Akamai

백서

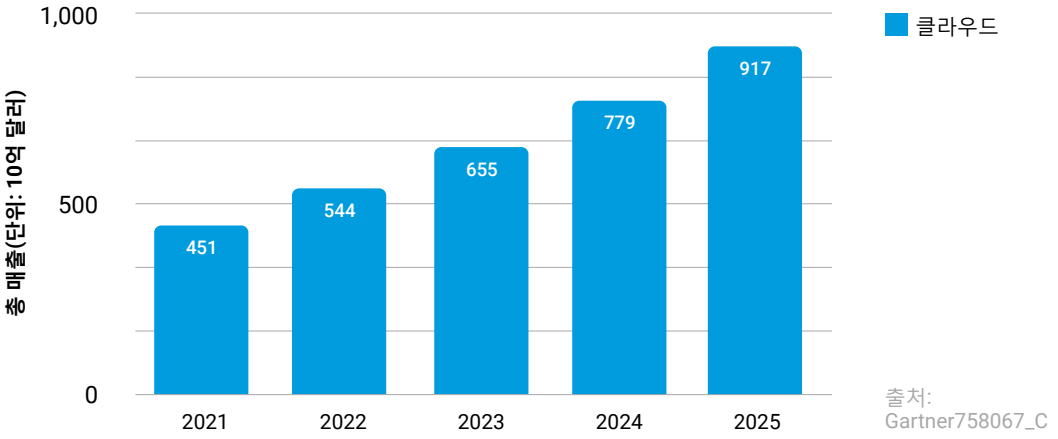
마이크로세그멘테이션으로 가는 길 확보

하이브리드 클라우드에서 마이크로세그멘테이션을 구축하기 위한 전략 가이드

클라우드의 증가 예상

막대한 양의 데이터와 데이터 처리를 클라우드(더 정확히 말하자면 멀티클라우드)로 전환하는 작업은 지난 10년간 기업 컴퓨팅에서 분명 가장 큰 변화였습니다. 더 많은 기업이 퍼블릭 클라우드(대개 퍼블릭-프라이빗 하이브리드 데이터 센터 아키텍처)로 전환하고 있습니다. 이와 함께 IaaS(Infrastructure-as-a-Service)를 활용해 민첩성 강화를 모색하고 있습니다. 기술 분석업체인 Gartner는 2025년까지 관련 서비스 시장 부문의 모든 IT 지출 중 절반 남짓이 기존 솔루션에서 퍼블릭 클라우드로 전환될 것으로 예상합니다. 이 수치는 2022년에 41%였으며, 2025년까지 퍼블릭 클라우드에 대한 총 매출 지출액은 9천억 달러를 초과할 것으로 예상됩니다.[1]

'클라우드'와 '멀티클라우드'의 구분은 사소한 일이 아닙니다. 멀티클라우드 플랫폼과 서비스 공급업체를 도입하는 기업이 증가하고 있습니다. 한 가지 사실은 분명합니다. 하나의 안전한 물리 공간으로서의 기업 데이터 센터가 이제는 사라질 것이라는 점입니다. 최신 데이터 센터는 물리 서버, 가상 머신, 온프레미스 시설의 컨테이너, 프라이빗 및 퍼블릭 클라우드 IaaS 공급업체를 결합하는 이질적인 환경 및 기술 조합이 되어가고 있습니다. 그리고 이러한 이질적인 설치는 정적이지 않습니다. 기업은 트래픽 수준과 처리 요구사항에 따라 다양한 온프레미스 및 클라우드 환경 간에 지속적으로 데이터와 워크로드를 이동하고 있습니다.



전 세계 퍼블릭 클라우드 서비스 매출 전망(단위: 10억 달러)

복잡성 증가에 따른 새로운 취약점 트리거와 공격표면 확장

클라우드 고객은 IaaS가 제공하는 민첩성, 탄력성, 확장성의 강화로 분명 혜택을 누리며, 바로 이것이 클라우드가 매력적인 이유입니다. 반면에 관리 복잡성 폭증, 환경에서 워크로드 가시성 저하, 그에 따른 사이버 보안 환경의 불투명성 등 문제가 발생합니다. 다수의 클라우드 공급업체와 협력하면 보안 팀은 매우 다양한 보안 표준과 기능을 다루어야 합니다. 온프레미스 서버와 엔드포인트를 위해 설계된 기존의 보안 툴로는 클라우드의 규모와 복잡성을 처리할 수 없습니다. IaaS 벤더사가 제공하는 보다 새로운 툴은 공급업체의 환경에서는 효과적일지 몰라도, 다수 제공업체 인프라에서는 가치가 거의 없습니다.

더군다나 오늘날과 같은 가상화와 '소프트웨어 정의'의 시대에서도 보안에 대한 관점(그리고 이에 따른 대부분의 투자)은 여전히 특히 진입 지점에서의 공격 차단 필요성에 근거를 두고 있습니다. 그렇다고 해서 경계 방어를 폄하하는 것은 아닙니다. 경계 방어는 IT 보안 스택과 여전히 밀접한 관련이 있지만, 경계가 끊임없이 변화하는 경우에는 제대로 작동하지 않는 것이 현실입니다. 데이터와 워크로드는 퍼블릭 클라우드와 프라이빗 클라우드, 온프레미스 데이터 센터 사이에서 계속 이동하고 있으며, 이에 접속하는 사용자는 적절한 보안 제어 확보 여부를 막론하고 원격 위치에서 작업하는 경우가 점점 증가하고 있습니다.

작년에 보고된 막대한 데이터 유출 횟수는 기민한 공격자들이 거의 마음대로 경계 방어를 뚫고 있음을 말해주기에 충분합니다. 그리고 내부에 침투하면 공격자들은 경계 내에 상주하는 자산이 사실상 보호되지 않는 플랫 네트워크를 찾습니다. 기업이 확보한 유연성에도 불구하고 멀티클라우드 인프라 관리 및 보안의 복잡성 증가로 인해 공격표면이 크게 확장되었습니다. 하지만 통신 제어를 거의 또는 전혀 갖추지 못한 상태에서 개별 서버는 그 자체가 저절로 공격표면이 됩니다. 결과적으로 공격자들은 가장 중요한 자산을 찾기 위해 동서 트래픽 워크로드 간에 탐지되지 않고 측면 이동에 더 많은 시간을 할애할 수 있습니다.

네트워크 세그멘테이션은 잘 이해되고 확립된 보안 관행이지만, 오늘날 워크로드가 통신하고 종종 세그먼트 간에 전환하는 클라우드 규모와 동적 IT 인프라에서는 실행하기 어려울 수 있습니다. 기업 클라우드 고객은 피해가 발생하기 전에 실시간으로 통신 흐름을 엄격하게 제어하고 데이터 센터 내부에서 위협을 탐지해 저지하기 위해서는 애플리케이션과 워크로드의 세그멘테이션을 강화할 필요가 있음을 깨닫게 되었습니다. 보안 팀이 더 많은 위협을 보다 신속하게 탐지하고 확산을 억제할 수 있도록 인프라 경계에 걸쳐 지속적으로 전체 공격표면 축소 작업을 수행함으로써 보안 복잡성을 감소시켜주는 솔루션이 필요합니다.

이것이 바로 마이크로세그멘테이션이 필요한 이유입니다.

마이크로세그멘테이션의 정의

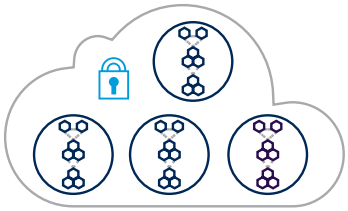
Gartner는 마이크로세그멘테이션을 '가상 데이터 센터 내에서 보안 목적으로 격리와 세그멘테이션을 구축하는 프로세스'로 정의합니다. 또한 마이크로세그멘테이션은 '기업 데이터 센터에서 고급 공격의 측면 확산 리스크를 축소하고, 기업이 온프레미스와 클라우드 기반 워크로드 전반에 걸쳐 일관된 세그멘테이션 정책을 적용하도록 지원합니다.'[2]

일반적으로 마이크로세그멘테이션은 하이브리드 데이터 센터 내 상주 위치와는 상관없이 개별 애플리케이션 또는 애플리케이션 그룹에 대한 보안 정책을 수립함으로써 작동합니다. 이러한 정책은 서로 통신할 수 있는 애플리케이션 및 구성요소와 서로 통신할 수 없는 애플리케이션 및 구성요소를 지정합니다. 따라서 모든 무단 통신 시도는 위협의 즉각적인 지표라고 할 수 있습니다. 최고의 경우에 마이크로세그멘테이션 기술은 인프라에 구애받지 않으므로, 보안 정책은 클라우드 환경 사이를 이동하면서 각각의 애플리케이션을 계속 보호할 수 있습니다.

세그멘테이션을 위한 솔루션 분야

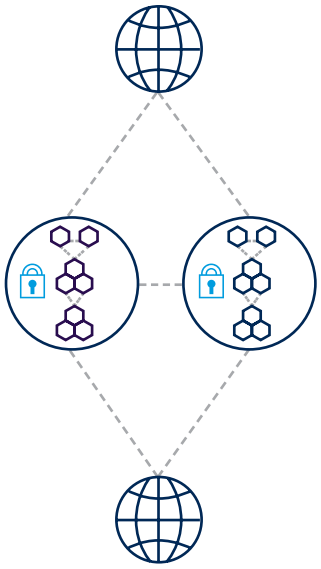
인프라 세그멘테이션

특정 인프라 내부의 안전한 애플리케이션 트래픽.



애플리케이션 세그멘테이션

애플리케이션과 외부 네트워크 사이의 안전한 트래픽



마이크로세그멘테이션

프로세스 수준 특성 등과 같은 추가 맥락을 이용해 애플리케이션 내 트래픽을 보호하는 룰

2 Gartner, "Technology Insight for Microsegmentation", 2017년 3월, "Hype Cycle for Cloud Security 2017", 2017년 7월

마이크로세그멘테이션의 사례

오늘날의 동적인 데이터센터에서 기업은 관심을 침입 방지와 접속 관리에서 워크로드와 애플리케이션 자체로 이동해야 합니다. 그리고 이러한 추세는 가속화하고 있는 것으로 보입니다. 이미 2017년에 Gartner가 주목하기 시작한 트렌드는 이렇습니다. '기존 경계 및 시그니처 기반 보호를 우회하는 최신 표적 위협으로부터의 서버 워크로드 보호에 대한 집중력이 증가했습니다. 일반적으로 이러한 공격은 그 동기가 금전적이며, 민감한 데이터나 트랜잭션에 도달하는 방법으로 서버와 애플리케이션 워크로드를 표적으로 삼습니다.'[3]

마이크로세그멘테이션의 주요 동인은 미션 크리티컬 애플리케이션과 워크로드의 보호 필요성입니다. 이는 단순히 자체 이익이나 비즈니스의 문제로 보일 수도 있지만, 상당수의 경우 보안 정책과 규제 요구사항에 따른 의무이기도 합니다.

보안 팀은 데이터센터 내부의 공격표면 확장을 억제할 수 있는 방안을 모색해야 하므로, 애플리케이션을 실행하는 서버의 취약점을 축소시켜야 합니다. 시그니처 차단이나 애플리케이션 허용 목록 등과 같은 기존의 인증 기술은 정교한 공격자들이 너무 손쉽게 무력화합니다. 마이크로세그멘테이션을 이용해 팀은 엄격하면서도 세분화된 접속 및 통신 정책을 설정해 적용할 수 있습니다. 아울러 애플리케이션 흐름에 대한 가시성을 높으며, 이를 통해 팀은 보안 체계 평가를 강화할 수 있습니다.

마이크로세그멘테이션이 필요하신가요?

다음의 몇 가지 간단한 질문에 답변하면 마이크로세그멘테이션이 필요한지 확인하실 수 있습니다.

- 귀사는 규제 산업에 종사합니까, 아니면 데이터 및 트랜잭션의 보안에 적용되는 규정을 준수해야 합니까?
- 귀사는 워크로드가 여러 클라우드에 걸쳐 있는 하이브리드 인프라를 갖추고 있습니까?
- 귀사는 가상 머신이나 컨테이너에서 애플리케이션을 실행하고 있습니까?
- 귀사는 가시성과 워크로드 제어의 저하를 느낍니까?
- 언제든 귀사는 위협이 현존하거나 공격이 귀사의 데이터센터에서 진행 중이라고 말할 수 있습니까?
- '하나의 창'을 통해 인프라 전체의 보안을 제어할 수 있습니까?

마이크로세그멘테이션에 이르는 여정의 네 가지 주요 장애 요인

보안 전문가들이 일반적으로 오늘날의 동적인 데이터 센터에서 마이크로세그멘테이션의 필요성에 동의한다면, 효율적이고 성공적인 구축이 이토록 어렵게 여겨지는 이유는 무엇일까요? 기업이 일반적으로 다음의 네 가지 주요 장애 요인에 직면하는 기존 툴을 이용해 마이크로세그멘테이션을 구축하려고 하기 때문입니다.

1. **프로세스 수준의 가시성 부족**
   기업이 직면하게 될 첫 번째 장애 요인일 수 있습니다. 보이지 않는 것을 지킬 수는 없기 때문입니다. 마이크로세그멘테이션의 본질은 개별 애플리케이션과 애플리케이션 그룹 그리고 워크플로우 프로세스의 보안입니다. 보안 팀에는 맥락 속에서의 이해를 위해 동서 트래픽 흐름에 대한 가시성이 필요합니다. 대부분의 툴은 그러한 깊이를 제공하지 않습니다.

2. **하이브리드 멀티클라우드 지원 부족**
   마이크로세그멘테이션 보안 정책은 온프레미스와 퍼블릭 클라우드 환경에서 손쉽게 확장할 수 있어야 하며, 워크로드의 이동에 따라 워크로드를 추적할 수 있어야 합니다. 특정 환경에서 작동하도록 설계된 툴은 하이브리드 환경에서는 효과적이지 못합니다.

3. **유연하지 않은 정책 엔진**
   앞서 언급했듯이 오늘날의 데이터 센터는 정적이지 않습니다. 또한 보안 조치에서는 '설정하고 잊으세요'라는 사고방식이 통하지 않습니다. 유감스럽게도 클라우드 사업자의 기존 툴은 지속적으로 룰의 범위를 지정하고 룰을 테스트하고 개선하는 데 필요한 유연성을 허용하지 않습니다. 이러한 문제는 여러 정책 툴이 필요한 하이브리드 인프라에서 심화됩니다.

4. **보완적 제어와의 통합 미지원**
   올바르게 실행된다면 마이크로세그멘테이션은 프로세스를 보호할 수 있을 뿐만 아니라 공격을 포착할 수도 있습니다. 그러나 일반적으로 단일 기능 마이크로세그멘테이션 툴에는 유출 탐지 기능이 포함되지 않아, 툴 통합과 효과적인 작동은 사용자의 몫입니다. 이와 같은 패치워크식 접근 방식은 실패 리스크가 높습니다.

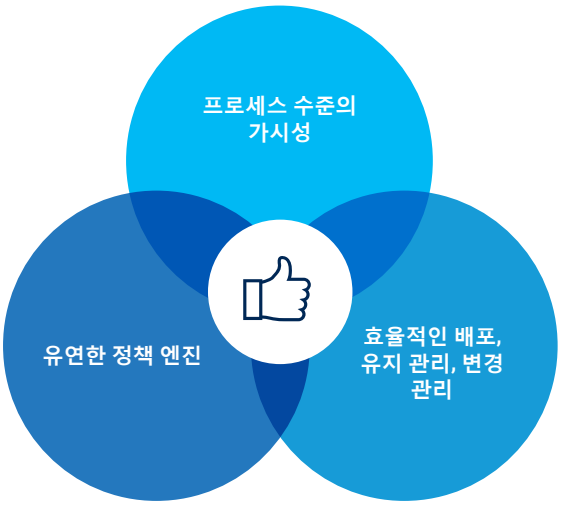
예외가 아니라 일반적으로 나타나는 프로젝트 실패

이러한 장애 요인을 고려할 때 대부분의 마이크로세그멘테이션 프로젝트가 매우 느린 구축 주기로 어려움을 겪는 경향이 있고, 비용 증가와 리소스 부담으로 인해 결국 목표 달성에 실패할 수 있다는 것은 놀라운 일이 아닙니다. 기업은 종종 세그멘테이션 대상 파악에 어려움을 겪으며(가시성 부족이 원인), 필요한 세그멘테이션의 강도를 결정하는 데 어려움을 겪습니다. 이에 따라 프로세스 수준 통신을 위한 복잡한 룰의 스프레드시트를 구축하면서 몇 달을 보낼 수도 있어, 애플리케이션 그룹화와 정책 효율화의 기회를 인식하지 못하게 됩니다. 조직이 지나치게 많은 별도의 정책을 설정해 "오버 세그멘테이션" 측면에서 실수하는 경우가 매우 흔합니다. 이는 결국 귀사가 극복하려고 노력하고 있는 과도한 보안 복잡성으로 이어집니다. 이에 대해 Gartner는 이렇게 지적했습니다. "... 세그멘테이션 프로젝트의 70% 이상이 오버 세그멘테이션으로 인해 최초 설계를 다시 아키텍처링하게 될 것입니다."[4]

오버 세그멘테이션은 애플리케이션의 속도를 저하시킬 리스크가 있고, 이는 결국 비즈니스의 속도 저하로 이어집니다. 그러나 추세가 충분한 세그멘테이션이 아닌 완전히 다른 방향으로 전환해 결국 귀사의 보안 체계를 감염시킬 가능성이 있습니다.

성공적인 마이크로세그멘테이션 여정을 위한 전략

마이크로세그멘테이션을 구축하는 길은 탄탄대로가 아니며, 환경에서 통신 흐름을 발견, 이해, 제어하면서 많은 우여곡절을 겪게 됩니다. 보안 팀은 애플리케이션을 침해하지 않고 지속적으로 새롭게 변경하고 추가하도록 보안 정책을 개발할 때 유연성이 필요합니다. 상당수의 솔루션에서 제공하는 정책 생성 엔진은 유연성이 부족하므로 보안 팀은 어쩔 수 없이 준비가 되기 전에 불완전하거나 비효율적인 룰을 구축해야 합니다.



간단히 말하자면 성공적인 구축이란 단계별 접근 방식을 통해 네 가지 주요 장애 요인을 극복하거나 우회하며 과도한 복잡성을 회피하고 언더 세그멘테이션 또는 오버 세그멘테이션의 리스크를 축소하는 구축입니다. 이는 아래의 요구사항을 충족하는 솔루션의 확보를 의미합니다.

- **프로세스 수준의 가시성:** 팀은 모든 동서 및 남북 흐름을 발견, 수집, 표준화할 수 있어야 하며, 팀에게는 애플리케이션의 자동 검색과 애플리케이션의 통신 요구사항의 이해를 구현하는 툴이 필요하고, 팀은 정책을 공유할 수 있는 자산의 레이블링과 그룹화를 촉진하는 여러 애플리케이션 속성을 필터링할 수 있어야 합니다.

- **유연한 정책 엔진:** 귀사는 대규모 세그먼트를 위한 높은 수준의 모범 사례 및 컴플라이언스 룰과 마이크로세그먼트를 위한 보다 세분화된 룰을 동시에 설계할 수 있어야 합니다. 이러한 솔루션을 이용해 알림에서 적용으로 서서히 전환할 수 있습니다. 아울러 이 솔루션을 통해 귀사는 모든 플랫폼, 디바이스, 클라우드에 걸쳐 적용할 수 있는 정책을 수립할 수 있을 것입니다.

- **효율적인 배포, 유지 관리, 변경 관리:** 시스템은 필요에 따라 룰을 손쉽게 배포하고 유지 관리하며 수정할 수 있어야 합니다. 시스템에는 내장된 유출 탐지와 인시던트 대응 기능이 포함되어야 합니다. 결국 귀사의 정책은 충분히 잘 정의되어, 실행된 각각의 새로운 애플리케이션을 위한 자동화 배포(CI/CD) 툴에 정책을 통합할 수 있을 것입니다.

이상적인 솔루션 기능

물론 시중에는 많은 마이크로세그멘테이션 툴이 있지만, 이러한 툴이 모두 마이크로세그멘테이션 여정을 손쉽게 구현하는 것은 아닙니다. 보다 원활하고 성공적인 구축을 위해서는 다음과 같은 기능을 갖춘 솔루션을 선택해야 합니다.

- 베어 메탈 서버, 가상 머신, 컨테이너에 대한 완전한 프로세스 수준의 가시성을 갖춘 **자동 애플리케이션 검색**

- **강력하고 광범위한 쿼리**를 정의해 맥락별 레이블과 개체 그룹을 생성하는 기능

- 정책을 구체화, 강화, 유지 관리하는 데 도움이 되는 지능형 룰 설계가 포함된 **유연한 정책 엔진**

- 더 많은 위협을 더 빨리 찾고 확산을 제한하는 통합된 다중 방법 **유출 탐지 기능**

- **하이브리드 인프라 지원** - 데이터 센터, 퍼블릭 및 프라이빗 클라우드 등 모든 인프라에서 작동하는 하나의 플랫폼

이러한 핵심 기능을 갖춘 솔루션은 마이크로세그멘테이션을 구축하는 가장 성공적인 경로로 안내하고, 알려진 장애 요인과 복잡성을 극복할 수 있게 하며, 보안을 희생하지 않고 유연한 하이브리드 클라우드 인프라의 모든 비즈니스 이점을 얻을 수 있도록 준비합니다.

하이브리드 데이터 센터, 멀티클라우드 플랫폼, IaaS는 '폐쇄형' 온프레미스 데이터 센터보다 더욱 큰 유연성, 확장성, 민첩성을 기업에 제공합니다. 그러나 이로 인해 애플리케이션과 워크로드(사이버 공격자들이 공격 대상으로 삼고 있는 실제 자산)의 노출과 취약점이 증가하기도 합니다. 마이크로세그멘테이션이 클라우드 워크로드 보호의 모범 사례로 널리 평가받고 있는 상황에서 기업은 올바른 구축에 어려움을 겪고 있습니다. 희소식은 한 번에 이를 구축할 필요가 없다는 사실입니다. 단계별 접근 방식과 결합된 오늘날의 첨단 솔루션을 이용하면 마이크로세그멘테이션을 구축하는 여정은 훨씬 수월해집니다. 또한 이는 기업의 가장 중요한 자산에 대한 보안 강화를 의미합니다.

akamai.com/guardicore에서 성공적인 마이크로세그멘테이션 구축에 대해 자세히 알아보세요.

1 "Gartner는 2025년까지 주요 시장 부문의 기업 IT 지출 중 절반 이상이 클라우드로 전환될 것으로 예상합니다." Gartner, 2022년 2월 9일.

2 Heiser, Jay. "Hype Cycle for Cloud Security, 2017." Gartner, 2017년 7월 17일.

3 MacDonald, Neil. "Market Guide for Cloud Workload Protection Platforms." Gartner, 2017년 3월 22일.

4 Young, Greg. "Best Practices in Network Segmentation for Security." Gartner, 2016년 7월 28일.