Case Study

AhnLab

공공기관 단말 보안은 점수 기반 관리로 해결

업종
공공기관

규모
직원 수
약 1,700~2,000명

도입제품
AhnLab ESA

D기관은 내부 단말을 통한 침해 위협에 대응하기 위해 백신, 보안 패치, 계정 정책 등 기본 보안 수칙을 적용해 왔다. 정상 도구를 악용한 공격과 내부 확산 위협이 증가하면서, 단말 보안 관리의 중요성이 더욱 강조되고 있었다. 그러나 단말별 설정 환경의 차이로 인해 일부 단말에서는 보안 설정이 미흡하거나 취약점이 존재할 가능성이 있었다. 특히 백신 비활성화, 패치 미적용, 공유 폴더 설정 등은 공격 확산의 주요 원인으로 작용했다. 이에 D기관은 AhnLab ESA를 도입해 단말 보안 상태를 점검 항목과 점수 기반으로 관리하고, 정책에 따른 조치 체계를 적용했다. 그 결과, 전체 단말의 보안 상태를 직관적으로 파악하고, 취약한 단말에 대한 체계적인 관리와 보안 수준 향상을 동시에 달성했다.

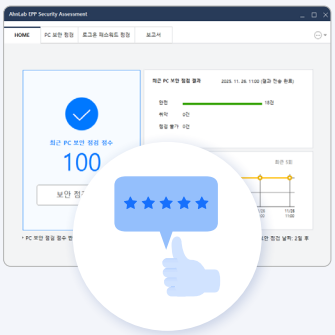
점검 리스트·점수 기반 관리로 직관적인 보안 상태 파악

AhnLab ESA는 백신 설치 여부, 엔진 업데이트, 보안 패치 적용, 비밀번호 정책, 화면 보호기 설정 등 약 70여 개의 점검 항목을 기반으로 단말 보안 상태를 평가한다. 이 중 핵심 10개 항목을 우선 점검 항목으로 구성해, 조직이 반드시 준수해야 할 최소 보안 기준을 명확하게 제시한다. 따라서 보안 담당자는 전체 단말의 보안 수준을 일관된 기준으로 관리할 수 있으며, 사용자 또한 자신의 단말 상태를 직관적으로 파악할 수 있다. 각 단말의 보안 상태는 100점 만점 기준으로 점수화해 제공된다. 이 같은 점수 기반 관리 방식은 단순한 설정 점검을 넘어, 조직 전체의 보안 수준을 정량적으로 평가하는 기반이 된다. 보안 담당자는 점수를 기준으로 취약한 단말을 신속하게 식별하고 우선순위를 설정할 수 있으며, 사용자 또한 자신의 보안 수준을 명확히 이해해 필요한 조치를 인지하게 된다.

핵심 보안 요소의 지속적 유지 강제

최근 공격자들은 새로운 악성코드를 개발하기보다는 LoL Bins와 같은 공격 기법과 이미 효과성이 확인된 기존 샘플을 혼합해 활용하며 백신 무력화나 취약점 악용을 시도하는 경향을 보이고 있다. 이런 상황에서 백신 설치 여부 및 엔진의 최신 업데이트 유지, 그리고 OS 및 소프트웨어 패치 적용은 여전히 가장 기본적이면서도 중요한 방어 수단이다.

Results



전체 단말 보안 점수
100점 달성(평균 99.9점)

70여 개 점검 항목 기반
보안 수준 관리

전사 단말 보안 가시성 확보

AhnLab ESA는 이들 핵심 보안 요소를 지속적으로 점검하고 관리함으로써, 단말 보안의 기본 태세를 유지하도록 지원한다. 특히 패치 누락이나 백신 비활성화와 같은 주요 취약 요소를 빠르게 식별하고 대응할 수 있다.

중앙 집중 관리로 사용자 설정 기반 보안 공백 해소

비밀번호 정책, 화면 보호기, 공유 폴더 설정 등은 단말 사용자 설정에 의존하는 경우가 많아 일관된 관리가 어려운 영역이다. 특히 AD(Active Directory) 등 중앙 관리 체계가 미흡한 환경에서는 보안 설정이 누락될 가능성이 높다.

AhnLab ESA는 이런 항목들을 중앙에서 통합적으로 점검하고 관리할 수 있도록 지원함으로써 사용자 설정에 따른 보안 편차를 줄이고, 조직 전체의 보안 수준을 균일하게 유지한다.

"단말마다 보안 설정 상태를 일일이 확인하기 어려웠는데, ESA 도입 이후에는 점수 기반으로 전체 보안 수준을 한눈에 파악할 수 있게 됐습니다. 기본적인 취약 요소에 대한 자동 점검 및 조치가 가능해져, 단말 보안을 안정적으로 유지할 수 있었습니다."

- D기관 정보보안 담당자

네트워크 차단 등 강제 조치로 보안 준수율 향상

AhnLab ESA는 점검 결과에 따라 다양한 조치 정책을 제공한다. 점검 유도 알림 및 위젯 제공, 네트워크 차단, 취약 항목 강제 조치 등 단계별 대응이 가능하다.

특히 네트워크 차단 기능은 보안 점수가 기준에 미달한 단말의 외부 네트워크 접근을 제한하고, 필요한 업데이트 서버만 허용함으로써 강력한 통제를 지원한다. 이를 통해 관리자의 직접적인 개입 없이도 보안 정책 준수를 유도하고, 조직 전체의 보안 수준을 효과적으로 끌어올렸다.

"네트워크 차단 등 정책 기반의 강제 조치를 적용해도 업무 사이트 접속 등은 예외로 처리해 최소화할 수 있어, 보안성과 운영 안정성 두 마리 토끼를 잡을 수 있게 된 것이 가장 큰 성과입니다."

- D기관 IT 운영 담당자

보안성과 업무 가용성의 균형 확보

일반적으로 보안 강화는 업무 가용성을 저해할 수 있다는 우려가 있다. 그러나 AhnLab ESA는 'ESA 점검 → 점수화 → 단계적 조치' 구조를 바탕으로 조직 상황에 맞는 정책 설정이 가능하도록 설계돼 있다.

D기관은 네트워크 차단 정책을 적극적으로 적용하면서도 업무 사이트 등은 예외로 처리해 영향도를 최소화하는 방식으로 운영하며 보안 수준 향상과 운영 안정성을 동시에 확보했다.

그 결과, 대부분의 단말이 백신, 패치, 계정 정책 등 기본 보안 요건을 안정적으로 유지하게 됐으며, 내부 단말 기반 공격에 대한 대응력도 크게 향상됐다. 실제로 매달 전체 단말에 대해 보안 점수 100점(평균 99.9점 - EPP 제품에서 식별되는 에이전트 기준)을 유지하고 있으며, 직원들의 기본 보안 수칙 준수율 역시 크게 개선됐다.

AhnLab ESA(EPP Security Assessment)는 업무용 PC의 보안 상태를 점검하고, 자동 조치를 통해 엔드포인트 보안 수준을 강화하는 취약 시스템 점검 및 조치 솔루션이다. AhnLab EPP 기반의 통합 관리 환경에서 취약 시스템 조치, 악성코드 대응, 패치 관리, 개인정보 보호까지 폭넓게 지원함으로써 기업의 엔드포인트 하드닝을 효과적으로 구현한다. 또한, 단일 에이전트와 통합 관리 환경을 바탕으로 운영 부담은 줄이고, 보다 빠르고 일관된 보안 대응 체계를 구축할 수 있도록 지원한다.