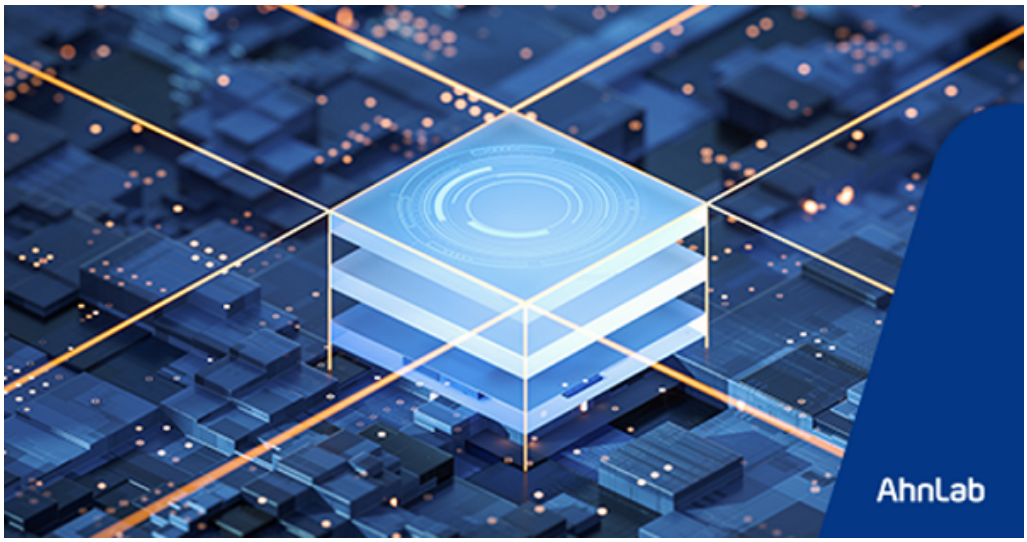
보안 이슈

AhnLab 보안 전문가의 심층분석! 보안 이슈 정보를 전해드립니다.

안랩 제품 간 연동, 이렇게 활용하자

AhnLab 2023-03-06

안랩은 엔드포인트부터 네트워크 그리고 보안 관제 서비스를 비롯한 다양한 전문적인 서비스들까지 통합해 제공할 수 있는 국내 유일의 통합 보안 기업이다. 그간 월간'안'을 통해 통합 보안에 관한 내용들을 다뤄왔는데, 이번 글을 통해 엔드포인트 및 네트워크 제품 간 연계 기능들은 어떤 것들이 있고 이러한 연계 기능을 활용하여 어떻게 하면 효율적인 업무 체계와 보안을 구축할 수 있을지에 대해 다시 한 번 살펴본다.



ChatGPT에게 통합 오퍼링을 묻다

안랩은 올해 고객 통합 커버리지 고도화 및 통합 보안에 대한 역량을 증진하여 고객들의 다양한 보안 요구사항을 해결하는 것을 최우선 과제로 삼고 있다. 이를 위해, 통합 오퍼링이 무엇보다 중요한데 통합 오퍼링이 무엇인지에 대해서 먼저 짚고 넘어가보도록 하겠다.

요즘 GhatGPT의 인기가 대단하다. 웹 검색 엔진과 달리 어떤 질문을 던져도 내가 필요한 정보만 쏙쏙 골라서 보여주니 너무도 신기할 따름이다. 그래서 필자도 ChatGPT의 도움을 받아 통합 오퍼링이 무엇인지에 대해 아래와 같이 정리해 보았다.

통합 오퍼링은 '고객에게 효율적이고 효과적인 방식으로 고객의 요구 사항을 해결하는 완벽하고 통합된 솔루션을 제공하는 것'이라 정의할 수 있다. 통합 오퍼링을 통해 가져올 수 있는 이점은 '모니터링 및 관리를 위한 단일 인터페이스를 통해 여러 보안 제품 및 서비스의 관리를 단순화하고, 제품 및 서비스를 단일 오퍼링으로 통합함으로써 보안 인프라를 관리하는데 필요한 시간과 노력을 감소시킬 수 있다'고 설명한다. 요약하면, 간소화된 관리, 향상된 효율성, 비즈니스 목표를 위한 더 좋은 환경, 개선된 보안 상태 및 비용 절감을 제공해주는 것이 통합 오퍼링이다 라고 말할 수 있다.

안랩이 제공하는 통합 오퍼링

그렇다면 안랩은 어떤 방식으로 통합 오퍼링을 제공하고 있을까? 크게 3가지로 나눌 수 있는데 첫 번째는 통합된 플랫폼, 두번째는 제품과 서비스의 연계, 세번째는 제품 간 연계 및 연동이 있다.

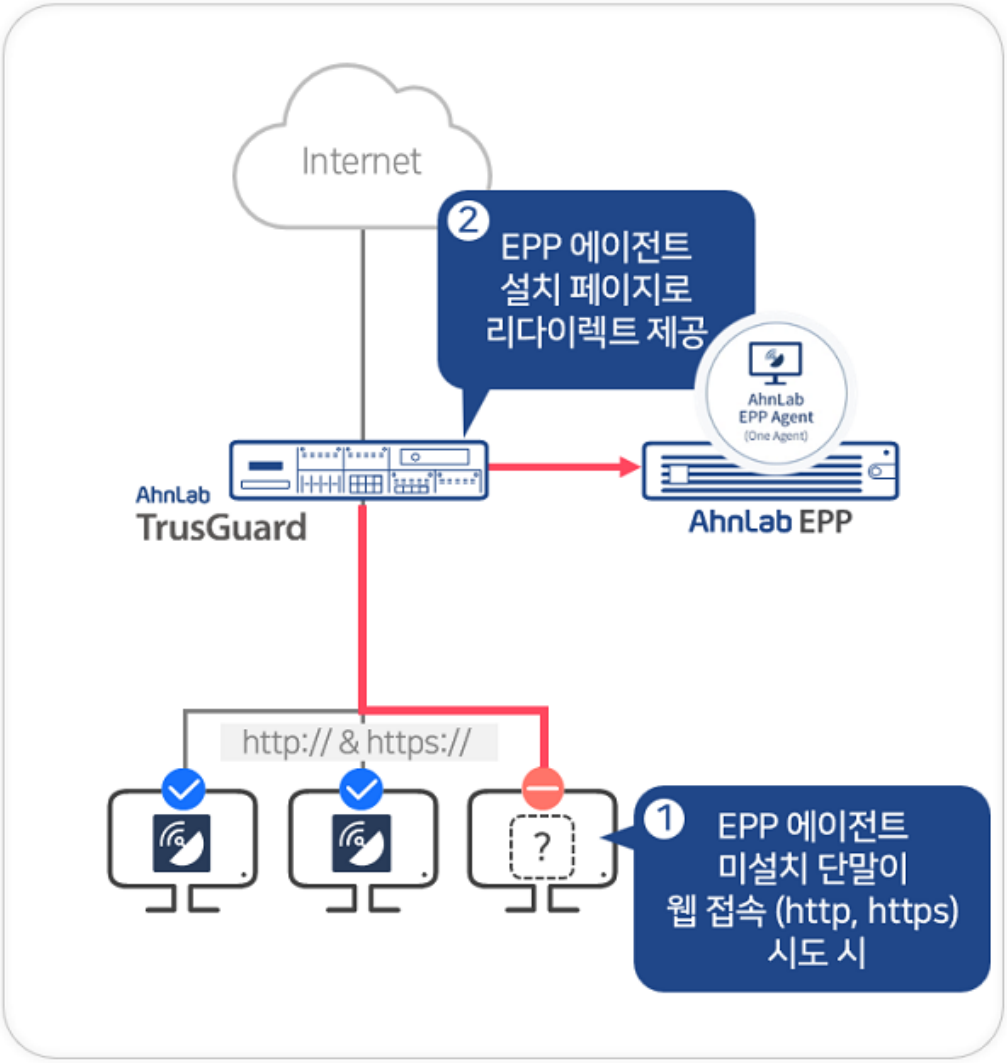
첫 번째로 통합 플랫폼을 살펴보면 우선 'AhnLab EPP Family'라 불리는 V3(백신), EPM(패치관리), ESA(취약점 관리), EPrM(개인정보유출방지), EDR(지능형 위협 대응) 등의 5가지 고유의 제품들을 하나의 플랫폼을 통해 관리하고 다양한 연계 규칙들을 활용할 수 있는 EPP 플랫폼이 있다. 또한, 하이브리드 클라우드 환경에서 AV, 호스트 기반 IPS/방화벽, 애플리케이션 제어 등 다양한 보안 모듈을 통합

으로 관리할 수 있는 AhnLab CPP 플랫폼, 그리고 AhnLab TrusGuard(방화벽), AhnLab AIPS(IPS), AhnLab DPX(Anti-DDoS) 등의 네트워크 장비들에 대해로 중앙에서 정책을 배포하고 통합 관리를 수행할 수 있는 위협 관리 시스템 AhnLab TMS 플랫폼이 있다.

두 번째로 제품과 서비스 연계 부분에서는 안랩의 가장 큰 강점인 AhnLab EDR에서 발생되는 다양한 위협 이벤트들을 안랩의 전문 분석가들이 원격으로 분석 및 대응을 수행해주는 EDR과 MDR 서비스가 있다. 또한, SECaaS(SECurity-as-a-Service) 기반으로 APT 대응 장비인 AhnLab MDS 도입 없이 단말 대상 에이전트 설치만으로 동일한 보안 강화 효과를 가져올 수 있는 MDS 서비스, 그리고 데이터 분석 서비스, 악성코드 분석 서비스 등 다양한 전문 서비스들을 제품과 연계해 제공하고 있다.

세 번째는 이번 글을 상세하게 살펴볼 제품 간 연계 및 연동이다. 본 연계 사례는 8가지 정도의 케이스로 나눌 수 있다.

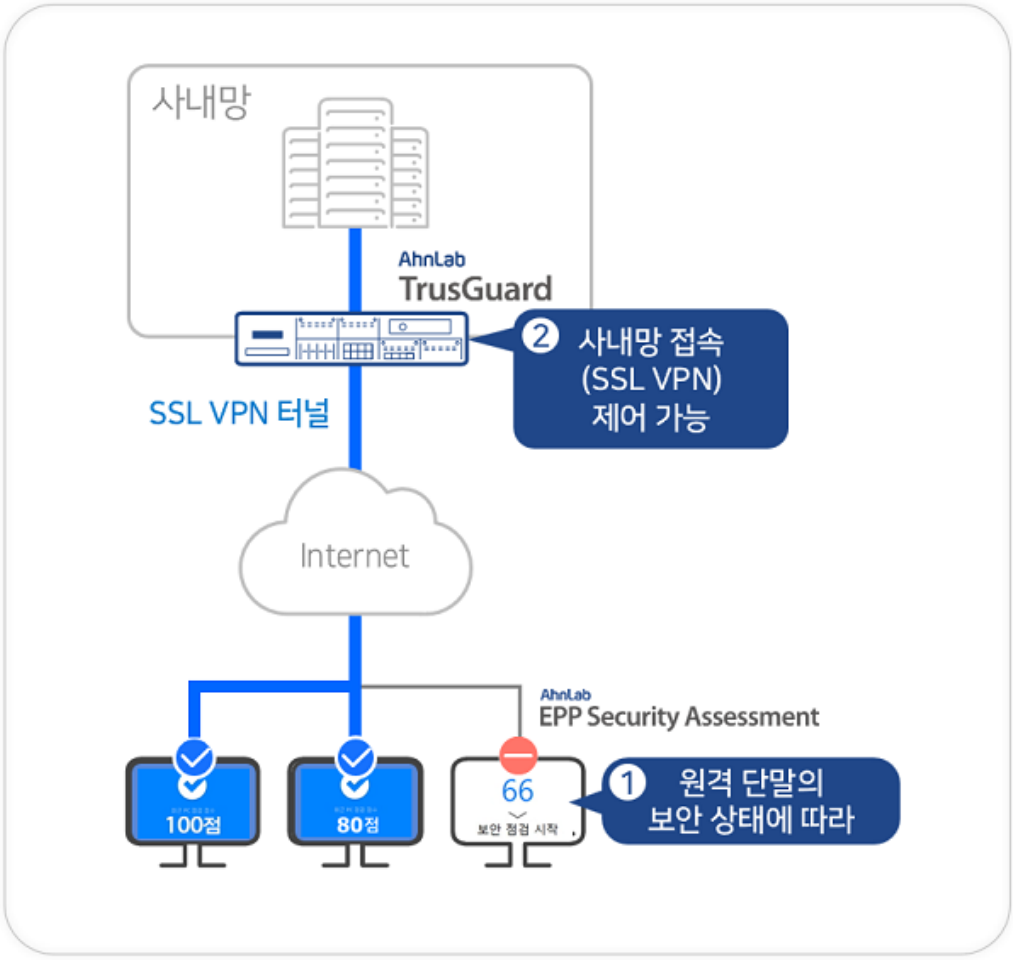
1. EPP + TrusGuard 연계를 통한 에이전트 강제 설치



[그림 1] EPP & TrusGuard 에이전트 강제 설치 구조

해당 연계 기능은 EPP 에이전트 설치 리다이렉트 기능으로 사용자가 백신 제품을 설치하지 않고 웹에 접속하는 경우 에이전트를 설치할 수 있는 웹 페이지로 리다이렉트 해주는 기능이다. EPP를 신규 도입하였거나 기존에 사용을 하고 있으나EPP 서버 하단의 네트워크 환경이 NAT(Network Access Translation)로 구성된 경우 TrusGuard 장비를 NAT 장비로 사용함으로써 EPP 에이전트 리다이렉트 환경을 구성할 수 있다. 해당 기능은 HTTP 및 HTTPS를 모두 지원하며 TrusGuard 하위 모델로도 기능 구현이 가능하기 때문에 비용에 대한 부담 없이 사용할 수 있는 강력한 연계 기능이다.

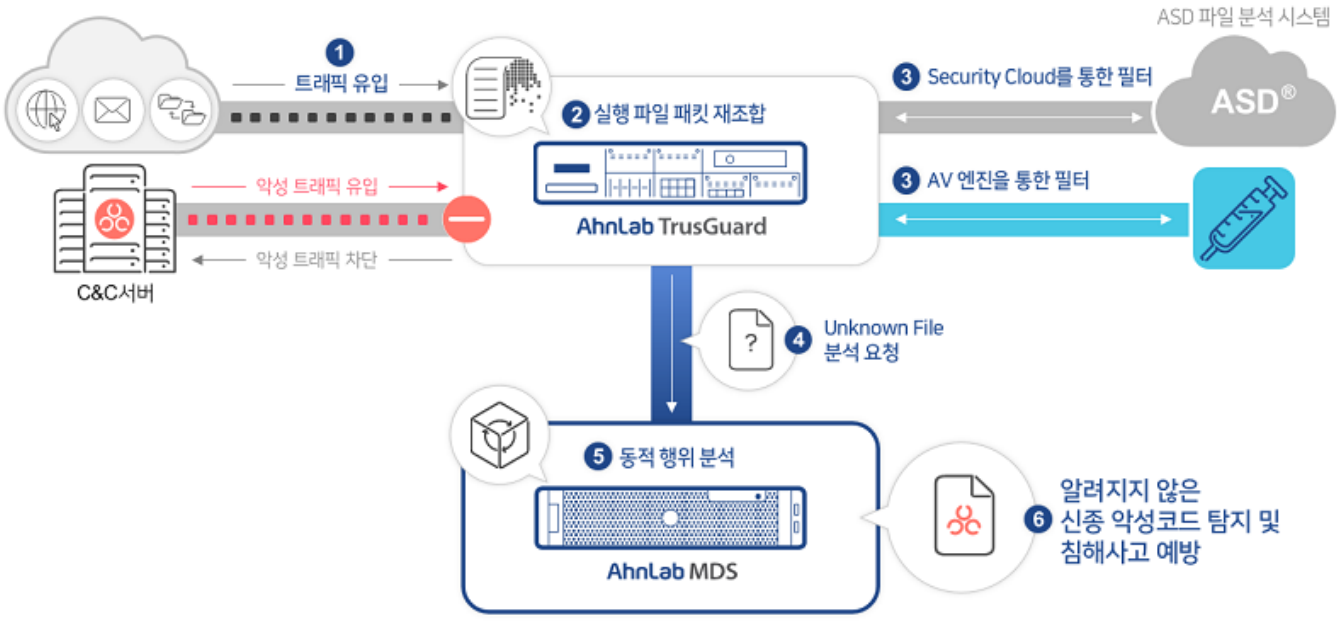
2. ESA + VPN 연계를 통한 보안 점수 기준 VPN 접속



[그림 2] ESA + VPN 연계 구조

조직에서 재택 근무용 단말 등 원격 단말 보안 강화가 필요한 경우 유용하게 사용할 수 있는 연계 기능으로, ESA 제품의 보안 점검 기능을 활용하여 원격 단말의 보안 점수 상태가 기준치 이하인 경우 사내망으로 접속할 수 있는 VPN 접속 권한을 제한하고 기준치 이상인 경우에만 접속할 수 있도록 제어한다. 재택 근무자 대다수 단말은 개인용 PC인 경우가 많기 때문에 이에 대한 보안 강화 방안으로 유용하게 활용할 수 있다.

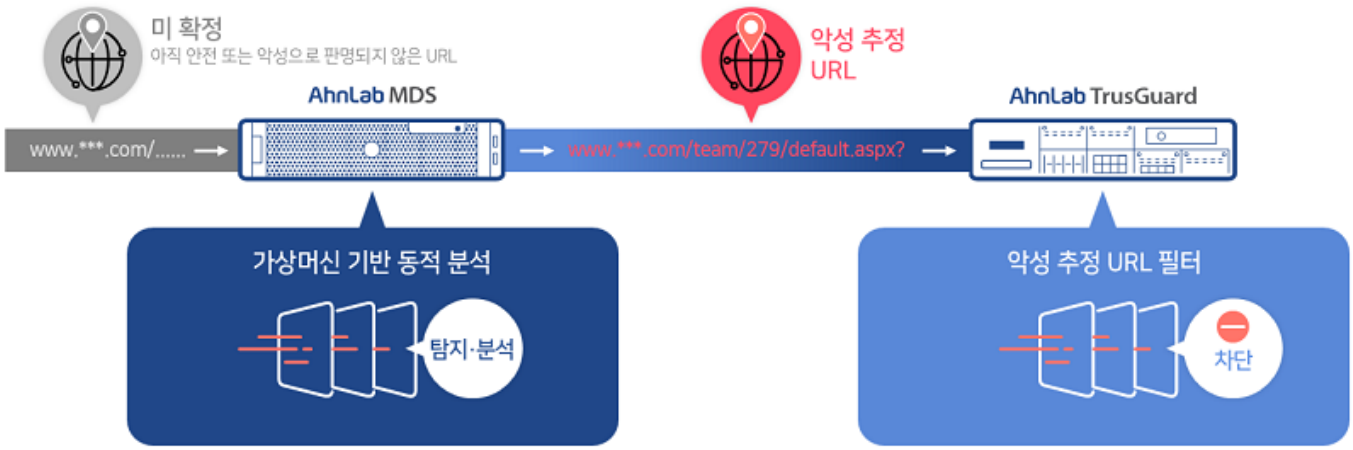
3. TrusGuard + MDS 연계 의심 트래픽 동적 분석



[그림 3] TrusGuard+MDS 연계 의심 트래픽 동적 분석

TrusGuard 장비를 통해 유입되는 트래픽 중 실행파일의 경우, MDS와 연동을 통해 유입된 실행파일 패킷을 재조합하여 MDS를 통한 동적 분석을 요청하고, 해당 분석 결과에 따라 대응을 수행할 수 있는 기능을 제공한다. 1차 필터링 기능으로 ASD 엔진을 통해 알려진 악성코드에 대해서는 분석을 수행하지 않으며, 알려지지 않은 악성코드가 유입된 경우에만 분석을 수행하고 해당 결과를 확인할 수 있다. 네트워크 구간이 다수인 환경에서 MDS를 미러링(Mirroring)으로 구성하지 않고 단독으로 사용하는 경우 유용하게 활용될 수 있다.

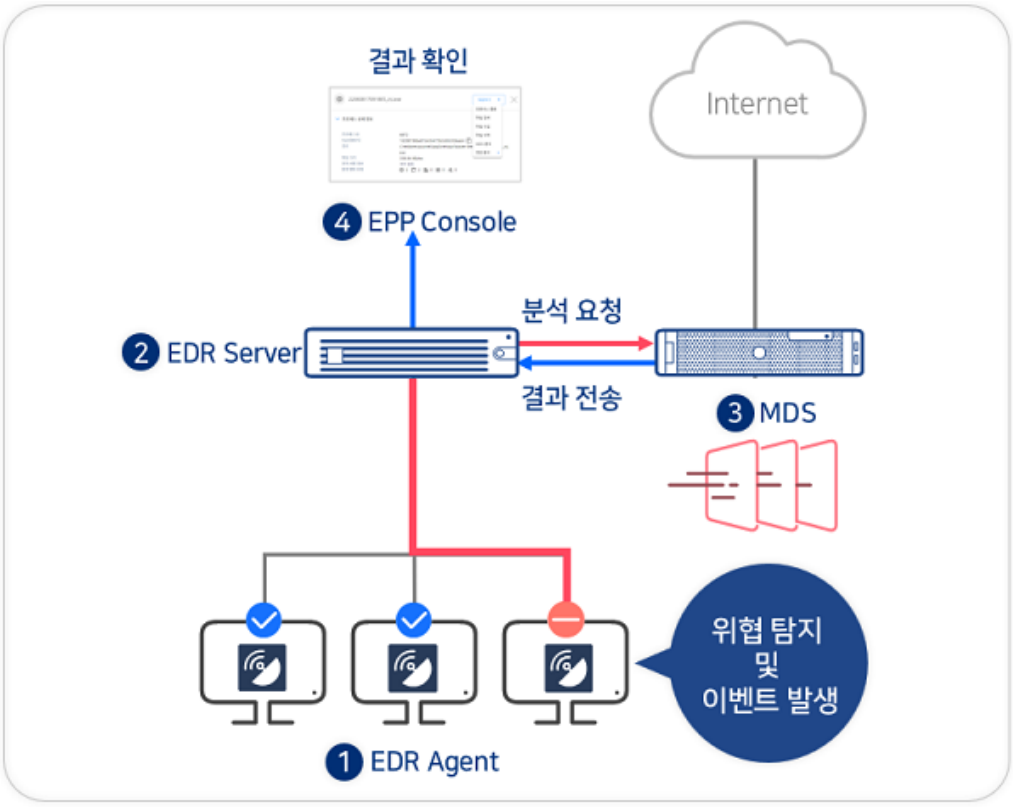
4. TrusGuard + MDS 연계 악성 URL 차단



[그림 4] TrusGuard + MDS 연계 악성 URL 차단

3번 사례와 같이 장비의 조합을 통해 활용할 수 있는 기능으로, MDS에서 탐지한 악성 추정 URL에 대해 TrusGuard 장비와의 연계를 통해 악성 URL을 자동으로 차단한다. TrusGuard에서 공유 받을 수 있는 최대 URL은 1,000개이고, 이후 신규로 확인된 URL에 대해서는 과거 항목 삭제 후 적용이 되는 구조로 되어 있다. TrusGuard를 통해 등록된 URL에 대한 수정 및 개별 선택 삭제도 가능하며, TrusGuard를 통합 관리할 수 있는 TMS 장비를 사용하는 경우에는 MDS로부터 수신한 악성 URL을 TMS를 통해 TrusGuard로 포워딩할 수 있다. 이후, 차단이 필요한 URL 정보를 물리적으로 분산되어 있는 TrusGuard를 통해 블랙리스트 등록도 가능하다.

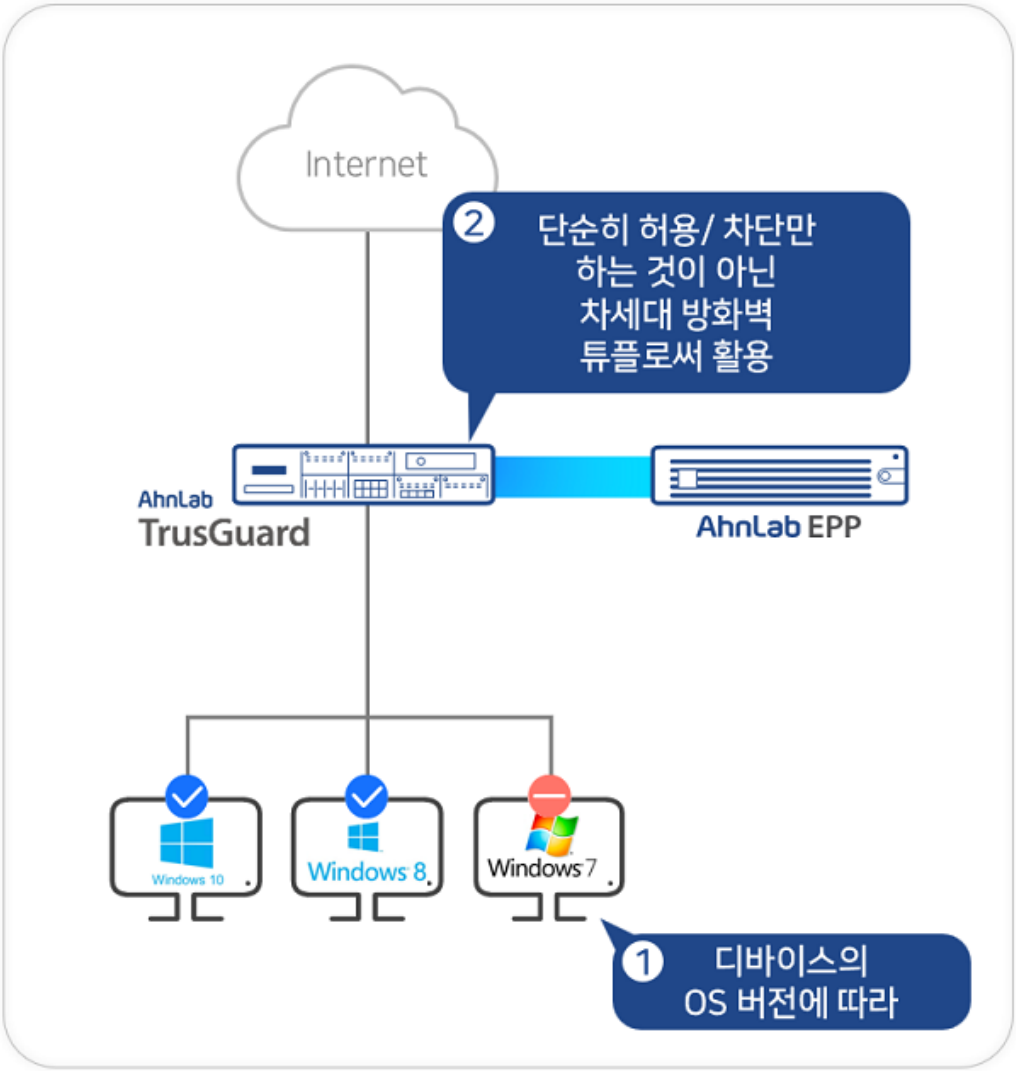
5. EDR + MDS 연계 위협 이벤트 교차 분석



[그림 5] EDR + MDS 연계 위협 이벤트 교차 분석

EDR에서 발생된 위협 이벤트를 MDS 연동을 통해 교차 분석할 수 있는 기능을 제공한다. 해당 기능은 EDR로부터 수신 받은 위협 이벤트 중 정상 및 악성에 대한 판단이 애매한 경우, 실행파일을 MDS를 통해 추가 분석 요청할 수 있으며 분석된 결과값을 관리자 콘솔에서 확인할 수 있다. 위협 가능성이 있는 의심 파일 대상의 추가 분석 진행으로 빠른 의사결정을 내리고자 하는 경우 유용하게 활용할 수 있다.

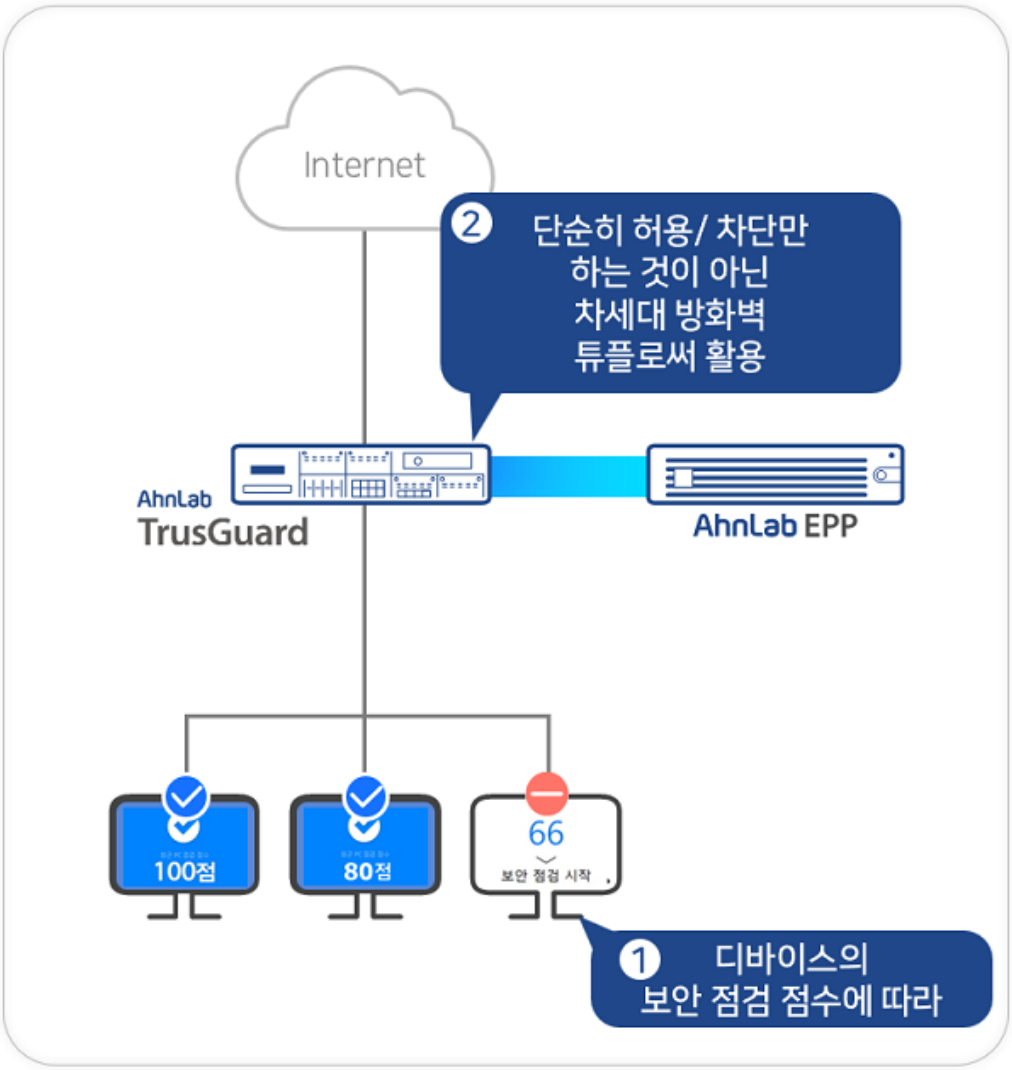
6. EPP + TrusGuard 연계 디바이스 제어 (OS 기준 제어)



[그림 6] EPP + TrusGuard OS 기준 연계 디바이스 제어

차세대 방화벽 특성을 활용할 수 있는 연계 기능으로 단말 OS 버전에 따라 다양한 제어 역량을 제공한다. 예를 들어, 정식 지원이 종료된 Windows 7을 사용하고 있는 단말을 대상으로 내부 네트워크 접근은 허용하되 인터넷 접속을 차단하는 룰셋을 적용할 수 있고, Windows 10 미만 버전을 사용하는 PC는 원격접속 애플리케이션인 RDP, 팀뷰어 등을 차단하거나 카카오톡 메신저의 파일 업/다운로드만 차단하는 등 다양한 보안 정책들을 OS 버전 기준으로 적용할 수 있다.

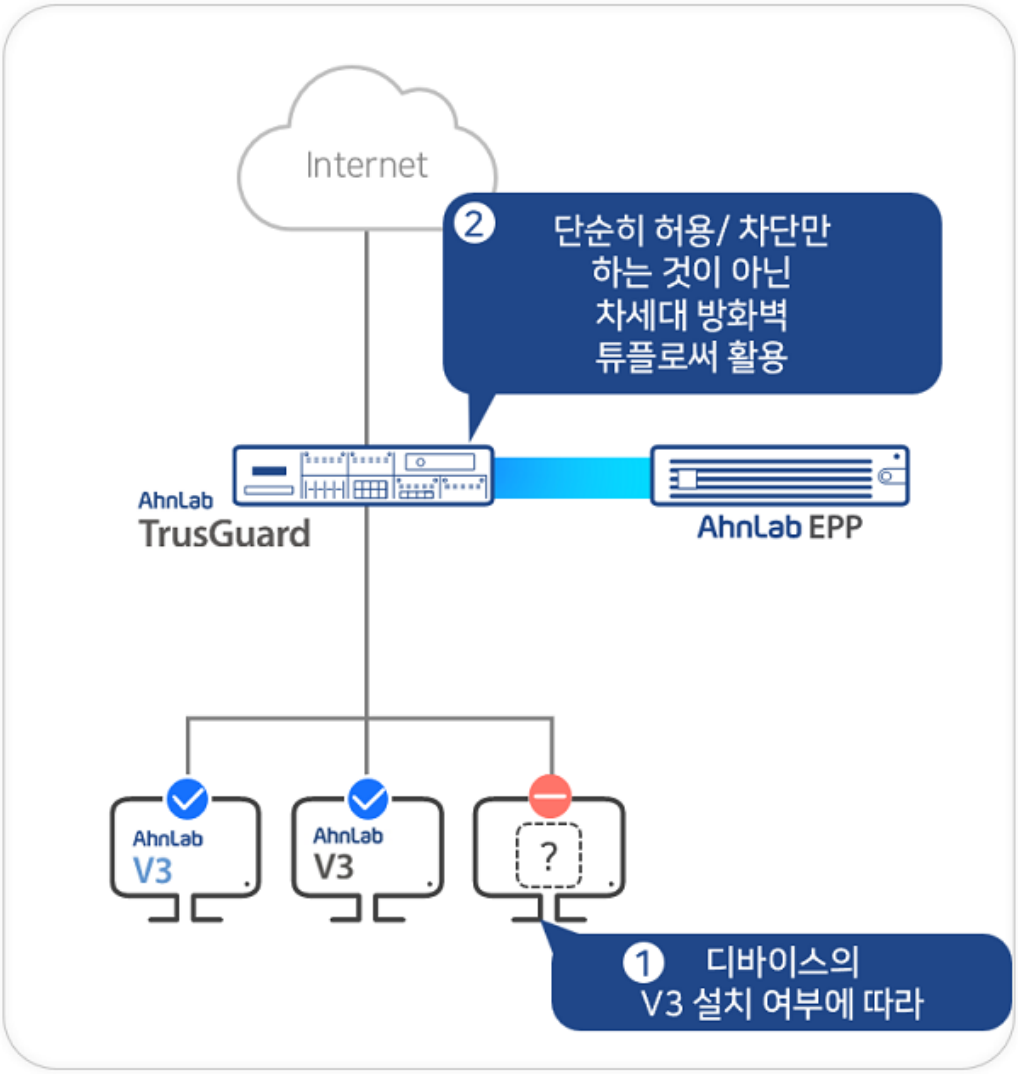
7. EPP(ESA) + TrusGuard 연계 디바이스 제어 (보안점검 점수 기준 제어)



[그림 7] EPP + TrusGuard 보안점검 점수 기준 연계 디바이스 제어

ESA를 활용하는 경우 단말의 보안점검 점수 기준으로도 다양한 제어 기능들을 사용할 수 있다. 예를 들어 보안 점수 80점 이하인 PC는 글로벌 카테고리 기반 URL의 보안 위협 카테고리와 미분류 카테고리 접속을 차단하거나, 보안 점수 60점 미만인 PC는 업무 시간 이외에는 사내 시스템 외 모든 네트워크 접근을 차단할 수 있다. 보안 점수 80점 미만인 PC는 주요 퍼블릭 클라우드(AWS, Azure, GCP) 접근을 차단하는 등의 기능을 활용할 수 있다.

8. EPP + TrusGuard 연계 디바이스 제어 (V3 설치 기준 제어)



[그림 8] EPP + TrusGuard V3 설치 기준 연계 디바이스 제어

마지막으로 디바이스 제어는 V3 설치 기준으로도 활용이 가능하다. 예를 들어 V3 미설치 PC는 특정 사이트만 접근할 수 있도록 허용한다 거나, V3가 설치된 PC만 특정 업무시간에 사내 시스템 접근을 허용하는 등의 조직 보안 정책 강화를 위한 다양한 제어 기능들을 활용할 수 있다.

결론

이번 글에서는 안랩이 제공하고 있는 제품간 연계 기능을 8가지 사례로 나눠 소개했다. 해당 기능들을 조직의 인프라 환경 및 특성에 맞게 적절히 활용한다면, 조직의 보안관리 역량과 제품간 연계 기반 모니터링을 강화하여 보안 가시성 향상과 같은 효과도 충분히 누릴 수 있을 것이다.

다음 월간안 4월호에서는 지난해 월간안 9월호를 통해 간략하게 소개했던 SOAR Basic을 활용한 위협 시나리오 기반 다양한 연계 기능 및 활용 방안들을 살펴보고자 한다. SOAR Basic 제품은 안랩이 제공하는 모든 제품들을 연계해 워크플로우(workflow) 자동화를 구현할 수 있는 솔루션이다. 이에 대한 구체적인 내용은 다음화에서 살펴보도록 하자.

AhnLab 솔루션컨설팅팀 함경호 차장