백서

제로 트러스트 아키텍처 구축을 위한 청사진

목차

서론

제로 트러스트는 Forrester Research가 2009년에 처음 홍보하면서 알려진 개념으로 기업의 네트워크 경계를 통과한 모든 사용자나 애플리케이션에 제한 없는 접속을 제공하던 기존의 방법을 재정비해야 한다고 경고해 왔습니다. 모든 디바이스, 사용자, 네트워크 흐름을 확인한 후에 접속을 제공해야 한다는 개념입니다. 그 후 몇 년 동안 여러 가지 요인으로 인해 제로 트러스트 개념을 도입해야 하는 시급성은 더욱 커졌습니다.

오늘날의 하이브리드 인력은 다양한 위치에서 업무를 수행하며, BYOD 프로그램을 통해 직원들은 관리형 및 비관리형 디바이스를 모두 사용해 기업 애플리케이션과 리소스에 접속할 수 있습니다. 애플리케이션은 클라우드, 온프레미스, 하이브리드 등 모든 곳에서 호스팅됩니다. 이러한 변화의 결과로 과거의 네트워크 경계는 더 이상 존재하지 않게 되었습니다. 랜섬웨어 공격의 빈도와 정교함이 증가하면서 공격자가 방어 체계를 뚫고 들어올 가능성이 높아졌고, 일단 공격이 발생하면 비용도 증가했습니다. IBM의 2024년 데이터 유출 비용 보고서에 따르면 미국의 데이터 유출 평균 비용은 936만 달러로 세계에서 가장 높습니다. 또한 사물 인터넷(IoT) 디바이스 같은 네트워크 연결 디바이스가 증가하고 파트너 및 고객의 네트워크 접속에 대한 추가 요구사항이 결합되면서 기업의 공격 표면이 크게 확장되었습니다.

사이버 보안 환경이 진화하는 가운데 네트워크 및 보안 소프트웨어 벤더사는 신속히 기존 제품을 제로 트러스트로 브랜딩하거나 신제품을 출시했고 컨설턴트와 애널리스트는 새로운 약어와 시장 정의를 소개하고 있습니다. 보안팀은 이로 인해 복잡한 개념을 설명하고 제로 트러스트 전략으로 전환하기 위한 토대를 마련하는 구매 결정을 내리는 데 어려움을 겪고 있습니다.

이 백서는 어디에서 시작할지 파악하고 주요 차별화 포인트를 설명함으로써 보안팀에게 제로 트러스트 기술 투자에 대한 청사진을 제공하기 위해 작성되었습니다.

네트워크 보안 패러다임을 무너뜨리는 하이브리드 근무와 클라우드 애플리케이션

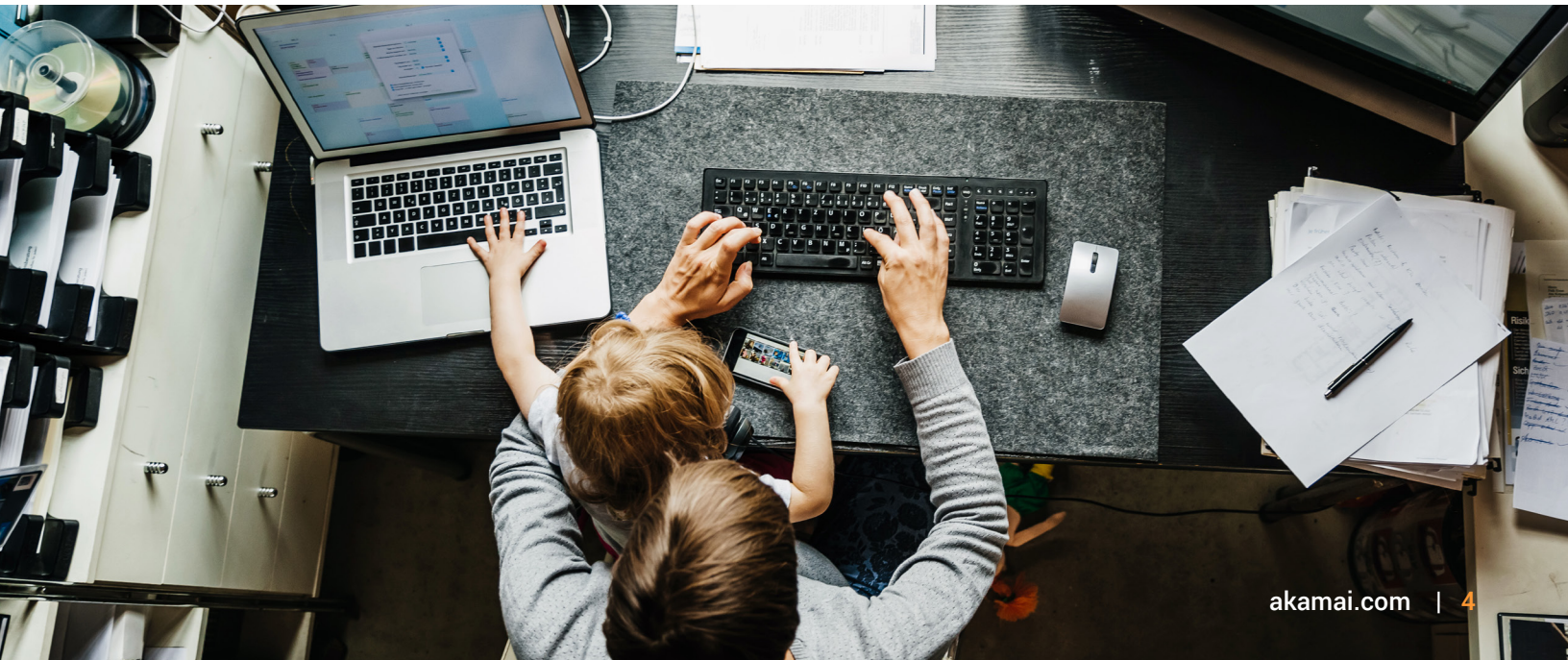
사람들이 일하는 시간, 방식, 장소는 사무실 외부로 이동했습니다.

따라서 네트워크 경계는 더 이상 존재하지 않으며, 적어도 인식할 수 있는 형태로는 존재하지 않습니다. 사용자가 경계 내부와 외부에 존재할 확률은 동일합니다. SaaS(Software as a Service)와 멀티클라우드 구축으로 사용하는 애플리케이션이 급증하고 있습니다. 위협이 진화하고 지속적으로 발생함에 따라 공격자가 일단 네트워크 내부에 들어오면 가장 중요한 자산에 접속할 수 있도록 의도치 않게 허용할 가능성이 커졌습니다. 포괄적인 제로 트러스트 프로그램이 마련되어 있지 않은 경우 내부로 들어온 공격자는 자유롭게 활동할 수 있습니다.

이건 그저 이론이 아닙니다. 최근 큰 손실이 발생한 데이터 유출 사건에서 알 수 있듯이 데이터 유출 사건의 거의 대부분은 네트워크 경계 내부에서 신뢰를 악용해 발생됩니다.

한편 네트워크 경계 내부에 배포되도록 설계된 애플리케이션의 보안 프로필이 최악인 경우가 많았습니다. 선의를 가진 인증된 직원들만 기업 시스템에 접근할 것이라고 생각하는 개발자가 해커 중 상당수가 인터넷 기반 애플리케이션을 악용해 공격한다는 사실을 알고 있는 오늘날의 코더만큼 방어적인 태도를 취했을까요?

마켓플레이스 전반에 걸쳐 이러한 문제를 해결하는 솔루션이 제로 트러스트입니다.



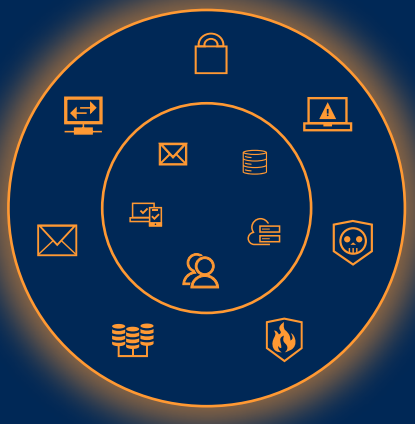
제로 트러스트 보안 아키텍처

제로 트러스트의 기본 개념은 상당히 간단하면서 강력합니다. 즉, 신뢰 여부는 위치의 문제가 아닙니다. 기업 방화벽 내부에 있다는 이유 하나만으로 누군가를 믿지 말아야 하며, 그 대신 위치에 관계없이 명시적으로 허용된 경우에만 작업을 신뢰해야 합니다. 궁극적으로 오직 일어나야 하는 것만 일어날 수 있습니다. 기업은 필요하지 않은 작업에 대한 모든 암묵적 신뢰를 제거해야 합니다. 예를 들어 회계 그룹의 일부만 접속해야 하는 재무 시스템에 대한 접속을 모든 사용자에게 부여하면 리스크만 일으킬 뿐 가치를 창출하지는 않습니다.

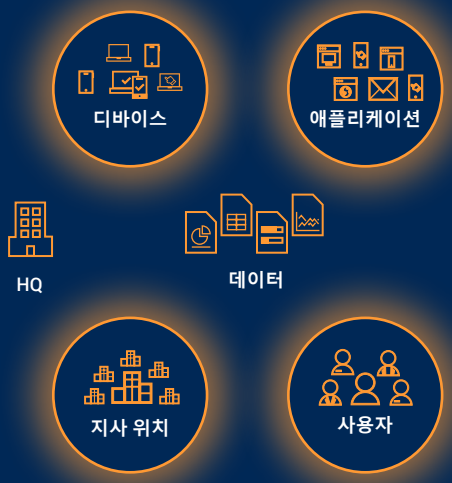
제로 트러스트의 입증 방식은 강력한 인증과 권한이며 시스템은 신뢰가 구축되기 전까지는 어떠한 데이터도 전송하지 않습니다. 또한, 애널리틱스와 로깅을 사용해 행동이 적절한지 확인하고 감염의 조짐을 계속해서 확인해야 합니다.

이러한 근본적인 변화로 인해 지난 10년 동안 등장했던 수많은 감염 사례를 극복할 수 있었습니다. 공격자는 경계 내에 진입했다는 이유만으로 더 이상 경계 내부의 취약점을 파고들어 민감한 데이터와 애플리케이션을 유출할 수 없게 되었습니다. 지금은 경계 자체가 없습니다. 이제는 애플리케이션과 사용자만이 존재하며, 양쪽 모두 서로 인증하고 권한을 확인해야만 접속이 이루어질 수 있습니다.

기존 보안 아키텍처



오늘날의 현실



기업은 제로 트러스트 아키텍처를 어떻게 구축할까요?

첫째, 모든 기업은 기존 환경에 대한 전략을 수립하고 신규 인력 채용 필요 여부와 시기를 결정해야 합니다. 본 백서는 프로세스의 핵심 단계만 집중 소개할 수 있지만 제로 트러스트 전략을 실행하는 데 도움이 되는 실제 제품은 세 가지 목표를 기반으로 해야 합니다.

1

아무것도 신뢰하지 말고 지속적으로 검증하라.

"아무것도 신뢰하지 말고 지속적으로 검증하라"라는 말은 일반적으로 생각하면 쉽게 들립니다. 모든 시스템과 모든 데이터에 대한 접속을 차단하면 네트워크가 잠깁니다. 가장 큰 문제는 대규모 비즈니스 중단을 초래하지 않고 지속적으로 검증하는 것입니다. 특히 대부분의 시스템이 암묵적 신뢰를 염두에 두고 설계된 경우 더욱 그렇습니다. 모든 종류의 접속에 대한 광범위한 가시성 및 제어와 정책을 적용하고 유지 관리하는 간단하고 실용적인 수단이 필요합니다.

2

검증된 후에도 최소한의 접속만 제공해야 합니다.

제로 트러스트 환경에서는 사용자를 검증한 후에 해당 업무에 필요한 접속만 제공해야 합니다.

3

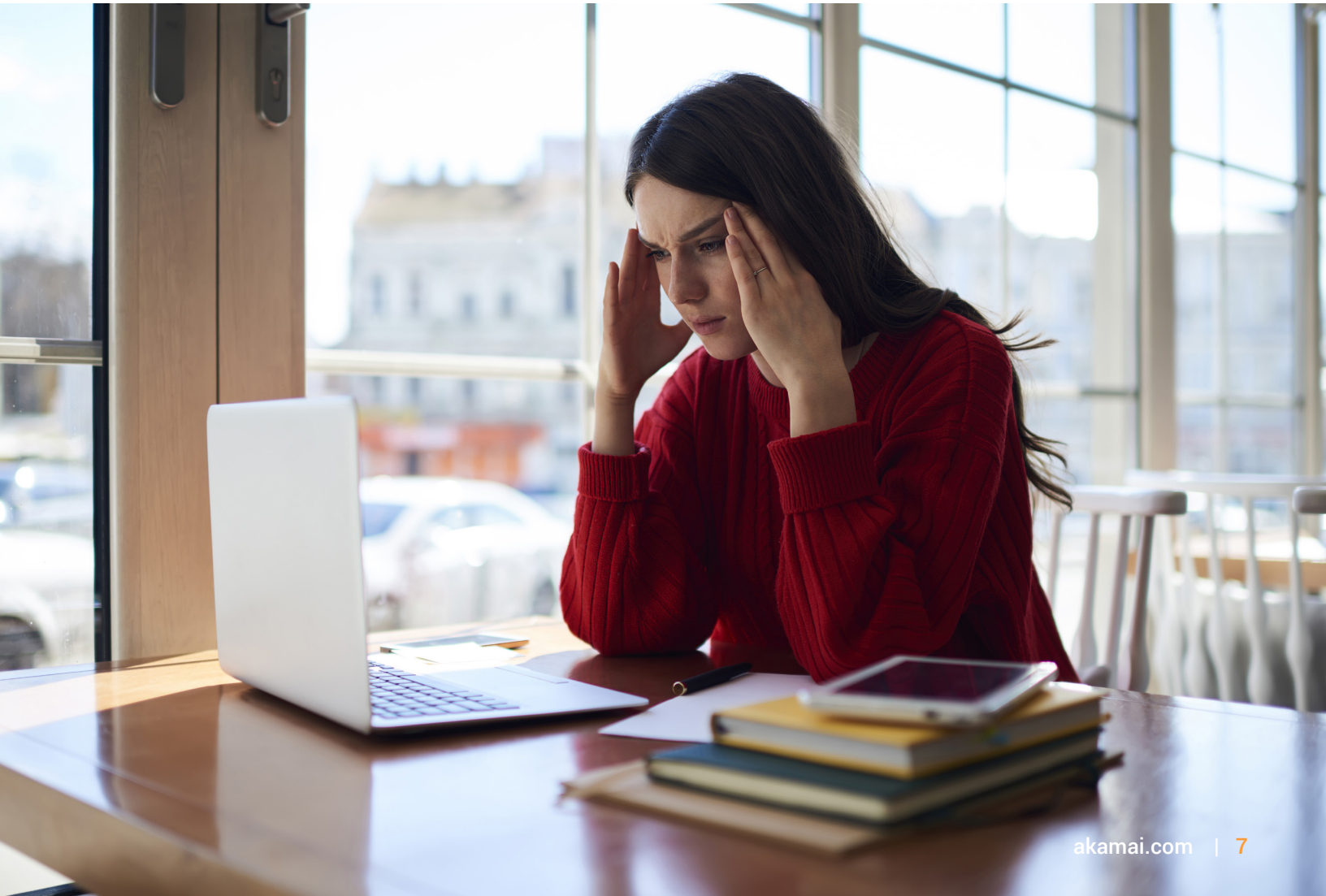
위협을 지속적으로 모니터링합니다.

대부분의 업계 전문가가 말하듯이 제로 트러스트는 지속적인 과정입니다. 기업의 방어 체계에 침입하려는 공격자가 점점 더 정교해짐에 따라 기업은 지속적으로 접속을 모니터링하고, 검증하고, 제한해야 합니다. 제로 트러스트 모델의 장점 중 하나는 공격자가 하는 일이 아니라 기업이 하는 일에 초점을 맞추고 있다는 것입니다. 진정한 제로 트러스트 정책이 도입되면 공격자는 기업이 한 번에 실행해야 하는 모든 것을 차단하기 어려워집니다. 이상적으로는 체인의 특정 지점에서 모든 공격을 차단할 수 있어야 합니다. 여기에는 아직 만들어지지 않은 공격을 차단할 수 있는 기능이 포함됩니다. 제로 트러스트는 제로데이 공격에 상관없이 방어하는 데 도움을 줄 수 있습니다.

제로 트러스트의 어두운 면

하지만 제로 트러스트를 구축하려는 기업은 이러한 불신과 접속 제한의 이면도 고려해야 합니다. 제로 트러스트의 기본 원리는 주로 허용 목록을 통해 접속을 제한하는 것입니다. 이것은 허용되는 것을 지정하는 방식입니다. 즉, 그 외의 모든 것은 거부됩니다. 그러나 공격자가 악성 캠페인을 진행하지 못하도록 막다 보면 종종 직원들이 업무를 제대로 못하도록 방해할 가능성도 커집니다. 또는 워크로드와 디바이스를 반복 검사하면 업무 지연과 중단으로 이어질 수 있습니다. 직원들이 효과적으로 일하지 못하게 만드는 제로 트러스트 전략은 전략이라고 할 수 없습니다.

강력한 제로 트러스트 전략은 보안과 접속 권한 간의 균형을 유지합니다. 효과적으로 달성할 수 있는 것과 보안팀의 리소스(예산 및 인력) 간의 균형도 유지해야 합니다.

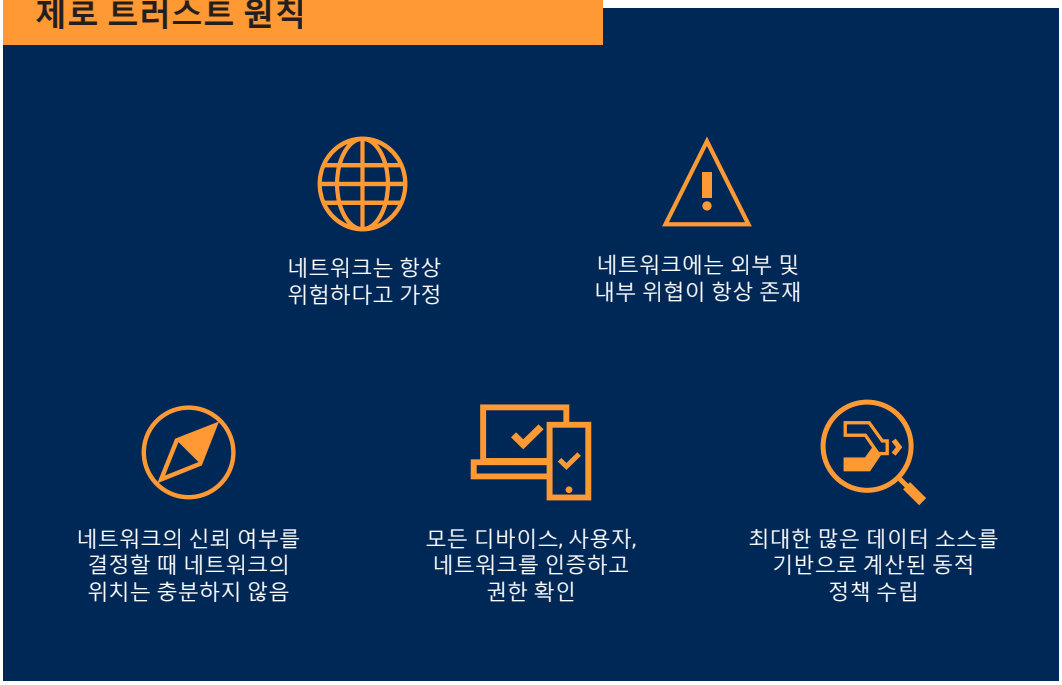


제로 트러스트의 구성요소

Forrester가 제로 트러스트 개념을 처음 소개한 지 15년이 되었습니다. 이제 많은 기업이 제로 트러스트 여정을 시작하며 복잡한 소프트웨어 제품 시장을 마주하고 있습니다. 오랫동안 사용되며 제로 트러스트 아키텍처의 일부를 담당하는 제품이 있는 반면 신제품도 등장했고, 많은 소프트웨어 공급업체가 제로 트러스트로 자사 제품을 신속하게 리브랜딩했습니다. 게다가 많은 애널리스트와 업계 관계자들은 "제로 트러스트는 제품이 아니라 포괄적인 전략입니다.", "제로 트러스트는 목적지가 아니라 여정입니다."라고 말합니다. 그러나 이렇게 자주 반복되는 주장은 제로 트러스트 기술 솔루션의 구매를 결정해야 하는 사람들에게 도움이 되지 못하며 실제로 더 많은 혼란을 야기할 수 있습니다.

기업은 하나의 제품으로 제로 트러스트를 구축할 수 없고 우선순위와 취약점이 다르기 때문에 그 출발점도 다릅니다. 하지만 기술 발전과 업계 통합 덕분에 이제 기업은 하나의 소스에서 제로 트러스트 정책을 구축하는 데 필요한 툴을 확보할 수 있습니다. 애널리스트 기업들도 이를 인식하기 시작했습니다.

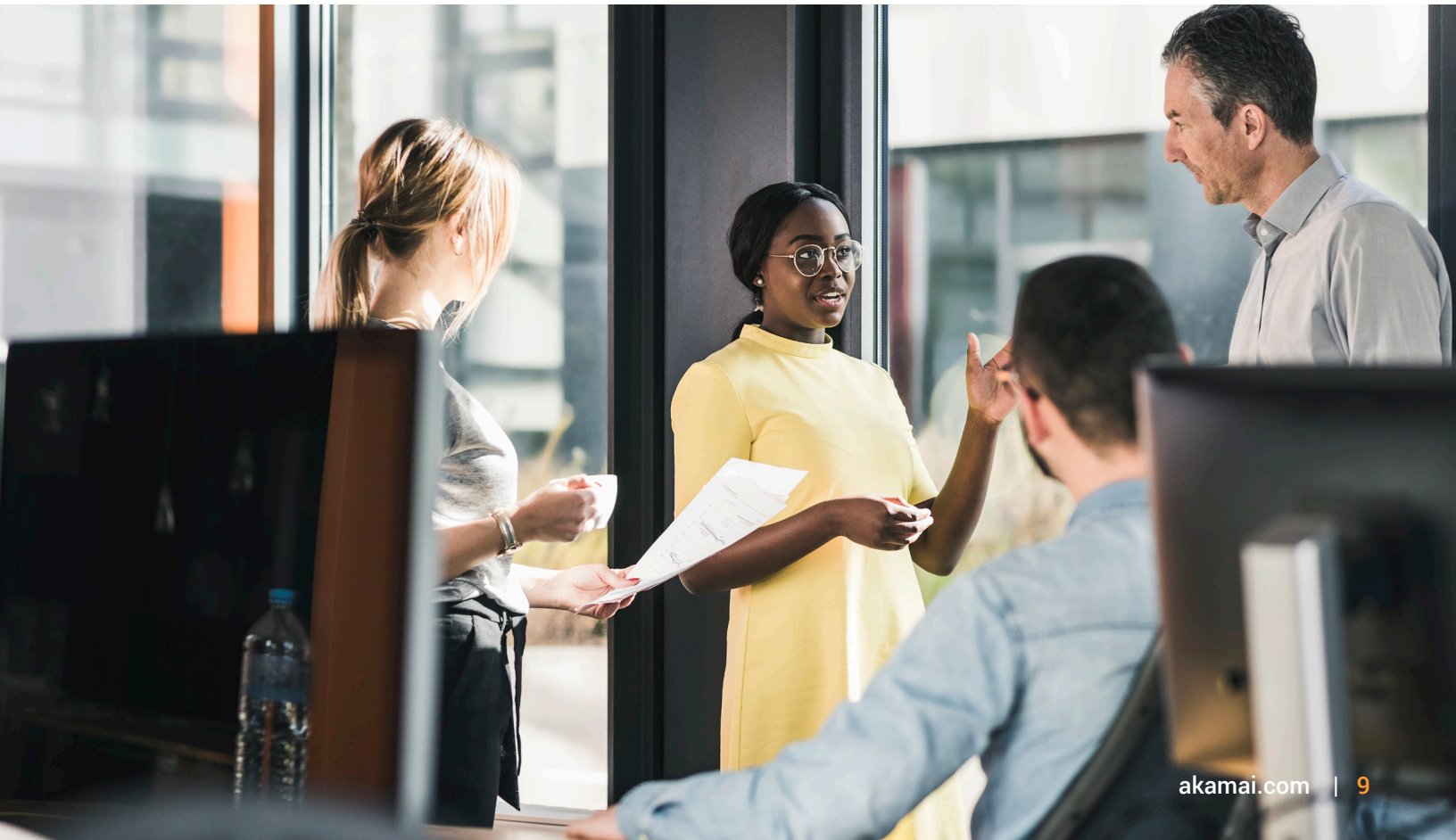
제로 트러스트 원칙



Gartner는 보안 웹 게이트웨이, 클라우드 접속 보안 브로커, 제로 트러스트 네트워크 접속(ZTNA)이 결합된 보안 서비스 엣지(SSE)를 조사합니다. Gartner는 제로 트러스트를 구축하기 위한 실용적인 프로젝트는 무엇일까요?라는 보고서에 '워크로드 투 워크로드 세그멘테이션'이라 불리는 마이크로세그멘테이션을 포함해 "실제로 이를 구축하려는 기업은 사용자 투 애플리케이션 세그멘테이션(ZTNA)과 워크로드 투 워크로드 세그멘테이션(ID 기반 세그멘테이션)이라는 두 가지 주요 프로젝트에 집중해야 한다"고 권장합니다.

마찬가지로 IDC는 제로 트러스트를 보안 접속과 세그멘테이션으로 구분하고 논리적 세그멘테이션, 접속 제어, 위협 탐지를 통해 컴퓨팅 시스템, 리소스, 데이터를 보호하는 데 사용되는 신규 기술과 레거시 기술에 대한 포괄적인 시각으로 정의합니다.

따라서 이러한 개별 시스템을 하나의 응집력 있는 전략으로 결합하는 것이 관건이 되었습니다. CIO, CISO, 기타 보안 전문가가 기업에 적합한 제로 트러스트 아키텍처를 구축할 때 고려해야 할 핵심 요소는 무엇일까요?



제로 트러스트 네트워크 접속

ZTNA는 제로 트러스트에 대한 전반적인 접근 방식과 혼동될 수 있는데 기술 스택의 기본적인 부분입니다. 보안 접속은 제로 트러스트 프레임워크의 주요 초기 단계입니다. 유감스럽게도 프로세스의 많은 요소와 마찬가지로 보안 접속은 아주 빠르게 복잡해지고 있습니다. 보안 접속은 이원론적인 결정이 아닙니다. 사용자와 애플리케이션이 광범위하게 분산됨에 따라 적절한 사용자에게 적절한 애플리케이션에 대한 적절한 접속 수준을 적시에 제공하는 것이 훨씬 더 복잡해졌습니다. 사실, 이제 사용자의 정의에는 직원뿐 아니라 고객, 공급업체, 파트너도 포함될 수 있습니다. 한편, 애플리케이션은 레거시 애플리케이션, SaaS 또는 모바일 앱을 포함할 수 있으며 데이터 센터, 인터넷 또는 클라우드 환경에 대한 접속을 필요로 합니다.

효과적인 ZTNA 솔루션은 사용자의 신원과 디바이스의 상태를 확인하고, 사용자가 어디에 있든 필요한 애플리케이션에 접속할 수 있는지 확인해 공격 가능 영역을 줄이고 유연성과 모니터링 기능을 향상시킵니다. 수십 년 동안 기업은 ID 공급업체가 지원하는 가상 프라이빗 네트워크(VPN)에 의존해 접속을 제공했습니다. 지금과 다른 시대에 맞게 설계된 이러한 VPN은 오늘날의 분산된 인력의 규모와 범위에 더 이상 충분하지 않습니다. ZTNA는 VPN을 대체하는 것 이상으로 발전했으며, 이제 사용자 및 디바이스의 ID를 확인하는 것뿐만 아니라 시간과 날짜, 지리적 위치, 디바이스 체계 등의 특성을 기반으로 접속을 부여해 적절한 신뢰 수준을 제공합니다.

제로 트러스트 네트워크 접속 솔루션 구매 시 주요 고려 사항

기업들이 구형 VPN을 보다 정교한 ID 관리 솔루션으로 교체하기 시작함에 따라 여러 가지를 고려해야 합니다. 오늘날의 고급 솔루션은 ID 및 접속 관리, 애플리케이션 보안, 멀티팩터 인증(MFA), SSO(Single Sign-On) 모두를 결합하여 하나의 인터페이스에서 관리하고 제어할 수 있는 가시성을 제공해야 합니다. 제로 트러스트 이니셔티브를 추진하는 기업은 현재 요구사항을 해결할 수 있을 뿐만 아니라 비즈니스 규모에 맞게 확장할 수 있는 솔루션을 찾아야 합병 또는 인수한 기업의 직원을 신속하게 온보딩하고, 다양한 시장 또는 지역에서 제조 또는 생산하고, 계약업체를 쉽게 추가하고 제거해 변화하는 비즈니스 요구사항에 적응하고, 보안을 희생하지 않으면서 비용 효율적으로 애플리케이션을 클라우드로 이전할 수 있습니다.

기업은 여러 디렉터리 및 ID 서비스 사업자를 포함하더라도 기존 ID 인프라와 직접 통합할 수 있는 솔루션을 찾아야 합니다. 이를 통해 기존 ID 인프라나 아키텍처를 변경하지 않고 ZTNA 서비스를 신속하게 배포할 수 있습니다.

엣지에 의지하기

제로 트러스트 구매팀이 고려하지 않을 수도 있지만 반드시 고려해야 하는 중요한 차별화 요소도 시장에 출시된 제품들 사이에 있습니다. 엣지 클라우드 플랫폼과 결합된 솔루션은 추가적인 장점을 제공할 수 있습니다. ID 인지 프록시 역할을 하면서 엣지 플랫폼과 연결되기 때문에 모든 인증이 데이터센터가 아니라 엣지에서 이루어집니다. DMZ 내에서 운영되는 프록시 아키텍처에 접속하는 기업도 있지만 이런 경우 공격을 차단하고, 캐싱용 대역폭을 제공하며, 필요에 따라 자동 확장하는 클라우드의 기능을 활용하지 못합니다.

클라우드에 구축된 ID 인지 프록시는 필요에 따라 확장하고, CPU 사용량이 많은 리소스를 실행하고, 공격을 차단할 수 있습니다. 또한 이 프록시는 인터넷에서 직접 연결할 수 없는 프라이빗 IP 주소에 위치합니다. 성능 및 보안에 가장 민감한 활동은 최종 사용자와 가장 가까운 엣지에서 이루어집니다. 애플리케이션에 대한 민감한 유입 경로는 역방향 애플리케이션 터널을 통해 만들어지기 때문에 경계의 IP 가시성을 효과적으로 제거하며 증폭 공격의 리스크가 줄어듭니다.

> **엣지 클라우드 플랫폼과 결합된 솔루션은 ID 인지 프록시 역할을 통해 추가적인 혜택을 제공할 수 있습니다.**

제로 트러스트 청사진 구축 시 멀티팩터 인증 고려 사항

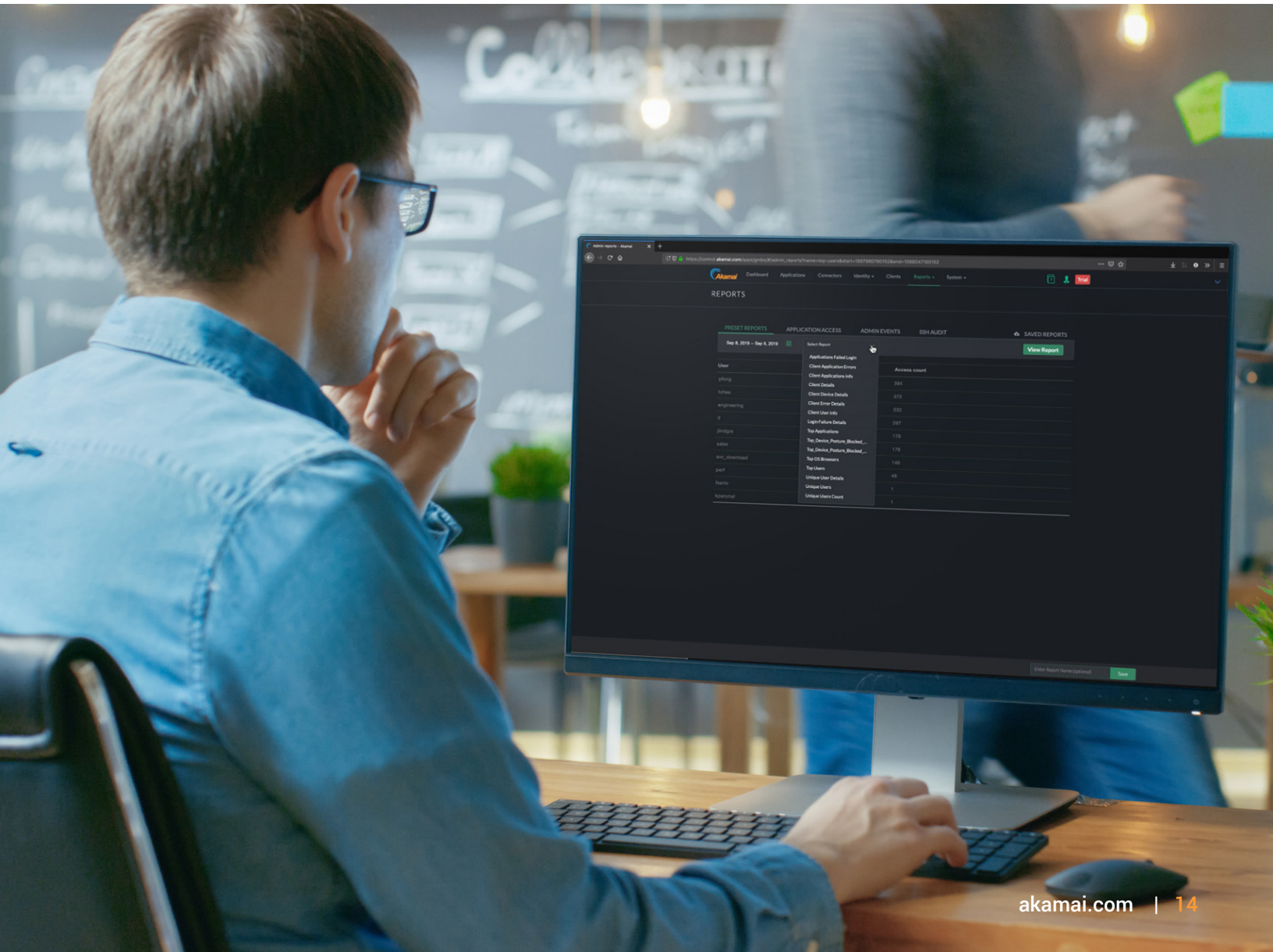
하이브리드 근무가 증가하고 접속 강화의 필요성이 커지면서 대부분의 기업은 이미 MFA를 도입했고 일부 솔루션을 사용하고 있습니다. 그러나 기업 전체 접속과 MFA의 조합이 각 부분의 합보다 크다는 점을 인식하는 것이 중요합니다. MFA는 비밀번호 이상의 기능을 필요로 하기 때문에 신뢰 개념의 핵심입니다. 가장 일반적으로 악용되는 신뢰 영역에서 피해자가 되지 않으려면 두 번째 검증이 필요합니다. 또한 모든 MFA 솔루션이 동일하지 않다는 점도 기억해야 합니다.

기업은 제로 트러스트 전략의 일환으로 MFA 솔루션을 평가할 때 다음과 같은 솔루션을 고려해야 합니다.

- ID 관리 및 기업 접속과의 통합
- FIDO2 준수(이를 통해 사용자의 개인 디바이스에서 사용자 인증정보를 분산, 격리, 암호화할 수 있는데, 이는 피싱 공격을 차단하는 데 특히 중요)
- 물리적 키에 의존하지 않고 스마트폰을 통해 사용자를 확인

마이크로세그멘테이션

완벽한 제로 트러스트 상태는 없습니다. 가장 끈질긴 공격자가 찾아내 악용할 수 있는 틈새는 불가피하게 존재합니다. 따라서 제로 트러스트에 대한 포괄적인 접근 방식은 마이크로세그멘테이션을 필요로 합니다. 오늘날 대부분의 네트워크는 세그먼트가 없거나 세그먼트가 매우 적습니다. 실제로 기업들은 이전에 중요한 애플리케이션을 방화벽으로 보호해 왔지만 여러 가지 이유로 인해 어려움을 겪고 있습니다. 방화벽을 사용하면 기본적으로 네트워크 정책을 적용해야 하므로 초크 포인트(choke point, 관문)를 생성하게 됩니다. 방화벽을 통과하려면 네트워크 연결이 필요하기 때문에, 비용이 빠르게 증가하고, 최신 네트워크 트래픽의 리스크를 인지하지 못하게 되고, 변경이 매우 어렵습니다. 대신 기업들은 노동 집약적인 프로세스 중 많은 것을 간소화하는 소프트웨어 기반의 마이크로세그멘테이션으로 전환하고 있습니다.



마이크로세그멘테이션의 차별화 포인트

마이크로세그멘테이션은 제로 트러스트 이니셔티브의 핵심 요구사항이지만 핵심 ZTNA 솔루션과 별도로 고려되는 경우가 많습니다. 마이크로세그멘테이션은 보안 플랫폼 공급업체가 단독으로 사용 가능한 솔루션으로 판매하지만 구매자가 이해해야 할 몇 가지 핵심적인 차이점이 있습니다.

어디에 배포할 수 있나요? 보안 우선 접근 방식 대신 네트워크 툴로 구축되었거나 온프레미스 시스템용으로 구축된 마이크로세그멘테이션 솔루션은 잠재 구매자에게 위험할 수 있습니다. 오늘날의 툴은 클라우드, 온프레미스 환경, 디바이스(에이전트를 설치할 수 없는 디바이스 포함), 하이브리드 환경 전반의 컨테이너 간에 배포되어야 합니다. 일반적으로 클라우드 기반 소프트웨어가 필요합니다. 마이크로세그멘테이션 솔루션이 환경의 80%만 지원할 수 있다면 충분하지 않습니다.

얼마나 많은 가시성을 제공하나요? 마이크로세그멘테이션 솔루션은 접속을 제한하지만, 제한이 너무 많으면 비즈니스 프로세스를 중단시키고 COO의 호출로 이어질 수 있습니다. 마이크로세그멘테이션은 사용자 환경에 대한 정교한 이해가 필요합니다. 어떤 서버가 어떤 서버에 접속할 수 있나요? 쿠버네티스 클러스터와 Windows 2008 서버 간의 정책을 정의할 수 있나요? 많은 툴은 2008년까지 거슬러 올라가는 에이전트가 없거나 쿠버네티스에 정책을 적용할 수 있는 만큼 미래 지향적으로 제작되지 않았습니다. 제로 트러스트를 효과적으로 배포하려면 마이크로세그멘테이션 소프트웨어가 이러한 복잡한 문제를 해결할 수 있어야 합니다.

또한 마이크로세그멘테이션 소프트웨어 구매자는 제품이 지원할 정책의 세분화를 고려해야 합니다. 대부분의 시스템은 포트 및 프로세스의 애플리케이션 레이어에서 정책을 적용합니다. 보다 정교한 제품은 마이크로서비스 레이어에서 정책을 적용할 수 있습니다. 예를 들어, 공격자는 Task Scheduler 같은 svchost의 일부 서비스를 사용해 네트워크 전체에서 측면으로 이동할 수 있습니다. 그러나 기업은 svchost가 중요한 일을 너무 많이 하기 때문에 완전히 막을 수 없습니다. 마이크로서비스 레이어에서 정책을 시행하는 마이크로세그멘테이션 솔루션은 이 부분에서 차이를 만들 수 있습니다.

구축이 얼마나 어렵나요? 현재 필요한 정책과 앞으로 필요한 정책을 얼마나 간단하게 표현할 수 있는지는 동일하게 마이크로세그멘테이션 솔루션의 핵심 고려 사항이어야 합니다. 계획 단계에 있든, 환경에 위협이 발생해 잠가야 하든, 투자하는 엔진이 두 가지 모두를 쉽게 지원할 수 있는지 확인하세요.

마이크로세그멘테이션 프로젝트에서 허용 목록으로 시작하는 것은 필요한 애플리케이션이나 서비스를 잘못 거부할 수 있는 리스크 때문에 보안팀에게 부담스러울 수 있습니다. 정교한 마이크로세그멘테이션 솔루션은 기업이 빠르고 쉽게 배포해 프로젝트에 대한 몇 가지 성공 사례를 빨리 만들 수 있는 거부 목록 템플릿이 함께 제공되어야 합니다. 이 작업이 완료되면 기업은 정확한 의존성과 상황별 재고 매핑 기능을 포함하는 포괄적인 허용 목록 보안을 위한 여정을 계속할 수 있습니다.

> **보안 우선 접근 방식 대신 네트워크 툴로 구축되었거나 온프레미스 시스템용으로 구축된 마이크로세그멘테이션 솔루션은 잠재 구매자에게 위험할 수 있습니다.**

DNS 방화벽

제로 트러스트 환경에서는 사람뿐만 아니라 인터넷 자체를 신뢰할 수 없습니다. 직원들이 인터넷에 접속해야 하고 SaaS 및 모바일 애플리케이션, 클라우드 서비스, 하이브리드 근무, IoT 디바이스가 확산됨에 따라 기업의 공격표면도 커졌습니다. 멀웨어, 랜섬웨어, 피싱, 데이터 유출 등의 위협으로부터 기업과 사용자를 보호하는 일은 점점 어려워지고 있습니다. 기업은 기존의 온프레미스 솔루션에서 보안 제어 지점의 복잡성과 보안 격차를 관리하는 데 필요한 리소스가 제한되어 있습니다.

사람과 인터넷 사이에 제로 트러스트를 적용하려면 모든 제로 트러스트 이니셔티브의 핵심 기능이 되는 DNS 방화벽이 필요합니다.

DNS 방화벽 투자의 핵심 제로 트러스트 요구사항

당연한 말이지만 기술 구매자가 DNS 방화벽에 투자할 때 고려해야 할 요구사항이 있습니다. 많은 기업에서 온프레미스 DNS 방화벽을 배포했지만 이제는 위치에 관계없이 사용자들에게 이런 보안 기능을 확장해야 합니다. ID 관리와 마찬가지로, 강력한 엣지 플랫폼을 보유한 공급업체는 일반적으로 확장된 플랫폼에서 얻은 위협 인텔리전스 덕분에 더 강력한 DNS 보안을 갖추고 있습니다. 의사 결정자는 이러한 핵심 요구사항을 신중하게 고려해야 합니다.

DNS 검사. 공급업체는 정교한 위협 인텔리전스를 통해 모든 도메인을 실시간 검사하고 악성 도메인을 자동으로 차단할 수 있어야 합니다. 모든 포트 및 프로토콜에서 효과적으로 작동해, 표준 웹 포트나 프로토콜을 사용하지 않는 멀웨어도 방어해야 합니다. DNS 검사 품질은 공급업체마다 크게 다를 수 있으며, 구매자는 고객 성공을 지원하고 시장 경험을 갖춘 공급업체를 모색해야 합니다.

모든 디바이스에 대한 보호. 공급업체는 노트북, 스마트폰, 태블릿 등 네트워크 안팎에서 사용되는 디바이스에 대한 에이전트를 보유해야 합니다.

유연한 DNS 온보딩. 공급업체는 최대한의 유연성을 제공하고 모든 사용 사례를 포괄할 수 있도록 DNS 요청을 DNS 방화벽으로 전달할 수 있는 다양한 방법을 보유해야 합니다.

DNS 유출 식별 및 차단. DNS 유출, 특히 처리량이 적은 변형을 통해 공격자는 DNS 채널을 통해 데이터를 유출할 수 있습니다. 독점 탐지 알고리즘을 기반으로 인라인 및 오프라인 DNS 유출 탐지 기능을 모두 갖춘 공급업체를 찾아보세요.

위협 모니터링

핵심 제로 트러스트 기술의 마지막 부분은 위협 모니터링입니다. 제로 트러스트는 아무것도 암묵적으로 신뢰할 수 없다고 가정하지만, 기업은 지속적으로 발생하고 있는 공격과 잠재적인 리스크(잘못된 설정 또는 지나치게 허용적인 접속 권한 등)를 발견하기 위해 경계를 늦추지 말아야 합니다. 보안팀은 시장의 소프트웨어를 평가할 때 위협을 효과적으로 모니터링하기 위해 다음 3가지 고려 사항을 검토해야 합니다.

주요 고려 사항

효과적인 알고리즘
사용자 및 네트워크 활동 이상, 실행 가능한 분석, 로그 분석 등을 기반으로 성공 이력을 갖춘 정교한 알고리즘은 위협 모니터링 서비스에 포함되어야 합니다.

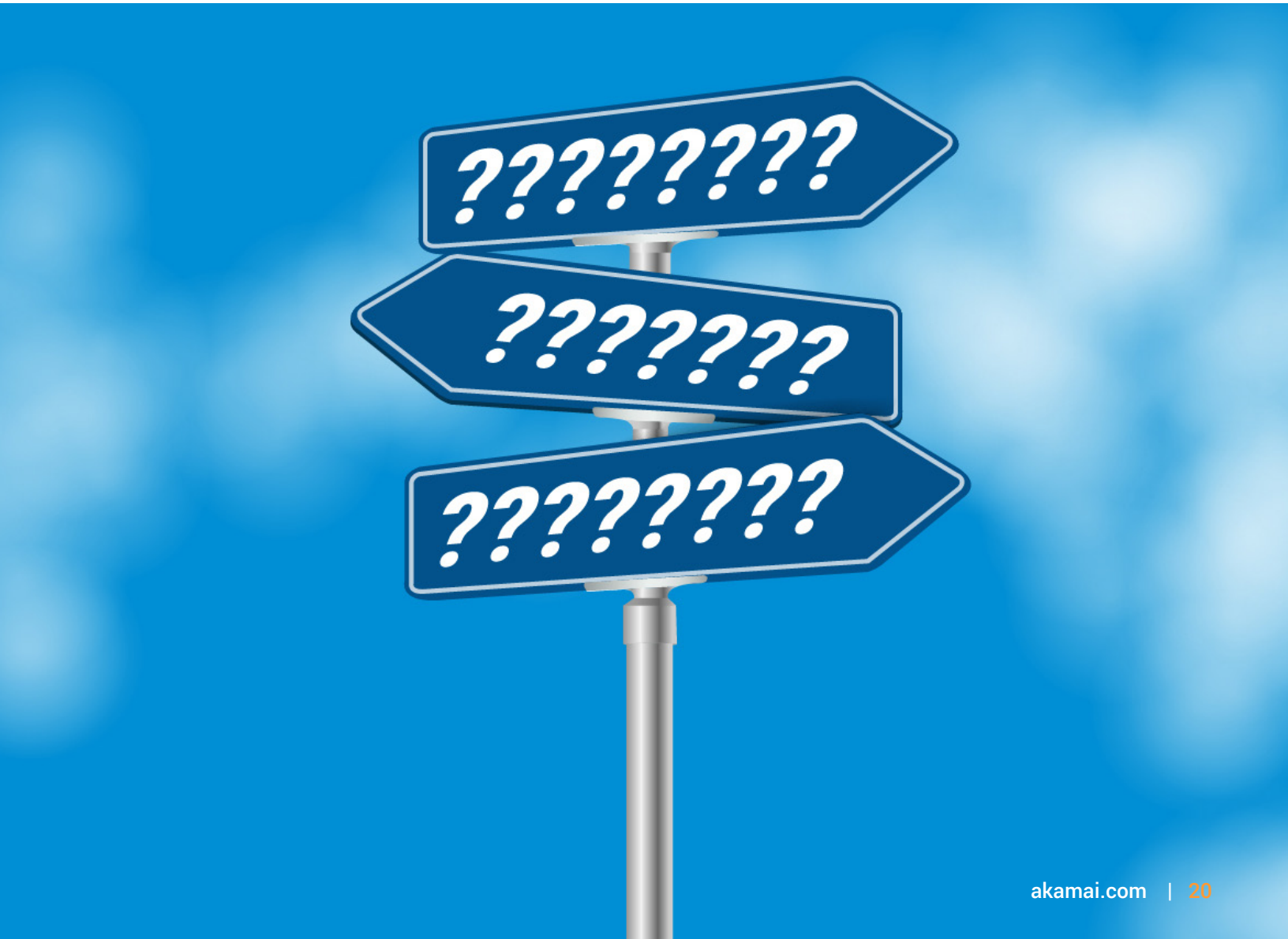
강력한 신호 탐지
소프트웨어와 인공 지능이 위협 모니터링에 필수적인 툴이기는 하지만 제로 트러스트 의사 결정권자는 함께 일하는 벤더사의 내부 전문 지식을 평가해야 합니다. 위협 모니터링 서비스는 알림 피로를 방지하고 정상 신호를 악성 신호와 구분해 모든 인시던트에 대해 즉시 알림을 제공할 수 있어야 합니다. 또한 주요 캠페인을 분석한 정기 보고서를 기업에 제공해야 합니다.

숙련된 직원
공격, 인시던트 대응, 데이터 과학 등 다양한 배경을 가진 사람들로 구성된 팀이 연중무휴 24시간 서비스를 제공해야 합니다. 이는 콘텐츠 전송 사업자가 상당한 혜택을 제공할 수 있는 부문입니다. 초당 수백 테라바이트를 모니터링해 얻은 인사이트는 모든 신호 탐지에 고유한 관점을 제공합니다.

어디서부터 시작해야 할까요?

제로 트러스트 이니셔티브는 완전하지 않습니다. 따라서 소프트웨어, 하드웨어, 고용 요구사항을 고려할 때 가장 중요한 질문은 "어떤 기술로 시작해야 하나요?"입니다.

많은 것과 마찬가지로 정답은 기업의 개별 요구사항, 리스크 평가, 상대적인 장점과 단점에 따라 달라집니다. 많은 업계 관계자는 ZTNA를 구축하는 것부터 시작하라고 권장합니다. 실제로 악성 남북 트래픽으로부터 기업을 보호하는 것이 좋은 출발점이 될 수 있습니다. 그러나 마이크로세그멘테이션, 특히 소프트웨어 정의 마이크로세그멘테이션을 통한 동서 접근 방식이 더 나은 방법이라고 믿는 사람들도 있습니다.



마이크로세그멘테이션을 시작하는 이유

많은 전문가가 말하는 것처럼 완벽한 방어 체계가 없고 악성 공격이 결국에는 방어를 뚫을 것이라고 생각한다면 가장 가치 있는 자산을 보호할 수 있는 능력을 갖추어야 합니다. 이것이 바로 마이크로세그멘테이션의 기능입니다. 기업이 마이크로세그멘테이션을 시작하는 것을 꺼리는 한 가지 이유는 복잡하다고 생각하기 때문입니다.

첫째, 마이크로세그멘테이션은 이분법적 접근 방식이 아닙니다. 제로 트러스트처럼 단계적으로 수행할 수 있습니다. 기업은 가장 가치 있는 자산을 파악하는 것부터 시작할 수 있습니다. 중요한 것에 집중하세요. 누군가 시스템에 침입하더라도 비즈니스를 중단시킬 수 없도록 해야 합니다. 자산 내의 데이터나 기존 보안 수준을 기반으로 자산의 중요성을 결정할 수 있습니다.

레거시 시스템은 비즈니스에 중요한 애플리케이션을 실행하는 경우가 많고 특히 취약한 경우가 많으므로, 레거시 시스템을 포괄하는 마이크로세그멘테이션 솔루션이 필요한 경우가 많습니다. 이러한 레거시 시스템의 보안을 지원하지 않는 일부 마이크로세그멘테이션 솔루션이 있습니다.

둘째, 소프트웨어 정의 마이크로세그멘테이션을 사용하면 복잡성을 상당히 줄일 수 있습니다. 하드웨어를 다루거나 네트워크 아키텍트 및 보안 아키텍트를 반복해서 호출할 필요가 없습니다. 소프트웨어를 배포하기만 하면 진입 장벽이 크게 낮아집니다.

일단 마이크로세그멘테이션 이니셔티브가 시작되면 초반에 확실한 이점을 확인할 수 있고 프로젝트의 나머지 부분을 추진하는 데 도움이 될 수 있습니다. 예를 들어, 사용자 환경에서 발생하는 일에 대한 정보를 얻을 수 있습니다. 정책을 실행하지 않고 이러한 정보를 바로 얻을 수 있으며, 실행한 후에는 흐름의 진행 상황을 잘 이해할 수 있습니다. 또한 기업에서 애플리케이션 링펜싱을 시작하면 중요한 특정 포트 및 프로세스를 통해서만 통신할 수 있도록 빠르고 쉽게 애플리케이션을 잠글 수 있습니다.

위협별 정책을 실행하면 빠르게 문제를 해결할 수 있습니다. 정교한 마이크로세그멘테이션 플랫폼에는 거부 목록이 내장되어 있습니다. 즉, 원격 데스크톱 서비스와 인터넷 간의 불필요한 연결을 차단하는 정책을 신속하게 만들 수 있습니다. 예를 들어, 기업은 Colonial Pipeline 공격을 일으키는 취약점을 신속하게 차단할 수 있습니다.

시작점이 무엇이든, 지속적인 제로 트러스트 여정의 핵심은 균형입니다. 세그멘테이션이나 웹 접속 보호가 제대로 이루어지지 않는 세계적 수준의 ID 관리로는 보안이 제대로 이루어질 수 없습니다.

플랫폼과 전용 툴 비교

많은 기술 결정과 마찬가지로 제로 트러스트 소프트웨어를 구입하는 것은 개별 전문가와 여러 구성요소를 결합한 플랫폼 중에서 선택해야 하는 경우가 많습니다. 보안팀, 통합 업체, 아키텍트, 애널리스트 사이에 제로 트러스트가 미치는 영향과 여러 콘솔, 다양한 에이전트, 여러 통합 사이에 정책을 유지해야 하기 때문에 플랫폼 라우팅이 불가피합니다. 이는 숙련된 사이버 보안 전문가가 부족한 노동 시장에서는 특히 그렇습니다. 여러 벤더사의 솔루션을 관리하면 서로 효과적으로 통신하지 않는 솔루션이 오탐을 유발하여 최종 사용자에게 부담을 주고 추가 지원과 교육이 필요할 수 있으므로 인건비가 크게 증가할 수 있습니다.

또한 지원 및 계약 협상과 관련해 단일 사업자를 두는 것은 플랫폼 공급업체와 함께 제로 트러스트를 구축해야 하는 강력한 근거를 제공합니다.

유연한 접근 방식을 갖춘 단일 공급업체, 즉 개별 포인트 제품과 함께 제로 트러스트를 위한 포괄적인 플랫폼을 제공하는 공급업체를 찾는 것이 가장 이상적입니다. 이러한 유연성을 통해 단일 공급업체의 혜택을 누리면서 제로 트러스트를 쉽게 달성할 수 있습니다.

> **기업이 마이크로세그멘테이션을 시작하는 것을 꺼리는 한 가지 이유는 복잡하다고 생각하기 때문입니다.**

제로 트러스트의 구성요소 재검토

사용자가 누구인지 알아야 합니다.
사용자를 검증해야 합니다.

자산을 보호하세요.
모든 거래에 대한 인증 및 권한을 확인하세요.

사용자를 보호하세요.
멀웨어에 감염되지 않도록 사용자를 보호하세요.

결론

사이버 공격을 방어하는 데 관심이 있는 대부분의 기업은 제로 트러스트 아키텍처로 전환해야 할 필요성을 인식하고 있습니다. 이미 많은 기업은 하이브리드 근무가 증가하면서 점진적으로 또는 갑자기 여정을 시작하게 되었습니다. 하지만 공격자들이 점점 더 정교해지고, 위협 표면도 확산되고, 원격 접속을 요구하는 직원들이 증가하면서 이와 함께 작동하는 포괄적인 솔루션 포트폴리오에 대한 필요성 역시 커지고 있습니다.

제로 트러스트 접근 방식의 구체적인 요소에 대한 자세한 내용은 akamai.com/zerotrust를 방문하거나 전문가에게 문의하시기 바랍니다.