[내부정보유출방지솔루션 특집]코소시스코리아 - 대한민국 IT포털의 중심! 이티뉴스

코소시스코리아(대표 강영호)는 자료유출방지 솔루션인 '엔드포인트 프로텍터 V4.0'을 주력으로 공급하고 있다.

엔드포인트 프로텍트 V4.0은 지난달 2일 국내용 호스트 자료유출방지 제품 국제공통평가기준(CC) 인증을 받았다. 이 제품은 매체제어, 이지락2 소프트웨어(SW) 보안USB를 포함한다.

매체제어 솔루션은 PC에 설치되는 에이전트가 필요하고 설치되면 USB 포트와 같은 특정한 포트를 '사용금지·사용허가·읽기전용' 등으로 설정해 정책적으로 통제한다. 개선된 매체제어 솔루션은 USB 포트에 항상 '사용금지' 상태를 유지하고 허락한 특정 USB 장치만 '사용허가' 혹은 '읽기전용'으로 허용해 더 정교해졌다.

보안USB 솔루션은 PC 혹은 USB에 설치되는 에이전트가 필요하다. 설치되면 USB 포트를 통제해 보안USB 사용 정책을 구현하고 USB로 이동되는 자료의 암호화를 실시한다.

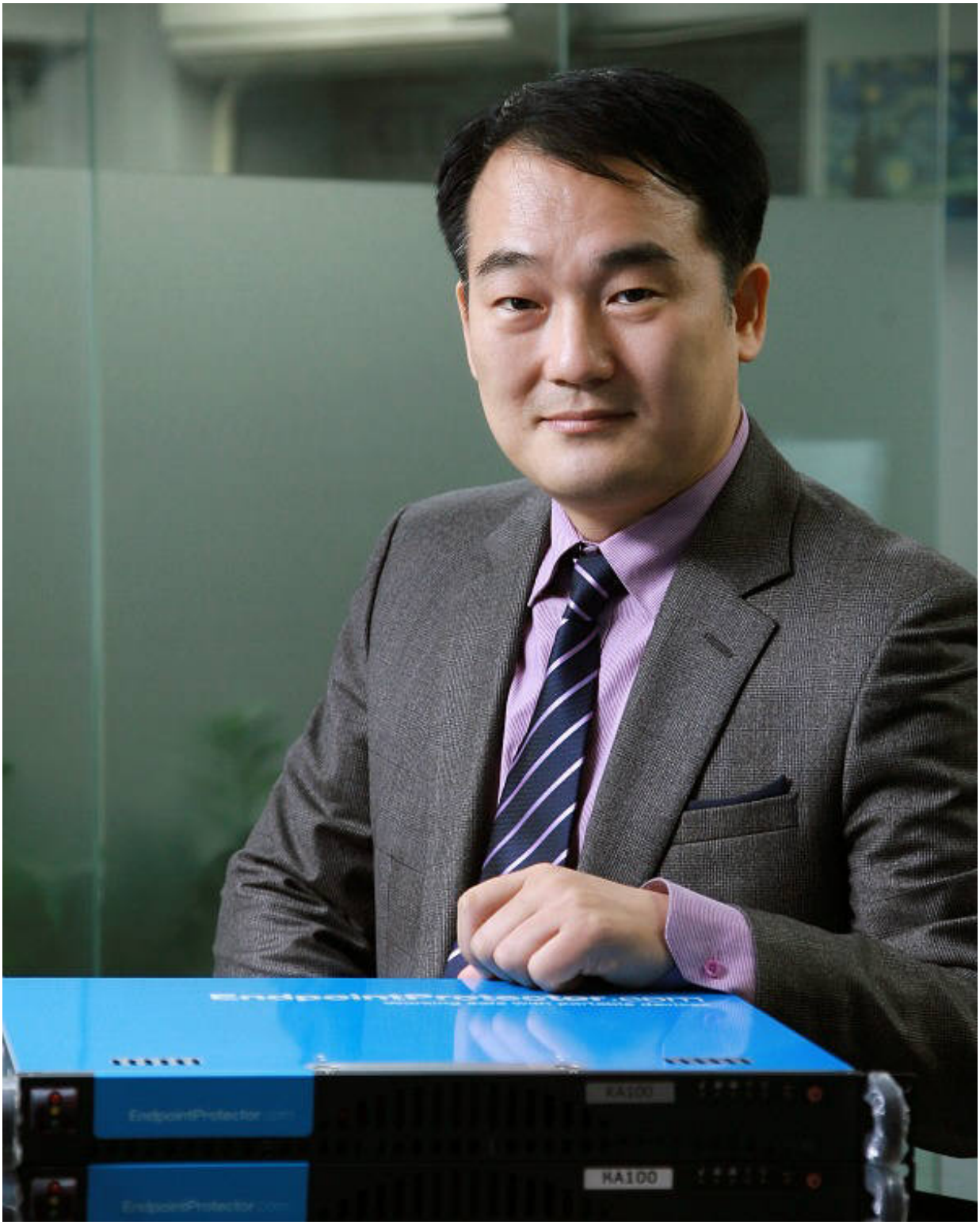
두 보안 솔루션은 모두가 PC에 설치되는 에이전트를 필요로 한다. 설치되면 이 에이전트들은 공통적으로 PC의 USB 포트를 '사용가능, 사용금지' 한다. 따라서 충돌이 불가피하며 두 보안 제품이 사용하는 정책구현 및 감사를 위한 콘솔이 달라 충돌 위험은 증가한다.

충돌을 피하고 보안정책의 통합운용으로 일관성을 확보하려면 두 제품의 통합은 당연하다. 추가로 윈도 PC만을 위주로 구축되던 자료유출방지 체계가 윈도 서버와 애플의 맥까지 통합, 구축할 수 있어야 한다.

통합된 매체제어 및 보안USB 제품은 PC에 설치되는 에이전트 수를 줄이고 통합된 정책설정 및 감시용 콘솔을 운용해 일관성이 있는 매체제어를 구현할 수 있다. 보안USB는 매체제어 정책에 통합되고 유연하게 운용된다.

조직 네트워크 내부에서 사용되는 휴대형 장치 및 USB 저장장치 등을 완벽하게 통제할 수 있다 해도 네트워크 내부에는 여전히 많은 정보유출 경로가 존재한다. 이런 부분은 주로 DLP(Data Loss Prevention) 솔루션으로 자료 유출을 예방하게 되는데 DLP 제품은 USB와 같은 휴대형 저장매체를 통제하는 기능을 포함한다.

DLP 솔루션은 크게 네트워크 DLP 제품과 호스트 DLP 방식으로 구분된다. 최근 통합운용과 매체제어, DLP 솔루션 통합이 강조됨에 따라 호스트 DLP 방식 특히 전문적인 매체제어 기능이 있는 호스트 자료유출방지 체계가 주목 받는다.



인터뷰/강영호 코소시스코리아 대표

“요즘 자료유출 방지 보안제품은 모두 비슷해 제품 간 충돌이 발생하고 있습니다. 이런 충돌을 피하는 것이 최고정보보안책임자(CISO)의 고민이라고 합니다.” 강영호 코소시스코리아 대표의 말이다. 이런 이유로 금융권을 비롯한 많은 기업의 CISO는 잠을 못 이룰 정도다.

강 대표는 기업 자료유출방지 체계의 변화도 요구한다. PC 중심으로 개인정보를 검색하고 암호화하는 정도의 기능으로 자료유출방지를 체계를 구축했다면 이제는 다양한 경로로 개인정보 및 중요 정보 유출을 감지하고 차단할 수 있는 통합된 자료유출방지 체계로 전환해야 한다는 것이다. 강 대표는 “강력한 스마트폰과 롱텀에벌루션(LTE) 데이터 통신이 일상화된 요즘은 손쉽게 정보유출이 가능한 스마트기기를 관리하는 매체제어 정책이 중요하다”고 강조했다.

강 대표는 “다른 글로벌 DLP 벤더와 다르게 100% 국내에서 제품을 생산, 공급한다”며 “지원 서비스를 제공, 완전

한 한국 보안솔루션 업체로 자리 잡았다”고 말했다.

신혜권기자 | hkshin@etnews.com 기자의 다른 기사 보기