EDR, 보안의 "미래" 될까?

차세대 엔드포인트 보안 기술 도입을 위한 제언

AhnLab

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

목차

1. 개요

최근 보안 분야에서 가장 주목 받고 있는 솔루션은 'EDR(Endpoint Detection and Response)'이다.

EDR 시장에 대한 관심이 높은 이유는 기존 보안 솔루션만으로는 부족한 가시성(Visibility)과 대응(Response)을 한층 강화한 솔루션이라는 기대감 때문이다. 과연 EDR은 이런 기대를 충족시키는 새로운 해결책이 될 수 있을까. 아니면 잠시 반짝 유행을 타는 아이템에 그칠까.

본 문서에서는 EDR의 등장 배경과 시장의 요구를 살펴보는 한편, 최근 출시된 AhnLab EDR에 대해 간략히 알아본다.

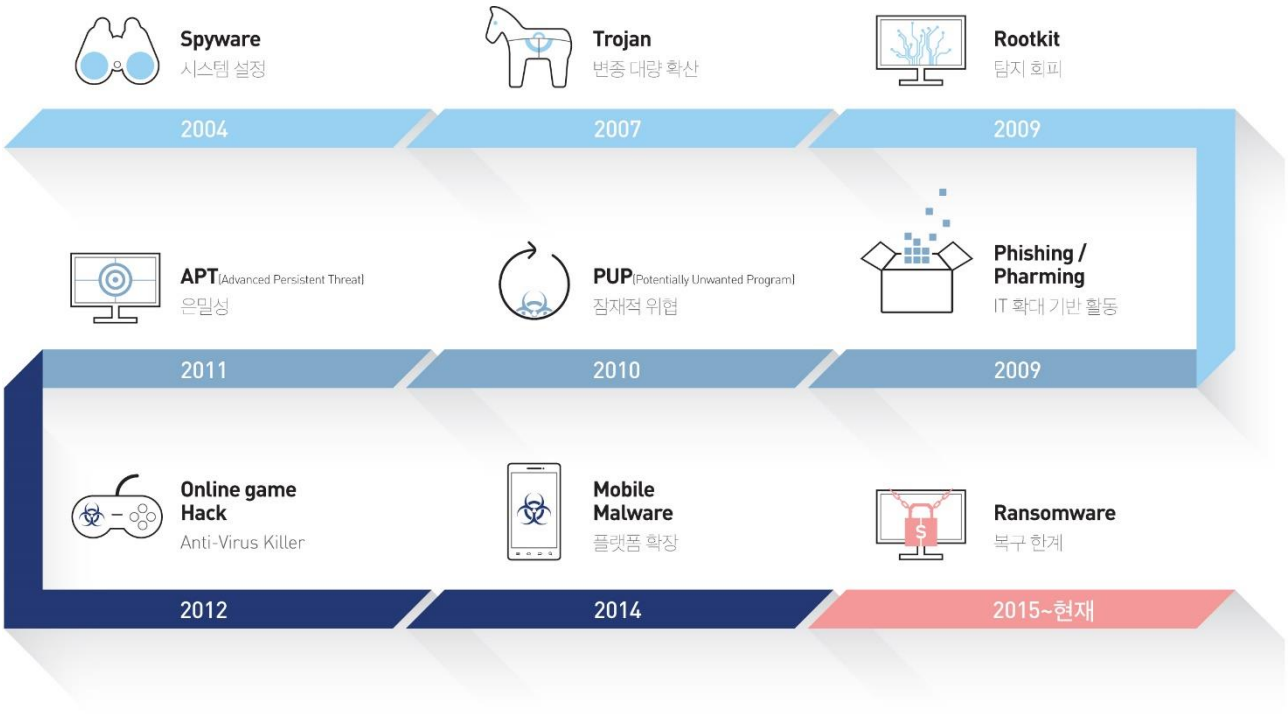
2. EDR 등장 배경

01. 보안 위협 동향의 변화

지난 2017년에도 대형 보안 사고들이 발생했다. 에퀴팩스(Equifax), 우버(Uber), 버라이즌(Verizon) 등의 기업들이 대규모 개인정보 유출사고를 겪었다. 또 전세계를 공포로 몰아넣은 워너크라이(WannaCry)와 페트야(Petya), 국내 인터넷 서비스를 업체를 파산에 이르게 한 에레보스(Erebus) 등 랜섬웨어로 인한 피해도 속출했다.

이들 공격의 시작점은 엔드포인트로, 악성코드를 이용해 전개되었다. 이는 최초의 바이러스로 불리는 '브레인(Brain)'의 등장 이후 지난 30여 년 동안 변함없는 패턴이다.

변화가 있다면 악성코드의 기술이 진화해 보안 솔루션의 탐지를 회피하는 양상을 보인다는 점이다. 변하지 않은 것은 공격자는 계속 악성코드를 활용하고 공격에 성공할 것이라는 점. 따라서 엔드포인트에서 보안 위협을 통합적으로 관리하고 대응할 수 있는 효과적인 전략과 솔루션이 필요하다.



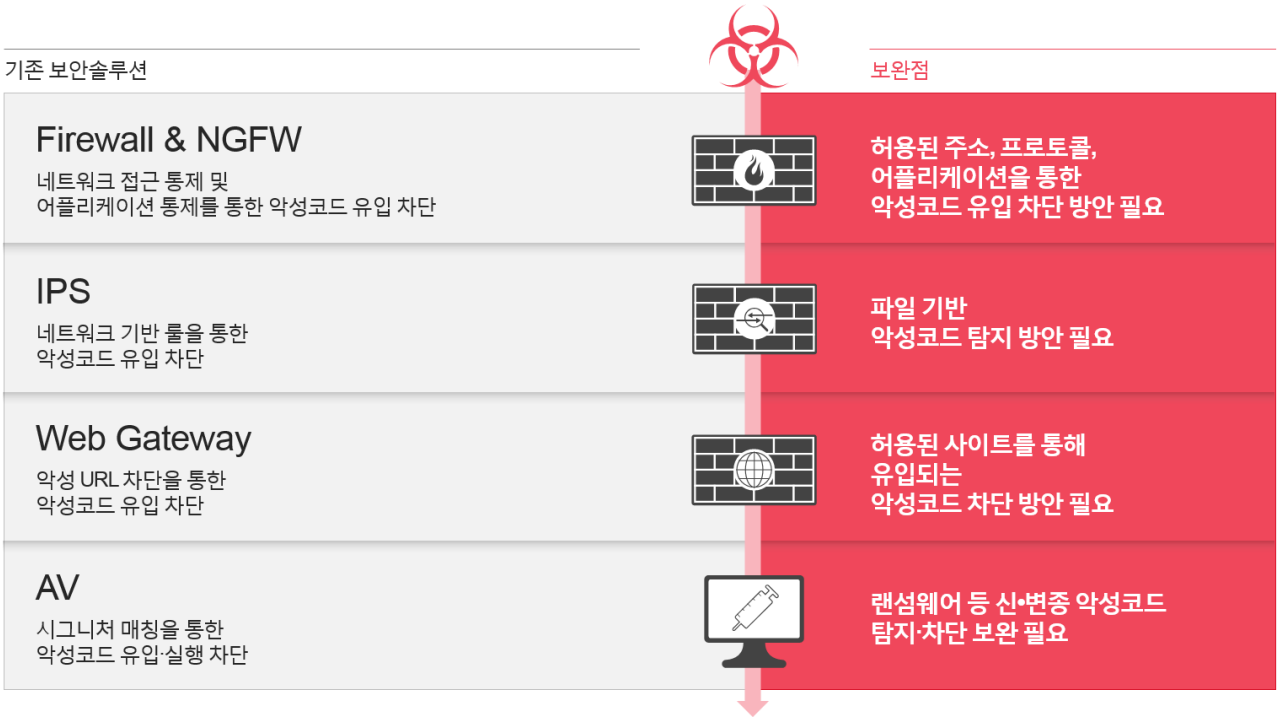
[그림 1] 주요 악성코드 변천사

02. 기존 보안 솔루션의 한계와 시장의 요구

위협 대응 전략의 변화에 대한 필요성은 보안 업계뿐만 아니라 보안 솔루션을 이용하는 고객, 즉 일반 기업 및 공공기관에서도 대두되고 있다. 기업들은 일반적으로 엔드포인트 영역에는 안티바이러스, 패치 관리, 매체 제어, NAC 등의 보안 제품을, 네트워크 영역에는 방화벽(Firewall), 침입방지시스템(IPS), DDoS 방어시스템, 웹 방화벽(WAF) 등을 도입해 운영하고 있다. 그럼에도 불구하고 여전히 악성코드에 감염되고 시스템 마비, 데이터 유출과 같은 피해가 발생한다.

공격자는 안티바이러스 제품은 물론 지능형 위협(APT, Advanced Persistent Threat) 방어 전용 솔루션을 우회하며 정교한 공격을 전개하고 있다. 특히 패치를 적용하지 않은 응용 프로그램, 취약한 웹 사이트 접속 등을 통해 악성코드에 감염되는 사례는 여전히 빈번하게 발생하고 있다. 또한 네트워크 보안 제품은 허가된 주소, 프로토콜, 애플리케이션을 통한 악성코드 유입 차단에 한계를 가진다.

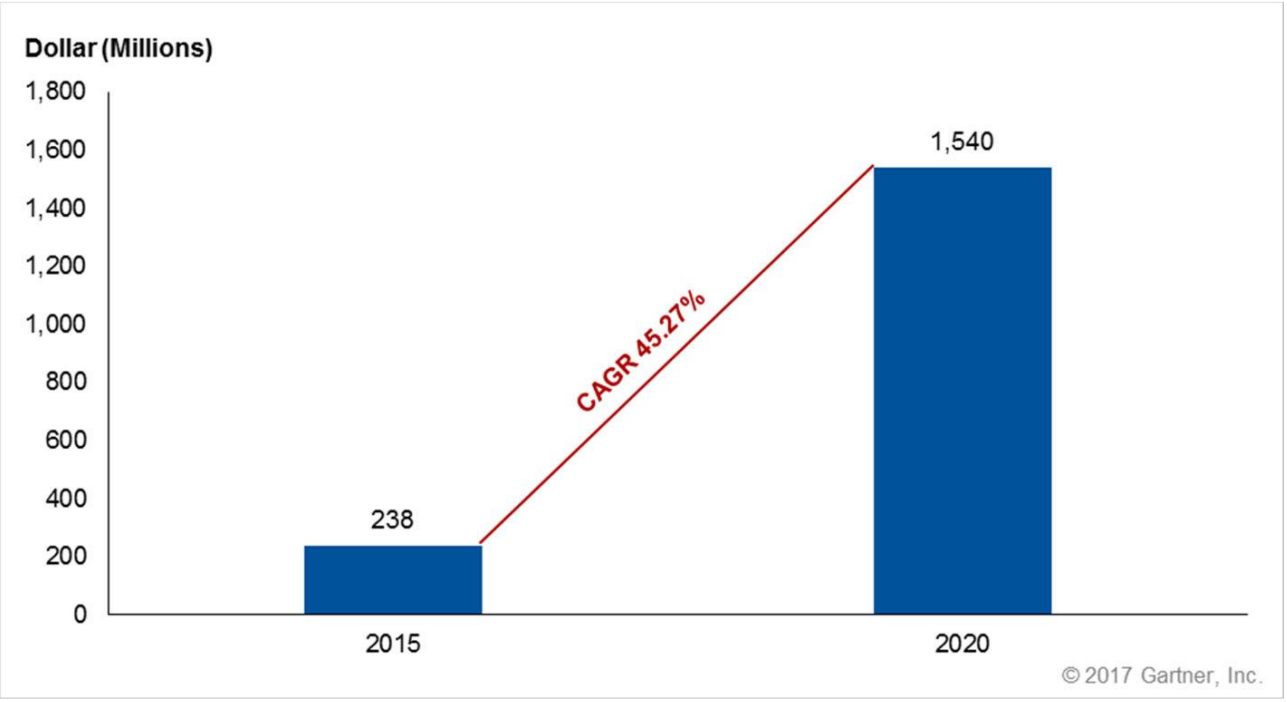
비교적 최신 보안 기술이자 솔루션으로 평가받는 행위 및 데이터 기반의 분석 제품인 UEBA(User and Entity Behavior Analytics)나 SIEM(Security Information and Event Management)도 보안 위협을 100% 차단하는 것은 아니다. UEBA는 행위 기반이기 때문에 SIEM와 같은 데이터 수집 서버가 별도로 필요하다. SIEM은 연동된 단위 보안 제품에서 로그가 전송되지 않을 경우에는 분석할 수 없기 때문에 단위 보안 제품에 의존적일 수 밖에 없다.



[그림 2] 기존 보안 솔루션의 한계

이제 기업은 지금까지 도입한 보안 솔루션만으로 보안 위협을 방어하기에 충분하지 않다는 것을 이해하기 시작했다. 또, 신종 악성코드나 제로데이 취약점을 악용한 '알려지지 않은 위협', 그리고 내재해 있으나 언제 발현될 지 예측할 수 없는 '보이지 않는 위협'에 대응해야 한다는 것을 알고 있다. 기업은 이제 너무 많은 피해가 발생하기 전에 신속한 탐지와 대응을 할 수 있는 솔루션이 필요하다는 것을 인지하고 있다는 것이다.

이러한 관점에서 현재 기업의 보안 담당자들이 가장 관심을 갖고 있는 솔루션이 바로 EDR(Endpoint Detection and Response)이다. 국내뿐만 아니라 세계적으로도 EDR에 대한 니즈와 관심이 높다. 글로벌 리서치 기관 가트너(Gartner)는 전세계적으로 EDR 시장 규모가 2015년 2억 3천 8백 달러에서 2020년 15억 달러로 연평균성장률(CAGR) 45.27% 증가할 것으로 예측했다. 또한 2020년까지 대기업의 65% 이상과 중견 기업의 절반 이하가 완전한 기능을 갖춘 EDR에 투자할 것이라고 전망했다.



[그림 3] EDR 시장 규모 및 성장 전망 (*출처: Gartner)

3. EDR의 정의

그렇다면 현재 보안 분야의 최대 화두인 EDR이 무엇인지 알아보자. EDR의 등장은 지난 2013년으로 거슬러 올라간다. 가트너는 지난 2013년 블로그를 통해 ETDR(Endpoint Threat Detection and Response, 이후 EDR로 축약)을 처음으로 소개했다. 이후 2014년부터 시장과 기술 트렌드, 그리고 주요 벤더들의 움직임을 소개하는 'EDR 마켓 가이드(Market Guide for EDR Solutions)' 보고서를 매년 발행하고 있다.

가트너가 정의하는 EDR은 엔드포인트 레벨에서 지속적인 모니터링과 대응을 제공하는 보안 솔루션을 의미한다. 또, EDR은 ▲보안 침해 탐지(Detect security incident) ▲보안 침해 조사(Investigate security incident) ▲엔드포인트에서의 보안 통제(Contain the incident at the endpoint) ▲치료를 통한 감염 전 상태로의 엔드포인트 회복(Remediate endpoint to a preinfection state) 등 4가지 기능을 제공해야 한다고 설명하고 있다.

즉, EDR은 엔드포인트에서 일어나는 다양한 행위들을 얼마나 빨리 그리고 얼마나 많이 탐지할 수 있는지가 중요하며, 이렇게 탐지된 단말 이외에 또 어떤 단말이 피해를 입었는지 등 엔드포인트 레벨에서 발생한 침해 행위를 추적할 수 있는 가시성(Visibility)을 제공해야 한다. 또한 추가 피해가 발행하지 않도록 감염된 단말을 격리하거나 네트워크를 차단, 취약점을 찾아서 패치를 적용하는 것과 같은 대응(Response)이 가능해야 한다. 이 모든 행위의 목적은 위협의 잠복 기간(dwell time)과 피해를 최소화하는 것이다.

현재 전세계적으로 많은 보안 업체들이 EDR 솔루션을 선보이고 있다. 안랩, 시만텍, 트렌드마이크로와 같은 EPP(Endpoint Protection Platform) 업체들은 기존 제품에 EDR 모듈을 추가하는 형태로 시장에 제품을 출시하거나 준비중이다. 또, 차세대 안티바이러스(Next Generation Anti-Virus) 업체, 신생 EDR 업체도 관련 제품을 출시하고 시장을 선점하기 위해 치열하게 경쟁 중이다.

4. 엔드포인트 플랫폼 기반의 AhnLab EDR

안랩은 최근 AhnLab EDR을 출시했다. 이목을 끄는 점은 차세대 엔드포인트 보안 플랫폼인 AhnLab EPP를 함께 출시했다는 것이다.

최근 보안의 시작과 끝으로서의 엔드포인트가 다시 주목받고 있다. 이를 두고 일부에서는 '엔드포인트 보안'의 귀환이라고 표현하기도 한다. 그러나 안랩은 설립 당시부터 지금까지 엔드포인트 보안의 중요성에 대해 강조해왔다. 특히 지난 2017년에는 안랩 엔드포인트 보안 플랫폼 전략인 AhnLab SECURITY LADDERS를 발표, 엔드포인트 보안의 혁신이 필요하다는 점을 피력해왔다.

AhnLab SECURITY LADDERS는 레거시(Legacy), 적응(Adaptive), 탐지(Detection), 고객 주도(Driven), 엔드포인트(Endpoint), 대응(Response), 서비스(Service)의 약자로, 고객이 주도하는 '쉬운 보안, 실행 가능한 보안'을 의미한다.

► 안랩 엔드포인트 보안 플랫폼 전략 <Security LADDERS> 더 보기

이러한 전략 하에 안랩은 악성코드 탐지 중심이 아닌 위협 관리 대응 중심의 플랫폼으로 대응 관점을 전환하고, 차단을 통한 방어뿐만 아니라 탐지와 신속한 대응이 이루질 수 있도록 탐지(Detection)-분석(Analysis)-대응(Response)'의 순환 구조를 체계화했다.

EDR은 기본적으로 방대한 양의 데이터를 효율적으로 수집•저장•분석해야 하는 동시에 다양한 보안 솔루션과 연동할 수 있어야 한다. 따라서 이를 뒷받침할 수 있는 아키텍처가 반영된 새로운 플랫폼이 필요하다. 이를 구현한 것이 차세대 엔드포인트 보호 플랫폼인 AhnLab EPP이며, 안랩이 EDR과 차세대 플랫폼인 AhnLab EPP를 함께 출시하는 이유다.

[그림 4] 차세대 엔드포인트 보안 플랫폼 AhnLab EPP 기반의 AhnLab EDR 개념도

일반적인 EPP(Endpoint Protection Platform)는 파일 기반 악성코드를 방지하고 응용 프로그램의 악의적인 활동을 탐지•차단하고, 보안 사고에 대응하는데 필요한 조사와 치료를 위한 엔드포인트 보안 솔루션이다.

이에 반해 AhnLab EPP는 안랩의 다양한 엔드포인트 보안 솔루션을 유기적으로 통합•연계하여 지속적으로 발생하는 보안 위협에 대해 탐지•모니터링•대응하는 차세대 플랫폼이다. 이 플랫폼은 단일 에이전트(One Agent)•단일 매니지먼트 콘솔(Single Management Console)을 기반으로 다수의 보안 솔루션을 유기적으로 통합 운영할 수 있다는 것이 가장 큰 강점이다.

예를 들어, V3와 EPP 에이전트 사용 고객이라면 추가 에이전트 설치 없이 AhnLab EDR 라이선스만 추가하여 AhnLab EPP를 통해 통합 관리•모니터링•대응이 가능하다. 뿐만 아니라 이 관리 콘솔을 통해 고객은 패치관리 솔루션(AhnLab Patch Management), 취약점 점검 솔루션(AhnLab 내PC지키미), 개인정보 유출 의심 파일 차단 솔루션(AhnLab Privacy Management) 등 원하는 제품을 선택적으로 사용할 수 있다

5. 결론: 차세대 보안 솔루션 도입을 위한 제언

현재 EDR 시장은 EPP 시장과 빠르게 융합되고 있으며 EDR, EPP, 차세대 엔드포인트 보안 제품은 향후 3~5년 내로 하나의 매니지먼트 콘솔과 에이전트 방식으로 재편될 것이다. 기존 EPP 업체는 공격자를 보다 잘 모니터링하기 위해 EDR 기능을 신속하게 적용하고 있으며, EDR 업체들은 EPP 업체와 경쟁하고 대체할 수 있는 더 나은 탐지•대응 기능을 추가하고 있다.

많은 보안 업체들이 EDR 제품을 출시하고 있고 이를 도입하려는 고객이 늘어나면서 EDR이 '보안의 최종 해결사'처럼 여겨지고 있다. 그러나 한 가지 분명한 것은 EDR이 매우 중요한 역할을 해주지만, 이 또한 보안 위협에 대응하기 위한 또 다른 도구에 불과하다는 점이다. EDR은 이를 활용할 수 있는 사람과 프로세스가 동반되지 않는다면 충분한 효과를 발휘하기 어렵다는 것을 분명하게 인지해야 한다.

