AKAMAI 솔루션 설명서

Akamai Guardicore Segmentation를 활용해 인시던트 대응 및 랜섬웨어 방어 솔루션을 강화한 Deloitte

도전과제

견고하게 구축된 보안 제품 카테고리는 최신 위협에 대한 기업 네트워크의 보안 수준을 높여줍니다. 그러나 온프레미스 하드웨어, 클라우드에서 호스팅되는 워크로드, 최종 사용자 디바이스, 컨테이너 등 악성 측면 이동을 방어해 공격표면을 줄이는 포괄적인 단일 솔루션 방식을 제공하는 솔루션은 거의 없습니다. 기존의 방화벽, EDR 등 기존 보안 제품을 우회하는 공격을 차단하는 프로젝트를 실행하려면 기술적 제약과 인적 전문성의 한계로 인해 기업 고객이 초기 제로 트러스트 세그멘테이션 이니셔티브를 완료하는 데 몇 년은 아니더라도 수개월이 걸렸습니다.

기업 고객은 세그멘테이션 프로젝트에 접근할 때 일반적으로 다음과 같은 문제에 직면합니다.

- 모든 환경의 모든 자산, 네트워크 흐름, 사용자, 연결에 대한 가시성 부족
- 하이브리드 클라우드 인프라, 레거시 운영 체제, OT/IoT 등 서로 다른 기술 및 인프라에 대한 보안 관리의 제약
- 기존 세그멘테이션 기술에서 종종 발생하는 다운타임을 방지해 비즈니스 연속성을 보장해야 할 필요성
- 제로 트러스트를 지원하는 이니셔티브를 구축, 배포, 관리할 수 있는 보안 리소스 및 인재 부족

솔루션의 특징

Akamai Guardicore Segmentation은 가장 간단하고, 빠르고, 직관적으로 네트워크에 제로 트러스트 원칙을 적용하는 방법을 제공하는 호스트 기반의 마이크로세그멘테이션 솔루션입니다. Akamai Guardicore Segmentation은 에이전트 기반 센서, 네트워크 기반 데이터 수집기, 가상 프라이빗 클라우드 흐름 로그를 혼합해 네트워크를 매핑하는 방식으로 레거시 및 최신 운영 체제, 운영 기술, IoT 디바이스를 비롯한 모든 자산과 인프라를 하나의 시각으로 제공합니다. 이를 통해 원치 않는 통신을 제한하는 정책을 쉽게 생성하고 적용함으로써 공격표면을 줄이고 비즈니스 연속성을 보장할 수 있습니다.

대표적인 사용 사례

- **동서 트래픽 제어**
  통신할 필요가 없는 환경, 애플리케이션, 사용자, 인프라 분리
- **랜섬웨어 방어**
  다양한 종류의 랜섬웨어 공격에 사용되는 것으로 알려진 공격 경로를 차단하기 위해 AI/ML이 포함된 정책 템플릿 배포
- **애플리케이션 링펜싱**
  비즈니스 크리티컬 애플리케이션의 구체적인 의존성에 집중해 보안을 엄격하게 제어

- **사용자 기반 세그멘테이션**
  사용자가 업무에 필요하지 않은 애플리케이션, 환경, 디바이스에 접속하지 못하도록 차단
- **감염된 디바이스 격리**
  하나 이상의 디바이스가 감염된 경우 유출 확산 억제
- **컴플라이언스**
  네트워크, 디바이스, 잠재적 공격 경로에 대한 심층적인 맥락 이해를 통해 컴플라이언스에 즉각적으로 대응

고객이 얻는 혜택

- 서버, 엔드포인트, 클라우드, 컨테이너, 사용자 등을 포함해 전체 네트워크 및 연결을 보여주는 단일 창으로 가시성 문제 해결
- 제로 트러스트 정책을 시행해 랜섬웨어 공격의 성공 가능성 차단
- 위협 인텔리전스 및 포괄적인 유출 탐지 및 사기 기능을 사용해 인시던트 대응 시간 단축
- 실시간 및 기록 기능을 모두 사용해 네트워크 포렌식 및 컴플라이언스 프로젝트 간소화

Deloitte의 전문성

1. **자문**
   기업 고객은 영향력 있는 사이버 보안 의사 결정 지원, 보안 격차 분석, 구축 로드맵 작성에 대한 Deloitte의 경험을 통해 유출이 발생했을 때 뿐만 아니라 미래를 계획할 때도 적절한 의사 결정을 내릴 수 있습니다.
2. **전문 서비스**
   완전한 매니지드 구축 서비스는 물론 기존의 보안, ITSM, 클라우드 솔루션과의 맞춤형 통합 서비스를 제공합니다.
3. **인시던트 대응 관리 서비스**
   유출을 억제하고 향후 인시던트 예방을 지원하는 Deloitte의 인시던트 대응 전술가로부터 즉각적이고 정밀한 지원을 받을 수 있습니다.
4. **라이선스 구독**
   Deloitte는 다양한 방식으로 라이선스 구독을 지원합니다.

고객 사례 연구 - Akamai와 Deloitte가 고객의 랜섬웨어 문제를 해결하는 방법

주요 랜섬웨어 사건으로 인해 고객들은 중요한 시기에 즉각적인 도움을 줄 수 있는 컨설팅과 솔루션을 찾게 되었습니다. Deloitte는 인시던트 대응 및 보안 팀의 역량을 결합하고 네트워크 가시성, 유출 포렌식, Akamai Guardicore Segmentation이 제공하는 공격표면 감소를 위한 후속 조치를 통해 도움이 필요한 고객에게 성공적인 조합을 제공했습니다.

배경

핵심적인 비즈니스 운영을 중단시키는 심각한 랜섬웨어 이벤트를 경험한 한 기업은 문제를 어떻게 해결해야 할지 몰랐습니다. 수천 대의 서버로 구성된 데이터 센터 전체가 감염됐고, 유출을 안전하게 즉시 봉쇄해야 했습니다. 고객은 Deloitte의 안내에 따라 전화를 걸어 대응 방안을 문의했습니다. Deloitte 팀은 이미 Akamai Guardicore Segmentation를 제안하고 배포할 준비가 되어 있었기 때문에 고객은 공격 규모에 대한 가시성을 신속하게 확보하고, 영향을 받은 자산과 애플리케이션을 파악하고, 모든 관련 애플리케이션의 의존성을 확인할 수 있었습니다.

솔루션

Akamai Guardicore Segmentation은 고객의 전체 환경을 개별 프로세스 수준까지 매핑함으로써 감염된 인프라에서 멀웨어가 이동했을 수 있는 모든 잠재적 경로를 파악할 수 있었고, Deloitte 팀은 이를 바탕으로 네트워크의 특정 부분에 집중해 추가 포렌식 분석을 수행할 수 있었습니다. 이를 통해 고객이 비즈니스 운영과 데이터 센터에 대한 접속을 복구한 후에도 감염된 디바이스가 남아 있지 않도록 했습니다.

결과

랜섬웨어 공격이 해결되고 데이터 센터가 다시 온라인 상태가 되어 비즈니스 운영이 재개된 후, 이러한 공격이 다시 발생할 가능성을 줄이기 위한 조치를 취했습니다. 많은 기업 고객과 마찬가지로 이 고객도 디바이스, 애플리케이션, 사용자 등을 보호하기 위해 여러 주요 솔루션으로 레이어된 보안 접근 방식을 사용합니다. 하지만 피싱 이메일처럼 단순한 요소가 공격자의 게이트웨이가 될 수 있기 때문에, 이러한 솔루션만으로는 공격을 막기에 충분하지 않았습니다. 고객은 네트워크, 애플리케이션 의존성, 데이터 센터에 접속할 수 있는 사용자에 대한 전체 맥락을 통해 정밀한 마이크로세그멘테이션 제어를 구축함으로써 향후 랜섬웨어 유출이 발생할 수 있는 경로를 크게 줄일 수 있었습니다.

솔루션의 가치를 경험하고 Deloitte의 전문성에 대한 신뢰가 강해진 고객은 제로 트러스트 세그멘테이션을 계속 제공하기 위해 솔루션을 유지하기로 결정하고 Deloitte에 일상적인 기술 관리를 요청했습니다.

요약

Deloitte는 고객의 제로 트러스트 프로젝트를 실행한 경험과 심도 있는 기술 전문성을 바탕으로 고객을 위해 Akamai Guardicore Segmentation를 전문적으로 배포하고 관리할 수 있는 이상적인 파트너입니다. 고객은 Deloitte를 믿고 이 기술을 공격표면 감소, 측면 이동 제어, 애플리케이션 링펜싱, 랜섬웨어 방어 등 모든 보안 이니셔티브에 활용할 수 있습니다.

Deloitte 소개

Deloitte는 Fortune 선정 500대 기업의 약 90%와 7000개 이상의 민간 기업을 포함해 세계에서 가장 존경받는 많은 브랜드에 업계 최고의 감사, 컨설팅, 세무 및 자문 서비스를 제공합니다. Deloitte의 직원들은 공공의 이익을 위해 힘을 합쳐 오늘날 시장을 주도하고 형성하는 다양한 업계에 종사하며 자본 시장에 대한 대중의 신뢰를 강화하고, 고객이 도전을 혁신과 성공의 기회로 인식하도록 영감을 주고, 더 강력한 경제와 더 건강한 사회를 향한 길을 선도하는 데 도움이 되는 측정 가능하고 지속적인 성과를 제공합니다. Deloitte는 고객에게 가장 중요한 시장에서 서비스를 제공하는 세계 최대 규모의 글로벌 전문 서비스 네트워크의 일원이 된 것을 자랑스럽게 생각합니다. 175년 이상의 서비스를 바탕으로 구축된 회원사 네트워크는 150개 이상의 국가와 지역을 아우릅니다. 전 세계 41만 5천여 명의 Deloitte 직원들이 어떻게 영향력을 발휘하고 있는지 알아보려면 deloitte.com을 방문하세요.

연락처

Ola Sergatchov
Akamai 글로벌 전략 제휴 책임자
osergatc@akamai.com

©2024 Akamai Technologies | 지원 | 2024년 3월 발행