AhnLab

Case Study

AhnLab EDR · MDR로 달성한 반도체 기업 보안 혁신

S사는 전력관리반도체(PMIC) 솔루션 전문 업체로, 최고의 전력반도체 전문가들로 구성된 조직이다. 아시아 최고 수준의 아날로그 및 전력반도체 제품 라인업을 갖추고 있으며, 국내외 주요 스마트폰, TV, 노트북, PC 제조업체에 대량으로 공급하고 있다.

Introduction 개요

국내 PMIC(Power Management Integrated Circuit) 업체인 S사는 2023년 9월 AhnLab EDR을 처음 도입했다. 기존에 사용하던 안랩의 V3(V3 Internet Security, V3 Net for Windows) 제품을 통해 보안을 유지해 왔으나, 침해사고에 대한 효과적인 방어와 보안 강화를 위해 새로운 방안을 검토한 끝에 AhnLab EDR(Endpoint Detection and Response)을 채택하기로 결정했다. AhnLab EDR은 매니지드 탐지 및 대응 서비스 MDR(Managed Detection and Response)과 함께 제공되어 실시간 위협 탐지와 모니터링은 물론, 탐지된 이벤트 로그를 안랩 원격 관제 플랫폼으로 전달한다. 이를 통해 안랩의 보안 전문가들이 위협 행위를 분석하고 대응하여 포괄적인 보안 시스템을 구축했다. 또한, S사가 추가적인 위협에 대비할 수 있도록 정기적으로 위협 분석 및 월간 통계 보고서도 발송하고 있다.

S사는 AhnLab EDR을 도입함으로써 보안 인프라를 더욱 견고하게 구축하고, 운영 효율성과 안정성을 크게 향상시키고 있다. AhnLab EDR 외에도 안랩의 패치 관리 솔루션인 AhnLab EPM(EPP Patch Management)과 V3, EDR, EPM을 통합적으로 관리할 수 있는 AhnLab EPP Management도 함께 운영하고 있다.

Benefit 도입 효과

- 클라이언트 PC 행위 실시간 모니터링 시스템 구축
- 해커 침입 징후 사전 탐지 및 선제적 대응
- 정기적인 위협 보고서를 통한 보안 가시성 확보

- 단일 에이전트를 통한 통합 관리로 운영 효율성 향상
- 복잡한 설정 없이 직관적이고 간편한 보안 관리로 사용자 편의성 향상

- 랜섬웨어로 인한 침해 사고 발생 시 데이터 자동 복구로 데이터 손실 최소화, 시스템 정상화 실현
- 위협 발생 시 자동 대응 및 시스템 복구를 통한 서비스 연속성 유지

AhnLab EDR이 조직에 미치는 영향

정량적 효과

- 보안 사고 탐지율 향상
- 보안 위협 대응 시간 단축
- 보안 운영 비용 절감

정성적 효과

- 위협 대응 체계 간소화
- 조직 내 보안 상태에 대한 투명성 제공
- 신속한 의사결정 지원
- 비즈니스 생산성 향상

> AhnLab EDR과 MDR 도입 이후, 위협 탐지와 대응, 운영 관리 부문에서 상당한 효과를 보고 있습니다. 실시간 위협 탐지와 자동 대응 시스템을 통해 이상 징후 탐지율이 향상되어 잠재적 침해사고를 보다 효율적으로 예측하고 방지할 수 있게 되었습니다. 또한, 자동화된 대응과 안랩 보안 전문가의 원격 지원 덕분에 보안 담당자의 업무 부담이 크게 줄었습니다. 특히, AhnLab EDR은 저희가 가장 필요했던 PC 행위 분석 기능이 뛰어나, 비즈니스 환경에 매우 적합한 솔루션으로 평가합니다.
>
> – S사 IT팀 보안 기술 담당자

Customer Story 고객의 이야기

AhnLab EDR과 MDR이 현재 귀사의 비즈니스 환경에서 어떤 영향을 미치고 있나요?

AhnLab EDR과 MDR을 도입한 이후, 보안 측면에서 실질적인 개선을 경험하고 있다. 실시간 위협 탐지와 자동화된 대응 체계 덕분에 보안 사고에 대한 대응 속도와 보안 관리 효율성이 크게 향상됐다. 또한, EDR과 함께 제공되는 MDR 서비스를 통해, 보안 위협 탐지와 모니터링 외에도 발견된 위협 이벤트에 대한 분석 결과와 해결책을 함께 제공받을 수 있다는 점이 편리하다. AhnLab EDR은 단순한 경고를 넘어, 구체적인 대응 방안을 제시해주기 때문에 보안 담당자의 업무 부담을 많이 덜어주며, 이상 징후 발생 시 빠르게 원인을 파악하고, 대응 방법을 명확하게 알 수 있어 능동적인 방어가 가능하다.

정량적 효과: 시스템 이상 징후 및 보안 사고 탐지율이 현저히 높아졌으며, 기존에는 발견되지 않았던 잠재적인 위협들을 사전에 차단할 수 있게 됐다. 여기에 더해, 보안 위협 대응에 소요되는 시간을 단축하고, 보안 운영 비용도 크게 절감했다.

정성적 효과: 자동화된 탐지와 대응으로 위협 방어 프로세스가 간소화됨에 따라, 업무 효율성과 비즈니스 생산성이 증대됐으며, 보안 담당자의 스트레스도 줄었다. 또한, MDR 분석 보고서는 경영진에게 보안 상태에 대한 투명한 정보를 제공하여 보안 이슈에 대한 신속한 의사결정에 많은 도움이 됐다. 그 결과, 보안 사고에 대한 대응 속도뿐만 아니라, 전반적인 비즈니스 생산성도 높아졌다.

여러 업체 중에서도 안랩의 EDR을 선정한 이유는 무엇인가요?

침해사고를 효과적으로 방어하고, 보안을 강화하는 방안에 대해 검토하던 중 EDR을 도입하기로 결정했다. 약 한 달간 PoC를 진행하고, 국내 보안업체 B사와 안랩을 비교하던 끝에, 안랩을 최종 선택했다. 안랩은 빠른 응대와 고객 니즈를 파악하려는 적극적인 태도를 보여 신뢰를 주었다. 무엇보다 AhnLab EDR은 기존에 사용 중이었던 V3 제품군과 연계 제품이기에 UI(User Interface)가 다른 제품들보다 사용자 친화적이고 편리하다는 점이 가장 마음에 들었다. 이 외에도, 안랩의 제품은 다른 보안 솔루션과 호환성이 우수하다. 따라서 기존에 내부에서 사용 중이던 자체 솔루션과도 쉽게 연동이 가능하여 관리 효율성이 뛰어나다는 점이 차별화 요소가 됐다. 향후에도 안랩과 지속적인 협력을 통해 성과를 달성할 것으로 기대하고 있다.

고객이 추천하는 AhnLab EDR의 주요 강점

- 실시간 위협 탐지 및 자동 대응, 모니터링
- 단일 에이전트를 통한 간편한 관리와 높은 호환성
- 정기적인 위협 분석 보고서 제공
- 랜섬웨어 복구 및 데이터 보호
- 전문적인 기술 지원

AhnLab EDR이 B사 제품 대비 어떤 점이 더 적합하다고 판단하셨나요?

B사는 글로벌 벤더인 T사의 제품을 제안했다. 이 제품은 기능이 광범위하고 맞춤형 설정 옵션도 다양했다. 그러나, UI가 복잡하고 직관적이지 않아 모든 기능을 완전히 이해하고 특정 요구사항에 알맞게 활용하는 데 다소 어려움이 있었다. 또한, 다양한 기능을 제공함에도 불구하고 실질적인 사용 측면에서 우리 비즈니스 환경과는 맞지 않은 부분이 있었으며, 담당자의 대응 측면에서도 아쉬움이 있었다. 반면, AhnLab EDR은 사용자 친화적인 UI와 요구 사항에 최적화된 기능을 제공하여 우리에게 더욱 적합한 선택이었다.

귀사가 IT 및 보안 제품을 선택할 때 가장 중요시하는 원칙이나 기준이 있다면 무엇인가요?

우선, 국내에서 검증된 다양한 레퍼런스를 보유한 제품을 선호한다. 이와 함께, 시스템 충돌 및 관리상 어려움을 최소화하기 위해 조직의 특성과 운영 환경에 잘 맞는지 검토하고, 기존 솔루션과의 호환성도 신중하게 고려한다.

이런 기준을 종합적으로 고려하면, 안랩의 보안 솔루션은 국내에서 쌓은 인지도와 고객 신뢰도를 바탕으로 우리 조직의 IT 환경에 적합한 뛰어난 보안 기능과 기술 지원, 운영 안정성을 제공할 수 있는 파트너라고 생각한다.

AhnLab EDR을 사용하면서 경험한 특장점 3가지를 꼽자면 무엇인가요?AhnLab EDR을 사용하면서 경험한 특장점 3가지를 꼽자면 무엇인가요?

AhnLab EDR은 솔루션이 무겁지 않고, 엔드포인트 보안 플랫폼 EPP(Endpoint Protection Platform)에서 에이전트 하나로 모든 관리가 가능하다. 별도의 추가적인 관리 툴이나 복잡한 설정 없이도 효율적으로 보안을 관리할 수 있고, 조직의 IT 인프라에 미치는 영향을 최소화할 수 있기 때문이다. 이뿐만 아니라, 하나의 에이전트를 통한 통합 관리로 운영 효율성을 높이고, 관리 비용을 절감할 수 있는 효과도 있다.

AhnLab EDR을 활용하여 어디서 어떤 행위가 발생했는지 실시간으로 모니터링하고, 악성 행위를 사전에 차단할 수 있다. 예를 들어, 파워셸(PowerShell)을 실행하면 입력된 커맨드라인이 정상적인 파워셸 명령인지, 아니면 비정상적인 파워셸 명령인지 구별할 수 있다.

AhnLab EDR은 자동 롤백 기능을 제공하여 랜섬웨어와 같은 사이버 공격이 발생했을 때 중요한 파일이나 시스템이 암호화되거나 손상됐을 경우 데이터를 이전 상태로 신속하게 복구한다. 따라서 시스템 사용자는 데이터 복구 과정에 소요되는 시간을 줄이고, 데이터 손실을 최소화할 수 있다. 결과적으로, 조직에 막대한 피해를 입힐 수 있는 랜섬웨어 공격에 대한 심리적 불안감을 해소하고, 보안 사고가 발생하더라도 빠르게 정상화할 수 있다는 자신감이 생겼다.

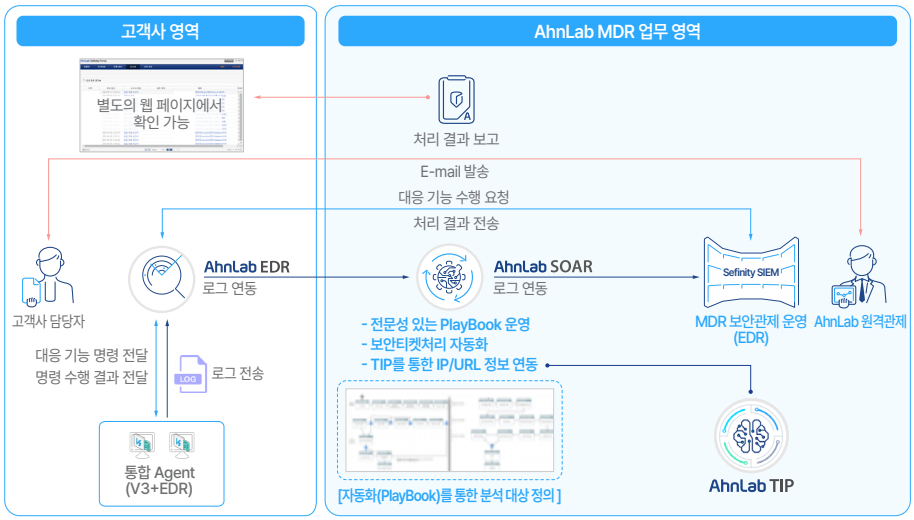
AhnLab EDR과 MDR의 시너지

- 즉각적인 위협 인식 및 전문가의 원격 대응
- 위협 상세 분석 및 맞춤형 대응 전략 지원
- 보안 운영 및 관리 효율성 증대

AhnLab EDR 도입 후 서비스와 기술 지원에 대한 만족도는 어느 정도 인가요?

안랩의 기술 지원에 대한 전반적인 만족도는 매우 높다. 가장 긍정적인 점은 지원 티켓에 대한 빠른 응답이다. 분석 대상의 난이도에 따라 다르지만, 일반적으로 티켓을 제출한 지 하루 만에 문제 해결을 위한 답변을 받을 수 있어 긴급한 상황에서도 신속한 대응이 가능하다.

매달 제공되는 MDR 분석 보고서도 유용하게 활용하고 있다. 이 보고서에는 조직 환경을 위한 맞춤형 보안 분석과 위협 탐지 정보가 포함돼 있어 보안 상태를 정확히 진단하고 이후의 대응 방안을 결정하는 데 큰 도움이 된다. 보고서의 내용에 대해서는 별다른 개선점을 찾지 못했으며, 현재 수준에 충분히 만족한다.



[그림 1] MDR 시스템 구성

Conclusion 결론

결론적으로, AhnLab EDR과 MDR은 조직의 보안 수준을 강화하는 데 중요한 역할을 한다. 실시간 위협 탐지와 모니터링, 자동 대응 및 복구 시스템으로 보안 담당자가 짧은 시간 안에 문제를 해결하고, 능동적으로 위협에 대응할 수 있는 환경을 제공한다.

특히, AhnLab EDR과 MDR의 결합은 단순한 위협 탐지를 넘어, 발생한 보안 사고에 대해 상세한 분석과 구체적인 해결책을 함께 제시하여 보안 관리의 질을 높이는 데 기여한다. 더 나아가, 보안 위협에 대한 분석 결과와 대응 방안을 경영진에게 제공하여 신속한 의사결정을 지원하고, 비즈니스 생산성 향상에도 큰 영향을 미친다.

AhnLab EDR은 기존 솔루션과의 뛰어난 호환성, 직관적이고 사용자 친화적인 인터페이스, 간편한 관리 방식으로 보안 운영의 효율성을 극대화한다. 이와 더불어, 빠르고 전문적인 기술 지원은 고객으로부터 높은 평가를 받고 있으며, 정기적인 MDR 보고서는 보안 상태를 정확히 파악하고, 효과적인 대응 전략을 세우는 데 중요한 기준이 된다.

이처럼 AhnLab EDR은 조직의 보안 강화뿐만 아니라 운영 및 관리 편의성 측면에서도 우수한 성과를 보여준다. 향후 다양한 업계와의 지속적인 협력을 통해 고객의 보안 역량 향상에 기여하는 든든한 파트너로서 자리매김할 것이다.

AhnLab

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