paloalto NETWORKS | CORTEX CLOUD

모든 조직이 반드시 알아둬야 할 새로운 클라우드 공격

실시간 보호는
침해 방지에 필수적입니다.

7.5억+
2025년까지 예상되는 클라우드 네이티브 애플리케이션[1]

80%
클라우드 환경에서 발견된 노출 비율[2]

66%
작년 한 해 동안 증가한 클라우드 공격[3]

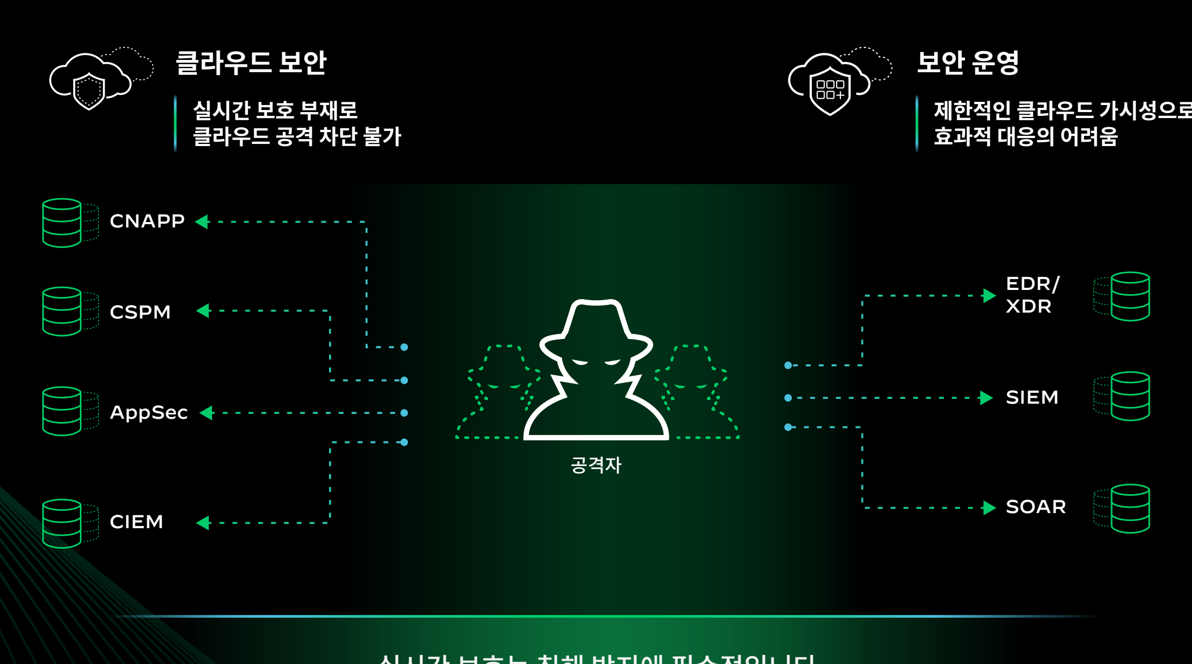
517만 달러
퍼블릭 클라우드 데이터 침해의 평균 비용[4]

조직에 필요한 것은혁신적인 접근법으로, 클라우드 보안과 보안 운영 팀 사이의 장벽을 허물고, 민첩성을 발휘하여 위협을 **탐지**, **조사**, 및 **대응하며** 공격의속도와 견줄 수 있는 솔루션입니다.

클라우드 보안 격차

공격자는 하나의 공격 표면에 집중하며
보안팀은 사일로에서 모니터링 및 대응

사일로로 위험한 사각지대가 생기며
클라우드 공격에 대한 취약점 발생



실시간 보호는 침해 방지에 필수적입니다.

현대 클라우드 보안의 주요 문제점

클라우드 보안을 특히 복잡하게 만드는 몇 가지 근본적인 문제가 있습니다.

동적 분석

클라우드 리소스는 일시적이며, 이제 기존의 보안 접근 방식은 적절하지 않습니다.

AI 기반 위협

공격자들은 AI를 활용하여 공격을 자동화하고 탐지를 회피합니다. 따라서 기존의 규칙 기반 보안으로는 클라우드 환경을 보호하기 어렵습니다.

실시간 가시성

기존의 도구는 피해가 발생한 후에야 위협을 탐지합니다. 클라우드 환경에서 알림을 발생시키고 공격을 차단하기 위해서는 즉각적인 가시성이 필요합니다.

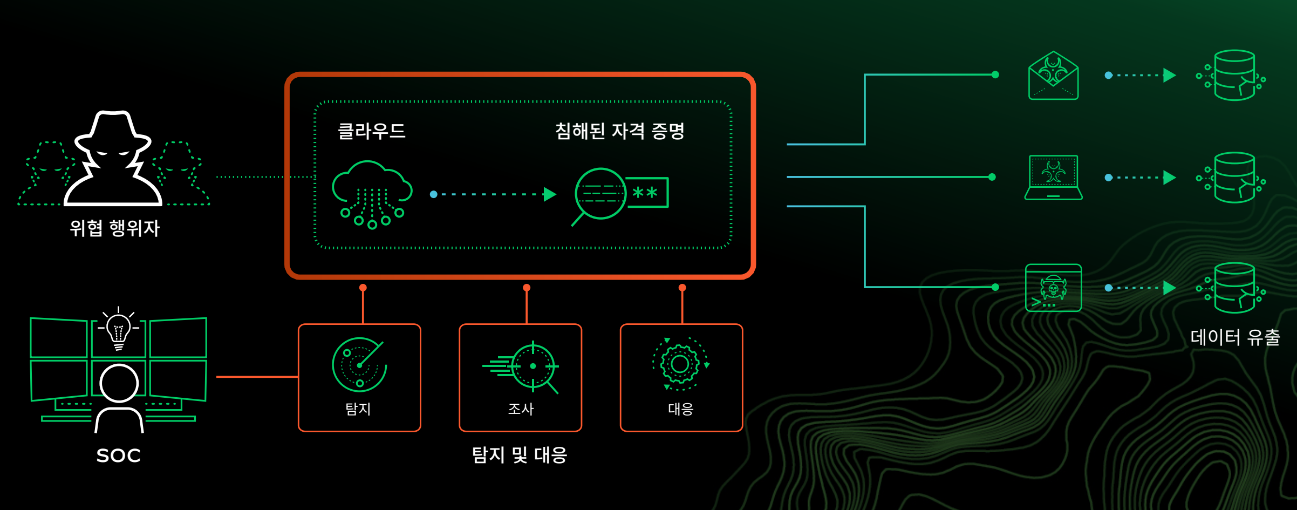
리스크 우선순위 지정

클라우드 환경에서는 매일 수천 개의 알림이 발생합니다. 런타임 컨텍스트가 없으면 즉각적인 조치가 필요한 위협을 효과적으로 판단할 수 없습니다.

보안 소유권

DevOps, SecOps, IT 팀 간에 책임이 분산되어 보안 대응의 혼란과 지연을 초래하며, 클라우드에 위험한 보안의 공백이 발생합니다.

더욱 확대되는 클라우드 위협 환경



공격자가 상호 연결된 클라우드 인프라를 악용하면서 클라우드 공격 표면이 급격히 확대되었습니다. 이제 자격 증명 침해 또는 구성 오류가 광범위한 피해를 초래할 수 있습니다.

클라우드 보안은 사후 고려 사항이 되어서는 안 됩니다. 조직에게 필요한 것은 코드, 클라우드, SOC에 걸친 포괄적 전략입니다.

빠른탐지 및 대응 능력이 필요하며, 이를 통해위협이 비즈니스에 지장을 주는 침해로확대되기 전에 차단해야 합니다.

주요 공격 벡터

사이버 범죄를 방지하는 Unit 42

대규모 자격 증명 수집

대규모 조직적인 공격 캠페인에서는 수천 개의 도메인에 걸쳐 환경 변수(.env) 파일을 표적으로 삼아 자격 증명 수집을 시도했습니다. 특히 클라우드 서비스 플랫폼의 API 키와 호스팅된 애플리케이션의 OAuth 토큰을 집중적으로 노렸습니다. 이번 공격의 전례 없는 규모는 TA가 하드코딩된 자격 증명과 구성 오류를 악용하여 클라우드 환경에 액세스하는 방식을 보여줍니다.

111,000
표적 도메인 개수

90,000+
수집된 자격 증명 개수

7,000
클라우드 서비스 포털의 침해된 자격 증명 개수

1,200+
영향을 받는 조직 수

환경 유출 테크닉

공격 흐름의 분석을 통해 공격이 성공한 이유를 상세하게 파악하고, 유사한 공격을 탐지하는 데 도움이 되는 주요 위치와 기법을 확인할 수 있습니다.

1. 리소스 스캔

TA는 표적 도메인을 스캔하고 노출된 .env 파일을 찾아 공격을 시작했습니다. Cloud XDR 에이전트는 수집 작업을 탐지하여 이를 방지할 수 있습니다.

- 하드코딩된 자격 증명(CSP 구성)
- 노출된 .env 파일(CSP 구성)
- 해당 파일에 대한 액세스(XDR 에이전트)

2. 리소스 생성

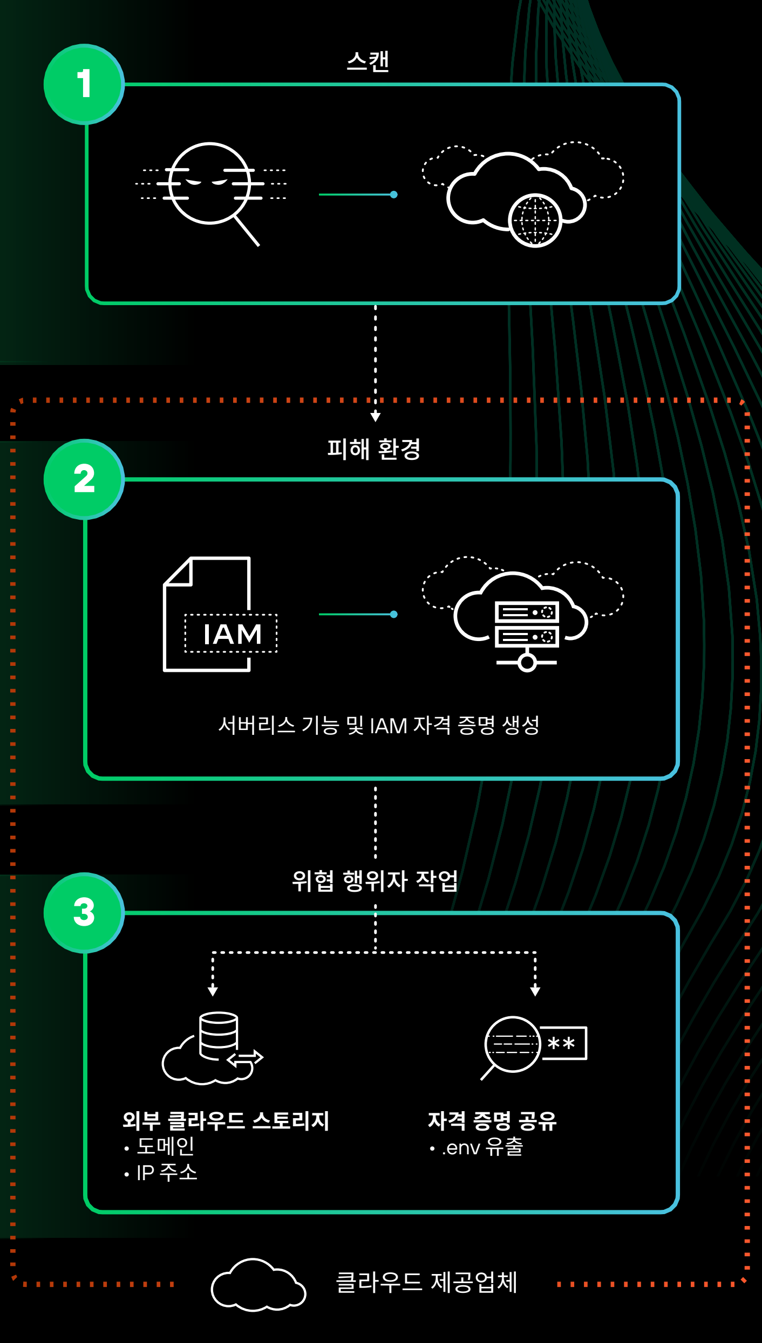
TA는 수집된 자격 증명을 악용하여 액세스 범위를 확장하고 새로운 리소스를 생성했습니다. 클라우드 탐지 및 대응(CDR)은 이처럼 신규 IAM 또는 서버리스 기능을 탐지합니다.

- 서버리스 함수 생성(CSP 로깅)
- IAM 생성(CSP 로깅)

3. 데이터 유출

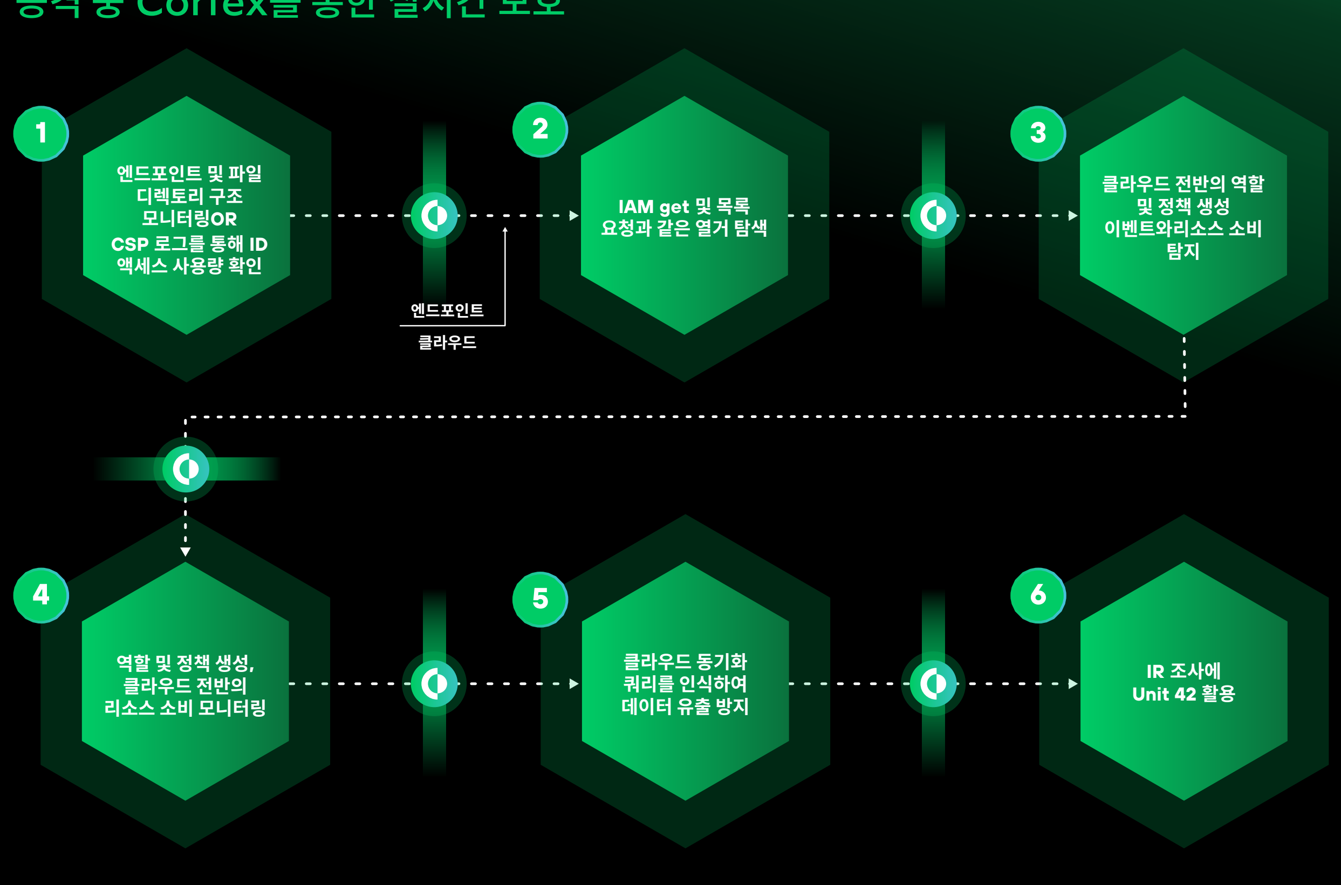
마지막으로, TA는 발견된 클라우드 데이터를 탈취했습니다. SOC 팀은 CDR의 데이터 이동 작업 탐지 기능을 활용하여 적절하게 대응할 수 있습니다.

- 데이터 동기화/이동(CSP 로깅)



최신 공격 경로의 실시간 차단

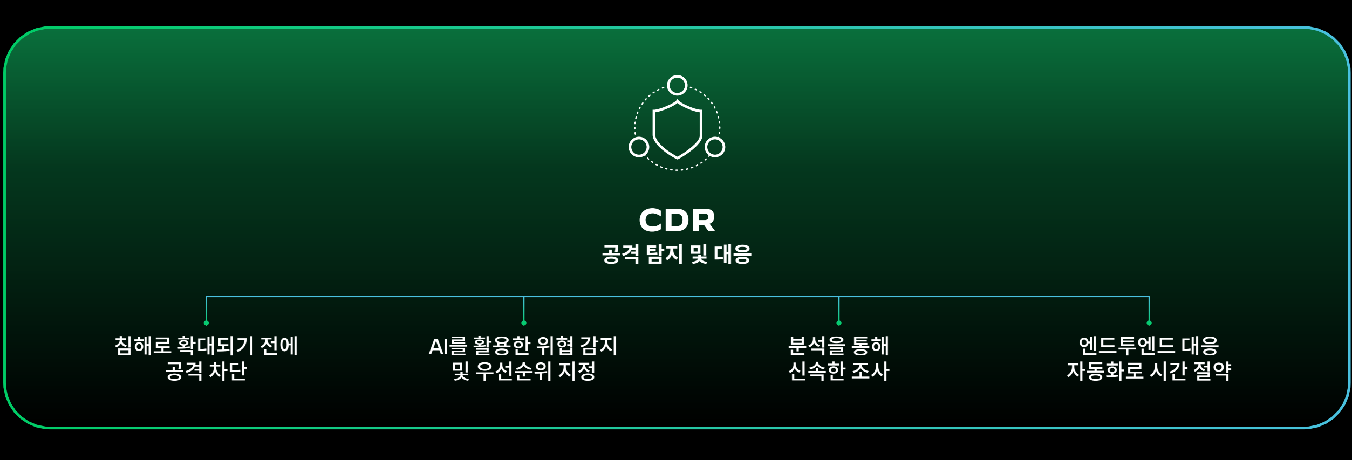
공격 중 Cortex를 통한 실시간 보호



클라우드 탐지 및 대응의 이점

SecOps 및 클라우드 보안팀에게는 클라우드 속도로 탐지하고 대응할 수 있는 통합 접근 방식이 필요합니다. 클라우드 워크로드는 수천 번까지 복제될 수 있으므로 취약점과 구성 오류를 신속하게 감지하는 것이 중요합니다. CDR은 AI 기반 예방, 실시간 탐지, 자동 대응 기능을 제공하여 침해가 발생하기 전에 SecOps 및 클라우드 보안팀이 인시던트를 차단할 수 있도록 지원합니다.

클라우드 탐지 및 대응에 대한 접근 방식



Cortex CDR은 보안 침해로 번지기 전에 공격을 차단하고가장 취약한 순간에 클라우드 환경을 보호합니다.

Cortex CDR은 광범위한 보안 전략에 클라우드 보호를 통합하는 AI 기반 보안 운영 체계를 제공합니다.
AI와 자동화의 힘을 직접 경험해 보세요. 운영을 간소화하고, 대규모 위협을 차단하고, 인시던트 복구 업데이트를 가속화하세요.

100%
MITRE ATT&CK®
평가의탐지점수 -
수정 또는 탐지 지연 없음

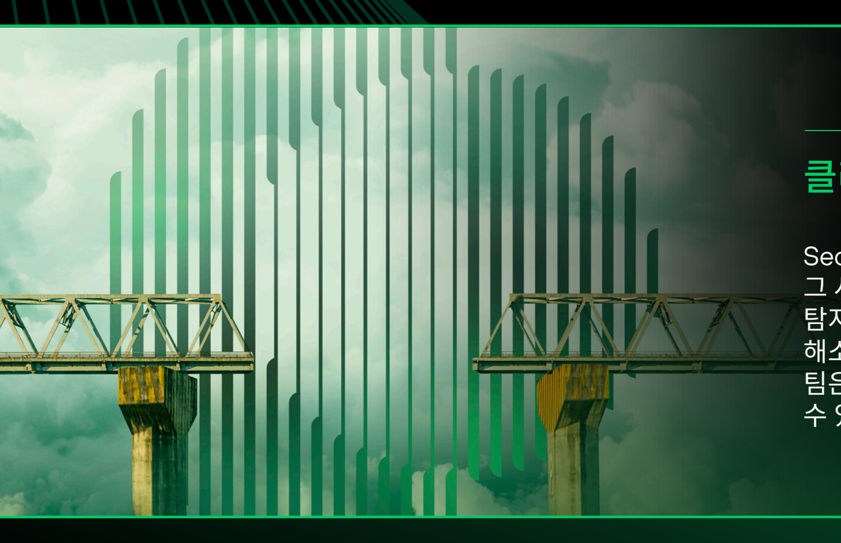
90%
평균 대응 시간(MTTR)
단축 - 며칠에서 몇 분으로

75%
AI 기반 자동화를 통한
애널리스트 업무량 축소

Cortex CDR
실시간 보호

Cortex CDR은 모든 클라우드 워크로드 및 애플리케이션을 대상으로 실시간 보호 기능을 제공합니다.

- **컨테이너와 Kubernetes®:** 코드부터 클라우드까지 컨테이너 및 Kubernetes 애플리케이션 보안 확보
- **호스트 및 VM:** 예방부터 시작하는 심층적 방어 접근법으로 호스트 및 VM 보호
- **서버리스 기능:** 전체 애플리케이션 수명 주기에 걸쳐 서버리스 기능 보호
- **클라우드 API:** 의심스러운 활동에 대해 API 모니터링 및 보호



클라우드 보안 공백 해결

SecOps와 클라우드 보안팀이 각자 작업하는 환경에서, 공격자는 그 사이의 간극을 이용합니다. Cortex CDR은 AI 기반 보호, 실시간 탐지 및 자동 대응 기능을 통해 팀을 통합하여 이러한 공백을 해소합니다. 그 결과 위협은 며칠이 아니라 몇 분 안에 차단되며, 팀은 현대적인 공격의 속도와 규모에 맞춰 클라우드 환경을 보호할 수 있습니다.

지금 바로 클라우드 보안을 혁신하세요

데모 요청

Cortex CDR 자세히 알아보기

---

[1] "IDC FutureScape: The Digital Business Era Has Arrived, Augmented by GenAI," IDC, 2023년 11월 29일.
[2] 2023년 Unit 42 공격 표면 위협 보고서, Palo Alto Networks, 2023년 9월 14일.
[3] 2024년 Unit 42 인시던트 대응 보고서, Palo Alto Networks, 2024년 2월 20일.
[4] Cost of a Data Breach Report 2024, IBM Security, 2024년 7월 30일.

paloalto NETWORKS | CORTEX CLOUD