Special Report

제로트러스트 보안전략 : 기기 및 엔드포인트 (Device/Endpoint)

SI/솔루션사업그룹 보안 SI 사업팀 황병권 책임

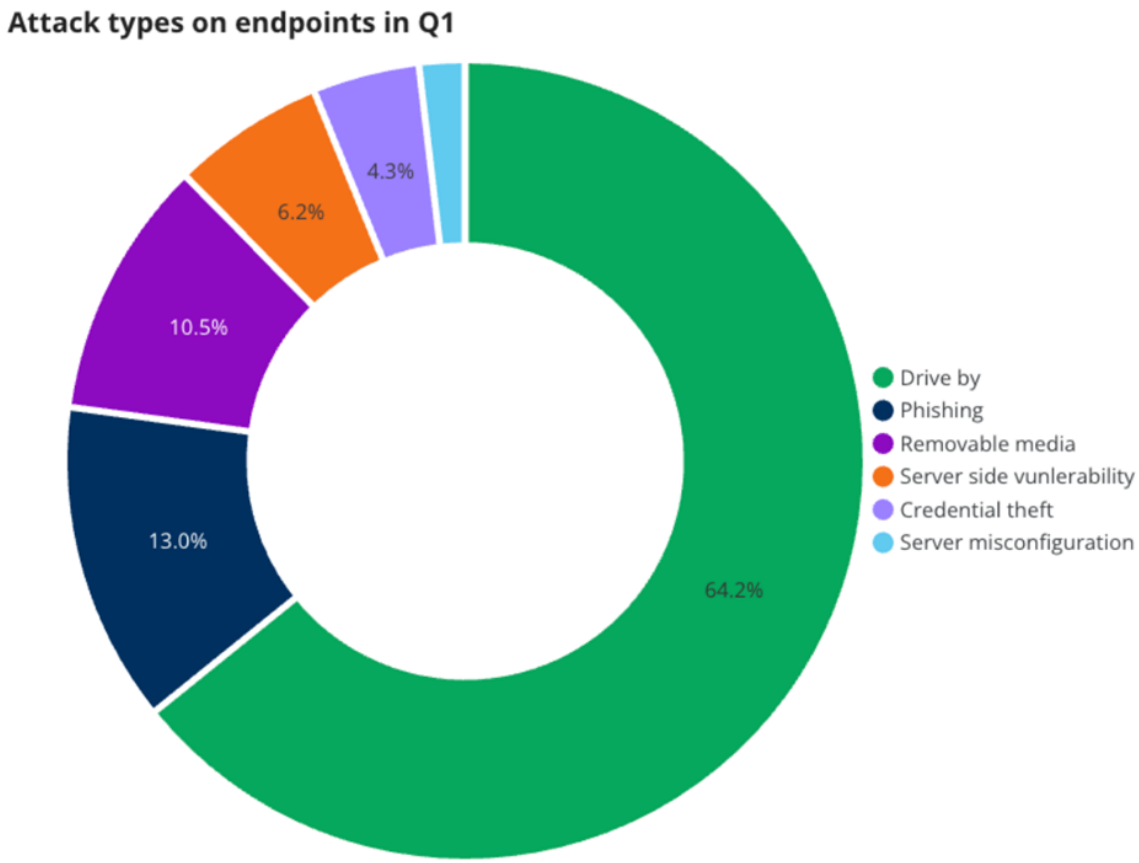
■ 기기 및 엔드포인트 (Device/Endpoint) 필러 개요

제로트러스트 아키텍처에서 기기(Device) 및 엔드포인트(Endpoint) 필러는 식별자·신원(Identity) 필러와 긴밀하게 연계되어, 사용자가 민감한 리소스에 접근하기 전에 디바이스 상태와 보안 신뢰도를 기반으로 최종 접근 여부를 판단하는 핵심 통제 지점으로 작동한다. 사용자의 신원이 확인되더라도, 해당 디바이스가 검증되지 않았거나 보안 기준을 충족하지 못할 경우, 접근은 제한되어야 한다. 이는 CISA 의 가이드라인에서 강조하는 사용자와 디바이스의 상태, 위치, 행위 등의 다양한 요소를 기반으로 접근 정책을 동적으로 조정하는 체계를 적용해야 함을 의미한다.

코로나 19 팬데믹 이후 업무 환경은 급격히 변했다. 이에 따라 조직의 주요 정보들은 사용자들이 일상적으로 사용하는 PC, 노트북, 태블릿 등 다양한 디바이스에 분산되어 저장돼 사용하는 형태로 전환되었다. 이러한 디바이스들은 내부망과 외부 망, 클라우드 환경 등 여러 보안 경계를 넘나들며 연결되고 있으며, 특히 재택근무, 출장, 외부 고객 미팅 등으로 기업 소유 또는 개인 소유(BYOD)의 디바이스를 공공장소나 외부 네트워크로 빈번하게 활용하고 있다.

특히 국내의 경우, 물리적 망분리를 중심으로 설계된 기존 보안 환경이 원격·유연 근무 확대로 구조적 제약으로 작용하고 있다. 이를 해소하기 위해 국가정보원 주도의 '국가 망 보안체계 가이드라인(N2SF)', 금융위원회의 '금융분야 망분리 개선 로드맵' 등에서 망 분리 환경의 단계적 완화와 제로트러스트 기반 보완책을 함께 제시하고 있다. 이러한 흐름은 디바이스 및 엔드포인트 수준에서의 실질적인 보안 검증과 제어 체계를 더욱 정교하게 요구하고 있다.

디바이스 및 엔드포인트 환경의 다변화와 더불어, 엔드포인트를 노리는 공격은 꾸준히 증가하고 있다. 최근 Expel 의 "2025 년 1 분기 엔드포인트 위협 보고서"에 따르면, 조직을 대상으로 한 전체 보안 사고 중 68%가 엔드포인트에서 발생하였으며, 아래 그림을 보면 '드라이브 바이(Drive by)', 피싱(Phishing), 이동식 저장매체(Removable media), 서버 취약점(Server side vulnerability) 등 다양한 공격 유형이 확인됐다. 특히, '드라이브 바이' 공격이 전체 엔드포인트 공격의 64.2%로 가장 높은 비중을 차지하고 있어, 기존 네트워크 중심의 수동적 방어만으로는 대응에 한계가 있음을 보여준다.



출처 : Expel "2025 년 1 분기 엔드포인트 위협 보고서"

그림 1. 2025 년 1 분기 엔드포인트 공격 유형

"Expel, CrowdStrike 등 글로벌 리포트에서 말하는 디바이스와 엔드포인트에는 시스템(서버)까지 포괄하는 경우가 많지만, 국내 제로트러스트 실무에서는 사용자 디바이스 중심의 엔드포인트 관점으로 해석할 필요가 있다."

이처럼 디바이스 및 엔드포인트에 대한 위협이 고도화·지능화됨에 따라, 단순한 방화벽·백신 중심의 대응만으로는 충분하지 않다. 행위 기반 탐지(EDR/XDR), 통합 엔드포인트 관리(UEM), 지속적인 보안 상태 모니터링, 정책 기반 접근 통제 등 다양한 대응 전략을 동시에 적용하는 다층적 방어 체계가 필요하다. 제로트러스트 관점에서는 디바이스 및 엔드포인트의 신뢰성을 동적으로 평가하고, 위협을 실시간으로 탐지·차단하는 체계 구축이 핵심이다.

특히 제로트러스트 환경에서는 사용자의 신원을 검증할 때, 해당 사용자가 실제로 접근하는 디바이스의 신뢰성과 보안 상태 또한 연계하여 함께 확인하는 것이 필수다. 예를 들어, 동일한 자격을 가진 사용자라 하더라도, 미승인 혹은 위험도가 높은 디바이스(패치 미적용, 악성코드 감염, 이상 행위 탐지 등)로는 기업 내 중요 시스템이나 데이터에 대한 접근을 자동으로 제한해야 된다. 이처럼 식별자와 디바이스 필러의 연계적 통제는 조직 내 민감 자산이 실질적으로 보호받을 수 있도록 하며, 단일 인증 체계의 취약점을 보완하는 결정적 역할을 수행하게 된다.

디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처 내에서 단순한 접속 수단을 넘어, 조직 접근 정책과 실시간 위험 평가의 핵심 축으로 기능한다. 특히 디바이스는 실제 사용자가 업무에 활용하는 실질적 접근 주체이기 때문에, 정책 판단 과정에서 각종 속성 정보와 보안 상태를 제공하는 PIP(Policy Information Point, 정보제공지점)로서의 역할이 강조된다.

결과적으로 디바이스 및 엔드포인트 영역을 제로트러스트 아키텍처 관점으로 고도화할 때, 조직은 점차 정교해지는 위협에 효과적으로 대응하는 것은 물론, 핵심 자산과 정보를 안전하게 보호할 수 있는 기반을 만들 수 있다.

■ 기기 및 엔드포인트 (Device/Endpoint) 필러의 주요 요소

디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처에서 사용자 신원(Identity)과 더불어, 실제 리소스 접근의 전 단계에서 적용되는 핵심 보안 통제 영역이다. 디바이스는 사용자가 업무에 활용하는 실질적 접점이자, 조직 자산 및 데이터에 대한 다양한 위협이 현실적으로 발생하는 지점이다.

특히, 제로트러스트 환경에서는 모든 디바이스와 엔드포인트를 신뢰할 수 없는 대상으로 간주하고, 디바이스의 상태·신뢰도·위험 수준 등을 기반으로 실시간 검증과 세분화된 정책 적용이 요구된다. 이를 위해, 디바이스 인벤토리(자산 목록화), 디바이스 인증, BYOD 관리, 취약점 및 패치 관리, 위험 평가 등 다양한 요소별 통합 관리 체계가 마련되어야 한다.

아래에서는 디바이스 및 엔드포인트 필러의 주요 요소들과, 이를 구현하기 위한 관리적·기술적 방안을 구체적으로 살펴본다.

1. 디바이스 인벤토리

제로트러스트 환경에서 디바이스 인벤토리는 조직 내 리소스에 접근 가능한 모든 기기를 체계적으로 식별·관리하는 기반이 된다. 관리 대상은 데스크톱, 노트북, 스마트폰, 태블릿은 물론, IoT 기기와 프린터, 이동식 저장장치 등으로 확장된다. 이에 따라 조직은 디바이스의 형태, 운영체제, 하드웨어·소프트웨어 특성 등 세부 속성을 기준으로 식별 정책을 마련하고, 각종 인벤토리 정보를 통합적으로 관리해야 한다.

디바이스 인벤토리는 단순 목록화가 아닌, 네트워크에 새로 연결되는 기기의 자동 등록, 디바이스 상태 변화·위치 이동·폐기 등 라이프사이클 관리가 포함된다. 자동화된 자산관리 시스템이나 UEM(Unified Endpoint Management), AD 등과 연계해 인벤토리 정보의 정확성과 최신성을 유지하는 것이 중요하다.

등록된 인벤토리 정보에는 소유자, 소속 부서, 용도, 보안 등급, 연결 이력 등 다양한 데이터가 포함되며, 이러한 정보는 보안 정책 적용, 이상행위 감지, 사고 대응의 핵심 자료로 활용된다. 또한, 중요도·위험도·업무 유형 등에 따라 디바이스를 그룹화하고, 그룹별로 차등화된 접근통제 및 보안 정책이 적용될 수 있다. 예를 들어, 관리용 디바이스와 일반 사용자, 외부 협력업체 디바이스를 구분해 관리함으로써, 불필요한 권한 확산과 내부 위협을 효과적으로 통제 가능하다.

2. 디바이스 인증

제로트러스트 환경에서 디바이스 인증은, 단순히 기기가 등록되어 있다는 사실만을 신뢰하지 않는다. 조직은 접근 요청이 들어오는 각 디바이스에 대해 고유 식별 정보(예: MAC 주소, 디지털 인증서, 시리얼 등)를 활용해 신뢰할 수 있는 기기인지 여부를 반드시 확인해야 한다. 이 과정에서는 단순 인증 정보뿐만 아니라, 소유자, 등록 이력, 관리 상태 등의 교차 검증 절차를 반드시 병행해야 한다. 미승인·비인가 디바이스에 대해서는 네트워크 접근을 원천적으로 차단할 수 있도록 정책을 설계하는 것이 중요하다.

디바이스 인증은 일회성 절차에 머물러서는 안 된다. 조직은 디바이스의 네트워크 연결 현황, 운영체제 및 소프트웨어 최신화 여부, 물리적 위치와 사용자의 접속 이력, 행위 패턴 등 다양한 요소를 종합적으로 평가해 신뢰도 점검을 주기적으로 해야 한다. 예를 들어, 패치 미적용 기기, 악성코드 감염, 비정상적인 위치·시간의 접근 등이 감지되는 경우, 추가 인증 또는 접근 제한 등의 추가 절차를 반드시 반영해야 한다. 이러한 신뢰도 평가는 UEM, EDR 등 보안 시스템과 연계해 실시간으로 자동화하는 것이 효과적이다.

조직은 디바이스 신뢰도 평가 결과를 기반으로, 각 디바이스에 대해 접근 허용, 제한, 격리, 추가 인증 등 세분화된 대응 정책을 마련해야 한다. 신뢰도가 낮은 기기에 대해서는 민감 자산 접근을 자동으로 차단하거나, 별도의 관리 체계로 이관하는 방안을 검토해야 한다. 이러한 모든 과정은 ICAM, SSO, EDR, UEM 등과의 통합 운영 체계를 통해 보안 정책과 연동하여, 조직 전반의 위험 대응 능력을 향상시키는 데 기여해야 한다.

3. BYOD(Bring Your Own Device) 관리

제로트러스트 환경에서 BYOD 관리는 개인이 소유한 노트북, 스마트폰, 태블릿 등 각종 디바이스가 업무 목적으로 조직 리소스에 접근할 수 있도록 허용하는 대신, 반드시 적정 수준의 보안통제와 정책 준수가 병행되어야 한다. 개인 디바이스를 통한 업무는 사용 편의성과 생산성을 크게 높일 수 있지만, 한편으로는 조직의 민감 정보가 외부 환경에 노출될 가능성을 상존하게 만든다.

따라서 조직은 BYOD 도입 여부 및 허용 범위, 승인 절차, 보안 수준, 운영체제와 관리 플랫폼(MDM/UEM) 등을 명확히 정책으로 정의해야 한다. 허용된 디바이스 유형, 플랫폼, 소프트웨어 목록, 필수 보안 앱 설치 여부 등 기준을 구체적으로 마련하는 것이 중요하다.

BYOD 정책에는 디바이스 등록과 주기적 보안상태 점검, 접속 이력 기록, 중요 리소스 접근 시 강화된 인증(MFA), 클라우드·네트워크 분리 등 다양한 보안요건이 반영되어야 한다. 또한, BYOD 사용자의 개인정보 보호와 프라이버시 침해 방지 측면도 중요하게 다뤄져야 하므로, 최소한의 모니터링 범위와 용도, 접근 가능 정보에 대해 사용자에게 사전 고지 및 동의를 받는 절차를 마련해야 한다.

BYOD 위험도 평가는 기기 보안상태, OS 취약점, 악성코드 감염 여부, 백신·MDM 설치 여부, 정책 위반 이력 등을 종합적으로 반영해 주기적으로 실시하는 것이 필요하다. 이러한 평가는 UEM, MDM, EDR 등 통합관리 솔루션을 통해 자동화하는 것이 효율적이다. 위험도가 높게 평가된 디바이스는 민감 데이터 접근 제한, 추가 인증 요구, 조직 네트워크 격리 등 차등화된 대응 정책으로 관리할 수 있다.

BYOD 환경의 실시간 모니터링 역시 필수적이다. 운영체제·제조사·설치, 소프트웨어·네트워크 접속 이력 등 기초 정보뿐만 아니라, BYOD 정책 위반 여부, 비정상 접속 패턴, 의심 활동 발생 시 자동 경고 등 다양한 요소를 관리 시스템에서 수집·분석하도록 한다. BYOD 를 모니터링할 때에는 업무 중단이나 과도한 사생활 침해가 발생하지 않도록 업무 관련 데이터와 개인 데이터의 논리적 분리 원칙이 반드시 보장되어야 한다.

4. 디바이스 취약점 관리

제로트러스트 환경에서 디바이스 취약점 관리는 단순히 소프트웨어나 운영체제의 최신 패치를 적용하는 수준을 넘어, 조직 내에 존재하는 모든 기기(PC, 노트북, 모바일, IoT 등)에 대한 취약점 탐지와 영향 평가, 신속한 대응까지 전 주기를 포괄해야 한다.

우선, 조직은 정기적이고 체계적인 취약점 식별 및 평가 정책을 수립해야 하며, 이를 통해 기기별 취약점 진단 절차와 평가 기준, 자동화된 점검 주기, 발견 시 조치 프로세스 등 일련의 관리체계를 구체적으로 마련해야 한다.

취약점 진단 단계에서는 UEM, MDM, EDR 등 보안 시스템을 활용해 네트워크 상에 연결된 모든 디바이스를 주기적으로 스캔한다. 이 과정에서 운영체제 미 패치, 취약한 애플리케이션, 불필요한 서비스 구동 등 다양한 취약 요소를 식별하며, 위험 등급 및 우선순위에 따라 신속한 조치가 이루어져야 한다. 최신 보안 패치 배포, 취약 소프트웨어 제거, 설정 변경, 네트워크 격리 등 자동화된 대응을 병행하는 것이 바람직하다.

취약점이 발견되면, 해당 취약점의 영향도와 악용 가능성을 분석해 우선순위별로 대응 전략을 세워야 한다. 예를 들어, 내부 주요 시스템 침해, 데이터 유출, 랜섬웨어 감염 등 실질적 피해 가능성이 높은 취약점은 즉시 차단·패치·격리 등 강력한 대응 조치를 실행한다. 취약점 영향 분석 결과와 대응 과정은 별도의 보고서로 기록해, 향후 유사한 위협 발생 시 신속한 참고자료로 활용한다.

취약점 관리 결과는 디바이스 위험도 평가에 직접 반영할 수 있다. 반복적으로 취약점이 발견되거나, 미조치 상태가 지속되는 기기는 민감 데이터 접근 제한, 추가 인증 요구, 네트워크 분리 등으로 연동해 실질적 리스크를 줄일 수 있다.

종합적으로, 디바이스 취약점 관리체계는 디바이스 인벤토리·인증·신뢰도 평가와 연계해 운영함으로써, 조직 내에 존재하는 모든 단말의 보안 수준을 일관성 있게 유지하고, 침해사고 가능성을 선제적으로 차단할 수 있는 기반이 된다.

5. 디바이스 패치 관리

제로트러스트 환경에서 디바이스 패치 관리는 조직 내 모든 기기의 보안 수준을 일관되게 유지하기 위한 핵심 요소다. 패치 관리는 단순한 소프트웨어 업데이트가 아니라, 체계적인 정책 수립과 절차 정의, 그리고 패치 배포·검증·사후 관리까지 전 주기에 걸쳐 관리 체계를 갖추는 것이 중요하다.

조직은 먼저, 디바이스 운영체제와 디바이스 내에서 사용되는 애플리케이션, 펌웨어 등에 대한 패치 적용 원칙과 절차를 구체적으로 정의하는 패치 관리 정책을 마련해야 한다. 해당 정책에는 관리 대상 기기의 목록화, 패치 우선순위 산정, 패치 배포·설치 프로세스, 백업 및 복구 방안, 패치 적용 이력 관리와 같은 핵심 항목들이 포함되어야 한다. 패치 관리 정책은 실제 보안 환경의 변화와 기술 발전을 반영해 정기적으로 검토·갱신하는 것이 필요하다.

패치 배포 시에는 각 디바이스의 특성, 운영 환경, 업무 중요도 등을 종합적으로 고려하여, 자동화된 시스템(AD, PMS 등)을 적극 활용해야 한다. 모든 단말에 일괄 적용하는 방식이 아닌, 네트워크 환경이나 사용자 편의성, 업무 영향도를 반영해 배포 일정과 방식에 유연성을 두는 것이 효과적이다. 패치의 정확성, 완전성, 일관성, 확장성 등을 관리 지표로 삼아, 최신 패치가 신속하고 누락 없이 적용될 수 있도록 설계해야 한다.

패치 적용 이후에는, 설치 현황과 누락 여부를 실시간으로 모니터링할 수 있는 체계가 필요하다. 누락되거나 실패한 패치에 대해서는 신속하게 추가 조치를 수행하고, 예외 상황이나 실패 이력은 별도의 보고 체계를 통해 관리하는 것이 바람직하다. 또한, 패치 관리 결과와 이력은 정기적인 보안 점검, 위험도 평가, 내부·외부 감사 및 규제 대응 등에 적극적으로 활용할 수 있도록 체계적으로 기록·보관해야 한다.

디바이스 패치 관리는 디바이스 인벤토리, 취약점 진단, 신뢰도 평가와 연계해 운영함으로써, 조직 내 모든 단말의 보안 취약점을 선제적으로 차단하고, 일관된 보안 수준을 유지하는 기반이 된다.

6. 디바이스 위험 관리

제로트러스트 아키텍처에서 디바이스 위험 관리는 조직 내 모든 업무용 기기의 물리적·논리적 위협에 대한 보호를 핵심 목표로 한다. 디바이스는 분실, 도난, 탈취, 비인가 접근과 같은 직접적인 물리적 위협뿐만 아니라, 내부자 위험이나 악성코드 감염, 데이터 유출 등 다양한 리스크에 노출될 수 있다.

먼저, 모든 디바이스는 자산 목록에 등록해 소유자와 위치, 사용 이력 등 주요 정보를 체계적으로 관리해야 한다. 물리적 분실이나 도난 사고에 대비해, 노트북이나 태블릿 등 주요 장비에는 시건장치(잠금장치) 등의 물리적 보호조치를 도입한다. 이동이 잦은 장치에는 GPS 기반 위치 추적 기능이나 분실 시 원격 잠금·데이터 삭제 등 즉각적 대응체계를 마련해야 한다.

디바이스 사용자는 분실·도난 등 사고 발생 시 즉각적으로 조직 내 IT 담당자나 보안 관리자에게 신고할 수 있는 절차를 숙지해야 하며, 조직은 이를 위해 정기적인 보안 교육과 가이드라인을 제공해야 한다.

이러한 다층적 관리·운영 체계를 기반으로, 조직은 단순히 기술적 보호조치에만 의존하지 않고, 사람과 정책, 프로세스가 결합된 통합적 보안 환경을 구현해야 한다. 디바이스 위험 관리는 결과적으로 정보 유출, 자산 손실, 내부자 위협 등 다양한 리스크를 최소화하고, 업무 연속성과 정보보호 수준을 실질적으로 강화하는 기반이 된다.

7. 통합 엔드포인트 관리(UEM)

조직 내 엔드포인트 환경이 PC, 노트북, 모바일, IoT 등으로 다변화됨에 따라, UEM(Unified Endpoint Management)은 단일 플랫폼에서 다양한 기기의 등록, 인증, 정책 배포, 보안 관리, 데이터 보호까지 통합적으로 지원해야 한다. 단순히 모바일 단말의 원격 제어에 머무는 기존 MDM 에서 진화해, 업무 현장의 모든 엔드포인트에 대해 일관성 있는 보안 정책과 운영 효율성을 동시에 추구하는 것이 핵심이다.

UEM 정책은 조직의 정보보호 방침, 디바이스 관리 원칙과 연동되어야 하며, 디바이스 등록과 인증, 엑세스 제어, 보안 위협 감지 및 대응, 데이터 보호 등 주요 보안 요구사항을 세부적으로 포함해야 한다. 이때, UEM 은 단독으로 운영되지 않고 ICAM, 통합 모니터링 시스템 등과 연계하여, 조직 내 디바이스 영역에 제로트러스트 보안체계의 실질적 실행 플랫폼 역할을 수행해야 한다.

엑세스 제어 측면에서, UEM 은 각 디바이스가 조직 리소스에 접근하는 경로와 수준을 세밀하게 관리해야 한다. 네트워크 기반의 접근제어와 더불어, ICAM 연동을 통해 RBAC, ABAC 등의 정책을 적용할 수 있다. 또한, UEM 은 사용자 행동 분석 결과를 반영하여 위험도가 높거나 이상 징후가 탐지된 기기에 대해 별도의 제한 또는 추가 인증 절차를 적용하는 등, 동적이고 자동화된 엑세스 제어 체계를 마련해야 한다.

데이터 유출 방지 역시 UEM 의 중요한 기능이다. 디바이스 내 민감 데이터는 자동 식별과 암호화해 보호되어야 하며, 데이터 손실 방지(DLP) 기능과 연계하여 의도적, 비의도적 유출 모두를 효과적으로 차단해야 한다. 조직은 정기적으로 UEM 정책과 시스템의 효과성을 평가·개선하며, 새로운 유형의 디바이스와 위협에 능동적으로 대응할 수 있도록 관리체계를 지속적으로 고도화해야 한다.

8. 엔드포인트 확장 탐지 및 대응 (EDR)

최근 사이버 위협의 지능화로 전통적인 시그니처 기반 보안 방식만으로는 모든 위협을 감지하고 대응하는 데 한계가 있다. 이에 따라 EDR(Endpoint Detection & Response)은 실시간 탐지, 사용자 행동 분석, 지속적 모니터링 등 다층적인 접근으로 조직의 디바이스 및 엔드포인트 보안의 핵심 축으로 자리잡고 있다.

EDR 의 실시간 위협 탐지 및 차단 기능은 다양한 유형의 악성 코드, 내부자 위협, 익명 공격, 사회공학 기반 공격 등 폭넓은 위협을 신속하게 감지하고, 자동화된 정책에 따라 사전에 설정된 차단 조치를 수행할 수 있도록 한다. 이 과정에서는 행동 기반 탐지, 파일 및 네트워크 트래픽 분석, 프로세스 감시 등 다양한 기법을 조합해 알려진 위협과 미지의 공격까지 아우르는 대응 체계를 마련할 수 있다. 또한, 위협이 감지될 경우 파일 삭제, 네트워크 연결 차단, 응용 프로그램 실행 제한 등 자동화된 방어 조치가 신속하게 이뤄져야 한다.

EDR 은 단순한 위협 탐지를 넘어, 엔드포인트 사용자 및 행동을 분석하는 고도화된 기능을 제공해야 한다. 정상적인 사용 패턴을 학습·정의한 후, 이와 다른 비정상적인 행위나 정책 위반 징후를 실시간으로 감지해 이상 행위 발생 시 즉각적인 대응이 이뤄질 수 있도록 한다. 사용자별로 세분화된 정보 수집과 통계 분석을 통해, 잠재적 내부자 위협이나 계정 탈취와 같은 고위험 사건에 효과적으로 대응할 수 있다.

지속적인 디바이스 상태 모니터링 역시 EDR 의 중요한 역할 중 하나다. 단순히 위협 발생 시에만 작동하는 것이 아니라, 사용자 행동, 시스템 설정, 네트워크 접속, 소프트웨어 설치 현황 등 다양한 요소를 실시간으로 모니터링해 정책 위반이나 취약점 노출을 조기에 탐지해야 한다. 수집된 데이터와 이상 행위 정보는 ICAM, 통합 관제 시스템 등 조직 내 타 보안 시스템과 연계되어, 보다 통합적이고 신속한 대응 체계 구축의 기반이 된다.

9. 정책 및 프로세스

디바이스 및 엔드포인트의 효과적인 관리와 보호를 위해서는 명확한 정책 수립과 체계적인 관리 프로세스가 필수적이다. 제로트러스트 보안 모델을 기반으로 한 관리 정책에는 기기 승인 절차, 인벤토리 등록 및 온보딩, 암호화 범위와 방식, 정기 백업 및 복구, 소프트웨어 관리, 보안 로그 모니터링, 감사 및 정책 검토 등 다양한 관리 항목이 포함되어야 한다. 이러한 항목들은 세부적인 운영지침과 실행 절차로 구체화되어야 하며, 조직 내 모든 구성원이 일관되게 준수할 수 있도록 체계적으로 관리할 필요가 있다.

특히, 디바이스 및 엔드포인트 관리 프로세스는 각 기기의 전체 라이프사이클을 아우르는 단계별 관리 체계를 수립하는 것이 중요하다. 신규 기기의 도입·배포, 사용 중 보안 유지, 운영 소프트웨어의 정기적 업데이트 및 취약점 관리, 사용 종료 후 반납과 폐기, 외부 반출이나 이동식 매체 사용에 대한 별도 절차까지, 각 단계별로 표준화된 운영 프로세스를 마련해야 한다. 조직은 이러한 프로세스 정립을 통해 보안 수준을 높이고, 실시간 자산 현황 파악 및 효율적인 리소스 배포·운영을 달성할 수 있다.

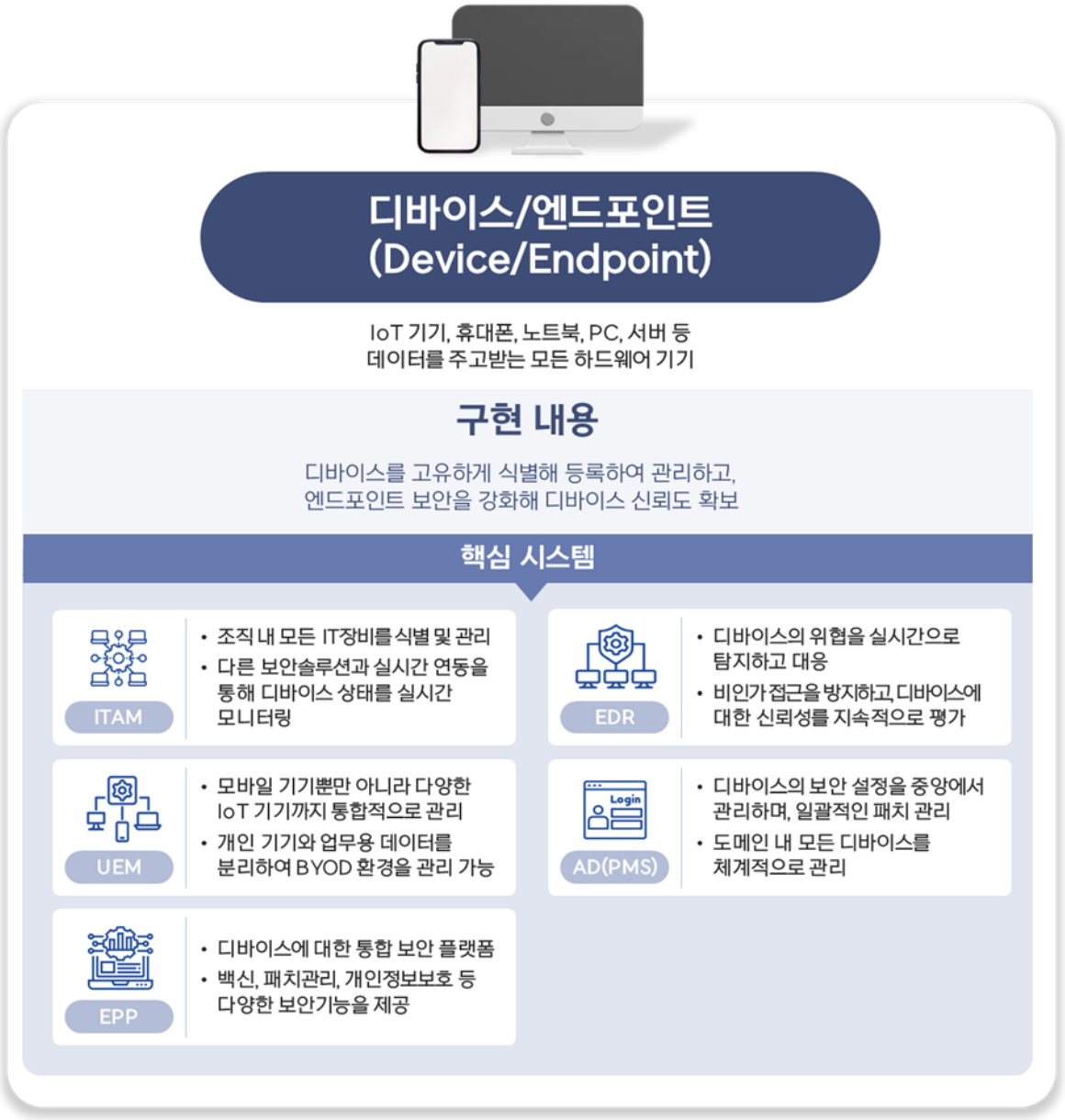
정책과 프로세스의 정교화는 디바이스 및 엔드포인트 영역의 일관된 보안 태세 유지와, 변화하는 업무 환경에서의 신속한 위험 대응에 반드시 필요한 과정이다.

이러한 주요 요소들을 기반으로, 디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처의 실질적인 보안 통제 축이 된다. 조직 내 모든 디바이스의 신뢰성과 보안 상태를 정밀하게 관리하고, 실시간으로 검증함으로써 사용자의 신원뿐만 아니라 실제 접속에 활용되는 기기의 위험까지도 일관성 있게 통제할 수 있다. 내·외부 위협으로부터 핵심 자산을 효과적으로 보호하며, 변화하는 업무 환경과 진화하는 사이버 위협에 신속하게 대응할 수 있는 유연성과 확장성을 제공한다. 디바이스 및 엔드포인트 필러의 고도화는 조직의 보안 정책과 관리 프로세스가 실질적으로 구현되는 기반이 된다.

■ 주요 시스템별 제로트러스트 기능 구현

제로트러스트 환경을 성공적으로 구현하기 위해서는 기술적 방안과 이를 수행하는 시스템이 필수적이다. 제로트러스트 아키텍처는 "신뢰하지 않고 항상 검증한다"는 원칙을 기반으로 한다. 이를 실현하기 위해 사용자와 엔터티의 신원을 확인하고, 지속적으로 검증하며, 최소 권한 접근 보장을 수행하는 시스템이 반드시 갖춰져야 한다.

아래 주요 시스템 등은 각각 제로트러스트 환경에서 중요한 역할을 담당하며, 상호 연계되어 조직의 보안 태세를 강화할 수 있다. 각 시스템 별로 제로트러스트 환경 구현을 위해 수행해야 할 기능과 이를 통해 조직이 얻을 수 있는 보안 강화 효과를 구체적으로 살펴보고자 한다.



출처 : SK 쉴더스, "제로트러스트의 시작:SKZT 로 완성하다"

그림 2. 디바이스/엔드포인트 주요 시스템

1. ITAM (IT Asset Management, IT 자산관리시스템)

ITAM(IT 자산관리) 시스템은 제로트러스트 아키텍처에서 디바이스 및 엔드포인트의 인벤토리로서 출발점이자 기반 인프라로 기능해야 한다. 조직은 모든 IT 및 OA 자산(PC, 노트북, 모바일, 서버, 프린터, IoT 장비 등)에 대해 도입, 등록, 사용, 이동, 반출, 폐기 등 전 라이프사이클을 아우르는 관리 체계를 마련해야 하며, 자산 정보가 실시간으로 정확하게 반영될 수 있도록 자동화된 등록·변경·삭제 프로세스를 구축해야 한다. ITAM 은 각 조직의 업무 환경에 따라 별도의 상용 솔루션을 커스터마이징 후 도입하거나, 자체 SI(시스템 통합) 개발을 통해 구축할 수 있다.

ITAM 은 각 디바이스에 대한 자산번호, 바코드, 소유자, 소속 부서, 위치, 용도, 운영체제, 소프트웨어 설치 현황, 보안 등급, 연결 이력 등 다양한 속성 정보를 통합 관리할 수 있어야 한다. 신규 자산이 도입되거나 반출·폐기 등 상태 변경이 발생할 경우, 인벤토리 시스템에 자동 반영되어 관리 공백이나 정보 누락 없이 전체 현황을 한눈에 파악할 수 있도록 해야 한다. 특히 네트워크 접근이 가능한 디바이스에 대해서는 미등록 자산이 조직 네트워크에 접속하는 경우 자동으로 탐지·차단하거나, 보안 담당자에게 즉시 알림이 전달되도록 해야 한다.

ITAM 은 자산관리 고유 기능을 넘어서, EDR, UEM, AD, ICAM, ZTNA 등 주요 보안 솔루션과 연동하여, 인벤토리 정보의 최신성과 정합성을 유지하고, 실제 네트워크 환경에서 일어나는 변화까지 실시간으로 반영할 수 있어야 한다. 자산별 보안 상태(예: 패치 적용 현황, 취약점 점검 결과, 위험 등급, 접근 이력 등)는 ITAM 과 보안 시스템 간 데이터 교환을 통해 지속적으로 업데이트되며, 이를 기반으로 디바이스의 접근 통제·격리·추가 인증 등 동적 정책이 적용될 수 있다.

제로트러스트 환경에서는 등록되지 않은 디바이스의 네트워크 접근을 원천적으로 차단해야 하며, 반입·반출·폐기 등 주요 자산 흐름에 대해서는 추적성과 기록 관리를 통해 감사 및 사고 대응에도 활용할 수 있도록 해야 한다. 또한 ITAM 은 자산 반입 시 기본 보안점검(초기 상태 확인, 악성코드 탐지 등), 사용 중 정기 상태 점검, 반출·폐기 시 데이터 완전 삭제 및 인증 기록 보관 등 전체 라이프사이클에 걸쳐 보안 요건이 내재화될 수 있도록 연계되어야 한다.

관리자는 ITAM 을 통해 자산의 사용 현황, 이상 징후, 보안 정책 위반 사례 등을 한눈에 파악하고, 조직 내 어디에서 어떤 디바이스가 어떤 목적으로 운영되고 있는지 실시간으로 관리할 수 있다. ITAM 시스템은 내부·외부 보안 감사, 규제 대응, 침해사고 분석 등 다양한 요구사항에도 즉시 대응할 수 있도록 정확성, 추적성, 신뢰성을 갖춘 관리 환경을 제공해야 한다.

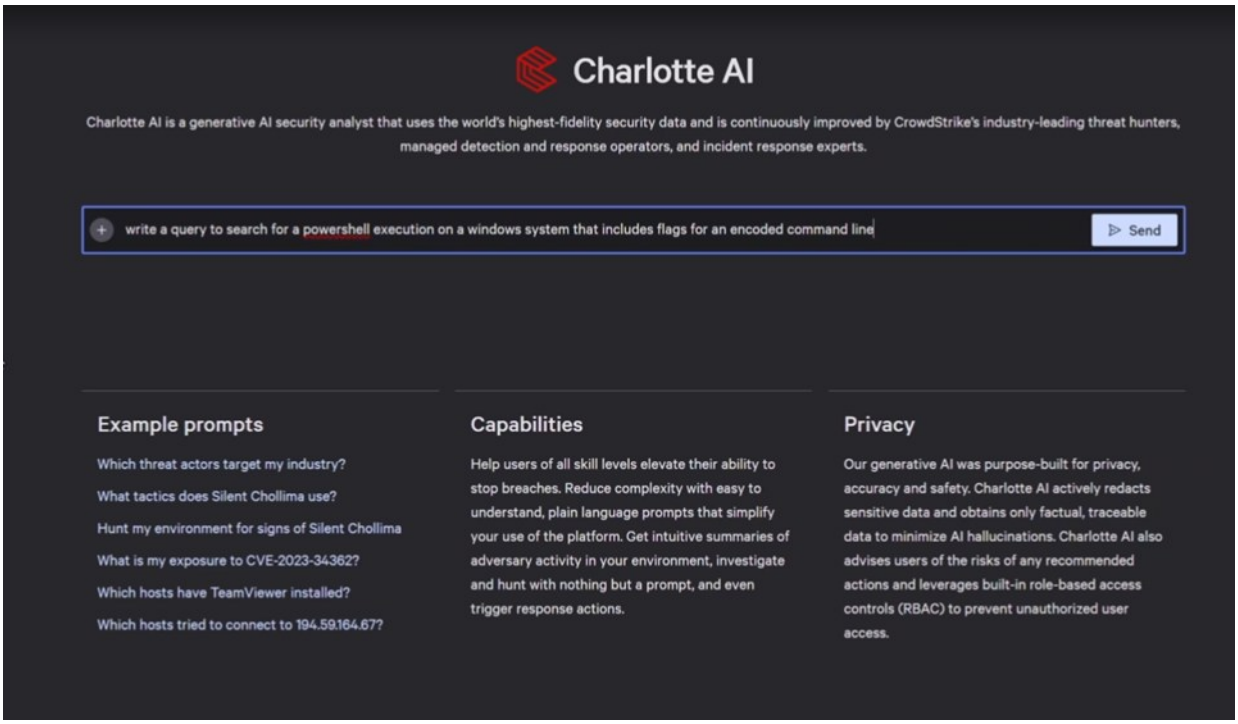
ITAM 의 고도화는 조직이 디바이스 및 엔드포인트 신뢰성 검증을 실질적으로 수행하는 기반이 되며, 네트워크 접근 통제 및 자산 보호 정책의 출발점으로 작동해야 한다. 이를 통해 조직은 제로트러스트 원칙에 따라 모든 디바이스에 일관된 접근 정책을 적용하고, 내부·외부 위협에 대한 실시간 대응력을 크게 향상시킬 수 있다.

2. EDR(EndPoint Detection & Response, 엔드포인트 탐지 및 대응)

EDR 은 PC, 노트북, 서버 등 조직의 모든 엔드포인트 단말에 설치되어, 실행 중인 프로세스, 파일 변경, 사용자 행위, 네트워크 활동 등 다양한 정보를 실시간으로 수집·분석하고, 이상 행위나 침해 징후를 탐지하여 신속한 대응까지 아우르는 고도화된 보안 시스템이다. 기존에는 안티바이러스(Anti-Virus) 알려진 악성코드 차단에 집중했었다. EDR 은 알려지지 않은 위협이나 내부자 이상행위, 제로데이 공격 등까지 대응 범위를 확장하며 엔드포인트 보안의 핵심으로 자리 잡고 있다.

EDR 은 단순한 위협 탐지 기능을 넘어, 실제 업무 환경에서 발생하는 다양한 보안 이벤트를 실시간으로 상관분석하고, 각 단말별 보안 상태와 취약점, 이상 행위, 비인가 소프트웨어 실행 등 복합적인 위협 징후를 한눈에 파악할 수 있는 통합 대시보드를 제공한다. 주요 EDR 제품은 프로세스 간 행위 추적, 메모리 기반 공격 탐지, 파일 및 네트워크 포렌식, 취약점 자동 탐지, 사용자별 행동 패턴 분석 등 고도화된 기술을 적용하여, 보안 담당자가 이상 상황을 신속히 인지하고, 자동 또는 수동으로 적절한 대응조치를 취할 수 있도록 지원한다. 또한, 자동화된 인시던트 대응 플레이북, 감염 단말 자동 격리, 위협 지표(IOC) 실시간 업데이트, 샌드박스 연동 분석 등 고급 대응 기능까지 점차 표준화되고 있다.

글로벌 EDR 솔루션들은 인공지능(AI)과 머신러닝 기반 탐지 및 분석, 프롬프트(자연어) 입력을 통한 정책 자동화 등 최신 기술을 적극적으로 도입하고 있다. 예를 들어 아래 '그림 3'과 같이 관리자가 영어로 "특정 명령 줄 플래그가 포함된 PowerShell 실행 탐지 정책을 생성해줘"라고 프롬프트를 입력하면, AI 가 관련 탐지 룰을 자동 생성·적용한다. 또한, AI 기반 위협 인텔리전스와 연동하여 실시간으로 신규 공격 유형이나 공격자의 행동 패턴을 반영하고, 정책 수정 및 룰 등록이 훨씬 직관적으로 이루어질 수 있다. 이와 함께, 위협 사냥(Threat Hunting) 기능과 자동화된 포렌식, 경보 우선순위 조정, 행위 기반 위험 점수 할당, 대응 프로세스 최적화 등 조직 규모와 환경에 따라 맞춤형 보안 운영을 지원하는 다양한 기능도 제공되고 있다.



출처 : CrowdStrike, "Conversations with Charlotte AI Demo"

그림 3. 프롬프트 입력을 통한 정책 쿼리 생성 화면

제로트러스트 아키텍처에서는 EDR 이 각 디바이스 및 엔드포인트의 신뢰성 검증을 위한 필수 수단으로 기능해야 한다. EDR 은 단순히 위협 탐지에 머무르지 않고, 감지된 위험 요소에 따라 접근 제한, 네트워크 격리, 추가 인증 요구 등 다양한 대응 정책을 자동화할 수 있어야 한다. 또한 SSO, IAM, MFA, ICAM 등 접근제어 시스템과 연동하여, 위협이 발생한 기기나 사용자의 접근 권한을 즉시 조정하고, 사고 확산을 효과적으로 차단할 수 있는 체계 마련이 중요하다.

최근 EDR 의 탐지·대응 범위를 사용자·네트워크·시스템·클라우드 등으로 확장하는 XDR(eXtended Detection and Response) 개념이 부상하고 있으나, 실제로는 데이터 연계 범위, 벤더 종속성, 표준 부재 등의 한계로 완전한 XDR 구현이 쉽지 않은 상황이다. 이에 따라 많은 조직은 EDR, NDR, SIEM/SOAR 등 각 필러별 전문 시스템을 별도로 구축하고, 상호 연동을 통해 현실적인 제로트러스트 보안 체계를 실현하는 방식을 택하고 있다.

EDR 도입을 통해 조직은 단순한 악성코드 차단을 넘어, 다양한 위협 유형과 공격 벡터에 실시간으로 대응하고, 디바이스 및 엔드포인트의 보안 신뢰도를 효과적으로 관리할 수 있다. 또한, AI 기반 자동화와 직관적 정책 관리, 상호 연동성 향상 등 기술 고도화를 바탕으로, 제로트러스트 환경에서 필요한 실시간 보안 검증과 대응 능력을 갖출 수 있다.

3. UEM (Unified Endpoint Management, 통합 엔드포인트 관리)

조직 내 디바이스와 엔드포인트는 한때 PC 와 노트북 등 전통적인 IT 기기에 국한되어 있었으나, 업무 환경의 변화에 따라 스마트폰, 태블릿, 웨어러블, IoT, 그리고 개인 소유의 BYOD(Bring Your Own Device)까지 다양한 형태로 빠르게 확장되었다. 이러한 변화는 디바이스 관리의 복잡성을 크게 높였고, 단일 플랫폼에서 모든 단말을 효과적으로 통합 관리해야 할 필요성이 대두됐다.

환경 변화에 대응하기 위해, 엔드포인트 관리 기술 역시 MDM(Mobile Device Management)에서 EMM(Enterprise Mobility Management), 그리고 UEM(Unified Endpoint Management)으로 진화해왔다.

MDM 은 모바일 단말(스마트폰, 태블릿 등)에 대한 원격 제어와 보안 관리 기능에 초점을 맞췄으나, 점차 모바일 업무가 확대되고 디바이스의 종류가 다양해지면서 한계가 드러났다.

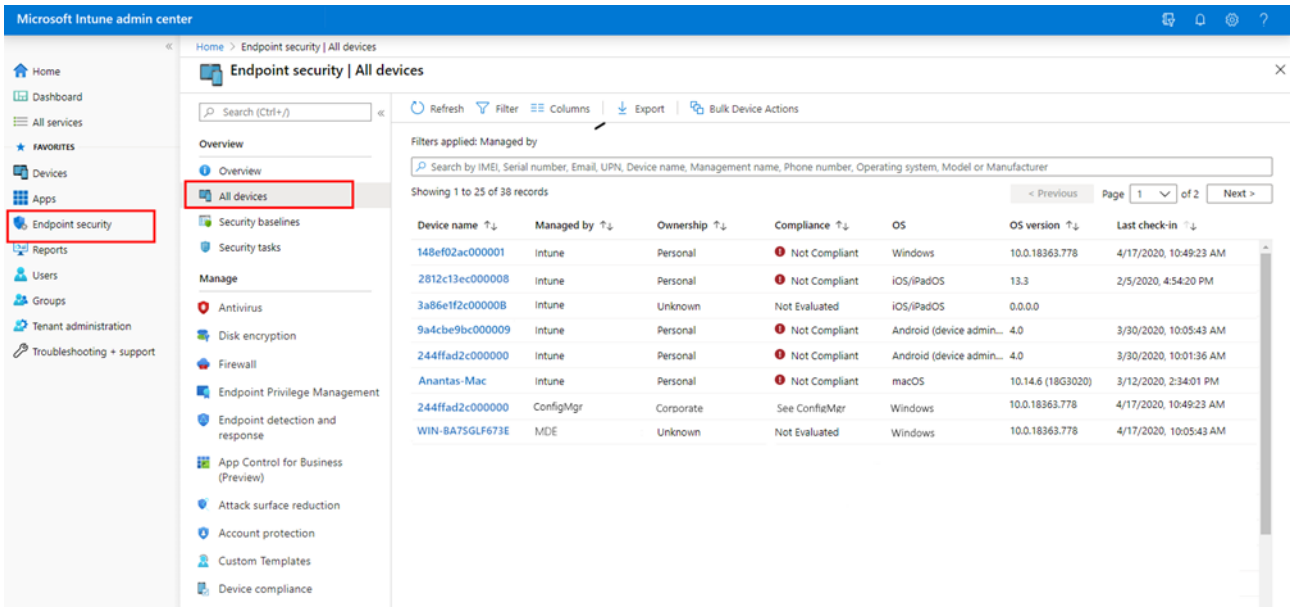
EMM 은 이러한 한계를 극복하기 위해 등장한 개념으로, 모바일 디바이스 관리(MDM)뿐만 아니라, 앱 관리(MAM), 콘텐츠 관리(MCM), 이메일·네트워크 보안 등 모바일 환경 전반을 포괄적으로 제어할 수 있게 기능이 확장됐다. 업무용·개인용 앱과 데이터의 분리, 정책 기반의 접근 제어, 클라우드 연계 등 EMM 을 통해 모바일 업무 환경의 보안성과 유연성이 한층 높아졌다.

UEM 은 EMM 의 기능을 더욱 확장하여, PC, 노트북, 스마트폰, 태블릿, 웨어러블, IoT, BYOD 등 조직 내 모든 IT 자산과 엔드포인트를 단일 플랫폼에서 통합 관리하는 체계를 제공한다. 단순한 모바일 관리 수준을 넘어, 운영체제와 장비 유형, 업무 환경을 불문하고 모든 디바이스의 등록·인증·정책 배포·보안 관리·애플리케이션 제어·취약점 점검·데이터 유출 방지·실시간 모니터링 등을 일원화한다.

UEM 은 제로트러스트 보안 아키텍처에서 모든 엔드포인트의 상태와 신뢰도를 실시간으로 검증하고, 미승인 또는 취약한 기기의 네트워크 접근을 제한하거나 격리할 수 있는 강력한 통제 기능을 제공해야 한다. 업무용·개인용, 내부·외부 소유를 불문하고 모든 디바이스의 보안 상태, 정책 준수 여부, 실시간 행위 분석 결과를 기반으로 접근 권한과 보안 정책을 동적으로 조정하는 것이 가능하다.

특히 UEM 은 기존의 EDR 이나 IT 자산관리 시스템만으로는 대응이 어려운 영역을 포괄적으로 통제할 수 있다는 점에서 차별성을 가진다. 예를 들어, EDR 이나 자산관리 솔루션은 PC, 서버 등 일반적인 IT 자산에 높은 수준의 통합·탐지·대응 역량을 제공하지만, 모바일 기기나 태블릿, BYOD, IoT 등 다양한 운영체제와 장비에는 에이전트 호환성 문제, 설치 제약, 통제 한계 등의 문제가 발생할 수 있다. UEM 은 이런 다양한 단말 환경과 보안 과제를 단일 플랫폼에서 통합적으로 관리할 수 있는 체계를 제공한다. 하지만, 국내외 실제 구축 사례는 아직 많지 않고, 조직 환경에 맞는 맞춤형 도입 및 운영이 쉽지 않다는 한계가 있다.

제로트러스트 아키텍처를 실질적으로 구현하기 위해서는 UEM 과 같은 통합 엔드포인트 관리 플랫폼의 도입과 고도화를 적극적으로 추진할 필요가 있으며, 엔드포인트 관리 체계 전반의 성숙도를 끌어올리는 노력이 병행되어야 한다.



출처 : Microsoft, “Technical documentation”

그림 4. MicroSoft Intune, UEM 콘솔 화면

4. AD(Active Directory/PMS, 패치 및 자산 관리)

Active Directory(AD)는 마이크로소프트 사가 제공하는 대표적인 디렉터리 서비스로, 조직 내 PC, 노트북, 서버 등 다양한 디바이스를 도메인 단위로 통합 관리하는 핵심 시스템이다. 기존에는 사용자 계정과 그룹 권한 관리에 주로 활용되었지만, 실제 기업 환경에서는 디바이스 등록·승인·삭제·정책 배포 등 엔드포인트 관리의 기반 인프라로 작동하고 있다.

AD 는 디바이스가 도메인에 가입되는 순간, 해당 기기의 보안 정책 적용, 접근 권한 부여, 패치·설정 일괄 배포, 인증 로그 집계 등 다양한 운영·보안 절차를 중앙에서 일괄 관리할 수 있도록 한다. 온프레미스 AD 뿐만 아니라, Microsoft Entra ID(구 Azure AD)와 연동된 하이브리드 환경에서도 동일하게 PC, 노트북, 태블릿, 일부 IoT 장비까지 디바이스의 통합 관리를 지원한다.

제로트러스트 관점에서 AD 는 단순한 디렉터리 서비스가 아닌, 엔드포인트 라이프사이클 전체를 관리하는 '디바이스 PMS(패치 및 자산 관리 시스템)'로 역할이 확장됐다 할 수 있다. 예를 들어, 도메인 가입된 모든 디바이스의 소유자, 위치, 사용 이력, 보안 상태(패치 적용 여부, 보안 정책 준수 등)를 실시간으로 집계·모니터링하고, 그룹 정책(GPO)이나 Intune(UEM) 등과 연동해 자동화된 보안 설정, 소프트웨어 배포, 이상 행위 탐지 및 격리 등 다양한 통제 체계를 일괄 적용할 수 있다.

또한, AD 와 연동된 UEM, EDR, ICAM, ZTNA 등 주요 보안 솔루션들은 AD 에서 제공하는 디바이스 속성 정보와 인증 기록을 활용해, 네트워크 접근 통제·격리·추가 인증 등 동적 정책을 구현한다. 이는 미승인·미등록 디바이스의 자동 탐지 및 네트워크 차단, 패치 미적용 기기 경고, 주요 자산 접속 기기 실시간 모니터링 등, 실질적인 엔드포인트 보안 통제의 기반이 된다.

최근에는 온프레미스 AD 뿐 아니라, 클라우드 기반 Entra ID 와 연동해 하이브리드 환경의 단말까지 통합 관리하는 사례가 빠르게 확산되고 있다. 디바이스 인벤토리, 패치 관리, 정책 배포, 위험도 평가 등 다양한 관리 기능을 점차 AD 기반으로 일원화하는 방향으로 발전할 것으로 보인다.

AD는 제로트러스트 아키텍처에서 사용자와 디바이스 모두를 아우르는 통합 인벤토리 및 정책 관리 엔진으로 기능해야 한다. AD 의 관리 범위와 데이터 정확성, 보안 통제력은 조직 내 모든 엔드포인트의 신뢰성 검증과 접근 통제, 정책 일관성 확보에 직결된다. AD 와 연계된 각종 보안 시스템이 제공하는 실시간 통합 관리는 조직 전체의 운영 효율성과 보안 수준을 한층 높일 수 있는 토대가 된다.

5. EPP (Endpoint Protection Platform, 엔드포인트 보호 플랫폼)

EPP 는 단일 플랫폼에서 엔드포인트(PC, 노트북, 서버 등)에 대한 다양한 보안 기능을 통합적으로 관리하고 제공하는 제품군을 의미한다. 본래 안티바이러스(AV)나 안티멀웨어를 중심으로 출발했지만, 최근에는 EDR, UEM, PMS, 취약점 진단 등 다양한 엔드포인트 보안 기능이 하나의 제품군으로 융합되는 방향으로 진화하고 있다.

EPP 는 통상적으로 하나의 콘솔에서 조직 내 여러 엔드포인트의 실시간 상태 모니터링, 정책 배포, 위협 탐지, 이상행위 분석, 취약점 점검, 패치 관리, 소프트웨어 설치 현황 파악 등 주요 보안 관리 업무를 일괄적으로 지원한다. 이런 통합적 관리 프레임워크는 운영 편의성과 가시성 측면에서 높은 효과를 제공하며, 실제 시장에서도 EPP 는 AV, EDR, PMS 등 다양한 엔드포인트 보안 솔루션을 통합해 라이선스를 판매하는 형태가 주류를 이룬다.

하지만, 실제 구현 단계에서 EPP 가 모든 엔드포인트 보안 시스템을 완전히 통합 관리하는 것은 제한적이다. 특히 대부분의 EPP 제품은 특정 벤더(제조사) 소프트웨어에 한정하여 통합 기능을 제공하며, 서로 다른 벤더의 보안 제품 간에는 연동의 한계가 존재한다. 이는 제로트러스트 환경에서 요구하는 '다양한 보안 시스템간 연동'이나, 조직 전반의 위협 정보, 정책, 인증 기반을 중앙에서 유연하게 다루는 데 있어 근본적 한계로 작용한다.

물론, 일부 조직에서는 다양한 벤더의 엔드포인트 보안 솔루션에서 제공하는 API 를 통합해 별도의 정보보안 포털이나 통합 관리 시스템을 자체적으로 구축하는 사례도 있다. 하지만, 시장에서 'EPP'라는 용어가 통용될 때는 대체로 벤더 중심의 제품군 혹은 솔루션을 의미하는 경우가 많다.

제로트러스트 환경에서 EDR, UEM, NDR, ZTNA, DSPM, SIEM&SOAR 등 필러별 주요 보안 시스템들은 각 필러별 영역에서 정책결정지점(PDP) 및 정책시행지점(PEP)의 역할을 수행할 수 있다. 하지만, 이러한 시스템들이 각각의 독립적 관점에서만 정보를 수집·통제하는 경우, 조직 전체에서 일관성 있는 정책 적용과 실시간 위험 대응, 보안 운영의 통합성이 저하될 수 있다.

제로트러스트 환경에서 궁극적으로 지향해야 할 것은, 각 필러별 보안 시스템이 제공하는 정보(PIP)를 ICAM(Identity, Credential and Access Management) 등 최상위 통합 플랫폼으로 연계하고, 식별자·엔드포인트·네트워크·데이터 등 조직 전반에 걸친 정보 기반의 통합 정책 및 접근 통제체계를 구현하는 것이다. ICAM 은 각 필러에서 전달되는 신원, 인증, 상태, 위험, 정책 이슈 등을 통합적으로 분석·판단하며, 조직 전체의 접근 정책(PDP)과 정책 집행(PEP) 역할을 중앙에서 일관되게 수행할 수 있어야 한다.

결국, EPP 를 비롯한 각종 영역별 보안 플랫폼을 개별적으로 운용하는 것은 제로트러스트의 전체론적 통합 아키텍처를 구현하는 데에 본질적 한계가 존재한다. 각 시스템이 정보를 제공하고 정책 집행에 참여할 수 있지만, 최상위 통합 관리체계인 ICAM 을 통해 조직 전체의 리스크와 정책을 통합적으로 통제하는 방향이 제로트러스트 보안 체계의 근간이 되어야 한다.

기기/엔드포인트 필러의 각 시스템은 단순한 기능 단위를 넘어, 제로트러스트 아키텍처를 기술적으로 구현하는 실질적인 수단으로 작동해야 한다. ITAM, EDR, UEM, AD, EPP 등은 각기 독립적으로 중요한 역할을 수행하되, 상호 유기적인 연동과 정보 공유를 통해 조직 내 모든 디바이스의 신뢰성 검증, 위험 탐지, 정책 집행이 일관되게 이뤄질 수 있도록 한다.

이러한 주요 시스템들의 기술적인 구현과 연계는 업무 환경과 디바이스 유형이 다양해지는 상황에서도, 일관된 보안 정책과 정밀한 통제를 구현할 수 있는 기반을 제공한다. 조직은 제로트러스트 환경 하에서 다양화되는 업무 환경과 디바이스 유형에 유연하게 대응하면서, 엔드포인트 보안의 신뢰성과 운영 효율성을 실질적으로 높일 수 있을 것이다.

■ 맺음말

제로트러스트 아키텍처에서 기기 및 엔드포인트(Device/Endpoint)는 단순한 업무 도구를 넘어, 조직의 모든 보안 전략을 실현하는 실질적이며 핵심적인 보안 요소이다. ITAM, EDR, UEM, AD, EPP 와 같은 주요 시스템들은 각각 독립적인 보안 기능을 수행하는 동시에, 상호 긴밀한 연계를 통해 모든 디바이스의 신뢰성을 평가하고, 실시간 위협을 탐지하며, 통합적인 정책 관리를 가능하게 한다.

디바이스 및 엔드포인트 필러의 정교한 설계와 운용은 조직의 모든 디바이스에 대한 철저한 보안 관리를 보장하는 동시에, 조직이 다양한 업무 환경과 지속적으로 진화하는 사이버 위협에도 유연하게 대응할 수 있는 '구조적 토대'를 제공한다. 특히 사용자의 신원과 디바이스의 신뢰성을 함께 검증하고 관리하는 접근 방식은 제로트러스트 환경에서 요구되는 일관되고 강력한 보안 통제를 구현하는 핵심 원칙이 된다.

제로트러스트 기반의 통합적 관리 체계는 디바이스의 유형과 사용 환경이 점차 다양화되고, 위협이 정교해지는 상황 속에서도 조직이 보다 효과적으로 위협을 예방하고 신속히 대응할 수 있도록 돕는다. 이는 단순히 개별 솔루션의 효용성을 넘어, 조직의 전반적인 보안 수준과 운영 효율성을 획기적으로 향상시키는 데 기여할 수 있다.

결론적으로 디바이스 및 엔드포인트 필러는 제로트러스트 아키텍처의 핵심적이고 필수적인 구성요소이며, 조직의 디지털 자산 보호를 위한 실질적인 기술 기반을 마련한다. 조직은 이 필러를 중심으로 기술적 고도화와 관리 체계의 정교화를 지속적으로 추진함으로써, 디지털 환경의 복잡성과 리스크를 실질적으로 관리 가능한 수준으로 낮추고, 지속 가능한 디지털 보안 환경을 실현할 수 있을 것이다.

■ 참고 문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] NIST SP 1800-22, “Mobile Device Security: Bring Your Own Device (BYOD)”, 2023.09

[3] DoD, “Zero Trust Overlays”, 2024.06

[4] 과학기술정보통신부/KISA, “제로트러스트 가이드라인 V1.0”, 2023.06

[5] 과학기술정보통신부/KISA, “제로트러스트 가이드라인 V2.0”, 2024.12

■ 참고 자료

[1] SK쉴더스, “제로트러스트의 시작:SKZT로 완성하다” – 브로슈어

[2] Gartner, “Best Endpoint Protection Platforms Reviews 2025”

[3] Expel, “Expel Quarterly Threat Report, Q1 2025: Endpoint threats”

[4] CrowdStrike, “CrowdStrike Falcon guides”

[5] SentinelOne, " SentinelOne Resource Center, Documentation"

[6] Microsoft, “Microsoft Defender for Endpoint”