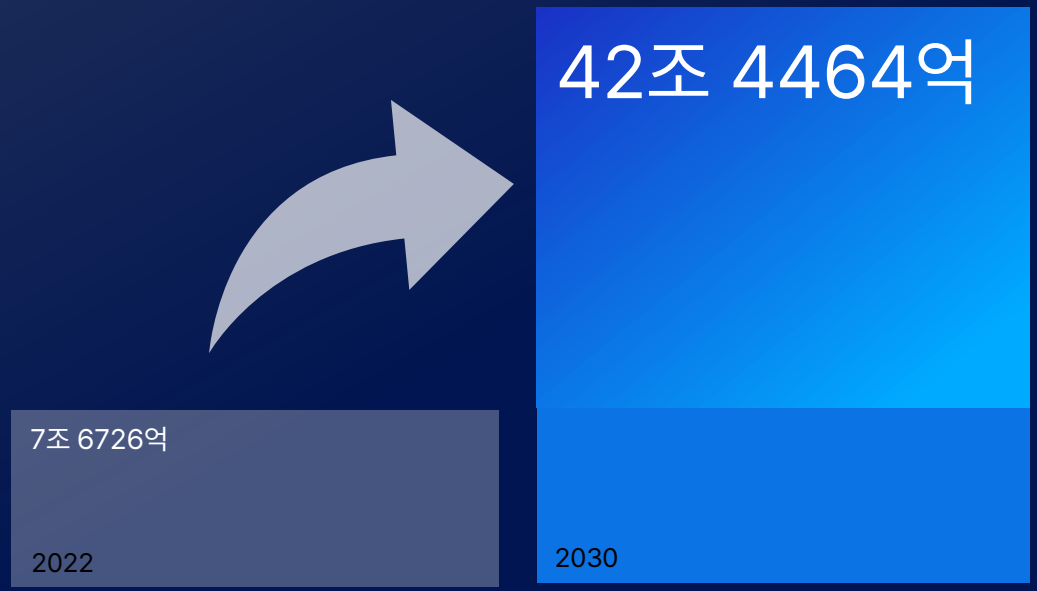
글로벌 클라우드 네이티브 환경 전환율

95%

Gartner

글로벌 클라우드 네이티브 시장 규모

CAGR:23.83%



360iResearch

공공부문에서 시스템의 100%를 클라우드 네이티브 환경으로 전환한다는 목표를 세우고 이행 중입니다

정부의 공공 클라우드 네이티브 추진 현황

공공 클라우드 네이티브 전환 로드맵

민간 클라우드 우선 도입

디지털 플랫폼 정부 부처 중심의 칸막이 극복

다양한 사업자 (클라우드 보안인증 등급제)

보안 위험이 상대적으로 낮은 경우 현행보다 완화된 보안 기준 적용

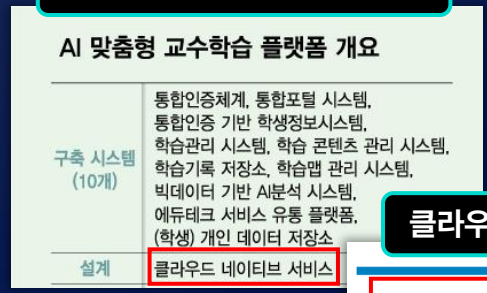
디지털 업무혁신 (SaaS)

디지털 전문계약제도를 통한 공급 등 SaaS 이용촉진을 위한 행적 규칙 개정(예정)

- 2023년: 시범 사업 추진
- 2024년: 대상 시스템 10% 달성
- 2026년: 대상 시스템 70% 달성
- 2030년: 대상 시스템 100% 달성

"정부는 21개 공공기관 시스템 클라우드 네이티브 전환 사업 추진 中"

AI 맞춤형 교수학습 플랫폼

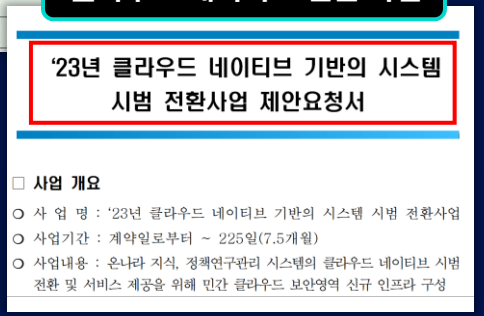


AI 맞춤형 교수학습 플랫폼 개요

구축 시스템 (10개)	통합인증체계, 통합포털 시스템, 통합인증 기반 학생정보시스템, 학습관리 시스템, 학습 콘텐츠 관리 시스템, 학습기록 저장소, 학습맵 관리 시스템, 빅데이터 기반 AI분석 시스템, 에듀테크 서비스 유통 플랫폼, (학생) 개인 데이터 저장소
설계	클라우드 네이티브 서비스

- 사업 예산: 약 340억

클라우드 네이티브 전환 사업



'23년 클라우드 네이티브 기반의 시스템 시범 전환사업 제안요청서

□ 사업 개요

○ 사 업 명 : '23년 클라우드 네이티브 기반의 시스템 시범 전환사업
○ 사업기간 : 계약일로부터 ~ 225일(7.5개월)
○ 사업내용 : 온나라 지식, 정책연구관리 시스템의 클라우드 네이티브 시범 전환 및 서비스 제공을 위해 민간 클라우드 보안영역 신규 인프라 구성

- 사업 예산: 약 51억

그러나 네이티브 전환을 저해하는 요인은 바로 '보안'입니다.

클라우드 보안 주요 위협

- 불충분한 액세스 관리
- 내부자 위협
- 알려지지 않은 비관리형 자산
- AI 기반 클라우드 공격
- API 위협

-Palowalto 2024 클라우드 네이티브 보안 현황-

공공기관 클라우드 전환 도입 시 우려사항

전환 이용 비용 과다 소요 등 비용 부담	41.4%
응용프로그램 재개발, 데이터 이관, 시스템 연계 등 클라우드 전환 업무에 대한 부담	28.0%
시스템의 중요성으로 인한 안정성 우려	**27.1%**
해킹 자료 유출 개인정보 유출 등 보안 이슈 발생 우려	**24.2%**
기존 장비의 폐기 등 매몰비용 발생	19.6%
클라우드 서비스에 대한 이해가 어려움	13.6%

-'23년 행정·공공기관 클라우드컴퓨팅 수요예보조사 결과-

실제로 클라우드 네이티브 위협으로 인한 보안 사고가 다양하게 발생하고 있습니다.

내부자 위협

TESLA

약 **7만 5천명**의 고객 데이터 유출

4조 4,134억 벌금 부과 위험에 처함

전직 테슬라 직원이 내부 직원들의
개인 정보를 독일 신문사에 전송

2023

사용자 설정 오류

Azure

Azure Blob 스토리지 버킷이

유출되어 **6만 5천개** 기업 데이터 노출

클라우드 스토리지 설정 오류로 인한
데이터 유출

2022

불충분한 액세스 관리

Uber

약 **5,700만 명**의 고객 데이터 유출

1,977억 벌금 부과

잘못 관리된 IAM을 이용하여 AWS
S3 버킷에 접근 후 고객 데이터 유출

2016

공공기관에 보안 사고 발생 시 국가 기밀 데이터 유출이라는 막대한 피해를 초래할 수 있습니다.

국가 기밀 데이터 유출로 국가 안보에 치명적

안전한 클라우드 전환을 위해서 공공기관은 '23년 국가 클라우드 컴퓨팅 보안 가이드라인을 개정하였습니다.

주요 내용

클라우드 보안 기본 원칙 및 기술적 / 정책적 준수사항 명시

가상환경에서의 인증 및 권한 식별, 컴플라이언스 준수,
로그 확보, 컨테이너 보안 등을 포괄적으로 강조

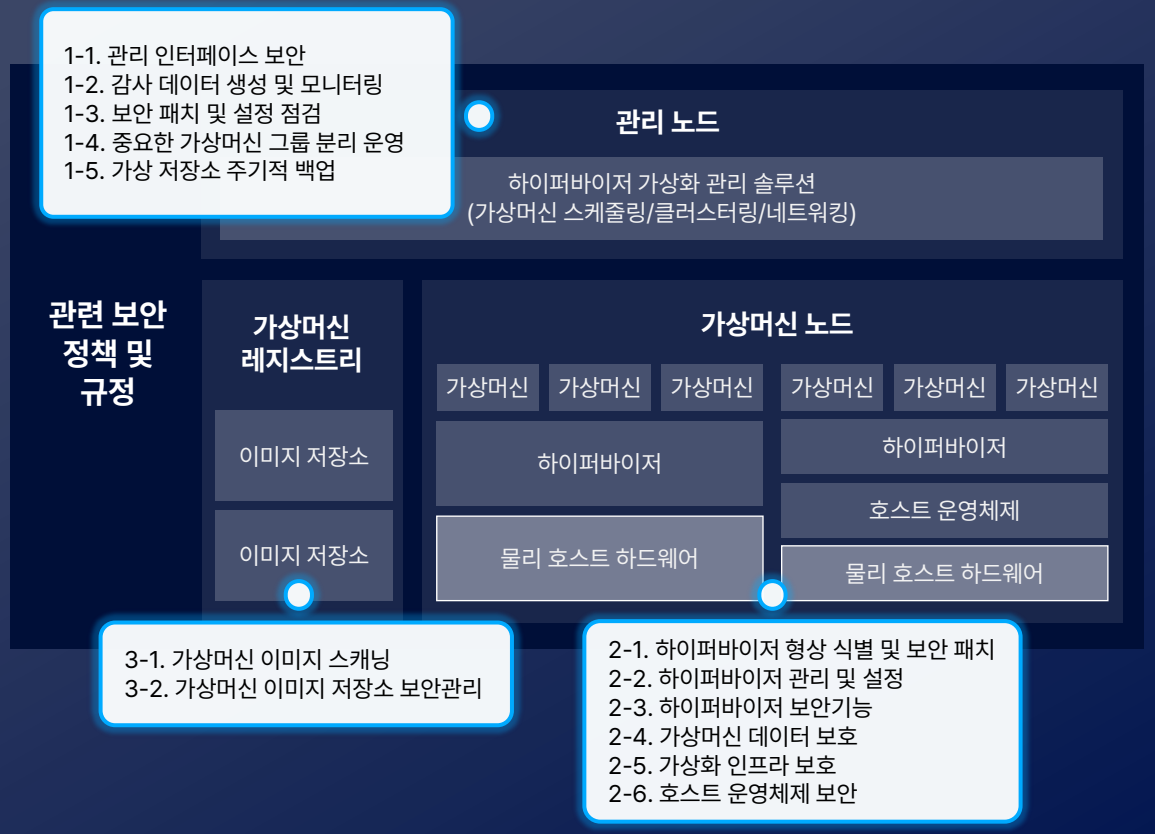
클라우드 컴퓨팅 보안 가이드라인을 요약해보면

위험 요인	대응 방안
클라우드 인프라 구성 및 설정 취약점	구성 및 설정 취약점 식별
변동성으로 인한 자산 식별의 어려움	자산 시각화 및 변동 내역 식별
복잡한 자산 및 계정 구조	계정 및 권한 관리
컨테이너 이미지 취약점	컨테이너 이미지 취약점 점검

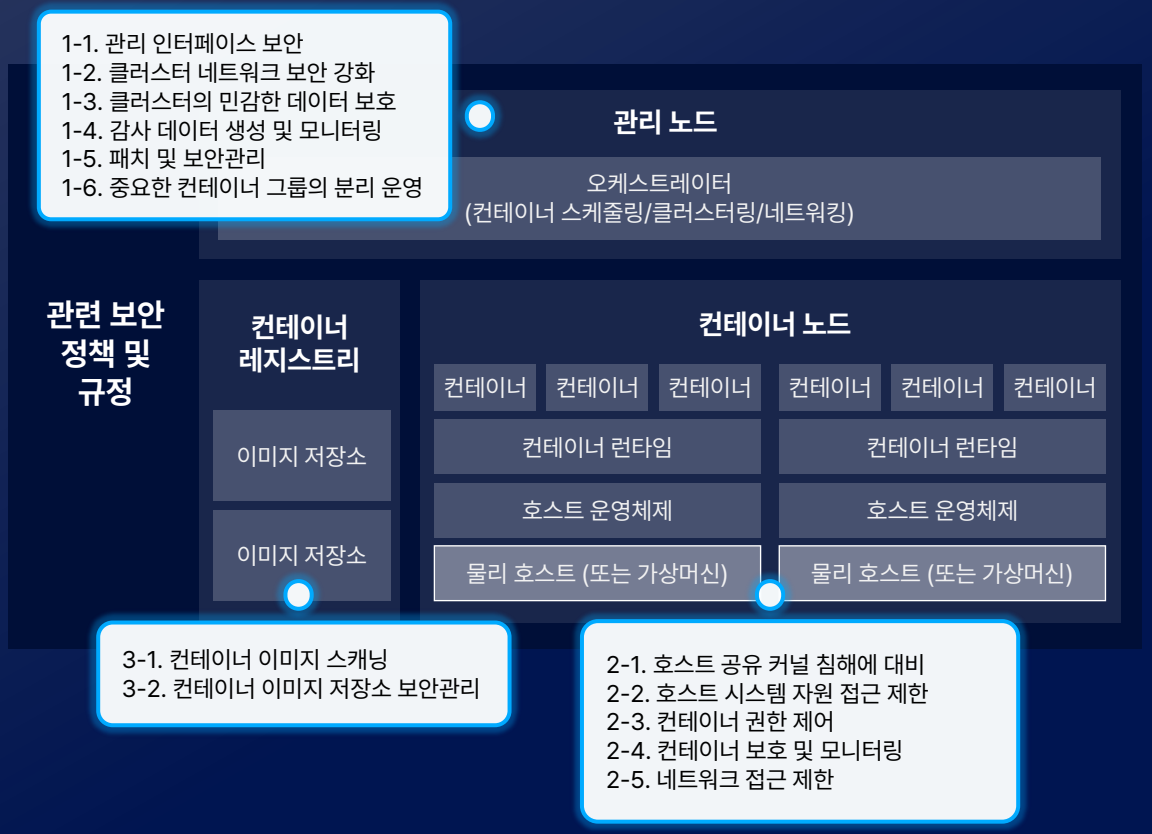
클라우드 자산, 계정, 컨테이너 등 다양한 워크로드 위협에 대한 대응 방안 구축 요구

국가 클라우드 컴퓨팅 보안 가이드라인 내 보안 요구사항

하이퍼바이저 가상화 스택 기술에 대한 보안 기준



컨테이너 가상화 스택 기술에 대한 보안 기준



다양한 보안 요구사항을 반영한 보안 시스템 수립 필요 → 높은 기술 난이도 요구

그러나

클라우드 보안 가이드라인의 모호함 으로 인해

제안사, 공공기관 모두 클라우드 보안을

제대로 적용하지 못하고 있습니다.

현 클라우드 네이티브 사업 관련 공공 RFP를 들여다보면

클라우드 네이티브 사업 RFP 일부 (~'24)

클라우드 전환 요구사항
CTR-008
클라우드 네이티브 컴퓨팅 보안 준수 요건
클라우드 서비스 제공자 등에 대한 보안 요구사항
○ 국가정보원의 국가클라우드컴퓨팅 보안가이드라인을 우선 준용하고 사업 기간 중 개정이 발생 할 경우 변경 사항을 반영해야함

「국가 클라우드 컴퓨팅 보안 가이드라인」 지침 **준용**

○ 컨테이너 플랫폼 보안 지침 - 독립된 K8s 구성으로 안전 분리 준수 - 국가클라우드컴퓨팅 보안 가이드라인에 따른 컨테이너 보안 지침 준수

「국가 클라우드 컴퓨팅 보안 가이드라인」 지침 **준수**

모든 RFP 내 '준용, 준수' 와 같은 모호한 표현 적시

제안사

클라우드 네이티브 보안과 관련하여
구체적인 요구사항이 없으니
공공기관이 원하는 보안 기능이 무엇인지,
평가 기준은 어떨지 전혀 모르겠어요

공공기관

「국가 클라우드 컴퓨팅 보안 가이드라인」 내
구체적인 내용이 없어서 RFP에 어떻게
요구사항을 기재해야 할지 모르겠어요

구체적인 가이드라인 부재로 인한 제안사, 공공기관 고충 발생

CNAPP

클라우드 네이티브 환경 에서

애플리케이션을 보호 하기 위한

포괄적인 보안 플랫폼

CNAPP란 클라우드 네이티브 통합 보안 솔루션으로 CSPM, CIEM, CWPP 3요소를 모두 제공합니다.

CSPM	CIEM	CWPP
자산 변동 식별 및 시각화	계정 및 권한 시각화	클라우드 네이티브 시각화
취약점 진단 및 실시간 탐지	계정 및 권한 변동 식별	컨테이너 이미지 취약점 스캔
취약점 조치 가이드 제공	최소 권한 관리	CI/CD 보호

개발, 배포, 운영 등 라이프사이클 전체에 걸쳐 포괄적으로 네이티브 환경 보호

제안사 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (1)

구분	점검항목	적합 솔루션
클라우드 인프라	가상자원에 대한 모니터링을 주기적으로 수행하고 있는가?	CSPM CWPP
인증 및 권한	서비스 관리환경, 가상머신, 가상 응용프로그램, SaaS 등의 접근 대상 및 주체를 식별하였고 이에 따른 인증 정책을 수립하였는가?	CIEM
	기관 필요에 따라 클라우드 접근 대상 별로 기관의 인증 체계와 연동할 수 있는 인증 시스템을 설계 및 구축하였는가?	CIEM
	접근대상, 권한 부여 절차 등을 담은 사용자, 관리자의 접근 권한 관리절차를 수립하였는가?	CIEM
	클라우드 접근 대상에 따른 접근 주체별 이용 및 관리 권한을 부여하고 있는가?	CIEM

구분	점검항목	적합 솔루션
가상환경 보안	가상환경에서 시스템, 애플리케이션, SaaS 등을 자체 또는 외주로 도입 및 개발하고자 하는 경우 보안대책을 수립하고 있는가? (운영 중인 클라우드 서비스 환경과 분리, 비인가 접근 통제 등)	CSPM CIEM CWPP
	가상환경을 구성하는 시스템, 애플리케이션, SaaS 등을 유지보수하고자 하는 경우 보안대책을 수립하고 있는가? (유지보수 인원관리, 지정 된 단말기만 접속, 유지보수 기록 유지 등)	CSPM CIEM CWPP
접근 통제	이동식 저장매체 사용 통제, 다중요소(Multi-factor) 인증, 자동 로그아웃 등 접근 제한 방안을 마련하였는가?	CIEM
	사용자 또는 장치를 유일하게 식별할 수 있는 식별 방법을 마련하고 식별 정보를 관리하는가?	CIEM
	계정 권한 생성 절차를 마련하였는가? ※ 계정 유형 식별, 계정 그룹 설정, 클라우드 시스템 및 서비스 접근허용자 식별, 게스트 또는 임시 계정에 대한 승인 및 모니터링 등	CIEM
	사용자계정 보안관리 방안을 마련하여 사용자계정(ID) 부여 및 보안관리를 수행하는가? ※ 사용자·그룹별 접근권한 부여, 사용자 식별 수단이 없는 계정 사용 금지, 5회 이상 로그인 실패 시 접속 중단 등	CIEM

CSPM, CIEM 기능(클라우드 환경에서의 자산 모니터링/ 접근 권한 식별 및 관리) 강조

제안사 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (2)

구분	점검항목	적합 솔루션
컨테이너 가상화 기술 보안	관리자 계정 접근에 대해 다중요소(Multi-factor) 인증을 사용하고 있는가?	CIEM
	컨테이너 운영 환경의 감사 데이터를 생성하고 모니터링하고 있는가?	CWPP
	주기적으로 취약한 설정을 점검하고 관리하고 있는가?	CWPP -KSPM
	컨테이너의 비정상적인 활동을 탐지할 수 있는 보안 솔루션을 활용하고 있는가?	CWPP
	컨테이너 상태에 대한 모니터링을 수행하고 있는가?	CWPP
	이미지 저장소에 취약하거나 오래된 버전의 이미지가 포함되지 않도록 관리, 운영하고 있는가?	CWPP

컨테이너 보안 기능의 경우 CWPP(클라우드 워크로드 보안)기능이 필수적

제안사 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (3)

구분	점검항목	적합 솔루션
기본원칙	이용 대상에 대한 시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안 기준을 확인하였는가? (시스템 중요도 및 클라우드 영역 관련 보안 기본 원칙 등)	CSPM CIEM CWPP
기술적 측면	관리자 또는 다른 이용자가 특정 이용자에 할당된 자원(메모리·HDD 등) 및 데이터에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 통제수단을 마련하고 있는가?	CIEM
	클라우드 컴퓨팅 서비스에 대한 보안관제를 수행하고 있는가?	CSPM CIEM CWPP

구분	점검항목	적합 솔루션
정책	클라우드 컴퓨팅 서비스 도입 시 관련 법률 및 지침, 보안체계, 정책, 규정, 표준, 가이드라인 및 도입기관 보안 사항 등을 참고하여 보안 요구사항을 마련하였는가?	CSPM CIEM CWPP
	클라우드 컴퓨팅 서비스를 구축하여 다루고자 하는 업무 또는 데이터와 연관된 법령, 수행 요구사항, 정책, 규정, 표준, 가이드라인 등을 참고하여 클라우드 컴퓨팅과 관련된 물리적 설비, 하드웨어 장비, 가상 인프라, 가상머신 내 소프트웨어 등에 대한 보안 위협을 식별하였는가?	CSPM CIEM CWPP
	형상 변경에 영향을 받는 물리적 논리적 요소를 식별하고 형상 변경 사항을 지속적으로 확인 및 검토하고 있는가?	CSPM
	클라우드 컴퓨팅 환경 내 모니터링 수집 대상 및 위치를 정의하고 모니터링 수단을 통해 시스템 운영 상황, 장애 발생 대응 도구 동작 여부 등을 모니터링하고 있는가?	CSPM CIEM CWPP
	보안 요구사항, 가용성 요구사항 ,감사 요구사항, 법적 요구사항 등과 같은 요구사항들에 대한 준수 여부를 판별하기 위한 모니터링 및 로그관리를 수행하고 있는가?	CSPM CIEM CWPP

단일 포인트 보안 솔루션으로는 가이드라인 충족 불가능

CNAPP만이 전범위 Cover

공공기관 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (1)

국가 클라우드 보안 가이드라인 요구사항		구체적인 RFP 작성 예시
기본 원칙	이용 대상에 대한 시스템 중요도 등급 분류 및 클라우드 영역 분류를 수행하고 관련 보안 기준을 확인하였는가?	1. 이용 서비스에 대한 식별 및 변경 추적관리가 가능하고, 상세 내용을 기록해야 한다. 2. 클라우드 자산 및 서비스에 대한 취약점 점검이 이뤄져야 한다.
기술적 측면	관리자 또는 다른 이용자가 특정 이용자에 할당된 자원(메모리·HDD 등) 및 데이터에 임의 접근하지 못하도록 접근제어 및 격리 등을 통한 기술적 통제수단을 마련하고 있는가?	1.관리자 및 이용자가 특정 클라우드 자산에 대한 접근 여부 관련 감시와 기록이 되어야 한다. 2.클라우드 자산의 취약점, 섀도우 IT에 대한 관리 및 취약점 점검을 실시하여야 한다. 3.변경된 자산, 계정에 대한 취약점을 진단하여야 한다.
기술적 측면	클라우드 컴퓨팅 서비스에 대한 보안관제를 수행하고 있는가?	1.클라우드 플랫폼 상 발생하는 취약점 정보, 로그를 수집하여 관제에 적용해야 한다. 2.클라우드 사용자의 위협 행위에 대한 정보, 로그를 수집하여 관제에 적용해야 한다. 3.클라우드 네이티브 환경 상 발생하는 취약점 정보를 수집하여 관제에 적용해야 한다.

공공기관 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (2)

국가 클라우드 보안 가이드라인 요구사항		구체적인 RFP 작성 예시
시스템 보호	사용자와 관리자를 지정하여 클라우드 컴퓨팅 시스템을 도입·운용하고 있는가?	1. 관리자와 사용자를 식별하고 권한에 대한 조회 및 변경내역 관리가 가능하여야 한다.
시스템 보호	클라우드 컴퓨팅 서비스를 구축하여 다루고자 하는 업무 또는 데이터와 연관된 법령, 수행 요구사항, 정책, 규정, 표준, 가이드라인 등을 참고하여 클라우드 컴퓨팅과 관련된 물리적 설비, 하드웨어 장비, 가상 인프라, 가상머신 내 소프트웨어 등에 대한 보안위협을 식별하였는가?	1. 클라우드 자산에 대한 식별 및 취약점 진단이 이루어져야 한다. 2. 클라우드 계정에 대한 식별 및 취약점 진단이 이루어져야 한다. 3. 클라우드 네이티브 자산에 대한 식별 및 취약점 진단이 이루어져야 한다.
인적 관리	클라우드 컴퓨팅 서비스에 접근 가능한 사용자 및 관리자를 식별하고 직무별 권한 부여, 폐기 등에 관한 절차를 마련하고 있는가?	1. 관리자 및 사용자를 구분할 수 있는 식별자를 지원하는지 점검하여야 한다. 2. 계정을 식별하고 생성시 조직, 직무, 성명, 연락처 등이 추가로 입력되었는지 확인하여야 한다. 3. 변경된 계정 및 권한을 실시간 식별, 기록하여야 한다.

공공기관 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (3)

국가 클라우드 보안 가이드라인 요구사항		구체적인 RFP 작성 예시
가상화 인프라	가상자원에 대한 모니터링을 주기적으로 수행하고 있는가?	1. 가상 자산 및 어플리케이션에 대한 생성, 변경, 삭제 관리가 이루어져야 한다. 2. 클라우드 네이티브 환경(쿠버네티스, 컨테이너 등)에 대한 생성, 변경, 삭제 관리가 이루어져야 한다.
가상화 인프라	접근대상, 권한 부여 절차 등을 담은 사용자, 관리자의 접근 권한 관리절차를 수립하였는가?	1. 계정 및 계정 그룹의 권한 모니터링, 클라우드 시스템 및 서비스 접근 허용자에 대한 기록을 관리하여야 한다.
보안 관리	가상환경에서 시스템, 애플리케이션, SaaS 등을 자체 또는 외주로 도입 및 개발하고자 하는 경우 보안대책을 수립하고 있는가?	1. 가상자산에 대한 식별과 변경관리를 하여야 하며, 취약점 진단을 실시하여야 한다. 2. 클라우드 계정 및 권한에 대한 관리를 하여야 하며, 권한상승, 미사용계정, 과도한 권한, 최소권한으로 운영되는지 등에 대한 관리가 이루어져야 한다.
접근 통제	계정 권한 생성 절차를 마련하였는가?	1. 계정 및 계정 그룹의 권한 모니터링, 클라우드 시스템 및 서비스 접근 허용자에 대한 기록을 관리하여야 한다. 2. 미사용 계정 관리를 통해 주기적으로 삭제 계정을 식별 관리한다.

공공기관 관점 – 공공 클라우드 보안 가이드라인 상세 분석 (4)

국가 클라우드 보안 가이드라인 요구사항		구체적인 RFP 작성 예시
관리 노드	컨테이너 운영 환경의 감사 데이터를 생성하고 모니터링하고 있는가?	1. 관리에 대한 로그가 활성화되어 있는지 점검하여야 한다. 2. 런타임 데몬, 필수 디렉토리, 필수 파일 등에 감사 설정이 적용되어 있는지 점검하여야 한다.
컨테이너 노드	컨테이너의 비정상적인 활동을 탐지할 수 있는 보안 솔루션을 활용하고 있는가?	1. 계정 및 계정 그룹의 권한 모니터링, 클라우드 시스템 및 서비스 접근 허용자에 대한 기록을 관리하여야 한다.
컨테이너 노드	컨테이너 상태에 대한 모니터링을 수행하고 있는가?	1. 워크로드에 대한 자원 모니터링을 제공하여야 한다.
컨테이너 레지스트리	이미지 저장소에 취약하거나 오래된 버전의 이미지가 포함되지 않도록 관리, 운영하고 있는가?	1. 이미지 저장소 및 배포 툴에 대한 이미지 점검을 수행하여야 한다. 2. 취약한 이미지에 대한 조치가이드를 제공하여야 한다.

아스트론은 국내 선두 기술력의 클라우드 네이티브 보안 전문 기업입니다.

회사소개

대표자	조근석
설립일	2019.03.26
사업 분야	클라우드 네이티브 보안, 제로트러스트 보안

기업 특징

1. 국내 최초 클라우드 네이티브 보안 전문 기업
2. CNAPP 기반 통합 보안 기술 보유
3. 정부 주도 클라우드 보안 정책수립 참여
4. 공공 조달 등록

주요 투자자

누적 투자금액 100억+

투자자명	네이버 클라우드, 안랩, KDB 산업은행, IBK 기업은행 외 5곳

주요 레퍼런스

금융	KB국민은행, 케이뱅크, 신한EZ손해보험, 신한투자증권
공공	**경남도청, KGC인삼공사, LH한국토지주택공사, 구리시, 농림축산식품부, 한국데이터진흥원, KERIS**
민간	안랩, 네이버 클라우드, 자비스, SK C&C, E1, 중앙대병원

특허 현황

구분	특허 등록 및 출원 건수
국내	총 20건
글로벌	총 14건
클라우드 보안	총 13건
AI 보안	총 21건

수상 및 인증 내역

과학기술정보통신부 장관상 ('22)	중소벤처기업부 장관상 ('22)
아기유니콘 선정 ('22)	초격차 스타트업 1000+ 선정 ('24)
GS 인증 1등급	CSAP 인증

ASTRON CNAPP은 CSPM, CIEM, CWPP의 핵심 기능을 통합하여 네이티브 환경 전반에 걸쳐 포괄적인 보안을 제공합니다.

CSPM

클라우드 인프라 설정 오류 탐지를 기반으로 지속적 위험 관리

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

국내 유일 CNAPP 기술

CIEM

클라우드 사용자 및 서비스에 대한 위협 식별 및 권한 관리

- 계정 및 권한 시각화
- 계정 및 권한 변동 식별
- 최소 권한 관리 지원

지속적인 기능 확장

CWPP

클라우드 환경에서 실행되는 워크로드 취약점 탐지

- 워크로드 취약점 현황 시각화
- 컨테이너, 쿠버네티스 취약점 탐지
- Shadow IT 탐지

국내 가격 경쟁력 보유

고객사 네이티브 환경 전반에 걸친 포괄적인 보안 구축

① CNAPP 보안 관리 ② 원활한 커스터마이징 ③ 공공 보안 요건 충족 ④ 신속한 고객 지원을 통해 보안 안정성 및 고객 편의성을 증대합니다.

1 CNAPP 보안 관리

- CNAPP 핵심요소 (CSPM,CIEM,CWPP) 통합 제공
  → 보안 복잡성 감소
- 심각도에 따른 보안 위협 대응
  → 컴플라이언스, Risk, 서비스 변동 시 사용자 지정 얼럿 제공

2 원활한 커스터마이징

- 고객사 요구사항에 따른 커스터마이징 지원
  → 다수의 공공 구축 사례 기반 표준 커스터마이징 적용

3 공공 보안 요건 충족

- 국가 클라우드 컴퓨팅 보안 가이드 라인 충족
  → 지속적 가이드라인 반영 가능

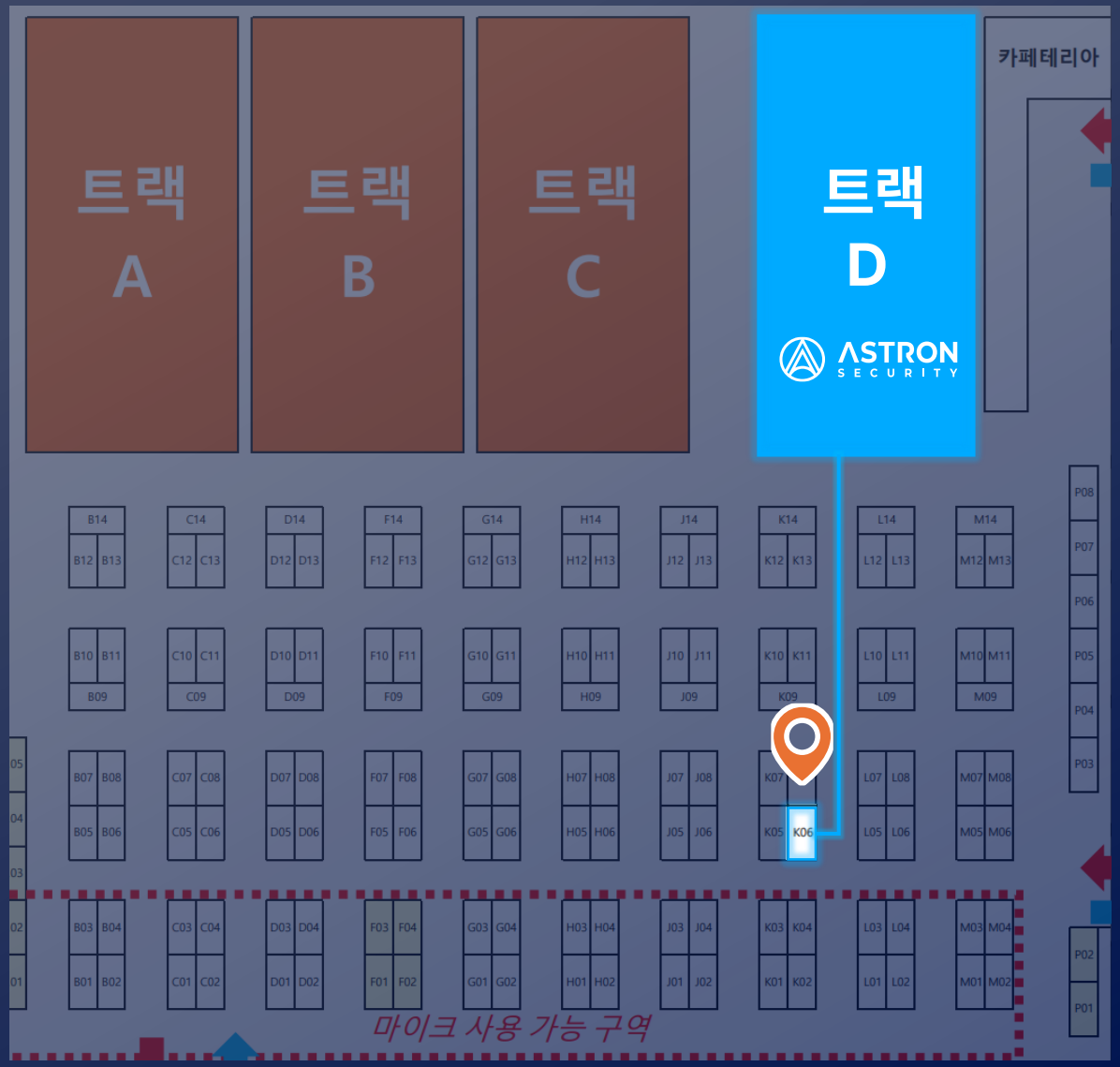
4 신속한 고객 지원

- 컴플라이언스 및 솔루션 업데이트
- 신속한 피드백 반영
  → 빠른 업데이트 및 즉각적인 개선

공공 환경에 최적화된 보안 및 운영 환경 제공

아스트론은 국내 및 글로벌 경쟁사 대비 선두 기술력을 보유하고 있습니다.

구분	기술 구분	기술 내용	대상 기업			제안사 우위 요소
			외산 기업	아스트론	국내 경쟁사	
Tech	CSPM	- 자산 식별 및 변동내역 관리 - 취약점 진단 및 탐지 - 구성 오류 관련 얼럿 지원	O	O	O	구성 오류 얼럿 제공
	CIEM	-계정 및 권한 시각화 -계정 변동내역 식별 - 최소 권한 관리, 이상행위 식별	O	O	부분 지원	최소 권한 관리 지원
	CWPP	- 쿠버네티스 및 컨테이너 취약점 관리 - CI/CD 및 런타임 보호	O	O	미지원	국내 유일 기술 지원 및 레퍼런스 보유
지원 내역	글로벌 클라우드 지원	- 해외 퍼블릭 클라우드 지원 (AWS. MS 등)	O	O	O	국내·외 동일 수준 기술 연동 지원
	국내 클라우드 지원	- 국내 퍼블릭 클라우드 지원 (네이버 클라우드, NHN클라우드, KT 클라우드 등)	미지원	O	부분 지원	
	국내 커스터마이징 지원	- 커스텀을 통해 국내 기업 환경에 최적화된 클라우드 보안 관리 체계 지원	미지원	O	O	금융권 표준 커스터마이징 확보
	국내 컴플라이언스 지원 (CSAP, ISMS-P 등)	- 국내 보안 컴플라이언스 지원	부분 지원	O	O	금융보안원 클라우드 보안 가이드라인 준수
	국내 인증 획득	- CSAP, GS인증 등	미획득	획득	부분 획득	기술 안정성 확보



부스 위치

K06

프로모션

1. 국가 클라우드 컴퓨팅 보안 가이드라인 필수 지침서 제공
2. CSPM/CIEM 솔루션 3개월 무상 지원 제공

궁금하신 점은 오셔서 편하게 문의해 주세요.

Thank You!

클라우드 네이티브 보안 기업 아스트론시큐리티와 함께
보다 안전한 클라우드 환경을 구축하세요!

ASTRON SECURITY