백서

제로 트러스트 네트워크 접속을 위한 청사진

이 가이드는 누가 읽어야 하나요?

네트워크 아키텍트, 보안 엔지니어, CTO, CISO, 기타 IT 및 보안 의사결정권자 모두 이 가이드를 읽고 유용한 정보를 얻을 수 있습니다.

제로 트러스트 네트워크 접속(ZTNA) 프로젝트의 범위 지정, 설정, 배포, 구축 및 관리 담당자를 위해 이 가이드에서는 잠재적인 이점과 시스템 간 차이점을 포괄적으로 검토합니다. 본 가이드의 내용은 다음과 같습니다.

- 애플리케이션 접속에 대한 레거시 접근 방식의 한계 및 보안 허점과 ZTNA가 필요한 이유
- ZTNA의 구성요소 및 작동 방식
- Akamai Enterprise Application Access 및 Akamai MFA를 통해 ZTNA를 빠르고 쉽게 제공하는 방법

비즈니스 세계가 변화하고 사이버 위협이 증가함에 따라 기업은 사이버 보안을 새롭게 바라보고 있습니다. 많은 기업들이 모든 관계자가 애플리케이션에 접속할 수 있는 중앙 집중식 위치에 의존하는 기존의 네트워킹 아키텍처가 취약하다는 사실을 깨닫게 되었습니다. 성에 해자를 두르듯 경계를 보호하며 경계 내의 모두가 안전하다고 믿는 이러한 접근 방식은 모바일 연결과 클라우드로 대표되는 오늘날의 환경에서 기업을 사이버 공격의 리스크에 노출시킵니다. 대신, 미래 지향적인 기업들은 중요한 자산을 보호하기 위해 제로 트러스트 아키텍처의 개념으로 전환하고 있습니다. 제로 트러스트 프로젝트의 핵심 원칙은 네트워크를 보호하는 것입니다. 이 백서에서는 네트워크 보안에 대한 기존의 허브 앤 스포크 접근 방식이 더 이상 충분하지 않으며, ZTNA로 전환하면 어떻게 중요한 자산을 보다 효과적으로 보호하고 포괄적인 제로 트러스트 아키텍처의 핵심 역할을 할 수 있는지 자세히 설명합니다.

그 어느 때보다 빠른 비즈니스 변화 속도

비즈니스의 운영 및 기술 사용 방식은 진화하고 있으며 그 속도도 점점 빨라지고 있습니다. 컴퓨팅의 진화로 기업 내 데이터 센터에서 비즈니스 애플리케이션을 호스팅하는 방식은 여러 퍼블릭 클라우드, 프라이빗 클라우드 또는 하이브리드 접근 방식(온프레미스 및 퍼블릭·프라이빗 클라우드 모두 지원)을 사용하는 방식으로 빠르게 전환되었습니다.

또한 비즈니스 모델의 발전으로 인해 기업 간 협업이 증가하고 파트너와 공급업체가 애플리케이션 및 리소스에 접속해야 할 필요성이 커졌습니다.

마지막으로, 기업이 원격 또는 하이브리드 근무를 지속적으로 도입하면서 사용자는 이제 모든 곳에서 관리형 디바이스와 비관리형 디바이스를 통해 비즈니스 애플리케이션과 리소스에 접속합니다.

이런 변화로 인해 애플리케이션 접속을 관리하는 기존 접근 방식은 더 이상 충분하지 않으며, 기업은 애플리케이션을 호스팅하는 위치나 사용자 위치에 상관없이 안전한 접속을 지원하는 새로운 접근 방식을 도입해야 합니다.

레거시 애플리케이션 접속

기업들은 강력한 보안 경계를 구축하기 위해 20년 이상 방화벽에 의존해 왔으며 그 경계 안에 있는 사용자를 신뢰해 왔습니다. 네트워크를 보호하는 것은 해자에 둘러싸인 성과 유사합니다. 두꺼운 벽과 철저한 보안이 유지되는 관문은 성(네트워크)을 보호하기 위해 경계를 구축하고 올바른 인증정보를 갖춘 사용자만 접속을 허용합니다. 경계 안으로 들어가면 사용자는 Microsoft Active Directory와 같은 ID 공급업체(IdP) 솔루션을 통해 제공되는 ID를 기반으로 특정 애플리케이션에 접속할 수 있습니다.

그러나 플랫 네트워크에서는 사용자가 실제로 전체 네트워크에 대한 IP 접속 권한을 갖기 때문에 다른 서버와 애플리케이션을 검색할 수 있습니다. 예를 들어, IdP가 올바르게 설정된 경우 사용자는 급여 애플리케이션이 호스팅된 서버를 찾을 수 있지만 애플리케이션에 로그인하려고 하면 접속이 거부됩니다.

이러한 제한 없는 측면 이동 문제를 해결하기 위해 기업은 VLAN(Virtual Local Access Network)을 통해 애플리케이션을 방화벽 뒤에서 별도의 세그먼트로 분할하고 개별 사용자 또는 그룹에 대해 지금은 구식인 IP 범위 기반 룰을 적용했습니다. 하지만 이 프로세스는 상당히 취약하며 오류가 발생하기 쉽습니다. 누군가가 유지 관리 작업 중에 머신을 새로운 랙으로 옮기거나 새로운 범위로 IP를 재설정해야 하는 상황을 생각해 보세요. 갑자기 사용자가 잠기고 지원 요청이 몰립니다. 또는 소프트웨어 업그레이드를 위해 애플리케이션의 아키텍처를 변경해야 하고 워크플로우의 일부로 사용자가 다른 머신으로 리디렉션될 수도 있습니다. 하지만 방화벽 룰이 업데이트되지 않았기 때문에 특정 사용자나 그룹이 해당 머신에 접속하지 못할 수 있습니다.

이러한 아키텍처는 매우 복잡하고 제로 다운타임을 보장하기 위해 변경 과정에서 애플리케이션 소유자, 네트워크 관리자, 보안 그룹 간에 매우 높은 수준의 커뮤니테이션이 요구됩니다.

조정에 실패하면 어떤 일이 벌어질지는 분명합니다. 관리자는 평소에는 모범 사례를 따르려 하지만, 급박한 상황에서는 영향을 받는 사용자가 근본적인 문제를 진단하고 해결할 때까지 모든 것에 접속할 수 있도록 엄격한 IP ANY·ANY ALLOW 룰을 신속한 해결책으로 추가합니다. 그러나 변경 사항을 되돌릴 시간적 여유가 없을 때가 더 많으며 이러한 임시 조치는 시간이 지남에 따라 회사의 보안 체계를 약화시킵니다.

복잡성, 성능, 보안 문제를 가중시키는 VPN

VPN(Virtual Private Network)은 일반적으로 경계 내부에서 호스팅되는 온프레미스 애플리케이션에 대한 접속을 원격 사용자에게 제공하며, 이를 통해 회사 네트워크에 대한 직접 터널링 접속을 지원합니다.

애플리케이션에 대한 사용자 접속을 관리하기 위해 기업에서는 전용 애플리케이션 전송 컨트롤러를 추가하거나 VPN 솔루션에 내장된 접속 제어를 사용하는 경우가 많습니다. 사용자의 위치에 관계없이 애플리케이션 접속 권한을 조정하는 것이 목표입니다. 사용자가 경계 내부에 있을 때 CRM 애플리케이션에 대한 접속이 거부되면 VPN을 통해 연결할 때도 접속이 거부되어야 합니다. 이것이 목표이기는 하지만 두 가지 사용 사례 및 임시 조치 사이에서 애플리케이션 권한을 동기화할 때 매우 복잡하기 때문에 사용자가 의도하지 않은 애플리케이션 접속 권한을 획득할 수 있습니다.

계약업체, 파트너, 공급업체를 위한 애플리케이션 접속

또한 기업들은 종종 VPN을 통해 계약업체, 파트너, 공급업체가 원격으로 애플리케이션에 접속하도록 허용합니다. 예를 들어, 공급업체가 인보이스를 제출할 수 있도록 재무 시스템에 대한 외부 접속을 허용할 수 있습니다. VPN을 통해 써드파티 애플리케이션에 접속할 수 있도록 허용하면 더 이상 엔드투엔드 보안을 유지하지 못하기 때문에 추가적인 보안 리스크가 발생합니다. VPN 접속 권한이 있는 써드파티 디바이스가 감염되면 공격자가 기업 네트워크에 접속할 수 있습니다.

VPN 및 성능

성능에 대해서도 동일한 딜레마가 발생합니다. 가장 단순한 형태의 VPN에서는 모든 트래픽이 데이터 센터 인프라로 다시 돌아갑니다. 헤어핀 현상으로 인터넷 속성 및 SaaS(Software-as-a-Service) 애플리케이션에 대한 접속 속도가 매우 느려지고 트래픽이 두 배로 증가합니다.

이 성능 부담을 극복하려면 관리자는 분할 터널을 배포해 VPN을 통과할 IP 범위와 인터넷으로 직접 송신될 IP 범위를 표시해야 합니다. 내부 경계가 단 한 개만 있을 때는 간단하고 효과적일 수 있습니다. 하지만 여러 데이터 센터와 가상 프라이빗 클라우드 공급업체를 추가하면 훨씬 복잡해지기 시작합니다. 그런 다음 관리자는 VPN 애그리게이터를 모든 데이터 센터에 설치해야 할지 결정하고 멀티포인트 분할 터널을 효과적으로 관리하는 방법을 결정해야 합니다.

VPN이 가치를 제공하지 않는다는 것은 아닙니다. 실제로 많은 가치를 제공합니다. 여러 데이터 센터 인프라에 대한 사이트 간 접속은 이러한 장점이 빛나는 사례 중 하나입니다. 그러나 네트워크 수준의 접속은 편의성과 보안 및 성능 사이에서 부자연스러운 타협을 강요하기 때문에 애플리케이션에 접속하는 사용자에게는 네트워크 수준의 접속이 적합한 패러다임이 아닙니다.

네트워크 기반의 애플리케이션 접속은 오히려 공격자에게 반가운 소식입니다.

지금까지 모든 직원에게 네트워크 수준의 접속 권한을 부여하는 방식과 관련된 리스크 및 도전 과제에 초점을 맞췄습니다. 그러나 이 접근 방식은 기업을 또 다른 리스크에 노출시킵니다. 도난당한 사용자 인증정보 또는 보안 취약점을 악용하는 사이버 범죄자도 네트워크 전반에 걸쳐 제한 없는 접속 권한을 얻을 수 있습니다. 예를 들어, 공격자가 감염된 직원 인증정보를 사용해 VPN 접속 권한을 획득하면 네트워크를 측면으로 이동해 가치가 높은 대상을 찾아 접속하고 공격할 수 있습니다.

이러한 접근 방식은 치명적인 유출의 가능성을 열어줍니다.

이론적으로는 이 접근 방식을 사용하면 제약 조건을 최소화하면서 안전하게 애플리케이션 접속을 관리할 수 있습니다. 이미 이들 중 몇 가지의 조합을 사용하고 계실지도 모르겠습니다. 문제는 이 방식을 제대로 구축하고 유지 관리하며 보안과 성능을 계속 적절히 제공한다는 것이 운영상 너무 복잡해서 지속적으로 유지하기 어렵다는 점입니다. 많은 경우, 기업은 직원들이 애플리케이션에 접속할 수 있으니 모두 최적의 상태일 것이라고 자기 위안을 합니다. 그리고 임시 조치 중 한 가지가 최악의 유출 사태를 일으키거나 장애 또는 직원 생산성에 심각한 악영향을 미치는 성능 문제가 발생하면 기업은 갑자기 예상치 못한 어려움에 빠지게 됩니다.

애플리케이션 접속에 대한 제로 트러스트 접근 방식

경계 보안 접근 방식의 내재된 결함과 애플리케이션 접속 관리와 관련된 특정 과제를 고려할 때 새롭게 등장하는 제로 트러스트 사이버 보안 모델은 더 나은 대안을 제시합니다. 2010년에 Forrester Research에서 처음 도입한 이 프레임워크는 기업이 IT 인프라, 보안 정책, 비즈니스 프로세스를 혁신하기 위해 활용합니다.

이 솔루션의 기본 개념은 상당히 간단하면서 강력했습니다. 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 것*만 *일어날 수 있습니다*. 리스크는 생기지만 가치는 생성하지 않기 때문에 필요하지 않은 작업에 대한 모든 암시적 신뢰를 제거합니다.

이를 위해서는 강력한 인증 및 권한 확인이 필요하며, 신뢰를 구축할 때까지 시스템은 데이터를 전송해서는 안 됩니다. 또한, 애널리틱스, 필터링, 로깅을 사용해 행동이 적절한지 확인하고 감염의 징후를 계속 확인해야 합니다.

이러한 근본적인 변화로 인해 지난 10년 동안 등장했던 수많은 보안 침해 사례를 극복할 수 있었습니다. 공격자는 내부에 진입했다는 이유만으로 더 이상 경계 내부의 취약점을 악용하여 민감한 데이터와 애플리케이션을 수집할 수 없게 되었습니다. 접속하기 위해 건너야 할 해자가 사라진 것입니다. 이제 애플리케이션과 사용자만이 존재하며, 양쪽 모두 서로 인증하고 권한을 확인해야만 접속이 이루어질 수 있습니다.

제로 트러스트 네트워크 접속

ZTNA는 강력한 인증, 권한 확인 및 컨텍스트를 기반으로 애플리케이션과 리소스에 대한 보안 접속을 허용하는 원칙을 기반으로 구축된 아키텍처입니다. ZTNA 아키텍처는 전체 네트워크가 아니라 사용자가 업무에 필요한 애플리케이션에만 접속할 수 있도록 허용합니다. ZTNA 접근 방식을 사용하면 사용자의 위치는 더 이상 중요하지 않으며 경계 내부나 외부라는 개념이 더 이상 존재하지 않습니다. 애플리케이션이 호스팅되는 위치는 온프레미스, 퍼블릭 클라우드, 프라이빗 클라우드 등 어떤 곳이든 상관 없습니다. 인증된 사용자는 사용 권한이 부여된 애플리케이션에만 접속할 수 있기 때문입니다.

예를 들어, 영업 직원은 인사 관리 또는 재무 애플리케이션이 아닌 영업 업무와 관련된 애플리케이션에만 접속할 수 있습니다.

Akamai ZTNA의 작동 방식

Akamai Enterprise Application Access 및 Akamai MFA를 사용하면 ZTNA 아키텍처로 전환할 수 있으며, 이는 제로 트러스트를 향한 여정의 중요하고 결정적인 단계가 될 수 있습니다.

Enterprise Application Access는 클라우드 기반의 ID 인식 프록시(IAP)입니다, 위협 인텔리전스, 디바이스 체계, 사용자 ID 정보와 같은 실시간 시그널을 기준으로 정밀하게 의사결정을 수행하는 유연하고 탄력적인 서비스입니다. Akamai MFA는 접속을 요청하는 사용자의 신원을 확인하기 위해 가장 강력한 인증 수준을 제공하는 멀티팩터 인증 서비스입니다.

시작하려면 방화벽 뒤에서 Enterprise Application Access 커넥터라는 작은 가상 머신을 실행한 후 애플리케이션에 연결해야 합니다. 이는 DMZ 내부에 위치할 *필요*가 없고, 위치해서도 안 됩니다. Akamai Connector의 주소는 프라이빗 IP 공간에 있어야 하고 인터넷에서 직접 접근하기가 불가능해야 합니다. 사실, 방화벽 뒤에 배치할 다른 모든 애플리케이션과 완전히 동일한 것으로 보여야 합니다.

멀티클라우드 환경을 지원하기 위해 커넥터를 온프레미스 데이터 센터 내부나 프라이빗 또는 퍼블릭 클라우드에 배포할 수 있습니다.

Enterprise Application Access 커넥터는 Akamai Connected Cloud의 IAP에 대한 암호화된 아웃바운드 연결을 즉시 설정합니다. IAP에 연결되면 커넥터가 해당 설정을 다운로드하고 연결을 지원할 준비가 됩니다. IAP에 대한 커넥터 간의 연결은 아웃바운드이기 때문에 모든 인바운드 방화벽 연결을 닫을 수 있고 퍼블릭 인터넷에서 애플리케이션이 거의 노출되지 않습니다.

IAP는 인증, 권한 확인, 디바이스 보안, 보안 체계 확인을 포함하여 사용자가 애플리케이션에 연결되기 전에 발생하는 모든 사전 처리 작업을 수행합니다. 사용자가 애플리케이션에 접속을 시도하면, DNS CNAME을 통해 Akamai로 이동되어 IAP에 연결됩니다. 최종 사용자 및 디바이스가 모든 확인 절차를 통과하면 인증, 멀티팩터 인증, SSO(Single Sign-On)으로 라우팅된 후 디바이스 ID 기능이 수행됩니다.

사용자와 머신이 인증되면, 최종 사용자의 접속이 Enterprise Application Access 커넥터에서의 아웃바운드 접속과 결합됩니다. 사용자 세션으로부터의 트래픽은 이렇게 연결된 IAP를 통해 흐른 다음 요청된 애플리케이션이나 서비스에 연결됩니다. 이 시점에서 완전한 데이터 경로가 수립되며, 모든 접속 결정은 ID, 디바이스, 사용자 컨텍스트를 기반으로 지속적이고 동적으로 수행됩니다.

이러한 접속 방법에는 분명하고 상당한 장점이 있습니다. 성능과 보안에 가장 민감한 활동은 사용자와 가장 가까운 위치의 엣지에서 수행되며, 이를 위해 Akamai는 134개국에 4200개가 넘는 위치를 보유하고 있습니다.

애플리케이션에 대한 민감한 유입 경로는 역방향 애플리케이션 터널을 통해 만들어지기 때문에 경계의 IP 가시성을 효과적으로 제거하며 증폭 공격의 리스크가 줄어듭니다.

Enterprise Application Access는 여러 디렉터리 및 ID 서비스 공급업체를 사용하는 경우에도 기업의 ID 인프라와 직접 통합되기 때문에 기존 ID 인프라나 아키텍처를 변경하지 않고 ZTNA 서비스를 신속하게 배포할 수 있습니다.

최신 인증 프로토콜을 지원하지 않는 레거시 애플리케이션의 경우 Enterprise Application Access에는 SAML 기반 IdP에 대한 인증을 제공하고 인증 토큰을 레거시 애플리케이션에서 지원하는 인증 프로토콜로 변환하는 IDP 브리지 기능이 있습니다.

Enterprise Application Access와 같은 IAP 기반 접근 방식의 장점은 애플리케이션 수준 접속을 제공한다는 점입니다. 애플리케이션 수준으로 접속하면 성능과 보안을 *복잡하지 않게* 달성할 수 있습니다.

서로 인접한(동일한 데이터 센터 또는 동일한 가상 프라이빗 클라우드에 모두 호스팅된 경우) 모든 애플리케이션을 프라이빗 네트워크 IP 공간이나 제한적인 VLAN에 배치하고 해당 마이크로 경계에 접속 프록시를 제공하기만 하면 그것으로 끝입니다.

애플리케이션 소유자는 접속 프록시에 접속할 수 있는 사람과 그 이유를 정하는 자체 보안 정책을 설정할 수 있습니다. 더욱 좋은 점은 사용자의 위치는 어디든 상관없다는 것입니다. 최종 사용자를 포함하는 네트워크 경계가 없기 때문에 온프레미스와 오프프레미스 간의 구분도 없습니다. 커피숍에서 일하는 직원과 사무실에서 일하는 직원이 완전히 동일하게 취급됩니다. 사용자가 인증되었는지, 사용하는 머신이 안전한지, 그 여부만 중요합니다.

애플리케이션 수준의 접속 기능 덕분에 배포와 사용이 쉬우면서도 동급 최고 수준의 성능을 얻을 수 있습니다. 사용자는 호스팅되는 곳이나 사용하는 위치와 무관하게 인터넷을 통해 애플리케이션에 직접 접속할 수 있으며, 인터넷에서 경로에 없는 애그리게이터나 매개체를 거칠 필요 없이 패킷을 목적지로 바로 보낼 수 있습니다.

사실 애플리케이션 수준 접속을 사용하면 내부 네트워크가 단순한 게스트 Wi-Fi로 통합됩니다. 제로 트러스트가 정말로 효과를 발휘하려면, 내부 사용자와 외부 사용자를 완전히 동일하게 취급해야 합니다. 즉, 기본적으로 누구도 신뢰하지 않습니다.

ZTNA의 바람직한 최종 상태

온프레미스든 오프프레미스든 상관없이 모든 사용자는 애플리케이션이 호스팅되는 위치에 관계없이 ID 인식 접속 프록시를 통해 모든 애플리케이션에 접속해야 합니다. 이러한 프록시는 표준 인증뿐만 아니라 Akamai MFA와 같은 피싱 방지 멀티팩터 인증도 사용해야 합니다. 또한 특정 애플리케이션에 대한 접속을 허용하기 위해 디바이스 기준을 수립하는 확실한 디바이스 체계 기능이 있어야 합니다.

Akamai는 ZTNA가 인증 및 권한 확인으로 끝나지 않는다고 확신합니다. 제로 트러스트 원칙을 지원하려면 활성화 세션 동안 초기 인증 및 권한 확인 단계에서 검사하는 모든 매개변수를 지속적으로 모니터링해야 합니다. 변경 사항이 탐지되면 사용자를 다시 인증하거나 애플리케이션에 대한 접속 권한을 제거하거나 애플리케이션에 대한 접속을 제한하는 등의 작업을 트리거해야 합니다.

접속 프록시 위에 계층식으로 구축해야 하는 중요한 보안 시스템 중 하나는 웹 애플리케이션 및 API 보안(WAAP)입니다. 이를 통해 최종 사용자는 의도적이든, 실수든 내부 애플리케이션에 대해 애플리케이션 수준의 공격을 할 수 없도록 보장할 수 있습니다. API를 사용하지 않는 사이트에서 인간 또는 봇 탐지와 같은 기타 고급 시스템을 활용하면 멀웨어가 유효한 엔드포인트 뒤에 정체를 숨기지 못하도록 할 수 있습니다. Akamai는 IAP에서 WAAP, 봇 탐지, 행동 애널리틱스, 캐싱을 계층식으로 구축할 수 있습니다. 이는 업계 최고의 성능을 발휘하면서 동시에 잠재적인 공격자와 기업의 물리적 위치, 애플리케이션, 데이터 간의 거리를 최대한 멀리 유지하도록 설계되었습니다.

애플리케이션을 온라인화하고 접속 프록시를 통해 접속 가능하도록 하면 DDoS(Distributed Denial-of-Service) 방어가 훨씬 더 중요해집니다. 마이크로 경계와 접속 프록시에 대한 공격을 흡수할 수 있는 사업자와 협업하여 트래픽이 부담스러울 때도 운영을 계속할 수 있어야 합니다.

그리고 마지막으로, 애플리케이션 성능을 업계 최고 수준으로 유지하고 사용자가 이런 접속 방식의 변화를 받아들이는 데 그치지 않고 적극적으로 지지하게 하려면, 접속 프록시는 성능 혜택을 제공하는 네트워크를 사용해야 합니다. 특히, 기업은 콘텐츠 전송 네트워크(CDN)와 인터넷 라우팅 오버레이를 툴로 활용해 접속을 제공하는 데 그치지 않고 이전보다 훨씬 뛰어난 성능도 제공해야 합니다.

위협 방어

Akamai Enterprise Application Access와 같은 솔루션은 악의적인 공격자로부터 애플리케이션을 보호할 수 있습니다. 하지만 멀웨어에 감염된 디바이스나 피싱 링크 및 랜딩 페이지를 통해 도난당한 인증정보 등 의도치 않게 감염된 공격자로부터 사용자를 어떻게 보호해야 할까요? 바로 이 부분에서 웹 트래픽에 대한 예방과 탐지가 중요해집니다.

이와 관련하여 Akamai Secure Internet Access와 같이 클라우드 기반 DNS 방화벽 솔루션을 배포하는 접근 방식이 있습니다. 이 제품은 사용자가 보내는 모든 DNS 요청을 검사하고 실시간 위협 인텔리전스를 적용해 정상 요청은 정상적으로 해결하지만 악성 도메인에 대한 요청은 사전에 차단됩니다. 이를 통해 직원의 디바이스가 멀웨어나 랜섬웨어로 인해 감염되거나 피싱 공격의 피해자가 될 리스크가 줄어듭니다.

요약

오늘날의 클라우드와 모바일 환경에서 기존의 허브 앤 스포크 네트워크 아키텍처는 보안에 사용되는 성과 성벽 보안 경계와 마찬가지로 성능과 보안을 효율적으로 제공할 수 없습니다. 이는 모든 기업이 해결해야 할 문제이며, 해결하지 못하면 취약한 상태로 남게 됩니다. 현재 기업 정보가 유출되는 가장 큰 원인은 기업이 안전한 보안 아키텍처로 전환하지 못했기 때문이며 유출 사례는 앞으로 더 늘어날 전망입니다. 한 마디로, 기업은 경계 뒤편에 있어도 안전하지 않다는 뜻이며, 그 이유는 경계라는 것 자체가 존재하지 않기 때문입니다.

다음 단계

제로 트러스트 네트워크 접속 아키텍처로의 전환은 어떻게 시작하나요?

Akamai의 클라우드 보안 서비스를 결합하면 포괄적인 ZTNA 아키텍처를 구축할 수 있습니다. 멀티클라우드 환경에서 안전한 애플리케이션 접속을 제공할 뿐만 아니라 클라우드를 활용하기 때문에 내부 기업 네트워크에 대한 필요가 거의 사라집니다.

Akamai의 고급 분산 IAP 및 피싱 방지를 위한 멀티팩터 인증을 강력한 Akamai Connected Cloud와 함께 사용하면 마이그레이션 리스크 프로필을 거의 없애고 긴 시간 동안 입증된 Akamai의 성능과 보안 솔루션을 활용하여 애플리케이션을 하나씩 단계적으로 전환함으로써 경계가 존재하지 않는 환경으로 아주 쉽게 전환할 수 있습니다.

여러분의 제로 트러스트 여정이 지속되는 동안 Akamai는 항상 모든 단계에서 고객을 지원합니다. 애플리케이션과 데이터에 대한 접속을 제공할 뿐만 아니라 가장 높은 수준의 보안과 성능을 유지할 수 있는 아키텍처로 네트워크를 전환합니다.

Akamai 제로 트러스트 포트폴리오를 통해 비즈니스 요구사항을 충족하는 방법을 자세히 알아보세요.