새롭게 변신한 보안 솔루션, 빨라지는 혁신

안랩은 최근 자사 엔드포인트, OT 및 클라우드 보안 영역에서 신제품 및 신규 버전 업데이트를 선보였다. 먼저, OT 엔드포인트 보안 솔루션 AhnLab EPS를 기존 2.8에서 3.0 버전으로 업그레이드했다. 또한, 엔드포인트 영역에서 매체 제어 솔루션 AhnLab EDC(EPP Device Control)을 출시해 AhnLab EPP 라인업에 추가했다. 클라우드 워크로드 보안 플랫폼 AhnLab CPP에는 Container Security 라인업이 추가됐다.

제품 업데이트와 신규 출시를 통해 올 하반기부터 안랩이 고객들에게 어떤 보안 효과를 가져다줄지 자세히 살펴보자.

AhnLab EPS 3.0: IT/OT 환경에 최적화된 유연하고 안정적인 운영

AhnLab EPS는 OT 시스템 보안에 최적화된 OT 엔드포인트 보안 솔루션으로, IT와 OT를 아우르는 통합 CPS(Cyber-Physical System) 보안에서 중요한 역할을 담당한다. 올해 선보인 3.0 버전을 통해 기능, 성능 및 사양이 대폭 개선됐다. 이를 통해 AhnLab EPS는 국내외 고객들에게 한 층 강화된 OT 엔드포인트 보안 역량을 제공할 수 있을 것으로 기대된다.

먼저, AhnLab EPS 3.0의 변경 사항을 간단히 살펴보자.

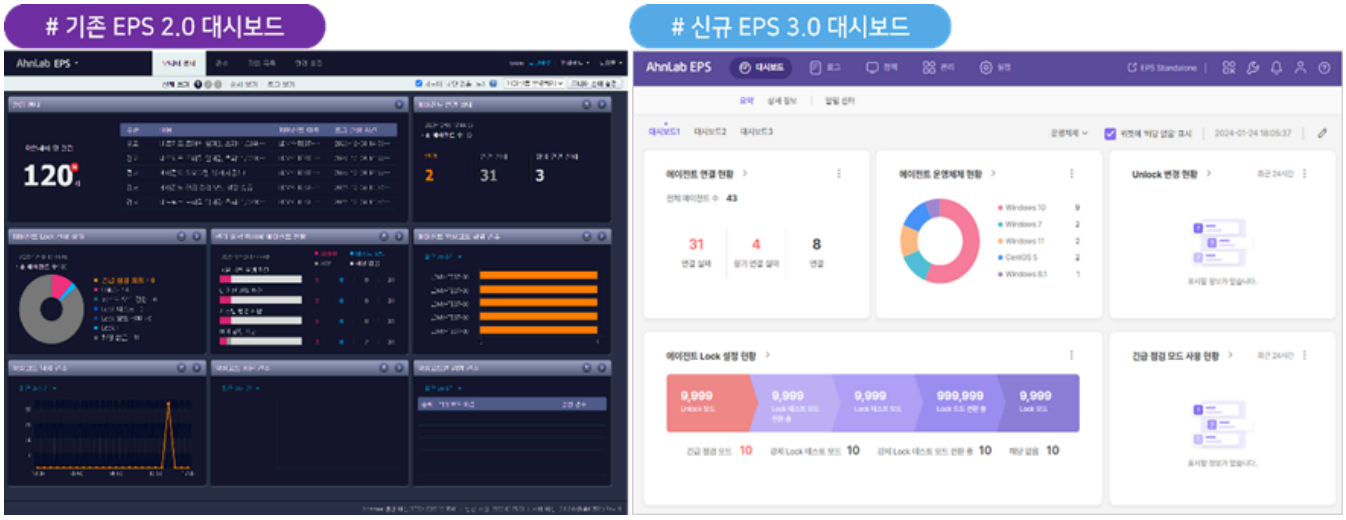
AhnLab EPS는 중앙 모니터링 및 정책 관리 서버(EPS Server)와 윈도우 및 리눅스 단말에 설치되는 에이전트(EPS Client)로 제공된다. 먼저 EPS Server의 성능을 향상시켜 기존 에이전트 최대 지원 수량인 8,000대에서 20,000대까지 지원하도록 향상하였다. 또한, AhnLab EPS 3.0에서는 VMware,

AWS 등 가상 환경에서도 운영이 가능하다. 브라우저 콘솔의 경우 구글 크롬(Google Chrome)과 마이크로소프트 엣지(Microsoft Edge)를 지원한다. AhnLab EPS 2.8이 지원하던 인터넷 익스플로러 8.0(Internet Explorer 8.0)는 파일 다운로드만 가능하며, 콘솔은 사용이 불가하다. 더 나아가, AhnLab EPS 3.0은 클라이언트 OS 지원을 확대해 윈도우 11 23 H2를 추가적으로 지원한다. 또한, 글로벌 시장 확대를 위해 언어 지원도 기존 국문, 영문, 중문에서 일문까지 확대됐다.

AhnLab EPS 3.0의 주요 변경 사항을 정리하면 다음과 같다.

1) UI/UX 전면 개편

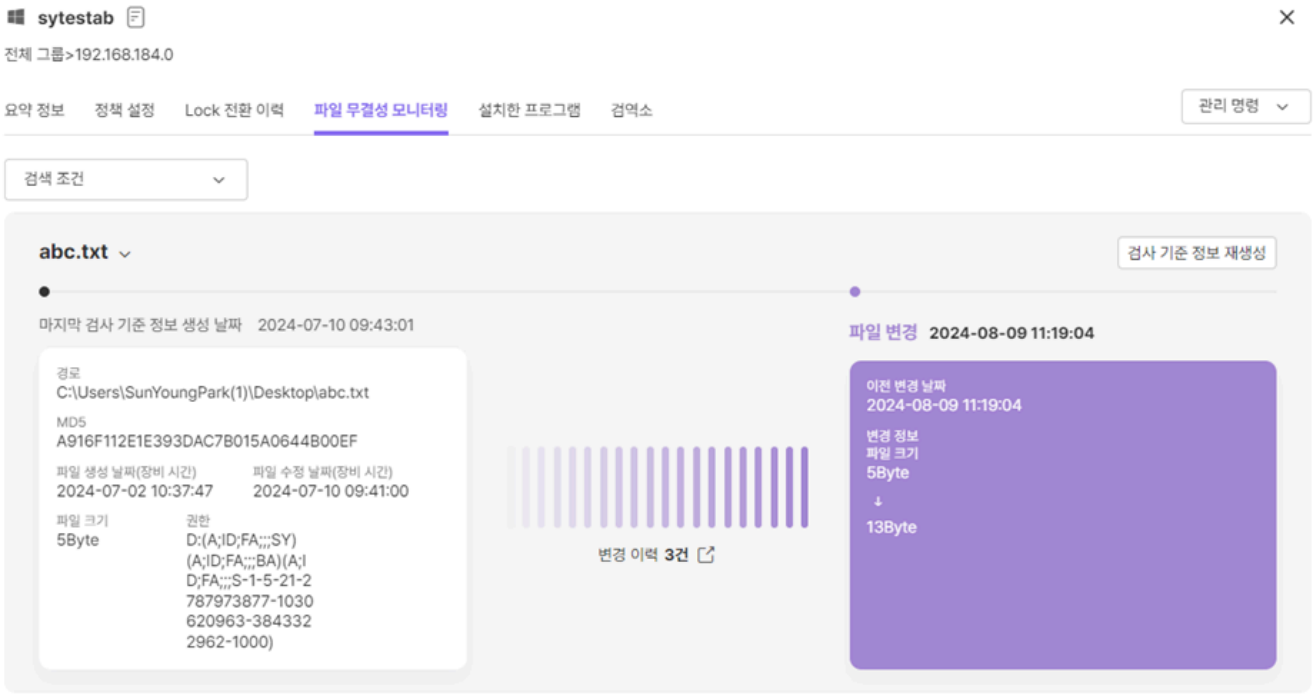
안랩은 AhnLab EPS 1.0부터 10년 넘게 유지해온 웹 프레임워크와 UI 스타일을 전면 개편했다. 최신 트렌드에 맞게 디자인을 획기적으로 개선했으며, 또한 UX 개선을 통해서 보다 편리한 제품 사용과 사용자 경험(User Experience)를 제공할 수 있게 되었다. 이를 통해서 고객은 보다 직관적인 제품 사용과 모니터링을 경험할 것으로 기대된다.



[그림 1] EPS 2.0 대시보드와 EPS 3.0 대시보드 비교

2) 주요 파일 무결성 감시 및 차단

AhnLab EPS 3.0은 EPS 설비 환경에서 시스템 운영에 필요한 중요 파일의 변경 여부를 모니터링하고, 필요 시 변경을 차단한다. 파일 baseline 생성을 위한 무결성 검사 정책 관리 및 에이전트 연동 기능을 추가하고, '모니터링' 상태로 설정한 파일의 baseline 및 변경 이력은 '파일 무결성 모니터링' 탭에서, '차단' 상태로 설정한 파일은 에이전트 로그에서 차단 이력을 확인할 수 있다.



[그림 2] AhnLab EPS 3.0 – 파일 무결성 모니터링

3) 에이전트 OS 패치 목록 수집 및 관리 현황 제공

AhnLab EPS 3.0은 에이전트를 통해서 디바이스의 OS 상세 정보를 수집하여 이에 대한 가시성을 제공한다. 사용자는 운영중인 디바이스들의 OS 상세 정보를 참고할 수 있으며, 이를 통해서 취약점 패치 및 대응을 위한 정보로 활용할 수 있다.

4) Relay Client 운영 환경의 독립망 클라이언트 미설치 시스템 검색

AhnLab EPS 3.0은 Relay Client가 운영되는 독립망에서 에이전트가 설치되지 않은 시스템을 검색하고 조회할 수 있는 기능을 제공한다. 이를 통해서 사용자는 에이전트가 설치되지 않은 시스템을 Active Scan 방식으로 검색하여 확인할 수 있고, 이를 통해서 보다 효율적으로 운영할 수 있도록 제공한다.

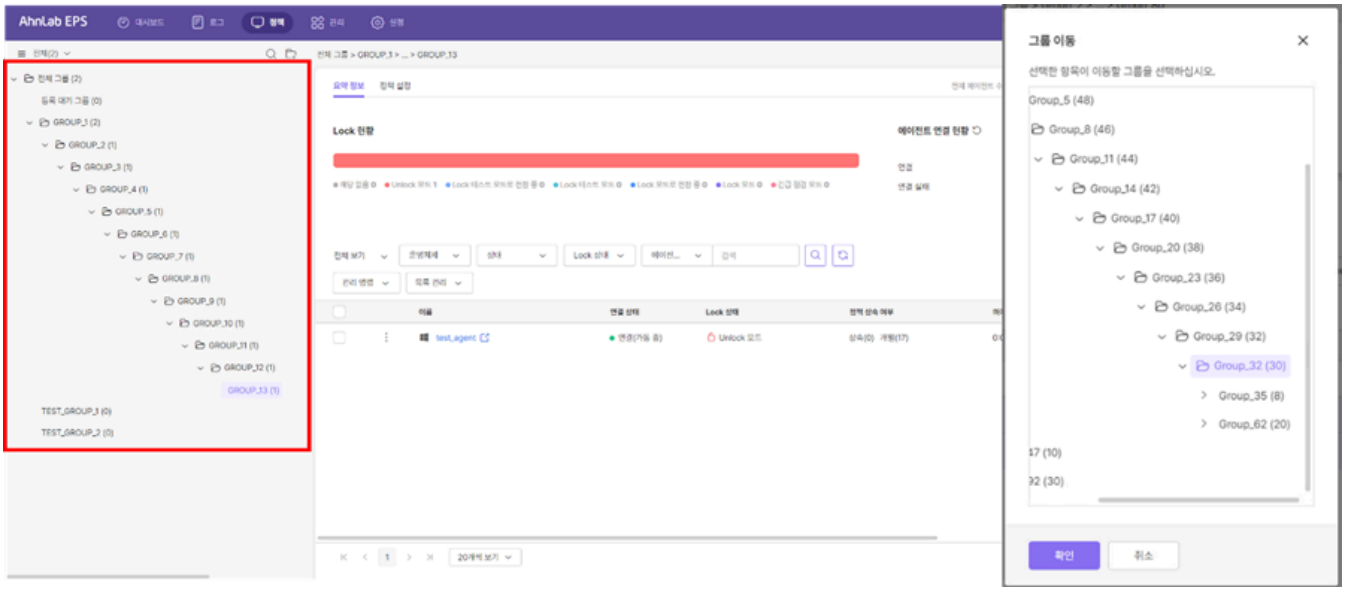
5) 긴급 점검 모드의 긴급 매체 허용 개선

AhnLab EPS 3.0은 에이전트 환경 설정에서 '긴급 매체 실행 허용' 설정 시 긴급 점검 모드에서 매체 실행을 허용한다. 그룹/에이전트 정책 설정을 통해서 '긴급 매체 실행 비밀번호'를 설정할 수도 있으며, 긴급 점검 모드 최대 유지시간도 기존 24시간에서 72시간으로 연장 가능하도록 개선되었다.

6) 그룹 관리 기능 개선

AhnLab EPS 3.0은 다수의 계층 구조와 그룹관리를 사용하는 고객의 환경을 지원하기 위해서 에이전트 그룹관리의 지원 단계를 기존 5단계에서 10단계 이상 생성할 수 있도록 개선하였다. 이를 통

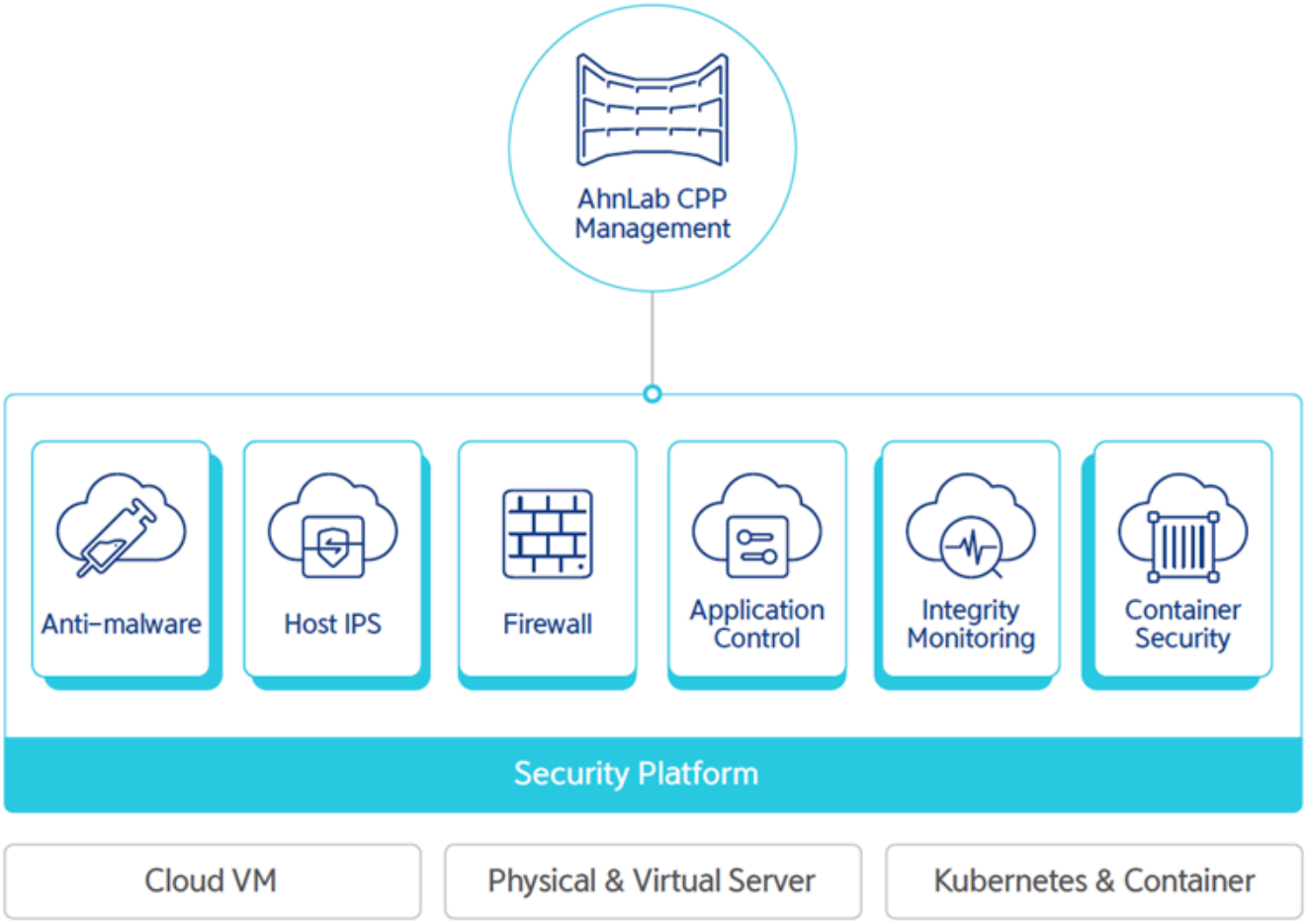
해, 고객의 다양한 환경 구성에 제약없이 관리 기능을 지원할 수 있게 되었다.



[그림 3] AhnLab EPS 3.0 - 웹 콘솔 그룹관리 depth

Container Security: 쿠버네티스 연동을 통한 기업의 컨테이너 환경 보안 강화

안랩은 지난 7월, AhnLab CPP에 컨테이너 보안 모듈인 'Container Security'를 추가했다. 이를 통해, 기존 Anti-malware, Host IPS, Application Control 모듈에 컨테이너 보안 역량까지 더하게 됐다.



[그림 4] AhnLab CPP 구성 및 연계 범위

Container Security는 쿠버네티스(Kubernetes) 환경에서 실행 중인 컨테이너를 식별해 토폴로지 뷰(Topology View)를 제공하며, 식별된 컨테이너 이미지의 악성코드 및 취약점 검사를 수행한다. 이를 통해 기업이 컨테이너 환경에 대한 보안을 강화하는 것은 물론, 잠재적인 위협까지 신속하게 식별해 대응할 수 있도록 지원한다. Container Security는 CPP Management 버전 업그레이드와 Container Security 라이선스 입력 및 인증 후 바로 사용할 수 있다.

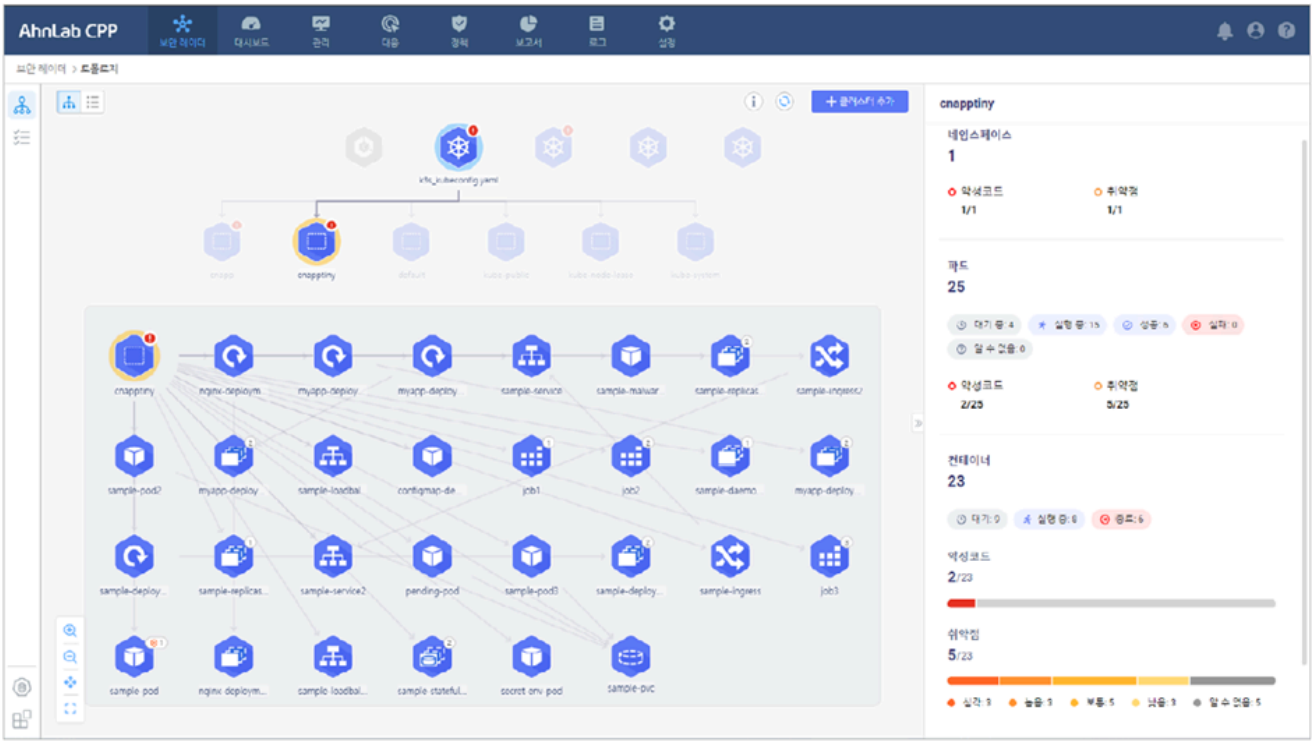
AhnLab Container Security의 특장점은 다음과 같이 크게 세 가지로 정리할 수 있다.

1) 간편한 쿠버네티스 클러스터 및 컨테이너 레지스트리 연동

Container Security는 Kuberconfig 및 계정 연동 방식을 통해 쿠버네티스 클러스터를 연동하고, Harbor, Nexus, Docker Hub, Amazon ECR 등 다양한 컨테이너 레지스트리 연동이 가능하다.

2) 쿠버네티스 토폴로지 가시화

AhnLab CPP의 Container Security는 클러스터, 네임스페이스, 피드 정보를 토폴로지로 시각화해 보안 담당자가 리소스 구성 및 보안 상태를 한 눈에 확인할 수 있도록 한다



[그림 5] AhnLab Container Security - 컨테이너 식별 및 자산 토폴로지 가시화 제공

3) 동작 중인 컨테이너 식별 및 검사

Container Security는 쿠버네티스 배포에 사용하는 컨테이너 이미지 레지스트리를 연동해 쿠버네티스 환경에서 실행 중인 컨테이너 정보를 식별하고, 해당 컨테이너 이미지에 대해 악성코드 및 취약점 검사를 실시한다.

검사가 완료되면, 토폴로지에 검사 결과와 함께, 취약한 이미지가 배포된 현황을 쿠버네티스의 클러스터와 파드, 컨테이너를 기준으로 확인할 수 있는 다이어그램과 목록 조회 기능을 제공한다. 만약 연동된 컨테이너 이미지 레지스트리에 이미지가 존재하지 않는 경우, 상태 정보와 연동을 바로 설정할 수 있는 기능을 제공한다.

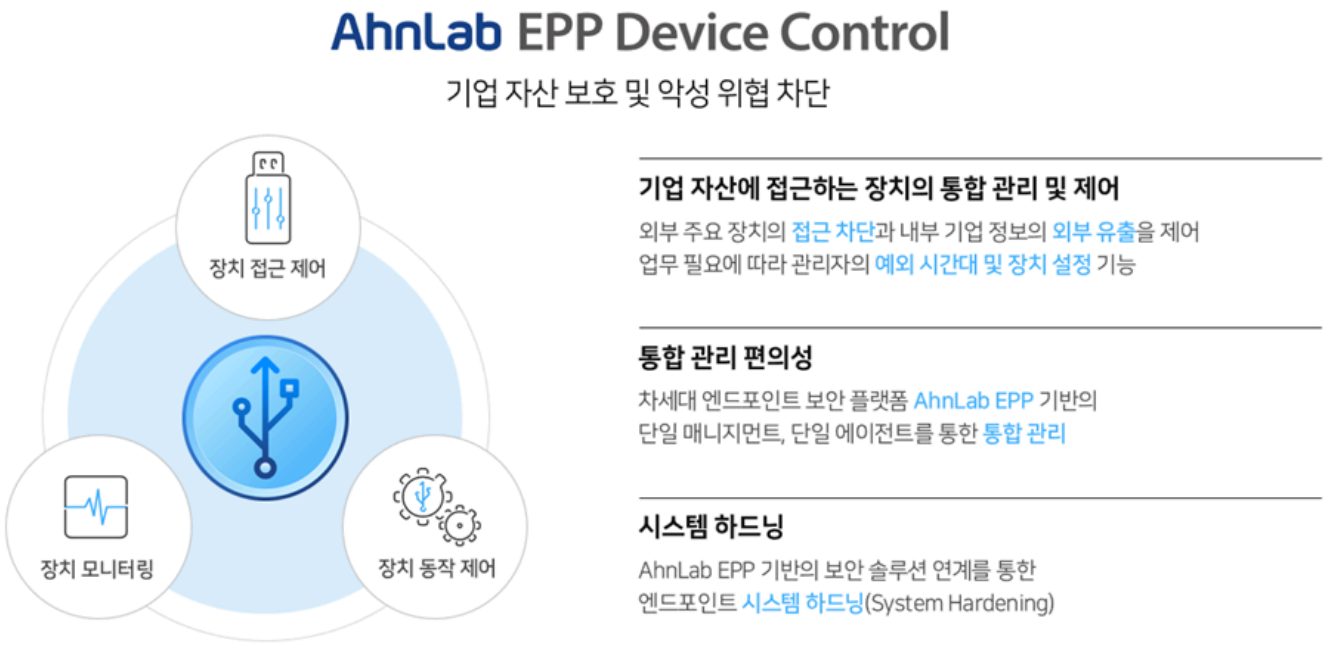
AhnLab EDC: 장치 제어 및 통합 관리로 안전한 비즈니스 환경 구축

안랩의 차세대 엔드포인트 보안 플랫폼 AhnLab EPP의 플러그인으로 출시된 AhnLab EDC(EPP Device Control)는 차세대 엔드포인트 보안 플랫폼 기반 장치 접근 및 동작 제어 솔루션이다. 기업 내부 인프라에 대한 USB, CD드라이브, 휴대용 장치 등 외장 매체의 접근과 동작을 제어하고 통합 관리함으로써 한층 더 강화된 위협 대응을 구현한다.

[그림 6] AhnLab EPP 구성 모듈

안랩이 AhnLab EDC를 신규 출시한 것은 외장 장치의 기업 자산에 대한 악의적인 접근을 제어하고, 이를 통해 대내외 보안 리스크를 사전에 예방하고 신속하게 대응하기 위함이다. 기업의 주요 데이터는 대부분 관리자가 가시성을 확보하기 어려운 엔드포인트 단말과 외장 장치에 저장돼 있으며, 최근 들어 감염된 USB를 통해 기업 기밀 데이터를 탈취하는 공격 건수가 과거에 비해 급증했다.

따라서 데이터 유출에 악용되는 외부 저장 매체에 대한 통제 방안을 마련하고, 사고 발생 시 리스크를 최소화하기 위한 가시성 확보의 필요성이 대두됐다. 또한, 개인정보보호법, 정보통신망법, ISMS 인증 기준 등 주요 정보 보호 관련 컴플라이언스에서도 보조 저장 매체에 대한 제어 및 통제 권한을 요구하고 있는 실정이다. AhnLab EDC는 이들 요건을 모두 충족하도록 설계됐다.



[그림 7] AhnLab EDC 개념도

AhnLab EDC는 기업 인프라 및 자산에 대한 주요 업무용 외장 매체 접근 및 연결 이후 동작 제어 기능 외에도, 고객사 환경에 따라 유연하게 확장 및 구성 가능한 차단 예외 장치 등록, 장치 제어 금지 시간대 설정 등 손쉬운 관리 옵션도 제공한다. 또한, 장치 제어 현황 모니터링 및 통계, 보고서 제공 등의 다양한 기능도 제공한다.

또한, AhnLab EDC는 AhnLab EPP를 기반으로 운영되기 때문에 라이선스 적용 만으로 간편하게 구축할 수 있으며, 백신, 개인정보, 패치 관리, 취약 시스템 점검, 엔드포인트 위협 탐지 및 대응(EDR) 등 AhnLab EPP의 다른 플러그인 보안 솔루션과의 효율적인 통합 관리가 가능하다.

이로써 보안 관리자는 조직 내 외장 매체 사용에 대한 가시성을 확보하고, 외장 매체로 인한 악성 코드 감염, 정보 유출 등 각종 보안 위협으로부터 생산설비 서버와 서비스 시스템 등 조직의 주요 자산을 안전하게 보호할 수 있다. 더 나아가, AhnLab EDC는 안랩의 전문 인력을 활용한 지속적인 전문 지원 서비스로 안정적인 운영과 관리가 가능하다.

AhnLab EPS, CPP, EDC에 대한 보다 자세한 정보는 안랩 홈페이지에서 확인할 수 있다.

►**AhnLab EPS 제품정보페이지 바로가기**

►**AhnLab CPP 제품정보페이지 바로가기**

►**AhnLab EDC 제품정보페이지 바로가기**

AhnLab

콘텐츠기획팀 서보경 사원