Case Study

보안 가시성 확보가 핵심, R사의 EDR 구축 성공기

산업

여신전문금융업

혜택

- 신속한 랜섬웨어 · 악성코드 유입 경로 파악
- 알려지지 않은 위협 탐지
- 내부 사용자 및 단말의 행위 기반 가시성 확대
- C2(Command & Control) 통신 차단으로 추가 피해 최소화
- 내부 보안 정책 및 운영 절차 개선을 위한 근거 데이터 확보
- 공격 전·중·후 전 단계에 걸친 가시성 확보로 대응 체계 고도화

솔루션

AhnLab EDR

개요

R사는 국내 최대 수준의 유통 및 서비스 네트워크를 기반으로 다양한 신용카드 상품과 서비스를 제공하는 대표 금융사다. 금융 산업 특성상 높은 수준의 보안은 필수이며, 고객 신뢰 유지를 위해 안정적인 보안 체계 구축이 무엇보다 중요하다.

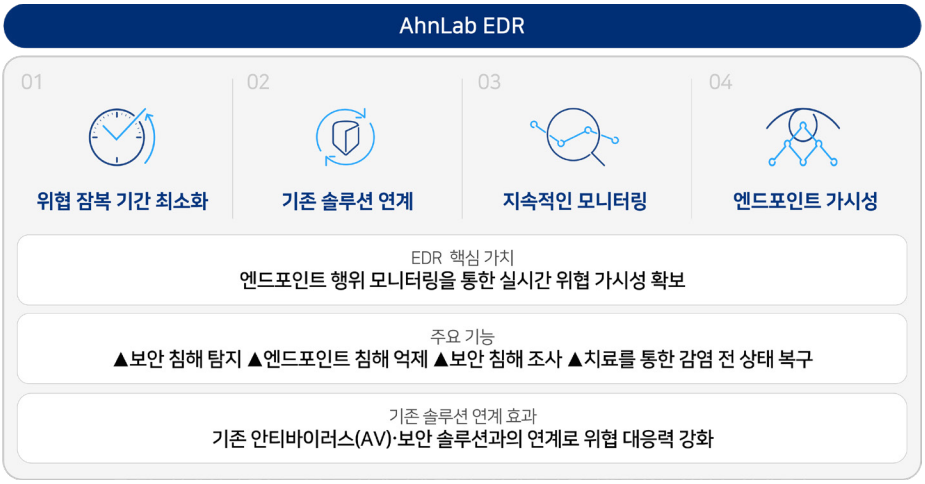
그러나 최근 R사는 반복적으로 발생한 랜섬웨어 공격으로 인해 심각한 업무 중단을 겪었다. 특히 공격 분석에 필요한 파일 확보가 어려워 감염 원인을 규명하는데 시간이 지연됐고, 이로 인해 대응과 복구 과정이 더욱 늦어지는 문제가 발생했다. 이런 배경에서 R사는 업무 효율성을 유지하면서도 보안을 한층 강화할 수 있는 새로운 솔루션의 필요성을 느꼈다.

R사는 기존에도 방화벽, 침입방지시스템(IPS), 악성코드 대응 솔루션 등 금융권 보안 기준에 맞춘 다계층 보안 체계를 운영하고 있었지만, 최근 공격자는 정상적인 행위를 위장하거나 정상 툴을 악용하는 방식으로 탐지를 우회하기 시작했다. 내부 단말에서 비정상적인 아웃바운드(Outbound) 통신을 시도하는 사례도 증가하면서, 단순히 악성 여부를 확인하는 수준을 넘어 이상 행위 자체를 식별하고 분석할 수 있는 가시성 확보가 필수 과제로 떠올랐다.

이러한 환경 변화를 직면한 R사는 엔드포인트에서 발생하는 다양한 행위를 기반으로 위협을 정밀하게 분석할 수 있는 솔루션이 필요함을 인식했다. 그 대안으로 R사는 AhnLab EDR을 도입했고, 이를 통해 엔드포인트 행위를 실시간으로 수집·분석하며 안랩의 위협 분석 역량과 결합해 알려지지 않은 위협까지 효과적으로 탐지하고 대응할 수 있는 기반을 확보하게 됐다.

도전 과제

- 반복되는 랜섬웨어 감염 원인과 유입 경로 분석에 한계
- 업무 효율성을 유지하며 알려지지 않은 위협을 탐지해야 하는 부담
- 기존 체계로는 행위 기반 분석 및 재발 방지 한계
- 내부 사용자 행위에 대한 가시성 부족으로 보안 정책 개선이 어려움



[그림 1] AhnLab EDR의 핵심 가치와 기능 요약

솔루션 도입 배경

1) 알려진 위협 중심 대응의 한계로 반복된 랜섬웨어 감염

R사는 시그니처 · 정책 기반 중심의 대응만으로는 최신 랜섬웨어를 차단하기 어려웠다. 실제 사용자 PC에서 감염이 반복되면서 업무 중단이 발생했고, 랜섬웨어의 유입 경로와 감염 원인을 분석할 수 있는 행위 기반 가시성 부족이 핵심 문제로 드러났다.

2) 업무 효율성을 해치지 않으면서 '알려지지 않은 위협'까지 탐지해야 하는 요구 증가

랜섬웨어 공격이 고도화되면서, R사는 단순 차단을 넘어 미탐 위협 탐지, 공격 경로 확인, 재발 방지 체계 확보가 필요했다.

이에 DRM, 문서 중앙화, 전통적 랜섬웨어 대응 솔루션 등 여러 제품을 검토했지만, 이들 솔루션은 ▲ 로그인 · 문서 절차 증가로 인한 업무 부담 ▲랜섬웨어 외 위협에 대한 낮은 가시성 ▲감염 원인 분석에 필요한 행위 정보 부족 ▲복구 · 회복 탄력성 제공 한계 등의 이유로 업무 효율성과 보안 요구를 동시에 충족하기 어려웠다.

3) 내부 사용자 행위 가시성 부족으로 인한 정책 개선 근거 부재

랜섬웨어 공격은 단순히 파일 다운로드 한 번으로 끝나는 것이 아니라, 그 이전 단계에서의 사용자 행위와 공격자의 준비 과정이 결합된 형태로 진행된다. 그러나 기존 체계만으로는 접속 및 다운로드 목적, 접속한 웹사이트, 스피어피싱 노출 여부 등의 기본 사용자 행위를 확인하기 어려웠다.

이로 인해 방화벽·IPS 정책을 객관적으로 개선할 근거가 충분치 않았고, 내부 단말 행위에 대한 가시성도 부족해 공격자가 내부 거점을 확보할 위험도 지속적으로 남아 있었다.

솔루션 구축 및 운영 현황

R사는 인터넷 접속이 가능한 단말과 내부 업무 시스템에 접속하는 단말을 분리해 네트워크 분리 환경을 운영하고 있다. 다만, 업무 특성상 외부에서 수집한 정보를 내부로 반입해야 하는 경우가 많고, 관련 서버를 포함한 핵심 업무 시스템을 외부와 완전히 분리하기는 어려운 구조적 제약이 존재한다.

솔루션 구축 및 운영 현황

- 인터넷망 모니터링
  - 악성코드 유입 경로, RDP 접근, 브라우저 접속, 자료 유출 감시
- 업무망 모니터링
  - 의심 행위 이벤트, 망 간 유입 · 유출 흐름, 서버 SSH · RDP 접속 확인

AhnLab EDR은 랜섬웨어를 비롯한 다양한 악성코드에 대한 행위 기반 탐지 기능을 제공하며, 감염 전 · 후 단말에서 발생하는 다양한 행위 정보를 수집해 사용자의 행위까지 종합적으로 분석한다. 이를 통해 단순 악성코드 유입과 실행 뿐만 아니라 공격자의 거점 마련을 위한 초기 침투 시도, 보안 솔루션 탐지 회피 행위 등 공격 전 단계에 걸친 전체 행위 흐름을 가시화할 수 있다.

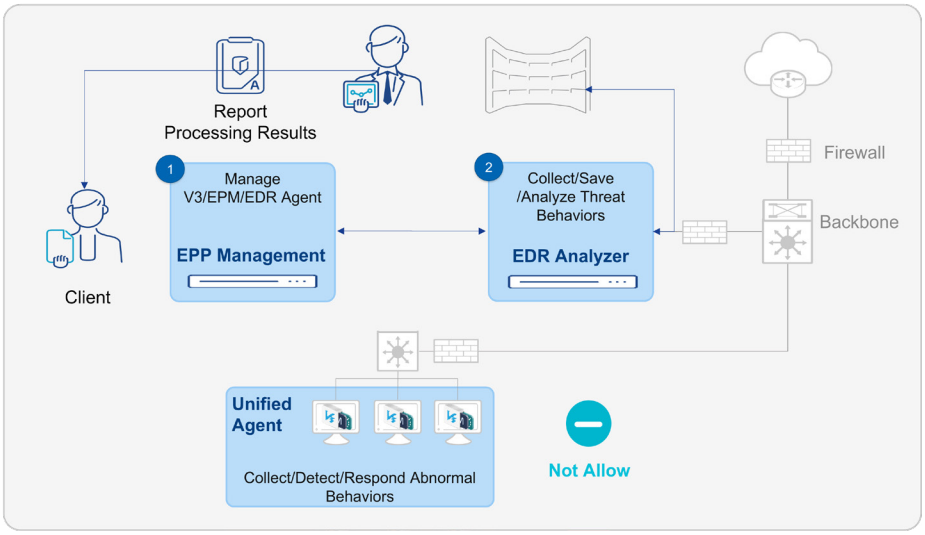
R사는 인터넷망 단말과 내부 업무망 단말 모두에 AhnLab EDR을 적용하고, 각 구간에서 아래와 같은 포인트를 중심으로 행위 기반 분석을 수행하고 있다.

1) 인터넷망

- 악성코드 진단 발생 시 AhnLab V3와 연동 및 유입 경로 추적
- 인터넷망 단말을 대상으로 한 RDP 비정상 접근 시도 모니터링
- 사용자 브라우저 접속 행위 분석
- 내부 업무 자료의 외부 유출 여부 확인

2) 업무망

- AhnLab EDR을 통한 의심 행위 전수 모니터링
- 업무망과 인터넷망 간 유입 · 유출 이벤트 분석
- 내부 단말에서 서버로 향하는 SSH 및 RDP 접속 행위 확인



[그림 2] R사의 AhnLab EDR 도입 현황

도입 효과

1) 손쉬운 악성코드 유입 경로 파악 및 복구

과거에는 랜섬웨어를 비롯한 악성코드 감염 시 유입 경로를 확인하기 어려워, 단말 포맷과 대체 PC를 투입하는 방식이 사실상 유일한 대응이었다. 여러 차례 포맷과 재설치를 반복하면서 유입 경로를 추적하려 했지만, 장애 시간만 길어질 뿐 재발 방지에 활용할 만한 분석 데이터를 확보하기도 어려운 구조였다.

AhnLab EDR을 도입한 후에는 AhnLab V3가 직접 진단하지 못한 경우라도 대량의 파일 확장자 변경과 같은 의심 행위 이벤트와 해당 시점의 사용자 행위를 함께 확인해 유입 경로를 상당 부분까지 추정할 수 있게 됐다.

도입 효과

- 악성코드 유입 경로 추적 및 복구 시간 대폭 단축
- 내부 사용자 행위에 대한 가시성 확보 및 정책 개선 근거 강화
- C2 통신 차단을 통한 추가 피해 예방 및 확산 억제
- 기존 체계로 탐지하기 어려웠던 알려지지 않은 위협 식별과 행위 기반 탐지 강화
- 스냅샷 기반 원격 복구로 업무 연속성 향상 및 단말 다운타임 최소화

또한, 단말에서 발생한 C2 접속 정보를 기반으로 방화벽에서 외부 통신을 즉시 차단하는 등 추가 대응이 가능해졌다.

아울러, AhnLab EDR의 스냅샷 복구 기능을 통해 랜섬웨어 감염 이전 시점으로 원격 복구를 수행함으로써 단말 정상화 시간을 크게 단축하고 업무 연속성을 신속하게 회복할 수 있었다.

2) 내부 사용자 행위에 대한 가시성 확대

AhnLab EDR은 악성코드 탐지를 넘어 내부 사용자 행위 전반에 대한 가시성을 제공한다. 이를 통해 비인가 사용자의 내부 서버 대상 SSH·RDP 접속 시도는 물론, 기존에 포착하지 못했던 내부 시스템 및 솔루션의 비정상 행위 패턴도 확인할 수 있게 됐다.

특히 이러한 비인가 접속이나 비정상 실행·등록은 공격자가 백도어를 심거나 윈도우 작업 스케줄러·레지스트리에 악성 스크립트를 등록할 때 나타나는 전형적인 징후와 일치한다. 동일한 유형의 행위가 실제 공격으로 이어질 경우 AhnLab EDR이 이를 탐지·경고해 조기 차단을 지원한다.

이를 바탕으로 R사는 설정 미비를 보완하고 접근 정책과 업무 절차를 재정비하는 등 내부 보안 정책과 운영 프로세스를 개선할 근거를 확보했다. 이처럼 R사는 AhnLab EDR을 통해 단말은 물론 내부 사용자 행위까지 아우르는 가시성과 분석 역량을 확보했다.

[그림 3] 악성 레지스트리 등록을 통한 공격 지속성 시도와 AhnLab EDR 대응

맺음말

이처럼 R사는 알려진 위협에 꾸준히 대응해왔지만, 반복적인 랜섬웨어 감염과 고도화된 공격 방식으로 인해 기존 대응 체계만으로는 한계에 직면해 있었다. 이에 AhnLab EDR을 도입해 단말 단의 행위 기반 정보를 폭넓게 확보함으로써, 그동안 파악하기 어려웠던 악성코드 유입 경로와 공격 전·후 단계의 이상 행위를 실질적으로 식별할 수 있는 기반을 마련했다. 이를 통해 반복 감염의 원인을 명확히 추적하고 장애 시간을 최소화하는 한편, 재발 방지를 위한 근본 원인 분석 체계를 강화할 수 있었다.

또한, AhnLab EDR은 내부 사용자 행위까지 포함한 가시성을 제공해, 기존 보안 체계만으로는 통제하기 어려웠던 비인가 접속, 비정상 통신, 내부 시스템의 이상 행위 등 다양한 리스크 요소를 조기에 식별하고 대응할 수 있도록 지원했다. 이를 통해 R사는 단순한 악성코드 차단을 넘어 조직의 업무 연속성을 강화하고, 내부 운영 프로세스와 보안 정책을 전반적으로 개선할 수 있는 실질적인 보안 체계를 구축하게 됐다.

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901