클라우드 탐지 및 대응(CDR) 핵심 요소

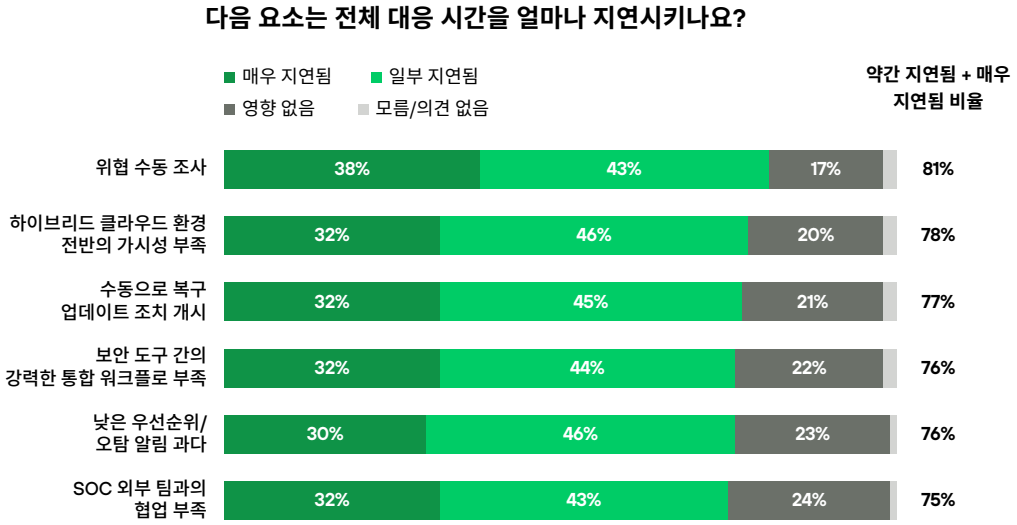
목차

클라우드 보안의 과제 이해

클라우드 보안 및 보안 운영 팀은 위협을 탐지하고 대응하는 과정에서 어려운 과제를 마주하고 있습니다. 이들은 위협이 침해로 확대되기 전에 한발 앞서 이를 발견하고 차단하는 중요한 임무를 맡고 있지만, 만성적으로 발생하는 과제들은 이들의 성공에 걸림돌이 됩니다.

과도한 알림에 의한 **알림 피로**는 팀의 시간을 낭비하며, 위협을 적절하게 분석하고 우선순위를 지정하는 것은 불가능에 가깝습니다. **가시성이 부족**해 효과가 저해되며, 특정 시점에 제한된 기존 스캔 도구는 취약한 클라우드 워크로드에 대한 실시간 위협 탐지나 즉각적 보호를 제공하지 못합니다. **클라우드 환경의 동적 특성** 자체도 문제입니다. 정적 네트워크 인프라를 고려하여 설계된 기존 보안 접근 방식으로는 지속적으로 변화하는 클라우드 워크로드에 적절한 대응을 할 수 없습니다.

뿐만 아니라, 많은 **기존 보안 솔루션**은 문제를 올바르게 파악한다 하더라도 유의미한 대응 조치를 취하지 못합니다.



81% 이상이 위협 수동 조사가 전체 대응 시간을 지연시킨다고 응답했습니다.

그림 1: 속도 / 대응 시간

출처: 글로벌 보안 운영 센터 연구 결과(Global Security Operations Center Study Results), IBM 및 Morning Consult, 2023년 3월

이러한 기존 도구는 클라우드 보안의 가장 큰 장애물이 되고 있으며, 이로 인해 발생한 취약점은 순식간에 공격의 대상으로 악용될 수 있습니다. 이러한 도구의 문제는 단순합니다. 간헐적으로 진행하는 취약점 스캔에 의존한다는 점입니다.

에이전트리스 스캔은 잠재적 리스크를 식별하는 데 매우 적합하지만, 스캔의 주기적 특성으로 인해 공격의 여지가 있습니다. 또한 경량 센서는 파일 무결성 변경, 네트워크 스캔과 같은 기본적인 의심 활동만 탐지할 수 있습니다. 고도화된 위협에 전혀 대비가 되어 있지 않으며, 제로데이 공격, 멀웨어 실행, 권한 에스컬레이션 공격을 방지하는 데 필요한 차단 기능이 부족합니다.

이러한 한계는 보안팀의 작업 지연을 야기할 뿐 아니라 가장 취약한 시점을 노려 취약점을 노출시킵니다.

오늘날의 고도화된 위협으로부터 조직을 철저하게 보호하기 위해서는 가시성과 탐지만으로는 충분하지 않습니다. 클라우드의 속도와 규모에 맞춰 실시간으로 작동하며 워크로드 수준에서 조직을 보호할 수 있는 솔루션이 필요합니다.

바로 이러한 지점에서 대두되는 것이 바로 클라우드 탐지 및 대응(CDR)입니다.

본 가이드에서는 CDR을 활용하여 클라우드 보안의 핵심 과제를 해결하는 방법을 살펴보고, CDR이 현대적 SecOps 전략의 핵심 요소로 자리 잡고 있는 이유를 알아봅니다. 다음 섹션에서는 기술 파악부터 비즈니스 영향 평가에 이르기까지, CDR 솔루션을 자신 있게 평가하고 도입하기 위해 필요한 모든 사항을 안내합니다.

클라우드 탐지 및 대응 소개

클라우드 탐지 및 대응(CDR)은 멀티 클라우드 환경에서 위협 방지, 탐지, 대응 기능을 제공하며, 클라우드 네이티브 탐지 및 대응(CNDR) 또는 클라우드 위협 탐지 및 대응(CTDR)이라는 명칭으로 불리기도 합니다. 에이전트 기반 및 에이전트리스 배포 옵션을 통해 클라우드 보안 보호, 실시간 가시성, 위협, 취약점, 구성 오류, 컴플라이언스 격차 식별 기능을 제공하며, 운영에 방해가 되지 않습니다.

CDR 작동 방식

CDR은 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP), 클라우드 워크로드 보호 플랫폼(CWPP)과 같은 보안 도구와 통합되어 의심스러운 활동을 탐지하고, 여러 클라우드 소스의 데이터 간 상관관계를 분석하여 즉시, 위협을 완화하는 조치를 취합니다.

CDR 기반 방어의 4가지 핵심 요소:

1. **런타임 보호** - 워크로드 인프라와 클라우드 네이티브 애플리케이션을 모두 보호하며, 호스트(VM), 컨테이너, Kubernetes, 서버리스 기능 등을 포함해 프로덕션 환경에서 실행 중인 워크로드를 지속적으로 모니터링합니다. 공격이나 이상 징후, 그 외 활성 상태의 위협 요소가 탐지되면 이를 격리하거나 방지하고 실시간으로 SOC에 알립니다.

3가지 CDR 핵심 과제

1. **클라우드 컨텍스트 부족:** 기존 도구는 클라우드 환경을 고려하여 설계되지 않았습니다. 따라서 클라우드 자산 간의 관계나 위협의 영향과 같은 중요한 컨텍스트를 놓치는 경우가 많습니다. 따라서 위협의 존재 여부나 대응 방법을 파악하기가 어렵습니다.
2. **비효율적 탐지 메커니즘:** 대부분의 솔루션은 현대적인 클라우드 네이티브 위협을 탐지하지 못합니다. 대신 과도한 알림과 오탐을 생성하며, 그 결과 분석가는 잘못된 알림을 추적하며 시간을 낭비하게 됩니다.
3. **제한적 격리 기능:** 위협이 탐지되면 일분 일초가 매우 중요합니다. 하지만 문제를 신속하게 격리하기 어려워 조직이 침해나 비즈니스 중단의 리스크에 노출됩니다.

3가지 CDR 기회

1. 실시간 보호를 통해 위협이 발생하는 즉시 이를 식별하고 차단하여 **클라우드 침해가 발생하기 전에 선제적으로 문제를 방지**합니다.
2. 중요한 알림을 표면화하고 근본 원인을 정확히 파악하는 컨텍스트 기반 클라우드 인텔리전스를 통해 **인시던트의 우선순위를 더 빠르게 지정하고 해결**합니다.
3. 사전 구축된 플레이북을 통해 위협이 주요 인시던트로 확대되기 전에 격리함으로써 **위협 대응을 가속화하고 자동화**합니다.

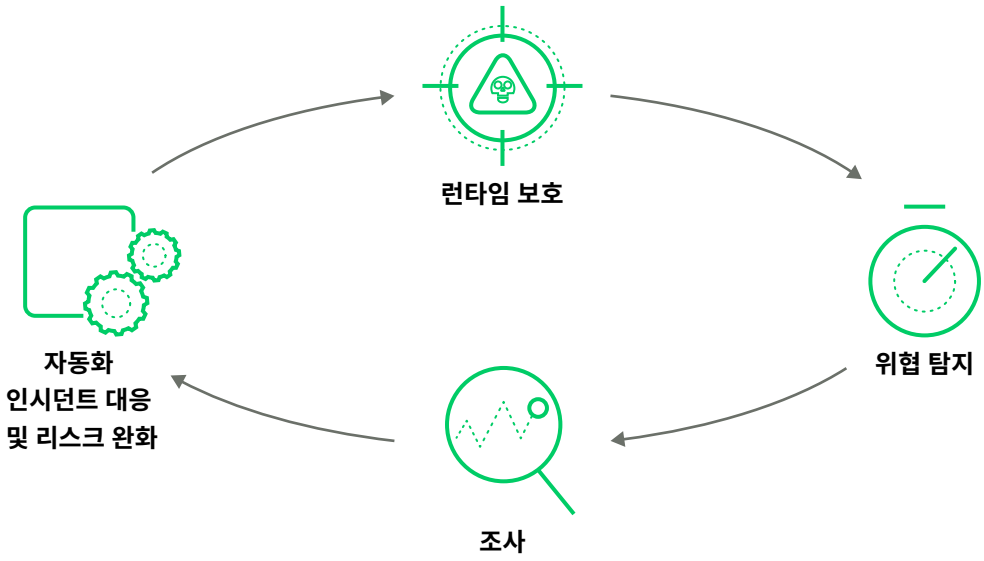


그림 2: 클라우드 탐지 및 대응 리스크 완화

2. **실시간 탐지** - 다양한 탐지 장치의 위협 신호를 수집하며, AI 기반 모델을 통해 즉시 위협을 파악합니다. 클라우드, 워크로드, 네트워크, 인프라, 런타임 에이전트 등 다양한 소스의 데이터를 결합하여 기존 클라우드 위협은 물론 신종 위협도 탐지할 수 있습니다. 일부 CDR 솔루션은 탐지한 이벤트를 MITRE ATT&CK(Adversarial Tactics, Techniques, and Common Knowledge) 프레임워크에 직접 매핑하여 공격 주기의 여러 단계에서 사이버 공격자의 움직임을 파악합니다.
3. **풍부한 컨텍스트 기반 조사** - 대량의 단편적 알림을 우선순위가 적용된 인시던트로 변환하여 공격의 전체적인 맥락을 파악할 수 있도록 지원합니다. 이를 통해 보안팀은 수동으로 데이터를 수집하고 상관관계를 분석하는 대신 조사에 집중할 수 있습니다. 이러한 컨텍스트를 활용하면 위협을 차단하거나 리스크의 근본 원인을 해결할 수 있습니다.
4. **자동 인시던트 대응** - 자동화를 통해 대응 시간을 크게 단축하고 분석가의 업무 부담을 줄입니다. 자동 인시던트 대응은 사전 구축된 플레이북이나 보안 오케스트레이션, 자동화 및 대응(SOAR) 도구를 활용하여 워크플로, 문제 해결, 침해 격리 작업을 자동화합니다. 과거의 인시던트를 바탕으로 AI 기반의 지속적 학습을 통해 자동화를 개선하고 미래에 대비합니다.

CDR로 해결할 수 있는 문제

공격자는 클라우드 인프라와 조직 구조를 구분하지 않습니다. 이들은 조직을 하나의 공격 표면으로 간주하고 여러 환경을 자유롭게 이동하면서 민감한 데이터를 훔치거나 운영 중단을 일으키며, 연결된 시스템에 멀웨어를 배포합니다.

클라우드와 온프레미스 리소스가 서로 밀접하게 연결되어 있기 때문에, 한 쪽에 침투하면 다른 쪽으로도 침투하여 랜섬웨어를 심거나 데이터를 유출할 수 있습니다.

예를 들어, 해커가 공개 저장소에서 탈취한 API 키로 클라우드 계정에 액세스하면, 추가 클라우드 리소스에 침투하여 권한을 상승시키고 데이터를 유출하거나, 멀웨어를 심거나, 크립토재킹 소프트웨어를 설치할 수 있습니다. 클라우드 리소스가 침해되면, 공격자는 기업 인프라와 연결된 애플리케이션, 서비스, ID와의 연결 지점을 찾아 온프레미스 리소스에 더 깊이 침투하는 크로스도메인 공격을 시작할 수 있습니다.

클라우드에서 발견되는 보안 노출 비율

지난 3년간 클라우드 공격

188%

증가

출처: Unit 42 공격 표면 위협 보고서, 2023 9월

이와 같은 침투 후 내부망 이동을 탐지하기 위해서는 IT 인프라 전반에 걸친 가시성과 대응 역량이 필요하며, 이를 지원하는 것은 오직 CDR뿐입니다.

문제	설명
클라우드 보안 태세에 대한 가시성 부족	SOC 분석가는 모든 클라우드 자산, 취약점, 구성 변경, 실행 중인 애플리케이션 등을 파악할 수 없습니다. 그 결과 관련성이 없어 보이는 대량 알림을 조사하기 어렵고, 도메인 간 공격을 놓칠 위험이 커집니다.
클라우드 환경의 개발 및 배포 속도	개발자는 지속적으로 새로운 코드를 배포하고, 인프라가 지속적으로 변경되며, 컨테이너나 VM과 같은 호스트가 빈번하게 생성되고 삭제됩니다. 그리고 공격자는 이보다 더 빠르게 움직입니다. 자산 인벤토리 태세와 알려진 취약점 목록을 24시간마다 스캔하여 업데이트할 경우, 공격자는 이러한 시간적 공백을 악용하여 내부망 이동, 권한 상승, 데이터 유출을 수행할 수 있습니다.
수동 프로세스에 의한 조사 지연 및 대응 방해	도구가 분산되어 있어 보안팀은 수동으로 협업과 워크플로를 수행해야 하므로 위협의 범위와 심각성을 적절하게 파악하기 어렵습니다. 이는 MTTR을 크게 지연시키고 조직을 지속적인 리스크에 노출시킵니다.
경고 우선순위 지정 불가	컨텍스트가 부족해 고위험 공격 경로를 파악할 수 없으며, 비즈니스 핵심 데이터와 애플리케이션에 영향을 미치는 활성 공격 및 취약점에 대한 알림의 우선순위를 지정할 수 없습니다.

CDR의 5가지 비즈니스 이점

CDR의 목표는 두 가지입니다. 공격이 침해로 확대되기 전에 차단하고, 문제를 최대한 빠르게 탐지하여 대응하는 것입니다.

이는 조직에 다음과 같은 이점을 제공합니다.

1. **침해 비용 대폭 절감**
   정교한 공격이 중요한 비즈니스 운영에 영향을 미치거나 민감한 데이터가 유출되기 전에 선제적으로 차단합니다.
2. **보안 팀의 효율성 향상**
   위협을 정밀하게 탐지하고 알림 피로를 제거하며, MTTR을 며칠에서 몇 분 단위로 단축할 수 있습니다.
3. **전략적 비즈니스 의사결정 지원**
   명확한 통합적 방식으로 공격을 시각화하여 정보 기반의 더 신속한 보안 대응을 뒷받침합니다.
4. **리소스 배분 최적화**
   고위험 위협의 우선순위를 자동으로 지정하여 중요도가 높은 이니셔티브에 집중할 수 있도록 지원합니다.
5. **운영 비용 절감**
   대응 워크플로를 자동화하여 수동 개입을 줄이고, 문제 해결 비용을 절감하며, 비즈니스 중단을 최소화합니다.

공격 가능성이 가장 높은 상호 연결된 클라우드 보안 결함을 자동으로 찾는 솔루션이 조직에 도움이 될 것이라는 데에 동의합니다.

출처: 2024년 클라우드 네이티브 보안 현황 보고서

SecOps 워크플로의 CDR 적용

CDR은 SOC 기술 스택에 적합한 추가 요소로서 실시간 모니터링, 지능형 분석, 자동 대응 메커니즘을 활용하여 클라우드의 이상 징후와 잠재적 보안 인시던트를 탐지합니다.

CDR & 엔드포인트 탐지 및 대응(EDR)

- 엔드포인트 보호와 클라우드별 위협에 모두 집중하며 EDR을 보완합니다.
- 클라우드 인프라와 엔드포인트를 모두 보호하는 통합 보안 접근 방식을 제공합니다.
- 클라우드 워크로드와 엔드포인트 간의 가시성 공백을 해소합니다.

CDR & 보안 정보 및 이벤트 관리(SIEM)

- 클라우드별 텔레메트리와 컨텍스트 기반의 인사이트로 SIEM 데이터 세트를 강화합니다.
- 알림 시스템을 통합하여 조율된 대응 메커니즘을 지원합니다.
- 클라우드, 하이브리드, 온프레미스 환경 전반에 걸쳐 통합된 가시성을 제공합니다.

CDR & 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)

- 런타임의 실시간 위협 탐지 및 대응을 통해 활성 상태의 클라우드 공격을 신속하게 차단합니다.
- 코드부터 빌드, 배포, 실행에 걸친 애플리케이션 라이프사이클 전반을 보호합니다. CNAPP는 배포 단계에 이르기까지 개발 환경을 보호하며, CDR은 런타임의 워크로드를 보호하여 코드에서 클라우드까지 지속적 보안을 보장합니다.
- CNAPP의 심층적 리스크 컨텍스트(구성 오류, 취약점, 노출)와 CDR의 실시간 탐지를 결합하여 더 빠르고 정확하게 위협의 우선순위를 지정하고 대응합니다.

CDR & 클라우드 워크로드 보호 플랫폼(CWPP)

- CWPP의 워크로드별 보호 기능을 광범위한 클라우드 환경으로 확장합니다.
- 서비스, 애플리케이션, 네트워크의 지속적 모니터링을 통해 보안을 강화합니다.
- 개발부터 런타임에 이르기까지 엔드투엔드 보호 기능을 제공합니다.

클라우드 탐지 및 대응 평가 체크리스트

강력한 위협 방지, 정밀한 위협 탐지, 민첩한 조사, 클라우드 환경의 자동 대응을 지원하는 핵심 기능과 역량을 고려하여 조직에 적합한 CDR 솔루션을 선택하세요.

다음 체크리스트는 CDR 솔루션 평가의 핵심 기준에 해당합니다.

1. **포괄적 런타임 보호**
   - **실시간 보호:** 행동 기반 위협, 취약점 악용, 악성 프로세스, 랜섬웨어, 멀웨어 등 고도화된 공격이 확산되기 전에 차단합니다.
   - **엔드투엔드 워크로드 보호:** VM, 컨테이너, Kubernetes, 서버리스 워크로드 전반에 걸쳐 일관된 보안을 구축하며, 다양한 클라우드 아키텍처와 원활하게 통합됩니다.
   - **익스플로잇 방지:** Log4Shell, SpringShell과 같은 취약점 익스플로잇을 차단합니다.
   - **멀웨어 차단:** 멀웨어, 랜섬웨어 및 파일리스 공격을 차단합니다.
2. **정밀한 위협 탐지**
   - **위협 인텔리전스:** 신종 위협 탐지 가속화에 대해 검증된 실적과 높은 신뢰성을 갖춘 위협 연구를 활용합니다.
   - **위협 탐지:** 머신 러닝(ML) 모델과 클라우드 컨텍스트를 위협 인텔리전스와 결합하여 기존 도구가 탐지하지 못하는 위협을 발견합니다. 독자적 및 공개적 위협 인텔리전스, 클라우드 제어 플레인, 데이터 플레인, 관리 플레인에 걸친 광범위한 데이터 세트를 통합한 ML 모델을 사용합니다.
   - **MITRE ATT&CK 매핑:** MITRE ATT&CK 프레임워크에 매핑된 탐지 결과를 활용하여 공격 주기에 대해 명확한 인사이트를 제공합니다. 분석 및 ML을 통해 고급 클라우드 위협을 자동으로 탐지하며, 탐지 결과가 MITRE ATT&CK 전술에 매핑됩니다.
3. **조사 가속화**
   - **공격 경로 분석:** 단편적인 알림을 일관된 공격 내러티브로 통합하여 최초의 침해 지표부터 인시던트에 대한 전체적 관점을 제공합니다.
   - **근본 원인 분석:** 클라우드 환경에 대한 포괄적 가시성을 통해 인시던트의 근본 원인을 신속하게 파악하여 수동 조사에 소요되는 시간을 줄입니다.
   - **지능형 리스크 점수 책정:** AI 기반 리스크 우선순위 지정을 통해 고위험 인시던트를 우선적으로 표면화하여 알림 피로를 해소하고, 관련 자산, 위협 인텔리전스, 과거 패턴 전반의 심각도에 따라 알림을 처리할 수 있도록 지원합니다.
   - **컨텍스트 기반 가시성:** 위협 탐지 및 분석에 컨텍스트와 텔레메트리 데이터를 활용해 조사를 가속화합니다. 조직 전체의 위협 활동에 클라우드 컨텍스트를 통합합니다.
   - **인시던트 관리:** 관련 알림을 인시던트로 그룹화하여 영향을 받은 호스트와 사용자, 주요 아티팩트를 포함한 공격의 모든 요소를 보여주는 인시던트 관리 뷰를 제공합니다.
4. **자동화된 대응**
   - **자동화된 플레이북:** 수동 개입 없이 인시던트를 격리하고, 오탐을 처리하고, 리스크를 완화하는 광범위한 자동 워크플로 라이브러리를 제공합니다.
   - **대응 시간 단축:** 반복적 작업을 자동화하고 문제 해결 전술에 대한 지침을 제공하여 MTTR을 축소합니다.
   - **대규모 리스크 복구:** 원활한 공격 차단 및 권장 해결 방안에 대한 지능형 추천을 제공합니다.
   - **통합 및 자동화:** 다른 보안 도구와 통합하여 클라우드 오케스트레이션, 알림 보강, 협업, 플레이북 기반 대응을 제공합니다.

5. 플랫폼 및 아키텍처 지원

› **클라우드 커버리지:** 퍼블릭, 프라이빗, 하이브리드, 멀티 클라우드 환경에서 클라우드 워크로드를 보호합니다.
› **에이전트 및 에이전트리스 배포:** 환경적 요구사항과 조직의 목표에 따라 에이전트 기반 배포와 에이전트리스 배포 중 원하는 것을 유연하게 선택할 수 있습니다.
› **운영 체제 지원:** 조직에게 필요한 Windows 운영체제, Linux 배포, 호스트, 서버리스 워크로드를 지원합니다.

Cortex® CDR을 통한 클라우드 공격 경로 차단

Cortex® Cloud Detection and Response(CDR)를 활용하여 공격이 침해로 확대되기 전에 선제적으로 차단하세요. 단일 데이터 레이크를 기반으로 구축된 CDR은 AI와 자동화를 활용해 클라우드 환경 전반에서 위협을 탐지, 조사, 대응하며 탁월한 가시성과 보호 기능을 제공합니다.

Cortex CDR의 기능:

- **최고 수준의 실시간 보호**: 클라우드 공격이 침해로 확대되지 않도록 방지합니다.
- **지능형 탐지**: 세계 최고 수준의 위협 인텔리전스와 AI에 기반한 고급 탐지 기능으로, 알려진 위협과 알려지지 않은 위협을 모두 식별합니다.
- **자동화된 플레이북**: 인시던트 대응 시간을 며칠에서 분 단위로 단축합니다.

검증된 Cortex CDR:

- 2024 MITRE Engenuity ATT&CK 평가에서 증명된 **100% 탐지율 및 강력한 보호**
- 대응 시간이 며칠에서 분 단위로 단축되며 **MTTR 90% 감소**
- **분석가 업무량 75% 감소**: 수동 작업 및 알림 피로 감소

Cortex Cloud를 직접 체험해 보시겠어요? 데모 예약

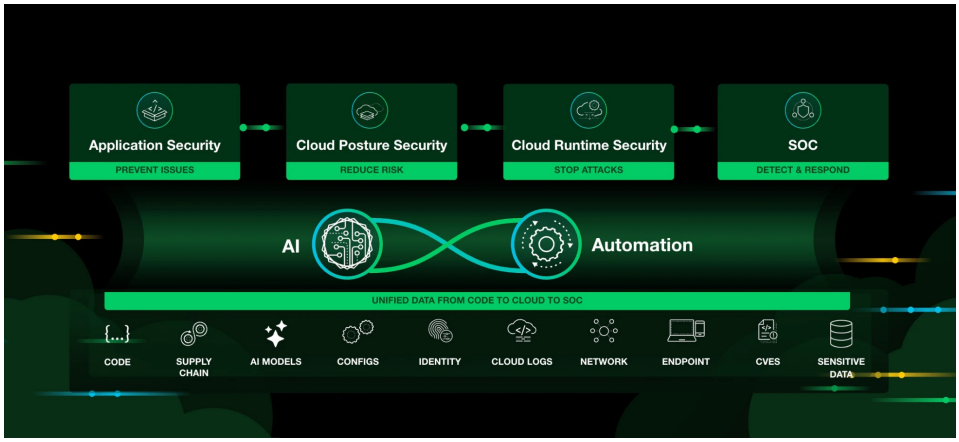


그림 3: Cortex Cloud는 코드부터 클라우드, SOC에 이르기까지 조직을 보호합니다.

paloalto NETWORKS

서울특별시 서초구 서초대로74길 4,
1층 (삼성생명 서초타워)
Tel: +82-2-568-4353
eMail: Sales-KR@paloaltonetworks.com
www.paloaltonetworks.co.kr

cortex_ds_the-essentials-of-cloud-detection-and-response-(cdr)_061225