AKAMAI 체크리스트

제로 트러스트 플랫폼 기능

효과적인 제로 트러스트 플랫폼을 갖추면 ZTNA(Zero Trust Network Access), 마이크로세그멘테이션, DNS 방화벽, 위협 탐색 등 개별적인 포인트 솔루션을 단일 콘솔 플랫폼으로 통합할 수 있습니다. 제로 트러스트를 빠르고 효과적으로 배포한다는 것은 랜섬웨어를 차단하고, 까다로운 컴플라이언스 의무를 준수하고, 분산된 인력과 하이브리드 클라우드 인프라를 보호한다는 것을 의미합니다. 이 체크리스트는 벤더사의 기능을 평가하는 데 사용하거나 단일 플랫폼으로 제로 트러스트를 구축하기 위한 요구사항 목록으로 사용할 수 있습니다.

카테고리 1: 플랫폼 요구사항

제로 트러스트 플랫폼 솔루션은 유연하고, 확장 가능하고, 관리하기 쉬워야 합니다.

- [ ] 트래픽 수요에 대응하고 성능 저하 없이 지속적인 보안을 제공하는 확장성
- [ ] SIEM, SOAR, EDR, CMDB 등 고객이 현재 사용 중인 기존 보안 툴과의 통합 가능성
- [ ] 하이브리드 및 멀티클라우드 환경, 레거시 시스템, 최종 사용자 디바이스, 쿠버네티스 클러스터, 가상 머신, IoT 및 OT 환경 등을 포함한 이기종 데이터 센터 지원
- [ ] 클라우드, 가상, 온프레미스 등 다양한 하이브리드 아키텍처를 지원하는 유연한 배포 모델
- [ ] 에이전트 기반 및 에이전트리스 배포(IoT 및 OT, PaaS)를 모두 수용하는 기능
- [ ] 레거시 운영 체제뿐만 아니라 Windows, Linux, macOS 지원
- [ ] 모든 작업 기록을 보장하는 감사 로그 기능

카테고리 2: 가시성 요구 사항

환경을 이해하고 의심스러운 연결을 식별하며 위협에 신속하고 정확하게 대응하기 위해서는 심층적인 가시성이 중요합니다.

- ☐ 모든 애플리케이션과 워크로드 흐름을 지도처럼 시각화하고 컨테이너, 서버리스, IaaS, PaaS 등 모든 환경에서 단일 콘솔을 통해 애플리케이션 접속
- ☐ 조사 및 포렌식을 위한 기록 및 실시간 플로우
- ☐ 스위치 디바이스와 같은 써드파티 방화벽 및 하드웨어와의 상호 운용성
- ☐ 맥락에 맞는 레이블과 룰을 위해 CMDB, EDR, 클라우드 API 등 다양한 써드파티 소스에서 데이터를 수집할 수 있는 기능
- ☐ 레이블링 지원, 가급적이면 속도와 정확성을 위해 AI 활용

카테고리 3: 정책 요구사항

랜섬웨어 보호, 원격 인력 보호, 제로데이 대응, 컴플라이언스 등 다양한 사용 사례에 적용 가능한 속성을 기반으로 동서(마이크로세그멘테이션) 및 남북(ZTNA) 정책을 한 곳에서 모두 적용합니다.

- ☐ 초크 포인트를 생성하는 물리적 내부 방화벽 없이 소프트웨어로 정의되고 기업 전체에 분산되는 정책
- ☐ IP와 포트뿐만 아니라 다양한 워크로드 속성을 기반으로 생성된 룰
- ☐ 세분화된 애플리케이션 중심 정책을 적용해 포트, 프로세스, 서비스 수준까지 워크로드 보호
- ☐ 기본 제공 및 사용자 정의 템플릿으로 정책 생성을 가속화하는 정책 권장사항 엔진(가급적 AI 활용)
- ☐ 에이전트 유무에 관계없이 정책 적용
- ☐ 포괄적인 플로우 매핑 기반의 정책 제어
- ☐ 업계 모범 사례를 기반으로 글로벌 리스크 감소에 도움을 주는 사전 구성된 정책
- ☐ 가상화, IaaS, PaaS 환경 전반의 하이브리드 클라우드를 위한 정책
- ☐ 워크로드가 이동, 전환 또는 변경되는 경우 이를 추적할 수 있는 기능으로 워크로드와 연결되는 정책
- ☐ 사무실 및 원격 근무 사용자를 위한 접속 정책

카테고리 4: 제로 트러스트 구성요소 요구 사항

통합 제로 트러스트 플랫폼에 통합된 다양한 기능 중 제로 트러스트 네트워크 접속과 마이크로세그멘테이션은 가장 핵심적인 요소입니다. 기업은 이러한 기술을 통해 인력 및 비즈니스 연속성에 부정적인 영향을 주지 않고 제로 트러스트 제어를 배포할 수 있습니다.

- ☐ 통합 접속 및 네트워크 정책 엔진(동서 및 남북 제어 결합)
- ☐ FIDO2 MFA(Multi-Factor Authentication)를 통한 강력한 ID 적용
- ☐ DNS 트래픽을 모니터링하고 필터링해 광범위한 위협으로부터 IT 환경과 사용자를 보호하는 기능
- ☐ 탐지하기 어려운 위협의 지속적인 탐지 및 보안 체계 모니터링
- ☐ 공격자가 접속 메커니즘을 뚫더라도 이를 차단할 수 있는 플랫폼 툴 간 신호 공유
- ☐ 공격자를 추적하고 격리할 수 있는 동적 디셉션 시스템 도입
- ☐ 엔드포인트 또는 서버에 취약점이 있는지 쿼리해 랜섬웨어 탐지를 신속하게 방어하는 기능

카테고리 5: 통합 AI 요구 사항

AI를 사용하면 제로 트러스트를 효과적으로 구축하기 위한 여러 기능을 간소화할 수 있습니다. 이를 통해 정책 수립, 컴플라이언스, 인시던트 대응, 취약점 평가를 신속히 처리하고 간소화할 수 있습니다.

- ☐ 네트워크 로그와 통신해 인시던트 대응 시간, 컴플라이언스 범위 지정 노력 등을 단축하는 데 도움이 되는 자연어 사용
- ☐ 고유한 트래픽 패턴을 기반으로 라벨과 정책을 제안하는 AI로 전체 정책 프로세스 간소화
- ☐ IOC를 리서치하거나 사용자 지정 쿼리를 작성할 필요 없이 네트워크의 취약점을 빠르게 찾아내도록 자연어를 구문으로 번역
- ☐ AI 위협 탐색 메커니즘으로 기존 툴이 놓치는 비정상과 악성 활동을 찾아내는 고급 탐지 방법 지원

자세한 내용은 Akamai 제로 트러스트 보안을 참조하시기 바랍니다.

©2024 Akamai Technologies | 지원 |
| 2024년 4월 발행