제로 트러스트와 엔드포인트 보안 보고서

1) 제로 트러스트 보안의 이해

- **정의와 원칙**: “네트워크 경계 신뢰”를 버리고 **항상 검증(verify explicitly)**, **최소 권한(least privilege)**, **침해 가정(assume breach)**을 전제하는 아키텍처. 사용자·디바이스·애플리케이션·데이터 단위로 지속 평가·정책 집행을 합니다.
- **실행 프레임**: CISA는 ZT를 Identity / Devices / Networks / Applications & Workloads / Data5개 기둥으로 성숙도 모델과 함께 제시합니다. 조직은 각 기둥별로 정책·원격측정·자동화 수준을 단계적으로 끌어올립니다.
- **참고 사례**: Google의 BeyondCorp는 사내망 특권을 없애고, 단말·사용자·컨텍스트 기반으로 애플리케이션 접근을 통제하는 ZT 구현 사례입니다. Google

2) 엔드포인트(단말) 보안의 핵심 취약점

- **초기 침투(Initial Access)**: 피싱·악성 문서·공개 서비스 악용, 그리고 탈취한 **유효 계정(Valid Accounts)**남용.
- **취약한 구성/패치 지연**: 미패치 소프트웨어, 약한 구성(예: 매크로 허용, LAPS 미사용). **구성·패치 표준 부재**가 상시 위험을 키웁니다.
- **과권한·자격증명 노출**: 로컬 관리자 상시 사용, 토큰/쿠키/비밀번호 저장소 탈취 후 권한 상승·내부 확산.
- **가시성 부족**: EDR 미도입·로그 수집 미흡으로 행위 기반 탐지와 포렌식이 어려움. (CIS Controls는 가시성·모니터링을 핵심 통제로 권고)

3) 제로 트러스트 관점의 엔드포인트 대응 방안

아래는 ZT 5개 기둥에 맞춘 **실행 체크리스트**입니다.

- Identity: 전 계정 **MFA(피싱 저항)**, SSO 연동, 조건부 접근(사용자·위치·리스크). 권한은 역할 기반으로 최소화·정기 재인증.
- Devices: **기기 신원·상태 attestation**(암호화·부팅 무결성·EDR 동작 여부), 불합격 단말은 격리. MDM으로 정책 표준화.
- Networks: 엔드포인트 방화벽/세그먼트, 원격 접근은 앱 단위 프록시·ZTNA로 세밀 제어(“사내망=신뢰” 제거).
- Applications & Workloads: 애플리케이션 화이트리스트·브라우저 격리·관리형 업데이트. 민감 앱은 기기 상태·사용자 리스크를 **매 요청 시**재평가.
- Data: 전체 디스크/폴더 **암호화**, DLP·클립보드/프린트 통제, 민감 데이터는 분류·라벨링 후 정책 기반 보호.

공통 베이스라인(필수 통제)

- **패치·취약점 관리**: OS/브라우저/플러그인 자동 패치, 고위험 CVE는 SLA 기반 신속 조치.
- **EDR/행위 탐지**: 프로세스·스크립트·자격증명 접근 이상 행위 탐지 및 격리. ATT&CK기법 기반 탐지 튜닝.
- **구성 표준화**: CIS Benchmarks 수준의 하드닝(서비스·포트 최소화, 매크로 차단, 로컬관리자 제거).

4) 도입·진단 절차(면접용 7단계 스크립트)

1. **현황 수집**: 자산·계정·단말 상태 인벤토리와 로그 파이프라인 가시화(CIS Controls 권고).
2. **성숙도 측정**: CISA **ZT Maturity Model**로 5개 기둥의 현재 레벨 진단.
3. **격차 분석**: NIST **SP 800-207**원칙에 맞춰 정책·데이터 흐름·신뢰 결정을 재설계.
4. **빠른 개선(0–90일)**: MFA 전면화, 관리자 권한 제거, EDR 전면 배포, 고위험 미패치 제거.

5. **정책·자동화(90–180일)**: 조건부 접근·디바이스 상태 검증, ZTNA 파일럿, 로그·경보 SOAR 연계.
6. **운영(상시)**: ATT&CK 기반 탐지 개선, 위협 헌팅, 취약점·구성 Drift 자동 교정.
7. **지속 검증**: 침투 테스트/가짜 피싱/비상복구 훈련으로 정책 효과를 **주기적으로 검증**.

5) 개인 의견

- 제로 트러스트는 "솔루션 구매"가 아니라 **정책·신원·단말 상태·데이터 맥락**을 결합해 **매 요청을 재평가**하는 **운영 모델**입니다. NIST 800-207을 기준으로, CISA 성숙도 모델을 **측정 지표**로 삼으면 좌표가 흔들리지 않습니다.
- 엔드포인트에서는 **MFA+EDR+패치**3가지를 최우선으로 표준화하고, 원격접속은 **ZTNA/BeyondCorp 접근제어**로 "사내망 특권"을 없애는 것이 가장 효과 대비 비용이 좋았습니다

6) 참고 자료

https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf
https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf
https://research.google/pubs/beyondcorp-a-new-approach-to-enterprise-security/