Akamai

보고서

컨테이너의 이점 실현

중요 자산 및 애플리케이션 세그멘테이션의 간소화 및 가속

서론

컨테이너화는 클라우드 및 하이브리드 환경에서 애플리케이션 배포를 위한 솔루션으로 급부상했으며, 컨테이너도 빠르게 확산되고 있습니다. Gartner는 2026년까지 글로벌 기업의 90%(2021년 기준, 40%)가 프로덕션에서 컨테이너화된 애플리케이션을 실행할 것으로 전망합니다.[1] 그리고 Capital One에 대한 Forrester 연구에 따르면, **설문조사에 참여한 IT 리더 중 86%가 더 많은 애플리케이션에서 컨테이너 사용 확장을 우선시**하는 것으로 나타났습니다.[2]

> Gartner는 2026년까지 글로벌 기업의 90%(2021년 기준, 40%)가 프로덕션에서 컨테이너화된 애플리케이션을 실행할 것으로 전망합니다

물론 IT 환경의 보안을 책임지는 사람에게는 이러한 모든 것이 특히 신속한 도입과 확장을 우선시하는 DevOps 모델에서 컨테이너 배포 속도를 맞추어야 한다는 부담을 가중시킵니다. 수많은 전문 컨테이너 보안 솔루션이 나오고 있지만 이러한 플랫폼별 컨테이너 전용 엔터티는 기업 데이터 센터 전체를 감당하지 못하며, 복잡성과 관리 오버헤드를 가중시켜 보안 팀의 업무를 더욱 복잡하게 만듭니다. 그래서 컨테이너를 포함해 온프레미스, 클라우드, 하이브리드 환경에서 실행되는 모든 애플리케이션과 기술 전반에서 일관적으로 작동하는 포괄적인 단일 보안 솔루션이 필요한 것입니다.

솔루션을 자세히 알아보기 전에 컨테이너가 부각된 현상, 이러한 현상의 동인, 보안 관점에서의 영향을 간단히 살펴보겠습니다.

현시점의 과제: 도입을 촉진하는 비즈니스 요구사항

컨테이너로의 전환과 예상되는 도입 증가는 기업의 IT 부서에 부가되는 비즈니스 요구사항에서 비롯될 수 있습니다. 오늘날의 기업은 경쟁 위협과 시장 기회에 대응해 더 빠르고 민첩하게 움직이고자 합니다. 이들에게겐 혁신을 지원하고 시장 출시 시간을 단축하는 솔루션이 필요합니다. 기업은 또한 지속적으로 효율성 개선을 모색하고 있습니다. 상호 연결성이 점차 강화되는 환경에서 기업은 공급업체와 벤더사, 비즈니스 파트너, 특히 고객과 디지털 방식으로 보다 쉽게 비즈니스를 수행하길 원합니다.

이것이 기업 IT가 클라우드로 전환하거나 보다 정확하게 온프레미스 및 클라우드 하이브리드 모델로 전환하는 주된 이유입니다. 또한 DevOps 트렌드의 이면에 자리한 주요 동인이기도 합니다. DevOps 트렌드는 아이디어에서 구축까지 제약 조건을 없애고 자동화를 활용하며 자동 확장을 통해 보다 신속하게 애플리케이션을 프로덕션에 배치함으로써 중요 애플리케이션의 더욱 신속한 배포를 추구합니다.

> **"기업은 프로덕션에서 컨테이너를 운영하는 데 필요한 노력을 과소평가하곤 합니다."**
>
> **— Gartner**

이 모든 것이 IT 부서에서 컨테이너화를 도입하는 이유를 설명해 줍니다. 컨테이너는 가상 머신에 비해 훨씬 쉽고 빠르게 실행할 수 있어 지연 시간이 거의 없이 적시에 제공할 수 있기 때문에 팀은 '서버가 아닌 서비스 회전'에 집중할 수 있습니다. 컨테이너의 주요 장점은 오늘날 동적 데이터 센터 환경에서의 이식성입니다. 컨테이너를 이용하면 온프레미스 설비 사이에서 멀티 클라우드 인스턴스로 애플리케이션을 쉽게 전환할 수 있습니다. 이러한 기능은 쿠버네티스('K8s')를 통한 컨테이너 오케스트레이션을 통해 더욱 강화되어 팀이 여러 환경에서 컨테이너화된 많은 애플리케이션을 배포하고 관리하도록 지원합니다. 오케스트레이션은 점차 컨테이너 구축 및 관리의 모범 사례로 인식되고 있습니다.

즉, IT는 컨테이너를 사용할 경우 다른 기술에 비해 더 저렴한 총 소유 비용으로 속도, 자동화, 안정성, 가용성에 대한 비즈니스 요구사항에 보다 효과적으로 대응할 수 있습니다. 그러나 구축 노력과 관련하여 단점이 없는 것은 아닙니다. 컨테이너화 모범 사례에 대한 2019년 Gartner 보고서에 따르면, '기업은 프로덕션에서 컨테이너를 운영하는 데 필요한 노력을 과소평가하곤 합니다.'[3] 컨테이너화의 높은 인기에도 불구하고 이 기술은 아직 초기 단계이며 안전한 배포를 위한 모범 사례가 완전히 통합되지 않았습니다. Red Hat의 2022 State of Kubernetes Security 보고서에 따르면, '컨테이너 도입과 관련해 가장 큰 문제는 [여전히] 보안이며, 보안 문제로 인해 프로덕션에 애플리케이션 배포가 계속 지연되고 있습니다.'[4] 기업은 분명 사이버 보안을 반드시 포함하는 구축 전략 없이는 컨테이너의 잠재적인 이점을 모두 얻을 수 없습니다.

> Red Hat의 2022 State of Kubernetes Security 보고서에 따르면 '**컨테이너 도입과 관련해 가장 큰 문제는 [여전히] 보안이며**, 보안 문제로 인해 프로덕션에 애플리케이션 배포가 계속 지연되고 있습니다.'

이것은 보안 팀에 무엇을 의미할까요?

Gartner의 모범 사례 보고서에 따르면 '보안은 나중으로 미룰 수 있는 것이 아니라, DevOps 프로세스에 통합해야 합니다.' 하지만 현실은 그렇지 않습니다. 보안 팀이 성급하게 컨테이너화를 구축하다 보면 불가능의 펜로즈 삼각형(Akamai에서 클라인(Klein)과 하워드(Howard)의 불가능한 삼각형이라고도 함)이라고 하는 '불가능한 삼각형' 착시 현상에 빠지기도 합니다.

> 레거시 보안 솔루션은 오늘날 기업에 적합하지 않습니다. 'DevOps' 접근 방식에 완벽하게 맞는 빠르고 적응력이 뛰어난 동적 보안 솔루션이 필요합니다.

삼각형의 맨 위 꼭짓점이 다른 두 꼭짓점보다 더 멀리 있듯이, 보안은 비즈니스 요구사항과 이를 충족하려는 IT 이니셔티브에 한참 뒤처져 있는 것 같습니다. 그러나 이 삼각형이 착시 현상에 불과한 것처럼 보안 솔루션은 실제 보기보다 더 가깝습니다. 팀은 과거에 사용하던 번거로운 레거시 솔루션을 넘어 오늘날 기업 IT가 제공하는 방식에 부합하고 'DevSecOps' 접근 방식에 완벽하게 맞는 솔루션을 살펴봐야 합니다. 즉, 빠르고 적응력이 뛰어나며 동적이고 그 자체로 DevOps 플레이북 접근 방식을 사용하는 솔루션이 필요합니다. 가장 중요한 점은 솔루션이 구축과 관리를 간소화하기 위해 기본 운영 체제와 플랫폼에서 분리되어야 한다는 것입니다.

클라인과 하워드의 불가능한 삼각형

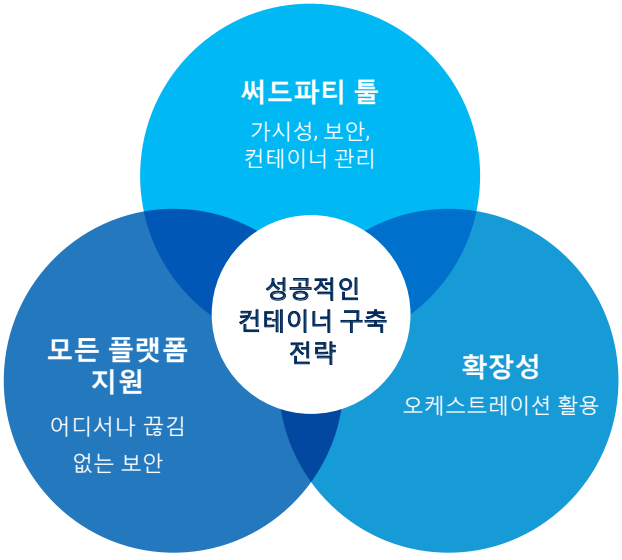
'네이티브'만으로는 충분하지 않은 이유

가상화 및 클라우드 전환의 초창기에는 기업이 워크로드를 시각화, 관리, 보호하는 데 클라우드 네이티브 제어만으로 충분하다고 믿으며 안심하곤 했습니다. 이후 IT 매니저들은 많은 시행착오를 거치고 나서야 기본 제어 이상의 보안을 제공하는 써드파티 솔루션을 통합하는 오버레이 관리 모델이 필요하다는 사실을 깨달았습니다.

Gartner와 Forrester Research의 보고대로, 성공적인 컨테이너 구축 전략은 다음과 같은 '컨테이너 3대 원칙'을 기반으로 합니다.

- 멀티 클라우드 및 온프레미스 아키텍처에서 어디서나 원활하게 구축할 수 있는 이식 가능하며 플랫폼에 구애받지 않는 방식으로 컨테이너 실행
- 대규모로 컨테이너를 실행하고 관리하기 위해 오케스트레이션 활용
- 컨테이너 관리, 가시성, 보안을 위해 써드파티 툴 사용

과거의 가상화 및 클라우드 노력과 달리, 컨테이너 업계는 처음부터 클라우드 네이티브 관리 시스템과 특히 보안 제어가 효과적인 컨테이너 전략에 적합하지 않음을 알고 있었습니다. 컨테이너 관리 솔루션에 대한 Gartner의 연구에 따르면, **응답자의 65%가 써드파티 관리 툴을 활용해 컨테이너화된 워크로드를 시각화, 관리, 보호하려고 한다고 답했습니다.**[5] 그러나 이러한 써드파티 툴은 온프레미스 및 클라우드 인스턴스 모두에서 원활하게 작동해야 하며, 정밀한 접근 방식을 통해 과거에 사용하던 번거롭고 혼합된 방식(예: 가시성이 없으며 세분화 수준이 미미한 보안 그룹, VLAN, 방화벽)의 리스크를 피할 수 있어야 합니다.



Akamai Guardicore Segmentation으로 컨테이너 도입 지원

Akamai Guardicore Segmentation은 오늘날 동적 하이브리드 데이터 센터 인프라의 도전 과제를 해결하기 위해 설계되었습니다. Akamai는 여러 환경에서 실행되는 모든 애플리케이션과 워크로드에 대한 포괄적인 가시성을 제공하며, 개별 또는 논리적으로 그룹화된 애플리케이션에 대한 보안 정책을 신속하게 생성, 배포, 적용함으로써 세분화된 소프트웨어 정의 세그멘테이션을 손쉽게 구축하도록 지원합니다.

명확히 말해, Akamai Guardicore Segmentation은 컨테이너 전용 제품이 아닙니다. 하지만 컨테이너 보안이 플랫폼의 핵심 기능이며, 베어 메탈 서버, 가상 머신, 서버리스 워크로드, 원격 디바이스도 포함할 수 있는 혼합 환경에서 일관되게 작동합니다. 따라서 Akamai는 기업이 여러 포인트 솔루션을 관리할 필요 없이 상주 위치나 배포 방식을 막론하고 모든 데이터 센터와 클라우드 자산을 보호할 수 있는 포괄적인 단일 솔루션을 제공합니다. 또한 Akamai의 솔루션은 기본 플랫폼 및 운영 체제와 분리되어 있기 때문에 보안 정책이 온프레미스와 클라우드 환경 사이를 이동하는 애플리케이션과 워크로드를 따르며, 이것이 이식성을 한층 높여 하이브리드 클라우드 인프라에 애플리케이션을 배포할 때 컨테이너의 이점이 한층 돋보입니다.

> 컨테이너 보안은 Akamai Guardicore Segmentation 플랫폼의 핵심 기능으로, 동적인 이기종 데이터 센터 환경에서 일관되게 작동합니다

Akamai Guardicore Segmentation은 컨테이너와 관련해 에이전트를 컨테이너 호스트 노드에 배치함으로써 팟 간(pod-to-pod) 및 팟과 가상 머신 간(pod-to-virtual machine) 통신 흐름을 포함한 전체 컨테이너 클러스터에 대한 가시성을 제공합니다. 이를 통해 프로세스, 사용자, 정규화된 도메인 이름(FQDN)별로 매우 정밀한 보안 정책을 구축하고 적용할 수 있습니다. 오케스트레이션 시나리오의 경우 Akamai는 쿠버네티스 오케스트레이션을 지원하고 강력한 맥락 정보를 위해 쿠버네티스 및 OpenShift 메타데이터에 대한 가시성을 허용합니다. 유연한 레이블링 모델을 통해 운영자는 네이티브 쿠버네티스 용어로 정책을 표현할 수 있습니다. Akamai는 쿠버네티스를 적용하기 위해 규모 제한 없이 쿠버네티스에서 정책을 적용하는 비침입적 방법인 네이티브 컨테이너 네트워크 인터페이스(CNI)를 활용합니다. 사용자는 전용 템플릿을 통해 네임스페이스, 애플리케이션, 기타 오브젝트 등 쿠버네티스 비즈니스 크리티컬 애플리케이션을 링펜싱할 수 있습니다. 또한 쿠버네티스의 워크로드 용량과 변경률에 맞게 확장할 수 있습니다. Akamai의 솔루션은 다른 모든 기업 워크로드에서도 비슷한 방식으로 작동하므로 전체 기업에서 자산을 시각화, 관리, 보호하는 단일 솔루션 역할을 합니다.

DevOps 환경에서 특히 중요한 것은 생성한 보안 정책이 지속적인 통합 및 배포(CI/CD) 프로세스에 효과적으로 통합되어 보안이 사후 고려 사항이 아니라 제공 모델에 완전히 통합되도록 보장하는 것입니다.

결론

컨테이너는 점차 많은 비즈니스 환경에서 필수적인 부분이 되고 있으며, 리소스 사용의 효율성을 높이고 프로세스를 간소화하며 이식성과 확장성을 강화할 수 있습니다. 그러나 컨테이너가 제공하는 내장형 보안 기능은 특히 하이브리드 환경을 활용하는 비즈니스에는 충분치 않습니다.

기업과 함께 성장할 보안 솔루션을 찾고 있다면, 수행 위치에 관계없이 종단 간 프로세스에 대한 세부적인 인사이트를 제공하는 플랫폼에 구애받지 않는 툴을 선택해야 합니다. Akamai Guardicore Segmentation은 오늘날 기업이 현재와 미래에 대비하는 데 필요한 다양한 특징과 기능을 제공함으로써 이러한 요건 이상의 이점을 발휘합니다.

보안 팀은 Akamai Guardicore Segmentation을 사용해 동적인 이기종 데이터 센터 환경에서 일관된 보안을 실현할 수 있습니다. 이를 통해 IT 팀이 컨테이너화의 이점을 실현하고 기업의 비즈니스 요구사항에 필수적인 중요 애플리케이션을 빠르고 비용 효율적이며 안전하게 개발하고 배포할 수 있도록 지원할 수 있습니다.

전체 환경에서 보안을 간소화합니다. akamai.com/guardicore에서 컨테이너를 위한 강력한 통합 보안 솔루션 등에 대해 자세히 알아보세요.

1 Chandrasekaran, Arun, Wataru Katsurashima. "The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem", Gartner, 2021년 8월 18일.

2 "Cloud Container Adoption In The Enterprise", Forrester, 2020년 6월.

3 "Best Practices for Running Containers and Kubernetes in Production", Gartner, 2019년 2월 25일.

4 "State of Kubernetes Security Report", Red Hat, 2022년 5월.

5 "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024", 2020년 6월 25일.

Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 인력, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있습니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 방문하거나 Twitter와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 05월 발행.