소프트웨어 기반의 세그멘테이션

인사이드 아웃 접근 방식으로 보안의 신뢰도 향상

목차

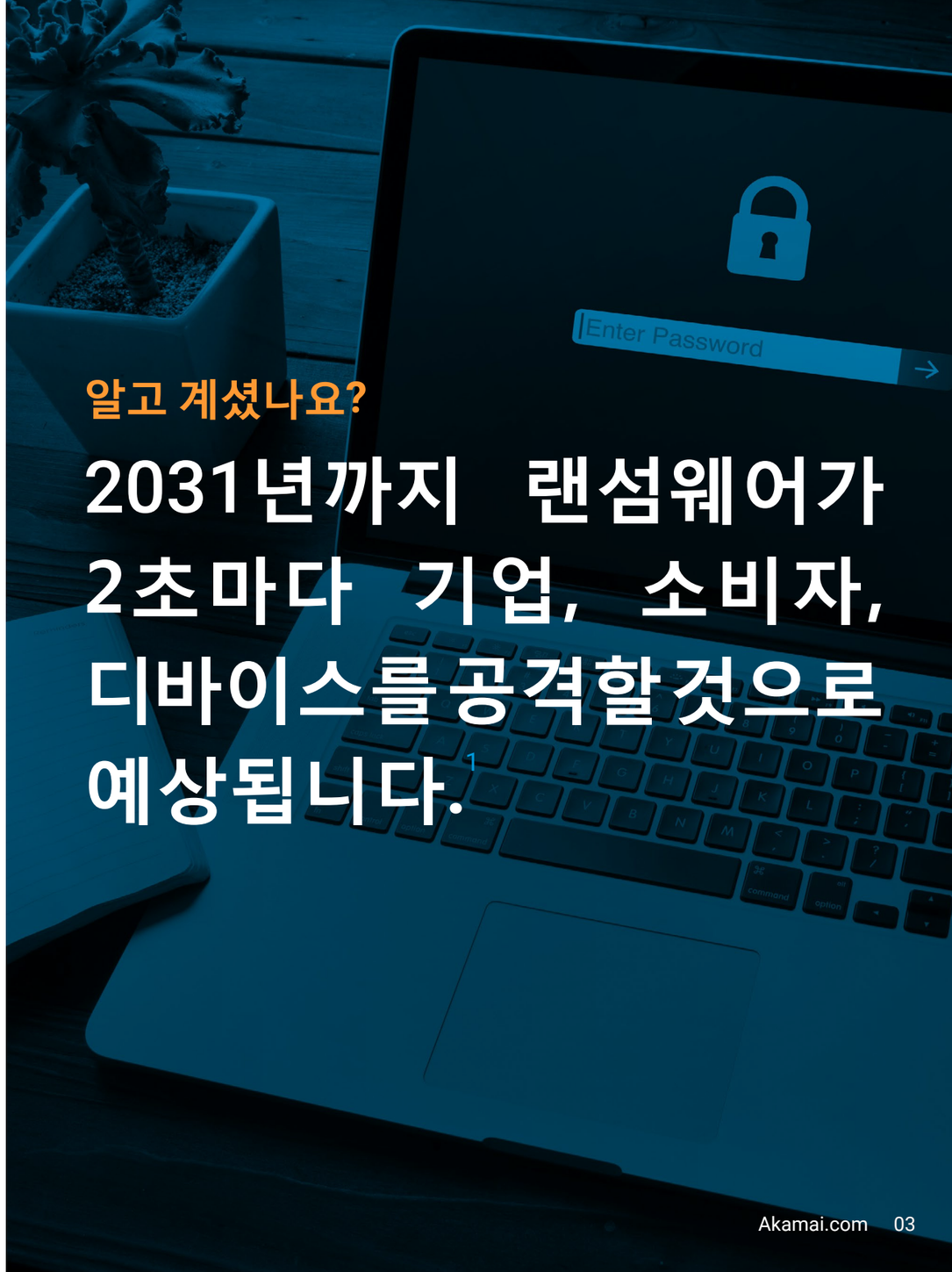
과거의 레거시 방화벽에서 벗어나기

오래된 온프레미스 방화벽 때문에 어려움을 겪고 계신다는 사실을 잘 알고 있습니다. IT 환경과 보안 요구사항은 레거시 방화벽이 처음 구축된 시대보다 훨씬 앞서 있습니다. 사이버 보안 환경도 진화해 공격 방법이 더욱 정교해졌고 사이버 범죄자도 더 많아졌습니다. 수십 년 전에 구축된 어플라이언스 아키텍처는 최신 멀웨어, 봇넷 공격, 피싱 사기, 소셜 엔지니어링, 데이터 갈취에 대응할 수 없습니다.

레거시 방화벽은 비싸고 이동성이 떨어지며 가시성이 결여되어 있는 등 문제가 많습니다. 하지만 그렇다고 해서 곧바로 사라지지는 않을 것입니다. 레거시 방화벽은 남북 트래픽을 처리하는 경계에서 중요한 기능을 담당하고 기업 주변에 단단한 벽을 제공합니다.

하지만 방화벽은 온프레미스 데이터 센터와 클라우드에서 동서 트래픽을 관리하지 못합니다.

그래서 소프트웨어 기반의 세그멘테이션이 필요합니다.



알고 계셨나요?

2031년까지 랜섬웨어가 2초마다 기업, 소비자, 디바이스를공격할것으로 예상됩니다.[1]

문제 해결!

레거시 방화벽의 3가지 문제점

1. 문제점: 가시성 부족

   데이터 흐름에 대한 가시성이 부족해 룰을 구축하고 유지 관리하기가 어렵습니다. 따라서 방화벽의 룰세트가 매우 긴 경우가 많고, 지나치게 허용적이거나 심지어 필요하지 않은 룰도 많습니다.

솔루션

비주얼 맵, 자산 분류, 애플리케이션 의존성 매핑을 정책 생성 및 관리와 통합하는 솔루션을 찾습니다.

문제 해결!

레거시 방화벽의 3가지 문제점

2. 문제점: 유지하기 어려움

애플리케이션 소유자와 방화벽 관리자는 통신해야 하는 적절한 IP 포트와 프로토콜을 거의 알지 못합니다. 따라서 방화벽 관리는 반복적인 트러블슈팅 프로세스가 됩니다.

솔루션

IP와 포트 같은 고정 네트워크 세션을 중심으로 정책을 구축하는 대신 애플리케이션이 사용하는 프로세스, 정규화된 도메인 이름(FQDN), 사용자 ID 등 유의미한 속성을 기반으로 정책을 설정합니다. 이렇게 하면 데이터 센터를 변경하거나 워크로드를 클라우드로 옮겨도 속성이 유지되고 정책이 계속 작동합니다.

문제 해결!

레거시 방화벽의 3가지 문제점

3. 문제점: 방화벽의 민첩성 부족

방화벽을 변경하려면 일반적으로 다운타임을 계획해야 합니다. 애플리케이션 소유자가 무엇을 변경해야 하는 경우 유지 관리 기간 중 변경 사항을 검토하고 구축할 때까지 일주일 이상 기다려야 할 수 있습니다.

솔루션

오늘날의 IT 기업은 변경 기간에서 벗어나 애플리케이션이 연속적으로 나타나고 업데이트되는 DevOps 모델로 이전했습니다. 애플리케이션에 사용하는 것과 동일한 DevOps 툴을 사용하는 자동화 가능한 기술 솔루션을 찾습니다. 이렇게 하면 애플리케이션이 지속적으로 진화하면서 보안 접근 방식도 함께 진화합니다.

여러분도 가능합니다

기존 방식에 대해 알아보겠습니다. 기존 방식은 복잡하고 변경 불가능합니다. 레거시 방화벽을 관리하는 기존의 접근 방식에서는 위치를 기반으로 세그멘테이션을 했는데, 위치는 쉽게 변경할 수 없습니다. 일반적으로 하드 코딩된 IP 주소를 기반으로 하거나 데이터 센터로 라우팅됩니다. 즉 방화벽으로 보호하려는 것을 물리적으로 옮겨야 합니다. 이 프로세스는 많은 리소스가 필요하고 리스크에 취약하며 느립니다. 클라우드 전환? 가시성? 적절한 보안? 잊어버리세요.

레거시 방화벽은 그대로 두면 됩니다. 심호흡하고 새로운 솔루션을 도입하세요. 소프트웨어 기반 세그멘테이션은 기존 방화벽과 함께 간편하게 구축할 수 있으며 조정이 가능합니다. 소프트웨어 기반의 세그멘테이션을 사용하면 관측한 것을 기반으로 정책을 설정하고 환경, 데이터 센터, 네트워크에 변경 사항을 적용할 수 있습니다. 워크로드와 정책은 클라우드, 데이터 센터 등 모든 곳에서 나타날 수 있습니다. 더불어 네트워크 변경이나 시스템 다운타임 없이 보안 정책을 적용하고 조정할 수 있습니다.

내부 세그먼트 드러내기

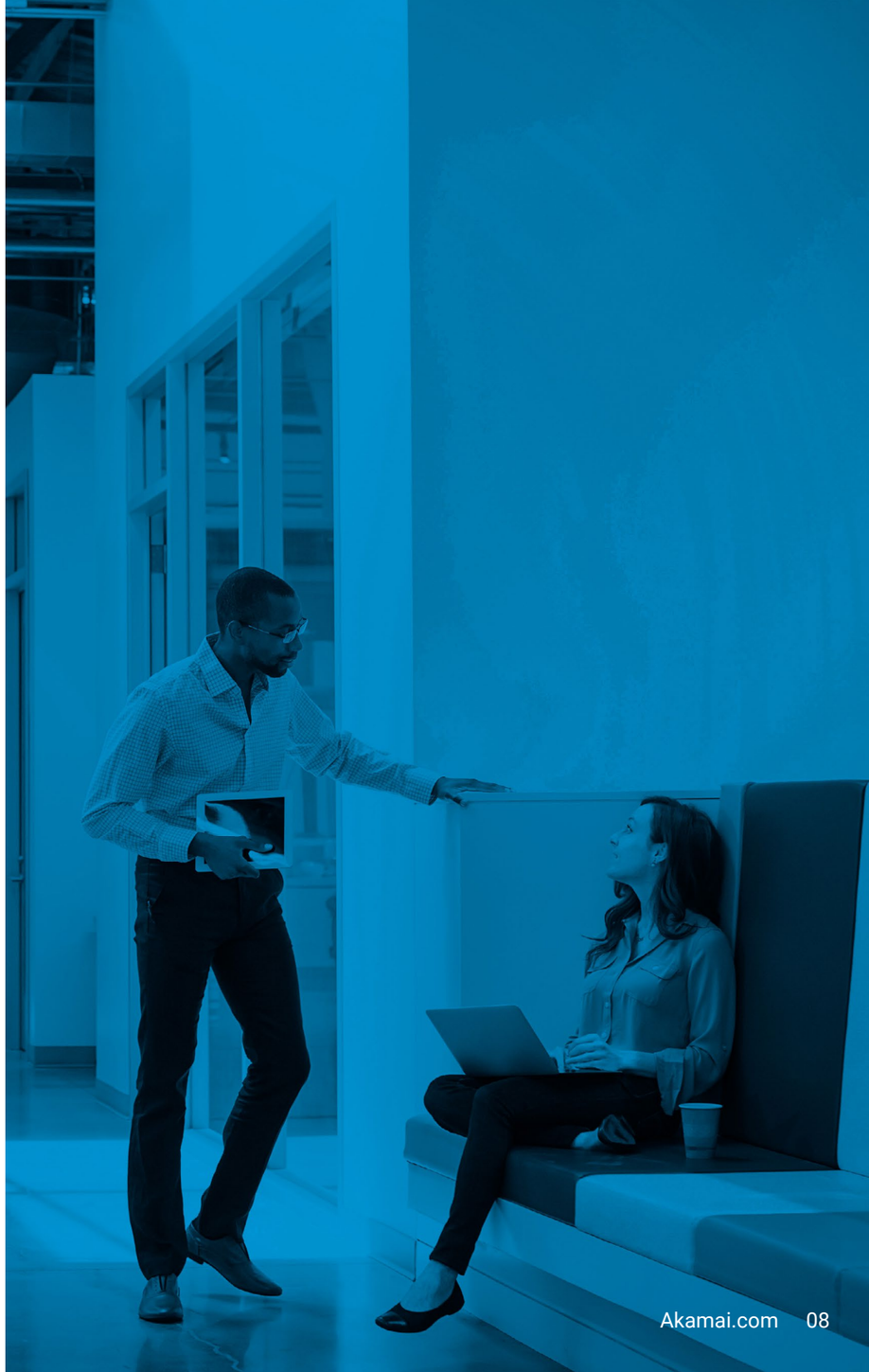
실제로 볼 수 없는 것을 신뢰하기는 어렵습니다. 보안도 마찬가지입니다. 하지만 방화벽 뒤에 보안 정책을 수립하는 것이 바로 볼 수 없는 것을 신뢰하는 것입니다. 방화벽 내부는 들여다볼 수 없습니다. 마치 건물을 보고 있지만 건물 안에 있는 사람들은 볼 수 없는 것과 같습니다.

소프트웨어 기반의 세그멘테이션은 운에 의존하지 않습니다. 완전한 분할을 통해 워크로드와 관련된 모든 활동을 완전히 파악할 수 있습니다. 환경 내부를 이해하면 계획을 수립하고 구체적인 사용 사례에 따라 의미 있고 효과적인 세그먼트로 나눌 수 있습니다.

경계 너머의 보안

레거시 방화벽은 변화에 맞춰 개발되지 않았습니다. 방화벽은 DDoS 방어와 트래픽 필터링 및 검사처럼 경계에서 중요한 역할을 하지만 네트워크 내부 보안은 방화벽으로 관리하기 어렵습니다. 왜 그럴까요? 방화벽은 초크 포인트(choke point, 관문)에 배포되는 것이 당연하기 때문에 모든 세그멘테이션 작업에는 네트워크 및 애플리케이션을 변경하고 제거해야 하는 운영상의 번거로움이 뒤따르게 됩니다. 이 작업은 지루하고 많은 리소스가 필요합니다.

소프트웨어 기반의 세그멘테이션을 사용하면 이러한 운영상의 어려움을 해결하고 엔드포인트와 경계의 너머까지 보안 체계를 이어갈 수 있습니다. 첫째, 소프트웨어 기반의 세그멘테이션은 초크 포인트 대신 분산된 방화벽 접근 방식을 사용합니다. 둘째, 워크로드 중심이기 때문에 호스트 시스템에서 데이터를 수집한 후 자산 분류에 적용하고 프로세스 수준 콘텐츠와 정책 등 보다 세밀한 방식으로 룰에 접근할 수 있습니다. 전반적으로 소프트웨어 기반의 세그멘테이션은 네트워크 내 중요 자산을 방화벽보다 탄력적이고 세밀하게 보호할 수 있으며 필요한 노력과 리소스도 적습니다.



4가지 세그멘테이션 종류

세그멘테이션은 그 어느 때보다 중요해졌습니다. 공격표면도 더 커졌습니다. 랜섬웨어 같은 정교한 공격이 유출 후 측면 이동하고 있으며 경계 너머 애플리케이션 의존성까지 고민해야 합니다. 하지만 세그멘테이션은 일회성 접근 방식이 아닙니다.

세그멘테이션의 일반적인 4가지 종류가 어떻게 다르고 왜 필요한지 알아보겠습니다.

1. 환경 세그멘테이션

이 세그멘테이션은 개발, QA, 스테이징, 프로덕션 같은 다양한 개발 환경에서 시스템을 분리합니다. 다양한 환경의 시스템을 분리해 필요한 사용자와 애플리케이션에만 접속을 제한적으로 허용하는 것이 최종 목표인 광범위한 세그멘테이션입니다. 많은 컴플라이언스 이니셔티브는 비프로덕션 시스템이 프로덕션 시스템에 접속하지 못하도록 요구합니다.

2. 네트워크 세그멘테이션

이 세그멘테이션은 네트워크를 다수의 작은 네트워크 세그먼트로 분할하는 아키텍처입니다. IT 운영자는 네트워크 세그멘테이션을 통해 네트워크 트래픽을 관리하고 성능을 강화하며 보안을 개선할 수 있습니다.

3. 마이크로세그멘테이션

이 세그멘테이션은 워크로드를 서로 고립시켜 개별적으로 보호하는 보다 세분화된 형태의 세그멘테이션입니다. 프로세스, 컨테이너, 사용자, 도메인 이름, 디바이스 같은 요소에 대한 세그멘테이션 룰을 설정할 수 있습니다. 동서 트래픽을 제어하고 측면 이동을 차단할 수 있는 우수한 접근 방식입니다.

4. ID 기반의 세그멘테이션

이 세그멘테이션은 통신 허용 여부를 결정하기 위해 사용자, 디바이스, 맥락 같은 ID를 평가하는 동적 룰을 활성화함으로써 단일 엔드포인트, 디바이스, 워크로드, 컨테이너를 보호하는 마이크로세그멘테이션의 기능을 확대합니다. ID 기반의 세그멘테이션 정책은 IP나 포트뿐만 아니라 태그, OS 종류, 애플리케이션 특성 같은 세분화된 설정을 기반으로 할 수 있습니다.

통념 vs 현실: 세그멘테이션에 대한 5가지 잘못된 통념 파헤치기

잘못된 통념 1

세그멘테이션 프로젝트는 너무 어렵고 완료하는 데 지나치게 오래 걸린다.

현실: 환경 내부 상황에 대해 명확하게 이해하고 가시성을 확보하면 몇 달이 걸리던 세그멘테이션을 몇 주 또는 며칠 내에 완료할 수 있습니다. 또한, 최신 세그멘테이션 기술은 AI를 사용해 프로세스를 가속할 수 있습니다.

잘못된 통념 2

세그멘테이션 프로젝트는 네트워크 인프라 변경과 다운타임이 필요하다.

현실: 소프트웨어 기반의 세그멘테이션은 보안을 인프라로부터 분리하므로 변경이나 다운타임 없이 기본 인프라와 독립적으로 세그멘테이션을 실행할 수 있습니다.

잘못된 통념 3

세그멘테이션은 네트워크의 정상 트래픽을 차단한다.

현실: 환경을 시각화하고 소프트웨어 기반의 세그멘테이션 정책을 사용해 정책이 비즈니스 활동에 끼치는 효과를 확인한 후 실시간으로 활성화할 수 있습니다.

잘못된 통념 4

세그멘테이션은 사용자 접속을 방해하고 불필요한 지연 시간을 유발한다.

현실: 모든 트래픽이 특정 방화벽 초크 포인트를 통과하게 하는 대신 분산 소프트웨어 기반의 세그멘테이션 정책을 사용하면 네트워크 병목 현상이 해소됩니다. 애플리케이션과 ID를 인식하는 보다 정밀한 정책으로 부주의한 사용자 접속 문제 리스크를 줄일 수 있습니다.

잘못된 통념 5

온프레미스와 클라우드에서 동일한 세그멘테이션 툴을 사용할 수 없다.

현실: 세그멘테이션 정책을 인프라에서 분리하면 데이터 센터에서 사용하는 정책을 클라우드에서도 동일하게 사용할 수 있습니다.

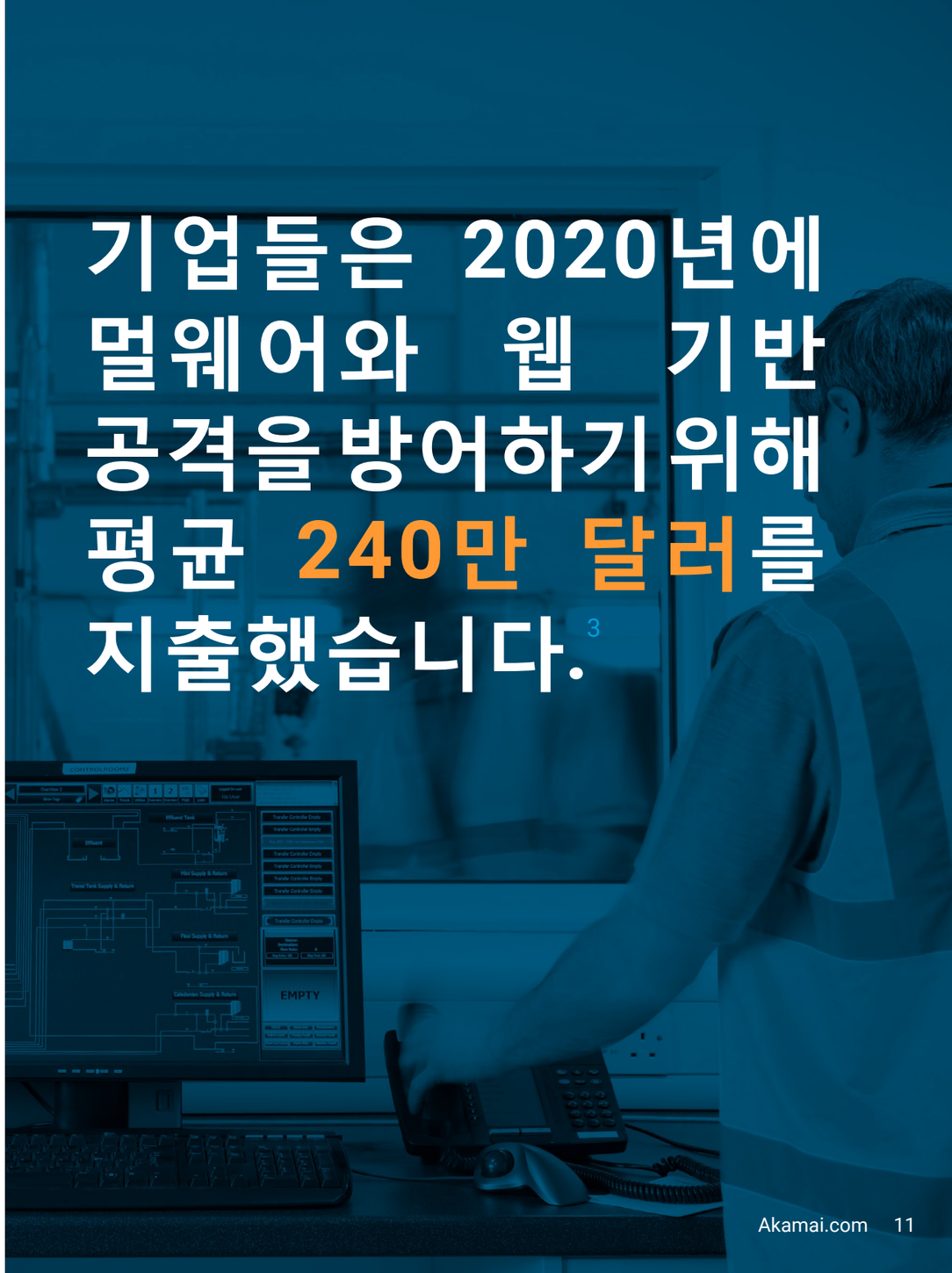
내부 리스크 감소

유출 사고는 발생하기 마련입니다. 보안 유출은 비즈니스를 방해하고, 데이터를 감염시키며, 브랜드를 훼손하고 수백만 달러의 비용을 발생시킵니다.

아직도 방화벽이 모든 공격을 막아낼 수 있다고 생각하시나요? 다시 한번 생각해 보십시오. 공격자가 네트워크, 환경 또는 데이터 센터에 침입하면 측면 이동을 통해 데이터를 유출하고, 애플리케이션 서버를 통제하거나 데이터베이스 서버에 접속하는 등의 피해를 줍니다.

사실 현재 모든 공격의 70%는 측면 이동 시도와 관련이 있습니다.[2]

방화벽은 측면 이동을 네트워크 내 정상 트래픽으로 인식하지만 소프트웨어 기반의 세그멘테이션은 이를 즉시 차단합니다. 소프트웨어 기반의 세그멘테이션은 보안 프로그램의 중요한 구성요소로, 측면 이동을 차단하고 유출이 발생해도 공격자가 환경을 탐색하기 어렵게 만듭니다. 데이터와 핵심 애플리케이션을 보호하고, 드웰 타임(dwell time, 순수 사용 시간)을 단축하며, 공격자를 탐지할 수 있습니다. 이런 접근방식은 확장성이 우수하고, 사용하기 쉬우며, 네트워크나 시스템을 변경하지 않고 신속하게 세그멘테이션을 구축할 수 있습니다.



제로 트러스트는 복잡할 필요가 없습니다

제로 트러스트는 누가 누구에게 무엇을 하고, 어떻게 하는가에 관한 것입니다. 다시 말해 네트워크 내에서 누가 무엇을 하는지 명확하게 통제하는 것입니다.

사용자에게 네트워크 내부의 모든 것에 접속할 수 있도록 허용하면 자동적으로 과도한 신뢰를 부여하게 되고 기업 전체가 위험에 놓이게 됩니다. 첫째, 직원들이 실수하면 심각한 보안 문제로 이어질 수 있습니다. 악의적인 의도를 가진 직원이 있을 수도 있습니다.

또한, VPN 네트워크와 디바이스 외부에 데이터 센터로 진입하는 엔트리 포인트가 많이 존재합니다. 예를 들어 공격자가 프로덕션 서버(SolarWinds 보안 유출의 경우), 취약한 인터넷 기반 애플리케이션, 취약한 VPN 등을 통해 네트워크 안으로 들어올 수 있습니다. 이 경우 운영자는 서버가 네트워크 내부에 있기 때문에 서버를 신뢰하지만, 공격자는 모든 것에 접속하고 제약 없이 측면으로 이동할 수 있습니다.

프로덕션 네트워크 내에서 제로 트러스트를 달성하려면 명시적으로 허용되지 않은 모든 활동을 차단해야 합니다.

이를 위해서는 IP 주소와 포트보다 더 세분화된 수준에서 속성을 확인해야 하는데 레거시 방화벽은 세분화된 수준에서 확인이 불가능합니다.

대신 소프트웨어 기반의 세그멘테이션을 사용하면 실제로 활동을 자세히 확인하며, ID를 포함하는 정밀하고 인간이 이해할 수 있는 정책을 만들 수 있습니다.

제로 트러스트 체크리스트: 확실한 제어를 위한 6가지 방법

간단하게 소개하겠습니다. 신뢰는 세그먼트의 크기에 기반해야 합니다. 중요 데이터, 자산, 애플리케이션을 보호할 때는 세그먼트가 작을수록 더 좋습니다. 운영의 복잡성 없이 제로 트러스트를 달성하는 6가지 방법을 소개합니다.

1 시각화 라벨을 사용해 민감한 데이터를 식별합니다.

2 자동화된 플로우와 의존성 매핑을 사용해 민감한 데이터의 흐름을 매핑합니다.

3 세그멘테이션 또는 마이크로세그멘테이션 정책을 신속하게 정의하는 적절한 툴을 사용해 제로 트러스트 마이크로 경계를 구축합니다.

4 실시간 모니터링 및 분석을 통해 지속적으로 제로 트러스트 생태계를 모니터링합니다.

5 보안 자동화와 오케스트레이션, API와 기술 통합을 도입합니다.

6 공격받을 경우 사용자나 세그먼트와 관계없이 사전 설정된 속성으로 머신에 대한 신뢰를 쉽게 해제할 수 있도록 사용자나 머신을 신뢰하지 않는 기능을 도입합니다.

Akamai

핵심 내용

이제 네트워크 내 보안 체계를 강화하기 위해 기존 솔루션을 어떻게 분할해야 하는지 궁금하실 것입니다.

걱정하지 마세요.

레거시 방화벽은 그대로 유지하세요. 네트워크 경계를 보호하는 데 유용합니다. 하지만 장점은 거기까지입니다.

가장 중요한 것, 즉 경계 너머에 존재하는 디지털 자산, 데이터, 애플리케이션 등 기업 인프라의 핵심은 기업의 중심에 있습니다. 아웃사이드 인 방식에서 중심을 옮기고 소프트웨어 기반의 세그멘테이션과 제로 트러스트 프레임워크를 구축하면 측면 이동을 탐지 및 차단하고, 세분화된 조정이 가능한 정책을 적용하며, 랜섬웨어 같은 사이버 공격이 네트워크를 침투하는 것을 막는 데 필요한 가시성과 제어를 확보할 수 있습니다.

세그멘테이션이 랜섬웨어, 제로 트러스트, 클라우드 보안 등을 지원하는 방법에 대해 **자세히 알아보세요**. 또는 **데모를 요청하실 수 있습니다**.

1 Cybersecurity Ventures. 2022 Who's Who In Ransomware Report. Conceal, 2022년.

2 Kellerman, Tom, Greg Foss. Global Incident Response Threat Report. VMware Carbon Black, 2020년 10월.

3 "2023 Cyber Security Statistics Trends & Data." PurpleSec, 2023년 2월 22일.