CLOUDFLARE

백서

Zero Trust 아키텍처로 이어지는 로드맵

네트워크를 변환하고 보안을 최신화하는 데 필요한 단계, 도구, 팀에 대해 알아보세요

목차

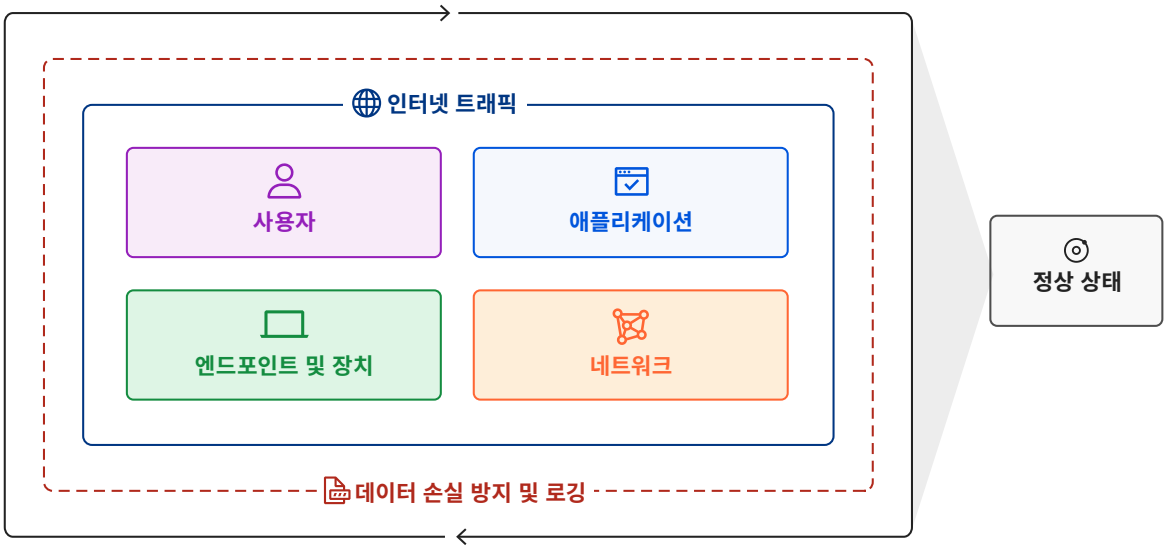
소개

전통적인 네트워크 아키텍처는 누군가가 네트워크에 접속하면 암묵적으로 신뢰 수준이 주어지는 경계 네트워크라는 개념에 따라 구축되었습니다. 클라우드 호스팅, 원격 근무, 기타 최신화로 전환하면서 기존의 경계 네트워크 아키텍처에 어려움이 생겼습니다.

이러한 어려움은 Zero Trust 아키텍처를 구현하여 해결할 수 있습니다. 이러한 아키텍처는 비즈니스를 오고 가는 모든 트래픽이 검증되고 승인되도록 보장합니다. 직원의 생산성과 연결 상태를 방해하지 않고도 Zero Trust 아키텍처를 구현하는 작업을 단계적으로 수행할 수 있습니다.

보안 전문가가 작성한 이 가이드에서는 벤더에 구애받지 않는 Zero Trust 아키텍처 및 구현 타임라인 예시를 보여줍니다. 이 타임라인에서는 Zero Trust 여정을 처음부터 시작하는 조직을 가정하지만, 모든 조직에 유용합니다.

포괄적인 Zero Trust 아키텍처를 구현하는 과정에는 조직 보안에 고려해야 할 일곱 가지 주요 구성 요소가 있습니다. 아래에 나열하는 구성 요소 및 참조 아키텍처 섹션의 순서와 자신의 구현 순서가 일치해야 할 필요는 없습니다.



Zero Trust 아키텍처의 구성 요소

	구성 요소	목표	작업 수준	페이지
1단계	인터넷 트래픽	글로벌 DNS 필터링 배포	▮	9
	애플리케이션	인바운드 이메일을 모니터링하고 피싱 시도를 필터링함	▮	13
	DLP 및 로그	SaaS 도구에서 잘못된 구성 및 공개적으로 공유된 데이터 파악	▮	20
2단계	사용자	기업 ID 수립	▮▮	5
	사용자	모든 애플리케이션에 기본 MFA 시행	▮	6
	애플리케이션	HTTPS 및 DNSSEC 시행	▮	17
	인터넷 트래픽	SSL 뒤의 위협을 차단하거나 격리	▮▮	9-10
	애플리케이션	공개적으로 주소를 지정할 수 있는 앱에 ZT 정책 시행	▮	14-16
	애플리케이션	계층 7 공격으로부터 애플리케이션 보호	▮	16
	네트워크	앱 서비스 목적으로 인터넷에 공개된 모든 인바운드 포트 닫기	▮	12
3단계	애플리케이션	모든 기업 애플리케이션의 인벤토리 마련	▮▮	13-14
	애플리케이션	SaaS 애플리케이션에 ZT 정책 시행	▮▮	14-16
	네트워크	사용자 네트워크 액세스에 세그먼트 적용	▮▮▮	11
	애플리케이션	비공개로 주소를 지정할 수 있는 핵심 애플리케이션에 ZTNA 적용	▮	14-16
	장치	기업 장치를 제어할 수 있도록 MDM/UEM 구현	▮▮	7
	DLP 및 로그	중요한 데이터를 정의하고 해당 데이터의 위치를 확인	▮▮	18-19
	사용자	하드웨어 기반 인증 토큰 전송	▮▮	6
	DLP 및 로그	알려진 위협 행위자에 대한 최신 정보 파악	▮	21
4단계	사용자	MFA 기반 하드웨어 토큰 시행	▮▮	6
	애플리케이션	모든 애플리케이션에 ZT 정책 시행 및 네트워크 액세스	▮▮▮	14-16
	DLP 및 로그	로그 검토, 정책 업데이트, 완화 목적으로 SOC 수립	▮▮	20
	장치	엔드포인트 보호 구현	▮▮	7
	장치	모든 기업 장치, API, 서비스의 인벤토리 마련	▮	8
	네트워크	분기간 연결에 광대역 인터넷 사용	▮▮▮	11-12
	DLP 및 로그	중요한 앱에서의 직원 활동을 로그하고 검토함	▮▮	18
	DLP 및 로그	애플리케이션에서 중요한 데이터가 유출되는 것을 막음	▮▮▮	19
	정상 상태	새 리소스의 정책을 시행할 DevOps 접근 방식	▮▮	22
	정상 상태	온램프 리소스에 자동 크기 조정 구현	▮▮▮	22-23

각 단계에 필요한 다양한 작업 수준을 다음과 같이 나타냈습니다.

- ▮ - **소규모 작업.** 개인이나 소규모 팀에서 수행할 수 있음
- ▮▮ - **중간 규모 작업.** 팀과 사전 준비가 필요함
- ▮▮▮ - **대규모 작업.** 여러 팀과 프로젝트 계획이 필요함

Zero Trust로 이어지는 로드맵

사용자

직원, 협력업체, 고객이 사용자에 포함됩니다. Zero Trust를 구현하려는 조직이라면 실제로 신뢰하려는 대상과 더불어 신뢰를 제공할 수단, 즉 ID에 대한 개념을 먼저 정확하게 그려놓아야 합니다. 그런 다음에 사용자의 ID를 안전하게 인증할 방법을 마련해야 합니다.

기업 ID 수립

작업 수준	**- 중간 규모 작업**
관여하는 팀	• ID 공급자를 담당하는 팀 (일반적으로 보안팀 또는 IT팀) • 직원 및 파트너가 사용하는 내부 앱을 관리하는 관리자
제품	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
요약	기업 애플리케이션에 대한 사용자 액세스를 정확하게 인증하고 승인하려면 통합 기업 ID가 필요합니다. 기업 ID가 일관되면 세분화된 정책을 애플리케이션에 더욱 수월하게 시행할 수 있습니다. **고려해야 할 추가 요소:** • 회사에서 인수 합병이 활발하게 이루어지나요? ID 저장소는 어떻게 통합하려 하나요? • 사용 중인 비 웹 기반 인증 프로토콜이 있나요? (예: Active Directory, NTLM, Kerberos)
단계	1. ID 공급자에 모든 기업 사용자를 추가합니다 a. 이러한 값은 Workday, ADP 등의 HR 시스템으로 동기화할 수 있는 경우가 많습니다 2. 각 사용자의 정보가 정확한지 확인합니다 3. 새 사용자 등록 정보를 전송하여 로그인 자격 증명을 설정합니다

모든 애플리케이션에 멀티 팩터 인증 시행

작업 수준	- **소규모 작업** (기본 MFA를 적용할 경우) - **중간 규모 작업** (하드 키를 사용할 경우)
관여하는 팀	• ID 공급자를 담당하는 팀 (일반적으로 보안팀 또는 IT팀) • 직원 및 파트너가 사용하는 내부 앱을 관리하는 관리자
제품	**ID 공급자:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **애플리케이션 역방향 프록시:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access(ZPA) **하드 키:** Yubico
요약	멀티 팩터 인증(MFA)은 피싱이나 데이터 유출로 사용자 자격 증명이 도난당하는 것을 방지하는 최고의 보호 방법입니다. 대부분의 MFA는 IdP에서 바로 실행할 수 있습니다. IdP와 바로 통합되지 않은 애플리케이션에는 애플리케이션 전면에 애플리케이션 역방향 프록시를 사용하여 MFA를 시행하는 것을 고려하세요.
단계	1. 내부 사용자에게 곧 MFA를 시행한다는 사실을 알립니다. SMS로 등록하거나 앱 기반 인증자를 이용하는 옵션을 제공합니다 2. IdP에 MFA를 시행합니다 3. IdP와 통합되지 않은 애플리케이션 전면에 애플리케이션 역방향 프록시를 시행합니다 4. (추가) 메일을 이용하거나 대면하여 직원에게 하드웨어 키를 나누어줍니다 5. (추가) 가장 중요한 애플리케이션에 하드웨어 키 전용 MFA를 적용합니다

엔드포인트 및 장치

엔드포인트 및 장치에는 조직 내부에 위치하거나 조직의 데이터에 액세스할 권한이 있는 모든 장치, API, 소프트웨어 서비스가 포함됩니다. 조직은 먼저 장치, API, 서비스의 전체 집합을 이해해야 합니다. 그런 다음 장치, API, 서비스의 컨텍스트를 기반으로 Zero Trust 정책을 구현할 수 있습니다.

모바일 장치 관리 구현

작업 수준	**- 중간 규모 작업**
관여하는 팀	• IT팀
제품	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
요약	대부분의 Zero Trust 아키텍처에서는 최소한 사용자 컴퓨터의 하위 집합에 소프트웨어를 설치해야 합니다. 대부분의 조직에서는 소프트웨어를 관리하고 사용자 장치 인벤토리 전체의 구성을 관리하는 데 모바일 장치 관리(MDM) 방식을 이용합니다.
단계	자세한 내용은 MDM 벤더 사이트를 참조하세요.

엔드포인트 보호 구현

작업 수준	**- 중간 규모 작업**
관여하는 팀	• 보안팀 • IT팀
제품	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
요약	엔드포인트 보호 소프트웨어는 사용자의 컴퓨터에 설치되어 장치에 영향을 미칠 수 있는 알려진 위협을 검사합니다. 엔드포인트 보호 소프트웨어는 OS 패치 및 업데이트 규정을 준수하도록 시행하는 데 사용할 수도 있습니다. 엔드포인트 보호 소프트웨어에서 보내는 신호를 애플리케이션 액세스 관리 정책에서 사용할 수 있고, 사용해야 합니다.
단계	1. MDM을 사용해 사용자의 컴퓨터에 엔드포인트 보호 소프트웨어를 설치합니다 2. 엔드포인트 보호 플랫폼에서 위협 보호 및 규정 준수 제어를 실행합니다

모든 장치, API, 서비스의 인벤토리 마련

작업 수준	**- 소규모 작업**
관여하는 팀	• 보안팀 • IT팀
제품	**장치 인벤토리:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **API/서비스 인벤토리:** Cloudflare application connector, Zscaler Private Access(ZPA)
요약	엔드포인트 보호 소프트웨어 및 자산 관리 소프트웨어를 이용하여 사용자에게 널리 분포되어 있는 모든 장치를 추적할 수 있습니다. 정확한 장치 목록을 유지하여 어떤 장치가 유효한지 추적해야 하며 특정 애플리케이션에 액세스할 권한이 있어야 합니다. API와 서비스도 마찬가지로 인벤토리에서 파악하여 목록을 유지해야 합니다. 네트워크 검사를 활용해, 내부 네트워크나 외부 네트워크를 거쳐 통신할 수 있다고 새로 확인된 API 및 소프트웨어 서비스를 식별할 수 있습니다.
단계	1. MDM을 사용해 사용자의 컴퓨터에 엔드포인트 보호 소프트웨어를 설치합니다 2. 네트워크 내에 API/서비스 스캐너를 설치합니다

인터넷 트래픽

인터넷 트래픽에는 조직의 통제 범위 밖인 웹 사이트로 향하는 사용자 트래픽이 모두 포함됩니다. 이는 비즈니스 관련 작업부터 개인 웹 사이트 이용에 이르기까지 다양할 수 있습니다. 모든 아웃바운드 트래픽은 맬웨어 및 악의적 사이트에 취약합니다. 조직에서는 인터넷으로 향하는 사용자 트래픽을 확인할 가시성과 통제 능력을 마련해야 합니다.

알려진 위협이 있거나 위험할 수 있는 목적지로 향하는 DNS 요청 차단

작업 수준	**- 소규모 작업**
관여하는 팀	• 라우터나 컴퓨터 구성에 액세스할 권한이 있는 IT팀 • 보안팀
제품	**DNS 필터링:** Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
요약	DNS 필터링은 라우터 구성을 통해서 적용하거나 사용자 컴퓨터에서 직접 적용할 수 있습니다. 이 필터링은 알려진 악의적 웹 사이트에서 가장 빠르게 사용자를 보호할 수 있는 방법 중 하나입니다.
단계	**DNS 필터링:** 사무실 WiFi의 DNS 확인 구성을 업데이트하여 적절한 DNS 확인 서비스를 가리키게 합니다. 알려진 악의적 사이트를 차단하는 데 이용할 수 있습니다.

SSL/TLS 뒤의 위협을 차단하거나 격리

작업 수준	**- 중간 규모 작업**
관여하는 팀	• 라우터나 컴퓨터 구성에 액세스할 권한이 있는 IT팀 • 보안팀
제품	**TLS 암호화:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access(ZIA) **브라우저 격리:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

SSL/TLS 뒤의 위협을 차단하거나 격리(계속)

요약	일부 위협은 SSL 뒤에 숨겨져 있으며, HTTPS 검사만 수행해서는 차단할 수 없습니다. 사용자를 더 보호하려면, TLS 암호화를 활용해 SSL 뒤의 위협에서 사용자를 더 심층적으로 보호해야 합니다.
단계	**TLS 암호화:** 1. 사용자 컴퓨터에 올바른 클라이언트 소프트웨어가 설치되어 있는지 확인합니다 a. 아웃바운드 웹 트래픽을 방해할 수 있는 VPN이나 기타 소프트웨어가 있는지 장치를 점검합니다 2. TLS 암호화를 제공하도록 장치에 루트 인증서를 구성합니다 3. 사용자 트래픽을 어느 시점에 복호화하는지에 관한 정책을 실행합니다 a. 이는 인증서 고정 방식을 이용하는 사이트에 대하여 수행해야 합니다 b. 일부 회사에서는 사용자의 개인 트래픽(예: 은행 업무, 소셜 미디어 등) 복호화 과정도 우회합니다 **브라우저 격리:** 1. 장치상의 클라이언트 소프트웨어나 격리 링크를 통해 브라우저 격리를 배포할 수 있습니다. 두 가지 접근법을 모두 고려해야 합니다.

네트워크

네트워크에는 조직 내의 모든 공개 네트워크, 비공개 네트워크, 가상 네트워크가 포함됩니다. 조직은 먼저 기존의 네트워크 집합을 이해하고 이를 세그먼트화하여 내부망 내 이동을 방지해야 합니다. 그런 다음에 사용자, 엔드포인트, 장치가 어떤 네트워크 세그먼트에 액세스할 수 있는지 세밀하게 제어할 Zero Trust 정책을 생성할 수 있습니다.

사용자 네트워크 액세스에 세그먼트 적용

작업 수준	**- 대규모 작업**
관여하는 팀	• 보안팀 • IT팀
제품	**Zero Trust 네트워크 액세스(ZTNA):** Cloudflare Zero Trust(Access 및 Gateway 함께 사용), Netskope Private Access, Zscaler Private Access(ZPA)
요약	일반적으로 사용자는 VPN을 사용하거나 사무실 네트워크를 이용하는 동안 전체 비공개 네트워크에 액세스할 수 있습니다. Zero Trust 프레임워크에서 사용자는 지정된 작업을 완료하는 데 필요한 특정 네트워크 세그먼트에만 액세스할 수 있어야 합니다. Zero Trust 네트워크 솔루션을 이용하면 사용자가 로컬 네트워크에 원격으로 액세스하면서도 사용자, 장치, 기타 요소에 따라 세분화된 정책을 따를 수 있습니다.
단계	1. 사설 네트워크에서 ZTNA를 이용할 수 있게 합니다 a. 일반적으로 애플리케이션 커넥터, GRE 또는 IPSec 터널입니다 2. MDM을 사용해 사용자 장치에 ZTNA 클라이언트를 설치합니다 3. 사설 네트워크에서 사용자 액세스를 세그먼트화하는 정책을 설정합니다

분기간 연결에 광대역 인터넷 사용

작업 수준	**- 대규모 작업**
관여하는 팀	• 네트워크 엔지니어링팀 • IT팀
제품	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore

분기간 연결에 광대역 인터넷 사용(계속)

요약	사설 네트워크 위치(예: 데이터 센터 및 분기)간의 연결은 일반적으로 다중 프로토콜 레이블 스위칭(MPLS) 라인이나 통신 공급자가 서비스하는 기타 형태의 사설 링크를 이용하여 수행됩니다. 이러한 MPLS 링크는 보통 비용이 많이 듭니다. 상용 인터넷 품질이 높아지면서, 조직에서는 보안 터널을 통해 인터넷 상의 트래픽을 라우팅하여 동일한 수준의 보안 액세스를 적은 비용으로 제공할 수 있습니다.
단계	1. MPLS가 연결된 위치 중 시작할 두 군데를 선택합니다. 이러한 위치에는 어떤 형태로든 인터넷이 연결되어야 합니다. 2. 클라우드 WAN 공급자의 에지 네트워크에 이중화 Anycast GRE 또는 IPsec 터널 한 쌍을 인터넷 회로를 통해 설정합니다. 3. 터널 간의 상태와 연결을 확인합니다. 프로덕션 트래픽과 최대한 유사하도록 트래픽 워크로드의 성능(처리량, 대기 시간, 패킷 손실, 지터)을 테스트합니다. 4. MPLS에서 인터넷 터널로 프로덕션 트래픽을 마이그레이션하도록 라우팅 정책을 바꿉니다 5. MPLS가 연결된 다음 위치에서 반복합니다 6. MPLS 회로의 사용을 중지합니다

애플리케이션 서비스 목적으로 인터넷에 공개된 모든 인바운드 포트 닫기

작업 수준	**- 소규모 작업**
관여하는 팀	• 네트워크 엔지니어링팀
제품	**Zero Trust 역방향 프록시:** Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access(ZPA)
요약	공개된 인바운드 네트워크 포트는 스캐닝 기술로 찾을 수 있으며 흔하게 이용되는 공격 벡터입니다. Zero Trust 역방향 프록시를 이용하면 인바운드 포트를 공개하지 않고도 웹 애플리케이션을 안전하게 노출할 수 있습니다. 애플리케이션의 DNS 레코드는 유일하게 공개적으로 확인할 수 있는 애플리케이션 레코드입니다. DNS 레코드는 Zero Trust 정책으로 보호됩니다. 추가 보안 계층으로, Zero Trust 액세스 서비스를 이용해 내부/프라이빗 DNS를 활용할 수 있습니다(자세한 내용은 아래 참조).
단계	1. 역방향 프록시 애플리케이션 커넥터를 설치합니다. 일반적으로 동일 네트워크에 위치한 디먼 또는 가상 머신입니다 2. 역방향 프록시 애플리케이션을 애플리케이션 커넥터에 연결합니다 3. 방화벽 규칙을 이용해 사설 네트워크의 인바운드 포트를 모두 닫습니다

애플리케이션

애플리케이션에는 조직 데이터가 위치하거나 비즈니스 프로세스가 수행되는 리소스가 모두 포함됩니다. 조직에서는 존재하는 애플리케이션을 먼저 이해한 다음에 각 애플리케이션에 적용할 Zero Trust 정책을 수립해야 하고, 일부 사례의 경우에는 승인되지 않은 애플리케이션을 차단해야 합니다.

이메일 애플리케이션을 모니터링하고 피싱 시도를 필터링함

작업 수준	**- 소규모 작업**
관여하는 팀	• 이메일 공급자 구성을 담당하는 팀(일반적으로 IT팀)
제품	**클라우드 이메일 보안:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **브라우저 격리:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
요약	이메일은 공격자가 직원들에게 자유롭게 액세스할 수 있는 소수의 통신 채널에 속합니다. 보안 이메일 게이트웨이를 배포하는 과정은 직원에게 악의적이거나 신뢰할 수 없는 이메일이 전송되지 않도록 해주는 중요한 단계입니다. 이와 더불어, 보안팀에서는 완전히 차단하기에는 의심스러운 정도가 충분하지 않아 격리된 브라우저의 링크를 떼어 놓을 옵션을 고려해야 합니다.
단계	1. 보안 이메일 게이트웨이 서비스를 가리키도록 도메인의 MX 레코드를 구성합니다 2. 처음 몇 주간 긍정 오류를 모니터링합니다 3. (추가) 의심스러운 이메일 링크인지 확실하지 않은 경우에 맞게 링크 기반 브라우저 격리 접근법을 구현합니다.

모든 기업 애플리케이션의 인벤토리 마련

작업 수준	**- 중간 규모 작업**
관여하는 팀	• 보안팀
제품	**섀도우 IT를 파악할 수 있는 보안 웹 게이트웨이 및 CASB:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access(ZIA)

모든 기업 애플리케이션의 인벤토리 마련(계속)

요약	보안팀이 비즈니스 전체에서 사용되는 애플리케이션의 전체 인벤토리를 파악하고 있는 것이 중요합니다. 흔히 "섀도우 IT"라고 하는데, 보안팀에서는 승인되지 않았거나 알려지지 않은 애플리케이션이 비즈니스 전반에 사용되고 있는 경우를 발견하곤 합니다. TLS 복호화가 가능한 보안 웹 게이트웨이를 이용해 애플리케이션을 파악할 수 있습니다. 보안 웹 게이트웨이는 승인되지 않은 애플리케이션 또는 애플리케이션 테넌트(예: 개인 Dropbox 계정)를 차단하는 데도 사용될 수 있습니다.
단계	1. 보안 웹 게이트웨이에서 섀도우 IT 스캐닝을 실행합니다 2. 사용자 장치에 보안 웹 게이트웨이 클라이언트가 설치되어 있도록 합니다 3. 2~3주간 사용자의 트래픽을 허용합니다 4. 파악한 애플리케이션의 목록을 검토합니다 5. 승인되지 않은 애플리케이션은 보안 웹 게이트웨이 정책으로 차단해야 합니다 6. 승인된 애플리케이션은 Zero Trust 정책으로 보호해야 합니다

애플리케이션에 Zero Trust 정책 시행

작업 수준	- **소규모 작업**(가장 중요한 애플리케이션에 시행) - **대규모 작업**(모든 애플리케이션에 시행)
관여하는 팀	• 보안팀 • 애플리케이션 개발팀 • IT팀
제품	**Zero Trust 역방향 프록시:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access(ZPA) **Zero Trust 네트워크 액세스(ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access(ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB **원격 브라우저 격리:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation

애플리케이션에 Zero Trust 정책 시행(계속)

요약	애플리케이션은 액세스를 승인하고 인증하기 전에 사용자 ID, 장치, 네트워크 컨텍스트를 고려하는 Zero Trust 정책으로 보호해야 합니다. 애플리케이션에는 최소 권한을 시행하는 세분화된 정책이 있어야 하며, 중요한 데이터가 포함된 애플리케이션이라면 특히 그렇습니다. 주요 애플리케이션 유형은 세 가지이며 Zero Trust 보안 모델은 유형에 따라 다릅니다. 주요 애플리케이션 유형은 다음과 같습니다. 1. 자체 호스팅된 비공개 애플리케이션(기업 네트워크에서만 주소 지정 가능) 2. 자체 호스팅된 공개 애플리케이션(인터넷을 통해 주소 지정 가능) 3. SaaS 애플리케이션 **참고:** 장치 컨텍스트 또는 규정 준수 상태가 필수 보안 정책이라면, 일반적으로 장치 클라이언트 소프트웨어가 필요합니다.
단계	**자체 호스팅된 비공개 애플리케이션** 1. 애플리케이션과 Zero Trust 정책 계층 사이에 암호화된 터널을 구축합니다. 일반적으로 이는 "애플리케이션 커넥터"이거나 GRE이거나 IPSec 터널입니다 2. ZTNA 장치 클라이언트 사용자가 프라이빗 DNS 확인자를 이용할 수 있게 합니다 3. 사용자, 장치, 네트워크 컨텍스트에 따라 정책을 구축해 애플리케이션에 액세스할 수 있는 사용자를 설정합니다 **자체 호스팅된 공개 애플리케이션** 1. 권한 있는 DNS 또는 CNAME 레코드를 애플리케이션 역방향 프록시로 이동시킵니다 2. 애플리케이션 네트워크에서 인바운드 포트가 모두 닫혀있는지 확인합니다 3. 사용자, 장치, 네트워크 컨텍스트에 따라 정책을 구축해 애플리케이션에 액세스할 수 있는 사용자를 설정합니다 **SaaS 애플리케이션** SaaS 애플리케이션에는 Zero Trust 정책을 시행할 기타 옵션이 몇 가지 있습니다 **ID 프록시** Cloudflare, Netskope, Zscaler는 자체 호스팅된 역방향 프록시 애플리케이션과 같은 정책을 시행할 수 있게 해주는 ID 프록시를 제공합니다. 이렇게 하려면 SaaS 애플리케이션의 SSO 공급자로 ID 프록시를 설정해야 합니다 1. 기존에 SSO 통합이 되어 있다면 SaaS 앱에서 제거합니다 2. ID 프록시를 SaaS 애플리케이션과 통합합니다 3. 사용자를 생성하고 업데이트할 올바른 SAML 속성이 전송되었는지 확인합니다 4. 사용자, 장치, 네트워크 컨텍스트에 따라 정책을 작성합니다

애플리케이션에 Zero Trust 정책 시행(계속)

단계	**보안 웹 게이트웨이 및 SSO(Single Sign On)** 또 다른 방법으로, 기존 SSO 공급자를 이용하여 SaaS 애플리케이션에 액세스할 권한이 있는 사용자와 없는 사용자를 제어할 수 있습니다. 그런 다음 전용 IP 주소가 있는 보안 웹 게이트웨이를 사용해서 트래픽 검사로 관리되는 장치의 사용자만 SaaS 애플리케이션에 액세스하도록 할 수 있습니다. 1. SSO 공급자에 SaaS 애플리케이션을 추가합니다 2. 어떤 사용자를 인증할지 지정하는 정책을 작성합니다 3. 보안 웹 게이트웨이 인스턴스의 IP 주소를 SaaS 애플리케이션의 IP 허용 목록에 추가합니다(대부분의 SaaS 앱은 기본 보안 설정에서 IP 허용 목록을 지원합니다) 4. SaaS 애플리케이션에 액세스할 수 있는 사용자를 제어하는 보안 웹 게이트웨이 정책을 작성합니다

계층 7 공격으로부터 애플리케이션 보호(DDoS, 삽입, 봇 등)

작업 수준	- 소규모 작업
관여하는 팀	• 보안팀 • 애플리케이션 개발팀
제품	Akamai, AWS, Azure, Cloudflare, GCP
요약	자체 호스팅된 애플리케이션은 모두 DDoS, 코드 삽입, 봇 등의 계층 7 공격에 취약합니다. 보안팀은 비공개적으로 주소를 지정하는 자체 호스팅 애플리케이션과 공개적으로 주소를 지정하는 자체 호스팅 애플리케이션 모두의 전면에 웹 애플리케이션 방화벽 및 DDoS 방어를 배포해야 합니다.
단계	1. 공개 애플리케이션의 권한 있는 DNS 레코드를 추가합니다 2. 웹 애플리케이션 방화벽 및 DDoS 방어를 실행합니다

HTTPS 및 DNSSEC 시행

작업 수준	**- 소규모 작업**
관여하는 팀	• 보안팀 • 애플리케이션 개발팀
제품	Akamai, AWS, Azure, Cloudflare, GCP
요약	자체 호스팅된 웹 애플리케이션은 HTTPS 및 DNSSEC을 활용해야 합니다. 이렇게 패킷 스니핑이나 도메인 하이재킹의 가능성을 방지할 수 있습니다.
단계	1. 공개 애플리케이션의 권한 있는 DNS 레코드를 추가합니다 2. HTTPS를 엄격하게 설정하고 DNSSEC를 실행합니다

데이터 손실 방지 및 로깅

여기까지 아키텍처의 모든 Zero Trust 요소를 구축했다면, 아키텍처에서는 네트워크 내부에서 발생하는 작업에 대하여 방대한 데이터가 생성됩니다. 이제는 데이터 손실 방지 및 로깅을 구현해야 합니다. 이는 중요한 데이터를 비즈니스 내부에 보관하고 잠재적인 데이터 유출 기회를 알리는 프로세스와 도구입니다. 조직에서는 중요한 정보가 어디에 위치하는지 먼저 파악해야 합니다. 그런 다음에야 중요한 정보에 액세스하여 유출되는 상황을 차단할 수 있도록 Zero Trust 제어를 구축할 수 있습니다.

중요한 애플리케이션에서 트래픽을 로그하고 검토할 프로세스 수립

작업 수준	**- 중간 규모 작업**
관여하는 팀	• 보안팀
제품	**보안 웹 게이트웨이(SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access(ZIA) **SIEM(Security Incident and Event Monitoring):** DataDog, Splunk, SolarWinds
요약	보안 웹 게이트웨이 솔루션은 사용자 트래픽 로그를 SIEM 도구로 전달하는 기능을 갖추고 있습니다. 보안팀은 중요한 애플리케이션으로 향하는 트래픽 로그를 정기적인 활동으로 검토해야 합니다. 비정상적이거나 악의적인 트래픽을 알리도록 SIEM에 차츰 특정한 경고를 설정하고 조정할 수 있습니다.
단계	1. 중요한 애플리케이션으로 향하는 모든 사용자 트래픽이 SWG를 사용하여 프록시 설정되도록 합니다 2. SWG와 SIEM 간에 로그를 푸시하거나 가져오는 기능을 실행합니다 3. 보안팀이 트래픽 로그를 검토할 특정한 기간 간격을 정합니다 4. 차츰 나타나는 결과에 따라 SIEM에 경고를 구성합니다

중요한 데이터를 정의하고 해당 데이터의 위치를 확인

작업 수준	**- 중간 규모 작업**
관여하는 팀	• 보안팀 • 규정 준수/법무팀
제품	**SIEM(Security Incident and Event Monitoring):** DataDog, Splunk, SolarWinds

중요한 데이터를 정의하고 해당 데이터의 위치를 확인(계속)

요약	업계에 따라 중요한 데이터는 크게 다릅니다. 기술 회사는 소스 코드를 보호하는 데 집중하는 반면, 의료 공급자는 HIPAA 규정 준수에 큰 비중을 부여합니다. 회사의 중요한 데이터가 무엇이고 어디에 있는지 확고히 하는 것이 중요합니다. 중요한 데이터를 정확히 정의하고 인벤토리로 정리하면 데이터 손실 방지 도구를 구현하는 데 도움이 될 수 있습니다.
단계	1. SIEM 도구나 보안 웹 게이트웨이에서 바로 트래픽 로그를 검토해 대상 애플리케이션 및 데이터 저장소를 파악합니다 2. 기존 중요한 데이터의 인벤토리를 마련합니다

애플리케이션에서 중요한 데이터가 유출되지 않도록 방지합니다

작업 수준	**- 대규모 작업**
관여하는 팀	• 보안팀 • IT팀 • 규정 준수/법무팀
제품	**인라인 데이터 손실 방지(DLP):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access(ZIA)
요약	인라인 DLP 솔루션은 사용자 트래픽과 파일 업로드/다운로드에서 중요한 데이터를 검사합니다. 중요한 데이터는 잘 알려져 있는 미리 정의된 목록(예: PII, SSN, 신용카드 등)에서 사용 가능하거나 관리자가 특정 패턴을 직접 구성할 수 있습니다. 중요한 애플리케이션에는 DLP 제어를 실행해야 하며, 모든 사용자 트래픽으로 확장할 수 있습니다.
단계	1. DLP 공급자의 클라이언트 소프트웨어를 설치합니다 2. 연결에 지장을 초래할 기존 VPN이나 기타 도구가 없는지 확인합니다 3. TLS 암호화가 실행되고 있으며 각 사용자의 컴퓨터에 루트 인증서가 있는지 확인합니다 4. DLP 제어를 실행합니다 5. DLP 차단 이벤트를 모니터링해 올바르게 차단했는지, 긍정 오류인지 확인합니다

SaaS 도구에서 잘못된 구성 및 공개적으로 공유된 데이터 파악

작업 수준	**- 소규모 작업**
관여하는 팀	• 보안팀
제품	**API 기반 클라우드 액세스 보안 브로커(CASB):** Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
요약	CASB는 API 통합으로 주요 SaaS 애플리케이션과 통합됩니다. 통합된 다음 CASB는 SaaS 애플리케이션을 스캔하여 알려진 잘못된 보안 구성과 공개적으로 공유된 데이터가 있는지 확인합니다. 보안팀에서는 CASB 결과를 검토할 수 있게 정기적인 케이던스를 마련해야 합니다.
단계	1. 공급자의 API 통합 지침으로 각 SaaS 애플리케이션을 연결합니다 2. 각 SaaS 애플리케이션에 스캔을 수행합니다 3. 스캔 결과를 검토하고 적절하다면 각 SaaS 애플리케이션을 수정합니다

로그 검토, 정책 업데이트, 완화 목적의 보안 운영 센터(SOC) 수립

작업 수준	**- 중간 규모 작업**
관여하는 팀	• 보안팀
제품	**없음**
요약	Zero Trust 프레임워크에서는 SOC가 보안팀에 중요한 기능을 수행합니다. SOC는 로그 정보와 보안 경고를 검토하고 모든 핵심 보안 제품에 전체적으로 Zero Trust 정책을 조정하는 데 중점을 두어야 합니다.
단계	1. SIEM이나 보안 제품에서 바로 로그를 검토합니다 2. 경고나 비정상적인 활동을 확인합니다 3. 결과에 따라 각 도구의 Zero Trust 정책을 업데이트합니다

알려진 위협 행위자에 대한 최신 정보 파악

작업 수준	**- 소규모 작업**
관여하는 팀	• 보안팀
제품	**위협 인텔리전스 공급자:** Cloudflare Radar, CISA, OWASP
요약	알려진 위협 행위자와 악의적 웹 사이트의 목록을 작성하는 데 중점을 두는 여러 공급자가 있습니다. 공격자로부터 사용자를 보호할 수 있게 이와 같은 위협 피드를 보안 웹 게이트웨이에 자동으로 로드할 수 있습니다.
단계	1. 보안 웹 게이트웨이에 위협 피드를 연결합니다 2. DNS 및 HTTP 필터링에서 위협 보호를 실행합니다

정상 상태

조직의 다른 요소에 모두 Zero Trust 아키텍처를 구축했다면, 일련의 작업으로 조직을 Zero Trust 정상 상태로 바꾸어서 아키텍처를 발전시키면서 일관성을 유지할 수 있습니다.

모든 새 리소스에 일관적으로 정책을 시행할 DevOps 접근 방식 이용

작업 수준	**- 대규모 작업**
관여하는 팀	• 보안팀 • 애플리케이션 개발팀
제품	**인프라 자동화:** Ansible, Puppet, Terraform
요약	개발자는 인프라 자동화 도구를 이용하여 애플리케이션 개발 파이프라인의 일부로 Zero Trust 보안을 자동으로 배포할 수 있습니다. Zero Trust 역방향 프록시 보호로 애플리케이션을 배포할 때 트리거될 내부 테스트를 수립합니다.
단계	1. 새로운 애플리케이션에 적용할 표준 정책을 규정합니다 2. Zero Trust 역방향 프록시 보호가 필요한 애플리케이션 배포 프로세스에 테스트를 추가합니다

온램프 리소스에 자동 크기 조정 구현

작업 수준	**- 대규모 작업**
관여하는 팀	• 보안팀 • 애플리케이션 개발팀
제품	**로드 밸런서:** Akamai, Cloudflare **인프라 자동화:** Ansible, Puppet, Terraform

온램프 리소스에 자동 크기 조정 구현(계속)

요약	개별 애플리케이션 인프라에 과부하가 절대로 걸리지 않도록 해주는 효과적인 도구로 로드 밸런서를 이용할 수 있습니다. 애플리케이션 서버 하나에 문제가 생기기 시작할 때 이중화 수준을 제공할 수도 있습니다. 인프라 자동화 도구를 이용해 특정한 트래픽 임계값을 지날 때 새로운 리소스를 가동할 수도 있습니다.
단계	1. Zero Trust 역방향 프록시 애플리케이션 커넥터 전면에 로드 밸런서를 구성합니다 2. 트래픽 볼륨 및/또는 사용자의 지리적 위치에 따라 로드 밸런싱 규칙을 실행합니다. 3. 특정한 애플리케이션 집합에 로드가 충분히 생겼을 경우 새로운 가상 머신을 프로비저닝할 인프라 자동화 정책을 구현합니다

구현 타임라인 예시

Zero Trust 아키텍처를 배포하는 상황은 모두 유일무이하지만, 대부분의 프로젝트에서 따르는 일련의 공통 단계가 있습니다. 이는 Zero Trust 아키텍처 구현을 시작하는 비즈니스에 권장되는 타임라인입니다.

사고 경과		목표	관련 제품
1단계	☐	글로벌 DNS 필터링 배포	Cisco Umbrella DNS, Cloudflare Gateway, DNSFilter, Zscaler Shift
	☐	인바운드 이메일을 모니터링하고 피싱 시도를 필터링함	**클라우드 이메일 보안:** Cloudflare Area 1 Email Security, Mimecast, TitanHQ **브라우저 격리:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	SaaS 도구에서 잘못된 구성 및 공개적으로 공유된 데이터 파악	Cloudflare CASB, DoControl, Netskope, Zscaler CSPM
2단계	☐	기업 ID 수립	Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin
	☐	모든 애플리케이션에 기본 MFA 시행	**ID 공급자:** Microsoft Azure AD, Okta, Ping Identity PingOne, OneLogin **애플리케이션 역방향 프록시:** Microsoft Azure AD App Proxy, Akamai EAA, Cloudflare Access, Netskope Private Access, Zscaler Private Access(ZPA)
	☐	HTTPS 및 DNSSEC 시행	Akamai, AWS, Azure, Cloudflare, GCP
	☐	SSL 뒤의 위협을 차단하거나 격리	**TLS 암호화:** Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access(ZIA) **브라우저 격리:** Cloudflare Browser Isolation, Zscaler Cloud Browser Isolation
	☐	공개적으로 주소를 지정할 수 있는 앱에 ZT 정책 시행	**Zero Trust 역방향 프록시:** Azure App Proxy, Cloudflare Access, Netskope Private Access, Zscaler Private Access(ZPA)
	☐	계층 7 공격으로부터 애플리케이션 보호	Akamai, AWS, Azure, Cloudflare, GCP
	☐	앱 서비스 목적으로 인터넷에 공개된 모든 인바운드 포트 닫기	Akamai EAA, Cloudflare Access, Netskope, Zscaler Private Access(ZPA)
3단계	☐	모든 기업 애플리케이션의 인벤토리 마련	**섀도우 IT를 파악할 수 있는 보안 웹 게이트웨이 및 CASB:** Cloudflare Gateway, Microsoft Defender for Cloud Apps, Netskope Next Gen SWG, Zscaler Internet Access(ZIA)
	☐	SaaS 애플리케이션에 ZT 정책 시행	**Zero Trust 네트워크 액세스(ZTNA):** Cloudflare Access, Netskope Private Access, Zscaler Internet Access(ZIA) **CASB:** Cloudflare CASB, Netskope CASB, Zscaler CASB

	☐ 사용자 네트워크 액세스에 세그먼트 적용	**Zero Trust Network Access(ZTNA):** Cloudflare Zero Trust(Access 및 Gateway 함께 사용), Netskope Private Access, Zscaler Private Access(ZPA)
	☐ 비공개로 주소를 지정할 수 있는 핵심 애플리케이션에 ZTNA 적용	Cloudflare Access, Netskope Private Access, Zscaler Internet Access(ZIA)
	☐ 기업 장치를 제어할 수 있도록 MDM/UEM 구현	**Mac:** Jamf, Kandji **Windows:** Microsoft Intune
	☐ 중요한 데이터를 정의하고 해당 데이터의 위치 확인	DataDog, Splunk, SolarWinds
	☐ 하드웨어 기반 인증 토큰 전송	**하드 키:** Yubico
	☐ 알려진 위협 행위자에 대한 최신 정보 파악	Cloudflare Radar, CISA, OWASP
4단계	☐ MFA 기반 하드웨어 토큰 시행	**하드 키:** Yubico
	☐ 모든 애플리케이션에 ZT 정책 시행 및 네트워크 액세스	Cloudflare Access, Netskope Private Access, Zscaler Internet Access(ZIA)
	☐ 로그 검토, 정책 업데이트, 완화 목적으로 SOC 수립	해당사항 없음
	☐ 엔드포인트 보호 구현	VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender
	☐ 모든 기업 장치, API, 서비스의 인벤토리 마련	**장치 인벤토리:** VMWare Carbon Black, Crowdstrike, SentinelOne, Windows Defender, Oomnitza **API/서비스 인벤토리:** Cloudflare application connector, Zscaler Private Access(ZPA)
	☐ 분기간 연결에 광대역 인터넷 사용	Cloudflare Magic WAN, Cato Networks, Aryaka FlexCore
	☐ 중요한 애플리케이션에서 직원 활동을 로그하고 검토하는 프로세스 수립	**보안 웹 게이트웨이(SWG):** Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access(ZIA) **SIEM(Security Incident and Event Monitoring):** DataDog, Splunk, SolarWinds
	☐ 애플리케이션에서 중요한 데이터가 유출되는 것을 막음(예: PII, 신용카드, SSN 등)	Cisco Umbrella, Cloudflare Gateway, Netskope Next Gen SWG, Zscaler Internet Access(ZIA)
	☐ 모든 새 리소스에 정책을 시행할 DevOps 접근 방식 이용	Ansible, Puppet, Terraform
	☐ 온램프 리소스에 자동 크기 조정 구현	**로드 밸런서:** Akamai, Cloudflare **인프라 자동화:** Ansible, Puppet, Terraform

CLOUDFLARE

+82 70 4515 6893 | enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-3584.2022AUG09