# 보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

## EDR이 백신을 대체할 수 있나요?

AhnLab 2023-04-28

디지털 전환의 가속화, 비대면 서비스 일상화로 네트워크 연결 접점이 증가하면서, 침해사고에 대한 우려도 확산되고 있다. 많은 기업이 다양한 최신 보안 솔루션을 도입하고 있지만, 이는 운영 및 관리 소홀에 따른 또 다른 보안 홀(hole)을 야기한다. 갈수록 지능화되는 위협에 대한 정확한 탐지와 능동적인 대응, 효율적인 보안 솔루션 운영, 관리를 위해 보안 솔루션 간 연계는 이제 선택이 아닌 필수다.

안랩은 제품과 제품, 제품과 서비스를 유기적으로 연동해 통합 보안을 실현하고 있다. 지난 3월호에서는 안랩의 통합 오퍼링에 관해 자세히 소개한 바 있다. 이번 글에서는 안랩의 주요 엔드포인트 및 네트워크 보안 제품인 AhnLab V3와 MDS, EDR 각각의 특징과 상호 연계성을 살펴본다.


### 제품별 기능 및 특징

이들 3가지 제품 간의 연관 관계를 설명하기에 앞서, 각 제품의 주요 기능과 특징부터 간단히 소개한다.

**1) AhnLab V3**

AhnLab V3는 컴퓨터 보안을 위한 백신 프로그램으로, 안랩의 대표적인 엔드포인트 보안 제품이다. V3는 시그니처(Signature) 방식을 사용해 알려진 위협을 빠르게 탐지, 차단한다. 여기서 시그니처 방식이란 파일의 표면, 즉 외형 데이터를 분석해 정상 파일과 악성 파일 각각의 고유 특징을 추출하는 기법이다.

또한, V3는 1,500여 개의 악성 행위 패턴을 탐지해 알려진 위협에 대응한다. 다만, 전통적인 시그니처, 룰 기반의 진단으로는 랜섬웨어, 파일리스(Fileless) 공격 등을 포함한 신규 위협 및 알려지지 않은 위협 탐지에는 한계가 있다. 이에 V3는 '디코이 파일 진단', '앱 격리 검사', '랜섬웨어 보안 폴더' 기능을 통해 랜섬웨어에 대응한다.

또 '프로세스 메모리 진단' 및 'AMSI(Anti Malware Scan Interface)' 진단을 통해 매그니베르와 같은 파일리스 형태로 유포되는 악성코드를 탐지 및 차단할 수 있다.

**2) AhnLab MDS**

AhnLab MDS(Malware Defense System)는 지능형 지속 위협(APT) 공격에 대응하는 네트워크 샌드박스 솔루션이다. 네트워크, PC, 이메일 서버 앞단, 망연계 구간 등 파일이 존재하는 모든 영역에서 파일을 검사한다. 네트워크로 유입된 의심스러운 파일을 격리된 가상 VM 환경에서 실행하고, 행위 분석을 통해 악성 여부를 확인한다. 이를 통해 제로데이(Zero Day) 공격, 랜섬웨어, 취약점 공격, APT 등 다양한 보안 위협을 효과적으로 탐지하고 대응함으로써 내부 시스템의 악성코드 감염을 사전에 방지한다.

MDS는 데이터 DB와 머신러닝(ML), 인공지능(AI)을 활용해 위협을 정확하고 신속하게 탐지, 대응한다. 또한, 이들 기술을 바탕으로 피싱 및 스캠 메일에 포함된 URL 링크를 분석하고 악성 여부를 판단하는 MTA(Mail Transfer Agent) 기능을 제공한다. 더 나아가, MDS 에이전트(Agent)를 통해 파일 실행을 보류하고, VM 우회형 멀웨어 대응 기술도 지원한다.

V3와 차이점이 있다면, V3도 동적 검사 기능을 제공하지만 설치된 단말의 리소스를 일부 활용해 악성 진단을 하기 때문에 한정적인 검사만 가능하다. MDS의 경우 고성능 어플라이언스 내 샌드박스 환경에서 다수 엔진을 기반으로 다양한 운영 환경을 구현해 동적 검사를 수행한다. 이를 통해 MDS는 문서 파일을 실행 및 조작해 숨겨진 악성 행위를 찾아내거나, 알려지지 않은 위협에 대한 탐지가 가능할 뿐 아니라, 안티바이러스 솔루션에 대한 우회 동작을 하는 랜섬웨어도 진단할 수 있다.

**3) AhnLab EDR**

AhnLab EDR(Endpoint Detection & Response)은 자체 개발한 행위 기반 분석 엔진을 바탕으로 엔드포인트 위협을 탐지, 대응하는 솔루션으로, PC 및 여러 디바이스에서 발생하는 모든 행위를 모니터링한다. 엔드포인트를 노리는 알려지지 않은 위협의 잠복 기간 최소화, 잠재적 피해 및 재발 방지를 목적으로 한다.

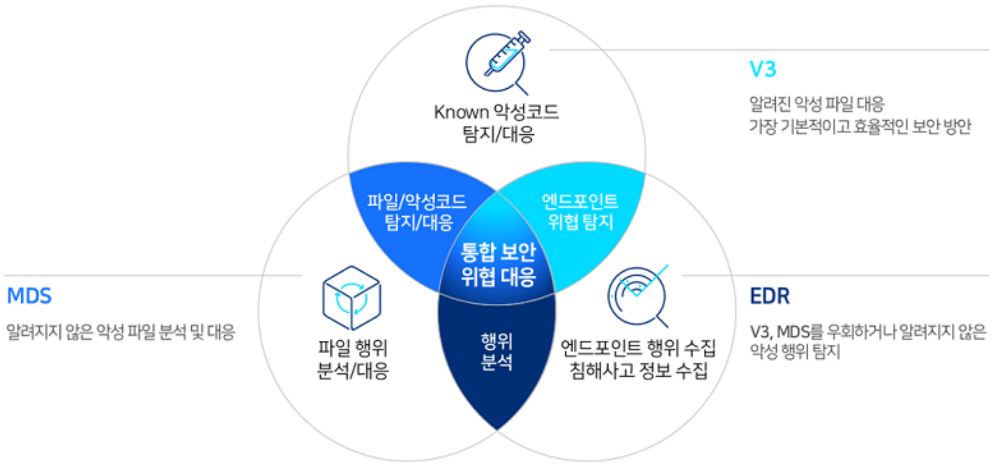
EDR은 모든 엔드포인트 행위 정보 수집, 연관 관계 및 공격 단계별 다차원 분석, 폭넓은 엔드포인트 가시성 기반 진일보한 위협 대응, 연속적인 모니터링 및 통합 보안 관리 기능을 중점적으로 제공한다. 또한, 안랩의 전문 기술력이 응축된 전용 콘솔, 'EDR Analyzer'를 지원함으로써 사용자가 탐지 및 분석, 대응 관점에서 위협을 정확하게 인지하고 조건을 설정하도록 하는 운영 편의성도 제공한다.

또한, EDR은 탐지 유형별로 위협을 분류해 위협 인지부터 분석, 대응까지 빠른 워크플로우를 지원한다.
AhnLab EPP, AhnLab MDS 등 다양한 솔루션과 연동해 위협 대응 역량을 극대화하고, 고객사 환경에 최적화된 엔드포인트 보안 운영이 가능하다.

궁극적으로, EDR을 활용하면 위협을 능동적으로 추적할 수 있어, 고객사는 사전 예방 및 재발 방지 체계를 보다 더 수월하게 구축할 수 있다.

**제품간 연계 및 보안을 통한 통합 보안 실현**

AhnLab V3와 MDS, EDR 모두 엔드포인트와 네트워크 보안 영역에서 뛰어난 성능을 자랑한다. 그리고 이들 제품을 연계해 사용할 경우 각 제품의 한계를 보완하고, 시그니처 기반 차단부터 샌드박스 동적 분석, 행위 탐지 및 대응 등 전방위적인 보안 역량을 확보할 수 있다.




[그림 1] V3, MDS, EDR 통합 보안

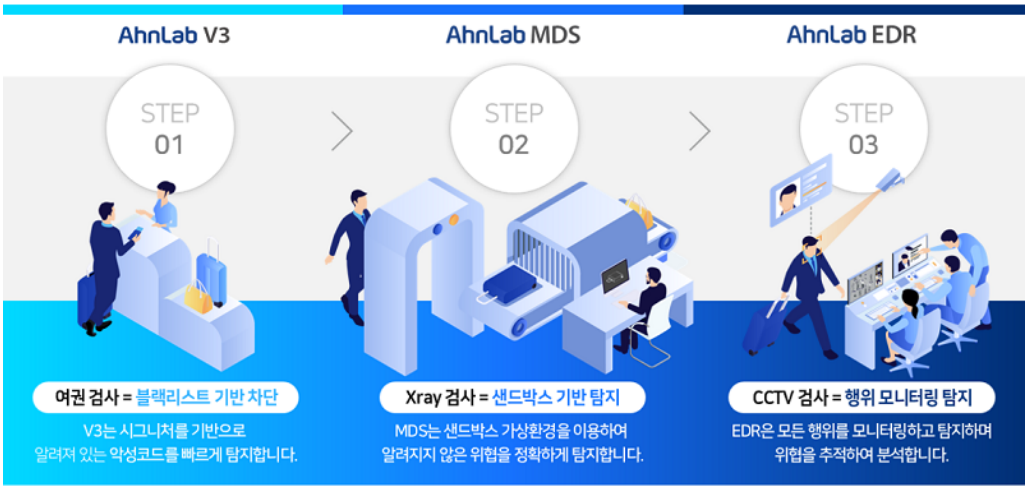
예를 들어, V3를 설치한 서버에 MDS와 EDR을 추가한다면, 에이전트에 악성 파일 삭제, PC 격리, 공지사항 전달 등의 대응 명령을 내리고, ML 및 빅데이터 기반 위협 탐지 기능을 통해 APT 공격 등 알려지지 않은 위협을 효과적으로 탐지 & 대응할 수 있다. 또한, 사용자에게 파일의 실행부터 종료까지의 행위를 상세 분석한 결과 보고서를 제공하고, 바이러스토탈(VirusTotal) 연동을 통해 악성 판단 여부를 효과적으로 판단할 수 있도록 한다.

이와 같은 체계에서, MDS는 네트워크 트래픽에서 파일을 추출, 수집해 백신보다 먼저 파일 분석을 수행한다. 실행 및 비실행 파일을 샌드박스 가상 환경에서 구동시키고 행위를 분석해 악성 여부를 판단하며, 미검사된 파일에 대해서는 실행을 보류해 위협 행위를 사전에 차단한다. 또, 스팸메일 솔루션과의 연동으로 메일 본문의 첨부 파일을 분석하는 등 이메일 검사를 실시해 통해 피싱 및 스캠으로 인한 피해를 최소화한다. 이 외에, 문서 검사를 위한 전용 엔진을 탑재하고 있어 문서를 악용한 공격도 방지한다.

EDR은 알려지지 않은 위협뿐만 아니라 V3와 MDS를 우회하는 공격도 차단한다. 엔드포인트에서 발생하는 모든 프로세스 및 파일, 네트워크, 레지스트리, 시스템 행위를 수집하고, 안랩의 노하우와 마이터 어택(MITRE ATT&CK) 프레임워크를 이용한 탐지 패턴 및 규칙(Rule)으로 위협을 모니터링하고 탐지한다. 고객사 환경에 맞는 IoC, 야라(YARA), 행위 규칙 생성을 통한 위협 탐지 및 대응도 가능하다.

또, EDR은 V3, MDS와 유기적인 연동을 통해 추가적인 분석이 가능하다. V3에서 악성코드로 진단된 정보를 기반으로 EDR이 유입 경로 등 상세 분석 정보를 제공하여 향후 발생할 수 있는 동일 위협을 선제적으로 막을 수 있도록 한다. EDR에서 수집된 다양한 프로세스/파일 정보를 샌드박스에서 분석하고자 할 경우 MDS를 통해 분석 결과를 확인하여 위협에 대한 추가 증적을 확인 할 수 있다.

정리하면, V3, MDS, EDR은 각 보안 영역에서 수행하는 역할이 조금씩 다르다. 이들의 역할은 입국 심사에 비유할 수 있다. 예를 들어, V3는 시그니처와 패턴을 기반으로 악성코드를 빠르게 탐지하고 문제가 되는 파일과 URL 등을 차단, 삭제 및 치료해 사전에 대응한다는 점에서 블랙리스트(Blacklist)를 기반으로 입국자를 심사하는 여권 검사와 같다고 할 수 있다. 여권 검사 이후 수하물 및 휴대품에 대해 안보위해물품과 반출입금지 품목을 정밀하게 스캔하는 X-ray 검사는 MDS가 샌드박스 기술을 기반으로 알려지지 않은 위협을 정확히 탐지하는 기능과 유사하다. 입국 심사의 마지막 관문인 CCTV 검사 단계에서 입국자의 동선과 움직임을 감시하는 것처럼, EDR은 엔드포인트에서 위협 가능성이 있는 모든 행위를 모니터링 및 탐지하고, 위협을 추적해 분석한다.




[그림 2] V3, MDS, EDR 역할 비교

기업 및 기관에서도 입국 심사 절차와 같이 단계 별로 철저한 보안 시스템 구축이 필요하다. 백신, 샌드박스, EDR로 이어지는 통합 보안 체계를 구축한다면 복잡다단한 시스템 환경을 철저하게 보호하고, 더 강력한 보안 태세를 확립하는데 도움이 될 것이다.

---

AhnLab 콘텐츠기획팀 서보경 사원