Cortex Cloud 런타임 보안

정교한 클라우드 공격의 실시간 차단

격리 조치를 통해 악성 프로세스, 워크로드 공격, 웹 기반 익스플로잇, API 남용을 차단하여 위협이 클라우드 환경을 손상시킬 수 없도록 방지합니다. Cortex® Cloud 런타임 보안은 클라우드 보안과 SOC 전반에 걸쳐 전체 컨텍스트와 워크플로를 공유하는 단일 신뢰 소스를 통해 전사적 가시성과 대응 기능을 제공하며, 이를 통해 업계 최고 수준의 클라우드 런타임 보호 역량을 확장합니다. 점점 더 빠르게 변화하는 위협 환경에서 클라우드 에코시스템을 보호하고 혁신적인 방식으로 비즈니스 연속성을 보장합니다.

그림 1: 수많은 위협에 대해 실시간 보호 기능을 제공하는 Cortex Cloud 런타임 보안

빠른 변화와 복잡성으로 클라우드 보안을 압박하는 위협

현대의 클라우드 보안은 인프라, ID, 사용자 정의 및 오픈 소스 코드, 그리고 클라우드에서 생성되는 방대한 데이터를 모두 포괄합니다. AI 기반 서비스의 빠른 도입으로 공격 표면이 더욱 확대되었고, 클라우드 리소스에 대한 분산 액세스로 개발자들은 전례 없는 속도로 배포할 수 있게 되었습니다. 이로 인해 기존의 보안 통제를 우회하는 경우가 늘어났습니다. 이러한 변화는 혁신을 가속화하지만, 공격자가 악용할 수 있는 보안 허점이 발생합니다.

3,800만 명의 개발자에 의해 7억 5천만개가 넘는 클라우드 네이티브 애플리케이션이 지원되면서 클라우드 환경에 대한 공격이 급증했으며, 지난 1년간 증가율이 66%에 달했습니다.[1] 클라우드에서의 보안 노출은 현재 모든 리스크의 80%를 차지하며,[2] 그 중 거의 절반은 매달 변화하므로[3] 방어 조치도 끊임없이 변화하고 있습니다.

공격의 빈도가 높아지며 아키텍처의 역동성이 커짐에 따라 탁월한 가시성과 보호 기능을 통해 실시간으로 위협을 보호, 탐지, 대응할 수 있는 중앙 집중식 솔루션의 필요성이 대두되고 있습니다.

Cortex Cloud 런타임 보안

다음과 같은 이점을 제공하는 업계 최고의 런타임 보호 기능을 활용하여 클라우드 공격을 실시간으로 차단하고 침해로 이어지지 않도록 방지하세요.

런타임 방어

예측 및 위협 기반의 선제적 보안으로 클라우드 환경을 대규모로 보호합니다. Cortex Cloud는 고급 머신러닝 모델을 활용하여 실행 중인 워크로드에 대한 공격을 감지하고 차단함으로써 성능 저하 없이 리스크를 최소화합니다.

호스트 (VM) 보안

실시간 위협 방지, 정책 시행 자동화, 워크로드 활동에 대한 심층적 가시성을 바탕으로 퍼블릭 및 프라이빗 클라우드 환경 전반의 가상 머신을 보호합니다. Cortex Cloud는 멀웨어, 무단 액세스, 지능형 악용 기법으로부터 VM을 보호합니다.

1. *Unit 42 인시던트 대응 보고서*, Palo Alto Networks, 2024년 2월 20일.
2. *Unit 42 공격 표면 위협 보고서*, Palo Alto Networks, 2023년 9월 14일.
3. *인시던트 대응 2024 보고서*, Palo Alto Networks, 2024년 2월 20일.

컨테이너 보안

전체 수명 주기 보호 기능을 통해 Kubernetes와 컨테이너식 애플리케이션을 보호합니다. Cortex Cloud는 이미지를 지속적으로 스캔하고 런타임 방어 기능을 적용하여 이상 동작을 감지함으로써 관리형 및 비관리형 환경을 모두 보호합니다.

서버리스 보안

구성 오류를 식별하고, 코드 취약점을 감지하고, 임시 환경에서 악의적 활동을 방지함으로써 서버리스 워크로드를 보호합니다. Cortex Cloud를 사용하면 개발 속도를 유지하면서도 일관적인 컨트롤을 적용할 수 있습니다.

웹 애플리케이션 및 API 보안(WAAS)

SQL 인젝션, 크로스 사이트 스크립팅, API 남용과 같은 정교한 공격으로부터 웹 애플리케이션과 API를 보호합니다. Cortex Cloud는 맞춤 구성된 적응형 보안을 제공함으로써 새롭게 등장하는 위협에 대해 마이크로서비스와 API가 유연하게 대응할 수 있도록 지원합니다.

클라우드 탐지 및 대응(CDR)

워크로드, ID, 네트워크 활동에 대한 심층적 가시성을 바탕으로 클라우드 네이티브 위협을 실시간으로 감지, 조사, 대응합니다. Cortex CDR은 런타임 원격 분석, 클라우드 제어 플레인 인사이트, AI 기반 분석을 통합하고 클라우드 보안과 SecOps를 연결하여 위협 요인을 탁월한 정확도로 감지합니다.

상관관계 분석을 자동화하여 단편적인 알림을 정확도 높은 인시던트로 전환함으로써 조사 속도를 향상하고 대응 시간을 단축합니다. 1,000개가 넘는 사전 구축된 플레이북과 자동화된 문제 해결 기능을 통해 위협이 확대되기 전에 소스 단계에서 격리할 수 있습니다.

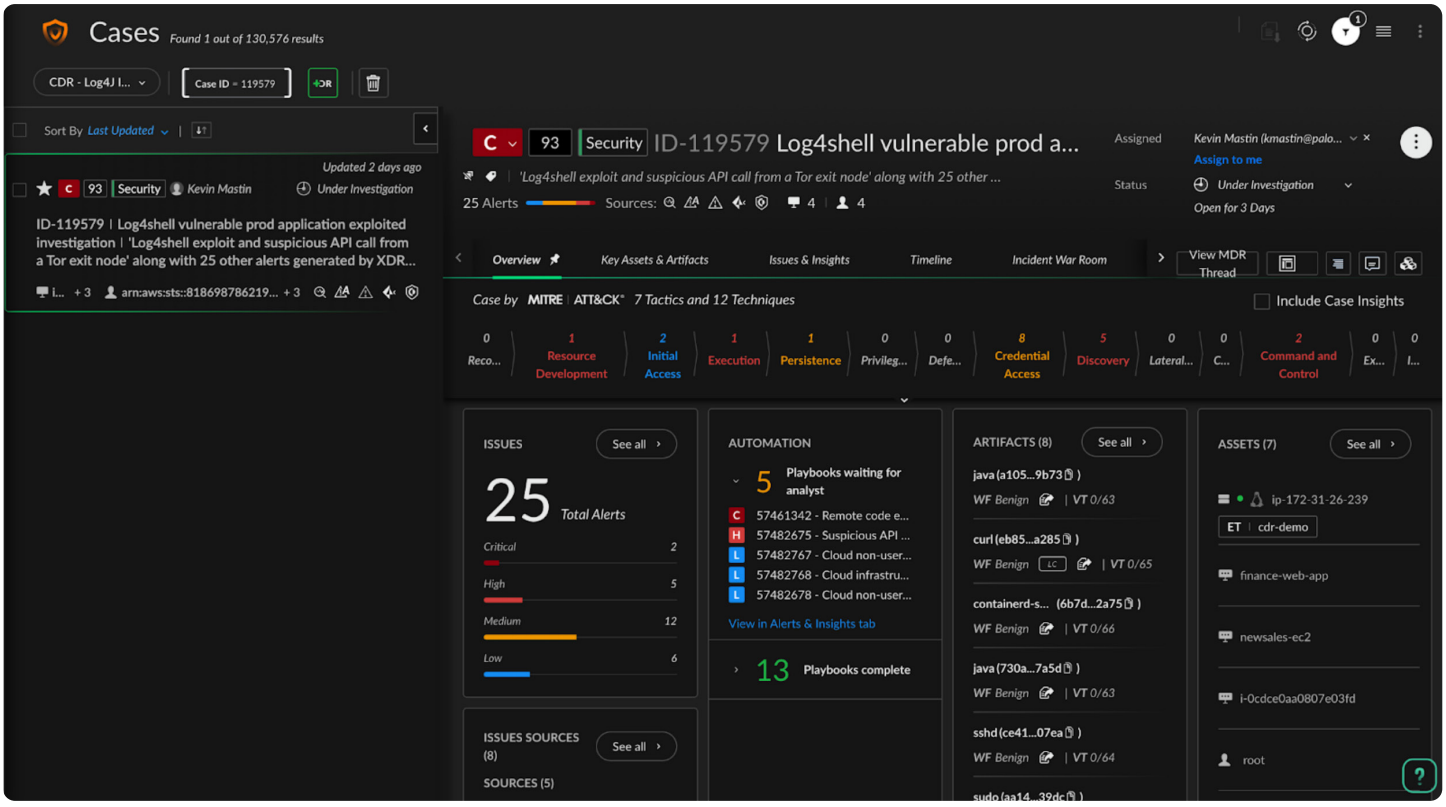

그림 2: AI 및 분석을 활용하여 여러 알림을 우선순위가 높은 사례로 자동 집계하는 Cortex Cloud

클라우드 공격에 대비하는 선제적 런타임 보안

클라우드 공격은 빠른 속도로 진행되며, 워크로드, 컨테이너, API 전반에 걸쳐 취약점을 노립니다. 보안팀에게는 가시성뿐 아니라 탐지, 차단, 대응 역량 또한 필요합니다.

Cortex Cloud 런타임 보안은 AI 기반 런타임 보호, 실시간 위협 탐지, 자동 대응을 통해 선제적 방어 기능을 제공합니다. SOC 운영과 클라우드 보안을 통합한 Cortex Cloud는 공격자보다 한발 앞서 움직이고 리스크를 줄이며 대규모 클라우드 환경을 보호할 수 있도록 도와드립니다.

Cortex Cloud 런타임 보안이 클라우드 보안을 변화시키는 모습을 직접 확인해 보세요.

실제로 구현된 CORTEX CLOUD 살펴보기

paloalto NETWORKS

서울특별시 서초구 서초대로74길 4,
1층 (삼성생명 서초타워)

Tel: +82-2-568-4353
eMail: Sales-KR@paloaltonetworks.com
www.paloaltonetworks.co.kr

© 2025 Palo Alto Networks, Inc. 미국 및 여타 관할권에서 사용되는 당사의 등록 상표 목록은 https://www.paloaltonetworks.com/company/trademarks.html에서 확인할 수 있습니다. 여기에 언급된 다른 모든 표시는 각각 해당 회사의 상표일 수 있습니다.

cortex_sb_cloud-runtime-security_020425