DELL Technologies

5 제로 트러스트 요구를 해결하기 위한 권고

1	2	3	4	5
절대 신뢰하지 않고 항상 검증하는 방향으로의 패러다임 전환 계획	**원하는 경로 결정**	**조직에 맞춰 제로 트러스트 환경을 구축하는 것이지, 그 반대가 아님**	**데이터에 집중**	**절대 신뢰하지 않고 항상 검증한다는 원칙을 IT 생태계 전반에서 구현**
위험 완화와 비즈니스 영향 간에 허용 가능한 상충 관계 결정	점진적인 보안 강화	비즈니스 요구에 맞춰 제어	모든 네트워크, 디바이스, 사용자 활동이 지속적으로 기록되는지 확인	다단계 인증 및 ID 관리와 같은 제로 트러스트 활동을 보편적으로 적용함으로써 틈새 위험 방지
비용, 운영 및 이해 관계자에 미치는 영향, 규정 준수 및 규제 요건 고려	하이퍼스케일러	프로세스, 역할, 책임 및 데이터 분류 문서화	AI와 ML을 활용하여 데이터를 분석하고 위협을 나타낼 수 있는 이상 징후 식별	제로 트러스트(zero trust) 프레임워크에 타사 물리적 및 디지털 공급망 포함
경계 기반 보안에서 마이크로 세분화된 데이터 중심 모델로 진화	전용 환경	사용자 경험은 여전히 중요함	제로 트러스트 아키텍처의 핵심 역할은 데이터 및 애플리케이션 보호라는 점을 유념	
필요한 경우 외부 지원 활용	ID가 새로운 경계	사용 편의성을 희생하지 않고서는 제로 트러스트와 같은 보안 강화가 불가능		
		성장과 혁신 같은 조직의 목표는 여전히 중요함		

제로 트러스트는 보안 아키텍처의 모범 사례로 널리 알려져 있습니다.

데이터에 따르면 대부분의 조직이 제로 트러스트 구현을 고려하기 시작했거나 구현 중임을 알 수 있습니다[1]. 제로 트러스트로의 전환은 커다란 작업이지만, 이 여정을 안내하는 데 도움이 될 만한 몇 가지 실용적인 고려 사항이 있습니다.

Dell Technologies SME(Subject Matter Expert)인 Project Fort Zero 솔루션 도입 담당 Director인 Tracy Emmersen 씨와 Principal Security Engineer인 Justin Vogt 씨가 Security Services Product Manager인 Ash Lakshmanan 씨에게 권고 사항 및 인사이트를 공유했습니다. 주요 제안들이 아래에 요약되어 있으며, dell.com/cybersecuritymonth에서 전체 대화를 볼 수 있습니다.

> "제로 트러스트를 전체론적 관점에서 한 걸음 물러서서 보면 결국 가장 중요한 것은 데이터임을 알 수 있습니다."
>
> **Tracy Emmersen**
> Dell Technologies Project Fort Zero 솔루션 도입 담당 Director

절대 신뢰하지 않고 항상 검증하는 방향으로의 (중대한) 패러다임 전환 계획

기본적으로 제로 트러스트 환경으로 전환한다는 것은 과거의 보안 모델에서 벗어나 절대 신뢰하지 않고, 항상 검증하며, 최소 권한 액세스만 제공한다는 원칙에 기반한 보안 모델로 전환하는 것을 의미합니다. "기존의 경계 기반 네트워크 보안 솔루션에서 벗어나 마이크로 세분화된 데이터 중심 아키텍처로 나아가면서 기존과는 다른 보안 태세를 모색해야 합니다"라고 Emmersen 씨는 말합니다.

원하는 경로 결정

Emmersen 씨는 제로 트러스트의 이점을 실현하기 위한 세 가지 경로를 설명했습니다.

- **증분:** 현재 환경에 제로 트러스트 핵심 원칙을 적용하는 반복적인 접근 방식
- **하이퍼스케일러:** 주요 클라우드 공급업체의 제로 트러스트 기능 활용
- **완벽하게 호환되는 전용 환경:** 처음부터 새로 구축된 프라이빗 온프레미스 환경으로 제로 트러스트 표준을 엄격하게 준수

이러한 세 가지 경로 외에도 가상화된 중소기업은 'ID가 새로운 경계'라는 접근 방식을 취할 수 있습니다. 이 방법론은 ID 및 액세스 관리에 중점을 두고 SaaS 툴을 활용하여 제로 트러스트 기반 보호를 달성합니다. 이 방법에서 중요한 요소는 모든 곳에 MFA(Multi-Factor Authentication)를 구현하는 것으로, 이 제로 트러스트 기능의 영향을 나타냅니다.

하이퍼스케일러 및 ID 접근 방식은 일반적으로 비용이 저렴한 편이지만 증분 및 전용 환경에서는 더 많은 투자가 필요합니다.

조직에 맞춰 제로 트러스트 환경을 구축하는 것이지, 그 반대가 아님

기본적으로 제로 트러스트 아키텍처는 조직의 워크플로, 사용자 역할 및 관련 권한, 디바이스, 데이터, 애플리케이션 및 네트워크를 관리하고 보호하기 위한 것입니다. 처음 구현할 때는 이러한 측면에 대한 강력한 문서화가 필요하며, 그 이후에 이를 규제하는 정책이 적용되도록 제어 플레인과 인프라스트럭처가 설계됩니다.

제로 트러스트 환경이 조직에 해를 끼칠 만큼 비즈니스 운영을 저해하거나 크게 바꾼다면 보안을 강화해서 얻는 이점이 사라지게 됩니다. "만약 [보안이]...조직의 핵심 임무를 방해한다면...저지하기 위해 맞서고 있는 적들과 다를 바가 없게 됩니다. 스스로에게 서비스 거부 공격을 거는 셈입니다"라고 Vogt 씨는 지적합니다.

데이터에 집중

Emmersen 씨는 "제로 트러스트를 전체론적 관점에서 한 걸음 물러서서 보면 결국 가장 중요한 것은 데이터임을 알 수 있습니다"라고 말합니다. 조직의 데이터 보호는 제로 트러스트로 전환함으로써 얻을 수 있는 가장 중요한 이점 중 하나이며, 지속적인 검증 및 세분화와 같은 원칙은 위협이 네트워크 내에서 수평적으로 이동하는 것을 방지하여 데이터와 애플리케이션을 보호합니다.

로깅 및 지속적인 모니터링은 제로 트러스트의 중요한 구성 요소이며, 데이터와 텔레메트리를 분석하여 위험 또는 위협을 나타낼 수 있는 이상 징후를 식별합니다. 예를 들어, 데이터 사용 패턴의 변화는 잠재적인 유출 또는 랜섬웨어 공격을 의미할 수도 있습니다.

1. Dell의 의뢰로 Enterprise Strategy Group에서 실시한 연구 "Assessing Organizations' Security Journeys: Insights Spanning the Attack Surface, Threat Detection and Response, Attack Recovery, and Zero Trust," 2023년 11월

DELL Technologies

모든 활동을 로깅함으로써 생성되는 방대한 양의 데이터를 감안할 때, 현대적인 분석 툴은 AI와 머신 러닝을 활용해야만 효과가 있습니다.

절대 신뢰하지 않고 항상 검증하는 것이 필수

데이터, 애플리케이션, 사용자 및 디바이스에 대한 초점은 대부분 내부에 맞춰져 있지만 제로 트러스트 아키텍처에 내재된 정밀한 조사는 IT 수명 주기 전반에 걸쳐 적용되어야 합니다. 그렇게 하지 않으면 심각한 보안 틈새가 발생할 수 있습니다.

공급망이 좋은 사례로, Vogt는 타사 하드웨어 및 소프트웨어에 대해 중요한 질문을 할 것을 제안합니다.

- "다른 누가 또 액세스할 수 있었는가?
- 어떻게 구성되어 있는가?
- 수면 아래에서는 또 다른 어떤 일이 벌어지고 있는가?
- 신뢰하지 않으며 [동시에] 몇 가지 검증 프로세스를 거치고 최소한의 권한만 부여하는 이러한 원칙을 현재 사용 중인 기술에 어떻게 적용할 수 있는가? 해당 기술이 기술 공급망에서 더 위쪽에 있는 경우에도 그럴 수 있는가?"

제로 트러스트 아키텍처로 전환하거나 이 원칙을 구현하는 것은 사이버 보안 성숙도를 높이기 위한 현행 모범 사례입니다. 비용, 위험 및 보안 강화 수준 간의 상충 관계에 따라 여러 갈래로 나뉩니다. 첫 번째 단계는 조직의 고유한 위치를 파악하고 이에 맞춰 기술을 결정하는 것입니다.

dell.com/cybersecuritymonth에서 오늘날의 주요 사이버 보안 과제를 해결하는 방법을 알아보십시오.

DELL Technologies