(개요) 체크포인트 코리아, 랜섬웨어 감염 여부 점검 진단 서비스

1. 랜섬웨어 위협 현황

- 2024 년~2025 년 동안, 국내 기업 대상 랜섬웨어 피해액은 수천억 원 규모로 집계되고 있습니다. 특히 중소·중견 기업도 더 이상 안전지대가 아닙니다.
- 공격 방식은 점점 정교해지고, AI·변종 랜섬웨어가 등장하면서 "예방이 아니면 복구도 어렵다"는 인식이 커지고 있습니다.
- 보안 예산 투자 부족, 전문 인력 한계, 클라우드·원격 근무 확산으로 공격 표면이 넓어지는 상황으로 인해서, 향후 랜섬웨어 피해 확대는 피할 수 없는 현실이 될 것 입니다.

이제는 **랜섬웨어 감염 여부 사전 점검**을 통해 취약점을 미리 발견하고 대응하는 전략이 필수입니다.

📌 국내 랜섬웨어 피해 사례

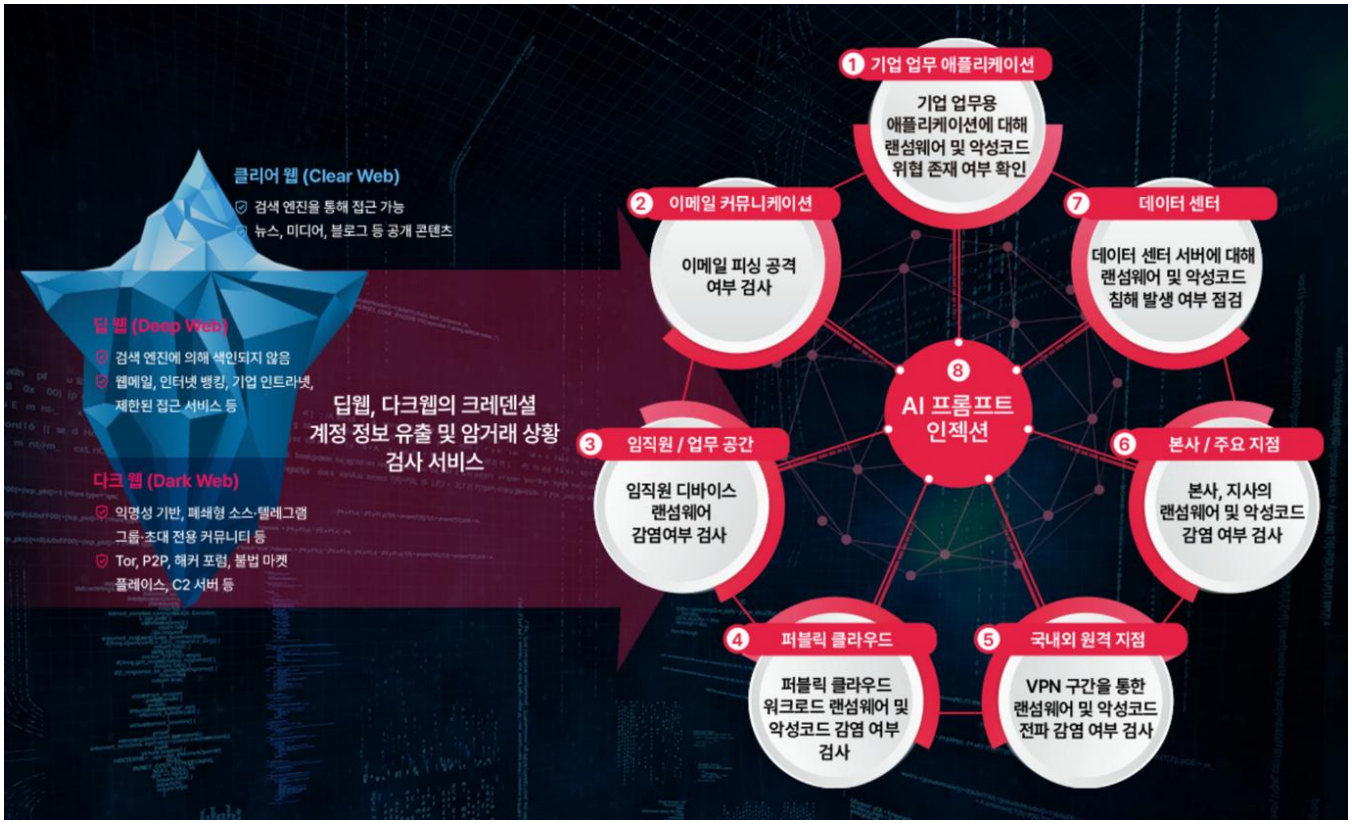
사례	피해 내용	시사점
온라인 서점 랜섬웨어 공격 (2025 년 6 월)	국내 대형 온라인 서점의 주요 시스템이 랜섬웨어에 감염되어, 웹사이트/앱 서비스가 전면 마비됨. 서버 설정 파일 및 스크립트 파일 등이 암호화됨. 한국경제	규모 있는 플랫폼도 한 순간에 마비될 수 있다는 경고. "나만은 안전하다"는 생각이 위험할 수 있음
1~4 월 국내 기업/기관 대상 공격 9 건	2025 년 1~4 월 사이 국내 기업 및 기관에 대한 랜섬웨어 공격 주장이 총 9 건 보고됨. 예: 삼*크, 신*크, 창*원 등. CBC 뉴스 | CBCNEWS+2SBS News+2	공격 빈도가 증가 추세임을 보여주는 지표. 다양한 업종이 공격 대상이 됨.
신종 랜섬웨어 '건라(Gunra)' 파생 공격 / 국내 기관 대상 위협	콘티(Conti)에서 파생된 신종 랜섬웨어 '건라'가 국내 기관을 노린 정황 보도됨. Chosunbiz	랜섬웨어 변종의 빠른 출현 → 보안 대응 체계는 유연하고 최신이어야 함

---

2. 랜섬웨어 감염 여부 사전 점검 진단 서비스의 대상 범위

이번 체크포인트 코리아 랜섬웨어 감염 여부 사전 점검 진단 서비스의 특징은, 최신 랜섬웨어 공격 트렌드에 맞춰진 다크웹/딥웹에서 불법 거래되고 있는 기업 계정 정보 유출 정보와 연계된 보안 침해 사고가 있었는지를 다각도로 탐지+분석+대응 할 수 있다는 것 입니다.

일반적인 랜섬웨어 점검 프로모션은, 네트워크 트래픽 또는 엔드포인트 디바이스 대상으로만 수행하기 때문에, 기업 IT 인프라에 대한 전방위적인 보안 위협 탐지가 어려운 한계가 존재합니다. (예: 몇 달 또는 몇 주 전 침해된 감염된 자산과 C2 아웃바운드 트래픽 탐지 및 식별 어려움, DNS 트래픽을 통한 내부 정보 탈취 이벤트 탐지 및 식별 어려움)



(이미지 설명: 체크포인트 랜섬웨어 감염 여부 사전 점검 진단 서비스의 대상 범위)

체크포인트 코리아, 랜섬웨어 감염 여부 점검 진단 서비스

기업 IT 인프라 중 핵심 사이버 공격 목표인 8 개 요소 및 점검 위치에 대한 랜섬웨어 감염 여부를, CISO 및 보안담당자가 보다 빠르고 정확하게 파악할 수 있도록 제공하는 것이 목표 입니다.

❖ 🔒 개인 정보 유출 탐지

- 기업 도메인 계정·임직원 이메일이 다크웹이나 해킹 포럼에 노출되었는지 확인.

  👉 사례: B 사의 직원 계정 200 여 개가 다크웹에서 발견, 2 차 공격 사전 차단 성공.

① 기업 업무 애플리케이션

- 점검: 사내/대외 업무용 웹·모바일·SaaS 앱의 랜섬웨어·악성코드 침투 경로, 취약 플러그인·취약 API, 노출 자격증명 악용 시도(크리덴셜 스터핑) 탐지.
- 결과: 위험 앱 목록, 취약 구성/버전, 차단·패치·MFA 강제 등 개선 권고.

  👉 사례: B 사의 직원 계정 200 여 개가 다크웹에서 발견, 2 차 공격 사전 차단 성공.

② 이메일 커뮤니케이션

- 점검: 다크웹에 유출된 조직·임직원 정보를 활용한 피싱/스피어피싱 캠페인 여부, 악성 첨부/URL, 도메인 사칭. DMARC/SPF/DKIM 적용 상태 확인 지원.
- 결과: 공격 캠페인 IOC·샘플, 게이트웨이 정책 보완안, 고위험 대상자 리스트 제시.

  👉 사례: C 사에서 임원 사칭 메일을 통한 송금 지시 사건 발생, 사전 점검 서비스를 통해서 동일 유형 탐지 후 방어 체계 강화.

  👉 사례: G 사의 브랜드명 유사 사이트가 발견되어 고객 피해 예방.

③ 임직원 단말/업무공간 (엔드포인트 디바이스)

- 점검: EDR/로그로 랜섬웨어 전조(Tool 설치, 권한 상승, PsExec/RDP 남용, VSS 삭제) 여부, 패치/취약 SW, USB·매크로 정책 탐지 지원.
- 결과: 고위험 단말·사용자, 격리·조치 우선순위, 하드닝 체크리스트 제시.

  👉 사례: I 사 랜섬웨어 감염 여부 진단 서비스를 통해서, 기존 솔루션이 탐지하지 못한 악성 Beaconing 발견.

④ 퍼블릭 클라우드 (워크로드)

- 점검: IaaS/컨테이너·서버리스의 노출 포트·보안그룹·저장소 공개 설정, 키/토큰 유출 연계 침투 흔적, 워크로드 내 악성 실행 흔적.
- 결과: 잘못된 구성(Misconfig) 목록, 워크로드 격리·IAM 최소권한·이미지 스캔 권고.

  👉 사례: E 사는 원격 접속 솔루션 취약점으로 랜섬웨어에 감염, 복구에 수주 소요.

⑤ 국내외 원격 지점(VPN/원격 구간)

- 점검: VPN (IPSec, SSL VPN) 접속 사용자 계정 탈취 징후, 취약 암호화·분할터널링, 원격지에서 본사로 L2/L3 확산 경로를 통한 랜섬웨어·악성코드 유입 탐지 지원.
- 결과: 취약 터널·계정, 강제 MFA·정책 재설계(Zero Trust 분리) 가이드 제시.

⑥ 본사/지사 및 주요 거점 네트워크 영역

- 점검: AD·파일서버·프린터 등 코어 자산의 측면이동 경로, 백업망 분리 여부, 네트워크 세그멘테이션·IPS 정책.
- 결과: "1 차 차단선" 보강 계획, 중요자산 보호 우선순위 매트릭스.

⑦ 데이터센터 (서버·스토리지 영역)

- 점검: 하이퍼바이저·DB/애플리케이션 서버의 침해 징후, SMB/NFS 공유지 암호화 위험, 백업/스냅샷의 불변성(Immutable)·격리 수준.
- 결과: 복구가능성(Recoverability) 점수, 백업 체계 개선 및 네트워크 격리 권고.

  👉 사례: F 사에서 백업 서버까지 암호화되어 수개월치 데이터 손실.

⑧ AI 프롬프트 인젝션 (GenAI LLM 연계 업무 흐름 영역)

- 점검: GenAI LLM/AI 에이전트가 내부 도구·데이터에 접근하는 경로의 프롬프트 인젝션·데이터 유출 위험, 입력검증·출력제한·권한분리 여부.
- 결과: 공격 시나리오·재현 보고, 가드레일(정책/필터/격리) 적용 지침.

  👉 사례: D 사의 연구소 서버에서 AI 학습 데이터 유출 시도 발견.

* 공통 분석 레이어 – 다크웹/딥웹 연계 인텔리전스

- 수집: 유출 계정·도메인·코드 조각·접속 로그·인프라 지표.
- 연계: 이메일·VPN·EDR·클라우드 로그와 상호대조, MITRE ATT&CK 기반 TTP 매핑, 실거래/협박 포스팅 여부 확인.
- 산출: "실제 악용 가능성" 중심의 위험평가와 즉시 실행 가능한 단기/중기 권고.

3. 랜섬웨어 사전 점검 진행 절차

1. 온라인 신청 👉 **[무료 보안 점검 신청하기]**
2. 보안 전문가와 사전 인터뷰
3. 원격/현장 점검을 위한 도구 설치 실행

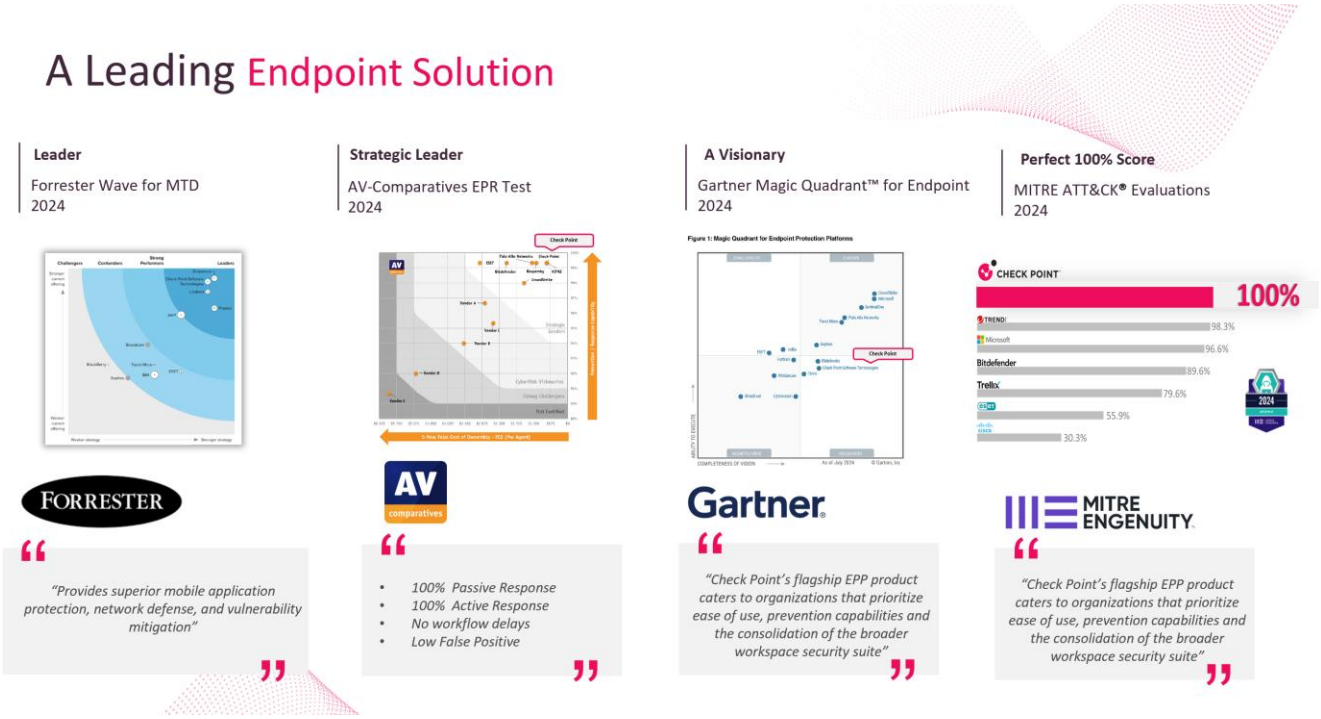
4. 맞춤형 취약점 리포트 제공

5. 후속 보안 대응 가이드 제안

4. 고객 혜택

- 무료 랜섬웨어 및 보안 점검 리포트를 제공해 드립니다 → 현재 기업의 보안 준비 태세 수준을 한눈에 파악할 수 있습니다.
- 실제 공격 시뮬레이션 결과를 기반으로 구체적인 대응 방안 및 솔루션을 제시해 드립니다.
- 30 년 이상 글로벌 사이버 보안 전문 회사, 체크 포인트의 최신 보안 기술 및 선진 사례를 함께 체험 할 수 있습니다 (랜섬웨어 차단 사례 포함).
- 참여 이벤트 : 신청 기업 대상 사은품 제공 (별도 공지된 내용 기준으로 제공)

5. 글로벌 사이버 보안 리더, 체크포인트 랜섬웨어 감염 여부 점검 진단 서비스를 이용하는 이유



6. 마무리 메시지

현존 일반적인 보안 솔루션은 **탐지 및 대응(reactive)** 중심으로 설계되어, 공격 발생 후 대응하는 방식이 대부분입니다 → 이로 인해서 대응 **비용 증가, 복잡성 증가, 보안 격차가 발생 합니다**.

이러한 문제점 극복을 위해서, 체크포인트는 **사전 예방(prevention)** 중심의 아키텍처를 제공하며, **서비스 제공 지연 없이 단일 플랫폼에서 대응 및 처리**하고, **대용량 차세대 보안위협 예방을 위한 대용량 클러스터링 기술(마에스트로) 제공**과 **온프레미스 및 클라우드 환경을 모두 지원하는 특장점을 제공 합니다.**

"귀사의 보안 태세는 지금 점검해야 합니다."

랜섬웨어 감염 여부 사전 점검 진단 서비스를 통해서, 랜섬웨어 위험을 사전에 차단하세요.

👉 **[무료 보안 점검 신청하기]**