



제로 트러스트 보안이 필요한 4가지 이유

목차

서론	3 - 4
01. 랜섬웨어 공격 증가	5 - 7
02. 하이브리드 인력	8 - 10
03. 클라우드 컴퓨팅 리소스 도입	11 - 13
04. 엄격한 컴플라이언스 요구사항	14 - 16
2주 내에 SWIFT 컴플라이언스를 달성한 글로벌 은행	17 - 18

서론

공격자가 더 정교해지고, 랜섬웨어 그룹이 확산하고, 기술의 발전으로 새로운 취약점이 발생함에 따라 제로 트러스트 보안 모델로 전환하는 기업이 증가하고 있습니다. 제로 트러스트 접근 방식의 핵심은 기존 보안 접근 방식의 핵심이었던 사용자, 애플리케이션, 디바이스에 대한 암묵적 신뢰를 없애는 것입니다. 실제로 제로 트러스트 보안 모델의 장점을 누릴 수 있는 4가지 주요 시나리오에는 기업에 대한 랜섬웨어 공격, 원격 근무로의 전환, 클라우드 환경 보안의 필요성, 다가오는 감사 등이 있습니다.

이러한 시나리오는 랜섬웨어 공격의 증가, 하이브리드 근무로 이동, 클라우드 컴퓨팅으로의 전환, 보안 감사에

대한 요구 증가 등 최근의 추세에 따른 결과입니다. 이로 인해 위치에 관계없이 신원을 확인하고 유출에 대처할 때 선제적인 조치를 취하는 보안 접근 방식이 필요해졌습니다. 제로 트러스트는 데이터에 접속하기 위해 강력한 사용자 신원을 요구하고 공격이 발생하면 선제적인 방어 조치를 제공하는 유일한 접근 방식입니다.

제로 트러스트 전략을 구축하는 것은 이미 업무가 과중한 보안팀에게 부담스러워 보일 수 있지만, 반드시 그렇지 않습니다. 단계적 접근 방식을 취하고 빠른 성과에 집중하면 기존 보안 솔루션과 관련된 복잡성과 리스크를 일부 줄이고 보안 체계를 개선할 수 있습니다.

기존 기술을 뜯어고치고 교체할 필요는 없습니다. 가장 시급한 비즈니스 요구사항에 맞춰 제로 트러스트 투자를 조정하는 것부터 시작하세요. 단기간에 기존 솔루션을 제로 트러스트로 리브랜딩한 벤더사가 아니라 신뢰할 수 있는 제로 트러스트 벤더사를 선택하세요. 제로 트러스트 보안의 여러 요소(제로 트러스트 네트워크 접속, DNS 방화벽, 마이크로세그멘테이션 등)를 단일 플랫폼에서 결합할 수 있는 벤더사를 적극 고려하세요. 도입 이유가 무엇이든 제로 트러스트는 비즈니스 민첩성, 비용 최적화, 톨 편의성을 실현하고 전반적인 운영을 개선할 수 있도록 지원합니다.

제로 트러스트를 선택해야 하는 4가지 이유



랜섬웨어 공격 증가



하이브리드 인력



클라우드 컴퓨팅 리소스 도입



엄격한 컴플라이언스 요구사항

01

랜섬웨어 공격 증가

랜섬웨어 차단 강화

지난 몇 년 동안 랜섬웨어 공격은 병원과 은행부터 파이프라인과 기타 중요 인프라에 이르기까지 전 세계 기업을 혼란에 빠트렸습니다. 실제로 **Cybersecurity Ventures**는 2031년까지 랜섬웨어로 인한 피해액이 연간 약 2650억 달러에 달할 것으로 예측합니다. 또한, 랜섬웨어 공격자들은 멀웨어 페이로드와 관련 갈취 활동을 점차 개선하면서 2초마다 새로운 공격(소비자 또는 기업 대상)을 시작할 것으로 예측됩니다.

제로 트러스트 전략이 없으면 랜섬웨어 조직은 다음과 같은 약점을 활용할 수 있습니다.

- ☒ 사용자, 애플리케이션, 네트워크에 대한 암묵적 신뢰를 통해 네트워크에 침투한 공격자가 측면으로 이동해 멀웨어를 전파할 수 있습니다.
- ☒ 감염을 허용하는 지나치게 허용적인 접속 정책을 통해 랜섬웨어가 주입될 수 있습니다.
- ☒ 비밀번호만 신뢰하는 시스템은 인증정보 도용의 기회를 제공합니다.

제로 트러스트의 장점

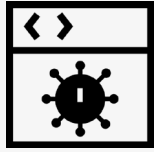
제로 트러스트 아키텍처를 구축하고, 접속 제어 정책을 적용하고, 마이크로세그멘테이션을 사용하는 기업은 이러한 공격으로 인한 피해를 최소화할 수 있습니다. 공격자들은 처음부터 시스템에 침투하기가 더 어려울 뿐만 아니라 확장 능력도 제한됩니다.

Akamai가 랜섬웨어 킬 체인을 끊는 방법

랜섬웨어 공격은 일반적으로 초기 감염, 측면 이동, 데이터 유출 및 암호화로 이어집니다. 기업은 제로 트러스트를 통해 각 단계가 발생할 때마다 또는 발생하기 전에 해결할 수 있습니다.

“랜섬웨어는
2초마다 기업,
소비자, 디바이스를
공격할 것입니다”

2031년까지, Cybersecurity Ventures의
2023년 Who's Who 랜섬웨어 보고서 인용



초기 감염

Akamai Guardicore Platform은 공격이 초기 진입 지점을 넘어 확산되는 것을 방지하고, Akamai MFA는 사용자의 인증정보가 도난 및 악용되지 않도록 보호합니다.



측면 이동

Akamai Guardicore Platform은 전파 경로를 줄이고 측면 이동을 방지합니다. Akamai Guardicore Access는 공격자가 악용하고자 하는 애플리케이션을 감염시키기 위해 이동하는 것을 제한합니다. Akamai Hunt는 네트워크에서 교묘하고 정교한 위협을 탐지하고 방어합니다.



데이터 유출 및 암호화

Akamai Guardicore Platform은 중요한 애플리케이션에 대한 접속을 제한해 공격자가 감염된 네트워크에서 중요한 데이터에 접속하지 못하도록 합니다. Akamai Secure Internet Access Enterprise는 피싱 사이트와 명령 및 제어 사이트에 대한 요청을 차단합니다. 마지막으로, Akamai Hunt는 비정상적인 행동을 탐지해 공격자들이 중요한 데이터를 암호화하지 못하도록 방지합니다.

02

하이브리드 인력

새로운 하이브리드 인력 보안

코로나19 팬데믹 기간에 새로운 하이브리드 인력이 성장하고 확장되었습니다. 이런 인력을 보호하는 것은 방화벽과 VPN 등 오래된 보안 툴을 사용하는 기업의 경우 더욱 어렵습니다. 30년 전 원격 접속 VPN이 처음 도입되었을 때는 모든 것이 지금과 달랐습니다. 당시는 인터넷 도입 초기 단계였고, 애플리케이션이 데이터 센터에서 실행되었으며, 원격으로 접속하는 사용자 수가

훨씬 적었습니다. VPN을 통해 사용자를 인증하고 전체 네트워크에 대한 접속 권한을 부여하면 공격 표면이 늘어나고 레거시 VPN과 관련된 수많은 제로데이 취약점에 노출됩니다. 필요한 인증정보를 가진 모든 사용자는 기업 VPN에 로그인할 수 있으며, 일단 VPN에 들어가면, 네트워크에서 측면으로 이동해 VPN이 보호하려는 리소스에 접속할 수 있습니다.

제로 트러스트의 장점

제로 트러스트는 최소 권한 접속의 원칙에 따라 어떠한 사용자나 애플리케이션도 기본적으로 신뢰하지 않아야 한다고 가정합니다. ZTNA(Zero Trust Network Access)는 VPN과 완전히 다른 접근 방식으로 원격 근무자의 접속을 보호합니다. 사용자는 전체 네트워크를 리스크에 노출시키지 않고, 필요한 애플리케이션과 데이터에만 직접 연결되므로, 민감한 데이터와 리소스에 과도하게 허용된 접속 권한을 가진 악성 사용자가 측면 이동할 수 없습니다. 유출 사고가 발생한 경우 효과적인 제로 트러스트 마이크로세그멘테이션 솔루션은 내부 네트워크를 분할해 유출이 확산되지 않고 네트워크의 다른 부분에 피해를 주지 않도록 합니다. **Gartner**에 따르면 2025년까지 VPN 서비스 대신 ZTNA가 신규 원격 접속 배포의 70% 이상을 지원할 예정이며, 이는 2021년 말 10% 미만에서 크게 증가한 수치입니다.

“Gartner에 따르면 2025년까지 VPN 서비스 대신 ZTNA가 신규 원격 접속 배포의 70% 이상을 지원할 예정이며, 이는 2021년 말 10% 미만에서 크게 증가한 수치입니다.”

Akamai가 하이브리드 및 원격 근무를 지원하는 방법

Akamai의 포괄적인 제로 트러스트 플랫폼은 하이브리드 인력의 요구 사항을 충족합니다. 주요 장점은 다음과 같습니다.



리스크 감소

Akamai는 적합한 사용자를 적합한 애플리케이션에 직접 연결해 공격 표면을 줄이고 측면 이동을 제한합니다.



사용자 경험 개선

원격 사용자는 애플리케이션, 디바이스, 위치에 관계없이 리소스에 접속할 수 있기 때문에 VPN에 연결하고 연결을 끊을 필요가 없습니다.



민첩성 향상

Akamai의 솔루션은 서비스로 소비되기 때문에 기업은 하드웨어를 배포할 필요가 없으며, 수요 증가에 따른 확장을 걱정하지 않아도 되기 때문에 비용과 복잡성이 줄어듭니다.

03

클라우드 컴퓨팅 리소스 도입

간편한 클라우드 전환

기업은 유연성과 민첩성을 갖추고 인프라를 최신화하기 위해 애플리케이션을 클라우드로 전환하고 있습니다. 하지만 클라우드 환경은 공격 표면을 확장시키고 새로운 보안 요구사항을 발생시킵니다. 다양한 클라우드와 온프레미스 환경 간의 통합으로 애플리케이션이 중단되고 보안 리스크가 발생할 수 있습니다. VPN과 방화벽 등 기존 네트워크 구조를 사용해 애플리케이션을

클라우드로 전환하려는 기업은 측면 위협, 낮은 확장성, 높은 비용이라는 리스크에 직면하는 경우가 많습니다. 전환이 완료된 후에도 자산은 안전해야 하며 사용자는 업무 권한에 따라 인증받아야 합니다. 클라우드 인프라 사용자는 일반적으로 온프레미스 환경보다 리소스, 서비스, 관리 권한에 더 많이 접속할 수 있기 때문에 리스크가 증가하고 차질이 발생할 가능성이 있습니다.

제로 트러스트의 장점

제로 트러스트 전략은 클라우드 전환을 지원합니다. 제로 트러스트는 많은 클라우드 기반 애플리케이션, 특히 취약점을 일으킬 수 있는 써드파티 애플리케이션에 내재되어 있는 암묵적인 신뢰를 제거합니다. 제로 트러스트 솔루션은 기업이 강력한 보안 기능을 통해 클라우드 기반 애플리케이션을 보다 쉽게 배포할 수 있도록 보장합니다. 클라우드에 제로 트러스트를 배포하면 다음과 같은 장점이 있습니다.

- ✓ 자산 및 리스크에 대한 가시성 개선
- ✓ 제로 트러스트 세그멘테이션 및 클라우드 리소스에 대한 최소 권한 접속으로 공격 표면 감소
- ✓ 속도와 민첩성을 제공하는 최신 네트워크 인프라
- ✓ 운영 비용 및 복잡성 감소



Akamai가 클라우드 전환을 지원하는 방법

Akamai의 제로 트러스트 솔루션은 자산과 해당 정책을 자동으로 전환할 수 있도록 지원합니다. 다운타임이나 업무 중단이 없습니다. Akamai는 다음과 같은 장점을 제공합니다.



가시성 개선

의존성에 대한 이해도를 높이면 효과적인 클라우드 세그멘테이션 정책을 생성해 공격 표면을 줄이고 리스크를 최소화할 수 있습니다.



ZTNA(Zero Trust Network Access)

사용자는 강력한 인증을 기반으로 접속 권한이 부여된 앱에만 접속할 수 있습니다.



위협 탐색

Akamai의 전문 위협 탐색 팀은 클라우드 환경 전반에서 이상 공격 행동을 지속적으로 검색하고 Akamai 고객에게 모든 네트워크 리스크에 대해 통보합니다.

04

엄격한 컴플라이언스 요구사항

컴플라이언스 간소화 및 리스크 축소

보안 리더는 컴플라이언스 요구사항을 충족하는 기업이 실제로 안전한 기업이 아니라는 것을 알고 있지만, 경영진에게 보안 감사는 여전히 가장 중요한 문제입니다. 보안 리더는 감사 실패가 심각한 비즈니스 혼란으로 이어지고 수익에 영향을 미칠 수 있다는 사실을 알고 있습니다. 컴플라이언스 평가는 보안팀에서 가장 많은 시간과 리소스를 투자하는 활동 중 하나입니다. 또한, 경계 없는 디지털 환경으로의 전환과 원격 근무의 확산으로 인해 컴플라이언스가 더욱 어려워졌습니다. 기업은 일반적으로 PCI DSS(Payment Card Industry Data Security Standard), HIPAA(Health Insurance Portability and Accountability Act), SWIFT(Society for Worldwide Interbank Financial Telecommunication) 등의 컴플라이언스 표준을 준수하기 위해 환경을 격리하고 규제 자산을 리팩토링해야 합니다.

또한, 기업은 원격 사용자, 기업 온프레미스 사용자, 파트너, 공급업체 등을 지원해야 하기 때문에 기업 환경의 경계를 정의하기가 거의 불가능합니다. 보안팀은 접속 제어가 성공의 주요 결정 요인이 되는 감사에 대비하는 과정에서 다음과 같은 질문에 답할 수 있어야 합니다.

- 권한이 있는 사용자만 민감한 정보에 접속할 수 있도록 어떻게 제한하나요?

- 감사 환경의 범위를 어떻게 정하나요?

- 어떻게 하면 감사 프로세스를 간소화하고 혼란을 줄일 수 있을까요?

제로 트러스트의 장점

다행히 제로 트러스트 접근 방식은 이러한 모든 질문에 답변하는 데 도움이 될 수 있습니다. 제로 트러스트의 2가지 핵심 요소, 즉 명시적 검증과 최소 권한 접속 지원 기능은 컴플라이언스 프로세스를 크게 간소화합니다. 기업은 데이터 센터나 클라우드의 다른 트래픽으로부터 규제 대상 자산을 격리하고 위치에 관계없이 ID를 기반으로 접속을 허용할 수 있습니다. 가시성을 개선하면 규제 대상 환경으로 들어오고 나가는 트래픽을 표시하고 규제 대상 범위를 파악하는 데 도움이 됩니다. 이렇게 하면 감사의 복잡성과 비용이 크게 줄어들고 감사 업무가 간편해집니다.

Akamai의 컴플라이언스 지원 방법

Akamai의 포괄적인 제로 트러스트 포트폴리오는 PCI DSS, HIPAA, ISO(International Standards Organization), SOX(Sarbanes-Oxley), 기타 프레임워크 등 모든 감사에 대비할 수 있도록 지원합니다. Akamai Enterprise Application Access는 GDPR(General Data Protection Regulation) 요구사항을 충족하면서 민감한 개인 정보에 대한 써드파티의 접속을 제어합니다. Akamai Guardicore Segmentation은 PCI DSS에서 규제되는 자산에 대한 이해도를 높이고, HIPAA에 대응하기 위해 클리어링 하우스(Clearing House) 기능을 격리하며, SWIFT 규제를 준수하기 위해 인터넷 접속을 제한하고 중요한 시스템을 격리합니다. Akamai MFA는 헬스케어 시스템의 비밀번호를 입수한 공격자로부터 HIPAA 환자 정보를 보호하고 인증정보의 유출을 방지해 SWIFT 컴플라이언스를 강화합니다.



2주 내에 SWIFT 컴플라이언스를 달성한 글로벌 은행

외부 규제 기관은 금융 기관 간 안전한 자금 이체를 위해 모든 중요 애플리케이션을 링펜싱해 SWIFT의 요구 사항을 충족하도록 Akamai의 고객사인 한 글로벌 은행에 요구했습니다. 일반적으로 이와 같은 애플리케이션에는 베어 메탈과 가상 서버를 포함해 다양한 위치에 100여 대의 서버가 배포되어야 합니다. 이 프로세스를 계획하고 실행하려면 여러 지역에 걸쳐 해당 세그먼트에 대한 VLAN(Virtual Local Area Network)을 만들어야 하기 때문에 평균적으로 이 정도 규모의 은행은 8~12개월이 소요될 수 있습니다. SWIFT 애플리케이션의 의존성을 파악하고 룰셋이 정확하고 어떤 것도 위반하지

않았는지 확인하는 작업으로 인해 일정이 더 지연됩니다. 한편 프로젝트를 위해 새로운 방화벽 장비도 구입해야 합니다. 또한, SWIFT 애플리케이션은 은행 비즈니스에 매우 중요하기 때문에 은행은 다운타임을 용납할 수 없었습니다. 전체적으로 세그멘테이션 프로젝트는 많은 사람들의 큰 노력이 필요할 것으로 예상됐습니다. 하지만 Akamai와의 협력을 통해 단 한 명의 보안 엔지니어가 약 2주만에 전체 프로세스를 완료했습니다. 네트워크를 변경할 필요가 없었으며, 은행은 애플리케이션 변경이나 다운타임을 피할 수 있었습니다.

컴플라이언스 간소화 및 가속



글로벌 은행

- SWIFT 애플리케이션 리팩싱 필요
- 베어 메탈, VMware, OpenStack 서버로 구성된 복잡한 환경



기존의 세그멘테이션

- 복잡한 인프라 전반에 걸쳐 세그먼트를 정의하기 어려움
- 애플리케이션 및 의존성에 대한 가시성 부재
- 다운타임 필요
시간: 8~12개월
인력: 최소 5명



Akamai Guardicore Segmentation

- 몇 시간 만에 SWIFT 애플리케이션 매핑 완료
- 세그멘테이션 정책의 자동 제안 및 미세 조정
- 새로운 하드웨어와 방화벽을 구매해 배포할 필요 없음
- 다운타임 없음
시간: 2주
인력: 아키텍트 1명

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

자세히 보기

Akamai Security는 성능이나 고객 경험에 영향을 주지 않으면서 모든 상호 작용 지점에서 비즈니스의 원동력이 되는 애플리케이션을 보호합니다. 글로벌 플랫폼의 규모와 위협에 대한 가시성을 활용해 고객과 협력함으로써 위협을 예방, 탐지, 방어하고 브랜드 신뢰를 쌓고 비전을 실현할 수 있도록 지원합니다. Akamai의 클라우드 컴퓨팅, 보안, 콘텐츠 전송 솔루션에 관해 자세히 알아보려면 **akamai.com** 및 **akamai.com/blog**를 확인하거나 **X**(기존의 Twitter), **LinkedIn**에서 Akamai Technologies를 팔로우하시기 바랍니다. 2024년 9월 발행.