ORACLE

제로 트러스트, 복원력은 최대로

‘신뢰는 금지, 검증은 필수’ 꼭 읽어야 할 보안 가이드

목차

제로 트러스트 보안을 지금 바로 적용해야 하는 이유

By Lorna Garey
Senior Writer

보안에 관한 더욱 선제적인 접근 방식이 필요한가요? 미 국방부는 제로 트러스트 아키텍처 도입을 가속화해 2027년으로 예정되었던 도입 기한을 무려 12개월 앞당겼습니다. 한 업계 조사 기관이 다양한 산업 분야의 IT 및 사이버 보안 전문가 약 650명을 대상으로 조사한 결과에 따르면, 응답자 중 약 3분의 1 이상이 이미 제로 트러스트 전략을 구현했고, 47%가 1년 이내에 도입할 계획이었던 것으로 나타났습니다.

아직 제로 트러스트 전략을 고려하고 있지 않은 기업은 그와 같이 중대한 전략적 전환을 주도하는 요인들이 무엇인지 살펴볼 필요가 있습니다.

제로 트러스트 보안(경계 없는 보안)은 빈번한 인증 및 권한 부여, 암호화, 철저한 세분화 등을 통해 자산을 보호합니다. 기본적으로 네트워크 내부 또는 외부의 개인, 기기, 애플리케이션 등의 모든 엔티티를 신뢰하지 않습니다. 조직은 언제나 시스템이 이미 침해되었다고 가정하고 사용자, 서비스, 기기를 지속적으로 모니터링 및 재인증합니다. 요청의 맥락, 신뢰 수준, 자산의 민감도 등의 데이터에 기반해 액세스 권한을 부여하고, 작업 수행에 필요한 최소한의 권한만 허용합니다. 세분화를 통해 재인증 없이 접근 가능한 범위를 제한하여 공격자가 네트워크를 자유롭게 이동하는 것을 차단하고 침해 사고 대응 시간을 단축합니다.

이는 기존의 '성곽과 해자(castle and moat: 경계 기반 보안 방식) 모델과는 매우 다른 극적인 변화입니다. 단계적으로 진행되는 것이 일반적인 제로 트러스트로의 전환 과정에는 많은 노력, 자원, 협력이 필요합니다. 그러나 이는 2025년 이후 대부분의 기업이 직면하게 될 위협에 대비하기 위한 필수적인 조치로 볼 수 있습니다. 보안을 위한 통제는 자동차의 브레이크에 비유할 수 있습니다. 언제든 멈출 수 있다는 확신을 가지고 빠르게 달릴 수 있도록 해주는 장치입니다. 충분한 보안 태세를 갖추지 못한 기업의 IT 리더들은 신기술 도입과 민감한 데이터 사용에 더 신중한 태도를 취하게 될 것입니다.

제로 트러스트의 수혜자들

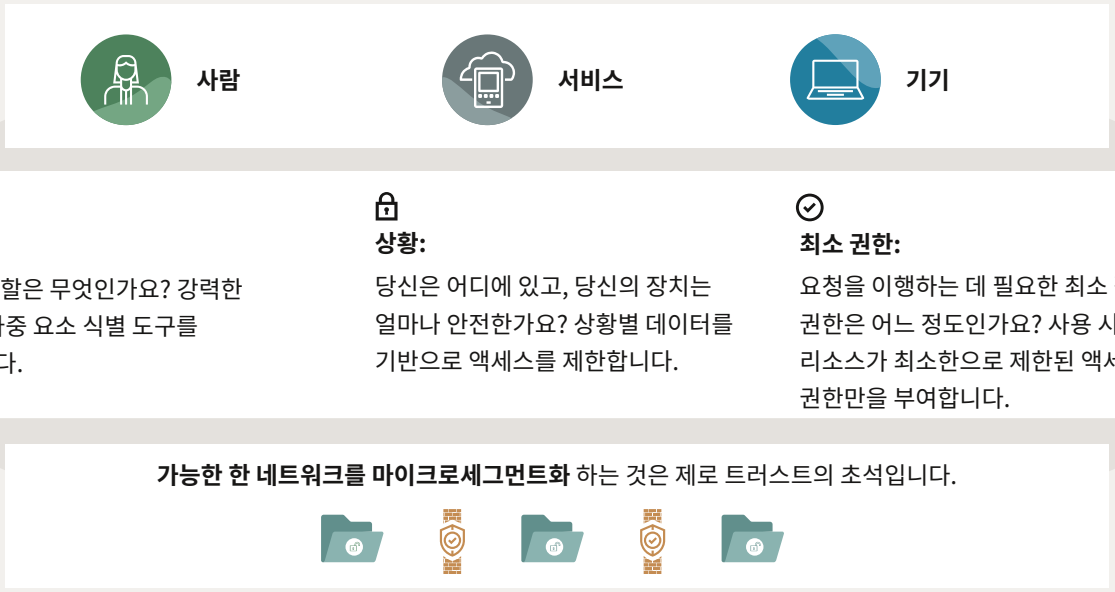
제로 트러스트 접근법은 네트워크 경계뿐만 아니라 네트워크 전역에 보안 통제 수단을 전략적으로 배치합니다. 이러한 방식은 제로 트러스트 아키텍처를 클라우드에서 워크로드를 운영하고, 신뢰할 수 있는 파트너사와 데이터를 공유하고, 원격 근무 및 다양한 기기를 지원하는 기업에 특히 효과적인 보안 수단으로 만들어 줍니다. 그러나 제로 트러스트는 클라우드 워크로드만을 위한 것이 아닙니다. 온프레미스, 하이브리드, 클라우드 환경 전반에 관련 원칙을 표준화해야만 성공적인 결과를 얻을 수 있습니다.

미국 국방부는 제로 트러스트를 전면 도입한 극도로 복잡한 생태계의 좋은 예시입니다. 미국 국방부의 사이버보안 담당 최고정보부책임자인 David McKeown은 자신의 팀이 새로운 도구 및 기능 통합, 제로 트러스트 기능이 내장된 상용 클라우드 솔루션 도입, 전용 온프레미스 프라이빗 클라우드 활용을 비롯한 하이브리드 구현 방식을 취하고 있다고 공식적으로 밝혔습니다.

미국 국방부의 사례를 통해 알 수 있듯이 제로 트러스트 보안은 적절한 기술을 활용하는 것이 필수적인 것은 사실이지만 버튼 하나로 간단히 켜고 끌 수 있는 제품 또는 서비스는 아닙니다. 조직의 기존 문화, 철학, 워크플로 등을 조정해야 하는 새로운 작업 방식에 가깝다고 보아야 할 것입니다.

제로 트러스트의 작동 방식

신뢰할 수 있는 엔티티는 절대 없다고 가정하고 가능한 최소한의 권한과 꼭 필요한 액세스 권한만 부여합니다. 네트워크를 분할해 침입자의 활동 범위를 제한합니다.



제로 트러스트의 장점

경영진들은 제로 트러스트 도입 시점에 대해 "왜 지금 바로 도입해야 한다는 것입니까?"라는 의문을 품을 수 있습니다. 그 이유는 다양합니다.
생체 인식 및 비밀번호 외의 새로운 로그인 방식을 지원하는 소프트웨어, 서비스, 하드웨어가 늘어남에 따라 기업은 더 다양한 인증 수단을 사용할 수 있게 되었습니다.

또한 이제 생성형 AI가 다음과 같은 방식으로 제로 트러스트 아키텍처 구현을 지원합니다.

- 생성형 AI 기반의 자동화된 위협 탐지 시스템은 방대한 네트워크 트래픽과 시스템 로그를 분석해 이상 징후 및 잠재적 위협을 식별하고, 공격자에게 권한이 부여된 경우 실시간으로 차단할 수 있습니다.
- AI는 정상적인 사용자 행동에 대한 기준을 설정하고 패턴을 분석해 도난당한 자격 증명을 사용한 로그인, 중요 데이터의 다운로드 시도와 같은 비정상적 활동을 탐지할 수 있습니다.
- AI 에이전트는 프로비저닝 및 디프로비저닝을 자동화하여 인적 오류의 위험을 최소화합니다.

나아가 AI 에이전트는 제로 트러스트의 또다른 원칙인 각 시스템 또는 사용자에게 업무 수행에 필요한 최소한의 액세스 권한만을 부여하는 과정도 지원할 수 있습니다. 이상의 요소들이 결합되어 2025년에는 더 많은 기업이 제로 트러스트 모델을 도입할 것으로 전망되고 있습니다.

핵심 개념 : 신뢰 기기 SSO

Trusted device single sign-on(SSO)은 사용자가 신뢰된 기기를 사용하고 있을 경우, 한 번의 인증으로 여러 애플리케이션과 서비스에 접근할 수 있도록 하는 기능입니다.

이를 통해 로그인 과정을 단순화하고, 사용자가 입력해야 하는 비밀번호나 추가 인증 횟수를 줄여 보안성과 편의성을 동시에 향상시킬 수 있습니다.

SSO를 사용하기 위해서는 먼저 신뢰할 수 있는 기기를 등록해야 합니다. 등록 과정에는 기기의 사양과 보안을 확인하는 과정이 포함되는 경우가 많습니다. 기기가 신뢰된 상태로 등록되면, 사용자는 추가 인증 요소를 더 적게 요구받으며 로그인할 수 있습니다. 다만, IT 팀은 신뢰된 기기의 보안 상태 변화를 지속적으로 모니터링해야 합니다. 신뢰 상태는 언제든지 해제될 수 있으며, 기기가 위험한 상태로 판단될 경우(예: 위치 이상, 소프트웨어 미업데이트 등) 추가 인증이 요구되거나 보안 기준을 충족하기 위한 조치가 필요할 수 있습니다.

핵심 개념 : 자동화된 ID 거버넌스

ID 거버넌스는 기업 전반의 디지털 ID 및 접근 권한을 관리하기 위한 프로세스입니다. 관련 활동으로는 ID 수명 주기 관리 자동화, 강력한 액세스 제어에 기반한 액세스 정책 및 업무 분리 원칙 적용, 최소한의 권한만 부여하는 제로 트러스트 접근 방식에 부합하는 사용자 활동 모니터링 등이 있습니다.

첫 번째 영역인 ID 수명 주기 관리를 위해서는 계정의 자동 생성/수정/삭제 기능, 업무 분리 정책에 기반한 직무 및 책임에 따른 사용자 역할 할당, 관련 속성들에 기반한 세분화된 액세스 제어 정의 등이 필요합니다.

사용자 계정 및 민감한 데이터에 대한 액세스 정책 적용은 먼저 업무 수행에 필요한 최소 권한만 부여한 뒤, 권한 및 활동을 모니터링하고 정기적으로 검토 및 감사하여 이상 징후와 잠재적 위협을 탐지하고 업계 규제 및 내부 정책 준수 여부를 확인하는 방식으로 이루어집니다.

핵심 개념 : 피싱 방지 MFA 및 비밀번호 없는 액세스

피싱 방지 다중 인증(MFA)은 공격자가 일회용 비밀번호(OTP) 코드를 가로채지 못하도록 방지하는 방법이고, 비밀번호 없는 액세스는 비밀번호를 더 강력한 인증 방식으로 대체하거나 보완하는 보안 접근법입니다. 사용자는 스마트폰과 같은 신뢰할 수 있는 기기 외에도 지문이나 얼굴 인식과 같은 생체 인증 요소를 사용하여 인증할 수 있습니다. 기업은 비밀번호를 사용하지 않는 강력한 인증 수단인 물리적 보안 키를 발급할 수 있습니다. IT 부서는 이동 중인 사용자, 시스템을 정기적으로 사용하지 않은 사용자 등 각 인증 시도의 위험을 평가하고, 필요하다고 판단될 경우 추가적인 확인 단계를 요구할 수 있습니다.

비밀번호를 사용하지 않는 액세스는 비밀번호 관련 침해 위험을 낮추는 것 외에도 비밀번호 재설정 및 계정 잠금으로 인한 비용을 절감시켜 줍니다. AI도 기본적 얼굴 스캐닝 또는 음성 인식을 통해 사용자의 신원을 정기적으로 확인함으로써 보안을 더욱 강화하는 데 도움을 줍니다.

사전 구축된 접근 방식

기업은 제로 트러스트 접근 방식을 처음부터 직접 설계하지 않아도 됩니다. 여러 기관이 무료로 제공하는 제로 트러스트 모델 아키텍처와 기술 지침을 사용할 수 있기 때문입니다.

Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model
CISA는 미국의 주요 인프라 보호 및 사이버 보안 증진을 담당하는 기관입니다. CISA의 Zero Trust Maturity Model(ZTMM) Version 2.0은 5가지 핵심 요소 및 여러 포괄적 원칙으로 구성되어 있으며, 급변하는 비즈니스/보안/기술 환경에 적용할 수 있도록 설계되었습니다.
CISA

Defense Information Systems Agency Zero Trust Reference Architecture
아키텍처 전반에 제로 트러스트 보안 원칙이 적용된 본 문서는 미국의 국방부 및 기타 일부 정부 기관에서 사용되고 있습니다.
DISA

National Cyber Security Centre Zero Trust Architecture Design Principles
이 유연한 프레임워크는 제로 트러스트 네트워크 아키텍처 구현을 지원하는 8가지 원칙을 설명합니다. NCSC는 기업, 기관, 개인을 위한 조언과 지침을 제공하는 영국의 정부 기관입니다.
NCSC

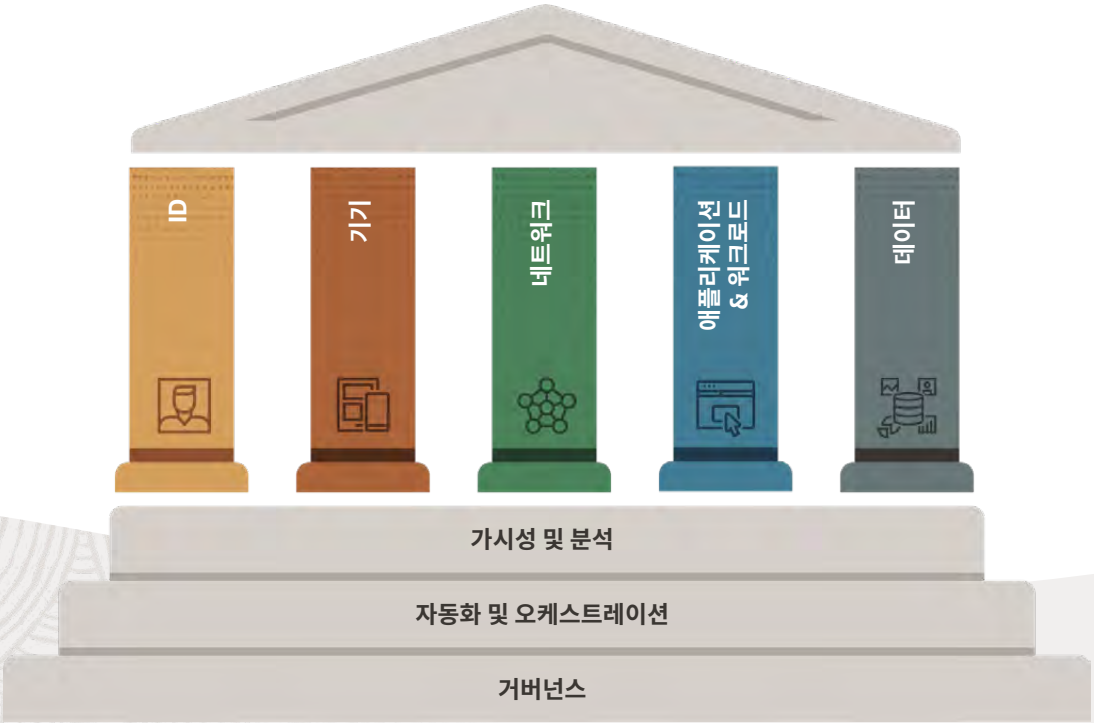
National Institute of Standards and Technology Zero Trust Architecture
Special Publication 800-207 프레임워크는 신원, 기기, 네트워크, 애플리케이션을 망라하는 제로 트러스트 구현을 위한 포괄적 접근 방식을 제공합니다. NIST는 혁신 및 산업 경쟁력 촉진을 지원하는 미국 상무부 산하의 비규제기관입니다.
NIST

성공을 위한 5가지 핵심 요소

사전 구축된 제로 트러스트 모델 중 상당수는 다양한 핵심 요소 및 원칙을 기반으로 구축되었습니다. 예를 들어, 미국 CISA ZTMM은 두 가지 핵심적인 전제에 기반합니다.

- 액세스 제어 적용을 가능한 한 세분화하여 권한이 없는 당사자가 데이터와 서비스에 접근하지 못하도록 차단하는 것을 목표로 합니다.
- 그 어떤 사용자 또는 자산도 신뢰해서는 안 됩니다. 언제나 침해가 이미 발생했거나 발생할 것이라고 가정하고, 그 어떤 엔티티에게도 경계에서의 단일 검증만으로 민감한 정보에 대한 액세스 권한을 부여해서는 안 됩니다. 모든 사용자, 기기, 애플리케이션, 서비스를 반드시 파악해야 하고 각 트랜잭션마다 지속적으로 검증해야 합니다. 또한 사용자 기기의 상태 및 행동을 지속적으로 평가 및 모니터링해야 합니다.

또한 ZTMM은 각 핵심 요소별 성숙도를 전통적 접근 방식부터 최적의 접근 방식까지 다양한 방식으로 차트화하여 팀이 각 영역에서 얼마나 잘 수행하고 있는지 평가할 수 있도록 합니다. ZTMM의 핵심 요소들 및 각 요소가 규정하는 내용에 대해 간략히 살펴보겠습니다.



핵심 요소 : ID

제로 트러스트 보안은 클라우드와 온프레미스 시스템 전반에 걸친 가시성을 제공하는 ID 거버넌스 및 관리 서비스로 뒷받침되는 강력한 ID 및 액세스 관리(IAM)를 전제로 합니다. ID는 사람, 애플리케이션, 기기 등의 신원을 의미하며, 특정 사용자의 본인 여부 및 파악된 기기 사용 여부를 검증하는 IAM 플랫폼을 통해 관리됩니다. 잘 구축된 IAM 플랫폼은 주요 ID 저장소 역할을 수행할 수 있지만, 많은 기업은 그 외에도 다양한 ID 관리 시스템을 사용하고 제로 트러스트 아키텍처를 구현하기 위해서는 그 모든 시스템을 관리해야 합니다.

> AI는 액세스 권한 및 클라우드 인프라 정책에 대한 인사이트를 제공하고 잠재적 이상 징후를 포착할 수 있는 데이터 분석 기반 액세스 보고서를 생성해 제로 트러스트 접근 방식에 기여합니다.

본 핵심 요소를 지원하는 다른 기술로는 속성 기반 액세스 제어(ABAC) 및 정책 기반 액세스 제어(PBAC) 기술을 함께 활용하는 역할 기반 액세스 제어(RBAC)가 있습니다. RBAC 시스템은 기업 및 애플리케이션 내 역할에 기반해 사용자에게 권한을 부여합니다. 또한 특정 역할의 사용자가 접근할 수 있는 데이터와 해당 데이터에 대한 작업 방식을 규정할 수도 있습니다.

ABAC는 시간대, 위치, 데이터 민감도 등의 추가적인 리소스 및 사용자 속성을 고려하는 보다 세분화된 접근 방식입니다. PBAC는 기업이 누가, 어떤 조건 하에서, 어떤 리소스에 액세스할 수 있는지 구체적으로 지정하는 규칙들을 기반으로 복잡한 정책을 정의할 수 있는 더욱 발전되고 유연한 시스템입니다. 정책 적용 지점(PEP)은 요청을 해당 규칙들과 비교해 평가함으로써 액세스 관리에 기여합니다. 예를 들어, 관련 정책에 따라 CRM 내 영업 실적 통계와 같은 특정 데이터로 인사 담당자의 데이터 열람 범위를 제한할 수 있습니다.

Extensible Access Control Markup Language(XACML) 표준이 보안 정책을 정의하지만, 기업은 선택한 액세스 제어 플랫폼이 자사의 핵심 애플리케이션과 호환되는지 직접 확인해야 합니다. 그와 관련해 기업 인프라의 다양한 계층별 정책 적용을 통합 관리할 수 있는 오픈 소스 기반의 유연한 정책 엔진인 Open Policy Agent가 XACML의 애드온으로 널리 사용되고 있습니다.

강력한 인증 역시 이 영역에서 중요한 요소입니다. 사용자는 액세스 과정에서 본인이 알고 있는 정보인 사용자명과 비밀번호(첫 번째 요소)를 먼저 제공한 뒤, 등록된 기기에서 생성된 코드 또는 지문과 같이 본인이 보유 중인 두 번째 요소를 추가로 제공해야 할 수 있습니다.

Just-in-time(JIT) 액세스 프로비저닝은 특정한 작업을 수행하는 데 필요한 최소한의 액세스 권한만을 필요한 기간 동안 부여하는 방식입니다. 액세스 권한은 요청 시마다 제공되고 더 이상 필요하지 않은 시점에 자동으로 취소됩니다.

핵심 요소 : 기기

기기는 스마트폰과 PC뿐만 아니라 기업이 보유한 데이터 센터나 클라우드 데이터 센터에서 사용되는 시스템까지 아우르는 개념입니다. CISA 모델의 예시에서 제로 트러스트를 위한 효과적인 기기 관리는 하드웨어, 소프트웨어, 펌웨어, 구성 등의 자산의 동적 인벤토리를 요구합니다. 일반적으로 권한 부여는 보수적으로 수행하고, 비활성 상태 또는 설정된 세션 기간을 기준으로 기기가 서버에 연결된 상태를 유지할 수 있는 시간을 제한하는 것이 좋은 관행입니다.

본 핵심 영역을 지원하는 기술은 엔드포인트 보안 및 모바일 기기 관리(MDM) 시스템에서 시작됩니다. 신뢰는 금지, 검증은 필수(never trust, always verify)' 원칙은 모든 액세스 요청이 철저히 인증되고 명시적으로 승인되어야 함을 의미하기 때문입니다. 엔드포인트 보안 솔루션은 데스크톱, 노트북, 서버 등 기기를 모니터링하여 보안 정책 준수 여부를 확인하고, MDM은 IT 부서의 모바일 기기 관리에 기여합니다. 이 두 기술이 결합되어 ID 및 상황별 정보에 기반해 액세스를 허용하는 강력한 보안 프레임워크 구축을 지원합니다.

엔드포인트 탐지 및 대응(EDR) 시스템은 노트북, 데스크톱, 서버 등의 기기에서 발생하는 위협을 탐지하고 대응하는 데 도움을 줍니다. EDR은 고급 분석 및 머신러닝을 활용해 데이터를 지속적으로 수집 및 분석함으로써 기기의 잠재적 오용이나 악성코드 감염 등을 식별할 수 있습니다.

핵심 요소 : 네트워크

제로 트러스트는 기존의 경계 중심 보안에서 벗어날 것을 요구합니다. CISA 예시에서 IT팀은 내부 트래픽 흐름을 세분화해 관리하고, 호스트를 격리하고, 암호화를 강제 적용하고, 활동을 세분화하고, 보안 통제 수단을 자산에 더 가깝게 배치하고, 전사적 네트워크 가시성을 확보해야 합니다. 이는 마이크로세그멘테이션(네트워크를 격리된 영역 분할, 영역 간 이동 통제, 가치있는 데이터 및 시스템에 더 엄격한 액세스 요구사항 적용)에 기반한 큰 도전 과제입니다.

여기서 사용되는 핵심 개념은 업무 분리(SOD)입니다. 성능 최적화를 위해 네트워킹팀은 네트워크를 관리해야 하고 보안팀은 액세스를 관리해야 합니다. 적절히 정의된 SOD 정책은 한 사람에게 민감한 프로세스나 거래에 대한 모든 통제권이 부여되지 않도록 방지하는 작업에 도움을 줍니다. 예를 들어, 사용자 계정 생성 및 관리를 담당하는 네트워크 관리자에게 보안 로그 항목 삭제 권한을 함께 부여하는 것은 바람직하지 않습니다.

핵심 요소 : 애플리케이션 및 워크로드

제로 트러스트는 온프레미스, 모바일 기기 및 클라우드에서 실행되는 애플리케이션과 워크로드에 모두 적용되는 원칙입니다. CISA는 소프트웨어 개발 수명 주기 전반에 걸쳐 보안 테스트를 내재화하고 모든 애플리케이션에 대한 자동화된 테스트를 수행할 것을 권장합니다.

클라우드 네이티브 개발 관행은 제로 트러스트 보안 모델에 도움을 줍니다. 모듈형 애플리케이션들은 마이크로서비스 아키텍처와 컨테이너화를 사용하여 구성 요소를 격리할 수 있기 때문입니다. 각 서비스는 독립적으로 운영되며 명시적으로 허용되지 않는 한 다른 서비스에 대한 액세스 권한은 최소화됩니다.

오늘날의 데이터 유출 사고 중 80% 이상은 직원들의 실수 또는 부주의로 인해 발생합니다. 기업은 제로 트러스트 원칙을 적용함으로써 최종 사용자의 부주의로 인한 피해를 최소화할 수 있습니다

출처 : SANS Institute

핵심 요소 : 데이터

데이터 보호는 기업이 제로 트러스트를 도입하는 주된 이유입니다. 본 핵심 요소는 다음과 같은 3가지 주요 영역을 개선함으로써 그 목적을 뒷받침합니다.

- 가용성 - 필요할 때 언제 어디서든 데이터에 액세스할 수 있도록 보장
- 기밀성 - 무단 액세스로부터 보호
- 무결성 - 데이터가 변경, 손실, 손상되지 않도록 보장

CISA 모델의 성공의 핵심은 자동화된 전사적 데이터 분류 및 라벨링, 민감 정보의 도난을 방지하기 위한 강력한 데이터 유출 방지 전략, 광범위한 강력한 암호화, 지속적인 권한 검토 등이 있습니다.

대부분의 기업은 데이터베이스에 이미 관련 기능들을 다수 구축해 놓은 경우가 많습니다. 관련 기능들은 역할 기반 액세스 제어(RBAC), 저장 중 및 전송 중인 데이터의 투명한 암호화, 사용자 활동 및 데이터베이스 변경 사항을 추적 및 기록하기 위한 세분화된 감사, SQL 인젝션 공격과 같은 일반적인 악성 행위로부터의 보호 등을 지원해야 합니다.

마지막으로, 가시성 및 분석, 자동화 및 오케스트레이션, 거버넌스 등의 3가지 핵심 역량은 CISA의 5가지 핵심 요소에 모두 적용됩니다.

가시성 및 분석은 정책 결정에 필요한 정보를 제공하고 문제에 신속히 대응할 수 있는 적절한 데이터를 확보하기 위한 것입니다. 자동화 및 오케스트레이션은 확보한 데이터를 기반으로 보안 사고를 처리합니다. 거버넌스 기능은 기업이 자사의 규제, 법, 환경, 연방, 운영 관련 요구 사항을 관리 및 모니터링해 위험 기반 의사결정에 활용할 수 있도록 지원합니다.

제로 트러스트 관련 문화적 도전 과제

CISA의 거버넌스 계층은 적절한 인력, 프로세스, 기술의 확보를 함께 요구합니다. 효과적인 제로 트러스트를 위해서는 이 3가지 요소가 함께 작동해야 하므로, 현재 귀사의 네트워크 보안 모델이 네트워크 내에 진입한 사용자에게 일정 수준의 자산 간 이동성을 허용하는 경우 제로 트러스트는 상당한 변화를 가져올 것입니다.

주된 문제는 종종 새로운 ID 및 액세스 관리 관행을 강조하는 과정에서 발생합니다. 더 엄격한 비밀번호 정책, 비밀번호 완전 폐지, 다중 인증, 사용자 ID 및 액세스 권한 관리에 대한 더 중앙화된 접근 방식 등이 그 좋은 예입니다. 느슨한 통제에 익숙했던 사람들은 이러한 변화를 불편하게 느낄 수 있으며, 사용자들이 새로운 모델에 익숙해질 때까지 실제로 생산성이 저하될 수도 있습니다.

제로 트러스트는 사용자 활동과 기기의 상태를 더 면밀히 조사할 것을 요구하므로 자신의 행동이 너무 면밀히 모니터링되고 있다고 느끼는 일부 직원들은 개인정보 보호에 대한 우려를 제기할 수 있습니다. 일부 직원은 개인 기기에 필수 소프트웨어를 설치하는 것을 거부할 수도 있습니다.

심지어 보안, 네트워크 운영, 애플리케이션 개발 전문가들도 제로 트러스트에 반발할 수 있습니다. 한마디로 제로 트러스트란 사용자들의 수용과 경영진의 강력한 리더십을 요구하는 근본적인 변화입니다.

원활한 전환을 위한 전략

명확한 커뮤니케이션 : 비즈니스적 이점을 중심으로 제로 트러스트를 도입하는 이유를 설명합니다. 직원들이 가질 수 있는 개인정보 관련 우려를 공개적으로 불식시키고, 제로 트러스트가 데이터를 보호하는 방식을 설명합니다. 제로 트러스트 원칙 및 모범 사례에 대한 교육 및 정보 세션을 고려해 볼 수 있습니다.

단계적 도입 : 직원, 파트너, IT 담당자에게 적응할 시간을 주는 것이 좋습니다. 가능한 한 워크플로 중단을 최소화하고 긍정적인 사용자 경험을 유지할 수 있는 방향으로 제로 트러스트를 구현해야 합니다. 클라우드 기반 기술이 많은 도움이 될 수 있습니다.

명시적 업무 분리 : 각 사용자의 할당된 역할 범위 외의 리소스 액세스 또는 작업 수행을 방지하기 위한 업무 분리를 전사적으로 적용합니다. 이는 부서 간 사기 행위를 예방하는 데 도움이 될 수 있습니다.

경영진의 감사 표현 : 직원들의 노력에 대한 감사를 표현합니다. 이는 전환 과정의 원활화에 큰 도움이 될 수 있습니다. 그러나 경영진은 제로 트러스트를 전략적 이니셔티브로 삼아 충분한 자원을 할당하고, IT팀과 협력하여 통제 수단을 자사의 비즈니스 목표와 연계하고, 성과를 측정하기 위한 핵심 성과 지표(KPI)를 반드시 활용해야 합니다.

제로 트러스트 성공의 6가지 지표

글로벌 사이버 보안 교육 및 인증 기관인 SANS Institute는 최근 발행한 전략 가이드에서 제로 트러스트 구현의 효과를 측정하기 위한 여섯 가지 메트릭을 제시했습니다.

1. **인증 성공률.**총 시도 횟수 대비 성공한 인증 시도 비율을 측정합니다.
2. **정책 준수율.** 제로 트러스트 정책을 준수하는 액세스 요청의 비율을 측정합니다.
3. **측면 이동 시도 횟수.** 초기 액세스 후 네트워크 내 측면 이동 시도의 탐지 횟수를 측정합니다.
4. **사고 탐지 및 대응 시간.** 보안 사고를 탐지하고 대응하는 데 걸리는 평균 시간을 측정합니다.
5. **사용자 및 엔티티 행동 분석 이상 징후.** 잠재적 보안 위협 추적을 위해 사용자 및 엔티티 행동과 관련해 탐지된 이상 징후의 갯수 및 심각도를 측정합니다.
6. **관계자 피드백.** 교차기능팀, 최종 사용자, 관리자를 비롯한 모든 집단의 기술직 및 비기술직으로부터 데이터를 수집합니다.

6가지 제로 트러스트 설계 모범 사례

CISA는 대부분의 연방 정부 기관 및 대기업이 레거시 시스템과 관련된 공통적인 도전 과제에 직면하였음을 지적했습니다. 레거시 시스템은 고정된 속성에 기반한 액세스 및 권한 부여를 수행하는 경우가 많고, 부여한 권한을 자주 재검토하지 않습니다. 기술적 차원에서, 이같은 오래된 구조에서 벗어나기 위해서는 아키텍처 단위의 변경이 필요합니다.

주요 모범 사례는 다음과 같습니다.

1

인증 프레임워크를 사용하는 시간이 제한되고 검증받는 액세스

예를 들어, 직원이 아침에 OAuth와 같은 인증 서비스를 통해 로그인하면 특정 시스템에서 제한된 기간 동안만 유효성을 인정받고 비밀번호 대신 작용하는 토큰이 발급됩니다. 직원이 데이터베이스에 액세스할 때 해당 시스템에 대한 사용 권한은 토큰의 인증 코드를 통해 확인됩니다.

2

광범위한 마이크로세그멘테이션

성능 저하가 없는 한 측면 이동은 세밀하게 제한할수록 좋습니다. CISA는 애플리케이션 구성 방식에 기반한 분산형 마이크로페리미터와 광범위한 마이크로 세그먼테이션을 권장합니다. 이는 모든 곳에 방화벽을 설치하라는 의미가 아닙니다. 애플리케이션별 가상 머신, 동-서 트래픽 암호화, 물리적 네트워크 내 소프트웨어 정의 네트워크 구축, 지능형 라우팅 알고리즘 등의 기법을 활용하면 트래픽 흐름을 과도하게 지연시키지 않는 방식으로 세그먼트를 격리하고 보호할 수 있습니다.

3

상황 인식 로깅

AI는 이상 징후 탐지 및 그 대응 과정에서의 인증 관련 도전 과제 해결 역량 강화에 기여하는 위험 평가 기법에 기반한 적응형 인증을 통해 상황 인식 로깅 방식을 크게 변화시킬 수 있습니다. 귀사의 공급업체는 실시간으로 로그를 분석해 이상 징후와 잠재적 위협을 식별할 뿐만 아니라, 이벤트들의 상호 연관성을 분석해 정교한 공격 가능성을 암시하는 복잡한 패턴을 포착할 수 있는 기능을 제공해야 합니다.

4 광범위한 암호화

데이터는 기업의 가장 중요한 자산일 가능성이 높으며, 저장 중, 전송 중, 사용 중인 데이터를 두루 보호하기 위해서는 무단 액세스 시도를 감지하기 위한 모니터링 기능 및 종단간 암호화 기능이 필요합니다.

5 최소 권한 액세스

최소 권한은 제로 트러스트의 핵심 원칙입니다. 사용자, 애플리케이션, 기기에 꼭 필요한 것들로만 액세스를 제한하는 것은 직원을 불신해서가 아닌 위험을 줄이기 위한 것입니다. 이같은 접근 방식은 악의적인 행위자가 도난당한 자격 증명, 침해된 기기, 취약점 등을 악용할 경우 발생할 수 있는 잠재적 피해를 최소화합니다.

6 기기의 신뢰성에 집중

제로 트러스트는 어떤 기기도 무조건적으로 신뢰하지 않습니다. 이는 해당 기기가 내부 경계 내에 있거나 기업 소유이거나, 과거 이미 액세스 권한을 부여받은 경우에도 마찬가지입니다. 신뢰할 수 있는 기기로 인정받기 위해서는 업데이트된 소프트웨어, 안티바이러스 보호 태세, 모니터링 체계 구축 등의 보안 상태 요구 사항을 충족해야 할 수 있습니다.

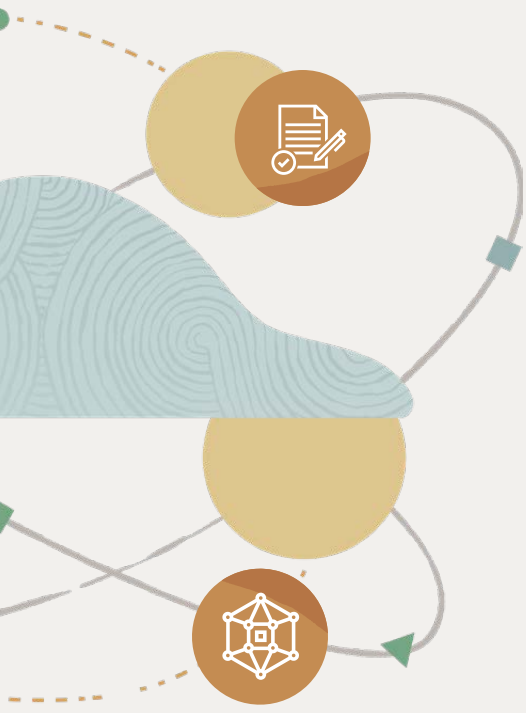
소프트웨어 버전 또는 멀웨어 시그니처 업데이트를 늦게 하거나 개인 기기에 보안 소프트웨어를 설치하는 것을 거부하는 사용자들이 있나요? 제로 트러스트는 정책에 정의된 보안 프로필이 없는 엔드포인트에는 액세스 권한을 부여하지 않으므로 그러한 사용자들도 결국 고집을 꺾을 수 밖에 없습니다. IT 부서는 기업 소유 기기의 엔드포인트 보안을 관리해야 하고, 새로운 세션이 시작될 때마다 규제 준수를 확인해야 합니다.

클라우드 공급업체 및 제로 트러스트

클라우드 서비스를 사용 중인 기업들은 제로 트러스트 구현을 시작하기에 유리한 위치에 있습니다. 하이퍼스케일러들은 사전 구성된 보안 솔루션, 템플릿, 도구를 제공하여 제로 트러스트 도구의 신속한 배포, 향상된 확장성, 중앙화된 관리 등을 지원합니다.

또한 많은 클라우드 공급업체들이 인적 오류를 최소화하고 고객사의 보안운영팀이 방화벽, 침입 탐지 시스템, 암호화, 지속적 검증, 최소 권한 액세스, ID 수명 주기 관리, 마이크로세그멘테이션 등 클라우드 공급업체가 제공하는 기본 보안 기능들을 최대한 활용한 통제 체계를 설정할 수 있도록 지원하는 생성형 AI 기반 자동화 기능을 출시했습니다.

클라우드 공급업체의 제로 트러스트 관련 노력의 바탕이 되는 핵심 기술은 Zero Trust Packet Routing(ZPR)입니다. ZPR은 관리자가 클라우드 내 자산에 대한 데이터 액세스 경로를 직접 정의할 수 있는 의도 기반 정책 언어입니다. 정책에 의해 명시적으로 허용되지 않은 트래픽은 네트워크를 통과할 수 없습니다.



ZPR의 이점

사람이 읽을 수 있는 정책 : 이해, 감사, 관리가 용이한 자연어로 정책을 작성합니다.

네트워크 보안 디커플링 : 네트워크 아키텍처에서 네트워크 보안을 분리하여 인적 오류 및 구성 복잡성에 따른 위험을 최소화합니다.

의도 기반 보안 : ZPR은 보안 속성을 활용해 리소스를 식별 및 구성하고, 해당 리소스에 대한 액세스 제어 정책을 관리합니다.

네트워크 레벨의 정책 적용 : 네트워크 아키텍처 변경 또는 잘못된 구성과 무관하게 네트워크 수준에서 정책을 적용합니다.

제로 트러스트를 지원하는 다른 기술로는 제로 트러스트 네트워크 액세스(ZTNA) 및 클라우드 액세스 보안 브로커(CASB)가 있습니다.

소프트웨어 정의 경계(SDP)라고도 불리는 ZTNA는 인증된 사용자에게 전체 네트워크에 대한 액세스를 허용하는 기존 VPN보다 훨씬 세분화된 방식으로 내부 애플리케이션 및 리소스에 대한 액세스를 제어하는 보안 접근 방식입니다. ZTNA는 리소스에 대한 액세스가 요청될 때마다 보안 자격 증명을 평가합니다. 시스템은 상황을 고려해 부분적인 액세스만을 허용할 수도 있습니다. 액세스가 허용되면 액세스를 요청한 엔티티와 특정 자산 간의 보안 세션을 통한 액세스가 진행됩니다. 이후 활동 내역 및 기기의 상태를 지속적으로 모니터링하여 위협 가능을 암시하는 비정상적인 행동을 탐지합니다.

CASB는 머신러닝을 활용하여 일정 기간 동안의 일반적인 활동을 모니터링함으로써 각 사용자의 표준적인 행동 기준선을 설정합니다. 이후 시스템은 데이터 분석을 통해 사용자의 행동을 기준선과 지속적으로 비교하여 악의적인 내부자 또는 계정 해킹 가능성을 암시하는 비정상적인 활동을 탐지합니다. IT 부서는 계정 정지 시점과 후속 조치를 위한 경고 발송 시점에 대한 규칙을 직접 설정할 수 있습니다.

마지막으로 클라우드 인프라 권한 관리(CIEM)는 IaaS, PaaS, SaaS 등의 클라우드 환경 내 ID 및 권한 관리에 중점을 둡니다. 안전한 인증 및 권한 부여를 위해서는 OAuth 2.0, 보안 검증 마크업 언어(SAML), OpenID Connect 등의 ID 표준이 통합된 시스템을 선택하고, 귀사의 클라우드 공급업체는 어떤 권한 및 액세스 제어 관리용 API들을 제공하는지 검토해 보아야 합니다.

정리하자면, 신뢰는 금지, 검증은 필수 라는 제로 트러스트 철학은 업계의 표준으로 빠르게 자리잡고 있습니다. 기존의 경계 중심 보안 방식을 버리지 못하는 기업은 파트너사, 고객, 직원의 신뢰를 잃을 수 있습니다. 다행히도 기업은 이미 구축된 다양한 관련 모델과 지원을 이용할 수 있고 클라우드 공급업체들이 제로 트러스트로의 전환을 선도하고 있습니다.

Oracle Access Governance와 제로 트러스트

Oracle Access Governance는 자동화 및 세분화된 액세스 제어를 통한 포괄적인 ID 거버넌스를 제공함으로써 클라우드 환경에서의 제로 트러스트 보안을 지원합니다. 사용자는 상황 및 정책에 기반한 지속적 액세스 평가 및 동적인 권한 부여를 활용해 신뢰는 금지, 검증은 필수 라는 원칙을 구현할 수 있습니다.

Oracle Advanced Authentication, Oracle Adaptive Risk Management, Oracle Universal Authenticator는 제로 트러스트 아키텍처 적용을 지원하는 강력한 기능들을 제공합니다. 해당 솔루션들은 다중 요소 인증(MFA), 피싱 방지 MFA, 적응형 인증, 비밀번호를 사용하지 않는 옵션이 포함된 기기 단위의 MFA 등을 지원합니다. 해당 솔루션들을 함께 활용하면 사용자 행동, 기기 무결성, 상황별 위험 등에 동적으로 대응할 수 있는 보안 조치들을 통해 중요한 리소스에 대한 안전한 액세스를 보장할 수 있습니다.

Oracle이 도와드리겠습니다

Oracle의 보안 우선 접근 방식에 따라, Oracle Cloud Infrastructure(OCI)에 액세스하기 위해서는 명시적 정책이 필요합니다. 각각의 구성 요소는 OCI 내의 개별적인 리소스로 간주되며 그에 대한 모든 액세스는 반드시 명시적으로 허용되어야 합니다. OCI 내의 모든 통신은 암호화되고, 액세스 권한은 관련 정책들에 따라 검증됩니다. 동적 액세스 구현을 비롯해 각각의 리소스에 대한 매우 세분화된 액세스 제어를 부여하는 액세스 정책들을 구축할 수 있습니다.

OCI는 클라우드 리소스에 대한 모니터링 및 감사를 구현합니다. 사용자는 기존의 객체 스토리지를 사용해 분석을 수행하거나 선호하는 보안 정보 및 이벤트 관리 도구를 사용할 수 있습니다. Oracle Cloud Guard Instance Security는 트리거된 이벤트에 대한 자동화된 대응을 제공해 잠재적 위협에 대한 대응 시간을 단축할 수 있도록 지원합니다.

또한 새로 출시된 OCI Zero Trust Landing Zone은 고객사의 클라우드 테넌시에 안전한 고성능 아키텍처를 원클릭 방식으로 프로비저닝할 수 있도록 지원합니다. 고객사는 특정 제로 트러스트 관련 요구 사항을 충족하기 위해 필요한 핵심 서비스를 배포하고 강화된 구성을 이용할 수 있습니다.

더 알아보기

문의처

한국 오라클 대표번호 02-2194-8000, 또는 oracle.com/kr 웹사이트를 통해 Oracle 담당자에게 연락하실 수 있습니다.

북미 지역 외 국가인 경우 oracle.com/kr/contact 에서 현지 지사를 찾을 수 있습니다.