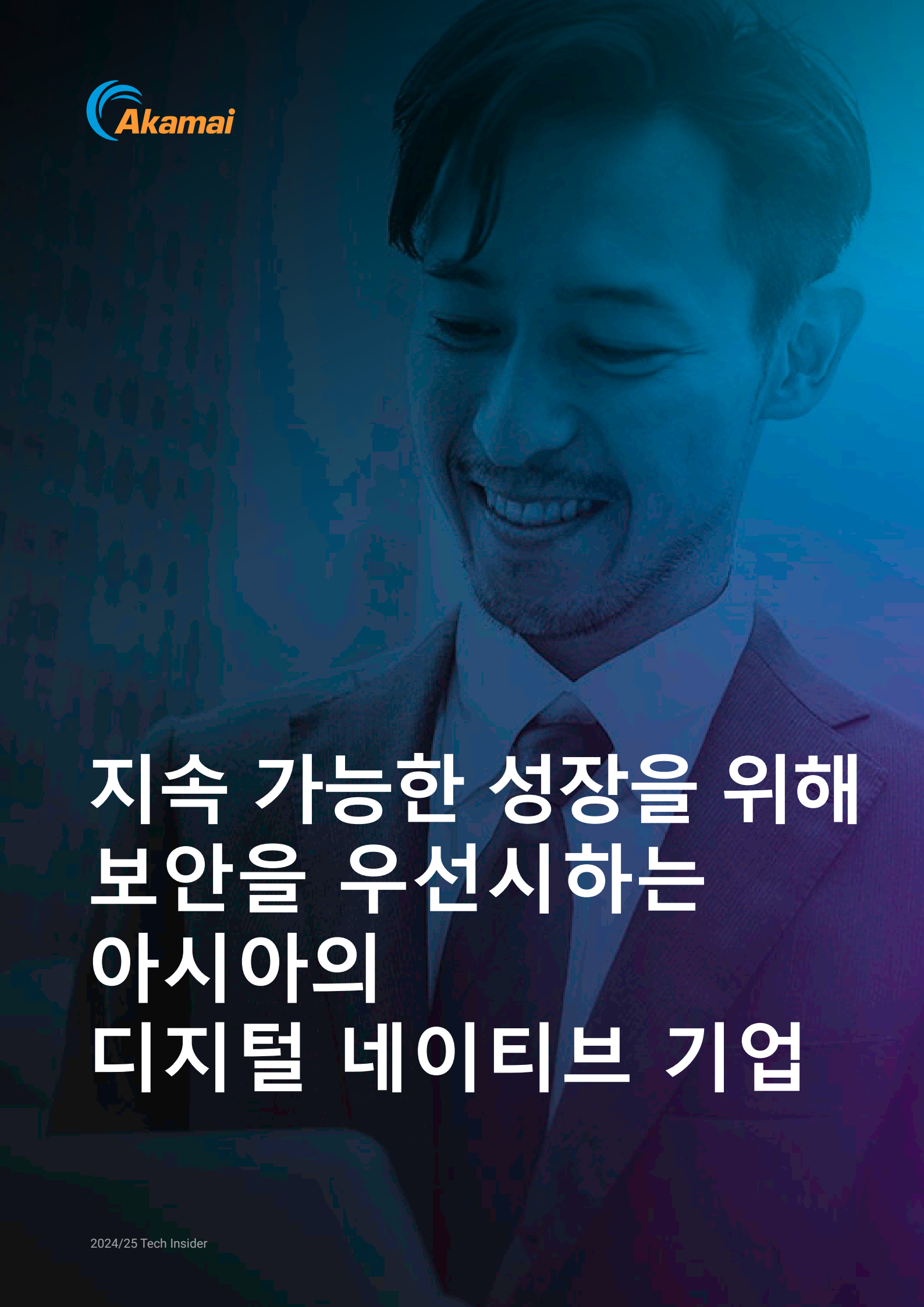


지속 가능한 성장을 위해 보안을 우선시하는 아시아의 디지털 네이티브 기업

2024/25 Tech Insider

핵심 요약

디지털 네이티브 기업(DNB)은 인터넷 시대에 탄생했으며, 탄생부터 최신 기술을 기반으로 설립되었습니다.

게이밍, 리테일, 교육 등 다양한 업계에 걸쳐 있는 디지털 네이티브 기업은 레거시 기술과 프로세스의 제약을 받지 않고 온라인에서 일하고, 생활하고, 즐기려는 고객의 수요에 부응하기 위해 기술의 속도로 움직입니다.

기술 리서치 기관인 IDC에 따르면, DNB는 2026년까지 기술에 최대 1289억 달러(USD)를 지출할 것으로 예상됩니다.

Akamai는 2024년 3월부터 5월까지 써드파티 리서치 기관 TechnologyAdvice와 함께 아시아 전역의 DNB의 기술 투자 우선순위와 기술 리더들이 밤잠을 설치게 하는 요인을 파악하기 위해 온라인 설문 조사를 실시했습니다.

호주, 동남아시아, 인도, 중화권에서 200여 명의 기술 리더가 설문 조사에 참여했습니다.

아시아 DNB의 비즈니스 우선순위와 기술 고민은 무엇일까요? 이러한 기술 중심 기업들은 솔루션 공급업체에 무엇을 기대할까요? 디지털 네이티브 기업들은 모두 같은 환경에서 성장했을까요?

시장 경쟁이 성숙해지든 빠르게 성장하는 소비자 기반 때문이든, 설문 조사에 참여한 DNB 약 10곳 중 9곳은 향후 12개월 동안 효율성과 생산성을 우선순위로 삼을 것이라고 답했습니다.

이는 DNB의 빠른 클라우드 도입을 보여주는 업계 데이터를 뒷받침하는 결과입니다. 2021~2026년 클라우드 기반 솔루션에 대한 기술 지출의 예상 성장률은 37%로, 비클라우드 소프트웨어(16%)와 IT 서비스(11%)를 앞질렀습니다.

이 지역의 DNB는 독립적으로 운영되고 API를 통해 커뮤니케이션하는 마이크로서비스를 중심으로 구축된 클라우드 네이티브 모듈식 아키텍처를 통해 빠르게 확장하고 증가하는 고객 디지털화에 대응할 수 있습니다.

그러나 이 점은 소프트웨어, 시스템, 서비스의 복잡한 매트릭스가 되어 DNB를 더 큰 사이버 취약점에 노출시킬 수 있습니다.

클라우드 전환의 어느 단계에 있든, 이 지역의 DNB는 보안이 클라우드 인프라 성능의 가장 큰 격차라는 사실을 잘 알고 있습니다.

실제로 대다수가 예산이나 컴플라이언스 문제보다 이 문제를 먼저 꼽을 만큼 점점 더 복잡해지는 IT 인프라가 사이버 보안 체계를 강화하는 데 있어 아킬레스건으로 작용할 수 있습니다.

기술 복잡성 증가에 따른 이러한 성장통은 클라우드 도입을 고려 중이거나 클라우드로의 전환을 모색 중인 기업들에게 경고의 메시지가 될 수 있습니다.

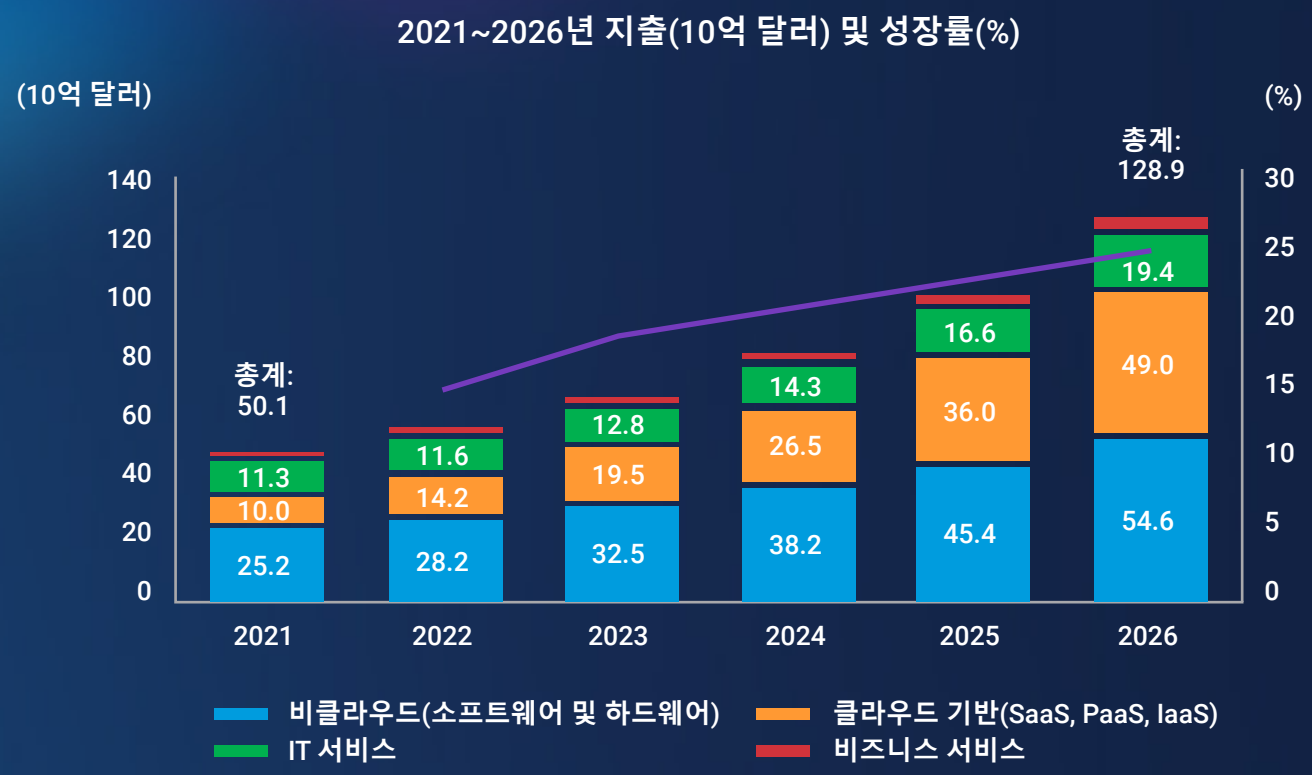
이 백서에서 이러한 리스크를 방어할 수 있는 실행 가능한 전략을 알아보세요.

속도와 효율성을 위해 클라우드를 활용하는 DNB

IDC Digital Native Business, Start-Ups and Scale-Ups CIS에 따르면, 디지털 네이티브 시장 부문은 '빠르게 성장하는 신흥 기업 그룹으로, 기술 중심적이고, 업계 비즈니스 모델의 근간이 되는 기술에 상당한 비용을 지출하고 있다'고 합니다.

업계나 시장에 관계없이 DNB는 기술을 차별화 요소로 활용하고 신속하게 대응하기 위해 기술을 활용합니다.

DNB는 본질적으로 기술 인프라를 구축할 때 클라우드 네이티브 설계 원칙을 준수합니다. 실제로 DNB의 클라우드 기반 기술에 대한 지출은 지속적으로 증가해 2021~2026년까지 37.3%의 성장률을 보일 것으로 예상됩니다.



일부 세그먼트 성장률

- 클라우드 기반(SaaS, PaaS, IaaS) CAGR 37.3%
- 비클라우드(소프트웨어 및 하드웨어) CAGR 16.7%
- IT 서비스 CAGR 11.5%
- 비즈니스 서비스 CAGR 10.4%

전체 시장 CAGR
20.8%

출처: IDC Press Release, Asia/Pacific Digital-Native Business Tech Spending from 2022-2026 to Grow at a CAGR of 20.8% and Hit US$128.9B in 2026, IDC Forecasts, 19 April 2023

DNB 기술 인프라는 마이크로서비스의 설정 가능한 아키텍처를 기반으로 구축되어 빠르게 성장하는 디지털 공간을 따라잡는 데 필수적인 유연성, 민첩성, 빠른 시장 출시 기간을 지원합니다.

설문 조사에 따르면, 이 지역 DNB의 4분의 3은 효율성과 생산성을 우선시해 클라우드 기술을 도입하고 있는 것으로 나타났습니다.

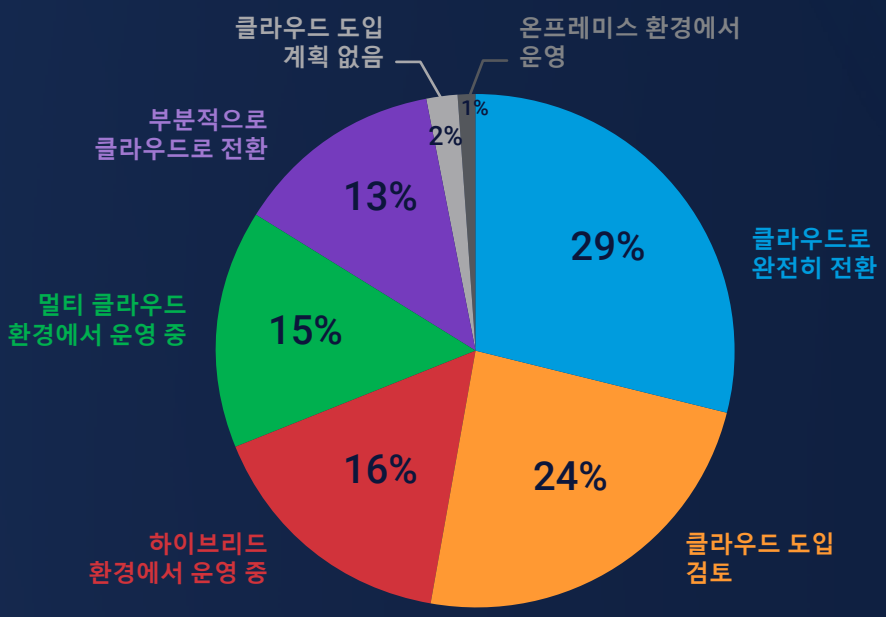
응답자의 74%는 클라우드로 완전히 전환했거나 클라우드 기술을 도입하고 있다고 답했습니다.

그러나 응답자의 26%는 클라우드 도입 계획이 없거나 아직 탐색 단계에 있다고 답했으며, 이는 전 지역에 걸쳐 일관되게 나타났습니다(호주 19%, 인도 20%, ASEAN 29%).

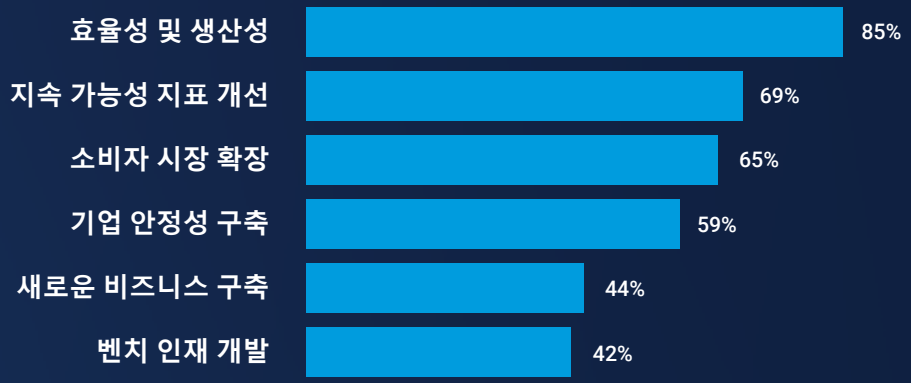
이러한 소극적인 태도는 강력한 규제를 받는 업계에 속한 기존 대기업들과 클라우드에 대한 오랜 신중한 접근 방식이 클라우드 도입의 걸림돌이 되고 있기 때문으로 보입니다.

하지만 DNB가 클라우드 투자를 늘리면서 상황이 달라지고 있으며 이는 클라우드 기술 지출의 높은 성장률로 입증됩니다.

클라우드 도입 여정의 어느 단계에 있나요?



향후 12개월 내 최우선 비즈니스 우선순위



온라인 라이프 보호

흔히 DNB는 기술에 능숙하다고 합니다. 그러나 이러한 숙련도는 전문 영역에 국한될 수 있습니다.

DNB는 클라우드에서 태어났지만 클라우드, 데이터 및 인공지능(AI) 분야의 신기술의 잠재력을 최대한 활용하는 데 어려움을 겪을 수도 있습니다.

응답자들이 클라우드 전환과 관련해 직면한 문제를 클라우드 여정의 현재 위치와 비교해 매핑했습니다.

클라우드로 완전히 전환한 응답자와 아직 클라우드 도입을 검토 중인 응답자 사이에서 클라우드 지출을 이해하는 데 일관된 어려움이 있었습니다.

대부분의 클라우드 공급업체는 가격을 투명하게 공개하지만 비용 내역이 복잡할 수 있습니다. DNB는 다양한 요인에 따라 다르게 확장되는 마이크로서비스 및 멀티클라우드 배포의 비용을 예측하고 해독할 수 있는 올바른 지식과 시간을 확보해야 합니다. 예를 들어, 확장성 문제를 일으키는 요인은 최종 사용자의 수요인가요? 아니면 프로세스 간 커뮤니케이션인가요?

클라우드 전환 시 직면하는 3가지 주요 과제

	보안 영향 관리	적합한 클라우드 공급업체 선택	기술적 타당성 평가
클라우드로 완전히 전환	45%	53%	57%
클라우드 도입 검토	63%	62%	52%
하이브리드 환경에서 운영 중	74%	49%	54%
멀티 클라우드 환경에서 운영 중	50%	44%	47%
부분적으로 클라우드로 전환	45%	41%	41%

기타 과제:
클라우드 속도 할당 이해, 전환할 앱 우선순위 지정, 최적의 인스턴스 크기 조정 및 선택, 온프레미스와 클라우드 비용 비교 평가, 기술 전문성 부족, 앱 의존성 이해

이로 인해 DNB는 성능, 안정성, 지원을 희생하지 않으면서 이해하기 쉬운 가격을 제공하는 클라우드 공급업체로 이동하고 있습니다.

그러나 하이브리드 환경에서 운영 중이거나 멀티클라우드 환경에서 운영 중이거나 부분적으로 클라우드로 전환한 경우 등 DNB의 클라우드 전환 단계 중 어디에 있든 보안에 미치는 영향을 관리하는 것은 여전히 일관된 도전 과제로 남아 있습니다.

실제로 대부분의 설문 조사 응답자들은 현재 클라우드 인프라에서 가장 큰 격차로 보안을 꼽았습니다.

Akamai는 매우 낮은 이그레스 요금, 충분한 월 이그레스 허용량, 데이터 센터, 클라우드 트래픽 부하 분산을 극대화하는 툴로 간단하고 투명한 가격 정책을 유지합니다.

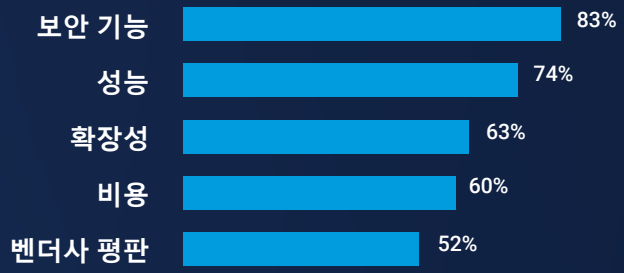
이와 더불어 Akamai의 글로벌 인프라를 활용해 데이터 및 트래픽 집약적인 애플리케이션의 비용을 최적화할 수 있는 수많은 기회를 창출합니다.

클라우드 공급업체를 선택할 때 보안 기능은 성능, 평판, 확장성, 비용보다 더 중요한 요소입니다.

클라우드 인프라의 성능이나 기능에서 가장 큰 격차가 있는 것은 무엇인가요?

	보안	네트워크 지연 시간	데이터 저장 및 가져오기	컴퓨팅 리소스
클라우드로 완전히 전환	65%	65%	67%	47%
클라우드 도입 검토	81%	58%	67%	62%
하이브리드 환경에서 운영 중	74%	66%	49%	46%
멀티 클라우드 환경에서 운영 중	84%	66%	66%	63%
부분적으로 클라우드로 전환	69%	62%	62%	24%

클라우드 공급업체를 선택할 때 고려하는 요소



기술 우선 사고방식은 DNB의 아킬레스건?

바로 이 부분에서 기술이 DNB에 득이 되기도 하고 실이 되기도 합니다.

대다수의 응답자는 사이버 보안 체계를 강화하는 데 있어 가장 큰 어려움으로 복잡한 IT 인프라를 꼽았습니다.

디지털 네이티브는 컴포저블 마이크로서비스와 이를 연결하는 API를 중시하는 클라우드 네이티브 설계 원칙을 받아들입니다.

이러한 API는 기술 배포와 시장 출시 속도를 가속해 DNB가 빠르게 반복하고 기능을 신속하게 제공할 수 있도록 지원합니다.

그러나 이러한 속도와 설정 가능성은 다양한 서비스를 담당하는 개발자가 DNB의 운영에 집중할 동기가 없을 때 복잡성이라는 대가를 치르게 됩니다.

대부분의 보안 툴이 하이브리드 환경을 지원하지 않고 임베디드 클라우드 보안이 공급업체의 클라우드에만 집중하는 경향이 있기 때문에 보안팀과 기술은 어려움을 겪을 것입니다.

예를 들어, 게임 공급업체는 게임 개발에 수년이 걸리기 때문에 벤더사가 아닌 신뢰할 수 있는 파트너인 클라우드 인프라 공급업체와 협력하기를 원합니다.

게임사와 개발자팀은 성능, 리소스 할당, 지연 시간, 처리량 등 클라우드 컴퓨팅의 모든 측면에 대한 인사이트는 물론 예측 가능한 가격 책정 및 과금 투명성을 원합니다.

종량제와 필요한 것만 지불하는 분산형 클라우드 컴퓨팅 인프라는 게임 개발이나 업그레이드와 직접 관련이 없는 운영 비용을 면밀히 모니터링하고자 하는 게임 공급업체에 매우 매력적입니다.

설문 조사 결과에 따르면, DNB는 점점 더 복잡해지는 IT 인프라에 직면하고 있으며, 이는 기업의 사이버 보안 체계에 영향을 미치고 있습니다.

사이버 보안 체계를 가로막는 가장 큰 도전 과제

	복잡한 IT 인프라	현지 컴플라이언스 요구사항	숙련된 인력 부족	예산 제약	빠르게 진화하는 위협
클라우드로 완전히 전환	43%	7%	13%	12%	25%
클라우드 도입 검토	37%	6%	10%	27%	21%
하이브리드 환경에서 운영 중	49%	3%	9%	23%	17%
멀티 클라우드 환경에서 운영 중	59%	13%	13%	6%	9%
부분적으로 클라우드로 전환	31%	7%	17%	14%	31%

리스크와 보상의 균형

현실을 점검해 봅시다. 클라우드 전반에 걸쳐 일관된 보안 정책을 적용하는 것은 어렵습니다.

신생 DNB는 클라우드 기술의 빠른 발전 속도를 선호할 수 있지만, 비즈니스가 성숙함에 따라 DNB는 각 기술 혁신에 따른 리스크와 보상의 균형을 맞춰야 합니다. 혁신적인 기술이 도입될 때마다 복잡성이 한층 커지기 때문입니다.

그렇다면 보안 유출이나 오용을 방지하기 위해 시장 출시 속도 및 고객 도입과 보안, 컴플라이언스, 거버넌스 간의 균형을 맞추는 방법은 무엇일까요?

이는 DNB의 클라우드 전환 단계에 관계없이 사이버 보안을 강화하는 데 있어 가장 큰 과제로 남아 있습니다.

Akamai Connected Cloud는 오픈 소스 및 멀티 클라우드 아키텍처를 포용하는 개방형 플랫폼입니다. 이 아키텍처는 개발자가 원하는 애플리케이션과 소프트웨어를 전 세계적으로 확장 가능하고 지역적으로 최적화된 저지연 워크로드를 지원하는 데 필요한 서비스와 함께 손쉽게 활용할 수 있도록 설계되었습니다.

클라우드 기술은 인프라만 제공하는 것에서 인프라 관리를 포함한 모든 서비스를 제공하는 형태로 변하고 있습니다.

클라우드 네이티브 인프라를 운영하면 복잡한 인프라 문제뿐만 아니라 집중 리스크도 발생합니다.

다음은 클라우드 도입 여정의 단계에 관계없이 고려해야 할 몇 가지 사항입니다.

멀티클라우드 전략 도입

기업은 벤더사 종속을 피하고 유연성을 높이며 클라우드 서비스 사용을 최적화하기 위해 멀티클라우드 접근 방식을 도입해야 합니다.

Forrester Research의 설문 조사에 따르면, IT 리더들이 클라우드 벤더사에 원하는 가장 중요하게 요구사항은 클라우드에서 엣지까지 배포 및 실행할 수 있는 능력입니다.

특정 벤더사에 의존하면 향후 기술 옵션이 줄어들고 해당 벤더사가 기업의 기술 미래에 상당한 영향력을 행사할 수 있습니다.

애그노스틱 분산 플랫폼을 활용하면 디지털 네이티브가 원시 데이터에 원활하고 빠르게 접속하고 여러 시스템에 분산된 데이터에서 인사이트를 얻을 수 있습니다.

정기적으로 검토 및 반복

클라우드 비용을 주기적으로 검토해 클라우드 지출을 분석 및 최적화하고, 절감할 수 있는 영역을 파악하고, 리소스 사용을 최적화하세요.

모니터링 데이터와 실시간 애널리틱스를 사용해 리소스 할당, 비용 관리, 보안 개선 등 최적화할 영역을 파악하세요.

정기적인 모니터링과 최적화를 통해 클라우드 투자에서 최대한의 비즈니스 가치를 얻을 수 있습니다.

클라우드 거버넌스 프레임워크 구축

특정 클라우드 공급업체에 의존하는 애플리케이션 및 비즈니스 프로세스가 많을수록 클라우드 서비스 문제가 잠재적으로 미치는 영향의 범위가 넓어져 비즈니스 연속성에 대한 우려가 커질 수 있습니다.

클라우드 거버넌스 정책을 개발하고 시행해 클라우드 리소스를 효과적으로 관리하고, 컴플라이언스를 보장하며, 비용을 통제하세요.

이 모델에는 접속 제어, 보안 조치, 비용 관리 및 컴플라이언스 요구사항이 포함되어야 합니다. 명확한 거버넌스 모델은 전사적으로 일관성과 모범 사례를 유지하는 데 도움이 됩니다.

기업은 집중 리스크에 대한 접근 방식이 다를 수 있는 여러 규제 기관의 집중 리스크 해결에 대한 규제 요구를 충족하지 못할 수도 있습니다.

고급 API 보안 우선순위 지정

DNB가 비클라우드, 클라우드, 멀티클라우드 아키텍처를 연결할 때 API는 핵심적인 역할을 합니다.

DNB는 내부 애플리케이션을 연결하고, 비즈니스 파트너와의 프로세스를 가속하고, 소비자에게 데이터 서비스를 제공함으로써 새로운 수준의 연결성, 생산성, 민첩성을 달성할 수 있습니다.

속도와 기술 중심의 혁신을 추구하다 보니, API와 관련된 애플리케이션과 비즈니스 프로세스는 보안팀이 그 상태를 평가할 수 있는 속도보다 더 빠르게 시작되고 배포되는 경우가 많습니다.

잘못된 설정과 취약점 그리고 API 보안 전문 지식의 부족은 혁신적인 DNB를 잠재적인 사이버 위협에 노출시킵니다.

실제로 **631명의 사이버 보안 전문가**를 대상으로 한 별도의 업계 설문 조사에 따르면, 개발자 2명 중 1명은 API 리팩토링 및 수정에 최대 절반의 시간을 소비합니다.

> **31%**: **Akamai가 방어하는 트래픽 중 API 트래픽의 비율. Akamai는 통합 사용자 경험 최적화 기능을 통해 애플리케이션과 워크로드를 일관되게 제어할 수 있는 툴을 제공합니다.**

아시아 전역의 DNB는 지속 가능한 비즈니스 성장을 위해 API 보안을 최우선 순위로 두고 있습니다.

호주에서 사업을 확장하든 인도와 ASEAN에서 시장 점유율을 높이든, DNB는 웹 및 애플리케이션 보안과 피싱 방지 기술에 앞서 최신 API 보안을 최우선 사이버 보안 투자 분야로 삼고 있습니다.

다음 사이버 보안 투자 영역의 순위를 가장 중요한 것(위)부터 가장 중요하지 않은 것(아래)까지 표시하세요

1. 최신 API 보안
2. 웹 애플리케이션 보안
3. 피싱 방지 기술
4. 분산 서비스 거부(DDoS) 방어
5. 제로 트러스트 관련 기술

API 보안 오류의 조건

API를 사용하는 비즈니스 크리티컬 프로세스의 신속한 배포 + API에 대한 가시성 부족 = 잘못 설정되거나 취약한 API

Akamai 트래픽 데이터를 살펴보면 아시아 태평양 및 일본 지역에서 제조 업계가 API 공격의 가장 높은 비율을 차지했습니다.

이는 부분적으로는 API를 통한 이 중요 인프라 부문의 연결성이 증가하고 공급망 중단 가능성이 높아졌기 때문일 수 있습니다.

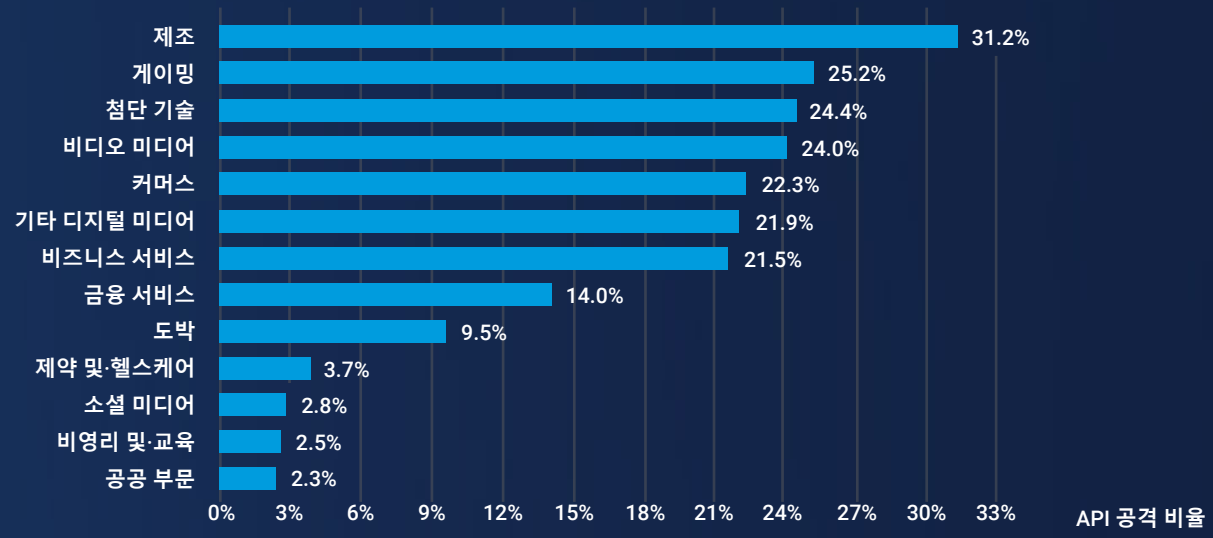
동시에 게이밍, 하이테크, 비디오 미디어, 커머스 등 디지털 기반 업계도 API 공격자의 표적이 되고 있습니다.

디지털 네이티브 기업이 가장 많이 표적이 되는 이유는 비즈니스의 상당 부분이 API에 의존하고, 클라우드 인프라를 가장 많이 배포하며, 레거시 기업 및 아키텍처에 비해 피싱, 계정 감염, 랜섬웨어의 가장 매력적인 표적이기 때문일 가능성이 높습니다.

로컬 파일 인클루전(LFI)이 여전히 최고의 API 공격 기법이지만, 2023년 데이터 세트에서는 명령어 인젝션(CMDi)과 서버 측 요청 위조(SSRF)와 같은 추가 기법이 등장했습니다. 이러한 기법은 취약하거나, 잘못 설정되었거나, 문서화되지 않은 API에 상당한 리스크를 초래합니다.

봇 요청도 우려되는 영역입니다. 동일한 12개월의 보고 기간 동안 2조 건 이상의 의심스러운 봇 요청 중 40%가 API를 겨냥한 것으로 나타났습니다.

APJ: 업계별 API 공격(2023년 1월 1일~2023년 12월 31일)



APJ: 기법별 API 공격(2023년 1월 1일~2023년 12월 31일)

중요한 API 보안 고려 사항

API 취약점은 끊임없이 진화하고 있습니다. 가장 큰 API 보안 리스크 몇 가지를 이해하는 기업은 경쟁에서 앞서나갈 수 있습니다.

검색 및 가시성

폐기되지 않았거나 제대로 문서화되지 않은 오래되거나 이전 버전의 API는 기업을 더 높은 수준의 리스크에 노출시킵니다. 섀도 API와 같은 사례는 관리 범위 밖에 존재하고 운영되며 취약점이 될 수 있습니다.

런타임 보안

API는 활발하게 데이터를 교환하기 위해 실행되므로 기존 보안 툴로는 API의 정상적인 요청과 악성 요청을 구분하기 어려울 수 있습니다. API 로직 남용과 같은 우회 위협은 정상적인 API 요청과 섞여 있기 때문에 탐지하기 어려운 것으로 알려져 있습니다.

API 테스트

속도 저하 없이 보안을 개선하려면 개발의 모든 단계에서 API 보안 테스트를 수행해야 합니다. 비용과 수정의 관점에서 볼 때, API가 프로덕션에 출시되어 활발하게 사용된 후보다 API 개발 단계에서 문제를 해결하는 것이 더 쉽습니다.

인증되지 않은 리소스 접속

머신 간 시나리오에서는 인증 및 권한 부여가 더 복잡합니다. 사용자나 시스템이 API 구축이나 설정의 취약점으로 인해 어떤 형태의 인증도 하지 않고 API 리소스에 접속할 수 있는 경우가 많습니다.

URL의 민감한 데이터

URL의 민감한 데이터는 로그나 캐시처럼 공격자가 접속할 수 있는 위치에 저장되는 경우가 많기 때문에 민감한 데이터 유출 및 컴플라이언스 문제가 발생할 리스크가 큽니다.

크로스 오리진 리소스 허용 정책

API는 필요 이상으로 광범위한 오리진(프로토콜, 도메인, 포트 등)에서 요청이 시작되도록 허용할 수 있습니다.

시작부터 API 보안을 우선시하는 문화

설문 조사에 참여한 DNB 10곳 중 9곳은 클라우드 및 보안 솔루션 공급업체를 평가할 때 API 보안을 매우 중요하거나 중요한 제품 기능으로 꼽았습니다.

기술 혁신과 써드파티 연결의 속도가 빨라지면서 DNB는 사이버 공격자가 악용할 수 있는 잠재적인 취약점을 파악하기 위해 벤더사의 지원이 필요합니다.

API 보안은 개발 프로세스의 모든 단계에 적용되어야 합니다. API 테스트 프레임워크와 특정 API 테스트 툴이 부족하면 취약한 API가 더 많이 게시되어 API 보안 관련 인시던트가 증가할 수 있습니다. API 비즈니스 로직 남용에 대한 가시성 부족은 API 데이터 유출 및 사기로 이어지는 또 다른 요인입니다.

예를 들어, 보안팀은 API가 운영 중에 악용되고 있는지 어떻게 알까요? 어느 시점에 어떤 공격이 기업의 API를 공격하고 있나요?

예를 들어, 보안팀은 API 엔드포인트의 목적을 완전히 이해하지 못할 수 있으며, 어떤 백엔드 워크로드가 엔드포인트와 상호작용을 하는지, 또는 어떤 데이터 종류가 교환되는지 파악하지 못해 어려움을 겪을 수 있습니다. 개발팀은 개발 주기 후반에 버그를 수정할 수 있는 능력을 과대평가할 수도 있습니다.

AI 기반 검색 및 프로파일링은 API 보안의 중요한 트렌드이지만, 개발 프로세스(DevSecOps) 초기에 보안을 우선시하는 자세는 DNB의 취약점을 조기에 축소해 설계부터 안전한 API 개발 철학을 확립하는 데 도움이 됩니다.

이러한 최신 API 보안 사각지대를 처음부터 파악하면 더 강력한 사이버 보안 체계를 구축하는 데 도움이 됩니다.

클라우드 또는 보안 솔루션 공급업체를 평가할 때 다음 제품 기능을 얼마나 중요하게 생각하나요?

	필수	중요	다소 중요	중간	다소 중요하지 않음
API 보안	45.60%	45.10%	7.40%	1.90%	0.00%
사용자 지정 가능한 클라우드 보안 정책	31.20%	53.90%	8.40%	6.50%	0.00%
엣지 컴퓨팅 기능	29.80%	47.00%	15.80%	6.00%	0.90%
옵저버빌리티	28.40%	52.10%	11.20%	7.00%	0.90%
실시간 애널리틱스 및 보고	45.60%	34.40%	11.20%	7.40%	1.40%
제로 트러스트	32.60%	39.10%	14.40%	9.30%	0.90%

일반적인 API 보안 사각지대

인증되지 않은 리소스 접속 시도

이는 이전 섹션에서 설명한 인증되지 않은 리소스 접속 체계 알림에서 더 긴급하게 파생된 것으로, 적절한 인증 없이 민감한 API 리소스에 접속하려는 구체적인 시도가 관찰되는 경우입니다. 관찰된 시도가 실패하더라도 이러한 시나리오는 API 취약점을 찾아 악용하려는 적극적인 시도를 의미하며, 결국 즉각적인 개입 없이도 성공할 수 있습니다.

비정상적인 JSON 속성

예상치 못한 데이터 종류, 비정상적인 크기, 과도한 복잡성 등 비정상적인 JSON 페이로드가 포함된 API 활동은 취약한 API를 악용하려는 시도가 활발히 이루어지고 있음을 나타낼 수 있습니다. 이러한 활동은 인젝션 공격, 서비스 거부, 데이터 유출, API 논리 취약점 악용 등 다양한 악성 행위를 시도하는 것을 나타낼 수 있습니다.

경로 매개변수 퍼징 시도

경로 매개변수 퍼징은 의도적으로 예기치 않거나 잘못된 데이터를 API 요청의 일부로 전송하는 또 다른 예시로, RESTful API가 특정 리소스나 작업을 지정하는 데 사용하는 URL 부분에 중점을 둡니다. 공격자가 정찰을 수행해 데이터 유출 또는 서비스 중단 시도의 표적이 될 수 있는 잠재적으로 취약한 API를 발견하는 데 사용하는 또 다른 기법입니다.

불가능한 시간 여행

API 활동을 분석할 때 타임스탬프, 지리적 위치 또는 API 호출 순서가 비논리적인 경우 공격자가 어떤 식으로든 이를 조작하려고 시도하고 있음을 시사하는 시나리오가 있습니다. 게다가 이러한 종류의 행동은 사기 행위의 일부로 데이터 조작과 같은 여러 가지 위협을 나타낼 수 있습니다.

데이터 스크레이핑

데이터 스크레이핑은 API의 의도된 사용 및 서비스 약관에 맞지 않는 방식과 양으로 API에서 데이터를 자동으로 추출하는 것을 말합니다. 공격자는 탐지를 피하고 지적 재산을 훔치거나 민감한 고객 데이터를 수집하거나 어떤 종류의 이익을 얻기 위해 데이터를 천천히 수집하는 경우가 많습니다. API 내에서 발견되지 않는 저속 데이터 스크레이핑은 잠재적으로 대규모 데이터 유출 공격으로 이어질 수 있습니다.

최신 API 보안 접근 방식

최신 API는 마이크로서비스, 멀티클라우드, 원활한 통합, 빠른 확장을 가능하게 하는 연결 조직입니다. API는 모든 애플리케이션 또는 워크로드의 소프트 하부 조직이며 비즈니스 성과를 최적화하기 위해 올바르게 설계, 개발, 배포되어야 합니다.

그러나 최신 API 트랜잭션은 빈번한 트랜잭션과 같은 고유한 특성이 있음에도 불구하고 기업은 동일한 보안 조치를 적용하는 경향이 있습니다.

1 자동화된 API 검색 구축

API 관련 보안 유출, 알 수 없는 의존성, 예기치 않은 불일치로부터 보호하기 위해 제공하고 사용하는 API를 올바르게 식별해야 합니다. API 데이터 소스에 대한 기본 통합을 통해 복잡성과 운영 오버헤드를 모두 줄일 수 있습니다.

2 API의 체계 관리

API 보안을 평가하려면 잘못된 설정을 탐지하고, 모의 해킹을 수행하거나, URL에 민감한 데이터를 노출하는 API와 같은 설정 문제를 미리 스캔하는 자동화된 평가 툴을 사용해야 합니다. 자동화된 응답은 응답 워크플로우의 일부로, API 개발팀과 같은 관련 당사자는 이를 통해 문제 해결을 요청할 수 있습니다.

3 API 런타임 보안

여기에는 악성 활동을 나타내는 패턴을 탐지하는 것이 포함됩니다. 유사한 공격의 데이터 세트에 대해 학습된 비정상 탐지 엔진은 위협을 식별하고 관련 당사자에게 알릴 수 있어야 합니다. 비정상적인 API 트래픽이 탐지되면 대응 워크플로우를 트리거해 해결 티켓을 올리거나 잠재적인 위협을 차단할 수 있습니다.

4 선제적 보안 테스트

동적 스캐닝 및 퍼징을 통한 API 보안 테스트는 초기 평가에서 잘못된 설정으로 탐지되지 않을 수 있는 기술적 취약점을 발견할 수 있습니다.

API 보안이 성숙해짐에 따라 보안 테스트는 API 개발 수명 주기에 더 긴밀하게 통합되어야 하며, 취약점이 발견되는 즉시 프로덕션에 도달하기 전에 해결해야 합니다. 이는 보안팀과 개발팀 간의 교차 기능 조율을 의미합니다.

5 API 보안 생태계

API 보안 솔루션이 기본적으로 써드파티 기술과 통합 및 상호 운용할 수 있는 풍부하고 강력한 기술 생태계를 갖추면 비용과 구축 시간이 단축됩니다. 또한, 데이터 소스에서 더 넓은 API 트래픽 가시성을 확보하고, 자동화된 워크플로우를 통해 위협에 더 빠르게 대응하고, 전반적으로 더 나은 API 보안 체계를 갖출 수 있습니다.

호주/뉴질랜드: 스타트업부터 스케일업까지

애널리스트 보고서에 따르면, 앞으로 호주 및 뉴질랜드(ANZ)의 국내 수요와 소프트 노동력 수요가 약세를 보일 것으로 예상됩니다.

고객은 이미 낮은 임금 상승과 지속적인 인플레이션으로 인해 재정적 압박을 느끼고 있습니다.

현재의 경제 환경에 대응하기 위해 ANZ의 DNB 응답자들은 효율성과 기업의 안정성을 우선시하고 있습니다.

또한, 클라우드 기술이 비즈니스의 필수 요소로 자리 잡으면서 사고방식에도 변화가 생겼습니다. 총 97%의 응답자가 클라우드를 도입했거나 클라우드 도입을 검토 중이라고 답했습니다.

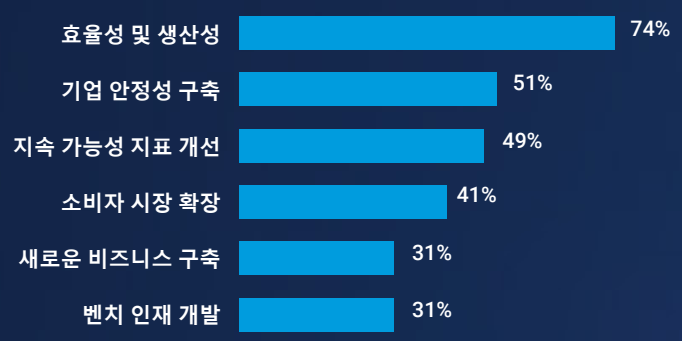
ANZ 기업은 냉각된 경제 상황에서 운영 효율성을 더 높이기 위해 클라우드 도입 곡선을 따라 더 나아갈 수 있습니다.

주요 예측 요약

달력 연도	2020	2021	2022	2023	2024f	2025f	2026f
실질 GDP[1](연평균 변화율)	-1.4	5.6	2.4	0.6	0.5	1.5	2.5
실업률(SA, 12월 분기)	4.9	3.2	3.4	4.0	5.1	5.5	5.0
CPI 인플레이션(연간 변화율, 12월 분기)	1.4	5.9	7.2	4.7	2.6	2.0	2.0
공식 금리(12월 분기 말)	0.25	0.75	4.25	5.50	5.50	4.75	4.00

[1] 프로덕션 기준
출처: Statistics NZ, REINZ, Bloomberg, ANZ Research

향후 12개월 내 최우선 비즈니스 우선순위



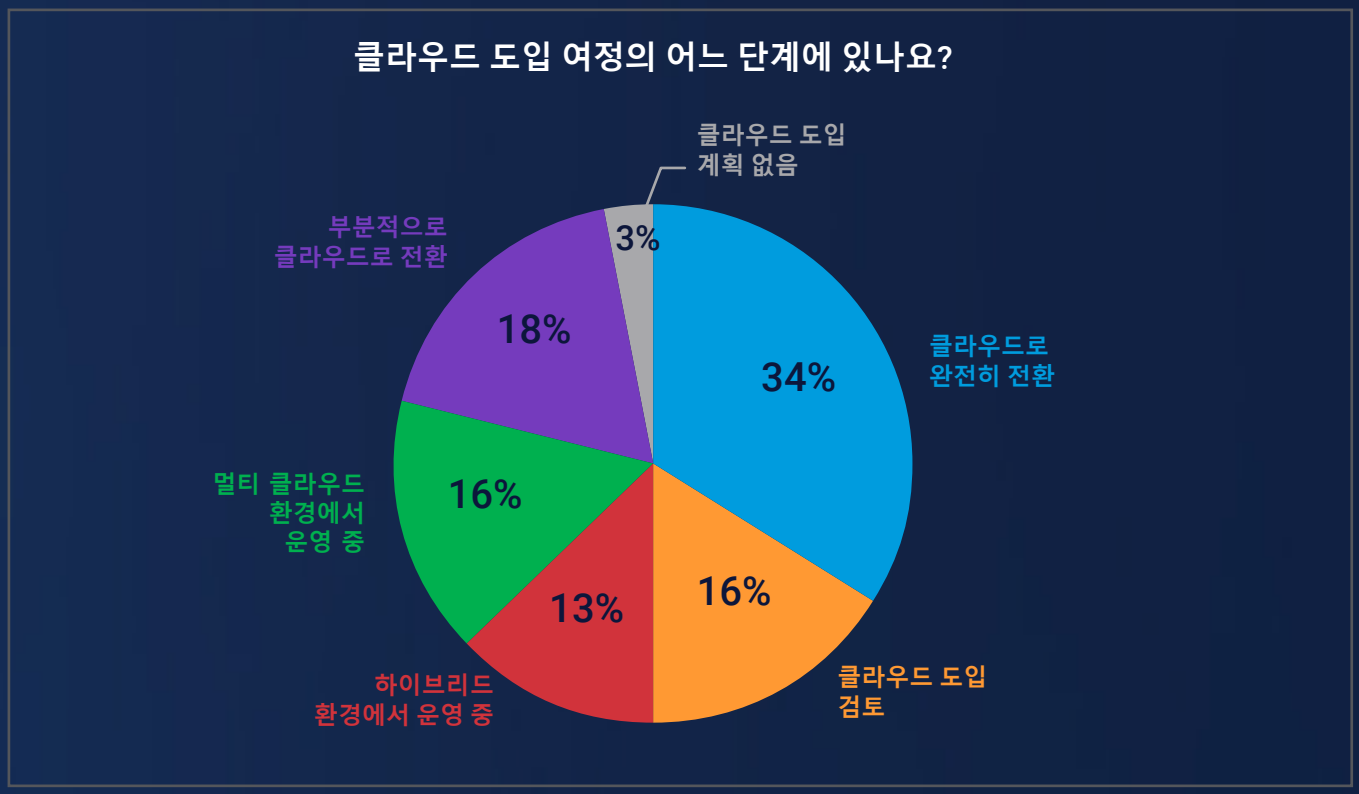
예를 들어, ANZ의 퍼블릭 클라우드 도입은 재해 복구와 같은 인프라 교체를 위한 개별 서비스형 소프트웨어 기반 솔루션을 넘어 기업 전반의 디지털 전환과 혁신을 주도하는 고급 사용 사례로 발전했습니다.

이러한 상대적인 클라우드 도입 성숙도에 따라 클라우드를 비즈니스 방해 요소로 보는 사고방식에서 비즈니스 필수 요소로 보는 사고방식으로 전환되었습니다.

또한, 공공 부문은 호주와 뉴질랜드 모두에서 클라우드 도입을 주도하고 있으며, 뉴질랜드는 2012년에, 호주는 2015년에 클라우드 우선 정부 정책을 발표했습니다.

호주 기업들은 2024년에 2023년보다 19.7% 증가한 154억 달러를 퍼블릭 클라우드에 지출할 것으로 예상됩니다 (출처: Gartner).

디지털 도입이 늦어지고 있다는 것은 ANZ 기업이 클라우드용으로 설계되지 않았거나, 컨테이너화되지 않았거나, 마이크로서비스 기반이 아닌 레거시 애플리케이션을 보유하고 있어 결국 클라우드 네이티브 애플리케이션보다 더 큰 비용이 소요될 수 있다는 것을 의미합니다.



ANZ 설문 조사 응답자들은 클라우드 전환 시 가장 큰 어려움으로 보안 문제, 기술 전문성 부족과 함께 클라우드 비용을 꼽았습니다.

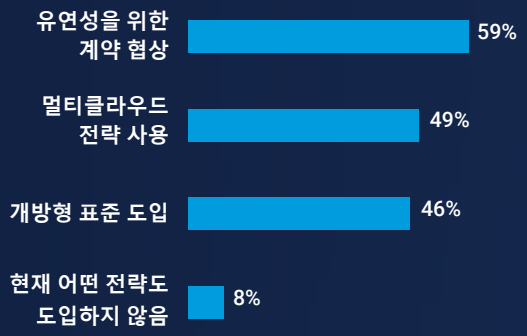
기술 도입의 규모와 혁신에 대한 압박, 경기 침체가 맞물리면서 클라우드 낭비를 최소화하는 데 대한 관심이 다시 높아졌습니다.

클라우드 비용은 다양한 요인에 따라 다르게 확장되는 마이크로서비스와 멀티클라우드 배포의 비용을 예측하고 해독하는 데 필요한 전문 지식과 시간으로 인해 복잡할 수 있습니다.

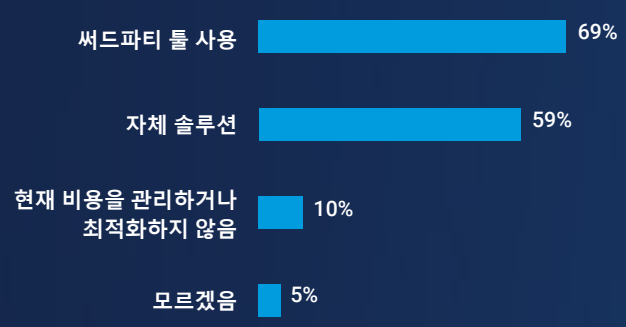
FinOps와 같은 클라우드 비용 관리 솔루션은 클라우드의 가변적 지출 모델에 재무적 책임을 도입합니다. 사용자는 기업의 클라우드 사용량과 생산성 최적화 기회에 대한 가시성을 확보해 지출 결정에 대한 책임을 집니다.

클라우드 전환과 관련해 가장 큰 어려움은 무엇인가요?

벤더사 종속을 피하기 위한 전략



클라우드 비용 최적화를 위한 써드파티 툴



ANZ의 IT 리더들은 써드파티 툴, 관리형 서비스, 할인을 대가로 더 많은 약정 지출액 또는 더 큰 약정 성장률을 제공하는 계약 협상을 활용하고 있습니다.

클라우드 운영 관리와 재무 거버넌스를 결합하면 연간 클라우드 예산을 하룻밤 사이에 소모할 수 있는 무제한 자동 확장으로부터 기업을 보호할 수 있습니다.

이는 DNB가 써드파티 툴과 관리형 서비스를 활용해 효율적이고 지속 가능한 확장을 위해 전담 인력을 보강함에 따라 상대적으로 클라우드 도입 성숙도가 높아졌다는 것을 의미합니다.

전 세계 *1200*개 네트워크에 통합된 Akamai의 글로벌 네트워크는 모든 주요 클라우드 공급업체와 최적화된 상호 연결을 유지해 고가용성, 짧은 지연 시간, 무한한 확장성을 보장합니다.

더 풍부한 고객 경험은 더 민감한 데이터를 의미

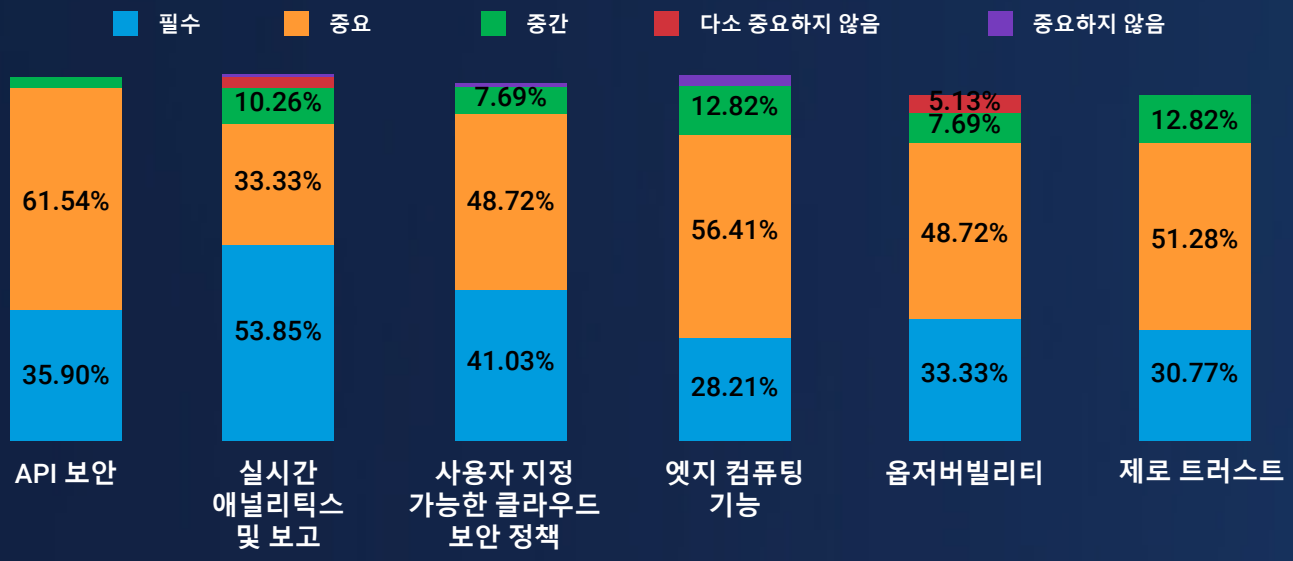
고객의 디지털 도입이 비교적 성숙해짐에 따라 ANZ 기업은 최적의 사용자 경험을 제공하기 위해 실시간 데이터를 수집하고, 처리하고, 분석하고, 조치할 수 있는 기능을 원합니다.

ANZ 응답자의 총 87%가 클라우드 및 보안 솔루션 공급업체를 평가할 때 실시간 애널리틱스 및 보고 기능을 매우 중요하거나 중요한 제품 기능으로 꼽았습니다.

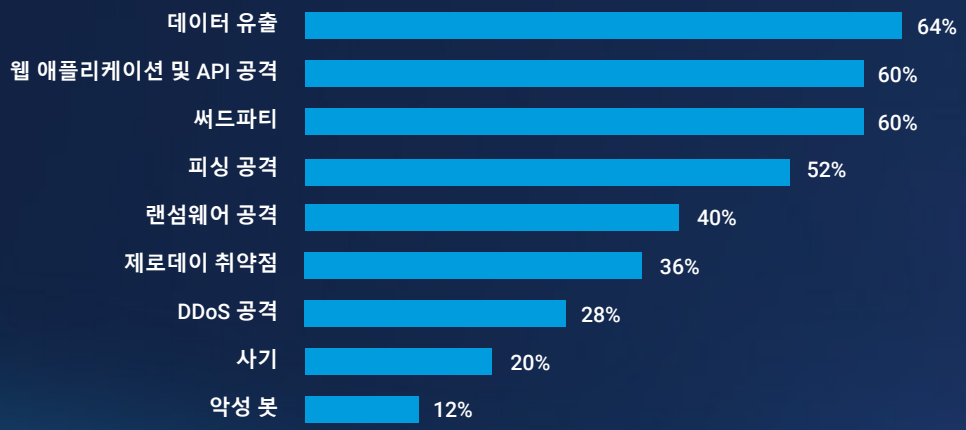
동시에, ANZ 디지털 네이티브들이 더 풍부한 고객 경험을 추구하면서 풍부한 개인 및 금융 데이터를 노리는 사이버 공격에 노출될 리스크도 있습니다.

Akamai의 금융 서비스 사이버 보안 보고서에 따르면 웹 애플리케이션 및 API 공격과 데이터 유출 및 탈취는 호주의 IT 리더들이 가장 우려하는 사이버 위협 중 하나였습니다.

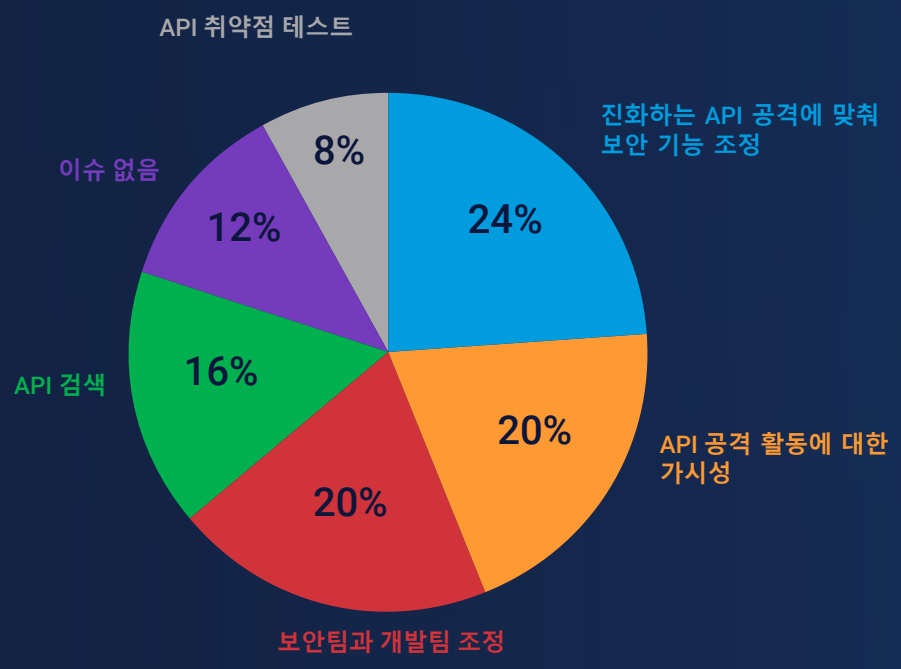
클라우드 및 보안 솔루션 공급업체를 평가할 때 다음 제품 기능을 얼마나 중요하게 생각하나요?



호주 IT 리더들이 가장 우려하는 주요 사이버 위협



API 보안과 관련해 가장 큰 이슈는 무엇인가요?



ANZ IT 리더들은 API 보안과 관련해 직면한 가장 큰 문제로 API 공격 활동에 대한 가시성 확보(20%)와 진화하는 API 공격에 맞게 보안 기능을 조정하는 것(24%)이라고 답한 만큼 보안 측면도 있습니다.

'볼 수 없는 것은 보호할 수 없다'는 격언이 있습니다. 실제 보유한 API의 수를 파악하지도 못하는 기업이 많기 때문에 리스크를 정량화하는 것은 어렵습니다.

API 활동에 대한 가시성을 높인 많은 기업이 놀라는 것 중 하나는 자신도 모르게 기업 환경에서 작동하는 섀도 엔드포인트의 수입니다.

그 결과, ANZ 응답자의 97%가 클라우드 및 보안 솔루션 공급업체를 평가할 때 API 보안을 매우 중요하거나 중요한 제품 기능으로 꼽았습니다.

실시간 애널리틱스 및 보고 기능을 통해 사이버 공격이 발생했을 때 더 빠르게 탐지하고 대응해 피해를 줄일 수 있기 때문입니다.

ASEAN 연결: 디지털 경제가 지역 성장을 견인

동남아시아는 세계에서 가장 빠르게 성장하는 인터넷 시장으로, 매일 12만 5000명의 신규 사용자가 인터넷에 접속합니다(출처: World Economic Forum).

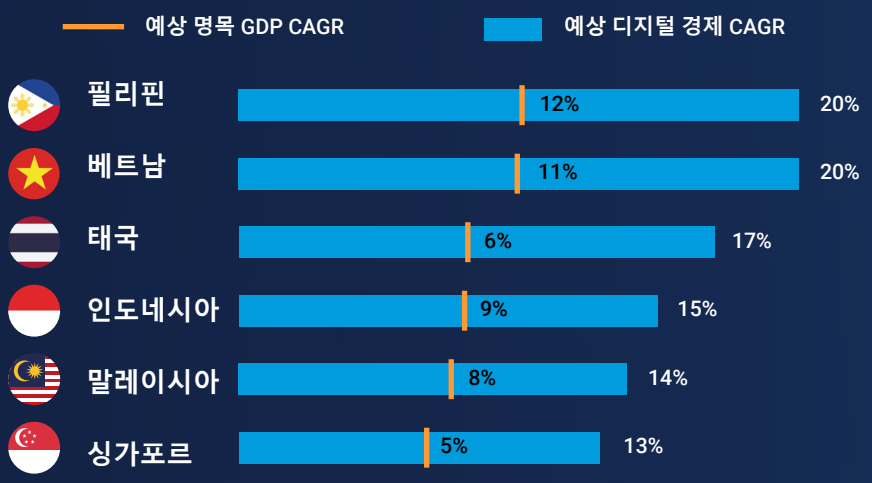
디지털 네이티브인 커넥티드 밀레니얼 세대와 Z 세대는 2030년까지 ASEAN 소비자의 75%, 인도네시아 소비자의 70%를 차지할 것으로 예상됩니다(출처: World Economic Forum).

실제로 디지털 경제의 총 시장 가치 성장률은 모든 ASEAN 국가의 GDP 성장률을 상회합니다(출처: e-conomy SEA 2023).

ASEAN 소비자들이 디지털 라이프를 빠르게 수용하고 있지만 ASEAN의 인프라는 여전히 뒤처져 있습니다. 디지털에 익숙한 젊은 세대는 서비스 가동 시간과 짧은 지연 시간에 대한 기대치가 높습니다.

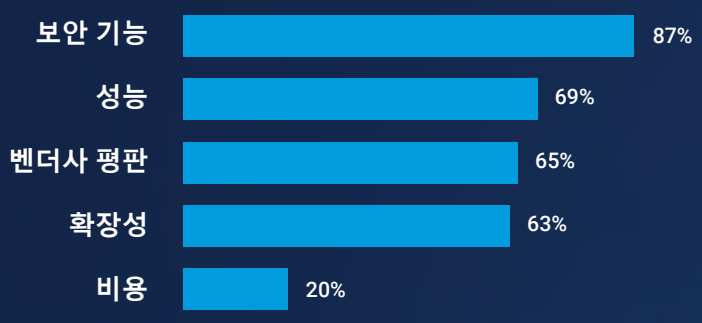
따라서 ASEAN 응답자들이 벤더사를 선택할 때 성능과 벤더사 평판이 각각 69%와 65%로 높은 순위를 차지한 것은 당연한 결과입니다.

디지털 경제 GMV 성장률과 GDP 성장률 비교(2023~2025년)



(출처: e-conomy SEA 2023, Google, Temasek, Bain & Company)

클라우드 벤더사 선택에 영향을 미치는 요인



동시에 네트워크 지연 시간은 여전히 ASEAN 지역 DNB의 문제입니다.

ASEAN 지역은 여전히 빠르고 안정적인 인터넷 연결과 도시 및 농촌 지역의 광범위한 전기 가용성을 보장해야 합니다. 1만 7508개의 섬으로 이루어진 인도네시아처럼 지리적으로 멀리 떨어져 있는 국가에서는 여전히 연결이 고르지 않습니다 (비공식적인 자료에 따르면 섬의 수가 2만 5000개에 가깝다고 합니다!).

응답자 3명 중 2명 이상이 기업의 클라우드 인프라 성능과 기능의 격차로 네트워크 지연 시간을 꼽았습니다.

지역 각국 정부는 지속적인 성장을 위해 연결성에 적극적으로 투자하고 있습니다.

인도네시아는 최근 Palapa Ring 프로젝트를 완료해 전국에 3만 5000km가 넘는 육상 및 해상 광섬유 케이블을 통해 가장 외진 지역까지 4G 인터넷 연결을 제공했습니다.

Akamai는 다른 공급업체보다 더 많은 지역에서 인프라를 제공하고, 코어와 엣지에서 클라우드 컴퓨팅 리소스를 제공하며, 지역별 선호도를 충족하도록 설계된 지연 시간이 짧고 데이터 집약적인 애플리케이션을 전 세계적으로 확장할 수 있는 역량을 갖추고 있습니다.

ASEAN에 중요한 제품 기능인 API 보안

ASEAN DNB는 API가 기업의 운영을 유지하고 다른 벤더사 및 생태계 파트너와의 협업을 촉진하는 데 도움이 된다는 사실을 뼈저리게 인식하고 있습니다.

ASEAN 응답자들은 지능형 API 공격을 인식하고 방어하는 데 있어 ANZ(69%)와 인도(91%)에 비해 가장 높은 자신감(99%)을 보였습니다.

실제로 ASEAN 응답자의 거의 모든 응답자(99%)가 API 보안을 매우 중요하거나 중요하다고 답했습니다.

그러나 API의 확산은 현실이며, 빠른 성장 속도는 가시성 부족을 의미하며, 이는 곧 보안 및 컴플라이언스 문제가 될 수 있습니다.

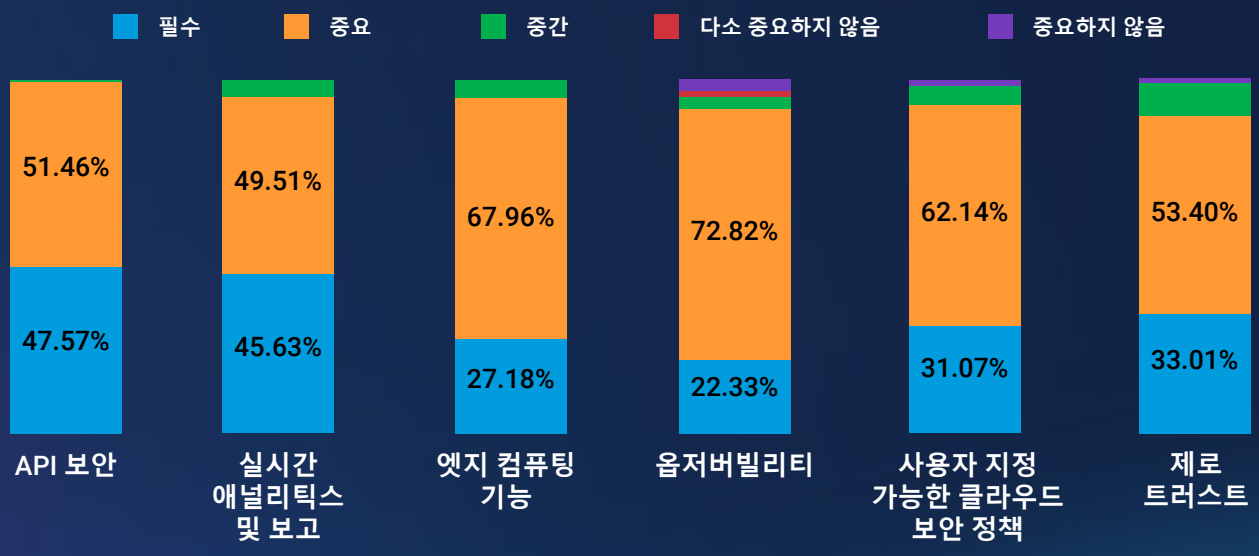
가시성은 API 보안의 중요한 측면입니다. 섀도 API나 악성 API와 같은 사각지대가 밝혀지면 보안팀은 이전에는 인식하지 못했던 취약점을 해결하기 시작할 수 있습니다.

따라서 실시간 애널리틱스 및 보고는 ASEAN 응답자의 95%가 매우 중요하거나 중요한 것으로 평가했습니다. 적절한 관리가 이루어지지 않으면 API는 데이터 유출, 컴플라이언스 위반, 거버넌스 부실의 주요 원인이 될 수 있습니다.

OWASP API 상위 10대 리스크와 같은 지능형 API 공격을 인식하고 방어하는 데 얼마나 자신 있나요?

지역	자신 있음/매우 자신 있음
ASEAN	99%
ANZ	69%
인도	91%

클라우드 및 보안 솔루션 공급업체를 평가할 때 다음 제품 기능을 얼마나 중요하게 생각하나요?



전례 없는 디지털 성장으로 인해 피싱 우려 증가

높은 디지털 도입률은 ASEAN DNB에 양날의 검이 되었습니다.

디지털 도입 속도가 워낙 빠르다 보니 온라인에서 정보를 교환할 때 개인정보 보호를 최우선으로 생각하지 않는 고객들이 많습니다. 피싱은 이메일 기반 공격에서 이제는 모바일 디바이스와 소셜 미디어를 포함한 공격으로 진화했습니다.

그 결과, 2023년에만 약 50만 건의 피싱 사례가 보고되는 등 APAC 지역에서 가장 높은 수준의 피싱이 발생하고 있습니다.

ASEAN 전역의 데이터 보호 및 개인정보 보호법은 빠르게 변화하는 디지털 커뮤니케이션 트렌드를 따라잡는 각국 정부의 능력에 따라 크게 달라집니다. 예를 들어, 문자 메시지의 클릭 가능한 링크는 여전히 인기 있는 사기 수법이지만, 많은 국가에서 이 일반적인 피싱 수법을 차단하기 위한 정책을 시행하고 있습니다.

설문 조사에 참여한 ASEAN DNB는 피싱 방지 기술에 대한 투자를 다른 지역보다 우선순위에 두고 있는 것으로 나타났습니다.

피싱은 사라지지 않을 것입니다.

생성형 AI의 등장으로 피싱 시도가 더욱 그럴듯해지고 범죄자들이 피해자를 표적으로 삼을 수 있는 옵션이 더 많아질 것입니다. 결국 피싱은 소프트웨어 취약점이나 시스템 악용이 아닌 인간의 본성에 초점을 맞추고 있습니다.

좋은 공격이 좋은 방어인 셈입니다. 피싱 시뮬레이션은 견고한 엔드포인트 보안과 결합해 피싱 게임에서 앞서 나가는 데 도움이 될 수 있습니다.

2023년 동남아시아에서 탐지 및 차단된 금융 피싱 건수

국가	금융 피싱 건수
필리핀	163,279
말레이시아	124,105
인도네시아	97,465
베트남	36,130
태국	25,227
싱가포르	9,502
총계:	455,708

출처: Kaspersky, 2024

다음 사이버 보안 투자 영역의 순위를 가장 중요한 것(위)부터 가장 중요하지 않은 것(아래)까지 표시하세요

1. 피싱 방지 기술
2. 최신 API 보안
3. 웹 애플리케이션 보안
4. 제로 트러스트 관련 기술
5. 분산 서비스 거부(DDoS) 방어

인도: 혁신을 위한 'I'

인도는 지난 10여 년간 혁신과 DNB의 진원지이자 클라우드 네이티브 아키텍처와 실험의 선도적인 원천이었습니다.

인도의 DNB는 성장과 혁신에 초점을 맞춰 왔으며, 클라우드 인프라 내 AI 통합률(98%)이 APAC 지역에서 가장 높고 거의 모든 DNB가 이미 클라우드를 사용하고 있거나 클라우드 도입을 모색하고 있습니다.

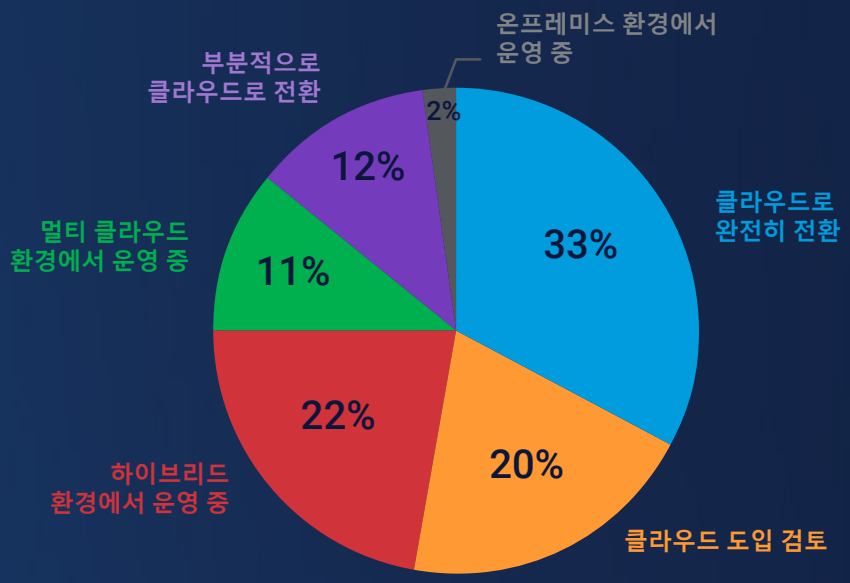
그러나 인도의 DNB가 성숙해지면서 보안과 비용 최적화에 초점을 맞추고 벤더사 선택을 면밀히 검토해 지속 가능한 성장을 모색하기 시작했습니다.

인도에서 초기 DNB의 고객은 바로 기술 기업인 경우가 많습니다.

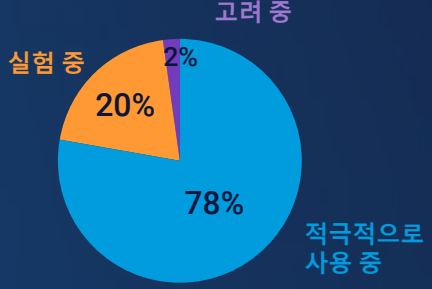
인도의 DNB는 API를 기반으로 고객의 데이터에 직접 접속하지 않고도 전 세계 기업에 기술 지원과 전문 지식을 빌려줄 수 있었습니다. 인도의 DNB는 일찍부터 전문 지식, API, 맞춤형 시스템에 투자했습니다.

이러한 기술적 우수성에 대한 깊은 유산을 바탕으로 인도의 디지털 네이티브는 다른 지역(ASEAN 2위, ANZ 4위)에 비해 벤더사의 성과를 더 중요하게 생각합니다.

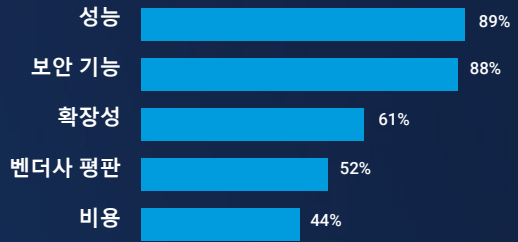
클라우드 도입 여정의 어느 단계에 있나요?



클라우드 인프라 내 AI 기술 통합의 현재 수준



클라우드 벤더사 선택에 영향을 미치는 요인



자체 전문성을 위한 'I'

인도의 디지털 네이티브는 다른 지역에 비해 클라우드 비용 관리에 대한 자체적인 접근 방식을 선호한다는 점도 눈에 띄는 특징입니다.

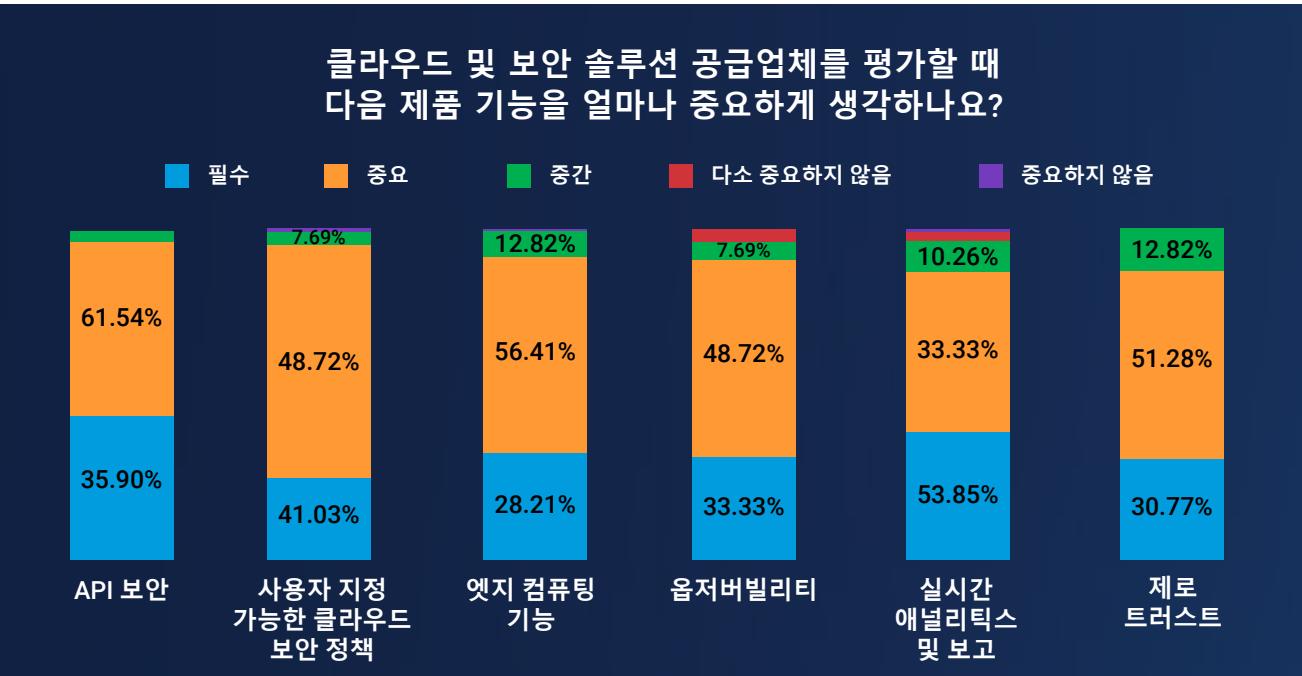
인도에서는 총 73%의 응답자가 클라우드 비용 관리 및 최적화를 위해 자체 솔루션을 사용한다고 답했는데, 이는 써드파티 툴을 선호하는 ASEAN(78%) 및 ANZ(69%) 응답자들과는 대조적인 결과입니다.

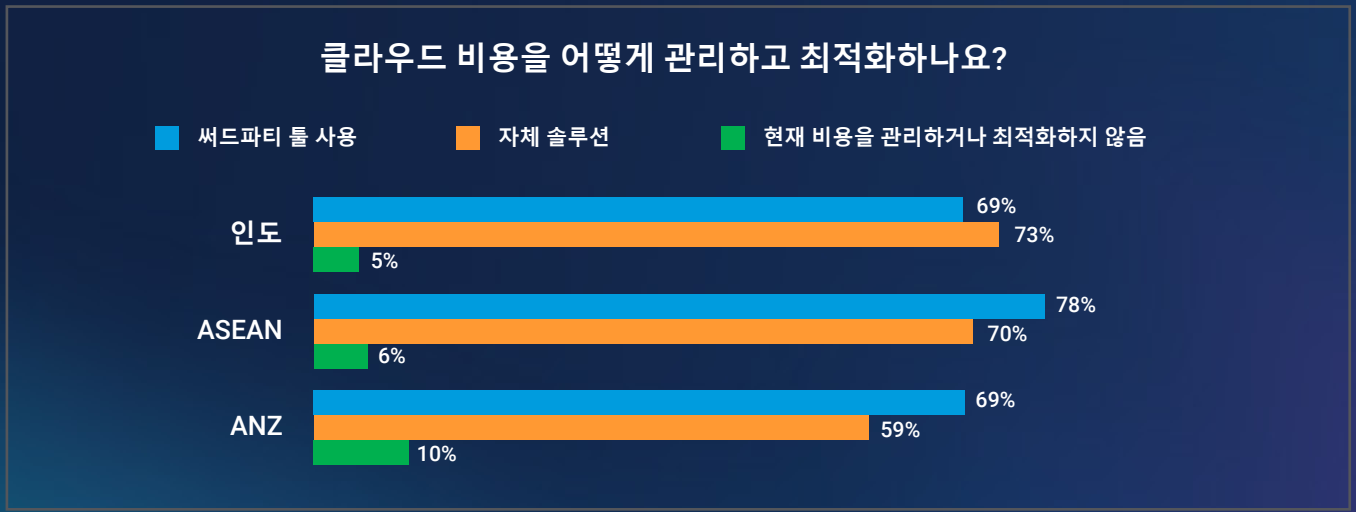
ANZ 응답자들이 써드파티 툴을 선호하는 이유는 현지 IT 기술 부족 때문일 수 있습니다.

예를 들어, ANZ는 매년 **5000명의 사이버 보안 인력**이 필요하지만, 현지 교육 시스템은 2026년까지 사이버 보안 전문 지식을 갖춘 인력을 약 2000명만 배출할 것으로 예상됩니다.

이와 대조적으로 인도에는 세계 기술 서비스 허브로서의 역사적 강점을 지닌 숙련된 인재가 풍부합니다.

현재 인도에 있는 **1600여 곳의 GCC(Global Capability Centre)**가 전 세계 기업에 기술 지원을 제공하고 있으며, 2030년까지 GCC가 약 2500개로 증가해 450만 명 이상의 직원을 고용하고 1000억 달러(USD)의 매출을 창출할 것으로 전망됩니다.





인도의 DNB를 취약점에 노출시키는 DIY

인도의 디지털 비즈니스가 기술 인프라를 관리하는 DIY 접근 방식은 기업이 확장되고 성숙해짐에 따라 취약점에 노출될 수 있습니다.

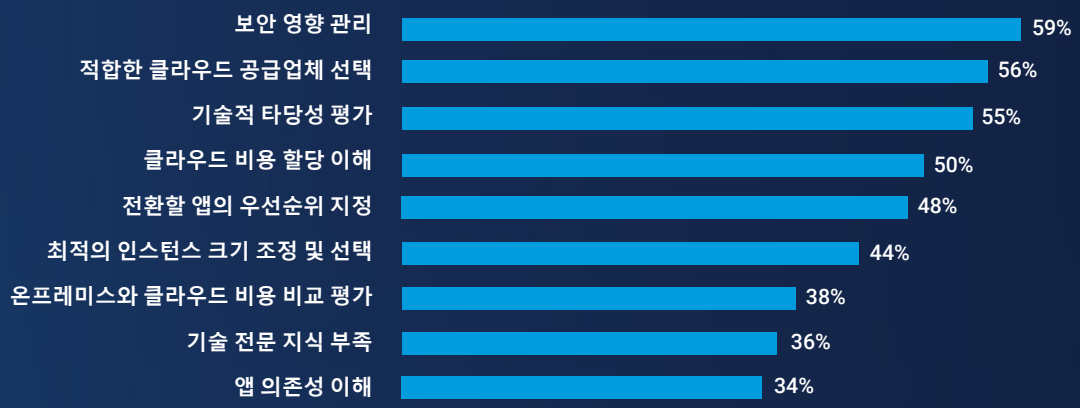
다양한 시스템을 여러 API와 통합하는 것은 이미 잠재적인 공격 표면을 증가시키고 있습니다. 이 문제는 클라우드에서 탄생해 온라인으로 서비스를 완전히 실행하는 기업의 경우 더 악화됩니다.

인도 응답자 5분의 3은 클라우드 인프라 및 전환과 관련된 보안 영향 관리를 가장 큰 문제로 꼽았습니다. 실제로 응답자의 4분의 3은 기업의 클라우드 인프라에서 가장 큰 격차로 보안을 꼽았습니다.

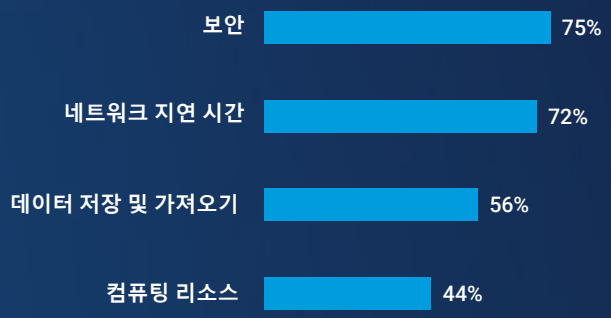
인도의 DNB는 기업의 취약점과 잠재적인 공격 시나리오를 파악하기 위해 양면을 모두 살펴볼 필요가 있습니다. 사이버 위협 환경은 빠르게 진화하고 있으며 새로운 공격 방법과 툴이 점점 더 정교해지고 있습니다.

인도의 DNB는 전문 기술을 보유한 써드파티와 협력해 기술 자급자족의 족쇄를 풀고 새로운 기술이 제공할 수 있는 효율성을 활용해야 할 수도 있습니다.

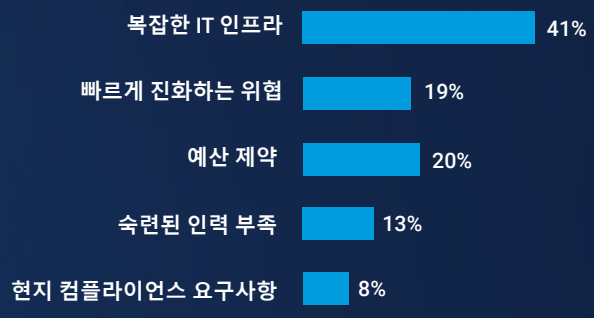
클라우드 전환과 관련해 가장 큰 어려움은 무엇인가요?



클라우드 성능에서 가장 큰 격차인 보안 및 네트워크 지연 시간



사이버 보안 체계를 가로막는 가장 큰 도전 과제



설문 조사 응답자의 상당수(41%)가 기업의 사이버 보안 체계를 강화하는 데 있어 가장 큰 과제로 복잡한 IT 인프라를 꼽았습니다. 이에 비해 ANZ는 응답자 중 36%가 복잡한 IT 인프라를 과제로 꼽았습니다.

특히 인도와 같이 빠르게 성장하는 시장이자 지역 최고의 사이버 공격 표적이 되는 국가에서는 연중무휴 24시간 전문가의 도움 없이 자체적으로 사이버 보안을 관리하려는 시도는 더 이상 실행 가능한 옵션이 아닐 수 있습니다.

이는 인도의 기술 인프라 퍼즐의 핵심 조각이 될 것입니다.

Akamai의 분산형 클라우드 플랫폼은 개발자가 컴퓨팅 리소스를 배포하고 확장할 위치를 제어할 수 있도록 지원합니다. 개발자는 데이터를 캡처, 처리, 관리할 위치를 정의할 수 있는 권한과 유연성을 갖습니다.

함께 더 강하게

이 설문 조사는 더 풍부하고 빠른 고객 경험을 추구하기 위해 AI, 클라우드 컴퓨팅, 빅 데이터를 도입하는 아시아 디지털 네이티브의 기술 리더들이 직면한 과제에 대한 획기적인 인사이트를 제공합니다.

하지만 모든 디지털 네이티브를 일괄적으로 정의하는 것은 순진한 생각일 수 있습니다.

이 리서치는 APAC 지역의 다양한 지역과 업계에서 디지털 네이티브의 클라우드 및 API 성숙도 및 사이버 보안 체계의 미묘한 차이를 구분합니다.

예를 들어, 규제가 심한 업계나 지역에 속한 기업들은 보안 및 개인정보 보호와 사용자 경험의 균형을 맞추고자 합니다.

밀리초가 중요한 디지털 네이티브는 지역 최적화를 통해 개인화된 경험을 제공하는 최첨단 기능이 무엇보다 중요합니다.

클라우드 네이티브 아키텍처는 디지털 네이티브가 확장 및 축소하고 풍부하고 개인화된 경험을 제공할 수 있도록 지원하는 잘 설계된 API와 엔드포인트의 장점을 활용합니다.

대부분의 기업은 클라우드를 효과적으로 잠그는 데 필요한 기본 가시성 및 보안 제어 기능이 부족합니다. 퍼블릭 및 멀티클라우드 환경의 보안을 유지하려면 보안 담당자가 환경 내에서 어떤 애플리케이션, 워크로드, 트래픽 흐름이 이동하는지 확인할 수 있어야 합니다.

Akamai는 최종 사용자와 더 가까운 곳에서 실행되어야 하는 고성능 워크로드에 이상적인 분산형, 저지연, 글로벌 확장성 설계를 강조하면서 기업의 클라우드 아키텍처 접근 방식을 변화시키고 있습니다.

전 세계 접근하기 어려운 시장에 핵심 컴퓨팅 지역을 구축하기 위해 노력한 결과, 131개국 4100개 이상의 엣지 PoP에 걸쳐 대규모로 분산된 공간을 확보할 수 있었습니다.

전 세계 대표 기업들이 디지털 경험의 구축, 전송, 보안을 위해 Akamai를 선택하는 이유를 알아보세요.

방법론

이 설문 조사는 지역 IT 리더들을 대상으로 한 현장 조사를 통해 이러한 인사이트를 발견했습니다.
설문 조사는 2024년 3월~5월에 실시했습니다.

이유

이 보고서는 디지털 네이티브 기업이 향후 트렌드와 위협을 어떻게 바라보는지 심층적으로 살펴봅니다.
이러한 결과는 현재의 현장 인사이트를 바탕으로 구축된 귀중한 벤치마크 역할을 합니다.

대상

다음 업계의 최고 정보 책임자, 최고 기술 책임자,
IT 책임자, 부사장:

- 항공
- 미디어, 방송, 출판
- 이커머스, 인터넷
- 게이밍
- 호텔 및 관광업
- 정보 기술
- 리테일, 도매

국가

- 호주
- 뉴질랜드
- 인도
- 싱가포르
- 인도네시아
- 태국
- 말레이시아
- 베트남