AhnLab

White Paper

최적의 랜섬웨어 대응을 위한 통합 보안 전략

최근 발생하는 랜섬웨어 감염 사건들을 보면 사이버 공격이 새로운 단계에 진입했음을 알 수 있다. 과거 단순한 파일 암호화나 금전 요구에 그쳤던 랜섬웨어 공격이 이제는 데이터 유출, 서비스 중단, 평판 훼손을 동반하는 복합 공격으로 진화했다. 그 파급력 또한 더 이상 단일 기업에 국한되지 않으며, 공격자는 '감염 후 공포를 심는 존재'에서 '침투 후 잠복하는 존재'로 변했다.

이처럼 고도화된 랜섬웨어 공격들도 겉으로는 예측 불가능한 것처럼 보이지만, 사실 그 안에는 분명한 흐름이 존재한다. 따라서, 사고는 예측할 수 없어도 대응은 예측 가능하게 만들 수 있다. 이 철학이 바로 안랩의 '랜섬웨어 통합 보안 전략'의 출발점이다.

랜섬웨어 보안을 위한 도전과제

진화를 거듭하는 랜섬웨어 공격은 기업들에게 새로운 도전과제들을 안긴다. 도전과제는 여러가지가 있지만 크게 다음 세 가지로 요약할 수 있다.

#1. 신/변종 랜섬웨어 대응: 랜섬웨어는 신종과 변종이 끊임없이 등장해 방어자들을 어렵게 한다. 이러한 랜섬웨어에 효과적으로 대응하기 위해서는 단일 솔루션으로 차단하는 것을 넘어, 랜섬웨어가 유발하는 악성 행위를 분석하고 솔루션 간 연계 및 연동을 지원하는 플랫폼 기반 전략이 필요하다.

#2. 다양한 구간 보호: 최신 랜섬웨어 공격은 엔드포인트, 네트워크, 이메일 등 다양한 구간에서 발생한다. 숙련된 공격자들은 목적을 달성하고 피해를 극대화 시키기 위해 여러 구간을 넘나들며 공격을 수행하기도 한다. 기업이 하나의 영역만 보호하면, 해당 영역의 보안 솔루션을 우회하거나 다른 구간으로 들어오는 공격에 피해를 입게 된다.

#3. 재발 방지 체계 수립: 랜섬웨어 공격은 한 번 차단하는 것으로 끝나지 않는다. 유사한 공격이 언제든 다시 감행될 수 있고, 특히 잠복 기술이 발달한 최근 공격들을 보면 이러한 경향이 두드러지게 나타난다. 랜섬웨어로 인한 연쇄적인 피해를 예방하기 위해서는 탐지 및 차단을 넘어 위협을 추적해 예방할 수 있는 보안 체계를 갖춰야 한다.

보안은 제품이 아닌 '프로세스'로 완성된다

새로운 랜섬웨어 보안 도전과제를 해결하기 위해 일반적으로 기업들이 내놓는 해답은 보안 솔루션의 '숫자'를 늘리는 것이다. 이러한 트렌드는 한국 뿐만 아니라 전 세계적으로 나타나고 있다.

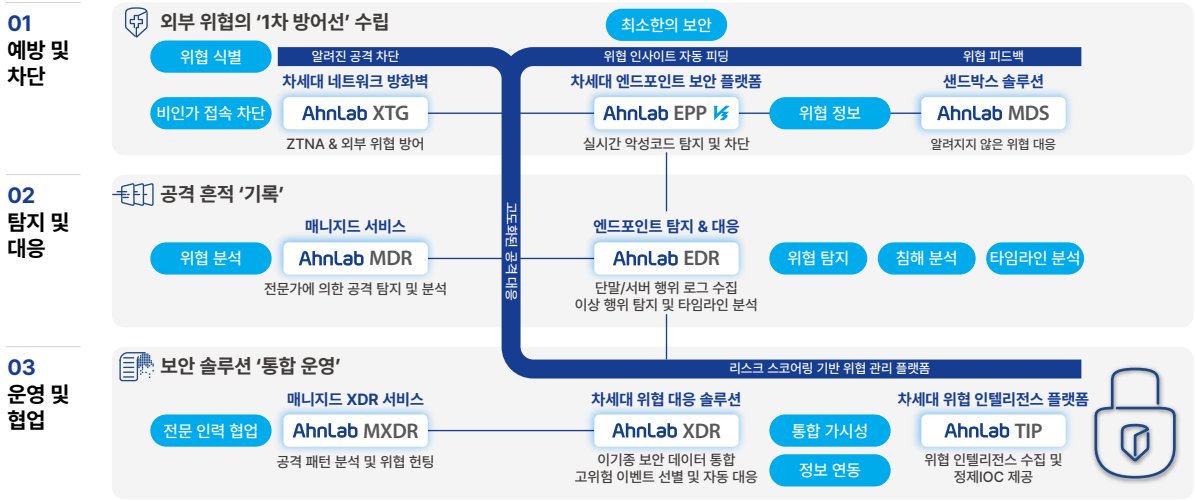
시장조사기관 가트너(Gartner)가 2024년 전 세계 대기업 162개를 대상으로 한 조사 결과, 응답자들은 평균 45개의 사이버 보안 솔루션을 운영하고 있다고 답했다. 그 전년도인 2023년에는 평균 43개로 크게 다르지 않았고, 응답자 중 절반이 "솔루션을 제대로 활용하지 못하고 있다"고 했다.

보안 솔루션 수는 기업 규모, 산업, 국가 별로 차이가 있지만 운영 상의 어려움을 호소하는 것은 전반적으로 동일하다. 그리고, 안랩이 실제로 침해를 당한 기업들의 사례를 분석해보면 보안 솔루션의 '부재'보다 '활용 미흡'으로 인해 피해를 입은 경우가 훨씬 많다.

사이버 보안 전문가 브루스 슈나이어(Bruce Schneier)는 "보안은 제품이 아니라 프로세스다."라는 명언을 남겼다. 보안 솔루션을 도입해 기능을 단편적으로 사용하는 정적 상태를 넘어, 보안 솔루션들이 유기적으로 동작하면서 사람과 시너지를 낼 수 있도록 하는 동적 노력을 기울여야 한다는 의미다.

최적의 랜섬웨어 대응을 위한 통합 보안 전략

안랩은 랜섬웨어 공격의 고도화, 현장에서 기업들이 마주하는 도전과제, 프로세스 관점 통합 보안의 중요성을 고려하여 랜섬웨어 보안에 최적화된 플랫폼 기반 오퍼링을 제공하고 있다. 안랩의 랜섬웨어 보안 오퍼링을 구성하는 솔루션들은 각자의 역할을 수행하지만, 상호 간 유연하게 연동되어 프로세스 관점에서 '탐지-분석-대응'이 유기적으로 순환하는 하나의 보안 생태계로 작동한다. 이를 통해, 고객으로 하여금 침해 전(Prevention) – 중(Detection) – 후(Response)를 잇는 순환 구조를 만들어갈 수 있도록 한다.



[그림 1] 안랩의 플랫폼 기반 랜섬웨어 보안 오퍼링

이를 위해, 안랩은 '차세대 방화벽(ZTNA) – 안티바이러스(EPP) – 샌드박스 – EDR – MDR – XDR – MXDR – 위협 인텔리전스(TI)'로 이어지는 연동 체계를 구축했다. 차세대 방화벽이 사용자와 기기 검증을 통해 접근 단계에서 신뢰를 보장하고, EPP와 샌드박스가 악성 행위 탐지 및 사전 차단, EDR과 MDR이 엔드포인트 행위 추적과 전문 분석, XDR과 MXDR이 조직 전반의 통합 가시성과 자동 대응을 담당한다. 여기에 최신 위협 인텔리전스가 더해져 보안 체계를 완성한다.

단계	솔루션	역할
1. 예방 및 차단	AhnLab XTG	사용자/기기 검증을 통한 접근 제어 (ZTNA)
	AhnLab EPP (V3)	알려진 악성코드 탐지 & 차단
	AhnLab MDS	샌드박스 기반 분석 – 알려지지 않은 악성코드 탐지 & 차단
2. 탐지 및 대응	AhnLab EDR	엔드포인트 이벤트 수집, 분석 및 대응
	MDR 서비스	전문가 주도 엔드포인트 위협 탐지, 분석 및 대응
3. 운영 및 협업	AhnLab XDR	리스크 스코어링 기반 통합 위협 관리
	MXDR 서비스	여러 보안 구간에 대한 전문가의 통합 공격 패턴 분석 및 위협 헌팅
	AhnLab TIP	침해지표(IOC) 포함 위협 인텔리전스 제공

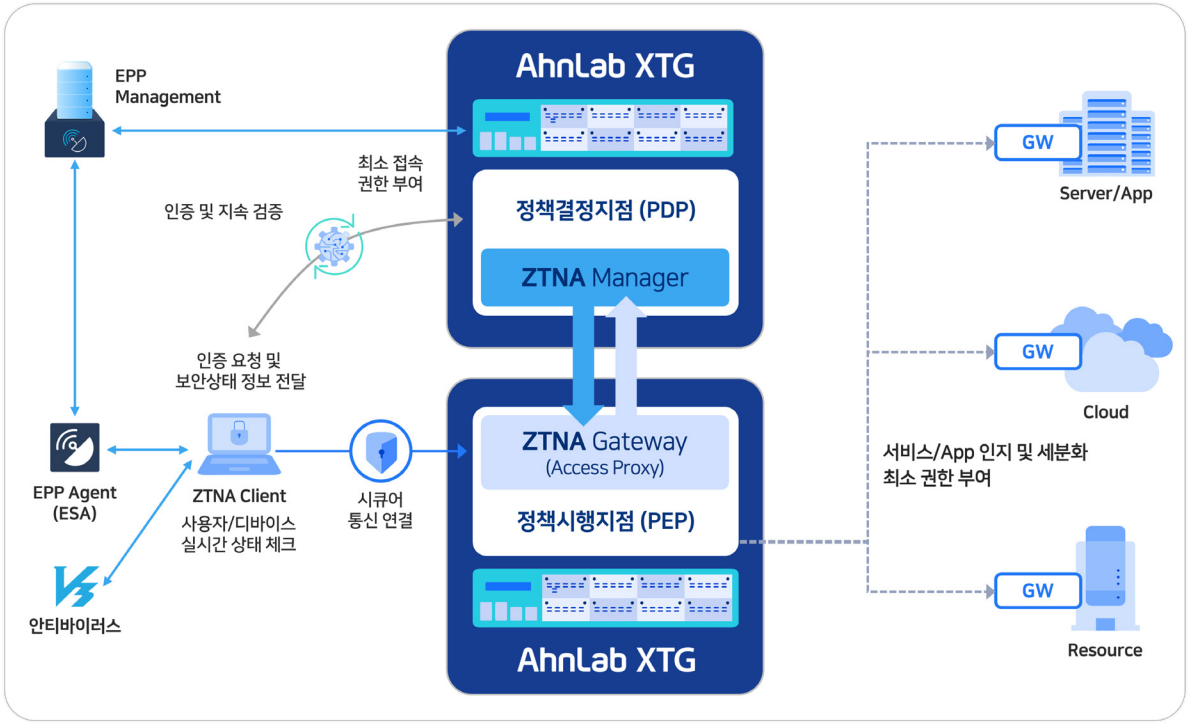
[표 1] 솔루션 별 역할

보안 솔루션들이 수행하는 역할에 관한 자세한 내용은 다음과 같다.

1단계: 예방과 차단 - "위협이 오기 전에 막는다"

① AhnLab XTG – ZTNA 기반 신뢰 검증 및 접근 제어

차세대 방화벽 AhnLab XTG는 ZTNA(Zero Trust Network Access)를 실제 네트워크 운영 환경에 구현한 솔루션이다. AhnLab EPP, AhnLab V3 등 엔드포인트 보안 솔루션들과 연계하여 사용자와 기기의 신원을 지속적으로 검증해 "누구도 기본적으로 신뢰하지 않는다"는 제로 트러스트 보안 모델을 실현한다.



[그림 2] AhnLab XTG - ZTNA 기반 네트워크 접근 제어 구조

AhnLab XTG는 비인가 사용자, 보안 상태가 온전치 않은 기기, 권한을 초과한 내부 접근을 실시간으로 제어한다. 네트워크 구간에서 내부 침입의 첫 관문을 원천 봉쇄하고, 네트워크-엔드포인트로 이어지는 통합 접근 제어 체계를 완성한다.

요약하면, AhnLab XTG는 '인증 – 권한 – 행위'를 축으로 하는 제로 트러스트 보안 플랫폼으로 조직의 내·외부 경계를 가리지 않는 최신 위협 방어를 위해 '신뢰 검증의 중심 축' 역할을 수행한다.

② AhnLab V3 – 통합 보안 체계의 '엔드포인트 1차 방어선'

AhnLab V3는 30년 넘게 기업과 기관에서 오랜 기간 신뢰받아 온 안티바이러스(AV) 솔루션이다. 기본적으로 탁월한 성능과 기술력을 갖춘 제품이지만 단순 '설치 여부'를 넘어 실시간 보호 활성화, 검사 주기 관리, 예외 정책 점검 등 사용자의 운영 여부에 따라 방어력이 달라진다. 같은 V3를 사용하더라도 얼마나 세밀하게 설정하고 운영하느냐가 보안 효과를 좌우한다.

AhnLab V3는 다음과 같은 핵심 기능을 중심으로 랜섬웨어 등 악성 행위를 탐지하고 차단한다.

A. 시그니처 기반 탐지

AhnLab V3의 기본 탐지 체계는 시그니처 기반의 실시간 감시(Real-time Scan)와 정밀 검사(Smart Scan)로 구성된다. 알려진 악성코드는 즉시 차단하고, 의심스러운 객체는 추가 검사를 거쳐 안전 여부를 판단한다. 시그니처 데이터베이스는 상시 업데이트되며, 최신 위협에도 빠르게 대응한다.

B. 랜섬웨어 보안 폴더

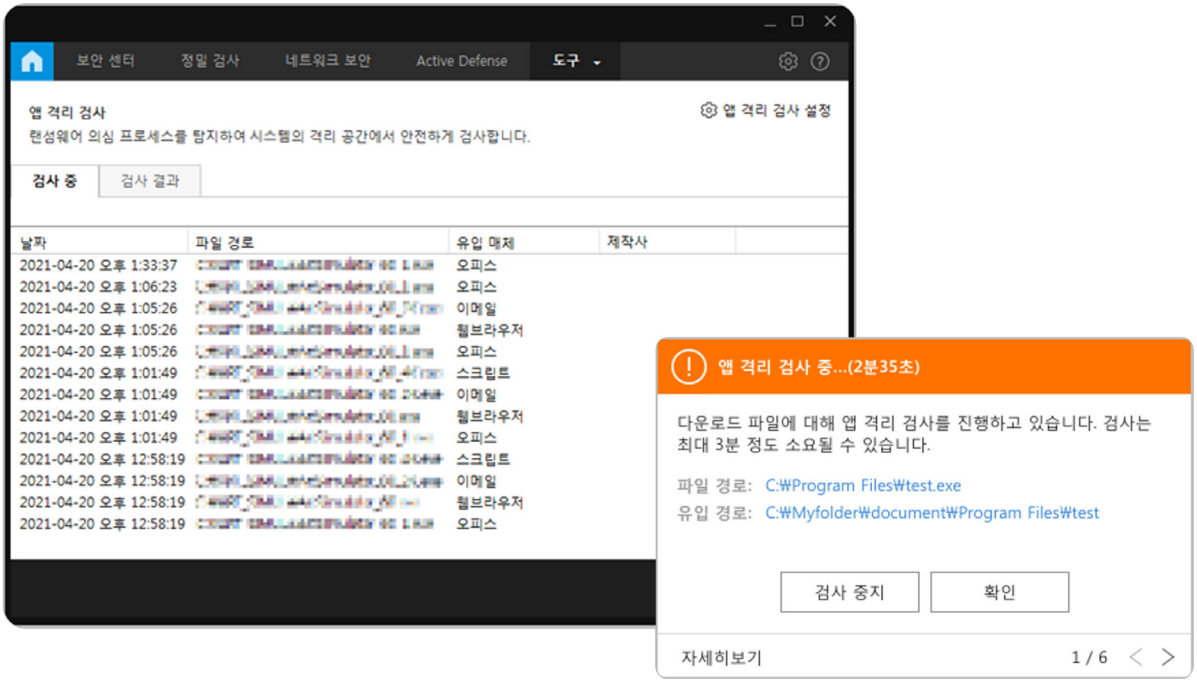
V3 사용자는 랜섬웨어 등 사이버 공격으로부터 꼭 지켜야 하는 폴더를 '랜섬웨어 보안 폴더'로 설정할 수 있다. 랜섬웨어 보안 폴더로 지정된 폴더는 '허용된 프로세스'만 접근할 수 있다. 예를 들어, 파워포인트나 엑셀 같은 정상 앱만 접근하도록 지정하면, 랜섬웨어는 해당 폴더에 영향을 미칠 수 없다.

안랩이 고객들의 보안 운영과 랜섬웨어 침해 사례를 보면, V3를 도입했지만 랜섬웨어 보안 폴더 기능은 사용하지 않는 경우가 많다. 랜섬웨어 보안 폴더는 혹시 시스템이 랜섬웨어에 감염되더라도 중요/민감 자료를 지킬 수 있는 중요한 기능임을 강조한다.

[그림 3] AhnLab V3 – 랜섬웨어 보안 폴더 설정

C. 앱 격리 검사

AhnLab V3는 PC 내 별도 가상 환경에서 랜섬웨어로 의심되는 파일을 실행하고 행위 기반 모니터링 기술을 바탕으로 검사하는 '앱 격리 검사' 기능을 제공한다. 이 기능을 활용하면 랜섬웨어가 시스템에 유입되더라도 행위 발현 전 검사를 수행해 피해 확산을 방지할 수 있다.



[그림 4] AhnLab V3 – 앱 격리 검사

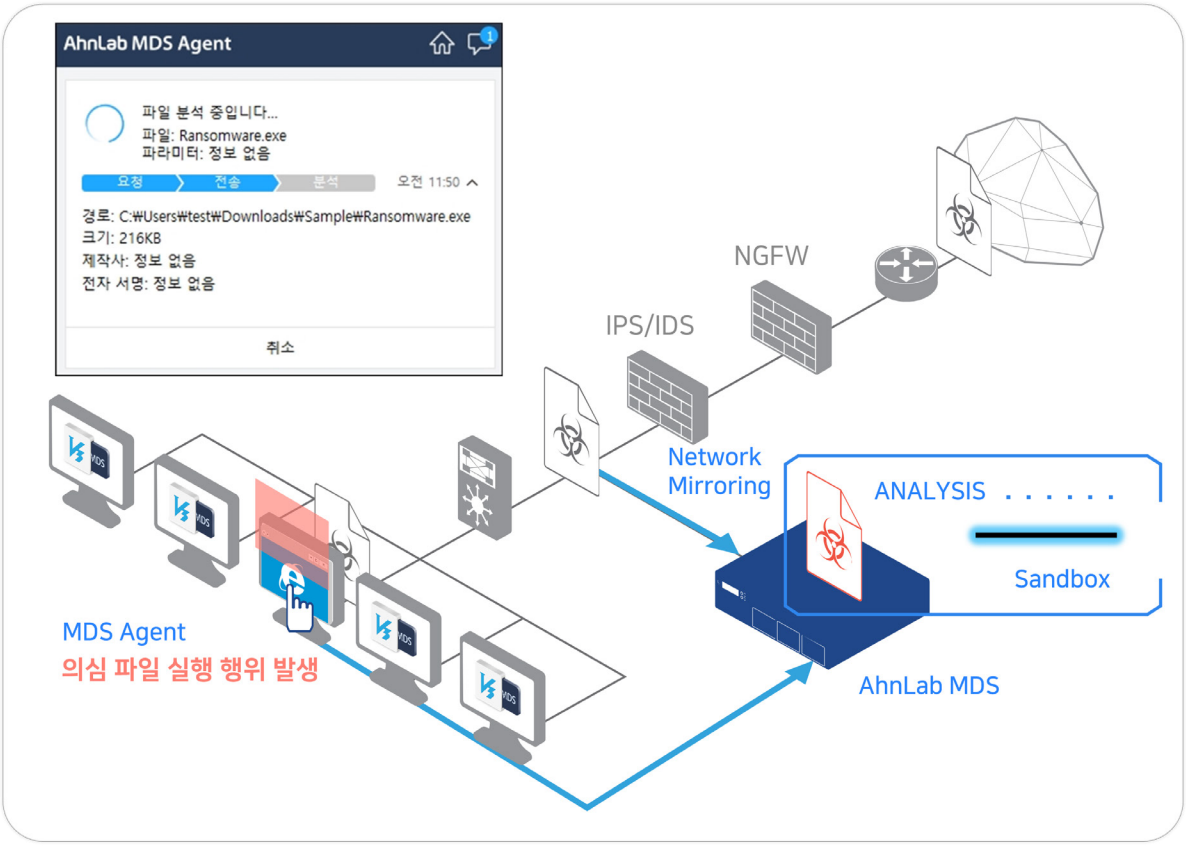
추가적으로, V3를 엔드포인트 보안 플랫폼 AhnLab EPP와 함께 사용하면 탐지 현황, 정책, 이벤트를 통합 관리해 보다 신속한 대응이 가능하다. EPP는 단일 PC나 서버를 넘어 조직 내 모든 엔드포인트 보안 상태를 통합 모니터링하고 정책을 일괄 적용할 수 있다. 이를 통해, 보안 담당자는 개별 단말의 탐지 이벤트를 하나의 흐름으로 파악해, 정책 관리, 패치 상태 점검, 디바이스 제어 등 다양한 보안 기능 간 연계 대응을 수행할 수 있다.

특히, 최근에는 리눅스 서버 환경에서의 취약점과 악성코드가 증가하면서, EPP를 통한 운영체제 간 통합 보안 관리의 중요성이 커지고 있다. AhnLab V3와 AhnLab EPP를 함께 운영하면, 엔드포인트 탐지/차단 역량과 중앙 관리의 효율성을 모두 확보할 수 있다.

③ AhnLab MDS – 샌드박스 분석으로 '랜섬웨어 실행 전 차단'

AhnLab MDS는 네트워크-엔드포인트-이메일 구간에 걸쳐 알려지지 않은 악성코드까지 방어하고, 탐지 후 대응 공백을 최소화하는 샌드박스 솔루션이다.

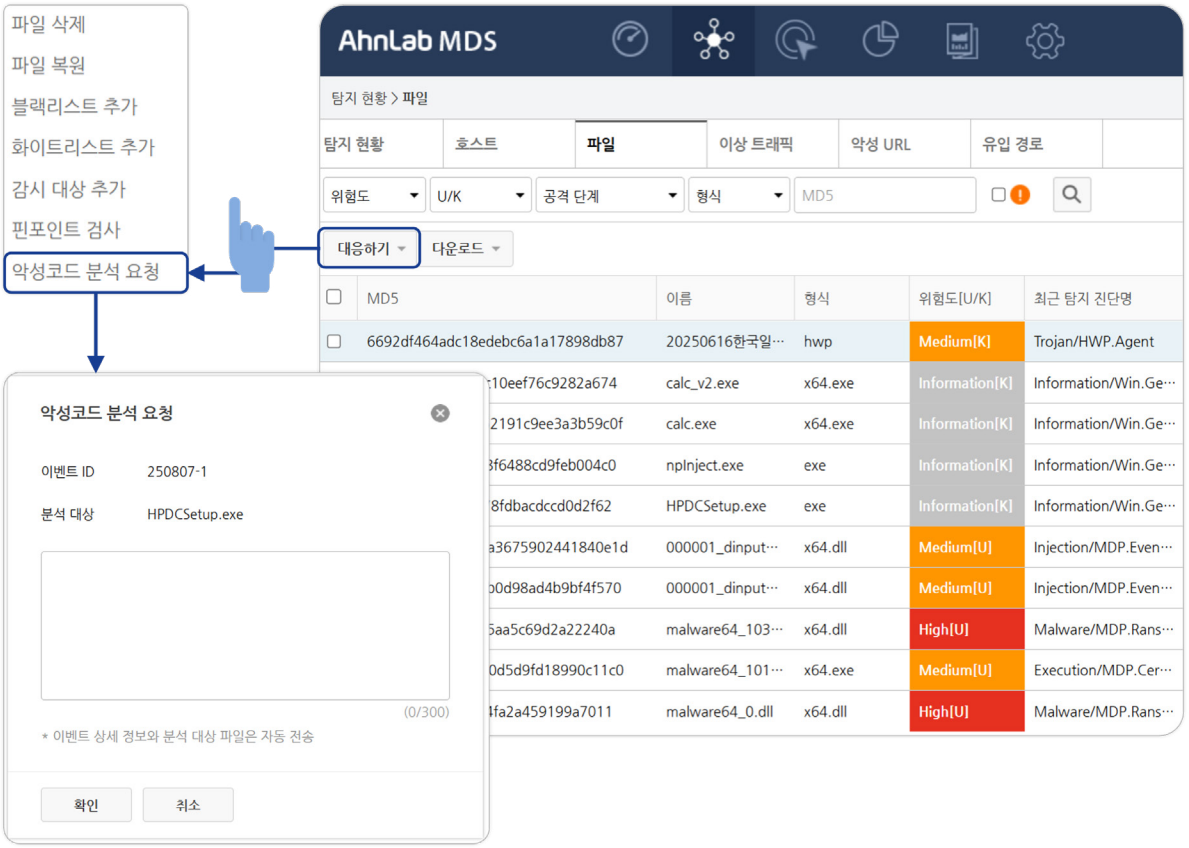
우선, AhnLab MDS는 네트워크 구간을 오가는 파일과 트래픽을 샌드박스 가상환경(VM)에서 분석해 '실행 전 차단(execution holding)', '행위 분석(behavior analysis)' 등을 수행한다. 엔드포인트 단에서도 의심 파일이 사용자 PC에서 탐지되면, AhnLab MDS가 이를 자동으로 수집해 샌드박스 환경에서 실제 행위를 관찰한다. 일정 시간 내 암호화, 삭제, 무단 접근 등 비정상 행위가 확인되면 즉시 실행을 차단한다. 또한, 분석 결과를 관리자 콘솔로 전달해 감염 가능성이 있는 다른 단말을 추적하고 내부 확산을 방지한다.



[그림 5] AhnLab MDS - 샌드박스 기반 행위 분석 및 실행 전 차단

이메일 구간에서도 AhnLab MDS의 MTA(Mail Transfer Agent)는 메일의 헤더, 본문, URL, 첨부파일을 종합적으로 검사한다. 본문에 포함된 URL은 직접 접속하여 이상 유무를 파악하고, 첨부파일은 샌드박스 환경에서 분석한다. 악성 이메일은 격리시켜 시스템에 유입되지 않도록 한다.

이 외에도 AhnLab MDS는 '악성코드 분석 요청' 기능을 제공해, 내부에서 발견된 의심 파일을 안랩의 전문 분석가들에게 전송·보고할 수 있도록 지원한다. 관리자는 분석 보고서를 통해 위협 유형, 감염 경로, 확산 여부를 확인하고 신속히 조치할 수 있다.



[그림 6] AhnLab MDS – 악성코드 분석 요청

2단계: 탐지와 대응 - "침투를 허용하더라도 확산은 막는다"

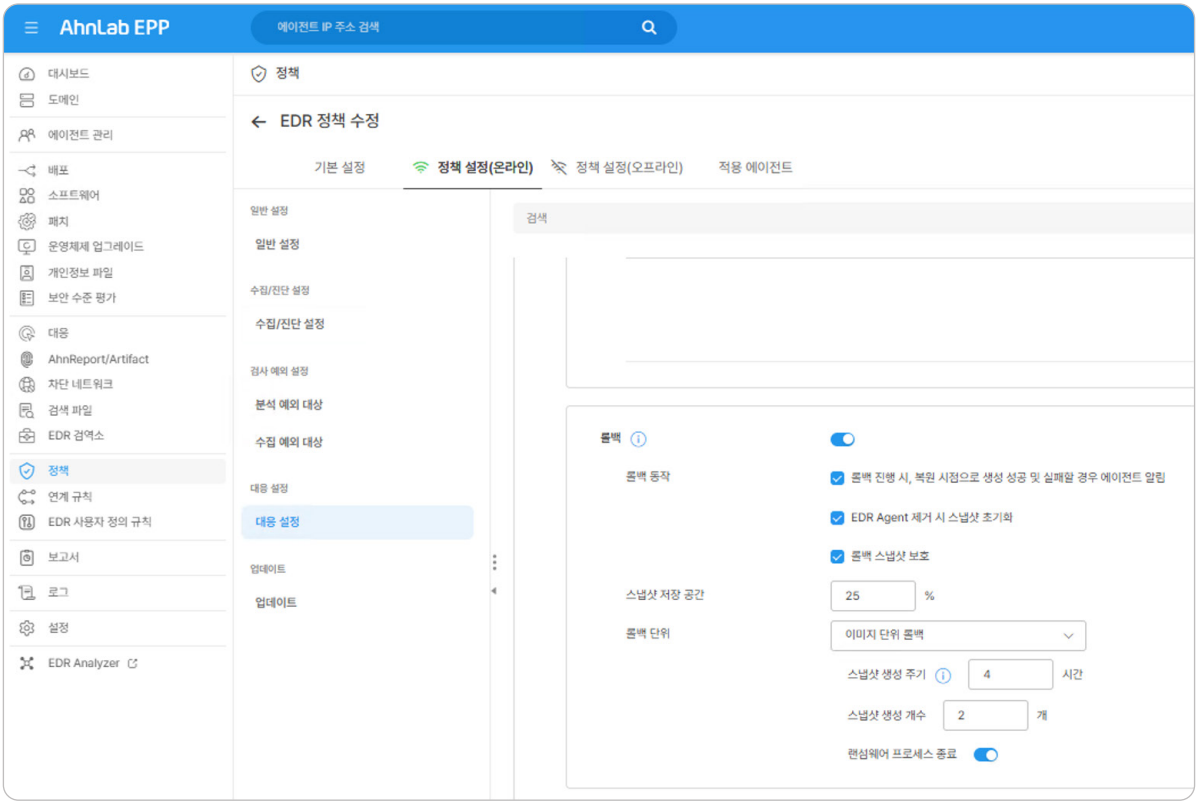
① AhnLab EDR – 위협의 '맥락'을 읽는 눈

AhnLab EDR은 단순한 이벤트 모니터링 도구가 아니다. 각 엔드포인트에서 발생하는 모든 행위를 시간과 프로세스 단위로 기록하고, 공격의 맥락을 분석해 위협의 흐름을 재구성한다. 즉, 단일 이벤트가 아닌 '행위 간 연관성'을 기반으로 위협을 인식하는 것이다. 이를 통해, 사용자의 엔드포인트 위협 관리, 알려지지 않은 위협의 잠복 기간 최소화와 잠재적 피해 및 재발 방지를 지원한다.

그리고, AhnLab EDR에도 랜섬웨어 보안에 특화된 기능들이 탑재되어 있다. 대표적인 기능은 다음과 같다.

A. 자동 롤백 (Auto Rollback)

감염 시점 이전 상태로 파일을 복원할 수 있는 기능이다. 과거에는 관리자가 직접 롤백을 수행해야 했지만, 현재는 자동 옵션을 통해 탐지 즉시 복구가 가능하다.

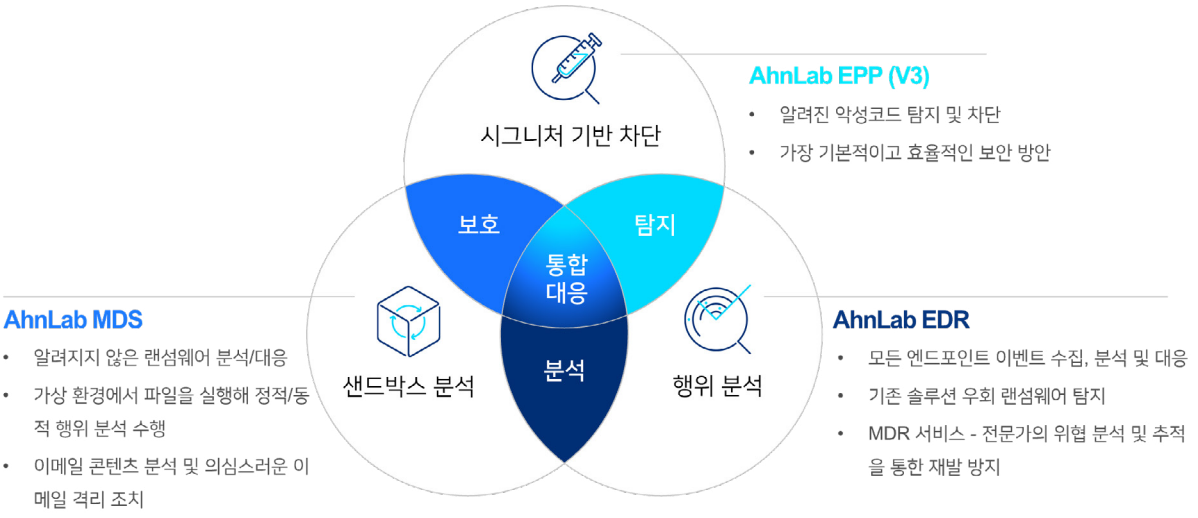


[그림 7] AhnLab EDR – 자동 롤백 기능 화면

B. 보안 뉴스 & IOC 위젯

AhnLab EDR은 안랩의 위협 인텔리전스 플랫폼 AhnLab TIP의 최신 보안 권고문에서 제공되는 IP, URL, 해시값 등을 자동 수집해 내부 로그와 비교 분석한다. 관리자는 '이 뉴스와 관련된 위험 단말'을 즉시 확인할 수 있어, 대응 속도를 단축할 수 있다.

지금까지 설명한 AhnLab EPP(V3), MDS, EDR은 안랩의 랜섬웨어 보안 오퍼링 중에서도 핵심 축을 담당한다. EPP(V3)가 엔드포인트 1차 보호, MDS가 네트워크-엔드포인트-이메일 행위 분석 및 차단, 그리고 EDR이 엔드포인트 전체 이벤트를 분석 및 대응하는 체계로 이뤄진다. 이 세가지 솔루션은 유연하게 상호연동하여 탐지 – 분석 – 대응이 유기적으로 연계된 멀티 레이어 보안 체계를 구축한다.

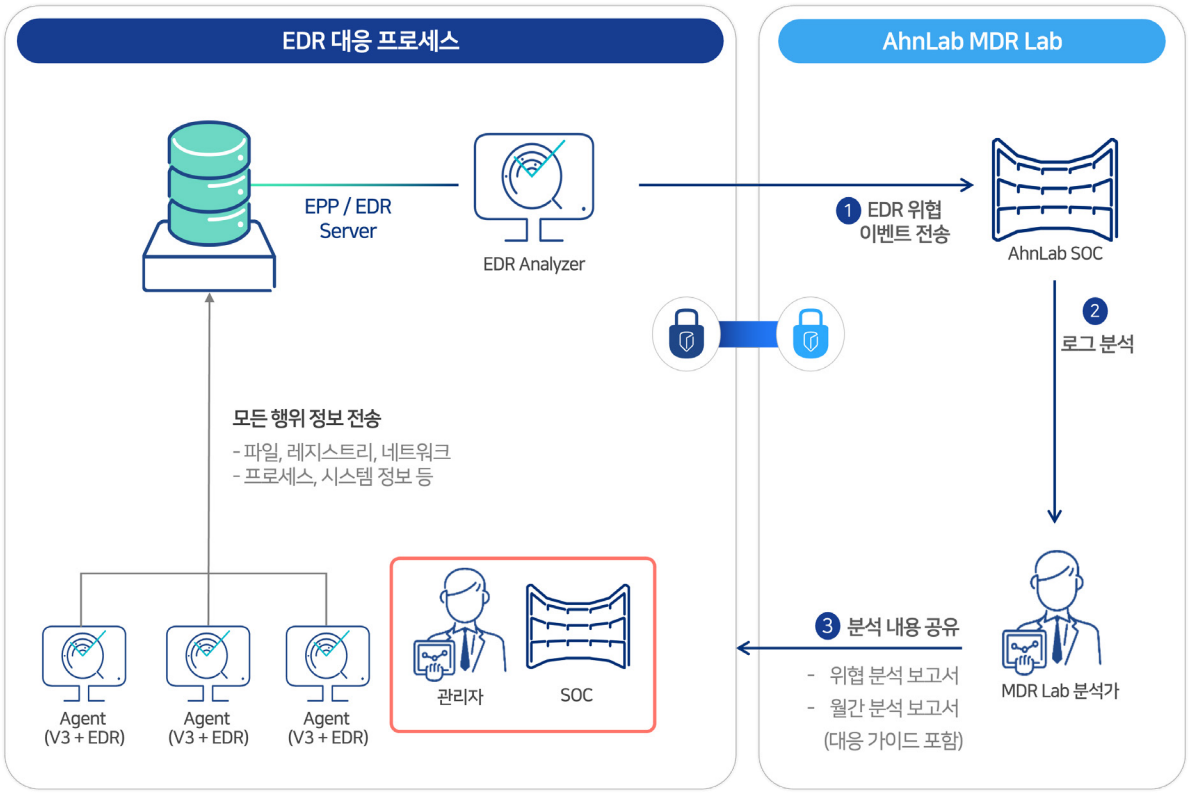


[그림 8] AhnLab V3-MDS-EDR 연동 보안 체계

② MDR – 탐지 그리고 '사람 중심 대응'

EDR이 기술적 기반이라면, MDR(Managed Detection & Response)은 사람의 경험이 더해진 위협 대응 프로세스다. 안랩의 보안 전문가들은 AhnLab EDR에서 탐지되는 위협을 24시간 감시하고, 침해 징후를 사전에 추적(hunting)한다. 이상 징후가 발견되면 신속한 대응과 탐지를 수행하는 전문적인 운영 프로세스를 통해 고객의 위협 이벤트를 상시 분석한다.

MDR의 강점은 실시간 분석력과 커뮤니케이션이다. 단순 로그 해석을 넘어 '이 이벤트가 단독 행위인가, 혹은 연쇄 공격의 시작인가?'를 판단하고, 위험도와 전파 가능성, 비즈니스 영향까지 고려한 대응 방안을 제시한다. 이를 통해 보안 인력이 부족한 기업도 탁월한 위협 탐지 및 대응 프로세스를 갖출 수 있다.



[그림 8] AhnLab V3-MDS-EDR 연동 보안 체계

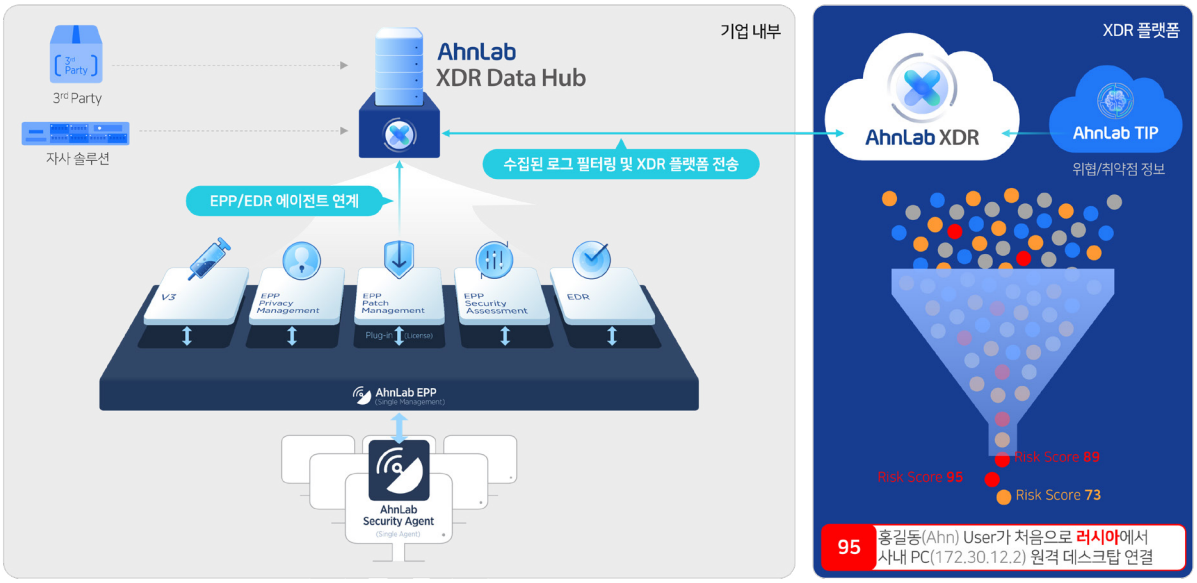
정리하면, EDR과 MDR의 결합은 사람과 기술이 함께 작동하는 실시간 위협 대응 체계를 완성한다. 공격을 막지 못하더라도 확산은 반드시 차단한다는 철학을 기술적으로 구현한 단계라 할 수 있다.

3단계: 운영과 협업 - "보안의 끝은 통합 관리"

랜섬웨어를 포함한 최신 위협은 엔드포인트, 이메일, 클라우드, 네트워크 등 보안 구간을 가리지 않는다. 따라서, 모든 보안 영역을 아우르는 통합 가시성을 확보하는 것이 최우선 과제가 되었다.

① AhnLab XDR – 데이터를 잇는 '보안 허브'

AhnLab XDR은 엔드포인트, 네트워크, 클라우드, 이메일 등 다양한 시스템 로그를 통합해 가시화하고, 이벤트 간 상관관계를 분석해 공격의 전체 흐름을 파악한다. 분산된 침해 징후를 하나의 맥락으로 재구성해 보안 담당자가 위협 전개 과정과 영향도를 쉽게 파악할 수 있도록 한다.

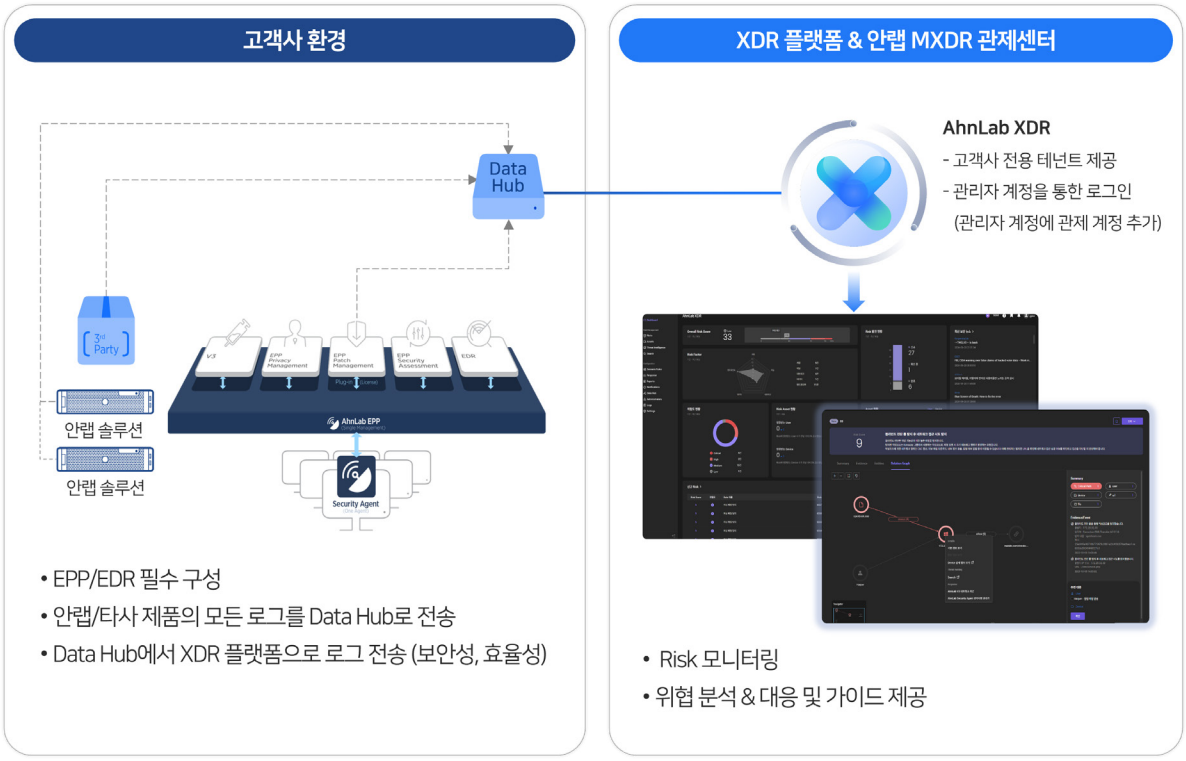


[그림 10] AhnLab XDR - 통합 데이터 플랫폼 기반 상관분석

이 과정에서 위협의 심각도는 리스크 지수로 정량화해 관리자가 대응 우선순위를 명확히 판단할 수 있도록 한다. AhnLab XDR에 탑재된 생성형 AI 'AhnLab Annie'는 사용자의 보안 의사결정 과정 전반을 지원한다. 또한, 오픈 API 기반의 Open XDR 구조를 통해 타사 솔루션과도 유연하게 연동할 수 있다. 기업은 보안 체계를 보다 확장 가능하게(scalable)하게 만들고 유기적인 플랫폼으로 발전시킬 수 있다.

② MXDR – '통합 운영'을 완성하는 전문가의 손길

XDR이 데이터를 통합해 리스크를 관리한다면, MXDR은 그 통합 데이터를 기반으로 전문가가 직접 보안을 운영하고 대응하는 단계다. 안랩의 MXDR 서비스는 고객사의 AhnLab XDR 플랫폼을 원격으로 관리하며, 24시간 모니터링, 위협 헌팅, 리스크 대응 등을 수행한다. 전문가가 단일 이벤트의 이상 징후부터 복합 공격까지 분석하고, 비즈니스 영향도를 평가해 최적의 대응 방안을 제시한다.



[그림 11] AhnLab MXDR의 통합 위협 대응 구조 (전문가 분석 서비스 + XDR 플랫폼)

MXDR은 단순한 관제 서비스가 아니라 보안 전문가가 고객사 보안팀의 일원처럼 상시적으로 협업하는 하이브리드 운영 모델이다. XDR의 데이터 기반 자동 탐지 능력과 사람의 분석 역량을 결합해 '탐지 – 분석 – 대응' 전 과정을 완성형 프로세스로 구현한다.

③ AhnLab TIP – 인텔리전스로 완성하는 선제적 보안

AhnLab TIP는 최신 침해지표(IoC), 위협 그룹 분석, 공격 전술·기법(TTP) 정보를 통합해 제공하는 예측형 보안 인텔리전스 허브다. 이를 통해 국내외에서 수집된 위협 정보를 표준화하고, 공격자 그룹의 전술과 행위 패턴을 기반으로 '예측 가능한 보안'을 구현한다.

또한, AhnLab TIP는 AhnLab EPP, AhnLab XTG, AhnLab EDR, AhnLab XDR 등 안랩의 주요 솔루션들과 실시간으로 연동해 새롭게 탐지된 IoC를 각 제품의 탐지 정책에 자동으로 반영한다. 이는 단순 정보 제공이 아니라, 보안 이벤트의 통합 가시성과 자동 대응, 연관관계 분석까지 아우르는 통합 보안 프로세스의 일부다.

이런 구조 덕분에 안랩 솔루션은 위협 인텔리전스 '수집 – 탐지 – 차단 – 대응'이 실시간으로 순환하는 자동화된 위협 대응 체계를 갖추고 있다. AhnLab TIP는 개별 솔루션 위에 존재하는 '보안 프로세스의 중심 허브'로 조직이 예측 불가능해 보이는 위협에도 한 발 앞서 대응할 수 있도록 돕는다.

전 세계적으로 검증된 기술력

안랩의 랜섬웨어 보안 오퍼링을 구성하는 핵심 솔루션들은 글로벌 사이버 보안 평가에서 우수한 성적을 거두며 탁월한 기술력을 입증해오고 있다.

우선, AhnLab V3는 2013년부터 AV-TEST에 참가해 60회 이상 인증을 획득했다. 2025년에는 '지능형 위협 방어 테스트(Advanced Threat Protection Test, 이하 ATP 테스트)'에서 만점을 획득하며 고도화된 공격 차단 역량을 검증받았다. ATP 테스트는 마이터어택 프레임워크를 토대로 설계된 10가지 사이버 공격 시나리오를 활용해 제품의 탐지 & 차단 역량을 평가했다.

또한, AhnLab EDR과 AhnLab XDR은 전 세계적으로 가장 공신력 있는 보안 제품 테스트 중 하나인 마이터 어택 평가(MITRE ATT&CK Evaluation)에서 우수한 성적을 거뒀다. 2024년 진행된 라운드 6에서는 주요 랜섬웨어 그룹 클롭(CL0P)과 록빗(LockBit)이 윈도우와 리눅스에 걸쳐 수행하는 실제 공격 기법으로 구성된 시나리오 중 95%를 탐지했다. 이는 전 세계 보안 기업들 중에서도 상위권에 해당하는 성적이다.

뿐만 아니라, 탐지한 56개 세부 단계(substep) 중 49개에서 최고 등급인 Technique을 받았는데, 이는 사용자가 탐지 정보를 통해 위협 행위에 대한 '맥락(context)'을 포괄적으로 이해할 수 있다는 방증이다.

이처럼 안랩의 주요 랜섬웨어 보안 솔루션들은 전 세계적으로 꾸준히 검증 받으며 고객 신뢰도를 높여가고 있다.

결론: 예측 가능한 보안, 사람과 기술의 시너지로 완성

랜섬웨어는 더 이상 단일 기법의 공격이 아니다. 침투 뒤에도 정보 탈취, 내부 전파, 외부 협박이 이어지는 복합적 위협 체인이 있다. 이제 필요한 것은 보안 솔루션의 나열이 아니라, 예측 가능한 프로세스 기반의 통합 대응 체계다.

안랩의 랜섬웨어 통합 보안 전략은 이러한 침해 대응 프로세스를 현실화한 모델이다. '사용자 및 기기 검증(XTG) – 위협 탐지 및 차단(EPP & MDS) – 엔드포인트 행위 분석 및 추적 (EDR) – 전문가 주도 엔드포인트 보안(MDR) – 통합 리스크 관리(XDR) – 전문가 주도 통합 위협 대응 (MXDR) – 위협 인텔리전스(TIP)'로 이어지는 멀티 레이어 구조가 바로 그것이다. 이 프로세스 하에서 보안 기술은 위협을 빠르게 식별하고 전문가는 공격의 맥락을 해석한다. 여기에 AI 기술이 더해져 최적의 대응이 가능해진다.

지금은 사이버 위협에 '얼마나 빠르고 정확하게' 대응하는지가 관건인 시대다. 안랩은 앞으로도 자사 솔루션과 서비스를 긴밀히 연동해 사람의 통찰과 기술의 자동화가 결합된 예측형 보안 체계로 고객의 비즈니스 환경을 함께 지켜 나갈 것이다.

AhnLab

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