백서

VPN을 제거했을 때 얻을 수 있는 4가지 혜택

Akamai

Executive Summary

기업의 경계란 더 이상 존재하지 않습니다. VPN(가상 프라이빗 네트워크)의 취약점이 빈번하게 발견되고 있고, 까다롭고 시간 소모적인 기존의 접속 솔루션은 아무런 보호 없이 기업 네트워크·애플리케이션에 대한 접속을 허용합니다. 경영진과 IT 실무진은 이러한 문제를 오랫동안 인지하고 있었지만 효과적인 대안을 찾기가 힘들었고 그 범위와 비용이 부담으로 작용했습니다. 다행히 지금은 시장 상황이 달라졌습니다.

일상 업무가 클라우드로 이전하면서 내부 기업 애플리케이션 역시 클라우드로 옮겨가고 있습니다. 이러한 상황 속에서 원활한 운영을 보장하기 위해 IT팀은 다양한 환경과 여러 지역에 걸쳐 하드웨어·소프트웨어 스택을 지원하고 유지 및 관리하며 복제해야 하지만 IaaS, SaaS, 온프레미스 애플리케이션에 대한 접속을 제공하는 작업은 매우 복잡합니다. 기업이 제로 트러스트 보안 모델을 1차 방어선으로 구축하면 리스크를 대폭 줄일 수 있고 IT팀에서 소비하는 시간과 비용 또한 최소화할 수 있습니다.

클라우드 기반 접속 솔루션은 인터넷의 편재성(ubiquity)을 활용하여 디바이스와 위치에 상관없이 모든 사용자에게 단순하고 확장성이 뛰어난 애플리케이션 접속을 제공하며 이와 동시에 IT의 프로비저닝 프로세스를 간소화합니다. 현재 기업은 VPN과 전체 네트워크 접속으로 인해 만들어진 공격면을 줄이고, 활동에 대한 상세한 로깅 및 리포팅 기능을 제공하며 사용자가 실제 네트워크에 접속할 수 없도록 하는 솔루션을 도입할 수 있습니다.

이 백서에서는 VPN을 제거했을 때 얻을 수 있는 4가지 혜택에 대해 살펴보고 최신 솔루션을 확인하여 기존의 원격 접속 프로세스에 적용함으로써 궁극적으로 더욱 효율적이고 효과적인 일상 운영 환경을 구축하는 방법을 알아봅니다.

VPN 제거에 대한 간략한 소개

'제거'라는 단어는 보통 부정적인 의미를 갖지만 VPN에 사용될 때는 그 반대입니다. 수많은 하드웨어 및 소프트웨어를 대충 조합하는 방식으로 구축된 원격 접속 기술로는 오늘날의 위협 환경에 대응할 수 없습니다. VPN은 대부분의 사람들이 사무실에 출근해 업무를 하던 때에 만들어진 기술입니다. 접속 경계와 IT 경계가 매우 분명했던 시대였고, 사용하는 디바이스 종류도 매우 제한적이었습니다. 공격의 정교함과 빈도 또한 현재보다 훨씬 낮은 수준이었습니다.

20년 전에 효과적이었던 기술은 더 이상 신뢰할 수 없습니다. 이는 권한 에스컬레이션과 신뢰할 수 있는 인증정보를 통한 네트워크의 래터럴 무브먼트(측면 이동)의 결과로, 데이터 유출 건수가 증가하는 현상을 통해서 수차례 검증된 바 있습니다. 전세계 모바일·원격 근무 인력이 갈수록 증가하는 오늘날, 사용자가 위치에 상관없이 업무 수행에 필요한 애플리케이션에만 간편하고 안전하게 접속할 수 있도록 하는 것이 무엇보다 중요해졌습니다.

기업에게는 과도한 부담으로 생각될 수도 있습니다. 전사적인 시스템 또는 프로세스를 대대적으로 변경하는 일은 매우 복잡하기 때문입니다. 하지만 간편하고 비용 효율적인 솔루션의 가용성과 기능을 좀 더 명확하게 이해한다면 대부분의 기업은 '왜 진작에 VPN을 없애지 않았을까?'라고 자문할 수밖에 없을 것입니다.

VPN의 일반적인 비효율성

관리 및 성능 측면에서 VPN의 한계를 일일이 설명할 필요는 없을 것 같습니다. IT 인력과 사용자 모두 VPN에 대한 불만이 높기 때문입니다. 지원 비용이 많이 들고 IT 대역폭을 끊임없이 소모합니다. 하드웨어는 구축이 까다로운데다 공격에 취약하고 단종되는 경우도 빈번합니다. 열악한 최종 사용자 경험으로 사용자의 불만과 번거로움이 커져 전반적인 생산성 저하를 초래합니다.

그러나 이같은 일반적인 문제는 빙산의 일각에 불과합니다. 절대로 간과할 수 없는 사실은 바로 VPN이 기업 보안에 심각한 위협이 될 수 있다는 점입니다. VPN은 본질적인 특성상 네트워크 방화벽에 구멍이 발생할 수밖에 없고 제약 없는 네트워크 접속을 제공하는 경우가 많습니다. 또한 인텔리전스도 부족합니다. VPN은 네트워크에 접속을 시도하는 사용자의 신원을 정확하게 확인하지 못하고 멀티팩터 인증(MFA)에 기반하여 접속 허용/차단 기능을 지속적으로 변경하는 기능도 제공하지 못합니다.

그 밖에도 VPN은 관리가 까다로워 숙련된 IT 전문가가 전담하는 경우가 많습니다. 접속을 제공하고 온보딩, 오프보딩, 일반 감사 등의 복잡한 일상 업무를 돕기 위해, VPN을 지원하는 데 소비한 시간과 여기에 사용되는 무수한 시스템에 대한 가시성이 확보되지 않는 경우가 빈번합니다.

> IDC에서 최근 실시한 설문 조사에 따르면, 50% 이상의 IT 실무진은 새로운 외부 사용자 그룹을 조직에 추가하기 위해 10개가 넘는 네트워크 및 애플리케이션 구성 요소를 여전히 사용하고 있다고 합니다.[1]

접속에 대한 설정, 배치, 사용, 구성, 권한 만료 처리는 IT 인력과 사용자 모두의 입장에서 간편하게 진행되어야 합니다. 현대적이고 진보적인 기업은 VPN의 함정과 시련을 이해하고 있을지도 모르겠지만 '그래서 어떻게 해야 할까?'라는 질문에 직면하게 됩니다. 그렇다면 과연 기업을 안전하게 보호하고 소중한 IT 자산을 절감하며 예산의 제약까지 고려하는 맞춤형 원격 접속을 구현하려면 어떻게 해야 할까요?

지금 변화가 필요한 이유

VPN을 없애는 것은 실행 가능한 대안일 뿐 아니라 인력 모빌리티, 다양한 디지털 생태계, 클라우드 전환, 위협 환경이라는 네 가지 현실을 고려해 볼 때 반드시 필요합니다.

모빌리티

기업의 사용자들은 여러 곳에 분산되어 있습니다. 대부분의 기업은 현재 직원의 원격 근무를 허용하고 있으며, 사용자는 매일 집, 공항, 회의장, 기차, 호텔, 카페 심지어 3만 피트 상공의 비행기 안에서 회사 네트워크에 접속해 업무를 처리합니다. 직원들은 근무 시간의 50%~60%를 사무실 이외의 공간에서 보냅니다.[2] 또한 글로벌 지식 근로자의 79%가 정규직 원격근무 근로자라는 통계가 발표되었습니다.[3] 회사에 소속되어 있으나 재택 근무하는 직원이 2005년 이래로 140% 증가했으며,[4] IDC Research는 이런 추세가 계속 확대될 것이라고 전망합니다.[5] 이러한 상황 속에서도 지역에 상관없이 모든 직원들은 업무 수행을 위해 기업 애플리케이션에 안전하고 간편하게 접속할 수 있어야 합니다.

디지털 생태계

오늘날 직원은 매우 다양하게 구성되어 있습니다. 이니셔티브를 지원하기 위해 계약직 근로자, 파트너, 공급업체, 개발자, 고객, 유통 채널, 기타 써드파티 업체에 의존하는 기업들이 점차 증가하고 있습니다. 현재 고용률이 유지만 되어도 2027년까지 미국 근로자의 50%(8600만 명) 이상이 프리랜서일 것으로 전망됩니다.[6]

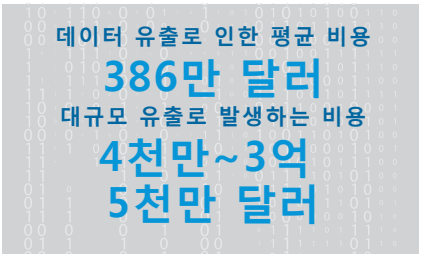
이렇듯 다양해진 생태계 속에서 기업은 전세계적으로 분산되어 있고 나아가 빠르게 확장하고 있습니다. 인수합병은 기업 환경에서 흔히 볼 수 있는 현상이며, 이러한 활동과 합병 규모 모두 2018년에 계속해서 증가할 것으로 예상됩니다.[7] 다시 말해, 더 많은 사용자가 데스크톱 컴퓨터, 노트북, 휴대폰, 태블릿, '스마트 커넥티드' 디바이스, BYOD(Bring Your Own Device) 같이 더 많은 디바이스를 통해 회사 네트워크에 접속하게 됩니다. 따라서 이러한 수요에 대응할 수 있는 접속 기술이 필요합니다.

클라우드 혁신

클라우드 아키텍처는 갈수록 복잡해지며 애플리케이션 또한 분산되는 범위가 넓어지고 있습니다(예: 온프레미스, IaaS, SaaS). 또한, 클라우드 애플리케이션의 사용도 증가하고 있습니다. 기업에서 사용하는 클라우드 서비스는 평균 1,427개가 넘고 직원들은 매일 평균 36개의 서비스를 적극적으로 사용하고 있습니다.8 기존 시스템을 사용하는 기업들은 중앙 보안 스택을 이용해 이러한 클라우드 트래픽을 WAN으로 백홀한 다음 직접 연결 또는 VPN을 통해 다시 IaaS와 인터넷으로 라우팅하는 경우가 많습니다. 그러나 이 방식은 애플리케이션 성능과 사용자 경험을 저하시키고 기업 보안 리스크를 증가시킵니다. 뿐만 아니라 지역과 벤더 전반에 걸쳐 보안 스택을 복제해야 하기 때문에 상당한 비용을 초래합니다.

보안

사이버 범죄로 인한 비용은 1조 달러에 육박합니다. 악의적 공격자들은 집요하고 금전적인 이득에 동기부여가 되어 있기 때문에 특정 표적을 겨냥한 맞춤형 공격을 개발하고 이를 판매합니다. 데이터 유출 1건당 평균 386만 달러의 손실이 발생하며, 최악의 경우인 '대량 유출' 시에는 4,000만 달러에서 3억 5,000만 달러의 손실이 발생할 수 있습니다.[9] 더욱 놀라운 사실은 40% 이상의 유출 사고가 권한이 있는 사용자와 관련되어 있다는 점입니다.[10] 접속 위치, 유형, 방법이 확장됨에 따라 사용자의 분류와 모든 요청의 자격 확인이 반드시 필요합니다. 일방적으로 적용되는 네트워크 수준 허용 방식은 케이스별로 이루어지는 애플리케이션 수준의 맞춤형 접속 방식으로 대체되어야 합니다.



복잡한 VPN으로는 오늘날의 분산된 다양한 모바일 기업의 요구사항을 충족할 수 없습니다. 또한 민첩성과 편의성을 위해 보안을 희생할 수는 없습니다. 클라우드 기반 접속 솔루션은 의사 결정에 인텔리전스를 적용해 사용자, 디바이스, 위치는 물론이고 접속 패턴까지 파악하여 보안을 강화합니다.

앞으로 가야 할 방향

VPN을 대신할 더욱 빠르고 간편하며 안전한 대안은 이미 존재합니다. 비용을 절감하고 불필요한 애플리케이션 접속을 제한하며 접속하는 사용자와 이용하는 콘텐츠를 상세하게 파악할 수 있는 중요한 시점에 직면해 있다는 점을 깨닫는 기업들이 점차 증가하고 있습니다.

설정한 후에 더 이상 관리하지 않는 VPN 시스템은 편의성과 효율성이 매우 낮고 이제는 과거의 솔루션이 되었습니다. 클라우드 기반 서비스는 모든 인바운드 방화벽 포트를 차단하고 사용자를 네트워크로부터 분리하여 IT팀이 제로 트러스트 보안 프레임워크를 구현할 수 있도록 지원합니다. 이와 동시에 사용자에게 업무 처리에 필요한 애플리케이션에 대한 접속을 즉각 제공합니다. 또한 이 모든 작업을 단일 포털을 통해 간편하게 진행할 수 있어 IT팀은 며칠씩 걸리던 업무를 몇 분 내에 완료할 수 있습니다.

애플리케이션 접속을 위한 클라우드 프레임워크의 작동 방식

애플리케이션 접속 클라우드 아키텍처를 VPN의 일반적인 문제나 복잡성 없이 VPN이 제공하던 모든 기능을 구입 즉시 이용 가능한 솔루션으로 이루어진 범용 포털이라고 생각해 보시기 바랍니다. 즉, 데이터 경로 보호, IAM(신원 관리 시스템), 애플리케이션 보안·가속, SSO(Single Sign-On)는 물론이고 명확한 가시성 및 제어까지 제공하는 통합 서비스를 모든 애플리케이션에 적용할 수 있습니다. 그 결과 기술 부채가 줄어들고 스택을 통합하는 동시에 프로세스를 단순화하고 시간(및 잠재적으로 비용)을 절약할 수 있습니다.

또한 모든 사용자는 회사 네트워크에 직접 접속하는 경로를 이용하지 않고도 원격 또는 다른 방식으로 서비스를 안전하게 이용할 수 있습니다. 즉, 데이터 센터 또는 클라우드에서 상호 인증된 TLS(Transport Layer Security) 연결을 사용자에게 제공하여 허용된 애플리케이션을 직접 이용할 수 있도록 합니다. 안전하지 않은 터널을 사용하지 않고 멀웨어가 침투할 수 있는 뚜렷한 경로가 없어서 중요한 시스템으로 감염을 확산시킬 수도 없습니다.

무엇보다도 이제 사용자는 자신의 디바이스에서 원하는 브라우저를 통해 애플리케이션을 사용할 수 있습니다. 회사 전체에서 SSO와 MFA를 활용함으로써 IT팀은 한층 높은 수준의 제어가 가능하고 사용자 경험 또한 크게 단순화되고 개선되어 더 이상 보안이 큰 이슈가 되지 않게 됩니다.

끝으로, 수많은 종류의 기업 인프라가 클릭 한 번으로 긴밀하게 통합되므로 별도의 스크립팅과 구축 작업이 사실상 필요하지 않다는 점도 빼놓을 수 없습니다. 그 결과 사용자가 필수 애플리케이션을 사용해야 하는 모든 위치와 중요한 워크로드가 배치된 모든 환경에 제로 트러스트 프레임워크를 구현하는 단일 소스 보안 접속 제공 모델이 탄생하게 됩니다.

클라우드 기반 보안 접속의 백엔드 이점

보안 강화
버튼 클릭만으로 방화벽 잠금, 애플리케이션 IP 주소 숨김, MFA 추가 작업을 수행하여 네트워크에서 원치 않는 트래픽을 제거합니다.

IT 복잡성 감소
추가적인 소프트웨어 없이 애플리케이션 전반에 걸쳐 VPN 및 MFA 기능을 하나의 유연한 SSO에 간편하게 통합합니다.

심층 리포팅
기존 툴과 손쉽게 통합되는 편의성과 내장형 리포팅을 통해 모든 사용자 활동을 완벽하게 감사하고 기록합니다.

도입 간소화
전 세계 어디서나 디바이스 유형에 상관없이 애플리케이션을 전송할 수 있으므로 도입이 간편해지고 시간 소모적인 IT 티켓이 감소합니다.

VPN을 제거했을 때 얻을 수 있는 4가지 혜택

사용자가 필요로 하는 애플리케이션을 명확히 결정하고 이에 따라 접속을 제한하는 것은 오늘날의 기업 보안과 사용자 경험에 있어서 다른 무엇보다 중요합니다. 기업이 사용자의 디바이스를 식별하는 동시에 접속을 요청하는 특정 개인의 신원을 확인하는 것은 갈수록 중요해지고 있습니다.

물론 이것이 간단한 일은 아니지만, VPN을 없애고 단일화된 애플리케이션 작업 영역 및 포털로 전환할 경우 누릴 수 있는 이점은 상당합니다. IT팀, 사용자, 기업 모두 클라우드 기반 접속이 기업 전반에 제공하는 4가지 주요 개선 사항을 거의 즉각적으로 확인할 수 있습니다.

1. 더욱 간편하고 구체적인 원격 접속

과제: 불필요한 전체 네트워크 접속

기업은 각 사용자에게 필요한 애플리케이션만을 식별하여 공격면을 최소화해야 합니다. 당연하게 들릴 수 있겠지만, VPN으로 인해 과도한 애플리케이션 접속이 이루어지고 있는 것이 현실입니다. VPN을 없애면 시간 소모적인 불필요한 보안 모니터링, 불필요한 권한 부여와 중복을 제거할 수 있습니다.

솔루션: 최종 사용자, 디바이스, 맥락 파악

사용자의 IP 주소만으로는 많은 것을 파악할 수 없습니다. 네트워크 내부의 IP 범위를 전적으로 신뢰하는 것은 잘못된 생각입니다. ID와 디바이스는 물론 위치, 이용 시간, 인증 상태, 사용자의 그룹 멤버십 등에 관한 여러 정보를 기반으로 신뢰 여부를 지속적으로 평가해야 합니다. 결국, 접근 권한을 기본적으로 거부하며 이를 최소한으로 유지하는 보안 시스템을 채택하면 각 사용자에게 반드시 필요한 특정 애플리케이션 접속이 현재 VPN에서 사용자에게 실제로 허용하는 접속에 비해 훨씬 줄어들게 됩니다. 결과적으로 사전에 예방 가능한 리스크가 크게 증가합니다. 또한, 오늘날의 모바일·디지털 인력을 고려했을 때 사용자가 한 가지 디바이스만 사용해 네트워크에 접속하는 일은 매우 드뭅니다. 이런 이유로 접속을 요청하는 개인을 인증하고 필요한 권한을 부여하는 동시에 요청에 사용된 디바이스와 맥락을 파악하는 것이 무엇보다 중요해졌습니다.

사용자는 검증 강화 또는 권한 철회가 없다는 가정하에 자신의 디바이스로 로그인하고 ID를 검증받고 권한을 획득한 애플리케이션에 접속할 수 있습니다. 즉, 즉각적이고 확장 가능한 가치를 제공하는 서비스를 간편하고 빠르고 안전하게 이용할 수 있게 됩니다.

2. 관리 및 IT 보안 부담 경감

과제: 비직원에 대한 권한 부여

직원의 접속을 제한하는 것이 최선의 방법인 경우, 협력사와 고객 등 생태계의 다른 구성원의 권한을 판단하고 접속을 제한하는 것이 반드시 필요합니다. IDC Research의 최근 조사에서는 IT 전문가의 46%가 소속 기업에서 매년 수 차례 주요 보안 사고가 발생하는 것으로 예측합니다.[11] 사용자 기반이 갈수록 모바일·다양화·분산화되고 클라우드를 가장 중시하는 경향을 보이기 때문에 보안 사고의 발생 가능성은 계속해서 증가할 수밖에 없습니다. 접속 제어는 ID와 IP 주소를 비교한 결과를 기반으로 하므로 그 다음으로 수행해야 하는 논리적 단계는 IT팀이 하드웨어 업그레이드나 많은 시간과 노력이 드는 네트워크에 대한 전반적인 변경 없이 사용자를 특정 애플리케이션과 연결시키는 정책을 빠르고 간편하게 설정할 수 있도록 지원하는 것입니다. 근본적인 문제는 VPN이 이러한 방식으로 작동하지도 않으며 작동할 수도 없다는 것입니다.

솔루션: 안전한 권한 부여 파라미터 설정

권한 부여 및 모니터링 모두를 제어하는 중앙의 통합 관리 지점을 구축하면 접속을 차단하고 네트워크 인증정보를 요구하는 잠재적인 악의적 공격자의 리스크를 줄일 수 있습니다. 이렇게 하면 경영진과 IT팀이 앞서 언급한 보안 사고에 신속하게 대응할 수 있는 필수적인 민첩성을 확보할 수 있어 안심하고 업무를 수행할 수 있습니다.

일반적으로 협력사, 파트너사, 공급업체, 기타 시간제 근무자는 단기 접속이 필요합니다. 처리하는 프로젝트와 과제는 다양하겠지만 VPN을 통해 이러한 접속을 설정, 관리, 모니터링, 배치하는 데에는 상당한 시간과 노력이 끊임없이 필요합니다. IT 전문가는 이미 과중한 업무에 시달리고 있습니다. 이제 VPN의 부담을 없애고 클라우드 환경으로의 원격 접속으로 전환하는 기업은 비즈니스 시간과 비용을 모두 절약할 수 있습니다.

비즈니스 측면의 주요 이점

시간 절약
IT, 보안, 관리팀이 사용자 접속 모니터링과 관리 업무 대신 우선 순위가 더 높은 프로젝트에 집중할 수 있습니다.

생산성 증대
일관성이 없고 성능이 열악한 애플리케이션이 없어지므로 사용자가 더 빠르게 작업을 수행할 수 있습니다.

데이터 보안
실시간 활동을 효과적으로 모니터링하여 회사 데이터, 고객 정보, 기타 지적 재산의 유실을 방지합니다.

비용 절감
값비싼 하드웨어와 설치에 소모되는 예산을 줄이는 동시에 예기치 않은 유출 사고로 인한 손실을 최소화합니다.

3. 효율적인 보안 정책

과제: 디지털 혁신으로 리스크 노출 증가

오늘날 위협의 정교함과 무분별한 교차 네트워크 접속이 초래한 리스크를 고려해 볼 때 '신뢰하되 검증'하는 방식은 더 이상 안전한 보안 옵션이 아닙니다. 40% 이상의 데이터 유출 사고가 권한이 있는 사용자와 관련되어 있지만,[12] 접속 수요는 빈도, 복잡함, 사용되는 디바이스 유형 그리고 오리진 포인트의 측면에서 여전히 증가하고 있습니다. 여러 개의 VPN 게이트웨이가 존재하면 일반적으로 IT팀과 비즈니스의 골칫거리도 그만큼 늘어나게 되는데, VPC(가상 프라이빗 클라우드)로는 필요한 모든 것을 충족할 수 없습니다. VPN이나 VPC를 사용하는 경우에는 세분화된 보안 정책을 채택할 수밖에 없고 지속적인 라우팅 환경 복잡성과 수동 배포로 인해 결국 회사는 점점 더 위협에 노출되게 됩니다. 설문조사 응답자의 50% 이상이 원격 접속 보안의 모든 측면이 어렵다고 답한 것도 놀랄 일이 아닙니다.[13]

솔루션: 제로 트러스트 전략 도입

전적으로 내부에서만 이루어지는 것은 더 이상 없습니다. 기업 IT 및 보안을 위한 클라우드 기반 모델로 전환하면 백엔드 프로세스가 단순화되고 애플리케이션을 퍼블릭 인터넷에서 숨길 수 있으며 멀티팩터 인증(MFA)을 추가적인 방어 레이어로 사용해 리스크를 줄일 수 있습니다. 새로운 애플리케이션이 몇 분 내에 가동되므로 IT팀과 경영진은 애플리케이션당 수백에서 수천 시간을 절약할 수 있습니다. 정책을 설정 또는 조정해야 하는 상황에서도 추가적인 설치 없이 신규 사용자를 빠르고 간편하게 설정할 수 있습니다.

제로 트러스트 전략의 이점은 여기서 끝이 아닙니다. 사용자 활동의 완전한 감사 및 리포팅 또한 백엔드에서 간편하게 수행할 수 있습니다. 이러한 보고서가 기존 툴에 통합되거나 빌트인 형식으로 제공되든 상관없이 원하는 대로 지정할 수 있습니다.

4. 원활한 접속으로 사용자의 불만 해소

과제: 복잡한 프로세스 제거

성공적인 기업은 원활한 도입과 지원을 보장하기 위해 사용 편의성을 항상 염두에 두어야 합니다. 사용 편의성이 보장되면 사용자는 느린 서버, 빈번한 서비스 중단, 긴 온보딩 프로세스 및 일반적인 연결 관련 문제에서 벗어날 수 있습니다. 동시에 IT 보안팀은 복잡한 스택과 시간 소모적이며 지속적인 하드웨어 유지보수 업무로부터 벗어날 수 있습니다. 그리고 경영진 역시 이를 통한 비용 절감과 숙련된 IT 전문가의 대폭적인 업무 부담 경감, 직원의 생산성 증대라는 이점을 누릴 수 있습니다

솔루션: 클라우드 환경에 적응

클라우드 기반의 솔루션은 애플리케이션별로 원활하게 접속을 제공하고 사용자가 선호하는 디바이스와 호환되며 관리 복잡성을 경감할 수 있는 가장 확실한 방법입니다 데이터 경로 보호, IAM, 애플리케이션 보안·가속, SSO, MFA 등이 더욱 쉽고 즉각적으로 통합, 관리, 모니터링 및 업데이트됩니다. 오늘날과 같이 치열한 글로벌 경쟁 시장에서 이처럼 빠르고 간편한 보안 솔루션은 기업의 발전과 더불어 성공에 기여하는 사람들의 역량을 강화하는 데 핵심적인 역할을 합니다.

VPN 제거를 위한 주요 절차

그렇다면 기업이 안심하고 사용할 수 있는 원격 접속 솔루션을 구현하기 위한 다음 단계는 무엇일까요? 참신하고 혁신적인 접근 방식이 매일 쏟아져 나오고 있지만 가장 먼저 해야 하는 일은 제로 트러스트 보안 철학에 기반한 효과적인 전략을 도입하는 것입니다. 이를 위한 최고의 방법은 단순성과 간편함을 유지하는 것입니다.

- **데이터의 차별화** - 퍼블릭에서 사용될 수 있는 데이터와 기밀 정보를 분류해야 합니다.
- **애플리케이션 식별** - 애플리케이션을 식별하고 접속을 요청하는 대상을 정확하게 파악합니다.
- **애플리케이션 확장 및 배치** - 전세계적으로 분산된 ID 인지 프록시 플랫폼을 퍼블릭·프라이빗 인프라 전체에 배치하여 고가용성 기능을 지원합니다.
- **클라우드 기반 아키텍처 도입** - '원격근무자'로 간주되는 재택근무자를 포함한 모든 사용자를 동일하게 취급하는 클라우드 기반 아키텍처를 도입합니다.
- **모니터링 강화** - 모든 사용자와 디바이스에 MFA 및 SSO를 적용하여 모니터링을 극대화하고 실시간 리포팅 기능을 사용하여 모든 애플리케이션이 언제나 안전하게 보호되도록 합니다.
- **선택 사항: 네트워크 세그먼테이션 기법 구현** - 서브넷 내에서 측면 이동하는 트래픽을 구분합니다.

결론

글로벌 기업은 여러 데이터 센터 또는 하이브리드 클라우드 환경에서 호스팅되는 오래된 VPN의 비효율성과 취약점에 더 이상 얽매이지 않습니다. 보다 빠르고 간편하고 안전한 솔루션으로 모든 인바운드 방화벽 포트를 차단하고 이와 동시에 사용자에게 필요한 애플리케이션에만 원격 접속을 제공할 수 있습니다. 네트워크 전체에 불필요한 접속을 제공하는 시절은 끝났습니다.

이제 기업의 인프라를 인터넷으로부터 분리해야 할 때입니다. 내부 공격 경로를 최소화하고 퍼블릿 인터넷으로부터 애플리케이션을 숨기며 최신 클라우드 기반 솔루션을 단 몇 분 만에 기업의 1차 방어선으로 배치할 수 있습니다. 이 모든 것이 사내에서 자체적으로 솔루션을 구축할 때보다 훨씬 저렴한 비용으로 가능합니다.

Akamai의 제로 트러스트 방식에 대해 자세히 알아보려면 akamai.com/eaa를 참조하시기 바랍니다.

출처
1) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
2) http://globalworkplaceanalytics.com/telecommuting-statistics
3) PGi Global Telework Survey, http://go.pgi.com/gen-genspec-15telesur-SC1129
4) http://globalworkplaceanalytics.com/telecommuting-statistics
5) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
6) https://www.upwork.com/press/2017/10/17/freelancing-in-america-2017
7) Deloitte Mergers and Acquisitons Trends report 2018, https://www.deloitte.com/content/dam/Deloitte/us/Documents/mergers-acqisitions/us-mergers-acquisitions-2018-trends-report.pdf
8) https://www.skyhighnetworks.com/cloud-security-blog/12-must-know-statistics-on-cloud-usage-in-the-enterprise
9) Ponemon Institute, 2018 Cost of Data Breach Study: Global Overview, https://www.ibm.com/security/data-breach
10) IDC Remote Access and Security Report, https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
11) 상동
12) 상동
13) 상동