디지털서비스

이슈리포트

Digitalservice Issue Report

2025 클라우드 트렌드

NIA 한국지능정보사회진흥원 디지털서비스 이용지원시스템

2025 Vol. 01

디지털서비스 이슈리포트

CONTENTS

Digitalservice Issue Report

디지털서비스 이슈리포트

01 2025 클라우드 트렌드

| 윤대균 아주대학교

개요

여러 전문 매체에서 2025년 클라우드 전망을 발표했다. 매체의 성격에 따라 다른 관점에서 트렌드 전망 또는 주요 클라우드 관련 이슈를 발표하기도 하지만 대체로 많은 항목이 중복되기도 한다. 특히 기술관점에서의 트렌드는 유사한 전망을 하는 경우가 많다. 다른 매체의 발표 내용을 그대로 옮겨 놓은 경우도 다수 있기에 이는 우선 배제하고 다음과 같은 8개 매체의 내용을 살펴보았다. 우선 각 매체에서 제시하는 2025년에 주목할 클라우드 전망을 요약하면 다음과 같다.

매체	클라우드 트렌드
어센드 클라우드 솔루션즈 (Ascend Cloud Solutions)	엣지컴퓨팅, 하이브리드/멀티클라우드 도입, AI 및 머신러닝 통합, 강화된 보안 및 규정 준수, 서버리스 컴퓨팅 성장 https://www.ascendcloudsolutions.com/the-cloud-in-2025-a-meta-analysis-of-trends-and-predictions
포레스터	통합 RAG 서비스의 부상, 프라이빗 클라우드 시장에서의 VMware 대체, 클라우드 네이티브 플랫폼에서의 보안 역량 압박 https://www.forrester.com/blogs/predictions-2025-cloud/
인포메이션 위크	멀티클라우드/하이브리드 클라우드 도입 확대, 클라우드 보안에 대한 CISO 역할 확대, 클라우드 비용 증가, 더욱 탄력을 받게 될 랜딩존(Landing Zone), 디지털 트윈을 활용한 사이버보안 회복력, 우주로 확대되는 사이버 공간 https://www.informationweek.com/it-infrastructure/6-cloud-trends-to-watch-in-2025
CNCF	AI로 무장한 클라우드, 엣지와 클라우드에서의 AI 통합, 보다 유연한 하이브리드/멀티클라우드 전략, 서버리스 컴퓨팅에 기반 확장 가능한 솔루션 서비스로서의 퀀텀컴퓨팅, 데브엣지옵스(DevEdgeOps) https://www.cncf.io/blog/2024/12/03/top-6-cloud-computing-trends-for-2025/
링크드인 - 윌 켈리	일부 영역에서의 하이퍼 스케일 클라우드 지배력 쇠퇴, 클라우드 비용의 투명성 촉진, AI 인프라에 대한 클라우드 공급업체의 시장 지배력 강화, 클라우드 서비스 제공자의 핵심 서비스로서 핀옵스(FinOps) 내장, https://www.linkedin.com/pulse/cloud-computing-predictions-2025-opportunities-challenges-will-kelly-hfb9e

매체	클라우드 트렌드
포브스	클라우드 컴퓨팅의 핵심 두뇌로 자리 잡는 AI, 클라우드와 엣지컴퓨팅의 경계 소멸, 클라우드를 통한 퀀텀컴퓨팅의 주류시장 진입, 보편화되는 하이브리드/멀티클라우드, 생성형AI로 촉진되는 클라우드 개발 혁신, 수퍼 클라우드가 궁극의 데이터 패브릭으로 등장, 지속가능성이 클라우드 필수로 자리매김 https://www.forbes.com/sites/bernardmarr/2024/11/04/the-7-revolutionary-cloud-computing-trends-that-will-define-business-success-in-2025/
MelonLeaf	하이브리드 클라우드 모델, 엣지컴퓨팅, AI 기반 클라우드 서비스, 지속가능성, 서버리스 컴퓨팅, 보안 및 규정 준수 강화, 버티컬 클라우드 솔루션 확대, 클라우드 네이티브 컴퓨팅 보편화, 클라우드와 5G 통합, 원격 근무를 위한 협력 도구 https://melonleaf.com/blog/future-of-cloud-computing-2025-trends-predictions/
SecureKloud	멀티클라우드/하이브리드 클라우드, 서버리스 컴퓨팅, 데이터 거버넌스 및 프라이버시, 컨테이너화 및 마이크로서비스, 엣지 컴퓨팅, AI 및 머신러닝, 퀀텀 컴퓨팅, 클라우드 네이티브 애플리케이션, 개발도상국에서의 클라우드 도입 확산 https://www.securekloud.com/blog/the-future-of-cloud-computing-trends-and-predictions-for-2025/

가장 비중 있게 많이 언급되는 것은 역시 AI이다. 그 밖에 공통으로 많이 등장하는 것은 멀티클라우드 및 하이브리드 클라우드, 엣지컴퓨팅, 클라우드 네이티브 컴퓨팅, 서버리스 컴퓨팅 등이며, 퀀텀 컴퓨팅 서비스에 대해서도 여러 군데에서 언급하고 있다. 그리고, 사이버 보안, 클라우드 비용 최적화, 지속가능성에 관해서도 관심 있게 지켜봐야 할 트렌드로 들고 있다. 이제 이 각각에 대해 좀 더 살펴보도록 하겠다.

주요 클라우드 이슈별 2025년 전망

1. AI와 클라우드 컴퓨팅

AI는 2025년 클라우드 컴퓨팅 시장에서 가장 중요한 트렌드 세터로 자리매김할 것으로 전망된다. 클라우드 컴퓨팅 제공자의 입장에선 AI 기반 다양한 서비스를 제공하는 것뿐만 아니라, 클라우드 운영의 모든 측면을 최적화하는 핵심 동력으로 AI를 적극 활용하게 될 것이다. 우선 클라우드 플랫폼의 AI 내재화가 본격화되며 클라우드 제공업체들은 AI와 ML을 자사 플랫폼의 핵심 아키텍처에 더욱 깊이

통합할 것으로 예상된다. 이를 통해 데이터 분석, 예측 모델링, 자동화 기능이 크게 강화되고, 특히 AI 에이전트를 활용하여 패치 관리, 스케일링과 같은 일상적인 작업의 자동화가 더욱 고도화될 전망이다. 이는 전례 없는 효율성, 비용 절감, 성능 향상을 가져올 것으로 기대한다.

RAG(Retrieval-Augmented Generation) 서비스의 부상도 눈여겨볼 필요가 있다. 주요 클라우드 사업자들은 생성형 AI의 정확성 향상을 위해 RAG 관련 솔루션 출시에 많은 노력을 기울일 것으로 예상한다. 이는 기존 파운데이션 모델의 한계인 환각과 정확성 문제를 보완하기 위한 전략으로, 기업의 주요 업무에 생성형 AI를 적용하기 위한 필수 요구 사항으로 대두되고 있다.

결과적으로 하이퍼스케일러의 AI 시장 지배력이 강화될 전망이다. 즉, AWS, 애저, 구글 클라우드 등 주요 클라우드 서비스 제공업체들의 AI 시장 지배력이 높아질 것이다. 왜냐하면, 이들은 이미 AI 생태계의 근간이 되는 인프라, GPU, 머신러닝 프레임워크를 보유하고 있기 때문이다. 또한 곧 닥칠 것으로 예견되는 AI 스타트업 생태계의 구조조정으로 인해 이들의 시장 지배력은 더욱 공고해질 수 있다.

다만, 이러한 변화는 혁신 저해와 벤더 종속성 심화라는 위험도 동반한다. 기업들은 하이퍼스케일러의 AI 도구가 제공하는 이점과 벤더 종속의 위험 사이에서 균형을 찾아야 하는 과제를 안게 될 것이다.

2. 하이브리드/멀티클라우드

2025년에는 기업들의 클라우드 전략이 더욱 정교화되고 다각화될 것으로 전망된다. 특히 단일 클라우드 공급자에 의존하는 방식에서 벗어나, 하이브리드 및 멀티클라우드 환경을 적극적으로 도입하는 추세가 강화될 것이다. 이러한 추세는 이미 수년 전부터 계속됐으나, 규제 준수 및 보안, 그리고 비용 최적화 관점에서 2025년에는 더욱 가속화될 것이다. 특히 의료, 금융, 정부 등 규제가 엄격하고 데이터 주권이 중요한 산업에서 더욱 두드러질 것이다.

멀티클라우드 전략의 고도화를 위해 기업들은 여러 클라우드 제공업체를 활용하여 위험 분산과 성능 최적화를 추구할 것이다. 특히 AI 워크로드의 경우, 각 클라우드 제공업체의 강점을 활용하여 분산 학습을 구현하는 방식이 증가할 것이다. 또한, 클라우드 제공업체 간의 데이터 이전 비용이 감소하면서, 워크로드 이동이 더욱 쉬워질 것이다.

아울러 온프레미스와 프라이빗 클라우드의 재부상을 예상할 수 있다. 데이터 주권, 비용, 보안 등의 이슈로 인해 온프레미스 컴퓨팅에 대한 관심이 다시 높아질 것으로 전망되기 때문이다. 시장에서는

그동안 프라이빗 클라우드 솔루션의 주류였던 VMware의 가격 정책 변화로 인해 Nutanix나 오픈스택 같은 대안적인 프라이빗 클라우드 솔루션이 주목받을 것으로 전망하기도 한다.

주요 퍼블릭 클라우드 제공업체들도 이에 대한 대응으로 은 프라이빗 클라우드 투자를 확대할 것이다. 특히, 클라우드 간 상호운용성을 강화하여, 데이터 이동 없이도 여러 클라우드 환경에서 분석과 활용이 가능한 기능을 다양하게 제공할 것이다.

3. 엣지 컴퓨팅

엣지컴퓨팅은 2025년에 클라우드 인프라 관점에서 더욱 많은 관심을 끌 것이다. 특히 엣지와 클라우드 컴퓨팅 간의 경계가 허물어지면서, 새로운 형태의 컴퓨팅 환경이 조성될 것으로 예측된다.

엣지-클라우드 통합이 가속화됨으로써 엣지와 클라우드 컴퓨팅 간의 인위적 경계가 사라지고, 원활한(Seamless) 컴퓨팅 패브릭이 형성된다. AI 워크로드가 엣지와 클라우드 사이를 동적으로 이동하면서, 각각의 장점을 최대한 활용할 수 있게 된다. 예를 들어, 복잡한 AI 모델 학습은 클라우드에서, 실시간 추론은 엣지에서 처리하는 방식이 보편화된다.

데이터 소스 근처에서 처리가 이루어짐으로써 지연시간이 최소화되어 전반적인 성능과 효율이 향상된다. 따라서, 대역폭 사용이 최적화되고 실시간 처리가 가능해진다. 차세대 엣지 플랫폼은 멀티클라우드와 엣지 환경 전반에 걸친 종합적인 자동화 솔루션을 제공하게 될 것이다.

주요 활용 예는 다음과 같다.

- 자율주행차: 로컬에서의 즉각적인 의사결정과 클라우드 기반 인텔리전스를 결합
- 로봇 수술: 엣지 컴퓨팅의 정밀성과 클라우드의 딥러닝 능력을 통합
- 스마트 제조: 실시간 데이터 처리를 통한 생산 공정 최적화를 실현
- 의료 및 소매 분야의 IoT 기기: 신속한 데이터 처리와 의사결정을 지원

4. 클라우드 네이티브 컴퓨팅

2025년에는 클라우드 네이티브 컴퓨팅 기반의 소프트웨어 개발이 주도적인 위치를 차지할 것이다. 기업은 클라우드 환경을 활용하여 확장 가능하고 민첩하며 비용 효율적인 방식으로 애플리케이션을 구축하고 배포하는 방향으로 나아가고 있다.

마이크로서비스와 컨테이너 기반의 클라우드 네이티브 아키텍처가 보편화되며, 분산 운영을 통해 시스템 복원력이 향상된다. 또한 인프라 종속성이 감소하여 유연한 개발이 가능해진다. 개발 프로세스 측면에서는 애플리케이션 개발 및 배포 주기가 단축되며, 리소스 활용 또한 최적화할 수 있다. 이에 애플리케이션 및 서비스 확장이 용이해진다.

이러한 변화는 기업들이 더 효율적이고 혁신적인 방식으로 애플리케이션을 개발하고 운영할 수 있는 원동력이 될 것이다. 따라서, 클라우드 네이티브 접근 방식은 기업의 디지털 전환과 경쟁력 강화에 핵심적인 요소가 될 것으로 예상된다. 하지만 기업의 입장에서는 이러한 새로운 패러다임 확대로 인한 복잡해진 사이버 보안 위협에 대응해야 한다. 이는 뒤에서 언급하겠다.

5. 서버리스 컴퓨팅

서버리스 컴퓨팅은 개발자들이 기반 인프라에 대한 걱정 없이 애플리케이션을 구축하고 배포할 수 있게 하는 새로운 패러다임이 되었다. 2025년에는 애플리케이션 개발 분야에서 더욱 인기 있는 트렌드로 자리 잡을 것으로 전망된다.

서버리스 컴퓨팅의 주요 이점은 다음과 같이 정리할 수 있다.

- 확장성: 수요에 따라 자동으로 리소스가 조정
- 비용 효율성: 실제 사용량에 기반한 과금으로 비용 최적화
- 혁신 촉진: 인프라 관리 부담 없이 새로운 솔루션 개발에 집중
- 민첩성: 빠른 서비스 배포와 변경이 가능

서버리스 컴퓨팅은 스타트업부터 대기업까지 모든 규모의 기업에서 활용할 수 있으며 클라우드 네이티브 컴퓨팅과 함께 향후 몇 년간 다양한 산업 전반에 걸쳐 개발 혁신을 주도할 것이다. 이는 기업의 경쟁력 강화에 크게 기여하게 될 것이다.

6. 퀀텀 컴퓨팅

2025년에는 퀀텀 컴퓨팅이 실험실 수준을 넘어 비즈니스 주류로 진입할 것으로 조심스럽게 전망하는 분위기이다. 특히 클라우드 서비스를 통해 이의 실현이 가능해질 것으로 보고 있다. IBM, 구글, 마이크로소프트, 아마존 등 주요 기업이 주도하여 클라우드 기반 퀀텀 컴퓨팅 서비스가 확산될 것으로 예상되며 이는 퀀텀 컴퓨팅 접근성을 높일 수 있을 것으로 기대한다. 즉 고가의 하드웨어 투자 없이도

클라우드를 통해 퀀텀 컴퓨팅 능력을 활용할 수 있게 되며, 모든 규모의 조직이 퀀텀 컴퓨팅 기술을 이용할 수 있게 되는 것이다.

신약 개발, 더욱 강력한 암호화 등 기존 컴퓨터로는 어려웠던 복잡한 문제의 해결이 가능해질 것으로 기대 하에 퀀텀 데이터 센터에 대한 퍼블릭 클라우드 제공업체들이 투자를 확대하고 있다. 여전히 실제 활용할 수 있는 수준의 안정성 확보는 과제로 남아있지만, 구글의 새로운 퀀텀 칩 개발 등 기술적 진보가 지속해서 이루어지고 있다는 것에 희망을 걸고 있다.

이러한 발전은 퀀텀 컴퓨팅이 클라우드를 통해 더욱 접근 가능해지고, 이전에는 불가능했던 혁신을 가능하게 할 것으로 전망된다. 다만, 실용적인 수준의 안정성 확보까지는 아직 시간이 필요하다는 것이 일반적인 견해다.

7. 클라우드 보안

AI 확산, 클라우드 네이티브 및 서버리스 컴퓨팅 보편화 등 클라우드 컴퓨팅 트렌드의 변화로 인해 사이버 위협 유형이 다양해지고 더욱 고도화되고 있으며 또한 공격표면(Attack Surface)도 넓어졌다. 이에 대응하는 2025년에 주목할 만한 클라우드 보안 트렌드는 다음과 같다.

- AI와 머신러닝 기반의 고도화된 보안 솔루션 확산
- 제로 트러스트 보안 모델이 표준으로 정착
- 엔드투엔드 암호화와 블록체인 기술을 통한 데이터 보호 강화
- 컴플라이언스 자동화 도구를 활용하여 진화하는 규제 환경에 대응

이에 보다 전문적인 보안기술 및 플랫폼에 대한 요구 사항이 전보다 크게 늘어날 것이다. 글로벌 네트워크와 데이터센터를 운영하는 대형 클라우드 업체(Hyperscaler)에서 자체적으로 제공하는 네이티브 보안 기능보다는 시스코, Fortinet, 팔로 알토 네트웍스, Wiz 등 전문 보안업체들의 솔루션에 더 많이 의존하게 되며, 따라서 이들 전문 보안업체의 영향력이 더욱 커질 것이다. 포레스터는 2025년까지 전체 클라우드 고객의 60% 미만이 하이퍼 스케일러의 자체 보안 기능을 선호할 것으로 예측한다. 이들 전문 보안업체는 클라우드 보안 태세 관리[1], 권한 관리, 인프라 코드 스캐닝, 컨테이너 보안 등 종합적인 기능을 제공한다.

1) 보안 태세(Security Posture): 조직의 전반적인 보안 상태와 보안 위험에 대응할 수 있는 능력을 의미하는 용어로, 보안 정책, 보안 통제, 보안 도구 및 프로세스 등이 포함

AI를 활용한 사이버 공격에는 AI 기반 방어 체계 구축을 통해 대응하는 사례가 늘 것이다. 클라우드 기반 디지털 트윈을 활용한 '랜섬웨어 워게임' 시뮬레이션을 통해 엣지에서 코어, 클라우드까지 전체 인프라에 대한 공격 시나리오 테스트가 이루어진다. 이에 따른 SecOps팀의 역할도 다소 변화하게 될 것이다.

이 밖에도 데이터 거버넌스는 더욱 강화되어 GDPR, HIPAA 등 산업 규제 준수를 위한 투자가 지속되며, 이에 데이터 보안과 사용자 프라이버시 보호가 클라우드 환경 신뢰도 향상의 핵심 요소가 될 것이다. 규제 준수를 위한 고도화된 보안 정책 및 기술에 대한 투자도 확대될 전망이다.

8. 클라우드 비용 최적화

2025년에는 대부분 기업에서 AI 도입으로 인한 클라우드 자원 수요 및 비용 증가가 예상되며 이에 따른 비용 최적화 전략의 수정이 필요하게 된다. 단기적 비용 절감에서 장기적이고 지속 가능한 최적화 전략으로의 전환이 바람직하며 이를 위한 클라우드 비용 관리의 투명성과 책임성을 강화해야 한다.

특히 핀옵스(FinOps)[2]의 중요성이 대두되고 있으며, 전담 핀옵스팀 구성이 필수적인 요소로 자리 잡고 있다. 이에 핀옵스 시장도 2023년 55억 달러에서 2025년까지 연평균 34.8% 성장할 것이라 한다.[3] 핀옵스팀의 역할도 사후 비용 검토에서 개발 및 배포 단계의 사전 비용 가이드 역할 비중을 높여야 한다. 이렇게 함으로써 데브옵스팀과 핀옵스의 협업을 통한 공동 책임 문화가 자연스럽게 형성될 수 있다.

비용 최적화 지표도 진화하여야 한다. 기존의 애플리케이션별 비용 추적에서 더 포괄적인 지표로 발전하여야 하며, 여기에는 애플리케이션 운영에 필요한 직접 비용뿐만 아니라, 전반적인 엔지니어링 비용, 비즈니스 가치 연계성, 그리고 좀 더 세분화된 비용 가시성이 포함되어야 한다. 궁극적으로는 탄소 발자국 최적화와 연계된 지표가 중요해질 것이다.

9. 지속가능성(Sustainability)

2025년 클라우드 컴퓨팅에서 지속가능성과 그린 컴퓨팅은 더 이상 선택이 아닌 필수 요소로 자리 잡고 있다. 클라우드 제공업체들은 탄소 배출량 감소와 친환경 에너지 활용에 큰 비중을 두고 있으며, 이는 단순한 기업의 사회적 책임을 넘어 비즈니스 생존의 핵심 요소가 되고 있다.

---

2) FinOps(Financial Operations): 클라우드 재무 관리 방법론이자 실무 프레임워크를 의미하며 비즈니스팀, 개발팀, 운영팀 간의 협업을 촉진하여 클라우드 비용을 효과적으로 관리하고 최적화하는 것을 목표로 한다,

3) CloudKeeper, “Top Emerging Cloud Computing Trends & Statistics for 2025 & Beyond”, Dec. 6, 2024

특히 AI 기술의 발전과 클라우드 컴퓨팅 사용량 증가로 인해 2030년까지 데이터 센터의 전력 수요가 160% 증가할 것이라 예상한다. 이에 따라 탄소 배출량은 2030년까지 약 25억 미터톤에 달할 것으로 전망된다.[4] 이러한 환경적 도전과제에 대응하기 위해 클라우드 업계는 다양한 친환경 솔루션을 개발하고 도입하고 있다.

EU의 에너지 효율성 지침과 같은 규제 강화로 인해 데이터 센터 운영자들은 에너지 사용량을 의무적으로 보고해야 한다. 이에 따라 데이터 센터는 강력한 데이터 분석에 바탕을 둔 에너지 소비 최적화를 위해 노력하고 있다.

핀옵스는 이러한 지속가능성 목표 달성을 위한 핵심 도구로 부상하고 있다. 이는 클라우드 기술을 통한 비즈니스 가치 극대화를 돕는 운영 프레임워크로, 비용 최적화와 효율적인 클라우드 사용을 통해 에너지 소비 절감에 기여한다. 클라우드 지출 절감은 곧 탄소 발자국 감소로 이어져, 비용 효율성과 환경적 책임이 동시에 달성되는 효과를 가져온다.

기업은 이러한 변화에 빠르게 적응하여 혁신과 경쟁력을 확보해야 하며, 클라우드 기반의 지속 가능한 비즈니스 모델을 구축하는 것이 향후 성공의 핵심 요소가 될 것이다.

맺으며

이상 여러 이슈별 2025년 또는 그 이후에 대해 전망해 보았지만, 이 중에서도 2025년에 가장 중요한 핵심 이슈 3개를 뽑으라면 AI, 비용 최적화, 그리고 보안을 들겠다. 사실 앞서 열거한 모든 이슈가 서로 밀접하게 연결되어 있고, 이러한 변화의 트렌드를 더욱 두드러지게 하는 가장 중요한 핵심 이슈는 AI이다. 특히, 자체적으로 프론티어 모델을 구축해 활용할 여력이 없는 대다수 기업은 당장 클라우드 비용의 부담으로 인한 AI 기술 도입에 뒤처질 가능성이 높다. 엣지컴퓨팅 또는 온-디바이스 AI가 특히 관심을 받는 이유도 이러한 비용 이슈와 무관하지 않다.

전 세계 퍼블릭 클라우드 시장은 계속 커지고 있지만, 특정 산업 분야에서는 대형 클라우드 서비스 제공 업체(AWS, 애저, 구글 클라우드)의 지배력이 감소할 것으로 전망하는 측도 있다. 정부, 의료, 금융 서비스 분야에서는 규제 준수, 데이터 주권, 특수 요구 사항으로 인해 지역 기반 또는 '틈새 클라우드 제공 업체'를 선호할 수 있다는 것이다. AI의 경우 단일 대형 서비스보다는 전문화된 여러 서비스

4) SoftwareOne, "4 big-picture trends influencing cloud in 2025", Jan 10, 2025

제공자에 의해 시장이 재편될 수 있으며, 특히 데이터 주권, 소버린 클라우드/AI 관점에서 유럽 및 아시아에서 이런 경향이 두드러질 가능성이 높다. 이러한 변화는 클라우드 시장이 더욱 다양하고 전문화된 형태로 발전하고 있음을 시사하며, 2025년 클라우드 시장에서 이러한 변화를 본격적으로 체감할 수 있을 것으로 예상한다. 기업은 이러한 변화에 대응하여 더욱 전략적인 클라우드 선택과 관리가 필요할 것으로 보인다.

02 유럽의 소버린 엣지 클라우드 Virt8ra 출시

| 한상기 테크프론티어 대표

8개 유럽 기술 기관으로 구성된 컨소시엄이 힘을 합쳐 Virt8ra라는 브랜드의 소버린 엣지 클라우드 플랫폼을 개발했다. 이는 유럽의 디지털 자율성과 클라우드 역량을 강화하는 것이 목표이다.[5] Virt8ra는 '버토라'라고 읽는다.

Virt8ra 플랫폼 개발에 참여한 기업은 Arsys, BIT, 그단스크 공과 대학, Infobip, Ionos, Kontron, Mondragon Corporation, Oktawave 등 8개 기업이며 스페인의 오픈소스 기업인 오픈네뷸라 시스템즈(OpenNebular Systems)가 주도한다. 이 이니셔티브는 많은 클라우드 공급자를 연결하는 유연한 인프라를 구축하는 것을 목표로 하는데, 초기 출시는 크로아티아, 독일, 네덜란드, 폴란드, 슬로베니아, 스페인 등 6개 EU 회원국을 대상으로 한다.

이 이니셔티브는 차세대 클라우드 인프라 및 서비스에 대한 공통 유럽 이익의 중요 프로젝트(IPCEI-CIS)에 의해 추진하는 것으로, 2023년 12월 유럽 위원회가 승인했고 12개 EU 회원국과 공공 및 민간 소스에서 30억 유로 이상의 자금을 지원한다.

IPCEI-CIS는 유럽에서 제작된 오픈소스 기술의 개발을 촉진함으로써 "근접 클라우드" 서비스 제공업체의 등장을 가속화하고 유럽의 빅 테크 공급업체와 하이퍼 스케일러에 대한 산업 의존도를 줄이는 것을 목표로 한다. 30억 유로가 투입되는 이 전략적 프로젝트는 12개 EU 회원국의 100개 이상의 유럽 기업에서 시행되고 있으며 EU 역사상 가장 큰 오픈소스 프로젝트이다. 오픈네뷸라 시스템즈는 IPCEI-CIS 산업 촉진 그룹의 의장이다.

5) CLOUDTECH, "Europe unites to launch its first sovereign edge cloud," Jan 21, 2025

프로젝트의 핵심은 30개 이상의 유럽 기업 네트워크에서 개발한 가상화를 위한 오픈소스 소프트웨어 스택이다. 초점은 클라우드-엣지 연속체라고 알려진 클라우드와 엣지 컴퓨팅의 증가하는 통합을 관리하도록 맞춤화된 공급업체 중립적 프레임워크를 만드는 것이다.

좀 더 설명하면 오픈네뷸라에서 조정하는 virt8ra 이니셔티브는 가상화에 대한 IPCEI-CIS 통합 클러스터의 주요 성과물이며, 주요 목표는 다중 공급자 클라우드 엣지 인프라에서 고급 관리 및 오케스트레이션 기능을 지원하기 위한 아키텍처 모델과 통합 프레임워크를 정의하는 것이다.[6)]

Virt8ra에 기여하는 각 기업의 역할을 보면, Ionos는 독일 시설에서 제공하는 베어 메탈 서버, 슬로베니아의 Kontron에서 제공하는 클라우드 리소스, 스페인 바스크 지방의 Mondragon에서 인프라를 제공한다. 스페인 디지털 혁신 및 공무원부는 오픈내뷸라의 ONExtgen 이니셔티브의 일부이며 유럽 연합의 NextGenerationEU 프로그램과 함께 공동으로 자금을 지원한다.

이 협력적 노력의 목표는 디지털 인프라를 관리하기 위한 강력한 오픈소스 대안을 제공하고, 유럽 기업과 공공 기관에 더 큰 유연성과 기술적 주권을 제공하며, 제한적인 라이선스 및 지원 모델의 제약 없이 IT 환경에 대한 제어력을 회복할 수 있는 능력을 제공하는 것이다.

Virt8ra는 유럽의 디지털 환경에서 시급한 문제인 대규모 비유럽 클라우드 공급업체에 대한 의존성을 해결하고자 한다. 이 인프라는 5G 셀 타워에서 데이터 센터에 이르기까지 다양한 분산 컴퓨팅 서비스를 관리하도록 설계했다. 따라서 스마트 팩토리, 커넥티드 카, 원격 수술, 산불 관리와 같이 낮은 대기 시간이 중요한 애플리케이션에 특히 적합하다.

Virt8ra 이니셔티브의 첫 번째 결과는 6개 EU 회원국(최근 7개로 확장)에 걸쳐 8개 IPCEI-CIS 파트너의 베어 메탈 리소스를 결합한 클라우드 엣지 인프라 테스트베드를 구축한 것이다. 이 접근 방식을 통해 전체 컴퓨팅 연속체에 걸쳐 분산된 클라우드 엣지 공간을 생성하여 혁신을 촉진하고 전략적 산업 분야에서 시범 배포를 가능하게 한다.

Virt8ra 테스트베드는 다양한 파트너의 인프라 리소스와 기술 구성요소를 통합하여 IPCEI-CIS 가상화 아키텍처를 인스턴스화하는 독립형 오픈소스 소프트웨어 스택을 기반으로 하며, 이를 통해 확장성, 상호운용성, 작업 이동성, 모니터링, AI/ML, 보안, 지속가능성과 같은 차세대 클라우드 기능을 실제 환경에서 테스트할 수 있다.

6) PRESSWIRE, “The EU Tech Industry Joins Forces to Launch the First Sovereign Edge Cloud for Europe,” Jan 20, 2025

그림 1 Virt8ra 이니셔티브 테스트베드 파트너들 [출처: 오픈네뷸라 시스템즈 유튜브]

오픈네뷸라 시스템에서 제시하는 Virt8ra의 주요 역량은 다음과 같다.

그림 2 Virt8ra의 주요 역량 [출처: 오픈네뷸라 시스템즈]

초기 버전은 이미 주요 기능을 보여 주는데, 단일 제어 평면을 통해 사용자는 다양한 클라우드 공급자에서 물리적 리소스, 가상 머신 및 쿠버네티스 클러스터를 관리할 수 있다. 인프라는 이식성에 중점을 두고 개발되어 애플리케이션을 다른 위치 간에 쉽게 배포하고 마이그레이션할 수 있다. 각 기능에 대한 데모는 유튜브 영상[7]을 통해서 확인할 수 있다.

이 과제는 앞으로 시스템의 도달 범위를 확장하고, 더 많은 위치를 통합하고, 엣지 기반 AI 애플리케이션과 같은 차세대 사용 사례를 위해 설계된 고급 기능을 추가하려는 계획을 하고 있다. 이는 앞으로 복잡한 디지털 환경에서 유럽 기업의 요구를 충족하기 위한 것이다.

7) https://www.youtube.com/watch?v=PGpCeoqtHWg&t=88s

나가며

유럽 클라우드 시장은 여전히 어려움에 직면해 있다. 고객은 데이터 이탈 수수료와 같은 높은 비용과 공급업체 간 상호운용성 부족으로 어려움을 겪는 경우가 많다. 마이그레이션 절차도 번거로워서 서비스를 전환하기 어려울 수 있는 문제가 있다.

2025년 9월에 발효될 예정인 EU의 데이터법은 클라우드와 엣지 공급자 간의 원활한 전환을 촉진하여 이러한 문제를 해결하는 것을 목표로 하고 있으며, Virt8ra는 이 법률에 맞춰 전환을 보다 원활하게 하기 위해 설계된 오픈소스 기술 스택을 제공하고자 하는 것이다.

2020년에 시작된 가이아-X 이니셔티브는 원래 미국의 주요 클라우드 공급업체에 대한 의존도를 줄이는 것을 목표로 했지만, 나중에 하이퍼스케일러와 직접 경쟁하기보다는 유럽 가치에 맞춰 클라우드 정책과 표준을 정의하는 데 초점을 맞추고 있다.

최근 가이아-X는 유럽의 독특한 지리적 분포를 활용하기 위해 소규모 클라우드 공급업체를 하나로 모으는 펄크럼(Fulcrum) 프로젝트를 지원했다. 또한, 전 가이아-X CEO인 프란체스코 본필리오(Francesco Bonfiglio)는 유럽 공급업체를 위한 분산형 클라우드 마켓플레이스를 만드는 것을 목표로 하는 다이나모 프로젝트를 추진하고 있다.

Virt8ra는 유럽에서 가장 큰 규모로 추진하는 오픈소스 기반의 엣지 클라우드 플랫폼이라는 점에서 매우 주목할 수 있지만 참여 기업이 하이퍼스케일러가 아니라는 점에서 발전 역량과 기술 대응에 의문을 가질 수 있다. 그럼에도 중소형 클라우드 기업이 추가로 참여해 지리적으로 분산된 유럽의 지정학적 특성을 반영할 수 있게 많은 중소 클라우드 기업의 참여가 이루어진다면 우리에게는 매우 중요한 참고 사항이 될 것이다.

03 클라우드 보안을 위한 AI 솔루션

| Senior Program Manager 김영욱

들어가며

2024년 1월 러시아 정부의 지원을 받는 해킹 그룹으로 알려진 미드나잇 블리자드(Midnight Blizzard)가 마이크로소프트에 사이버 공격을 시도하고 일부의 내부 이메일 계정에 접근하여 이메일 내용과 첨부 문서를 탈취했다.[8] 마이크로소프트 보안 팀은 즉시 탐지와 동시에 대응 프로세스를 가동하여 공격 활동을 조사, 차단하여 피해를 최소화하였다. 이 사건은 레거시 시스템과 다단계 인증 미적용 계정의 취약성을 악용한 사례로 정교한 공격에 대비하는 보안 모니터링과 신속한 대응 체계의 중요성을 부각시켰다.

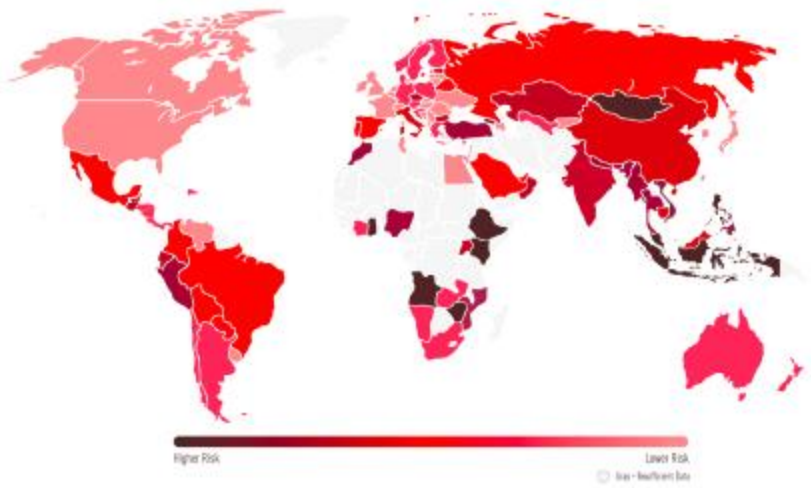


그림 3 글로벌 사이버 위협 인덱스 맵 (출처: 체크포인트 리서치)

사이버 공격 사례는 매년 증가한다. 글로벌적으로 2024년에는 전년 대비 58% 증가하였고, 이것은 매주 1,673회의 공격 횟수로[9] 지속해서 증가하고 있을 뿐만 아니라, 그 전문성 역시 더욱 정교해지고 있다. 디지털 전환으로 클라우드 플랫폼이 기업과 조직 대부분의 기본 업무 환경이 된 상황에서 AI 기술이 클라우드 컴퓨팅 보안의 새로운 돌파구로 평가받고 있다.

8) Microsoft, Midnight Blizzard: Guidance for responders on nation-state attack, Jan 25, 2024
9) Check Point Research, THE STATE OF CYBER SECURITY 2025

현재 많은 산업에 AI가 빠르게 도입되고 있으나 아직 클라우드 보안 환경에 AI를 도입하여 사용하는 기업은 약 50% 정도에 지나지 않는다.[10] 더욱 심각한 것은 AI 기술이 도입된 후에 이를 관리하기 위한 정책을 세우는 기업이나 조직은 그 절반에도 못 미친다는 점이다. 이에 이번 글에서는 AI 기술이 클라우드 보안에 주는 이점과 중요성, 그 시장에 대해 다루어 본다.

AI의 도입 이점과 잠재적 위험

AI 기술을 클라우드 보안에 도입하면 효율성과 보안 강화에 강점을 기대할 수 있다. 동시에, 공격자의 위협을 강화할 수도 있기에 잘 이해하고 사용할 수 있어야 한다.

도입 이점

클라우드 보안에 생성형 AI를 도입하였을 때 기대할 수 있는 효과는 많다.

먼저 위협 탐지에 효과적인 대응이 가능하다. 대규모 언어 모델(LLM)은 방대한 양의 클라우드 보안 데이터를 분석하여 기존 시스템에서 놓칠 수 있는 이상 또는 잠재적 위협을 선제적으로 식별할 수 있다. 비정상적인 로그인 패턴이나 데이터 접근 요청 또는 API 호출을 감지하여 보안 팀에 실시간으로 알림과 경고를 할 수 있다.

두 번째는 자동화된 프로세스의 운영이 가능하다는 점이다. 생성형 AI를 사용하면 수많은 클라우드 보안 작업 프로세스를 자동화하는 데 많은 이점이 있다. 보안 경고 내용을 분석하고 심각도와 잠재 영향에 따라 우선순위를 지정할 수 있고, 해당 팀에 적절한 조치를 제안할 수 있다. 또한 클라우드 환경 전반의 보안 정책을 정의하고 구현 및 시행하여 일관된 보안 규정 요구 사항을 준수할 수 있어 자동화된 정책 관리가 가능하다. 그뿐만 아니라 사고에 대한 데이터를 수집하고 영향을 받은 시스템을 식별하여 수정을 제안할 수 있다.

세 번째는 잠재적인 위협과 취약성을 먼저 탐색하고 발견하여 공격이나 악용되기 전에 선제적으로 위험을 식별할 수 있다. 클라우드 구성을 분석하여 잘못된 보안 구성 사항이 있는지 식별하고 전반적 보안 상태를 개선하기 위한 시정 조치를 제안할 수 있다. 또한 생성형 AI는 IT 관리자가 클라우드를 관리 시 보안 문제를 식별하고 그 내용 이해를 도울 수 있고, 개발자에게는 좀 더 안전한 코드를

10) Kaspersky, More than half of companies use AI and IoT in their business processes, Mar 01, 2024

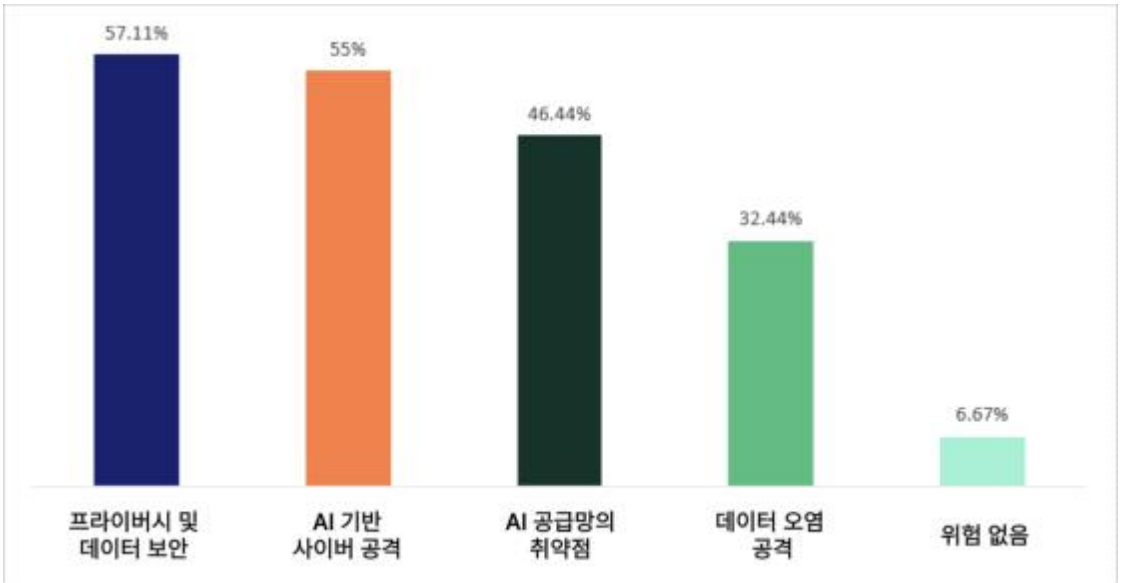
생성하는 방법을 제안함으로써 보안 전문가의 업무 부담을 줄이고 효율성을 개선할 수 있다.

잠재적 위험

잠재적 위험의 첫 번째는 공격자 무기를 강화할 수 있다는 것이다. 생성형 AI는 사이버 공격자의 공격도 효율적으로 만들고 강화할 수 있다. 기존 보안 방어 수단을 우회하고 탐지하기 어려운 악성 코드를 생성할 수 있을 뿐만 아니라 공격 대상 조직의 특정 역할의 인물을 타깃으로 삼을 수 있다. 이는 개인화된 설득력 있는 피싱 이메일을 작성할 수 있게 하여 공격의 성공 가능성을 높인다. 음성이나 영상을 사용하는 딥페이크를 생성하여 개인을 사칭하는 등 정교한 공격 및 접근이 가능해진다.

두 번째는 학습 데이터 자체의 문제가 드러날 수 있다. 조직에서 사용 중인 생성형 AI의 학습 데이터를 조작하여 생성 결과물에 영향을 미치고 보안 기능을 손상시킬 수 있다. AI에 민감 정보를 무의식적으로 입력한 경우 적절한 보호 장치가 없다면 해당 데이터는 무자비하게 노출될 수 있다.

세 번째는 기존 클라우드의 보안 문제를 악화시킬 수 있다. 클라우드 아키텍처의 복잡성이 증가하면서 공격할 수 있는 영역 또한 넓어졌다. AI는 이러한 환경을 보호하는 데에 사용될 수도 있지만 공격자가 이를 더 효과적으로 악용할 수도 있다. 공격자가 본인 활동을 은폐하고 클라우드 환경의 가시성을 확보하고 제어할 수 있다. 이런 경우 위협 또는 공격을 식별하고 대응하기 어려워진다.

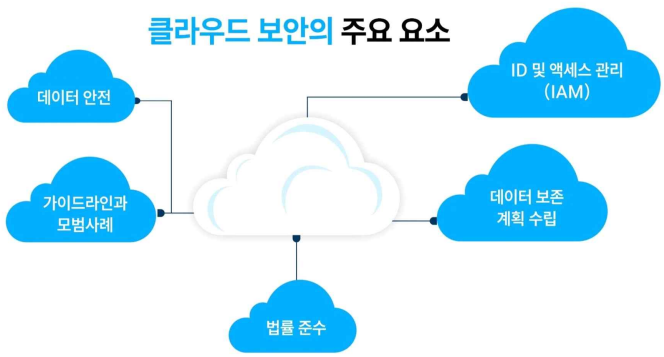


11)

그림 4 클라우드 환경 내 AI의 주요 위험 (출처: SUSE)

AI 도입을 위한 보안 이니셔티브

AI의 도입은 기술 혁신의 가능성을 열어 주는 동시에 보안 리스크를 더욱 심각하게 만들 수 있는 잠재적 위험성도 동반한다. 따라서 이를 도입할 시 클라우드 환경 보안 강화를 위한 정책과 솔루션 도입이 필요하다. 보안을 강화하기 위한 중요 요소로는 제로 트러스트 원칙[12], 데이터 안전 관리를 위한 태그 지정, 자동 백업 및 실시간 모니터링 시스템이 있다. 조직에서 생성형 AI포함 AI 기술을 올바르게 사용하고 보안을 강화하기 위해선 개인정보와 데이터 보안을 위한 대책을 마련하고, 안전한 사용을 위한 가이드라인도 필요하다.



13)

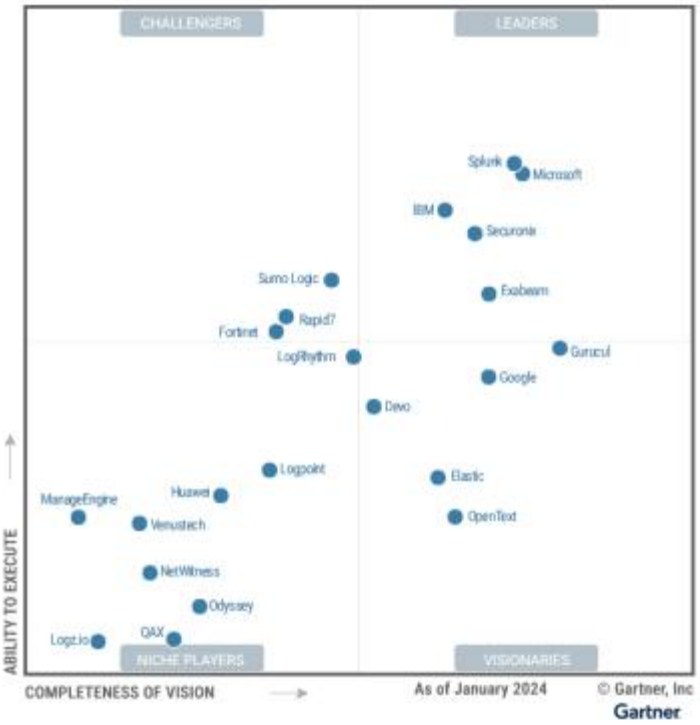
그림 5 클라우드 보안의 주요 기본 요소 (출처: peoplactive)

다층 보안 전략(Multi-Layer Security)

다층 보안 전략은 데이터 백업, 이메일 필터링, 엔드포인트 탐지 및 대응(EDR), 정기적인 소프트웨어 업데이트, 액세스 제어, 보안 평가 등을 포함한다. 동시에 API 보안, ID 및 접근 관리, 강력한 API 게이트웨이, 다단계 인증, 클라우드 보안 태세 관리(CSPM)와 같은 고급 클라우드 보안 솔루션 도입도 필요하다. 특히, 소프트웨어 공급망 보안을 강화하여 AI 모델 및 소프트웨어의 신뢰성을 보장하고, 공급망 전반에서의 보안 점검을 정기적으로 수행해야 한다. 마이크로소프트는 애저 액티브 디렉토리를 활용하여 다중 요소 인증 및 조건부 액세스 정책을 통해 제로 트러스트 아키텍처를 제공한다.[14] 또한 Splunk, IBM의 QRadar, 마이크로소프트 센티넬(Sentinel)과 같은 보안 정보 및 이벤트 관리(SIEM)

11) SUSE, “Securing the cloud”, Oct 2024
12) '절대 신뢰하지 않고 항상 확인'한다는 접근 방식을 취하는 보안 모델이다. 마치 회사 건물의 모든 출입구에 보안 게이트를 설치하고, 조직원이라도 매번 신분증을 확인하는 시스템과 같다.
13) Peoplactive, “A Face-off Between Cybersecurity and Cloud Security”, Nov 2023
14) Microsoft, What is Conditional Access?, Mar 19, 2024

솔루션을 통해 실시간 위협 감지 및 대응 체계를 강화한다.



15)

그림 6 SIEM 매직 쿼드런트 (출처: 가트너)

AI 기반 예방 및 탐지 시스템

AI 기반 예방 및 탐지 시스템은 위협이 확산되기 전에 이를 감지하고 완화하는 데 필수적이다. 조직은 ID, 클라우드, 엔드포인트, 데이터 보호 간의 상호 작용을 통합적으로 이해하고 공격표면에 대한 360도 가시성을 확보해야 한다. 의료 산업의 경우 CSPM 도구를 통해 클라우드 환경의 구성 오류를 점검하고, 비정상적인 데이터 접근 시도를 실시간으로 탐지하여 차단하는 시스템을 도입해 환자 데이터를 보호할 수 있다. 네이버클라우드가 9개 국립병원의 병원정보시스템(HIS)을 자사 클라우드 플랫폼 기반으로 통합 구축한 사례가 있다.[16] 이는 공공 의료기관의 병원정보시스템을 클라우드로 전환한 첫 사례로 네이버클라우드는 자체 보안 서비스와 모니터링 활동을 통해 의료 데이터를 안전하게 관리하고 취약점 관리, 위험 탐지, 대응 등을 통해 데이터 보안을 강화했다.

15) 가트너, Magic Quadrant for Security Information and Event Management, May 8, 2024
16) 이코노믹데일리, 네이버클라우드, 9개 국립병원 차세대 병원정보시스템 구축, May 20, 2024

새로운 위협에 대한 지속적 대응

제로데이 공격(Zero-Day Attack)[17]과 같은 새로운 취약점에 대비하기 위해 취약점 관리 프로그램을 운영하고 최신 위협 정보를 반영한 대응 방안을 지속해서 업데이트해야 한다. 조직에서 취약점 발견 즉시 대응팀을 구성하여 신속하게 패치를 적용하고 추가적인 보안 조치를 취함으로써 보안 사고를 예방할 수 있다. IT 인프라에 대한 액세스를 간소화하고 보호하는 데 중점을 둔 사이버 보안 회사인 텔레포트(Teleport)의 CI 파이프라인의 취약점을 통해 공격자가 시스템에 무단 접근하여 회사의 기밀 사항을 공개하는 사건이 있었다.[18] 이는 취약점 테스트와 모니터링, 데이터 마스킹 및 합성 데이터 사용, 최소 권한 원칙 적용 등을 통해 보안 수준을 높여야 한다는 교훈을 제공한다.

클라우드 AI 보안 솔루션의 중요성

클라우드 컴퓨팅의 빠른 변화에 수동으로 보안 사항에 일일이 대응하는 것은 거의 불가능한 일이다. 이제는 머신러닝과 생성형 AI를 통해 방대한 데이터를 분석하고, 패턴을 식별하고, 악의적인 활동을 선제적으로 탐지할 수 있어야 한다. 사이버 위협이 AI로 인해 정교하고 강화되고 있는 데 반해 보안 분야의 인력은 부족하다.[19] AI 기반의 보안 솔루션은 기존 보안 팀의 역량을 강화하여 작업을 자동화하고, 워크플로우를 간소화하여 전문가의 인력 문제를 해결할 수 있기에 전략적 이니셔티브에 집중할 수 있는 역량을 지원한다.

클라우드 AI 보안 솔루션 리더

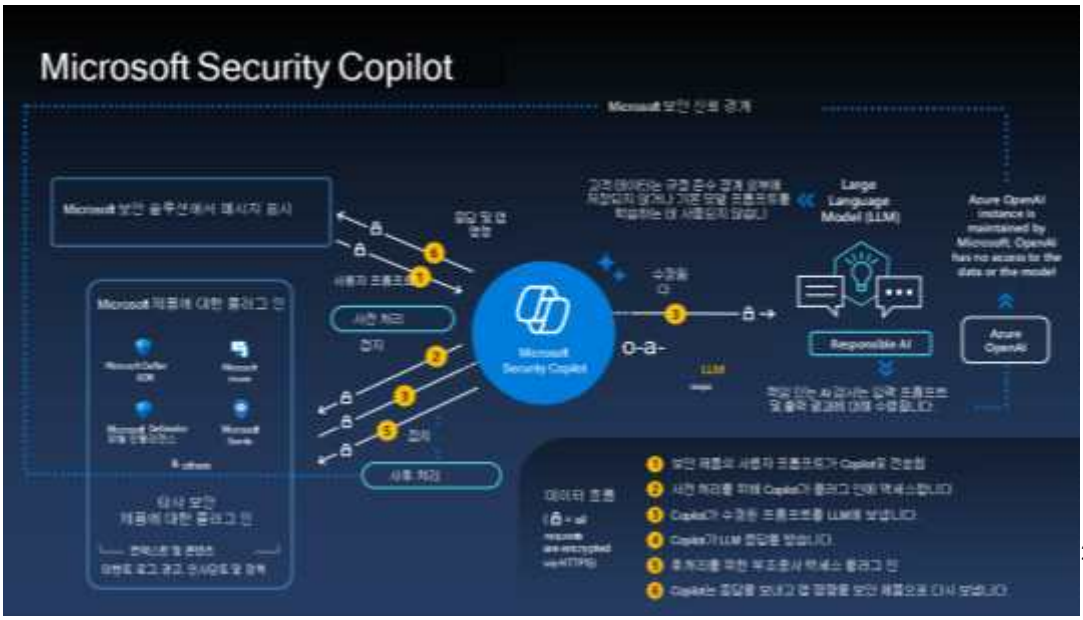
보안 솔루션이 갖춰야 할 핵심 요소를 중심으로 클라우드 AI 보안 솔루션을 소개하고자 한다. 대규모 조직과 클라우드 기반 인프라의 복잡성을 효과적으로 보호하기 위한 확장성, 실시간 탐지, 자동화, 행동 기반 분석을 기준으로 선정해 보았다.

1. 마이크로소프트

마이크로소프트 센티넬, 클라우드 디펜더, 엔드포인트 디펜더, 보안 코파일럿 등의 풀 스택 보안 솔루션을 제공한다. 이 중에서 최근 가장 각광받는 보안 코파일럿은 복잡한 위협 데이터를 분석하여

17) 소프트웨어나 하드웨어의 보안 취약점이 개발자나 사용자에게 알려지기 전에, 또는 알려진 지 얼마 되지 않아 해당 취약점에 대한 패치나 해결책이 제공되기 전에 이를 악용하는 사이버 공격을 말한다. '제로데이'란 취약점이 공개된 후 개발자에게 남겨진 시간이 0일이라는 의미로, 즉시 대응이 어렵다는 점을 강조한다.
18) CodeSigning, 8 Steps for Securing Your CI/CD Pipeline
19) Google Cloud, Deloitte, Entering the Era of Generative AI-Enabled Security

심층 분석과 대응 전략이 포함된 인사이트를 제공한다. 또한 대화형 인터페이스와 자연어 처리를 통해 보안 팀의 업무 효율성을 크게 향상시킨다. 마이크로소프트의 다른 서비스를 이용하는 고객이라면 애저 생태계 통합을 통해 큰 편리함과 효율을 기대할 수 있으며 멀티클라우드 지원, 그리고 다층 보안 전략을 통해 360도 가시성과 강화된 보안을 기대할 수 있다.



20)

그림 7 마이크로소프트 보안 코파일럿 동작 다이어그램 (출처: 마이크로소프트)

2. 센티넬원(SentinelOne)

센티넬원은 특허받은 행동 AI를 통해 군사 등급 예방, 감지, 대응을 지원한다. 인터넷 연결이 필요하지 않으며 사람의 지속적인 감독 없이 위협을 탐지하고 대응과 해결을 자동화하여 대응에 필요한 시간을 대폭 단축시킨다. 또한 랜섬웨어 공격 시 파일 및 시스템 상태를 원래대로 되돌릴 수 있는 강력한 복구 기능을 제공한다는 차별점을 갖고 있다. 하이브리드 및 멀티클라우드 환경을 보호하며 높은 효율성을 제공하기도 한다. 기존 보안 방식보다 빠르게 위협을 식별하고 완화하는 자율형 AI와 기존 인프라와의 원활한 통합을 제공하여 큰 시스템 개편 없이도 전반적 보안을 강화할 수 있는 것이 특징이다. 금융 보험 도메인에 많은 고객을 갖고 있는 프로바이더이다.

20) 마이크로소프트, Microsoft Security Copilot이란?, Nov 19, 2024

그림 8 센티넬원 싱귤래리티 플랫폼 (출처: 센티넬원)

3. 다크트레이스 (DarkTrace)

다크트레이스는 사전에 정의된 규칙이 아닌 네트워크와 디바이스의 조직 운영의 고유한 패턴을 자율적으로 학습하고 이해하여 새로운 위협과 이상 징후를 탐지하는 AI 기능을 제공한다. 위협이 생기면 자율적으로 실시간 대응 조치를 취하고 감염된 디바이스를 네트워크에서 격리하거나 비정상적인 트래픽을 자율적으로 차단할 수 있다. 또한 온프레미스, 클라우드, 하이브리드, IoT 등 다양한 환경에서 보안 솔루션을 제공하며 탐지된 위협의 심각성과 우선순위를 판단하여 긴급 조치를 취해 보안 리소스를 효율적으로 사용할 수 있다.

그림 9 다크트레이스 클라우드 AI 보안 솔루션 구조 (출처: 다크트레이스)

마무리

클라우드 플랫폼이 조직의 디지털 환경 전반을 중앙에서 통합 관리하여 기존의 단편적인 보안 솔루션에서 발생하던 가시성 부족 문제를 해결할 것이란 관점에서, AI 기술은 클라우드 보안 솔루션에 통합되어 대량의 데이터를 분석하고 악의적 활동 패턴을 감지하여 실시간 진화하는 위협을 선제적으로 식별 및 대응할 수 있을 것으로 전망한다. 특히 식별된 결과를 데이터 시각화와 요약을 통해 보안 전문가에게 직관적이고 실질적인 인사이트를 제공할 때 그 부가가치는 극대화될 것으로 전망한다.

보안 전문가가 부족한 상황에서, 금융이나 유통과 같은 특정 산업에서 생성형 AI가 악용될 가능성이 증가함에 따라 이를 보완할 수 있는 AI 기반 보안 솔루션 도입이 필요하다. 기업이나 조직에서는 보안 강화를 위해 엔드포인트 간 연계를 이해하여 360도 가시성을 확보해 공격 목표가 될 수 있는 모든 표면 모니터링이 필요하며, 취약점 관리 프로그램을 통해 패치 우선순위를 설정하고, 위협 인텔리전스와 공격표면 관리 도구를 활용하여 새로운 취약점에 신속히 대응해야 한다. 보안 솔루션 및 AI를 통해 반복 작업을 자동화하고 보안 전문가가 전략적 업무에 집중할 수 있도록 지원하고 교육 등을 통해 조직의 보안 인식을 강화하는 다층 보안 접근법을 실행하면 심각한 보안 사고를 예방하고 변화하는 위협 환경에 빠르게 적응할 수 있을 것이다.

04 클라우드 기반 스마트팩토리 - 입문

| 정채상 인이지 연구소 기술 책임자

들어가며

스마트팩토리(smart factory)는 첨단 정보통신기술(ICT)을 활용하여 제조 공정 전반을 자동화하고 최적화하는 제조 환경을 말한다. 기존의 전통적 공장이 인간의 노동력을 중심으로 운영되었다면, 스마트팩토리는 사물인터넷(IoT), 로봇공학, 빅데이터, 인공지능 등을 결합하여 공정의 효율성을 극대화한다. 이는 단순한 자동화된 공장을 넘어선 개념으로 실시간으로 생산 현황을 모니터링하고 최적의 의사결정을 내리는 것을 목표로 하며, 이를 통해 불량률 감소, 에너지 효율화, 생산 원가 절감 등 다양한 효과를 얻을 수 있으며, 나아가서는 다품종소량생산과 같은 유연한 제조 환경에도 효과적으로 대응할 수 있게 된다.

클라우드 기술은 스마트팩토리를 구현하는 데 있어 필수적인 요소로 자리 잡고 있다. 방대한 양의 생산 데이터를 저장하고 분석하기 위해서는 강력한 컴퓨팅 자원과 많은 저장 공간이 필요하며, 클라우드는 이러한 요구를 충족시킬 수 있는 최적의 솔루션으로 다음의 특징들을 가진다.

- 데이터 저장 및 분석: 생산 현장에서 발생하는 방대한 양의 데이터를 클라우드에 저장하고, 빅데이터 분석 기술을 활용하여 유용한 정보를 추출한다.
- AI 활용: 클라우드 기반 AI 서비스를 활용하여 예지 보전, 품질 예측 등 고급 분석을 수행한다.
- 유연한 확장성: 필요에 따라 컴퓨팅 자원을 유연하게 확장하거나 축소할 수 있어 비용 효율적인 시스템 운영이 가능하다.
- 협업 환경 구축: 다양한 사용자가 클라우드 기반 플랫폼을 통해 실시간으로 협업하며 생산 과정을 관리할 수 있다.

클라우드는 스마트팩토리의 핵심적인 역할을 수행할 수 있으며, 제조업의 디지털 전환을 가속하는 데 기여하고 있다. 본 글에서는 스마트팩토리를 위한 입문으로 운영의 핵심 요소들과 클라우드 기반 솔루션들을 소개한다. 주로 IoT 관련 서비스 제품들이 표준화되어 이용된다.

스마트팩토리 운영의 핵심 요소

1. 데이터 수집 및 관리

데이터를 어떻게 다루는가가 스마트팩토리의 핵심으로, 데이터의 실시간 수집과 통합 관리가 필수적이다. 이를 위해 생산 설비, 작업자, 원자재, 제품 등 공장 내 모든 요소로부터 발생하는 데이터를 신뢰성 있게 수집하고 통합하는 체계가 갖춰져야 한다. 산업용 IoT 센서, 스마트 디바이스, 통신 네트워크 등의 인프라가 체계적으로 구축되어야 하며, 이렇게 수집된 데이터는 표준화된 형태로 저장되고 관리되어야 한다. 데이터 정제와 처리 기술이 필수적이고, 이 데이터들은 해당 기업의 핵심 자산이기에 철저한 보안 체계를 갖추는 것도 중요하다.

2. 실시간 모니터링 및 예측 분석

스마트팩토리는 단순히 데이터를 수집하는 데 그치지 않고, 이를 기반으로 실시간 모니터링과 예측 분석을 수행한다. 이를 통해 공정 중 발생할 수 있는 문제를 조기에 감지하고, 장비의 이상 상태나 품질 결함을 예측하여 신속히 대응할 수 있다. 의미 있는 인사이트를 도출하고 미래를 예측할 수 있어야 하고, 빅데이터 분석 기술과 AI 기술을 활용하여 설비 고장 예측, 품질 예측, 수요 예측 등을 수행할 수 있으며, 이를 통해 선제적인 의사결정이 가능해진다.

3. 제어 및 생산 공정 최적화

수집된 데이터를 바탕으로 생산 현장의 상황을 파악하고, 문제가 발생했을 때 신속하게 대응할 수 있는 체계가 필요하다. 유기적으로 연동된 MES(Manufacturing Execution System)나 SCADA (Supervisory Control And Data Acquisition) 같은 제조 실행 시스템이 구축되어야 하며, 이는 불필요한 다운타임을 줄이고, 생산성을 향상하는 데 큰 역할을 한다.

더 나아가서는 유연하고 적응력 있는 생산 체계를 통해 공정 효율성을 높인다. 공정 최적화를 통해 고객의 요구 사항에 맞춘 대량 맞춤형 생산과 같은 새로운 제조 패러다임을 가능하게 하고, AI와 머신러닝 기술을 활용하여 다양한 생산 공정 최적화를 이룰 수 있다.

4. 협업 및 연결성

스마트팩토리는 다양한 장비와 시스템이 서로 원활히 통신할 수 있도록 높은 수준의 연결성을 요구한다. 위의 유기적으로 연동된 데이터에 더해 전사적 자원 관리(ERP) 시스템, 공급망 관리(SCM) 시스템 등과의 통합은 공장의 전반적인 운영 효율을 높이고, 부서 간 협업을 강화한다.

AWS의 IoT 서비스

AWS에서는 IoT 관련해서 다양한 솔루션을 이용할 수 있는데, 스마트팩토리를 구현하는 방법으로 먼저 엣지 디바이스에서 정보들을 관리하는 솔루션들을 아래 그림 10의 솔루션들을 이용할 수 있다.

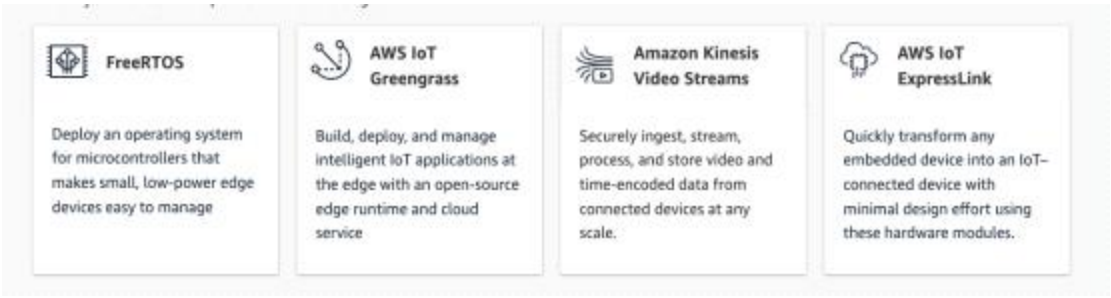


그림 10 AWS IoT 디바이스 솔루션들

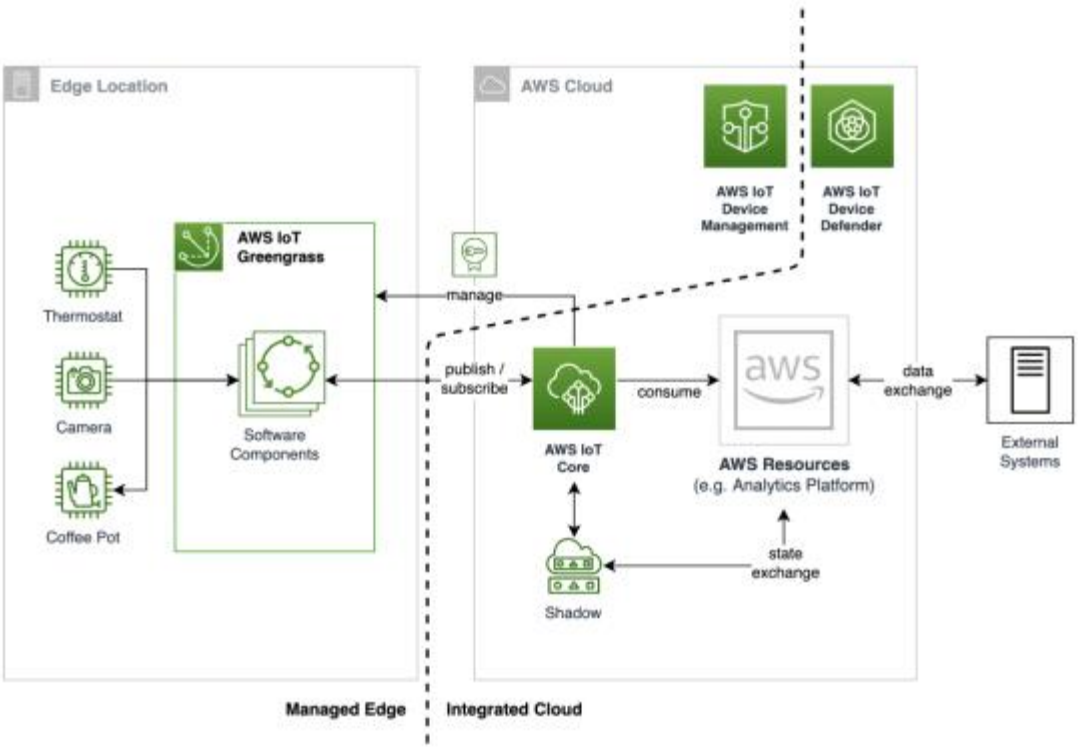
이들을 클라우드에 연결하는 방식으로 아래 그림 11의 솔루션들을 이용할 수 있다.

그림 11 AWS IoT 클라우드 연결 솔루션들

마지막으로, 관리자 혹은 사용자의 시각에서 이 데이터들을 운영하기 위해 아래 그림 12의 솔루션들을 사용할 수 있다. 이후에는 모인 데이터들은 AWS의 일반적인 서비스들과 도구들을 이용해서 사용할 수 있다.

그림 12 AWS IoT 분석 솔루션들

아래 그림 13은 AWS IoT 그린그래스, AWS IoT 코어, AWS IoT 디바이스 디펜더, AWS Iot 디바이스 매니지먼트를 이용해서 연결되어 운영되는 사례의 구조를 나타낸다.



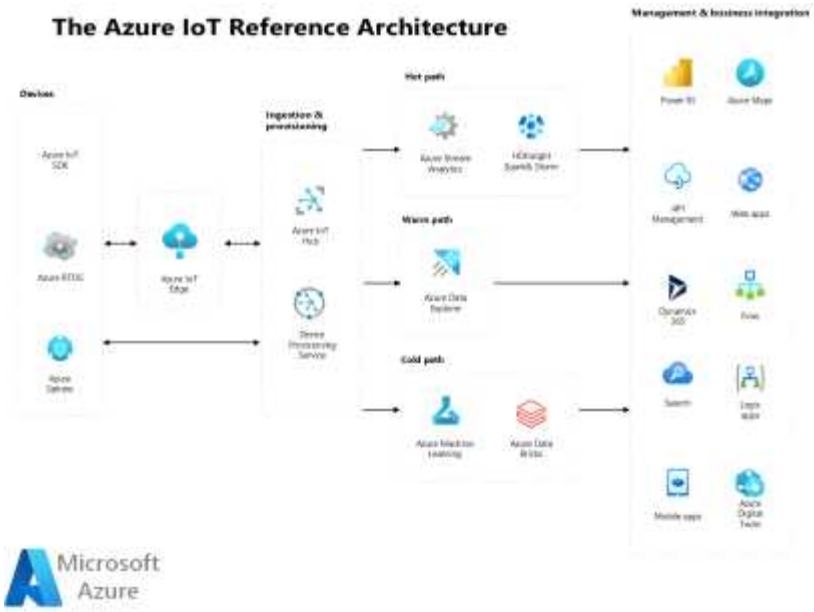
21)

그림 13 일반적인 AWS IoT 연결 예제

애저(Azure)의 IoT 서비스

마이크로소프트의 애저에서도 IoT를 위한 제품들이 준비되어 있고, 아래 그림 14와 같은 레퍼런스를 볼 수 있다. 엣지 디바이스에서 모이는 데이터들이 애저 IoT 허브(Hub)를 통해서 클라우드에 모이게 되고, 데이터의 성격에 따라 스트림 데이터를 위한 서비스 혹은 메시지를 위한 서비스 등으로 나누어 저장되고, 관리된다. 이후에도 역시 일반적인 서비스들과 도구들을 이용해서 사용할 수 있다.

21) https://aws.amazon.com/blogs/architecture/optimizing-your-iot-devices-for-environmental-sustainability/

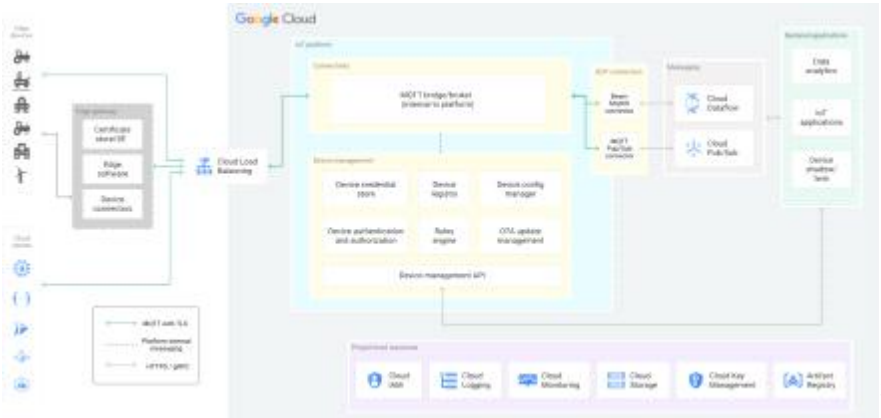


22)

그림 14 일반적인 애저 IoT 연결 구조

구글 클라우드 플랫폼(GCP)의 IoT 서비스

구글 클라우드 플랫폼도 IoT 관련해서는 유사한 방식을 지원한다. 아래 그림 15는 산업계에서 널리 쓰이는 메시징 표준인 MQTT 방식의 메시지를 이용해서 엣지 디바이스들로부터 메시지들을 클라우드에 전송하는 예제를 나타낸 그림이다.



23)

그림 15 GCP에서 IoT 제품 연결 예제

22) https://azure.github.io/IoTTrainingPack/modules/DevOps/sample-iot-application.html

맺으며

지금까지 스마트팩토리를 고려하며 주요 클라우드 업체의 IoT 서비스들을 간단히 훑어보았다. 특별한 서비스를 이용하지 않고, 엣지 디바이스 용 솔루션을 따로 고려하지 않더라도 일반적인 방식으로 클라우드에 연결해서 처리하는 경우들도 있고, 일반적인 공장들은 맞춤형으로 구현해야 하는 부분들이 많아서 클라우드 솔루션들을 바로 적용하기 힘든 경우가 대부분이다.

스마트팩토리를 새로 도입하거나 기존의 온프레미스 환경에서 클라우드로 고려할 때 여러 가지를 고려해야 하지만, 사물인터넷 서비스들을 이용해서 클라우드 기반으로 구축하면 아래의 장점들이 있다.

- 빠른 구축: 기존 IT 인프라 구축에 비해 빠르고 간편하게 스마트팩토리를 구축할 수 있다.
- 높은 확장성: 사업 규모가 변화하더라도 유연하게 시스템을 확장하거나 축소할 수 있다.
- 낮은 초기 투자 비용: 하드웨어 구매 비용을 절감하고, 필요한 만큼의 자원만 사용하여 비용 효율성을 높일 수 있다.

다음 회에는 여러 방식으로 스마트팩토리에 접근하는 과정에서 맞이하는 이슈에 관해 사례를 나누어 보겠다.

23) https://cloud.google.com/architecture/connected-devices/iot-platform-product-architecture