paloalto NETWORKS | CORTEX® CLOUD

애플리케이션 보안

완벽한 코드, 클라우드 및 런타임 컨텍스트를 기반으로 하는 업계 최고의 애플리케이션 보안으로 위험 원천 방지

전례 없이 빠른 개발 속도.
보안도 이에 맞춰 빨라야 합니다.

애플리케이션 개발 속도가 빨라지면서 보안팀은 상당한 압박을 받게 되었고, 보안을 저하시키지 않으면서도 속도는 빨라야 한다는 요구에 부응하기 위해 신속하게 적응해야 했습니다. DevSecOps의 등장으로 보안 취약점을 해결하는 책임이 대부분 개발자에게 넘어갔지만, 기존 AppSec 도구는 개발자의 요구를 충족하지 못하고 있습니다. 기존 AppSec 도구는 주로 보안팀을 중심으로 만들어졌으며 클라우드 네이티브 개발에 원활하게 통합될 수 없습니다.

현대의 클라우드 네이티브 엔지니어링 생태계는 매우 다양하면서도 단편화되어 있으므로 팀에서 위험을 효과적으로 식별하고 우선순위를 정하여 해결하는 데 필요한 가시성과 컨텍스트가 부족한 경우가 많습니다. 이러한 문제를 극복하려면 팀은 위험 예방으로 눈을 돌려야 합니다. AppSec 팀의 문제는 개발 속도를 늦추지 않는 예방 정책을 구현할 컨텍스트가 부족하다는 것이었습니다. 따라서 제한적인 통제를 시행하기보다는 문제가 프로덕션 환경에 영향을 미치면 해결하는 데 집중하기로 결정했습니다.

Cortex Cloud 애플리케이션 보안

Cortex Cloud™는 위험을 예방하고 애플리케이션을 보호할 수 있도록 엔지니어링 생태계와 원활하게 통합되어 개발을 안전하고 더 빠르게 진행할 수 있습니다. 이 플랫폼은 최고의 AppSec 기능과 타사 스캐너를 통합하여 코드에서 클라우드까지 완벽한 보안을 제공합니다.

그림 1. Cortex Cloud ASPM 명령 센터

이점

- **포괄적인 가시성:** Cortex® Cloud는 코드, 공급망, 애플리케이션 인프라 및 런타임 전반에 걸쳐 AppSec 가시성을 중앙 집중화하여 수명 주기 전반에서 일관된 보안을 제공합니다.
- **보안 문제를 지능적으로 방지:** 새로운 문제와 기존 문제를 구분하는 타겟형 보안 가드레일을 시행하고, 컨텍스트를 활용하여 개발 속도를 늦추지 않으면서 위험이 프로덕션 단계에 도달하지 않도록 예방합니다.
- **AI 기반 위험 우선순위 지정:** 코드, 파이프라인, 런타임 및 애플리케이션 컨텍스트를 결합하여 악용 가능성과 잠재적인 비즈니스 영향에 따라 위험의 우선순위를 지정합니다.
- **자동 해결:** 애플리케이션 수명 주기의 모든 단계에서 업계 최고의 자동화를 통해 보안팀과 개발팀 간의 수동 수정 단계를 없애줍니다.
- **개발자 친화적:** 네이티브 통합을 사용하여 통합 개발 환경(IDE)과 버전 관리 시스템(VCS)에서 즉각적인 피드백을 받아 문제가 발생하면 바로 해결할 수 있습니다. 개발자에게 컨텍스트를 포함한 풀 리퀘스트(PR)를 보내 보안 문제를 쉽게 해결할 수 있도록 합니다.
- **코드에서 클라우드, SOC까지 일관된 보안:** 코드에서 클라우드, SOC에 이르기까지 모든 결과를 상호 연관시켜 전체 수명 주기에 걸쳐 활성 애플리케이션 위협을 감지하고 연관시키며 대응합니다.

주요 기능

Cortex Cloud는 다음과 같은 주요 AppSec 기능을 단일 솔루션으로 통합합니다.

- **애플리케이션 보안 태세 관리(ASPM):** AppSec 가시성을 단일 위험, 정책 및 자동화 엔진으로 통합하여 전체 애플리케이션 수명 주기에서 보다 손쉽게 위험을 방지하고 우선순위를 지정하며 해결할 수 있습니다.
- **소프트웨어 공급망 보안:** 엔지니어링 생태계에 대한 심층적인 가시성과 제어력을 확보하고, 파이프라인 도구 사용과 위험을 관리하고, Software Bill of Materials(SBOM)를 관리하며, 안전한 배포를 보장합니다.
- **코드형 인프라(IaC) 보안:** 런타임 추적 기능을 갖춘 포괄적이고 개발자 우선의 IaC 보안을 활용하여 잘못된 구성의 원천을 수정합니다.
- **소프트웨어 구성 분석(SCA):** 개발자 통합 및 상황 인식 우선 순위 지정으로 오픈 소스 취약점 및 라이선스 규정 준수 문제를 선제적으로 해결하세요.
- **비밀 보안:** 포괄적인 비밀 보안을 확보하여 자격 증명 노출을 정확하게 탐지하고, 우선 순위를 지정하고, 제거합니다.
- **타사 수집:** AppSec 도구를 연결하여 중앙 집중식 가시성을 확보하고 포괄적인 런타임 및 애플리케이션 컨텍스트에 따라 위험의 우선 순위를 지정하세요.

Cortex Cloud 지원

IDE

- Visual Studio Code
- JetBrains

VCS

- GitHub Enterprise Cloud
- Self-Managed GitLab on Cloud
- Bitbucket Cloud 및 Data Center
- Azure Repos
- AWS CodeCommit

CI/CD 시스템

- Jenkins
- CircleCI
- GitHub Actions
- AWS CodeBuild
- 모든 CI/CD 시스템에 Cortex Cloud CLI 통합

타사 스캐너

- Black Duck
- Checkmarx
- GitLab
- HashiCorp
- Semgrep
- Snyk
- Veracode
- SonarQube
- SARIF 형식을 사용하여 모든 스캐너에서 결과 수집

Cortex Cloud로 AppSec, 클라우드 및 SOC 통합

Cortex Cloud는 코드에서 클라우드, SOC에 이르기까지 실시간 보안을 위해 최고의 SecOps 플랫폼에서 세계 최고의 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)을 재구성합니다. 통합 데이터, AI, 자동화를 통해 위협 원천을 즉시 차단하는 적응형 방어 시스템을 구축하여 기업에서 성능 저하 없이 AI 기반 혁신을 수용할 수 있도록 지원합니다.

최초로 단일 통합 플랫폼에서 동급 최고의 애플리케이션 보안, 클라우드 보안, SecOps를 모두 누리며 위협을 훨씬 더 빠르고 효율적으로 차단하세요.

Cortex Cloud 소개

차세대 Prisma®인 Cortex Cloud는 동급 최고의 CDR과 업계 최고의 CNAPP를 병합하여 실시간 클라우드 보안을 제공합니다. AI와 자동화의 성능을 활용하여 런타임 컨텍스트에 따라 위험의 우선 순위를 지정하고, 대규모 수정을 활성화하며, 공격이 발생하는 즉시 차단합니다. 통합 Cortex 플랫폼에 클라우드와 SOC를 결합하여 엔드투엔드 운영을 혁신하세요. www.paloaltonetworks.com/cortex/cloud 에서 실시간 클라우드 보안의 미래를 경험해 보세요.

CORTEX CLOUD의 작동 방식 보기

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com

cortex_ds_application-security_071525