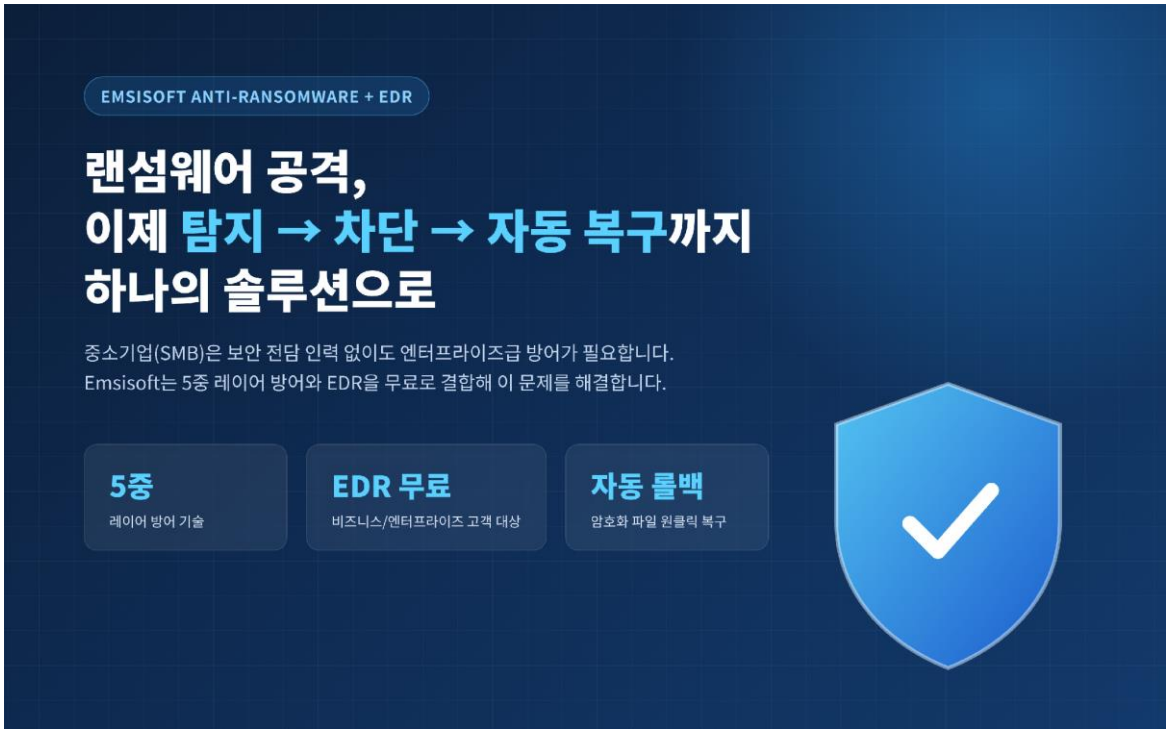
중소기업을 위한 랜섬웨어·EDR 도입 가이드

왜 지금, 중소기업은 Emsisoft 안티랜섬웨어 + EDR 을 선택해야 하는가

타사 EDR·엔드포인트 보안 제품과 비교해, Emsisoft 가 중소기업(SMB) 환경에서 실제로 운영 가능한 이유를 정리했습니다. 이 자료는 SoftMail 이 Emsisoft 공식 파트너로서 국내 도입을 검토하는 기업을 위해 작성했습니다.



SoftMail 은 emsisoft.co.kr 을 운영하며 Emsisoft 제품을 국내에 공급하고 있습니다 · 2026 년 9 월 기준 자료

01. 중소기업이 랜섬웨어 공격에 더 취약한 이유

중소기업은 대기업처럼 24 시간 보안관제(SOC)나 전담 보안 인력을 두기 어렵습니다. 공격자들은 이 점을 알고 있으며, 실제로 방어 체계가 상대적으로 얇은 중소·중견기업을 우선 표적으로 삼는 경우가 많습니다. 문제는 "더 정교한 탐지 엔진"이 아니라 "관리 인력 없이도 안전하게 운영되는 구조"입니다. Emsisoft 는 제품 설계 단계부터 이 문제를 정면으로 다룹니다 — 복잡한 정책 튜닝이나 전담 분석가 없이도, 기본 설정만으로 실질적인 방어력을 제공하도록 만들어졌습니다.

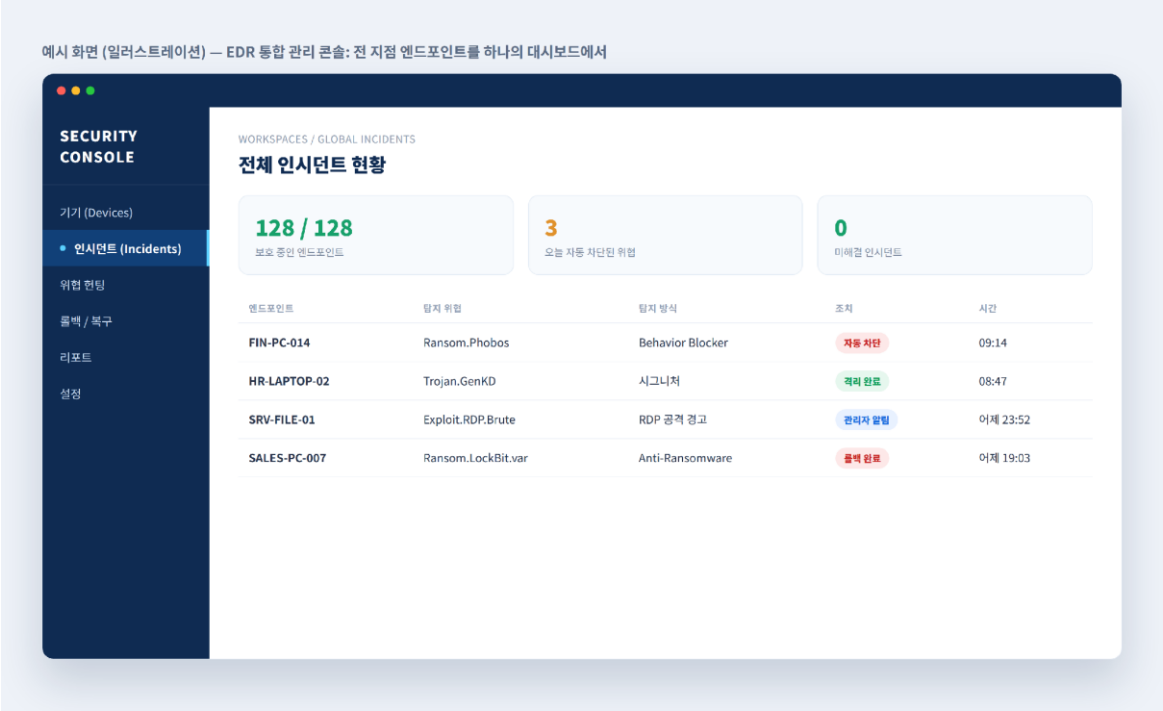
02. Emsisoft 의 5 중 레이어 방어 체계

Emsisoft 는 하나의 탐지 기술에 의존하지 않습니다. 공격 단계별로 서로 다른 5 개의 방어 레이어를 배치해, 하나가 우회되더라도 다음 레이어가 즉시 이어받아 차단합니다. 핵심 철학은 "파일이 암호화되기 전에 멈춘다"는 사전 차단 중심 설계입니다.

Emsisoft 랜섬웨어 방어 5 단계 — 시그니처 → 행동 탐지 → 익스플로잇 차단 → 설정 보호 → RDP 경고

03. 비용 부담 없는 EDR — 중소기업도 엔터프라이즈급 가시성을

EDR(Endpoint Detection and Response)은 엔드포인트 전반의 위협을 실시간으로 파악하고 대응 시간을 줄여주는 기술입니다. 문제는 대부분의 EDR 제품이 별도의 상위 요금제이거나, 운영을 위해 숙련된 보안 분석가를 필요로 한다는 점입니다. Emsisoft 는 이 진입장벽을 낮췄습니다 — Business Security 고객에게는 경량 EDR 을 기본 제공하고, Enterprise Security 고객에게는 데이터 보존과 고급 기능을 포함한 EDR 을 제공합니다. 규모와 예산에 맞춰 필요한 만큼만 확장하면 됩니다.

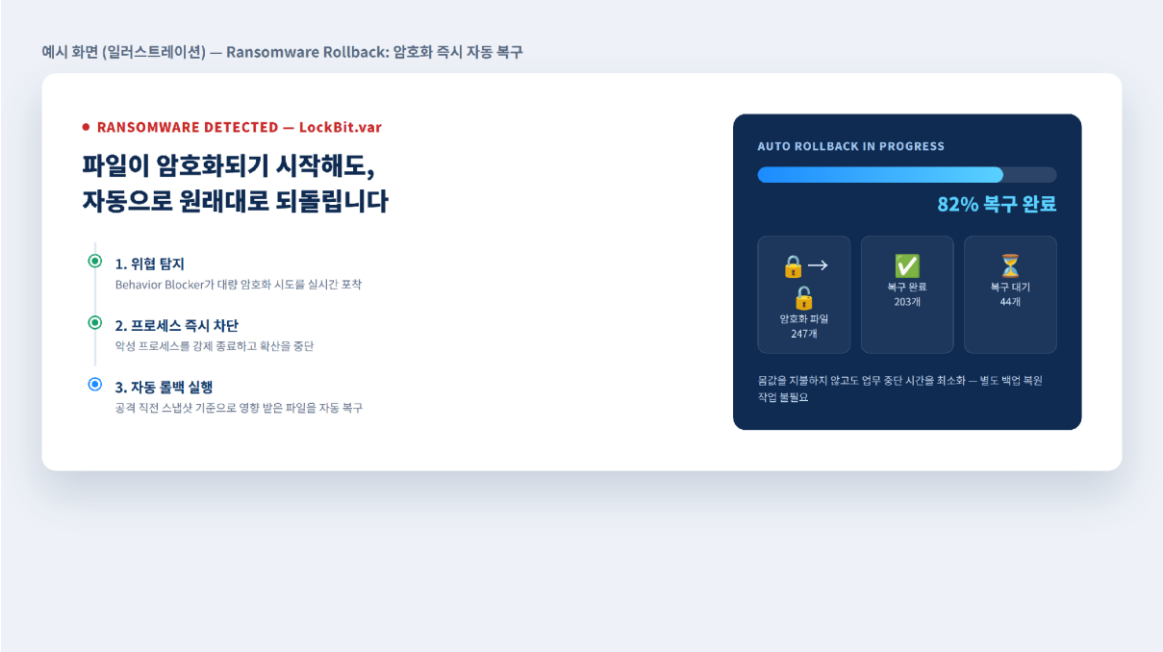


- **종합적인 위협 인텔리전스:** 클라우드 기반 행동 분석과 로컬 모니터링을 결합해 알려지지 않은 악성코드도 탐지
- **시각화된 위협 타임라인:** 조직 전체 엔드포인트의 감염 경로를 한눈에 파악
- **손쉬운 연동:** Syslog(CEF), Splunk 등 기존 SIEM 과 자동 연동해 별도 재구축 불필요
- **자동화된 대응 플레이북:** 인시던트 유형별로 사전 정의된 대응 절차를 자동 실행

04. 막지 못했다면? — 몸값 없이 되돌리는 자동 롤백

아무리 다층 방어를 갖춰도 100% 차단을 보장할 수는 없습니다. Emsisoft Enterprise Security + EDR 은 랜섬웨어가 파일 암호화를 시작한 순간에도 스냅샷 기반으로 영향 받은 파일을 자동으로 되돌리는

Rollback 기능을 제공합니다. 몸값을 지불하거나 백업에서 수동으로 복원할 필요 없이, 업무 중단 시간을 최소화할 수 있습니다.



05. 타사 EDR 과 비교했을 때 Emsisoft 가 유리한 지점

동일하게 "엔드포인트 보안 + EDR"로 분류되는 제품이라도, 중소기업이 별도 인력 없이 실제로 운영할 수 있는지는 전혀 다른 문제입니다.

비교 항목	Emsisoft	MS Defenderfor Business	CrowdStrikeFalcon Go	SentinelOne /Sophos
EDR 기본 포함	✓ 무료 제공	M365 번들 필요	별도 상위 요금제	일부 상위 티어
랜섬웨어 자동 롤백	✓ 지원	✗ 미지원	✗ 상위 요금제	제품별 상이
전담 보안인력 없이 운영	✓ 설계 목표	M365 지식 필요	MDR 병행 권장	MDR 병행 권장
특정 생태계 종속	없음	Microsoft 365 종속	없음	없음

※ 경쟁사 항목은 2026 년 기준 각 사 공식 페이지 및 공개된 제 3 자 리서치 자료를 참고했으며, 요금제·정책은 변경될 수 있습니다. 정확한 Emsisoft 국내 견적은 SoftMail 로 문의해 주세요.

예시 시나리오 — 임직원 40 명 규모 제조업체라면

전산 담당자가 1~2 명뿐인 40 인 규모 회사를 가정해 보겠습니다. CrowdStrike 나 SentinelOne 을 도입하면 EDR 알림을 매일 검토할 사람이 필요해 결국 MDR(관제 대행) 계약을 추가하게 되는 경우가 많고, MS Defender for Business 는 Microsoft 365 라이선스 구성에 따라 보호 범위가 달라져 별도 검토가 필요합니다. Emsisoft 는 기본 설정만으로 5 중 방어와 EDR 이 함께 동작하고, 이상 징후가 있을 때만 관리자에게 알림이 오도록 설계되어 있어 위 규모의 조직도 별도 관제 인력 없이 운영을 시작할 수 있습니다.

중소기업이 Emsisoft 를 선택해야 할 이유 — 요약

- **전담 보안팀 없이도 운영 가능** — 복잡한 튜닝 없이 기본 설정만으로 실질적 방어력 확보
- **EDR 을 별도 비용 없이 제공** — 경쟁사 다수가 상위 요금제나 MDR 계약을 요구하는 것과 대조적
- **사전 차단 + 사후 자동 복구를 모두 갖춤** — 5 중 레이어 방어와 Rollback 으로 이중 안전장치 확보
- **특정 벤더 생태계에 종속되지 않음** — Windows·기존 인프라 환경에 자연스럽게 통합
- **단순하고 투명한 가격 구조** — 숨겨진 옵션 비용에 대한 불확실성을 줄임

SoftMail 과 함께 시작하세요

SoftMail 은 emsisoft.co.kr 을 운영하며 Emsisoft 제품을 국내 기업에 공급하는 파트너입니다. 회사 규모와 환경에 맞는 라이선스 구성, 마이그레이션 지원, 도입 전 무료 상담을 제공합니다. 지금 문의하시면 우리 회사에 맞는 구성과 정확한 견적을 안내해 드립니다.

지금 도입 상담을 신청하세요

회사 규모·환경 진단부터 라이선스 견적, 기존 백신 마이그레이션까지 SoftMail 이 함께합니다.

www.emsisoft.co.kr | Emsisoft 공식 파트너 SoftMail (서울 가산디지털단지)

출처: Emsisoft 공식 웹사이트(emsisoft.com) — Business Security, Enterprise Security + EDR, Anti-Ransomware, Behavior Blocker, EDR 소개 페이지 및 공식 블로그(2026 년 9 월 기준). 경쟁 제품 정보는 각 사 공식 페이지 및 공개된 제 3 자 가격 리서치 자료를 참고했습니다.