제로 트러스트 수용: 안전하고 민첩한 비즈니스 혁신 전략

AWS 권장 가이드

AWS 권장 가이드: 제로 트러스트 수용: 안전하고 민첩한 비즈니스 혁신 전략

Table of Contents

제로 트러스트 수용: 안전하고 민첩한 비즈니스 혁신 전략

Greg Gooden, Amazon Web Services(AWS)

2023년 12월(문서 기록)

오늘날 조직은 그 어느 때보다 보안을 최우선 과제로 삼고 있습니다. 이를 통해 고객의 신뢰 유지부터 직원 이동성 향상, 새로운 디지털 비즈니스 기회 창출에 이르기까지 다양한 혜택을 누릴 수 있습니다. 그러면서 '시스템과 데이터에 대한 적절한 수준의 보안과 가용성을 보장하기 위한 최적의 패턴은 무엇인가'라는 오래된 질문을 계속 던집니다. 이 질문에 대한 현대적 해답을 설명하는 데 제로 트러스트라는 용어가 점점 더 많이 사용되고 있습니다.

제로 트러스트 아키텍처(ZTA)는 기존 네트워크 제어나 네트워크 경계에만 전적으로 또는 근본적으로 의존하지 않는 디지털 자산에 대한 보안 제어를 제공하는 데 초점을 맞춘 개념적 모델이자 관련 메커니즘입니다. 대신 네트워크 제어에는 ID, 디바이스, 동작 및 기타 풍부한 컨텍스트와 신호가 추가되어 보다 세분화되고 지능적이며 적응력이 뛰어나고 지속적인 액세스 결정을 내릴 수 있습니다. ZTA 모델을 구현하면 사이버 보안의 지속적인 성숙과 특히 심층적인 방어 개념에서 의미 있는 다음 반복을 달성할 수 있습니다.

의사 결정 프로세스

ZTA 전략을 구현하려면 신중한 계획과 의사 결정이 필요합니다. 여기에는 다양한 요인을 평가하고 조직 목표에 맞게 조정하는 작업이 포함됩니다. ZTA 여정을 시작하기 위한 주요 의사 결정 프로세스는 다음과 같습니다.

1. 이해관계자 참여 - 다른 CXO, VP, 고위 관리자를 참여시켜 조직의 보안 태세에 대한 우선순위, 우려 사항, 비전을 이해하는 것이 중요합니다. 처음부터 주요 이해관계자를 참여시킴으로써 ZTA 구현을 전체 전략 목표에 맞추고 필요한 지원과 리소스를 확보할 수 있습니다.
2. 위험 평가 - 포괄적인 위험 평가를 수행하면 문제, 과도한 표면적, 중요 자산을 식별하는 데 도움이 되며, 이를 통해 보안 통제 및 투자에 대한 정보에 입각한 결정을 내리는 데 도움이 됩니다. 조직의 기존 보안 태세를 평가하고, 잠재적 약점을 식별하고, 산업 및 운영 환경별 위험 환경을 기반으로 개선 영역의 우선순위를 정합니다.
3. 기술 평가 - 조직의 기존 기술 환경을 평가하고 격차를 식별하면 ZTA 원칙에 부합하는 적절한 도구와 솔루션을 선택하는 데 도움이 됩니다. 이 평가에는 다음 사항에 대한 철저한 분석이 포함되어야 합니다.
   - 네트워크 아키텍처

- Identity and Access Management 시스템
- 인증 및 권한 부여 메커니즘
- 통합 엔드포인트 관리
- 리소스 소유권 도구 및 프로세스
- 암호화 기술
- 모니터링 및 로깅 기능
- 견고한 ZTA 모델을 구축하려면 올바른 기술 스택을 선택하는 것이 중요합니다.

4. 변경 관리 - ZTA 모델 도입이 문화 및 조직에 미치는 영향을 인식하는 것이 필수적입니다. 변경 관리 관행을 구현하면 조직 전체에서 원활한 전환과 수용을 보장할 수 있습니다. 여기에는 직원을 대상으로 ZTA의 원칙과 이점에 대한 교육을 실시하고, 새로운 보안 관행에 대한 교육을 제공하고, 책임과 지속적인 학습을 장려하는 보안 중시 문화를 조성하는 것이 포함됩니다.

이 권장 가이드는 CXO, VP, 고위 관리자에게 ZTA 구현을 위한 포괄적인 전략을 제공하는 것을 목표로 합니다. 다음을 포함하여 ZTA의 주요 측면을 자세히 살펴보겠습니다.

- 조직의 준비 상태
- 단계별 도입 접근 방식
- 이해관계자 협업
- 안전하고 민첩한 비즈니스 혁신을 달성하기 위한 모범 사례

이 지침에 따라 조직은 Amazon Web Services(AWS) 클라우드에서 ZTA 환경을 탐색하고 보안 여정에서 성공적인 결과를 달성할 수 있습니다.는 AWS Verified Access, AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud(Amazon VPC), Amazon VPC Lattice, Amazon Verified Permissions, Amazon API Gateway 및 Amazon GuardDuty와 같은 ZTA를 구현하는 데 사용할 수 있는 다양한 서비스를 AWS 제공합니다. 이러한 서비스는 무단 액세스로부터 AWS 리소스를 보호하는 데 도움이 될 수 있습니다.

목표 비즈니스 성과

이 섹션에서는 조직 전반에 걸쳐 제로 트러스트 아키텍처를 정의하고 구현하는 것과 관련된 예상 결과를 설명합니다.

보안 태세 개선

조직은 제로 트러스트 원칙을 도입하여 보안 태세를 강화하고, 보안 위험을 완화하고, 클라우드 인프라 및 데이터를 보호할 수 있습니다. 필요에 따라 액세스 권한을 부여하는 제로 트러스트의 기본 원칙은 엄격한 통제와 함께 표면적을 크게 줄이고 보안 이벤트의 잠재적 영향을 제한합니다. 이러한 사전 예방적 접근 방식을 통해 조직은 새로운 보안 위험에 대비하고 자산의 기밀성, 무결성 및 가용성을 보장할 수 있습니다.

원활한 클라우드 도입

잘 정의된 제로 트러스트 아키텍처(ZTA) 도입 계획을 개발하면 클라우드 환경으로 원활하고 성공적으로 전환하는 데 도움이 될 수 있습니다. ZTA 원칙은 조직이 클라우드 컴퓨팅의 이점을 안전하게 누릴 수 있는 강력한 기반을 제공함으로써 클라우드 보안 모범 사례와 긴밀히 연계되어 있습니다. 처음부터 ZTA 원칙을 통합하면 조직이 보안을 핵심 요소로 하여 클라우드 아키텍처를 설계하는 데 도움이 됩니다.

규정 준수 및 규제 조정

ZTA 관행을 구현하면 조직이 산업 및 규제 요구 사항과 표준을 충족하는 데 도움이 될 수 있습니다. ZTA는 기본적으로 최소 권한 원칙을 장려하고 엄격한 액세스 제어를 시행합니다. 액세스 제어는 종종 다음과 같은 규정에 의해 의무화됩니다.

- 연방정부의 위험 및 인증 관리 프로그램(FedRAMP)
- HIPAA(미국 건강 보험 양도 및 책임에 관한 법)
- PCI DSS(지불 카드 산업 데이터 보안 표준)

조직은 제로 트러스트를 도입하여 데이터 보호, 개인정보 보호 및 규제 준수에 대한 노력을 입증하는 동시에 벌금이나 평판 훼손의 가능성을 최소화할 수 있습니다.

향상된 데이터 보호

조직은 데이터 암호화, 액세스 제어 및 정기적인 보안 평가를 구현하여 클라우드 도입 프로세스 전반에서 민감한 데이터를 보호할 수 있습니다. 조직은 다음과 같은 구체적인 조치를 취할 수 있습니다:

- 데이터 암호화 - 데이터 암호화 - 데이터 암호화는 데이터를 원래 일반 텍스트 형식으로 다시 복호화하려면 키가 필요한 방식으로 일반 텍스트 데이터를 사이퍼텍스트로 암호화하는 프로세스입니다. 따라서 권한이 없는 개인은 데이터 사본을 얻을 수 있더라도 민감한 데이터에 액세스하는 것이 훨씬 더 어려워집니다.
- 액세스 제어 - 액세스 제어는 민감한 데이터에 액세스할 수 있는 사용자와 해당 데이터로 수행할 수 있는 작업을 제한합니다. 이는 사용자 역할과 권한을 할당하고 다중 인증 또는 기타 방법을 사용하여 사용자 ID를 확인하는 방법으로 수행할 수 있습니다.
- 정기적인 보안 평가 - 정기적인 보안 평가를 통해 조직은 보안 문제를 식별 및 해결하고 사전에 해결할 수 있습니다. 내부 보안 팀이나 외부 보안 회사에서 이러한 평가를 수행할 수 있습니다.

제로 트러스트 아키텍처는 다양한 보안 조치를 구현하여 데이터 보호에 대한 포괄적인 접근 방식을 취합니다. 이러한 조치에는 강력한 인증, 데이터 암호화, 세분화된 액세스 제어가 포함됩니다. 이 접근 방식은 데이터 관련 보안 이벤트의 위험을 최소화하고 무단 액세스로부터 민감한 정보를 보호합니다.

효율적인 인시던트 대응

조직은 클라우드 환경에서 모니터링 및 인시던트 대응 프레임워크를 구축하여 보안 이벤트를 보다 빠르고 효과적으로 탐지하고 대응할 수 있습니다. 제로 트러스트 아키텍처는 지속적인 모니터링, 위협 인텔리전스 통합, 사용자 활동, 네트워크 트래픽 및 시스템 동작에 대한 실시간 가시성을 강조합니다. 그러면 보안 팀이 보안 이벤트를 사전에 식별하고 완화할 수 있습니다. 이 접근 방식은 잠재적 문제를 탐지하고, 대응하는 시간을 줄이고, 비즈니스 운영에 미치는 영향을 최소화합니다. 핵심 사항은 다음과 같습니다.

- 테스트 - 조직이 따르는 인시던트 대응 프레임워크 또는 방법론에 관계없이 인시던트 대응 계획을 정기적으로 테스트해야 합니다. 테이블탑 연습, 시뮬레이션 및 팀 구성을 통해 실제 환경에서 인시던트 대응을 연습하고, 도구 및 기능 격차를 발견하고, 인시던트 대응 담당자의 경험과 자신감을 쌓을 수 있습니다.
- 모니터링 - 클라우드 환경을 지속적으로 모니터링하여 비정상적인 활동의 징후가 있는지 확인합니다. 로그 분석, 네트워크 모니터링, 취약성 검사와 같은 다양한 도구 및 기법을 사용하여 이를 수행할 수 있습니다.

- 위협 인텔리전스 통합 - 모니터링 및 인시던트 대응 프레임워크에 위협 인텔리전스를 통합합니다. 이를 통해 조직은 더 빠르고 효과적으로 위협을 식별하고 이에 대응할 수 있습니다.
- 실시간 가시성 - 보안 인시던트를 신속하게 식별하고 이에 대응하려면 조직에 사용자 활동, 네트워크 트래픽 및 시스템 동작에 대한 실시간 가시성이 필요합니다.
- 사전 식별 및 완화 - 조직은 보안 이벤트를 사전에 식별하고 완화하여 잠재적 위협을 탐지하고 이에 대응하는 시간을 줄이고 비즈니스 운영에 미치는 영향을 최소화할 수 있습니다.

직원 생산성 향상

현대의 인력은 점점 더 많은 장소, 디바이스 및 시간에서 작업을 수행할 수 있는 유연성을 필요로 합니다. ZTA를 구현하면 조직의 보안 태세를 유지하거나 개선하는 동시에 이러한 요구 사항을 지원하고 직원 이동성, 생산성 및 만족도를 개선할 수 있습니다.

디지털 트랜스포메이션 활성화

디지털 트랜스포메이션의 일환으로 기존 네트워크 경계 외부의 디바이스, 기계, 시설, 인프라 및 프로세스의 상호 연결을 추구하는 조직이 점점 더 많아지고 있습니다. 사물 인터넷(IoT) 및 운영 기술(OT, 산업용 사물 인터넷 또는 IIoT라고도 함) 디바이스는 종종 텔레메트리 및 예측 유지 보수 정보를 클라우드로 직접 전송합니다. 워크로드를 보호하려면 기존의 경계 접근 방식을 넘어서는 보안 제어를 적용해야 합니다.

섹션 요약

조직은 이러한 목표 비즈니스 성과에 집중하여 ZTA의 잠재력을 최대한 실현하고 클라우드에서 보안 태세를 강화할 수 있습니다. 이러한 결과를 특정 조직 목표에 맞추고, 고유한 비즈니스 요구 사항에 맞게 조정하고, 정기적으로 효율성을 평가하여 지속적인 개선을 추진하는 것이 중요합니다.

제로 트러스트 원칙 이해

제로 트러스트 아키텍처(ZTA)는 보안 모델의 기초를 형성하는 일련의 핵심 원칙을 기반으로 합니다. 이러한 원칙을 이해하는 것은 ZTA 전략을 효과적으로 도입하고자 하는 조직에 필수적입니다. 이 섹션에서는 ZTA의 핵심 원칙을 다룹니다.

확인 및 인증

확인 및 인증 원칙은 사용자, 시스템, 디바이스를 포함한 모든 유형의 보안 주체에 대한 강력한 식별 및 인증의 중요성을 강조합니다. ZTA는 세션 전반에 걸쳐, 이상적으로는 각 요청에 대해 지속적인 ID 및 인증 상태 확인을 요구하며, 기존 네트워크 위치나 제어에만 의존하지는 않습니다. 여기에는 현대의 강력한 다중 인증(MFA) 구현과 인증 프로세스 중 추가적인 환경 및 컨텍스트 신호 평가가 포함됩니다. 조직은 이 원칙을 도입하여 리소스 권한 부여 결정에 가능한 최상의 ID 입력을 보장할 수 있습니다.

최소 권한 액세스

최소 권한 원칙에는 보안 주체에게 작업을 수행하는 데 필요한 최소한의 액세스 수준 부여가 포함됩니다. 최소 권한 액세스 원칙을 도입함으로써 조직은 세분화된 액세스 제어를 시행하여 보안 주체가 자신의 역할과 책임을 수행하는 데 필요한 리소스에만 액세스하도록 할 수 있습니다. 여기에는 노출 영역과 무단 액세스의 위험을 최소화하기 위한 적시 액세스 프로비저닝, 역할 기반 액세스 제어(RBAC) 및 정기적인 액세스 검토 구현이 포함됩니다.

마이크로 분할

마이크로 분할은 네트워크를 더 작고 격리된 세그먼트로 나누어 특정 트래픽 흐름을 승인하는 네트워크 보안 전략입니다. 워크로드 경계를 만들고 서로 다른 세그먼트 간에 엄격한 액세스 제어를 적용하여 마이크로 분할을 수행할 수 있습니다.

마이크로 세분화는 네트워크 가상화, 소프트웨어 정의 네트워킹(SDN), 호스트 기반 방화벽, 네트워크 액세스 제어 목록(NACLs) 및 Amazon Elastic Compute Cloud(Amazon EC2) 보안 그룹 또는 같은 AWS 특정 기능을 통해 구현할 수 있습니다 AWS PrivateLink. 분할 게이트웨이는 세그먼트 간 트래픽을 제어하여 액세스를 명시적으로 승인합니다. 마이크로 분할 및 분할 게이트웨이는 조직이 네트워크를 통한 불필요한 경로, 특히 중요한 시스템 및 데이터로 이어지는 경로를 제한하는 데 도움이 됩니다.

지속적인 모니터링 및 분석

지속적인 모니터링 및 분석에는 조직 환경 전반에서 보안 관련 이벤트 및 데이터 수집, 분석, 상관관계 파악이 포함됩니다. 조직은 강력한 모니터링 및 분석 도구를 구현하여 보안 데이터와 텔레메트리를 융합된 방식으로 평가할 수 있습니다.

이 원칙은 이상과 잠재적 보안 이벤트를 식별하기 위해 사용자 동작, 네트워크 트래픽 및 시스템 활동에 대한 가시성의 중요성을 강조합니다. 보안 정보 및 이벤트 관리(SIEM), 사용자 및 엔터티 행동 분석(UEBA), 위협 인텔리전스 플랫폼과 같은 고급 기술은 지속적인 모니터링과 사전 위협 탐지를 달성하는 데 중요한 역할을 합니다.

자동화 및 오케스트레이션

자동화 및 오케스트레이션을 통해 조직은 보안 프로세스를 간소화하고, 수동 개입을 줄이고, 응답 시간을 개선할 수 있습니다. 조직은 일상적인 보안 작업을 자동화하고 오케스트레이션 기능을 사용하여 일관된 보안 정책을 적용하고 보안 이벤트에 신속하게 대응할 수 있습니다. 이 원칙에는 사용자 권한을 시기적절하고 정확하게 관리할 수 있도록 액세스 프로비저닝 및 프로비저닝 해제 프로세스를 자동화하는 것도 포함됩니다. 자동화와 오케스트레이션을 도입함으로써 조직은 운영 효율성을 높이고 인적 오류를 줄이고 리소스를 보다 전략적인 보안 이니셔티브에 집중할 수 있습니다.

권한 부여

ZTA에서는 리소스에 액세스하려는 각 요청이 게이트 시행 지점에 의해 명시적으로 승인되어야 합니다. 인증 정책은 인증된 ID 외에도 디바이스 상태 및 상태, 동작 패턴, 리소스 분류, 네트워크 요인과 같은 추가 컨텍스트를 고려해야 합니다. 권한 부여 프로세스는 액세스 중인 리소스와 관련된 해당 액세스 정책을 기준으로 이 통합 컨텍스트를 평가해야 합니다. 기계 학습 모델은 선언적 정책을 동적으로 보완할 수 있는 최적의 모델입니다. 이러한 모델을 활용할 때는 추가 제한에만 초점을 맞춰야 하며, 명시적으로 지정되지 않은 액세스 권한을 부여해서는 안 됩니다.

섹션 요약

조직은 ZTA의 이러한 핵심 원칙을 준수하여 현대 기업 환경의 다양성에 부합하는 강력한 보안 모델을 구축할 수 있습니다. 이러한 원칙을 구현하려면 기술, 프로세스, 사람을 결합하여 제로 트러스트 사고방식을 계발하고 탄력적인 보안 태세를 구축하는 포괄적인 접근 방식이 필요합니다.

제로 트러스트 아키텍처의 주요 구성 요소

제로 트러스트 아키텍처(ZTA) 전략을 효과적으로 구현하려면 조직에서 ZTA를 구성하는 주요 구성 요소를 이해해야 합니다. 이러한 구성 요소가 함께 작용하여 제로 트러스트 원칙에 부합하는 포괄적인 보안 모델을 바탕으로 지속적으로 개선합니다. 이 섹션에서는 ZTA의 주요 구성 요소를 다룹니다.

ID 및 액세스 관리

ID 및 액세스 관리는 강력한 사용자 인증과 대략적인 액세스 제어 메커니즘을 제공하여 ZTA의 기반을 형성합니다. 여기에는 Single Sign-On(SSO), 다중 인증(MFA), ID 거버넌스 및 관리 솔루션과 같은 기술이 포함됩니다. ID 및 액세스 관리는 제로 트러스트 권한 부여 결정을 내리는 데 필수적인 높은 수준의 인증 보장과 중요한 컨텍스트를 제공합니다. 동시에 ZTA는 사용자별, 디바이스별, 세션별로 애플리케이션 및 리소스에 대한 액세스 권한을 부여하는 보안 모델입니다. 이를 통해 사용자의 보안 인증이 침해되더라도 조직을 무단 액세스로부터 보호할 수 있습니다.

Secure Access Service Edge

SASE(Secure Access Service Edge)는 네트워킹 및 보안 기능을 단일 클라우드 기반 서비스로 가상화, 결합 및 배포하는 네트워크 보안에 대한 새로운 접근 방식입니다. SASE는 사용자의 위치와 관계없이 애플리케이션 및 리소스에 대한 보안 액세스를 제공할 수 있습니다.

SASE에는 보안 웹 게이트웨이, 서비스형 방화벽, 제로 트러스트 네트워크 액세스(ZTNA)와 같은 다양한 보안 기능이 포함되어 있습니다. 이러한 기능이 함께 작동하여 멀웨어, 피싱, 랜섬웨어를 비롯한 광범위한 위협으로부터 조직을 보호합니다.

데이터 손실 방지

데이터 손실 방지(DLP) 기술은 조직이 민감한 데이터가 무단으로 공개되지 않도록 보호하는 데 도움이 될 수 있습니다. DLP 솔루션은 이동 중인 데이터와 저장 데이터를 모니터링하고 제어합니다. 이를 통해 조직은 데이터 관련 보안 이벤트를 방지하는 정책을 정의하고 시행하여 네트워크 전체에서 민감한 정보를 계속 보호할 수 있습니다.

보안 정보 및 이벤트 관리

보안 정보 및 이벤트 관리(SIEM) 솔루션은 조직 인프라 전반의 다양한 소스에서 보안 이벤트 로그를 수집, 집계 및 분석합니다. 이 데이터를 사용하여 보안 인시던트를 탐지하고, 인시던트 대응을 촉진하고, 잠재적 위협 및 취약성에 대한 인사이트를 제공할 수 있습니다.

특히 ZTA의 경우, 비정상 패턴의 탐지 및 대응을 개선하기 위해서는 다양한 보안 시스템의 관련 텔레메트리를 상호 연관시키고 이해하는 SIEM 솔루션의 기능이 매우 중요합니다.

엔터프라이즈 리소스 소유권 카탈로그

기업 리소스에 대한 액세스 권한을 올바르게 부여하려면 조직은 이러한 리소스를 분류하는 신뢰할 수 있는 시스템을 갖추고 있어야 하며, 중요한 것은 누가 해당 리소스를 소유하고 있는지 파악하는 것입니다. 이러한 정보 소스는 액세스 요청, 관련 승인 결정 및 이에 대한 정기적인 증명을 용이하게 하는 워크플로를 제공해야 합니다. 시간이 지나면 이 정보 소스에는 조직 내에서 '누가 무엇에 액세스할 수 있는가?'에 대한 답이 포함될 것입니다. 권한 부여, 감사 및 규정 준수에 대한 답변을 모두 사용할 수 있습니다.

통합 엔드포인트 관리

ZTA는 사용자를 강력하게 인증하는 것 외에도 사용자 디바이스의 상태와 태세를 고려하여 기업 데이터 및 리소스 액세스가 안전한지 평가해야 합니다. 통합 엔드포인트 관리(UEM) 플랫폼은 다음과 같은 기능을 제공합니다.

- 디바이스 프로비저닝
- 지속적인 구성 및 패치 관리
- 보안 기준 설정
- 텔레메트리 보고
- 디바이스 정리 및 사용 중지

정책 기반 시행 지점

ZTA에서는 각 리소스에 대한 액세스가 게이트 정책 기반 시행 지점에 의해 명시적으로 승인되어야 합니다. 처음에 이러한 시행 지점은 기존 네트워크 및 ID 시스템의 기존 시행 지점을 기반으로 할 수 있습니다. ZTA가 제공하는 다양한 상황과 신호를 고려하면 시행 지점의 역량을 점차 강화할 수 있습니다. 장기적으로는 통합 컨텍스트에서 운영되는 ZTA 전용 시행 지점을 구현하고, 신호 제공업체를 일관되게 통합하고, 포괄적인 정책 세트를 유지하고, 결합된 텔레메트리를 통해 수집한 인텔리전스를 통해 강화되는 ZTA 전용 시행 지점을 구현해야 합니다.

섹션 요약

ZTA 도입을 계획하는 조직에서는 이러한 주요 구성 요소를 이해하는 것이 필수적입니다. 이러한 구성 요소를 구현하고 보안 모델에 통합하여 조직은 제로 트러스트 원칙에 따라 강력한 보안 태세를 구축할 수 있습니다. 다음 섹션에서는 조직 내에서 ZTA를 성공적으로 구현하는 데 도움이 되는 조직의 준비 상태, 단계별 도입 접근 방식, 모범 사례를 살펴봅니다.

제로 트러스트 도입을 위한 조직의 준비 상태 평가

새로운 아키텍처 전략 도입은 조직적 요소를 신중하게 계획하고 고려해야 하는 중요한 작업입니다. 이 섹션에서는 전사적 제로 트러스트 도입을 위한 조직의 주요 준비 상태 고려 사항을 중점적으로 다룹니다. 이러한 고려 사항을 해결함으로써 조직은 보다 강력하고 성공적인 보안 태세를 위한 기반을 마련할 수 있습니다.

리더십 정비 및 커뮤니케이션

제로 트러스트를 성공적으로 구현하려면 리더십 정비와 커뮤니케이션이 필수적입니다. 리더십은 제로 트러스트의 이점과 필요한 리소스를 파악해야 합니다. 또한 리더는 조직의 문화와 프로세스를 바꿀 의지가 있어야 합니다. 신뢰와 지지를 얻으려면 직원과의 커뮤니케이션이 필요합니다. 직원들은 조직이 제로 트러스트를 구현하는 이유, 제로 트러스트가 자신에게 어떤 의미가 있는지, 어떻게 도울 수 있는지 이해해야 합니다. 커뮤니케이션은 개방적이고 투명하고 지속적이어야 합니다.

리더십 지원 및 동의

성공적인 제로 트러스트 아키텍처(ZTA) 구현을 위해서는 아키텍처의 목표, 이점 및 성공 척도에 대해 주요 이해관계자와 경영진을 조율하는 것이 중요합니다. 기존의 경계 기반 보안에서 벗어나 사용자 중심의 보다 세분화된 접근 방식으로 보안을 강화하고 비즈니스 민첩성을 지원하는 데 있어 제로 트러스트 원칙의 중요성을 공유합니다. 이 접근 방식으로 전환하면 조직이 변화와 위협에 더 빠르게 적응할 수 있습니다. 경영진 조율은 조직의 분위기를 조성하고 변화에 대한 잠재적 저항을 극복하는 데 도움이 됩니다.

투명한 커뮤니케이션

제로 트러스트 구현 프로세스 전반에 걸쳐 직원들과 개방적이고 투명한 커뮤니케이션을 유지합니다. 도입의 근거, 이점 및 예상 결과를 설명하고 우려 사항을 즉시 해결합니다. 구현 진행 상황에 대한 정기적인 업데이트를 제공합니다. 이를 통해 지지를 늘리고 저항을 줄이고 신뢰를 구축할 수 있습니다.

기술 개발 및 교육

리더십이 정비되고 열린 커뮤니케이션이 이루어진 후에는 제로 트러스트를 구현할 직원의 기술과 지식을 개발하는 것이 중요합니다. 여기에는 제로 트러스트 원칙의 이해, 업무에서 이를 이행하는 방법, 보안 이벤트에 대응하는 방법이 포함됩니다. 직원들이 이러한 기술을 습득할 수 있도록 교육 및 개발 기회를 제공합니다.

클라우드 지식 및 기술

클라우드 기술 및 제로 트러스트 원칙에 대한 조직의 기술 및 지식 격차를 평가합니다. 직원의 기술을 향상시키고 클라우드 중심 및 제로 트러스트 환경에서 효과적으로 작업하는 데 필요한 전문 지식을 갖추도록 교육 및 개발 프로그램을 제공합니다. 진화하는 기술 및 보안 관행과 보조를 맞추기 위한 지속적인 학습 문화를 조성합니다.

보안 문화 및 인식

조직의 보안 문화를 평가합니다. 직원들의 보안 인식 수준, 보안 모범 사례에 대한 이해, 정책 및 절차 준수 여부를 평가합니다. 보안 지식의 격차를 파악합니다. 직원들에게 제로 트러스트의 중요성과 보안 환경 유지에 있어 직원의 역할을 교육하는 보안 인식 교육 프로그램을 실시하는 것을 고려해 봅니다.

조직 구조 및 역할

제로 트러스트를 성공적으로 구현하려면 효과적인 조직 구조와 역할을 정립합니다. 여기에는 클라우드 혁신 센터(CCoE) 설립, 보안 운영 검토 및 수정, 취약성 관리, 인시던트 대응, 보안 모니터링을 위한 역할 및 책임 할당이 포함됩니다.

클라우드 혁신 센터

클라우드 운영 지침, 모범 사례 및 감독을 제공하기 위한 CCoE를 설립합니다. CCoE는 클라우드 관련 모범 사례, 지침 및 거버넌스 정책을 만들고 구현하는 일을 담당하는 팀 또는 개인 그룹입니다. CCoE에는 협업과 조율을 보장하기 위해 다양한 사업부와 IT 팀의 담당자가 포함되어야 합니다. CCoE는 클라우드 호스팅 워크로드에 제로 트러스트 원칙을 도입하는 데 중요한 역할을 합니다. 또한 CCoE는 조직 전반에 걸친 지식 공유를 용이하게 합니다.

보안 운영

제로 트러스트 환경의 요구 사항을 충족하려면 현재 보안 운영 조직을 검토하고 수정합니다. 모니터링, 인시던트 대응 및 위협 인텔리전스 기능을 개선하려면 보안 운영 센터(SOC) 또는 관리형 보안 서비스 제공업체(MSSP) 구현을 고려합니다. 취약성 관리, 인시던트 대응 및 보안 모니터링에 대한 역할과 책임을 정립합니다. 잘 작동하는 인시던트 대응 프로세스는 사소한 보안 이벤트를 신속하게 탐지하고 해결하여 이벤트 순서를 중단하는 데 매우 중요합니다. 이를 통해 사소한 이벤트가 더 큰 영향을 미치는 이벤트로 발전하는 것을 막을 수 있습니다.

IT 인프라 및 아키텍처

회사의 IT 아키텍처와 인프라를 검토하여 제로 트러스트 접근 방식 도입에 영향을 미칠 수 있는 제약이나 종속성을 찾습니다. 현재 애플리케이션 및 시스템이 필요한 제로 트러스트 아키텍처 구성 요소와 호

환되는지 확인합니다. 제로 트러스트 원칙의 성공적인 배포를 지원하기 위해 인프라 개선 또는 조정이 필요한지 분석합니다. 각 애플리케이션이나 시스템에 대해 제로 트러스트가 현재 구현되는 것이 가장 좋은지 아니면 대규모 현대화 노력을 통해 구현되는 것이 가장 좋은지 검토합니다.

위험 관리, 거버넌스 및 변경 제어

제로 트러스트를 성공적으로 구현하려면 효과적인 위험 관리, 거버넌스 및 변경 제어 프로세스를 수립합니다. 여기에는 제로 트러스트 원칙에 따른 위험 관리 조정, 인시던트 대응 계획 개발, 법률 및 규정 준수 부서와의 협력, 변경 제어 프로세스 수립 등이 포함됩니다.

위험 관리

회사에서 시행 중인 리스크 관리 전략을 점검하고 제로 트러스트 원칙을 얼마나 잘 준수하는지 확인합니다. 현재 인시던트 대응 시스템, 보안 조치 및 위험 평가 절차의 효율성을 분석합니다. 제로 트러스트 전략을 준수하기 위해 개선이 필요한 영역을 결정합니다. 자동화된 인시던트 대응 시스템 또는 지속적인 모니터링 및 분석 프레임워크 개발을 시작하여 해결 속도를 높입니다.

변경 제어 프로세스

모든 클라우드 관련 수정 사항이 보안 및 규정 준수 요구 사항을 준수하도록 하려면 효과적인 변경 제어 방법을 수립합니다. 보안 구성 분석, 위험 평가, 승인 및 문서화를 포함하는 체계적인 변경 관리 절차를 수립합니다. 제로 트러스트 아키텍처의 무결성을 보존하기 위해 업데이트를 자주 검토하고 감사합니다.

모니터링 및 평가

제로 트러스트를 성공적으로 구현하려면 조직에서 보안 상태를 지속적으로 모니터링하고 평가해야 합니다. 여기에는 핵심 성과 지표(KPI) 수립, KPI 모니터링 및 평가, 지속적인 개선 문화 조성 등이 포함됩니다. 이러한 단계를 수행함으로써 조직은 제로 트러스트 구현이 성공적으로 이루어졌는지, 그리고 보안을 개선하기 위해 항상 노력하고 있는지 확인할 수 있습니다.

핵심 성과 지표

제로 트러스트 배포의 성공과 효과를 측정할 수 있는 관련 핵심 성과 지표(KPI)를 설정합니다. 이러한 KPI는 사용자 만족도, 장비 및 롤아웃 진행 상황, 비용 절감, 규정 준수 및 보안 이벤트 발생 횟수를 측정할 수 있습니다. 전체 개발 상황을 추적하고 개선 기회를 찾으려면 이러한 KPI를 정기적으로 모니터링하고 평가합니다.

지속적 개선

이해관계자의 의견과 인사이트를 이끌어내는 시스템을 구축하면 지속적인 개선 문화를 조성하는 데 도움이 됩니다. 직원들이 클라우드 환경의 보안, 효과 및 사용자 경험을 개선하기 위한 생각과 제안을 제공하도록 장려합니다. 이 입력 내용을 활용하여 절차를 간소화하고, 보안 조치를 개선하고, 혁신을 촉진합니다.

섹션 요약

이러한 조직적, 문화적 고려 사항을 해결함으로써 조직은 제로 트러스트 보안 모델의 클라우드 도입을 위한 지원 환경을 조성할 수 있습니다. 다음 섹션에서는 단계적 도입 접근 방식을 살펴보고 실용적이고 관리 가능한 방식으로 제로 트러스트 원칙을 점진적으로 구현하는 방법에 대한 지침을 제공합니다.

제로 트러스트 사고방식 조성

제로 트러스트 구현은 기술적 구현 그 이상입니다. 조직 내에서 문화적 변화가 필요합니다. 제로 트러스트 사고방식을 조성하려면 다음과 같은 주요 측면을 강조해야 합니다.

제로 트러스트 교육 및 훈련

직원에게 제로 트러스트 아키텍처(ZTA)의 가치 및 이점에 대해 교육합니다. 교육 세션, 워크숍 및 기타 리소스를 통해 ZTA 개념과 접근 방식에 대한 기술적 및 비기술적 설명을 제공합니다. 직원이 제로 트러스트 보안 패러다임의 확립 및 유지에 대한 자신의 책임을 인식하도록 장려합니다.

협업 및 통신

ZTA 구현과 관련된 모든 팀과 부서 간 협업과 투명성을 장려합니다. 모든 사람이 계획을 철저히 이해할 수 있도록 부서 간 커뮤니케이션, 지식 공유 및 정보 교환을 장려합니다. 모든 사람이 비즈니스의 전반적인 보안에 기여하는 것의 중요성을 인식하는 공동 책임 문화를 조성합니다.

지속적 학습 및 개선

제로 트러스트의 컨텍스트에서 지속적 학습 및 개선의 우선순위를 정합니다. 직원이 최신 보안 추세, 기술 및 모범 사례를 최신 상태로 유지하도록 장려합니다. 직원이 조직의 보안 태세를 강화하기 위한 새로운 솔루션과 접근 방식을 알아보도록 장려하는 혁신과 실험의 문화를 조성합니다.

지표 및 책임

제로 트러스트 전략의 효과를 측정하기 위한 명확한 지표와 책임 메커니즘을 설정합니다. 조직의 보안 목표에 맞는 핵심 성과 지표(KPI)를 정의하고 진행 상황을 정기적으로 추적합니다. 개인과 팀이 제로 트러스트 원칙의 구현 및 유지 관리에 대한 기여에 책임을 지도록 합니다.

섹션 요약

조직은 이러한 측면을 해결하고 제로 트러스트 사고방식을 구축하여 제로 트러스트를 성공적으로 채택하고 구현하기 위한 탄탄한 기반을 마련할 수 있습니다. 이러한 문화적 전환은 조직의 모든 사람이 제로 트러스트의 중요성을 이해하고 성공에 적극적으로 기여할 수 있도록 돕는 데 필수적입니다.

다음 섹션에서는 단계적 도입 접근 방식을 살펴보고 실용적이고 관리 가능한 방식으로 제로 트러스트 원칙을 점진적으로 구현하는 방법에 대한 지침을 제공합니다.

제로 트러스트에 대한 단계적 접근 방식

제로 트러스트 아키텍처(ZTA)를 도입하려면 신중한 계획과 구현이 필요합니다. 원활한 전환과 비즈니스 운영 중단 최소화를 위해 단계적 도입 접근 방식을 권장합니다. 이 섹션에서는 ZTA 도입과 관련된 주요 단계에 대한 지침을 제공합니다.

1단계: 평가 및 계획

제로 트러스트 구현의 첫 번째 단계는 평가 및 계획입니다. 이 단계는 조직의 현재 보안 태세에서 부족한 부분을 파악하고 해결하는 작업을 포함하므로 전체 구현의 성공에 매우 중요합니다. 시간을 내어 현재 상태를 평가하고 보안 목표를 정의하면 성공적인 제로 트러스트 구현을 위한 기반을 마련할 수 있습니다.

동시에 완벽하고 정확한 평가가 항상 현실적이지는 않을 수도 있습니다. 다음 단계로 넘어가지 못하게 하는 분석 마비를 방지하려면 일정 수준의 불완전성을 구분하거나 수용할 준비를 합니다.

1. 현재 상태 평가 - 기존 보안 인프라, 정책 및 제어 평가를 수행합니다. 잠재적 취약성, 보안의 격차, 제로 트러스트 원칙의 구현으로 개선이 가능한 영역을 파악합니다.
2. 보안 목표 정의 - 현재 상태 평가 조사 결과를 바탕으로 제로 트러스트 원칙에 부합하는 보안 목표를 정의합니다. 또한 이러한 보안 목표는 조직의 전체 보안 전략에 부합하고 식별된 취약성과 격차를 해소해야 합니다.
3. 아키텍처 설계 - 조직의 보안 목표를 지원하는 ZTA를 개발합니다. 이 아키텍처에는 ID 및 액세스 관리 솔루션, 네트워크 세분화 메커니즘, 지속적인 모니터링 시스템 등의 필수 구성 요소가 포함되어야 합니다. 또한 아키텍처는 확장 가능하고 적응력이 뛰어나며 미래의 성장 및 기술 발전을 수용할 수 있어야 합니다. 이 아키텍처는 문서나 다이어그램뿐만 아니라 AWS CloudFormation 템플릿과 같이 구현을 담당하는 팀이 쉽게 사용할 수 있는 형식으로 표현하는 것이 가장 이상적입니다.
4. 이해관계자 참여 - 사업부, IT 팀, 보안 팀을 비롯한 모든 이해관계자를 참여시켜 인사이트를 얻고 목표를 ZTA 구현 계획에 맞게 조정합니다. 협업과 소통을 장려하여 제로 트러스트 접근 방식의 이점과 요구 사항에 대한 공통된 이해를 확립합니다.

2단계: 파일럿 및 구현

제로 트러스트 구현의 두 번째 단계는 파일럿 및 구현입니다. 이 단계에서는 소규모의 통제된 환경에서 ZTA를 테스트한 다음, 조직 전체에 반복적으로 배포합니다. 직원들에게 새로운 보안 조치와 제로 트러스트 환경을 유지하기 위한 각자의 역할에 대해 교육하는 것이 중요합니다.

1. 배포 파일럿 - 소규모의 통제된 환경에서 ZTA를 테스트합니다. 아키텍처 설계 단계에서 정의된 필수 구성 요소 및 보안 제어를 구현합니다. 파일럿 배포를 면밀히 모니터링하고 피드백을 수집하고 필요한 조정을 수행합니다. 제로 트러스트가 가상의 연습에서 실제 경험을 쌓는 과정으로 전환되는 프로세스 초기에 유연하게 대처할 수 있도록 준비합니다.
2. 반복적 배포 - 파일럿 배포에서 얻은 교훈을 바탕으로 조직 전체에 제로 트러스트를 반복적으로 배포하기 시작합니다. 중요한 배포 규모를 달성하기 위해 대규모 캠페인이 필요하지 않은 플라이휠 효과를 통해 추진력을 확보합니다. 롤아웃이 길어질 경우 필요할 수 있으므로 리더십 위임 또는 에스컬레이션을 예약하세요.
3. 사용자 교육 제공 및 인식 제고 - 직원들에게 새로운 보안 조치와 제로 트러스트 환경 유지 관리에 필요한 역할에 대해 교육합니다. 강력한 암호, 다중 인증, 정기적인 보안 업데이트와 같은 보안 관행의 중요성을 강조합니다.
4. 변경 관리 - 제로 트러스트 도입과 관련된 조직적, 문화적 변화에 대응하기 위한 포괄적인 변경 관리 계획을 수립합니다. 도입의 이점과 근거를 직원들에게 전달하고 우려 사항이나 저항이 있는 부분을 해결합니다. 원활한 전환을 위해 지속적인 지원과 지침을 제공합니다.

3단계: 모니터링 및 지속적인 개선

제로 트러스트 구현의 세 번째이자 마지막 단계는 모니터링과 지속적인 개선입니다. 이 단계에는 포괄적인 모니터링 및 분석 프로그램을 수립하고, 포괄적인 인시던트 대응 계획을 수립하고, 이해관계자와 사용자에게 정기적으로 피드백을 요청하는 작업이 포함됩니다.

1. 지속적인 모니터링 - 포괄적인 모니터링 및 분석 프로그램을 구축하여 보안 태세를 지속적으로 평가하고 잠재적 이상을 탐지합니다. 고급 보안 도구 및 기술을 사용하여 사용자 동작, 네트워크 트래픽 및 시스템 활동을 모니터링합니다.
2. 인시던트 대응 및 해결 계획 - 제로 트러스트 원칙에 부합하는 포괄적인 인시던트 대응 계획을 세웁니다. 명확한 에스컬레이션 경로를 설정하고, 역할과 책임을 정의하고, 가능한 경우 자동화된 인시던트 대응 메커니즘을 구현합니다. 인시던트 대응 계획을 정기적으로 테스트하고 업데이트합니다.
3. 피드백 및 평가 받기 - 이해관계자와 사용자에게 정기적으로 피드백을 요청하여 제로 트러스트 아키텍처(ZTA)의 효과에 대한 인사이트를 수집합니다. 보안 태세, 운영 효율성 및 사용자 경험에 미치는 영향을 측정하기 위해 정기적인 평가 및 평가를 수행합니다. 피드백 및 평가 결과를 사용하여 개선이 필요한 영역을 파악합니다. 시간이 지남에 따라 ZTA가 변경될 것으로 예상하고 개발 팀이 최소한의 노력이나 중단으로 이러한 업데이트를 구현하는 방법을 고려합니다.

섹션 요약

이러한 단계별 도입 접근 방식을 따라 조직은 위험과 중단을 최소화하면서 ZTA로 효과적으로 전환할 수 있습니다. 다음 섹션에서는 CXO, VP, 고위 관리자를 위한 주요 고려 사항과 권장 사항을 다루면서 제로 트러스트 구현으로 성공을 달성하기 위한 모범 사례를 논의합니다.

제로 트러스트로 성공을 거두기 위한 모범 사례

제로 트러스트 아키텍처(ZTA)를 성공적으로 도입하려면 전략적 접근 방식과 모범 사례 준수가 필요합니다. 이 섹션에서는 CXO, VP, 고위 관리자가 제로 트러스트를 성공적으로 도입하는 데 도움이 되는 일련의 모범 사례를 소개합니다. 조직은 다음 권장 사항을 따라 강력한 보안 기반을 구축하고 제로 트러스트 접근 방식의 이점을 실현할 수 있습니다.

- 명확한 목표 및 비즈니스 성과 정의 - 클라우드 운영의 목표와 원하는 비즈니스 성과를 명확하게 정의합니다. 이러한 목표를 제로 트러스트 원칙에 맞게 조정하여 비즈니스 성장과 혁신을 지원하는 동시에 강력한 보안 기반을 구축합니다.
- 포괄적인 평가 수행 - 현재 IT 인프라, 애플리케이션 및 데이터 자산에 대한 포괄적인 평가를 수행합니다. 종속성, 기술 부채, 잠재적인 호환성 문제를 파악합니다. 이 평가를 통해 도입 계획을 세우고 중요도, 복잡성, 비즈니스 영향에 따라 워크로드의 우선순위를 정할 수 있습니다.
- 도입 계획 개발 - 워크로드, 애플리케이션 및 데이터를 클라우드로 이동하기 위한 단계별 접근 방식을 설명하는 세부 도입 계획을 통합합니다. 도입 단계, 타임라인, 종속성을 정의합니다. 주요 이해관계자를 참여시키고 그에 따라 리소스를 할당합니다.
- 조기 구축 시작 – 제로 트러스트를 분석하고 논의하는 대신 실제로 구축하고 배포하기 시작하면 조직 내에서 제로 트러스트가 어떤 모습일지 확실하게 표현할 수 있는 능력이 크게 향상됩니다.
- 경영진 후원 확보 - 제로 트러스트 구현을 위한 경영진 후원 및 지원을 확보합니다. 이 이니셔티브를 지지하고 필요한 리소스를 할당할 수 있도록 다른 최고 경영진의 참여를 유도합니다. 성공적인 구현에 필요한 문화 및 조직 변화를 추진하려면 리더십의 의지가 반드시 있어야 합니다.
- 거버넌스 프레임워크 구현 - 제로 트러스트 구현을 위한 역할, 책임, 의사 결정 프로세스를 정의하는 거버넌스 프레임워크를 만듭니다. 보안 통제, 위험 관리 및 규정 준수의 책임과 소유권을 명확하게 정의합니다. 거버넌스 프레임워크를 정기적으로 검토하고 업데이트하여 진화하는 보안 요구 사항에 맞게 조정합니다.
- 부서 간 협업 지원 - 다양한 사업부, IT 팀 및 보안 팀 간의 협업과 커뮤니케이션을 장려합니다. 제로 트러스트 구현 전반에서 조율과 조정을 촉진하기 위해 공동 책임 문화를 조성합니다. 잦은 상호 작용, 지식 공유 및 공동 문제 해결을 장려합니다.
- 데이터 및 애플리케이션 보호 - 제로 트러스트는 리소스와 애플리케이션에 액세스하는 최종 사용자에만 적용되는 것이 아닙니다. 워크로드 내부와 워크로드 간에도 제로 트러스트 원칙을 구현해야 합니다. 데이터 센터 내에서도 사용 가능한 모든 컨텍스트를 사용하여 강력한 ID, 마이크로 세분화, 권한 부여 등의 동일한 기술 원칙을 적용합니다.
- 심층 방어 제공 - 여러 계층의 보안 제어를 사용하여 심층 방어 전략을 실행합니다. 다중 인증(MFA), 네트워크 세분화, 암호화, 이상 탐지와 같은 다양한 보안 기술을 결합하여 포괄적인 보호를 제공합니다. 각 계층이 다른 계층을 보완하여 강력한 방어 시스템을 구축해야 합니다.

- 강력한 인증 요구 - 모든 리소스에 액세스하는 모든 사용자에 대해 MFA와 같은 강력한 인증 메커니즘을 시행합니다. 제로 트러스트에 대한 높은 수준의 인증 보장을 제공하고 광범위한 보안 이점(예: 피싱 방지)을 제공하는 FIDO2 하드웨어 기반 보안 키와 같은 최신 MFA를 고려하는 것이 가장 좋습니다.
- 권한 부여 중앙 집중화 및 개선 - 특히 모든 액세스 시도를 승인합니다. 프로토콜 세부 사항에 따라 연결별 또는 요청별로 수행해야 합니다. 요청별이 이상적입니다. ID, 디바이스, 동작, 네트워크 정보 등 사용 가능한 모든 컨텍스트를 사용하여 보다 세분화되고 적응력이 뛰어나며 정교한 권한 부여 결정을 내릴 수 있습니다.
- 최소 권한 원칙 사용 - 최소 권한 원칙을 이행하여 사용자에게 직무 수행에 필요한 최소 액세스 권한을 부여합니다. 직무, 책임, 비즈니스 요구 사항에 따라 액세스 권한을 정기적으로 검토하고 업데이트합니다. 적시 액세스 프로비저닝 구현
- 권한이 필요한 액세스 관리 사용 - 권한이 필요한 액세스 관리(PAM) 솔루션을 구현하여 권한 있는 계정을 보호하고 중요 시스템에 대한 무단 액세스 위험을 줄입니다. PAM 솔루션은 권한이 필요한 액세스 제어, 세션 기록, 감사 기능을 제공하여 조직이 가장 민감한 데이터와 시스템을 보호하는 데 도움을 줍니다.
- 마이크로 분할 사용 - 네트워크를 더 작고 격리된 세그먼트로 나눕니다. 마이크로 분할을 사용하여 사용자 역할, 애플리케이션 또는 데이터 민감도를 기반으로 세그먼트 간에 엄격한 액세스 제어를 적용할 수 있습니다. 불필요한 네트워크 경로, 특히 데이터로 이어지는 경로를 모두 제거하도록 하세요.
- 보안 경고 모니터링 및 대응 - 클라우드 환경에서 포괄적인 보안 모니터링 및 인시던트 대응 프로그램을 구현합니다. 클라우드 네이티브 보안 도구 및 서비스를 사용하여 실시간으로 위협을 탐지하고, 로그를 분석하고, 인시던트 대응을 자동화합니다. 명확한 인시던트 대응 절차를 수립하고, 정기적인 보안 평가를 수행하고, 이상 또는 의심스러운 활동을 지속적으로 모니터링합니다.
- 지속적인 모니터링 사용 - 보안 인시던트를 빠르고 효과적으로 탐지하고 이에 대응하려면 지속적인 모니터링을 구현합니다. 고급 보안 분석 도구를 사용하여 사용자 동작, 네트워크 트래픽 및 시스템 활동을 모니터링합니다. 경고 및 알림을 자동화하여 적시에 인시던트에 대응할 수 있도록 합니다.
- 보안 및 규정 준수 문화 조성 - 조직 전체에 보안 및 규정 준수 문화를 장려합니다. 보안 모범 사례, 제로 트러스트 원칙 준수의 중요성, 안전한 클라우드 환경 유지를 직원의 역할에 대한 교육을 실시합니다. 정기적인 보안 인식 교육을 실시하여 직원들이 소셜 엔지니어링에 주의를 기울이고 데이터 보호 및 개인정보 보호와 관련된 책임을 이해하도록 합니다.
- 소셜 엔지니어링 시뮬레이션 사용 - 소셜 엔지니어링 시뮬레이션을 수행하여 소셜 엔지니어링 공격에 대한 사용자의 취약성을 평가합니다. 시뮬레이션 결과를 사용하여 사용자 인식을 개선하고 잠재적 위협에 대응할 수 있는 맞춤형 교육 프로그램을 마련합니다.

- 지속적인 교육 장려 - 계속되는 보안 교육 및 리소스를 제공하여 지속적인 교육 및 학습 문화를 구축합니다. 진화하는 보안 모범 사례에 대해 사용자에게 계속 알려줍니다. 사용자가 경계를 늦추지 않고 의심스러운 활동이 있으면 즉시 신고하도록 권장합니다.
- 지속적 평가 및 최적화 - 클라우드 환경을 정기적으로 평가하여 개선이 필요한 부분을 찾습니다. 클라우드 네이티브 도구를 사용하여 리소스 사용 및 성능을 모니터링하고 취약성 평가와 침투 테스트를 수행하여 약점을 식별하여 해결합니다.
- 거버넌스 및 규정 준수 프레임워크 수립 - 조직이 업계 표준 및 규제 요구 사항을 준수할 수 있도록 거버넌스 및 규정 준수 프레임워크를 개발합니다. 프레임워크에서 데이터 및 시스템을 무단 액세스, 사용, 공개, 중단, 수정 또는 파괴로부터 보호하기 위한 정책, 절차 및 제어를 정의합니다. 규정 준수 지표를 추적 및 보고하고, 정기적인 감사를 실시하고, 규정 미준수 문제를 즉시 해결하기 위한 메커니즘을 구현합니다.
- 협업 및 지식 공유 장려 - ZTA 도입에 관련된 팀 간의 협업과 지식 공유를 장려합니다. 이를 위해 IT, 보안 및 사업부 간의 부서 간 커뮤니케이션 및 협업을 촉진합니다. 또한 조직에서는 포럼, 워크숍, 지식 공유 세션을 마련하여 이해를 증진하고 문제를 해결하며 도입 과정 전반에 걸쳐 얻은 교훈을 공유할 수 있습니다.

핵심 고려 사항

이 가이드에서는 성공적인 제로 트러스트 아키텍처(ZTA) 전략을 개발하기 위한 필수적인 측면을 살펴보았습니다. 이 섹션에는 제시된 권장 가이드의 핵심 고려 사항이 요약되어 있습니다.

- 제로 트러스트 원칙 이해 - 제로 트러스트는 기존 네트워크 제어나 네트워크 경계에만 전적으로 또는 근본적으로 의존하지 않는 디지털 자산에 대한 보안 제어를 제공하는 데 초점을 맞춘 개념적 모델이자 관련 메커니즘입니다. 대신 네트워크 제어에는 ID, 디바이스, 동작 및 기타 풍부한 컨텍스트와 신호가 추가되어 보다 세분화되고 지능적이며 적응력이 뛰어나고 지속적인 액세스 결정을 내릴 수 있습니다. 최소 권한, 마이크로 분할, 지속적 인증, 적응형 권한 부여와 같은 제로 트러스트의 핵심 원칙을 숙지하세요.
- 명확한 목표 정의 - ZTA 도입의 목표와 원하는 비즈니스 성과를 명확하게 정의합니다. 이러한 목표를 제로 트러스트 원칙에 맞게 조정하여 비즈니스 성장과 혁신을 지원하는 동시에 강력한 보안 기반을 보장합니다.
- 포괄적인 평가 수행 - 기존 IT 인프라, 애플리케이션 및 데이터 자산에 대한 철저한 평가를 수행합니다. 종속성, 기술적 부채, 호환성 문제를 파악하여 도입 전략을 수립합니다.
- ZTA 도입 계획 개발 - 워크로드, 애플리케이션 및 데이터를 클라우드로 이동하기 위한 단계별 접근 방식을 설명하는 세부 계획을 세웁니다. 규정 준수 요구 사항 및 애플리케이션 현대화와 같은 요소를 고려합니다.
- 강력한 ZTA 구현 - 세분화된 액세스 제어, 강력한 인증 메커니즘 및 지속적인 모니터링을 시행하는 ZTA를 설계하고 구현합니다. 보다 효율적인 ZTA 도입을 위해 AWS Verified Access, Amazon VPC Lattice 등의 클라우드 네이티브 제로 트러스트 서비스를 사용합니다.
- 데이터 및 애플리케이션 보안의 우선순위 지정 - 강력한 ID, 마이크로 분할, 권한 부여 등의 제로 트러스트 원칙을 적용하여 사용 가능한 모든 컨텍스트를 제공하십시오. 시스템 및 리소스에 액세스하는 사용자와 백엔드 구성 요소 내부 및 백엔드 구성 요소 간의 통신 및 데이터 흐름에 이 컨텍스트를 사용합니다.
- 모니터링 및 인시던트 대응 프레임워크 수립 - 클라우드 환경에서 강력한 보안 모니터링 및 인시던트 대응 기능을 구현합니다. 실시간 위협 탐지, 로그 분석 및 인시던트 대응 자동화에 Amazon Inspector, AWS Security Hub CSPM, Amazon GuardDuty 등의 클라우드 네이티브 보안 도구를 사용합니다.
- 보안 및 규정 준수 문화 조성 - 조직 전체에 보안 인식 및 규정 준수 문화를 장려합니다. 보안 모범 사례와 안전한 클라우드 환경 유지를 직원의 역할에 대한 교육을 실시합니다.
- 지속적인 평가 및 최적화 - 클라우드 환경, 보안 제어, 운영 프로세스를 정기적으로 평가합니다. 인사이트를 수집하고 리소스 사용률, 비용 관리 및 성능을 최적화하려면 Amazon CloudWatch, AWS Security Hub CSPM 등의 클라우드 네이티브 분석 및 모니터링 도구를 사용합니다.

- 거버넌스 및 규정 준수 프레임워크 수립 - 업계 표준과 규제 요구 사항에 부합하는 거버넌스 및 규정 준수 프레임워크를 개발합니다. 보안, 개인정보 보호 및 규정 준수 표준을 준수하는 데 도움이 되는 정책, 절차 및 제어를 정의합니다.

다음 단계

제로 트러스트 아키텍처(ZTA) 도입은 조직의 태세를 개선하고 위험을 줄이는 가장 안전한 방법 중 하나입니다. 이 권장 가이드는 원칙 이해부터 준비 상태 평가, 필요한 구성 요소 구현에 이르기까지 제로 트러스트를 구현하기 위한 포괄적인 로드맵을 제공합니다.

이 워크스트림 또는 도메인의 다음 단계에는 다음이 포함됩니다.

- 도입 계획 구현
- ZTA 구현
- 정기 보안 평가 수행
- 지속적으로 클라우드 환경 및 보안 제어 최적화

ZTA는 강력한 보안 기반을 확보하기 위해 지속적인 모니터링, 평가 및 조정이 필요한 지속적인 프로세스입니다. 이 가이드에 설명된 모범 사례를 따라 조직은 보안 태세를 강화하고, 규정 준수를 보장하고, 민감한 데이터를 보호할 수 있습니다.

FAQ

이 섹션에서는 제로 트러스트 아키텍처(ZTA) 설계 및 구현에 대해 자주 묻는 질문에 대한 답변을 제공합니다.

제로 트러스트란 무엇인가요?

제로 트러스트는 기존 네트워크 제어나 네트워크 경계에만 전적으로 또는 근본적으로 의존하지 않는 디지털 자산에 대한 보안 제어를 제공하는 데 초점을 맞춘 개념적 모델이자 관련 메커니즘입니다. 대신 네트워크 제어에는 ID, 디바이스, 동작 및 기타 풍부한 컨텍스트와 신호가 추가되어 보다 세분화되고 지능적이며 적응력이 뛰어나고 지속적인 액세스 결정을 내릴 수 있습니다.

제로 트러스트 아키텍처를 구현 AWS 서비스 하는 데 도움이 되는 것은 무엇입니까?

AWS 는 AWS Identity and Access Management (IAM), Amazon Virtual Private Cloud(VPC), Amazon VPC Lattice AWS Verified Access, Amazon Verified Permissions, Amazon API Gateway, Amazon GuardDuty 등 제로 트러스트 구현을 지원할 수 있는 여러 서비스를 제공합니다.

를 사용하여 데이터 보안을 보장하려면 어떻게 해야 하나요 AWS?

AWS 는 저장 및 전송 중 데이터 암호화를 위한 AWS Key Management Service (AWS KMS), 네트워크 격리를 위한 Amazon Virtual Private Cloud(VPC) 및 보안 인증 정보의 안전한 저장 및 검색 AWS Secrets Manager 과 같은 서비스를 제공합니다.

제로 트러스트 환경에서 규정 준수 요구 사항을 AWS 지원할 수 있습니까?

예, 다양한 규제 요구 사항을 충족하는 데 도움이 되는 규정 준수 프로그램 및 서비스가 AWS 있습니다. 는 규정 AWS 준수 보고서에 AWS Config 대한 액세스를 AWS Artifact 제공하고 규정 준수에 대한 지속적인 모니터링 및 평가를 지원합니다.

제로 트러스트 환경에서 보안을 자동화하기 위한 AWS 도구나 서비스가 있나요?

AWS 는 보안 조사 결과를 중앙 집중화하고 자동화 AWS Security Hub CSPM하는와 같은 서비스와 보안 정책을 정의하고 적용하기 위한 AWS Config 규칙을 제공합니다.

를 사용하여 제로 트러스트 클라우드 환경에서 지속적인 모니터링 및 인시던트 대응을 보장하려면 어떻게 해야 합니까? AWS

AWS 는 실시간 모니터링과 AWS CloudTrail 로깅 및 분석을 위해 Amazon CloudWatch와 같은 서비스를 제공합니다. 인시던트 대응 모범 사례를 보려면 AWS 보안 사고 대응 안내서를 참조하세요.

리소스

참조

- What is a cloud center of excellence and why should your organization create one? - 이 블로그 게시물에서는 CCoE의 개요, 효과적인 CCoE를 만드는 방법에 대한 모범 사례 등을 제공합니다.
- 제로 트러스트 AWS-이 페이지에서는 AWS 환경의 제로 트러스트 보안 원칙 및 모범 사례에 대한 개요를 제공합니다.
- 제로 트러스트 아키텍처: AWS 관점 -이 블로그 게시물은 제로 트러스트가 구현되는 방식에 대한 정의와 지침 원칙을 공유합니다 AWS.
- AWS Identity and Access Management (IAM) 사용 설명서 -이 설명서는 제로 트러스트 아키텍처의 중요한 구성 요소인 IAM에서 사용자 액세스 및 권한을 관리하는 방법에 대한 포괄적인 설명서를 제공합니다.
- AWS Security Hub CSPM - 보안 알림 및 규정 준수 상태에 대한 포괄적인 보기를 제공하는 서비스인 Security Hub CSPM에 대해 알아봅니다 AWS 계정.
- AWS Well-Architected Framework – AWS에서 안전하고 성능이 뛰어나고 복원력이 뛰어나고 효율적인 아키텍처를 구축하는 방법에 대한 지침을 제공하는 Well-Architected Framework를 살펴보세요.
- AWS 보안 인시던트 대응 가이드 -이 가이드에서는 조직 AWS 클라우드 환경 내의 보안 인시던트에 대응하기 위한 기본 사항에 대한 개요를 제공합니다. 클라우드 보안 및 인시던트 대응 개념의 개요를 제공하고 보안 문제에 대응하는 고객이 사용할 수 있는 클라우드 기능, 서비스 및 메커니즘을 파악합니다.

도구

- Amazon API Gateway
- AWS Artifact
- AWS CloudTrail
- Amazon CloudWatch()
- AWS Config
- Amazon GuardDuty
- AWS Identity and Access Management

- AWS Key Management Service
- AWS Secrets Manager
- AWS Security Hub CSPM
- AWS Verified Access

문서 기록

아래 표에 이 가이드의 주요 변경 사항이 설명되어 있습니다. 향후 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하십시오.

변경 사항	설명	날짜
업데이트 추가됨	제로 트러스트 아키텍처의 주요 구성 요소 섹션에 정보가 추가되고, 제로 트러스트 도입을 위한 조직 준비 상태 평가 섹션이 변경되고, 모범 사례 섹션에 정보가 추가되고, FAQ가 변경되었습니다.	2023년 12월 4일
최초 게시	—	2023년 6월 19일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.