Akamai

백서

하이브리드 및 멀티클라우드 환경에서 워크로드 보호

하이브리드 및 멀티클라우드 환경에서 워크로드 보호

기업은 혁신, 경쟁 우위, 효율성을 추구하며 DevOps 기반 클라우드 인프라 모델로 이전하고 있습니다. 이에 따라 이례적으로 기업 IT 속도와 민첩성이 크게 향상되었습니다. 많은 기업이 컨테이너 및 서버리스 기술과 같은 새로운 배포 접근 방식과 퍼블릭 클라우드 인프라를 계속 도입하고 있습니다. 이 새로운 모델을 채택함으로써 최신 클라우드 컴퓨팅 기술은 변화를 급격히 가속화하고 있습니다. 이러한 사례에서 워크로드, 애플리케이션, 심지어 환경도 자동화하거나 자동으로 규모를 조정하거나 전환할 수 있습니다. 그리고 이를 통해 강력한 경쟁 우위를 확보할 수 있습니다.

이와 동시에 기존 데이터 센터 인프라와 같은 일부 레거시 서비스 및 시스템도 계속 사용 중입니다. 회사가 레거시 서비스와 시스템을 없애거나 최신화하는 과정에 있을 수도 있지만, 비즈니스 크리티컬 애플리케이션 및 워크플로우가 여전히 존재하기 때문에 기존 시스템을 그대로 유지할 수밖에 없는 상황입니다.

또한 기존의 보안 기법으로는 변화의 속도를 따라갈 수 없어서 새로운 하이브리드 클라우드 및 멀티클라우드 환경에서 클라우드 워크로드를 보호하는 방법이 문제로 대두되었습니다. 이러한 속도 문제 외에도, 대부분의 트래픽이 외부(북-남)에서 발생하는 것이 아니라 클라우드 또는 데이터 센터(동-서)에서 발생하는 경우 경계 기반 보안은 더 이상 효과적이지 않습니다. 또한 이러한 전환을 지원하기 위해 IT 경영진은 보안 플레이북을 재고해야 합니다.

하이브리드 및 멀티클라우드 환경에서 제대로 효과를 발휘하지 못하는 기존 보안 기술

실제로 기존 사이버 보안 모델은 IaaS(Infrastructure as a Service)를 염두에 두고 구축되지 않았습니다. 퍼블릭 클라우드에는 고유한 도전 과제를 해결하기 위한 새로운 전략이 필요합니다.

새로운 비즈니스 환경을 지원하기 위해 기업 보안이 변화해야 합니다. 기업은 비즈니스 요구사항과 민첩한 작업 방법론을 이행하기 위해 이미 큰 변화를 겪었습니다. 그러나 막대한 투자에도 불구하고 보안 수준은 한참 뒤쳐져 있습니다.

클라우드를 염두에 두지 않고 개발된 솔루션에 비용을 투자한 것이 잘못된 판단이었습니다. 현재 또는 미래의 유출을 탐지하고 방지하는 데 도움을 주지 못합니다. 그렇다면 중요한 데이터가 감염되지 않도록 하면서 퍼블릭 클라우드 서비스를 사용하고 속도와 민첩성의 이점을 누리려면 어떻게 해야 할까요?

최신 하이브리드 클라우드 데이터 센터

최신 데이터 센터의 구성, 워크로드의 세분화 증가, 개발 속도 등이 모두 빠르게 변화하고 있습니다. 일반적인 최신 하이브리드 데이터 센터는 온프레미스와 퍼블릭 클라우드 및 IaaS에서 실행되는 워크로드로 구성되며, 여러 벤더사를 이용하고 온프레미스 또는 클라우드에서 PaaS(Platform as a Service)를 활용합니다. 퍼블릭 클라우드에서 실행되는 워크로드의 양은 계속 증가하고 있습니다. 하지만 온프레미스 데이터 센터가 곧바로 사라지지는 않을 것입니다. 대표적인 사례로 기술 경영진을 대상으로 실시한 최근 설문 조사에 따르면, 오늘날 IT 환경에서 약 59%가 '일부는 클라우드, 대부분은 온프레미스'에서 워크로드를 실행하며, '대부분은 클라우드, 일부만 온프레미스'에서 실행하는 회사는 34%로 나타났습니다. '전체 클라우드'는 7%에 불과했지만 이 수치는 앞으로 크게 증가할 것으로 예상됩니다.[1]

우리가 알 수 있듯이 기업은 점점 더 많이 DevOps 사례를 도입하여 민첩성을 개선하고 있습니다. 네이티브 클라우드 서비스와 서버리스 기술은 그 어느 때보다도 쉽게 구축할 수 있습니다. 클라우드에서 컨테이너, VM 및 서버리스 워크로드를 함께 사용하면 전략적 관점에서 봤을 때 보다 비용 효과적이고 전환을 더 잘 뒷받침할 수 있습니다.

이제 이러한 하이브리드 클라우드 패러다임에 맞는 보안 솔루션이 필요합니다. 비즈니스는 테스트, 구축 및 계획에서부터 새로운 기능의 모니터링, 운영, 배포 및 릴리스에 이르기까지 모든 DevOps 프로세스 단계에서 보안 문제를 해결해야 합니다. 클라우드로의 전환이 성공의 장애물이 되어서는 안 됩니다.

새로운 클라우드 기술 사용의 걸림돌이 되고 있는 분산된 워크로드에 대한 적절하지 못한 보안

오늘날 많은 기업은 온프레미스, 코로케이션 및 여러 퍼블릭 클라우드/IaaS 플랫폼에 분산된 워크로드를 보호해야 합니다. 기존의 온프레미스 네트워크 보안 모델로는 이러한 워크로드를 안전하게 유지하기 어렵습니다.

새로운 클라우드 기술을 보호하기 위해 새로운 클라우드 기반 툴 및 기술을 배포하려고 하면 문제가 더욱 복잡해집니다. 비즈니스가 서로 다른 여러 환경에서 서로 다른 보안 제어를 적용하려고 하고 적절한 가시성을 확보하지 않은 상태에서 이러한 제어 기능을 배포해 리스크를 초래하면 복잡성은 배가됩니다.

다시 말해 기업의 역동성, 민첩성, 속도 및 혁신을 지원하는 클라우드로 인해 많은 기업이 이제 리스크에 처하게 된 것입니다. 관련 클라우드 중심의 보안 툴이 부족하기 때문에 기업은 사각지대와 더 많은 과제를 유발하지 않으면서 이러한 새로운 기술을 수용하는 능력이 제한됩니다.

그래서 적응형 워크로드 보호 기능이 필요합니다.

IaaS로 전환함에 따라 적응형 워크로드 보호의 필요성 대두

수명이 짧은 세분화된 워크로드를 보호하는 가장 좋은 방법은 워크로드를 사용하는 즉시 동적 애플리케이션 보호 기능을 적용하는 것입니다. 퍼블릭 클라우드 인프라를 이용하는 경우 워크로드 중심의 솔루션에서는 기존의 네트워크 보안 모델보다 보안 정책을 적용하는 방법이 훨씬 더 간단합니다.

플랫폼에 구애 받지 않는 워크로드 중심 보안 솔루션을 지원하는 클라우드 워크로드 보호 플랫폼

기본 인프라에 관계없이 정책이 워크로드를 따르기 때문에 전체 하이브리드 클라우드 데이터 센터 환경의 모든 워크로드에 이 모델을 적용할 수 있습니다. 그 결과 모든 플랫폼에서 일관된 보안 제어 방식을 구현할 수 있습니다.

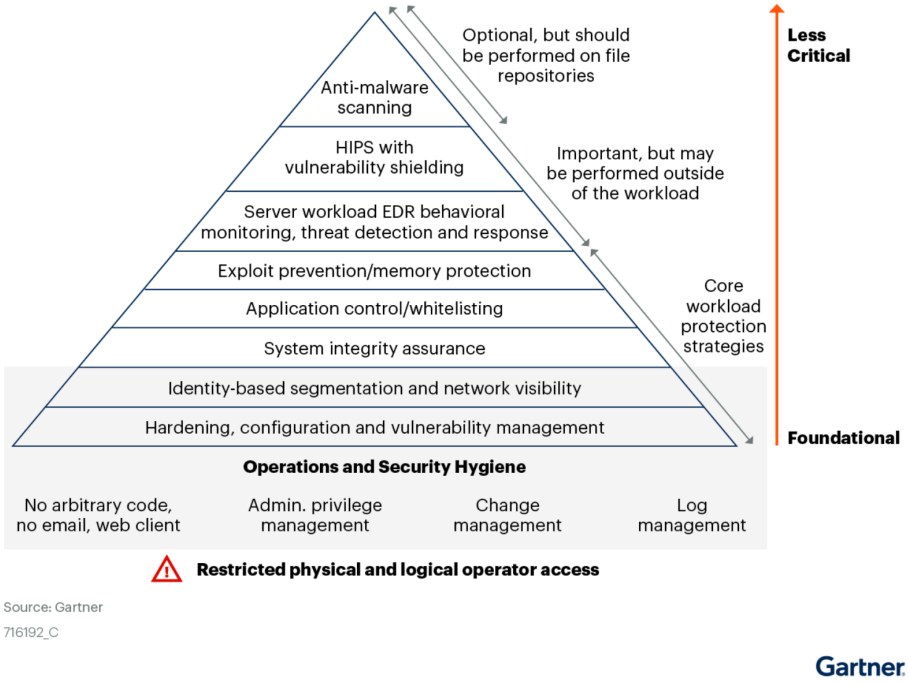
네이티브 클라우드 보안 툴이 있지만 적응형 클라우드 워크로드 보호 플랫폼(CWPP)은 프로세스, 사용자 및 정규화된 도메인 이름 수준에서 보다 포괄적이고 세분화된 제어를 제공합니다. 또한 여러 클라우드 공급업체 및 온프레미스에서 작동하면서 VM, 컨테이너 및 서버리스 워크로드에 대해 더욱 강력하고 포괄적인 보호 기능을 제공합니다.

실행 가능한 핵심 워크로드 보호 전략: Gartner의 클라우드 워크로드 보호 가이드라인에 제어 매핑

Gartner의 업계 전문가가 클라우드 워크로드 보호에 대해 가장 널리 보급된 가이드라인을 하나 작성했습니다. Gartner에 따르면 클라우드 워크로드를 보호할 때 명확한 제어 계층 구조가 존재합니다.

아래 피라미드는 근본적인 기능에서 덜 중요한 기능으로 올라가며, Gartner가 핵심으로 인지한 전략과 중요하지만 선택적인 전략을 보여줍니다. 이상적이라면 각 워크로드에 이러한 단계를 포함함으로써 클라우드의 모든 동작에 대한 보안을 구축하는 것이 좋습니다.

워크로드 보호 제어의 리스크 기반 계층 구조[2]



Gartner의 클라우드 워크로드 보호 가이드라인에서 기업에 명확한 보안 제어 계층 구조 제시

이제 하이브리드 또는 멀티클라우드 데이터 센터 보호 프로그램에 이러한 전략을 통합하는 최선의 방법을 파악하는 데 도움을 주기 위해 Akamai 솔루션이 충족하는 핵심 전략을 자세히 설명합니다.

- **보안 강화, 설정 및 취약점 관리**
  Gartner에 따르면 가장 근본적인 워크로드 보호 전략은 리스크를 줄이기 위해 시스템 및 설정을 적절히 구성하는 것입니다. 취약점 관리 툴은 공격 기법의 수동 제거에서 더 나아가 이 프로세스를 자동화합니다. 이후에 악의적인 의도에 취약할 수 있는 소프트웨어 문제를 찾아 해결할 수 있습니다.

- **ID 기반의 세그먼테이션 및 네트워크 가시성**
  Gartner는 클라우드 보호의 핵심 전략으로 네트워크 세그멘테이션 및 가시성을 강조합니다. 대부분의 기업은 온프레미스에서 차세대 방화벽을 사용하고 있으며 아직도 다수가 클라우드로 전환할 때 보안성이 낮은 솔루션을 채택합니다.

  보안팀은 차세대 방화벽이 클라우드 보호에 충분하지 않다는 점을 알고 있지만, 동적 하이브리드 데이터 센터 환경에서 이기종 인사이트 또는 제어를 확보하는 방법을 알지 못합니다. 이제 올바른 방법을 잠시 살펴보겠습니다.

  첫째, 가시성을 확보합니다. 모든 관계자가 즉시 자동으로 동일한 페이지에 표시되므로 신속하게 가시성을 확보하면 가치 실현 시간을 단축할 수 있습니다.

  네이티브 클라우드 툴은 스냅샷 맵 또는 텍스트 로그를 제공할 수 있지만 일반적으로 복잡하거나 불완전하거나 충분하지 않습니다. 최고의 솔루션은 네트워크의 모든 애플리케이션, 트래픽 및 의존성을 자동으로 검색할 수 있어야 합니다. 그래야만 기업이 하이브리드 방식으로 분산되어 있어도 전체 IT 생태계를 한 눈에 파악할 수 있습니다.

  또한 데이터 센터의 실제 상황에 대한 강력한 인사이트와 함께 강력한 맥락 정보를 솔루션에 포함해야 합니다. 대규모로 보안 운영 및 문의를 관리하려는 기업의 경우 개별 프로세스 및 서버 통신을 드릴다운하는 기능을 통해 모든 흐름에서 이 맥락을 포함해야 합니다. 그러면 정책 생성을 지원하는 데이터 중심의 의사 결정이 가능해집니다.

  가시성을 확보하고 맥락을 수립한 후에는 비즈니스의 모범 사례에 해당하는 세그멘테이션 룰을 생성합니다. 예를 들어 프로덕션 및 개발 환경을 분리하거나 고객 데이터를 격리해 컴플라이언스를 입증할 수 있습니다. 또한 보다 정밀한 마이크로세그멘테이션 정책을 개발해 특정 비즈니스 맥락에 맞는 방식으로 심층적인 보안 및 제어를 제공할 수 있습니다.

- **애플리케이션 제어 및 허용 목록 관리**
  보안팀이 정책을 설정하고 모든 곳에서 보안을 확신하면 모든 단계에서 더 간편하고 안전하게 클라우드로 전환할 수 있습니다.

  포트 및 IP에만 의존하는 방식은 전체 클라우드 워크로드 보호에 필요한 수준의 가시성을 확보할 수 없습니다. 강력한 마이크로세그멘테이션의 핵심은 애플리케이션 구성요소 간의 트래픽을 엄격하게 제어하는 데 있습니다. 최고의 기술은 해시 값, 체크섬, 전체 경로, 레졸루션, ID 저장소 인증과 같은 세부 정보를 사용해 애플리케이션 프로세스, 사용자 및 정규화된 도메인 이름에 대한 정밀한 가시성과 제어도 지원합니다.

  다음은 애플리케이션 제어를 강화할 수 있는 몇 가지 추가 기능입니다.

  - 동일한 애플리케이션 클러스터 내에서도 클라우드에서의 측면 이동을 제한할 수 있는 마이크로세그멘테이션
  - 보안 강화로 이어지는 단일 창 접근 방식
  - 권한이 없는 애플리케이션이나 트래픽을 차단하고 중요한 연결을 방해 받지 않고 실행할 수 있는 허용 목록과 거부 목록 모델을 모두 생성하는 기능

- **악용 방지 및 메모리 보호**
  Gartner의 CWPP 가이드에서 설명하는 마지막 핵심 서버 보호 전략은 악용 방지입니다. 유출 탐지 및 대응 기능을 제공하는 마이크로세그멘테이션 보안 툴을 찾아야 합니다. 그러면 중복된 툴을 대체하고 데이터 센터의 복잡성을 줄일 수 있습니다.

  또한 앞서 언급한 바와 같이 가시성과 매핑은 기본입니다. 전체 네트워크에 대한 완벽한 맵을 생성한 후에는 패치되지 않은 취약점이나 비정상적인 악성 통신을 쉽게 확인할 수 있습니다. 기업이 정상적인 트래픽에 대한 기준을 수립하면 승인되지 않은 움직임을 쉽게 확인할 수 있습니다.

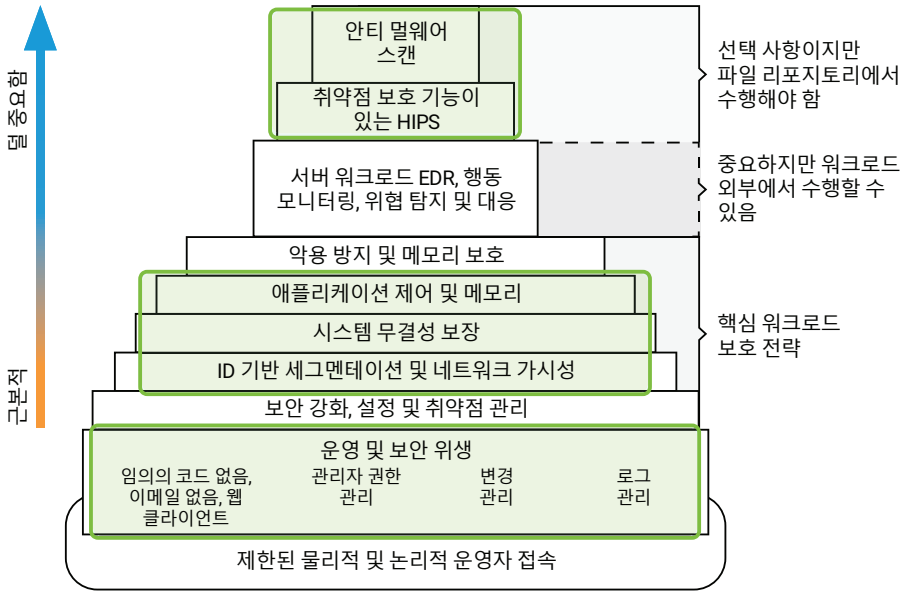
기타 중요한 보호 전략

위에서 언급한 핵심 서버 전략은 클라우드 보안의 기본입니다. 이와 함께 Gartner는 서버 워크로드 엔드포인트 탐지 및 대응(EDR), 행동 모니터링, 위협 탐지 및 대응(TDR) 등 하이브리드 또는 멀티클라우드 환경에서 보안을 강화할 수 있는 다른 여러 가지 전략도 소개합니다.

EDR, 행동 모니터링 및 TDR은 유출 탐지 및 인시던트 대응의 중요한 부분입니다. 이러한 보안 측면을 해결하려면 평판 분석을 포함하는 솔루션을 찾아야 합니다. 그러면 공격에 대한 추가 정보를 탐지할 수 있을 뿐 아니라 공격자가 공격을 중단하게 만들 수 있는 고급 디셉션 기능을 제공할 수 있습니다. 이러한 방식으로 정책 및 보안 절차를 한층 더 강화할 수 있습니다.

과거 이벤트에 대한 정보를 설정하려면 가시성 데이터가 필요할 수 있습니다. 최고의 공급업체는 몇 개월 동안 데이터를 저장하므로 사용자는 특정 애플리케이션, 프로세스 및 기간에 집중할 수 있습니다. 보안팀은 이 데이터를 포렌식 조사 및 향상된 인시던트 대응에 사용할 수도 있습니다.

Akamai Guardicore Segmentation: CWPP 계층 구조에서 하이브리드 클라우드 워크로드 보호



강조 표시된 영역은 당사의 솔루션이 CWPP 요구사항을 충족시키는 위치를 보여줍니다.

Akamai Guardicore Segmentation은 네이티브 클라우드 보안 툴에 내재된 격차를 해소함으로써 CWPP에 명시된 여러 기본 원칙을 충족할 수 있습니다. 또한 이 솔루션은 하이브리드 및 멀티클라우드 데이터 센터에서 가시성, 정책 생성 및 적용을 지능적으로 지원합니다.

Akamai 솔루션은 전체 데이터 센터에 대한 보기를 제공하는 단일 창을 통해 심층적인 가시성을 제공합니다. 하이브리드 데이터 센터에 대한 전반적인 가시성을 확보하면 애플리케이션 의존성 및 정책이 네트워크에 미치는 영향을 완전히 이해할 수 있습니다. 가시성은 클라우드 전환에 중대한 영향을 미치므로 고객은 네이티브 시각화 툴을 사용할 때보다 훨씬 빠르게 클라우드로 전환할 수 있습니다.

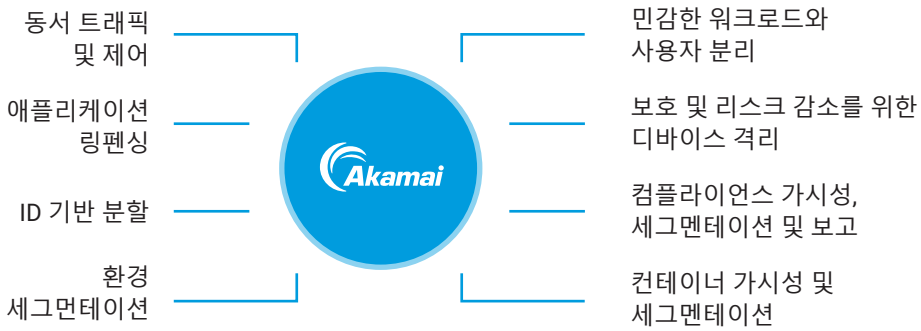
이러한 심층적인 가시성을 바탕으로 다음 작업을 지원할 수 있습니다.

- 클라우드에서 네트워킹을 위한 할 일 목록 작성
- 모든 인프라 및 애플리케이션 의존성에서 신속한 애플리케이션 탐지 - 성공적인 전환을 위한 핵심 기능
- 사전에 인프라 및 운영 비용 파악
- 전환 계획 단계에서 리스크를 줄이도록 최고의 정책 생성에 대한 인사이트 확보
- 클라우드에 대한 비즈니스 목표를 달성할 수 있는 가장 간단하고 가장 안전한 최단 경로 활용

Akamai는 포괄적인 가시성과 함께 모든 통신과 흐름에 대한 맥락을 제공하므로 오류와 전체적인

Akamai Guardicore Segmentation의 심층적인 맥락 기반 가시성으로 고객의 환경을 신속하고 완벽하게 파악

복잡성을 줄일 수 있습니다. 정보를 그룹화하고 필터링해 관계자가 맵을 쉽게 판독할 수 있도록 지원함으로써 필요한 정확한 정보를 쉽게 제공할 수 있습니다. 이러한 맥락 중심의 보기를 사용하면 써드파티 벤더사 및 정책 작성자에 대한 의존성이 줄어들게 되므로 환경을 신속하게 파악함으로써 적용 가능한 정책을 생성, 구체화 또는 수정할 수 있습니다.



Akamai Guardicore Segmentation 사용 사례

Akamai의 솔루션이 제공하는 기타 주요 기능은 다음과 같습니다.

- 프로세스 및 서비스 수준 정책: FTP 또는 Spark와 같은 동적 프로토콜을 처리할 때 보다 간단하고 강력한 보안 지원
- ID 기반 마이크로세그멘테이션 정책 - 연결을 생성하는 사용자에 따라 연결 적용
- 정규화된 도메인 이름 기반 정책: 동적 IP 주소를 사용하는 자동 확장 리소스에 도달 가능
- 기존 퍼블릭 클라우드 태그를 레이블로 사용: 하이브리드 또는 멀티클라우드 데이터 센터의 시각화 간소화
- 관찰된 트래픽으로부터 정책 자동 구축: 마이크로세그멘테이션 여정을 시작할 때 빠르고 전문적인 가이드 확보

플랫폼 및 인프라에 구애 받지 않고 전체 인프라에 대한 가시성과 정책 적용을 관리하는 Akamai 솔루션

하이브리드 데이터 센터를 보호하려는 궁극적인 목표는 복잡성을 줄이는 것입니다. 이러한 요구를 충족하기 위해 Akamai Guardicore Segmentation은 플랫폼 및 인프라에 구애 받지 않으며, 어디서든 워크로드를 따르는 전체 애플리케이션과 정책을 한눈에 파악할 수 있습니다. 각 룰은 vCenter 및 퍼블릭 클라우드(AWS, Azure, GCP)에서 베어 메탈 서버 및 컨테이너에 이르기까지 모든 워크로드에 적용됩니다.

복잡성을 줄이면 보안 체계가 강화될 뿐 아니라 IT 및 보안 워크로드도 완화됩니다. 클라우드 기반 보안 그룹을 사용하는 경우 각 벤더사에 대한 네이티브 클라우드 전문가가 필요합니다. 반면 전체 인프라에 대한 가시성 및 정책 적용을 관리하는 단일 보안 솔루션을 사용하면 단일 기술에 대해 인증된 사용자만 있으면 됩니다.

미래 지향적인 클라우드 워크로드 보호 플랫폼

애자일 방법론과 DevOps의 한 가지 기본적인 장점은 신속하고 빠르게 장애를 일으키고 '넥스트 빅 싱'(next big thing)으로 간편하게 전환하는 능력입니다. 하지만 다소 역설적이게도 서로 다른 클라우드 공급업체 사이에서 워크로드를 전환하면 속도가 엄청나게 느려질 수 있습니다. 보안 유지도 어려울 수 있습니다.

선택지를 열어 둘 수 있어야 합니다. 멀티클라우드 인프라로 전환하거나 워크로드를 새로운 클라우드 공급업체로 전환하려는 경우에도 보안에 부정적인 영향을 미치지 않아야 하며, 보안이 전환의 장애물이 되어서도 안 됩니다.

Akamai Guardicore Segmentation을 사용하면 비즈니스 속도에 맞춰 유연하게 기능하면서 보안 정책을 그대로 유지하고 워크로드를 전환할 수 있습니다. DevOps 프로세스나 민첩성을 저해하지 않으며 모든 단계에서 재설정이 필요하지도 않습니다. 대신, 신뢰할 수 있는 클라우드 워크로드 보호 플랫폼의 기반을 제공하므로 하이브리드 또는 멀티클라우드 데이터 센터의 보안을 유지할 수 있습니다.

Akamai Guardicore Segmentation은 클라우드로의 전환과 클라우드 간 전환을 안전하게 지원하며, 맥락 정보와 함께 탁월한 가시성을 제공합니다. Akamai 솔루션을 사용하면 프로세스 및 사용자 수준까지 정책을 적용하고 어디서든 워크로드를 추적할 수 있습니다.

이제 DevOps 프로세스의 모든 단계에서 보안을 제공해 민첩성을 높이고 비즈니스를 지원할 수 있습니다. 기업은 보안을 핵심으로 유지하면서 최첨단 클라우드 기능을 도입할 수 있습니다.

업계 최고의 마이크로세그멘테이션을 통해 클라우드 환경을 보호하는 방법에 대해 자세히 알아보세요. 지금 akamai.com/guardicore를 방문하세요.

1 2022년. Foundry (formerly IDG) Cloud Computing Study.

2 Market Guide for Cloud Workload Protection Platforms, 작성자: Gartner 분석가 Neil MacDonald 및 Tom Crow, 2020년 4월 14일 발행