



[Elastic + Azure 온라인 밋업]

# MS Azure 클라우드에서 Elastic 시작하기

(부제: Azure와 만난 Elastic)

Ian Choi

Developer Product Marketing Manager (a.k.a. Field Developer Relations)

Microsoft APAC

# 발표자 소개

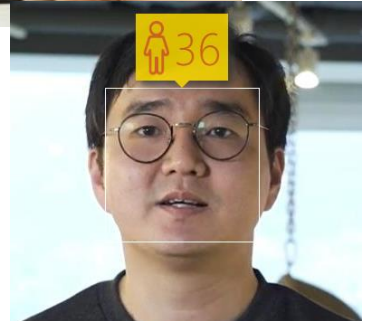
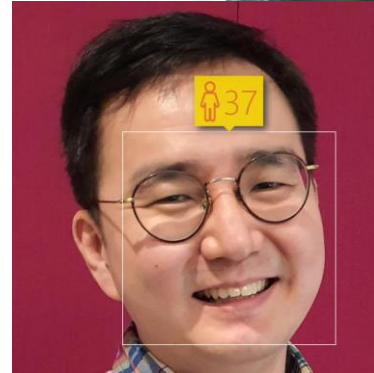
최영락 (Ian Choi) <yechoi@microsoft.com>

Developer Audience Product Marketing Manager

Microsoft

## <주요 활동>

- 퓨즈툴스코리아, 휴레이포지티브, 나임네트웍스, NoTag 등 역임
- Microsoft Certified Trainer (2009~현재)
- 오픈스택 한국 커뮤니티 3기 회장 (2017-19) & 국제화팀 리더
- 페이스북 뎀씨서울 리드 #DevCSeoul
- 2016년, “윈도우 서버 2012 R2 설치, 운영, 관리+실무 팁” 공저



<https://github.com/ianychoi>



<https://twitter.com/ianychoi>



<https://www.linkedin.com/in/ianychoi/>

## 발표 내용 (3-40분)

Azure에서 Elasticsearch 서비스를 시작하는 방법, 그리고 다른 Azure 서비스와 연계 & 활용 가능한 시나리오를 살펴봅니다.

- Azure 소개 및 현황
- Elastic Service on Azure
- Azure 서비스와 함께 보기
- DEMO
- 구성 시나리오
- 요약



(발표 시작 전에...)

장태희 MVP님, 감사합니다! (1부: <https://bit.ly/ianvideos> / 나머지도 곧  
공개예정입니다!)

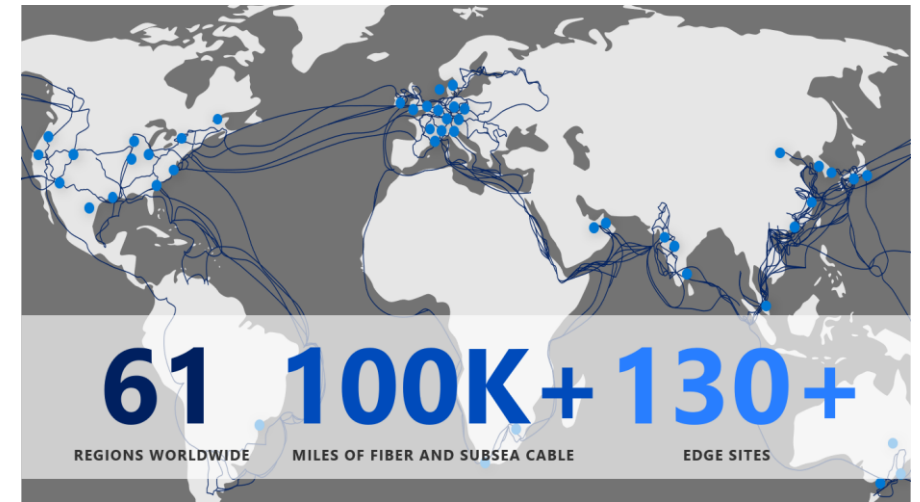
The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo and a search bar. The breadcrumb trail indicates the location: 대시보드 > 리소스 그룹 > IoTelasticGroup > iotelasticapp | 함수 > sendStreamtoElastic | 코드+ 테스트. The main content area displays the code for the 'sendStreamtoElastic' function in 'index.js'. The code is as follows:

```
1 const { Client } = require('@elastic/elasticsearch')
2 const client = new Client({
3   cloud: {
4     id: "elasticwithazuredemo:amFwYWSlYXN0LmF6
5   },
6   auth: {
7     username: 'elastic',
8     password: 'kuP6c5fRN1suK6kaQiatb50i'
9   }
10 })
11
12 module.exports = async function (context, req) {
13   req.body.forEach((message) => {
14     context.log(`data ${JSON.stringify(message)}`)
15     client.index({
16       index: 'iot-stream-function-elastic',
17       body: `${JSON.stringify(message)}`
18     })
19   })
20 }
```

On the right side, the '입력' (Input) tab is selected, showing the test output. The output is a JSON object: `{ "temperature": 28.38090613303196, "humidity": 74.66845012396 }`. The bottom right corner of the screenshot shows a small video feed of two people.

# Azure 소개 및 현황

Edge에서 Cloud까지, 전 세계 >300 서비스 제공



## Edge Devices

Azure Stack

Azure Data Box

Azure Sphere

Azure Kinect

HoloLens



## Serverless

Web

Mobile

Mixed Reality

Containers

Events + Integration

Databases

Analytics

AI + Machine Learning

Internet of Things

Media



## Tools

Visual Studio

GitHub

PowerApps

Power BI



## Infrastructure

Compute

Networking

Storage

Security

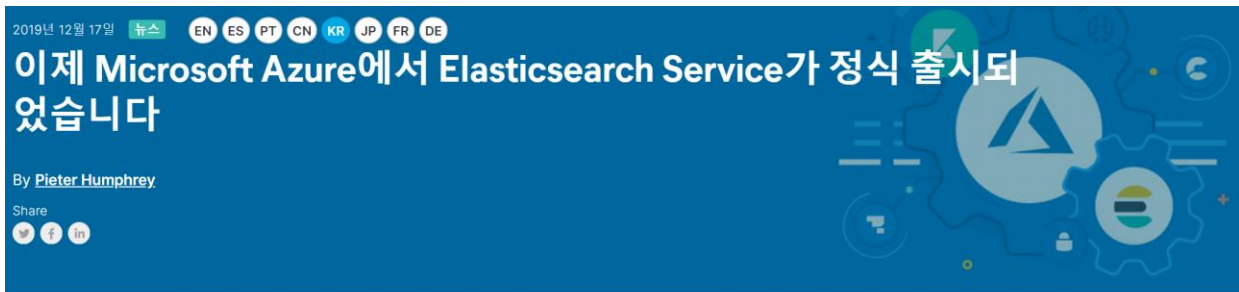
Identity

# Azure에서 Elastic을 사용하는 고객





# Elastic Service on Azure



올해 앞서, 모든 기능을 탑재한 Microsoft Azure의 Elasticsearch Service 공개 베타를 선보인데 이어 이제 기본 마음으로 공식 출시를 발표합니다! 기존 Elasticsearch Service 고객은 기존 계정으로 [로그인](#)하여 Azure에서 배포를 시작할 수 있으며 신규 사용자는 Elasticsearch Service의 [14일 무료 평가판](#)으로 시작할 수 있습니다.

## Elastic과 Microsoft의 성공적인 협업 강화

공개 베타 기간 동안 우리는 공동 고객들이 빠른 속도로 Azure의 Elasticsearch Service 사용을 시작하는 것을 확인한 바 있습니다. 그 결과, 다양한 프로덕션 작업 및 비프로덕션 작업에서의 베타 사용을 통해 Elastic과 Microsoft에서는 자신감을 갖고 강력하고 안정적인 서비스를 정식 버전으로 출시하게 되었습니다.

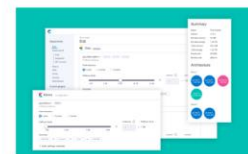
Azure의 Elasticsearch Service는 Elastic과 Microsoft 기술 사용자 모두에게 훨씬 더 나은 경험을 제공하는 방법 중 하나일 뿐입니다. Elastic Stack의 자체 관리형 배포를 선호하는 사용자는 Azure Marketplace를 사용하여 우리의 [Elastic Stack용 ARM 템플릿](#)(몇 년 전에 공동 출범됨)에 액세스 해왔습니다. Elastic에서는 또한 .NET 클라이언트, WindowsOS 이벤트 수집을 위한 Winlogbeat, Elasticsearch 클러스터를 보호하기 위한 Azure Active Directory 통합 및 Elastic APM 제품의 .NET 지원 등과 같은 다른 영역에서도 Microsoft 기술을 지원합니다. 우리의 기술 포트폴리오가 원활하게 함께 작동하고 새로운 혁신 기회를 제공하는 것이 우리의 공동 고객들에게는 그 어느 때보다도 중요합니다.

Elastic의 Craig Griffin 비즈니스 개발 담당 부사장은 "Microsoft와 우리의 협업이 계속해서 모멘텀을 구축하고 있다"며, "우리 사용자들이 강한 관심을 표시하고 있기 때문에 Azure에서 Elastic 솔루션을 제공하는 것이 우선순위"라고 말했습니다.

## Azure를 사용한 Elasticsearch 및 사용자가 좋아하는 모든 기능

Elastic Cloud의 Elasticsearch Service는 Elastic에서 만들고 제공하는 공식 호스팅형 Elasticsearch와 Kibana 서비스입니다. Elastic에서는 Elastic App Search, Elastic APM, Elastic SIEM, Elastic Maps 등의 솔루션만 제공하는 게 아니라, SRE, 기술 지원, 컨설팅 팀을 통해 Elastic 전문성도 제공해 드립니다. 클릭 한 번으로 자동 중단 시간이 전혀 없이 업그레이드되어 언제나 최신 Elastic 소프트웨어 릴리즈와 보안 패치를 이용하실 수 있다는 자신감으로 Azure에서 배포하세요.

### Recommended Content



#### Elasticsearch: Getting Started

Get an understanding of what Elasticsearch is capable of, how to implement basic functionality, and where to find more...

[Learn More](#)



#### Securing Elasticsearch with SSL, TLS, and HTTPS

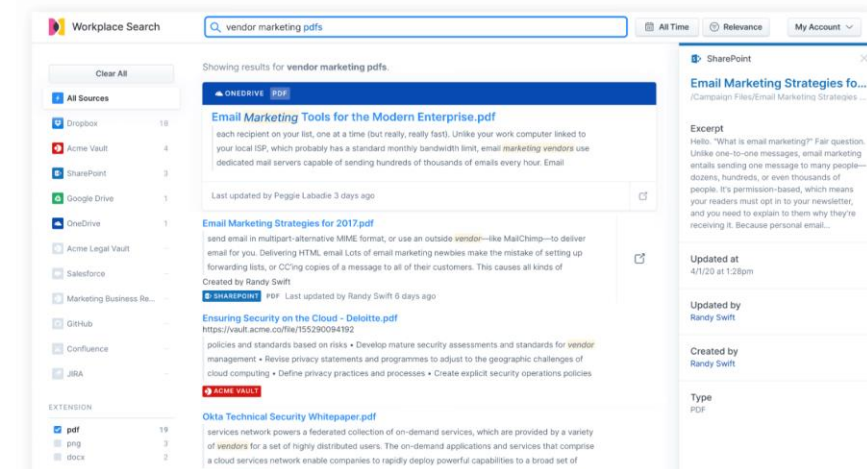
Step-by-step instructions for setting up TLS encryption and HTTPS on Elasticsearch, Kibana, Logstash, and Beats to secure...

[Learn More](#)



귀사도 전 세계의 대다수 기업(Elastic도 포함해서!)과 마찬가지로, 생산성 스택에서 아마도 SharePoint, Microsoft 365(이전의 Office 365), OneDrive 등 여러 Microsoft 제품을 사용하고 계실 것입니다. 그러나 [Zendesk](#) 또는 [GitHub](#) 같은 보완 도구들과 더불어 G Suite나 Dropbox 같은 "경쟁사" 도구들도 섞여서 아마 다양한 다른 애플리케이션도 사용 중이실 것입니다. 이로 인해 사용자 환경에 어느 정도 균열이 있게 됩니다. 동료 직원들은 특정 작업이나 프로젝트를 완료하는 데 필요한 것을 찾기 위해 일상적으로 여러 플랫폼에서 검색을 해야 하는 것입니다. 이것은 "그걸 어디서 또 봤더라?"라는 말이 낯설지 않으실 수 있다는 뜻이기도 합니다.

Elastic Workplace Search를 이용해보세요. Elastic Workplace Search는 플랫폼과 상관없이 조직 전체의 모든 애플리케이션 제품군에서 복잡하지 않으며 정확한 검색을 해야 하는 상황을 위해 설계되었습니다. G Suite에서부터 Salesforce에 이르기까지 [여러 다른 콘텐츠 소스](#) 외에도 SharePoint Online, Microsoft 365, OneDrive 등 Microsoft 소스에서 검색할 수 있는 기본 기능을 갖추고 있습니다. 서로 다른 소스들이 모두 평화롭게 공존할 수 있으며, 팀원들이 각 플랫폼에서 제공하는 모든 다른 검색 환경에 들어가 시간을 낭비하며 답답해할 필요 없이 한 곳에서 모든 것에 대해 검색할 수 있습니다.



<https://www.elastic.co/blog/searching-microsofts-cloud-productivity-suite-with-elastic-workplace-search>

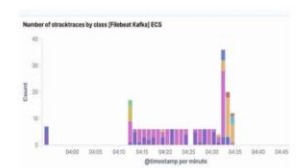
### Recommended Content



#### How to build React search experiences quickly

Search UI is an open source search library for building React search experiences. App Search is a refined search API with elegant...

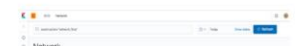
[Learn More](#)



#### Monitoring Kafka with Elasticsearch and Kibana

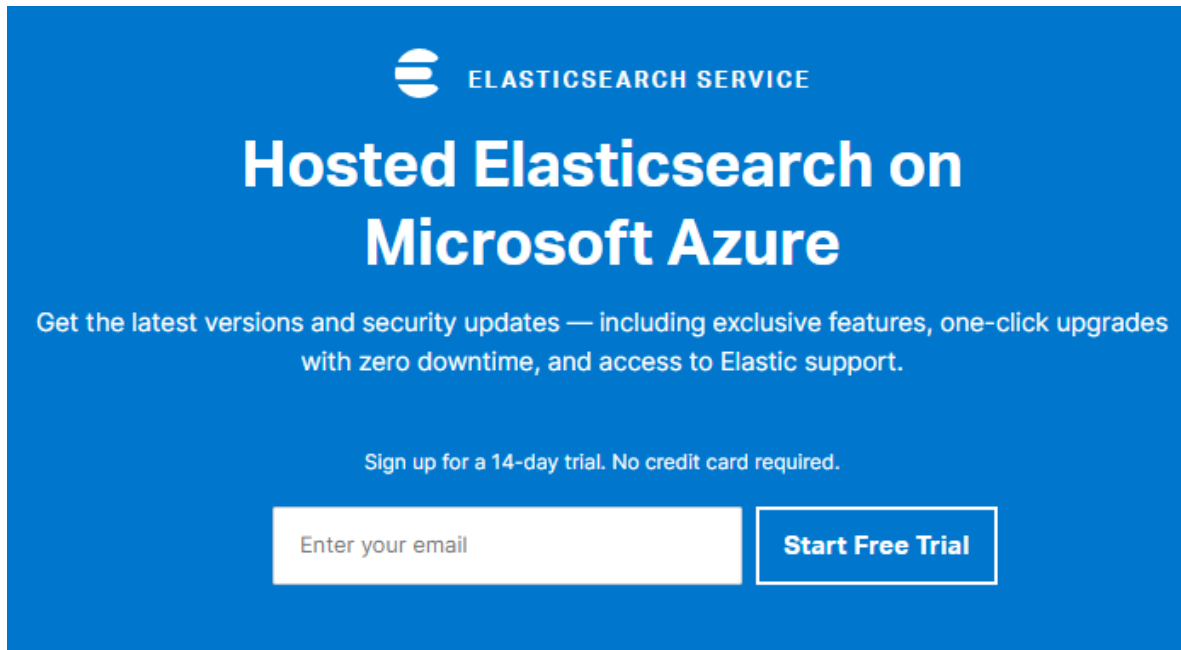
Kafka modules in Filebeat & Metricbeat simplify configuration of log and metric collection and create handy Kibana...

[Learn More](#)



# Elasticsearch를 Azure에서 시작하는 2가지 방법

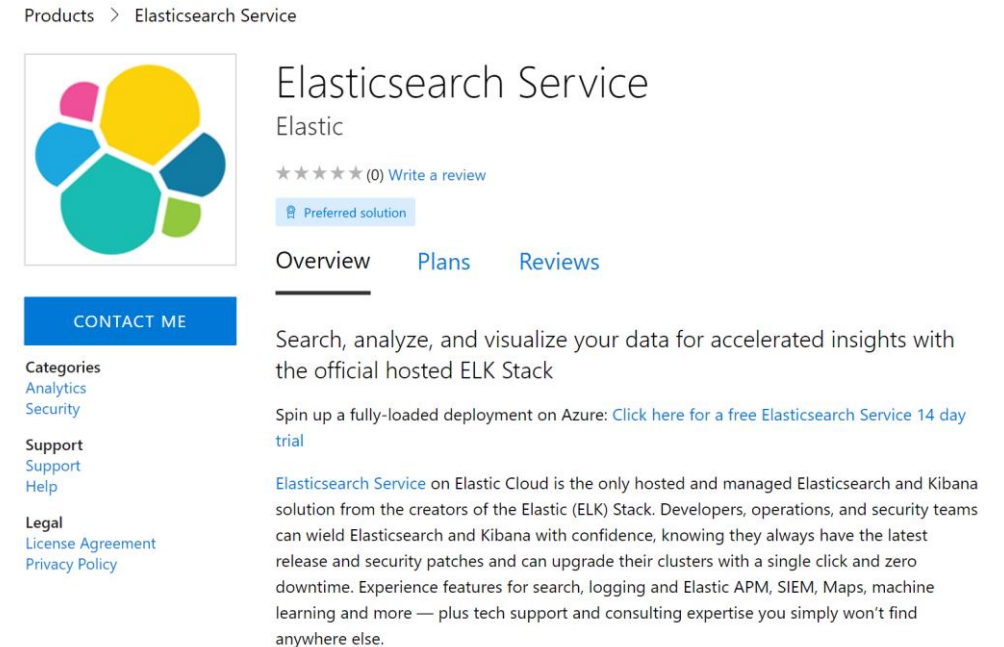
## A. Elasticsearch Service (SaaS) 를 사용하는 서비스에 가입하여 Azure에 배포



<https://info.elastic.co/elasticsearch-service-trial-microsoft-azure.html?elektra=ess-azure-ga-blog>

완벽한 Managed Service로 이용 가능

## B. Azure 마켓플레이스 (IaaS) 배포판 사용하기 Azure portal 에서 [리소스] > “Elasticsearch” 검색 \* [GitHub에 있는 ARM Template](#)를 사용한 사용자 지정 배포 가능



클라우드 환경에 직접 배포, 모든 권한 허용



# Elasticsearch Service on Azure – Managed Service인 Elastic Stack 환경을 Azure에 배포

## 배포시 클라우드 플랫폼 & 리전 선택

Deployments / Create

### Create deployment

#### 1 Name your deployment

Give your deployment a name

htelaz

#### 2 Select a cloud platform

Pick your cloud and let us handle the rest. No additional accounts required.



Azure

#### 3 Select a region

East US 2 (Virginia)

West Europe (Netherlands)

West US 2 (Washington)

Japan East (Tokyo)

#### 4 Set up your deployment

Generally available versions

☒ 7.6.1 ☐ 7.5.2

☐ 6.8.7

☐ Select a deployment to restore from one of its snapshots

Monitoring

☐ Enable monitoring by shipping metrics to a deployment

## 유연한 스케일 업 / 스케일 아웃

### Data 1 configuration

azure.data.highio.e32sv3

Data

Coordinating

Master

An I/O optimized Elasticsearch instance running on an Azure E32s with 8 P30 disks attached.

During a trial, you can have a cluster with up to 4 GB RAM across 2 zones. Using less could adversely affect the performance of the deployment.

[Learn more ...](#)

Fault tolerance

☐ 1 zone ☒ 2 zones ☐ 3 zones

RAM per Node

1 GB 2 GB 4 GB 8 GB 15 GB 29 GB 58 GB

Nodes

1

RAM per Zone

4 GB

Summary

4 GB RAM

120 GB storage

×

1 node

×

2 zones

=

8 GB RAM

240 GB storage

> User setting overrides

azure.data.highstorage.e16sv3

Data

Coordinating

Master

Instance configuration to be used for a higher disk/memory ratio, based on Azure Standard\_E16s\_v3.

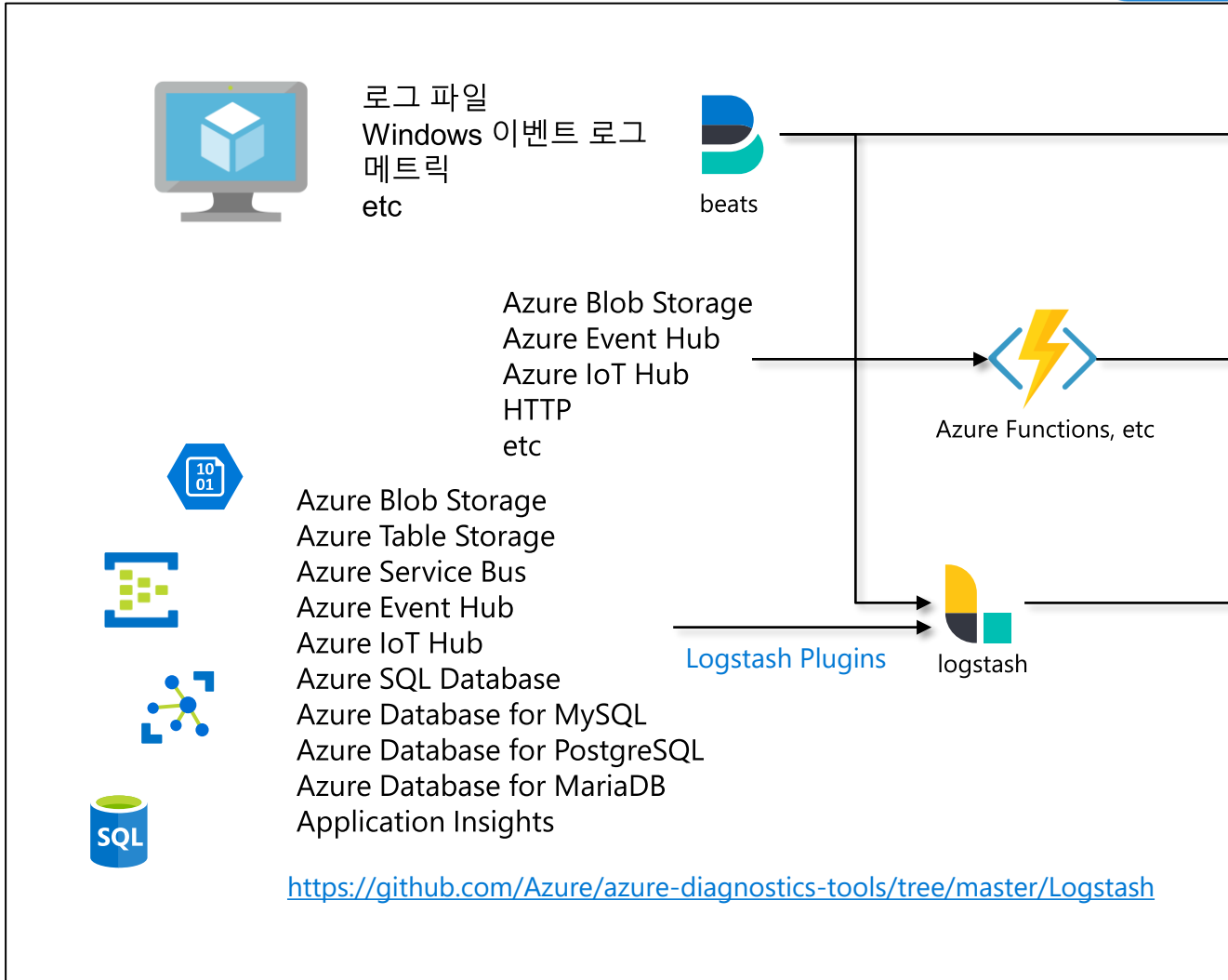
Enable

Allows the storage of indices that require less frequent querying on warm configurations, saving on processing costs. [Learn more](#)

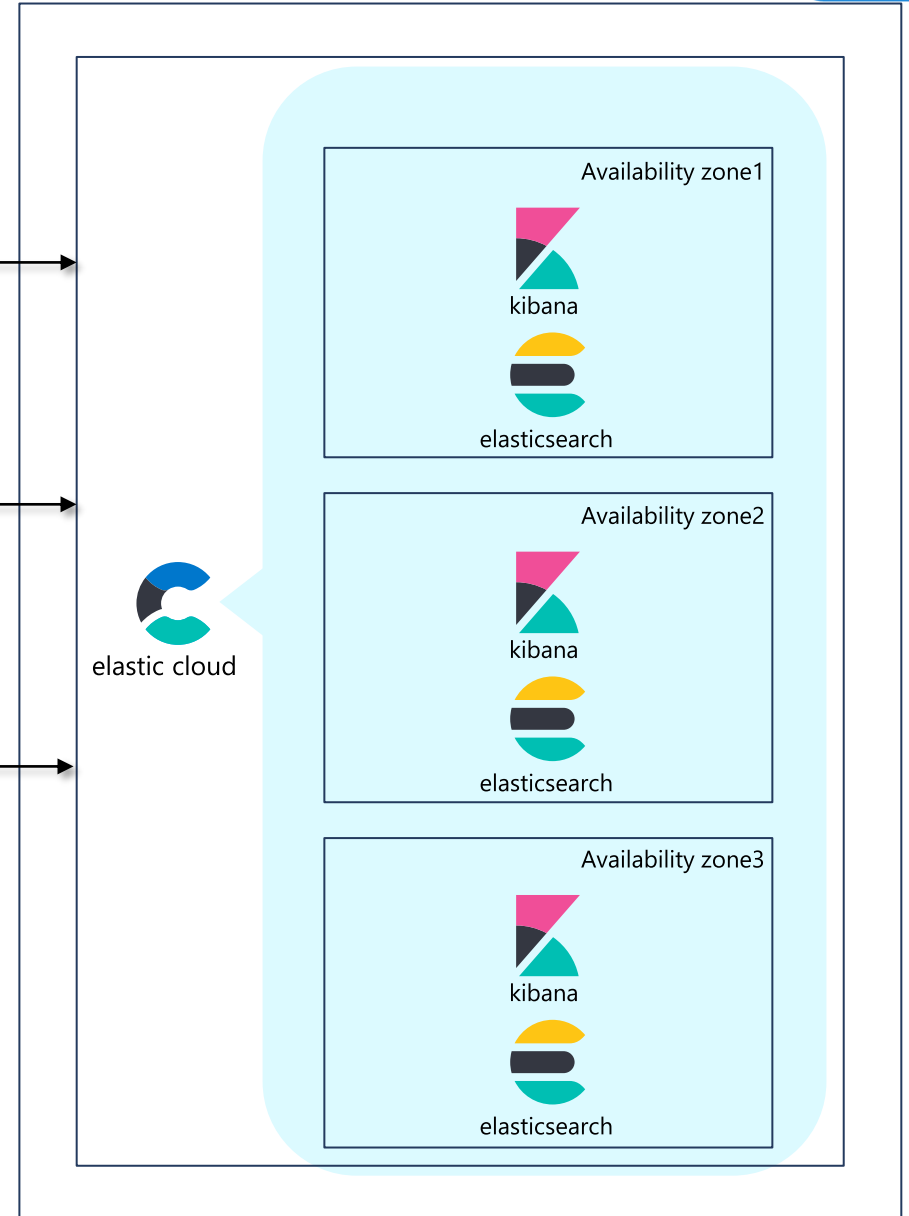
# Azure 서비스와 함께 하는 패턴 (예시)

## Beats & Logstash 등으로 데이터를 연계

고객이 관리하는 Azure 환경



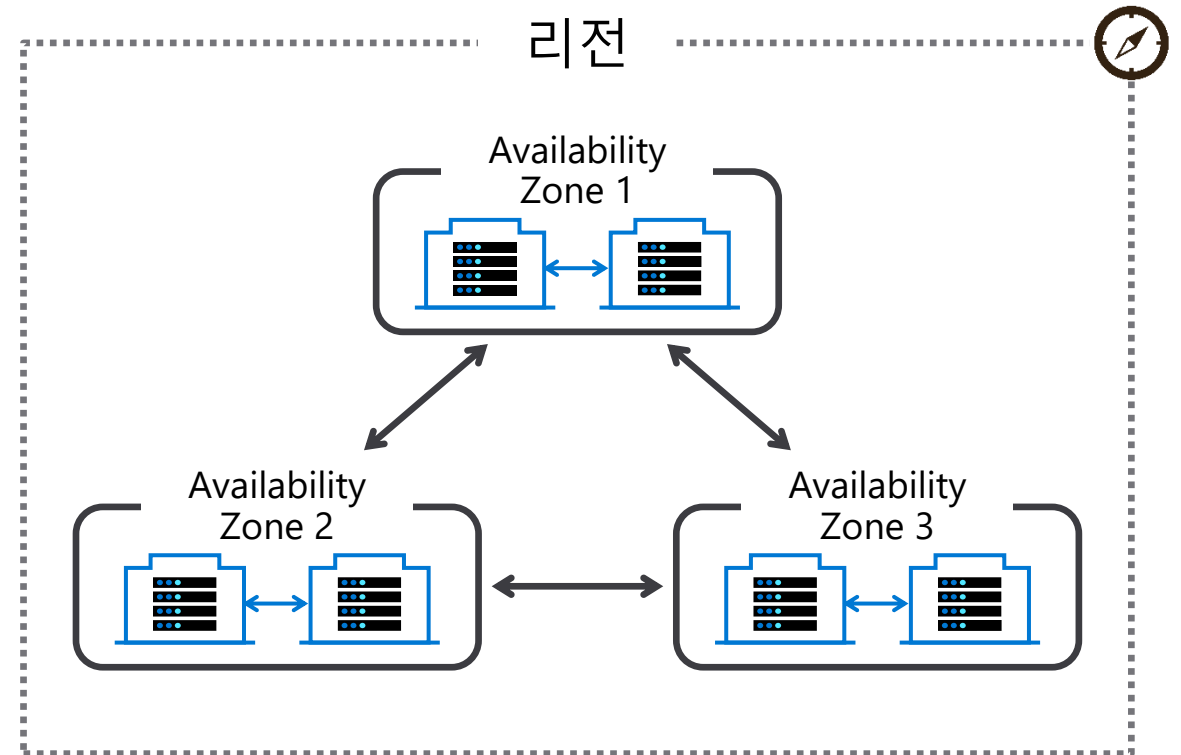
Elastic 에서 관리하는 Azure



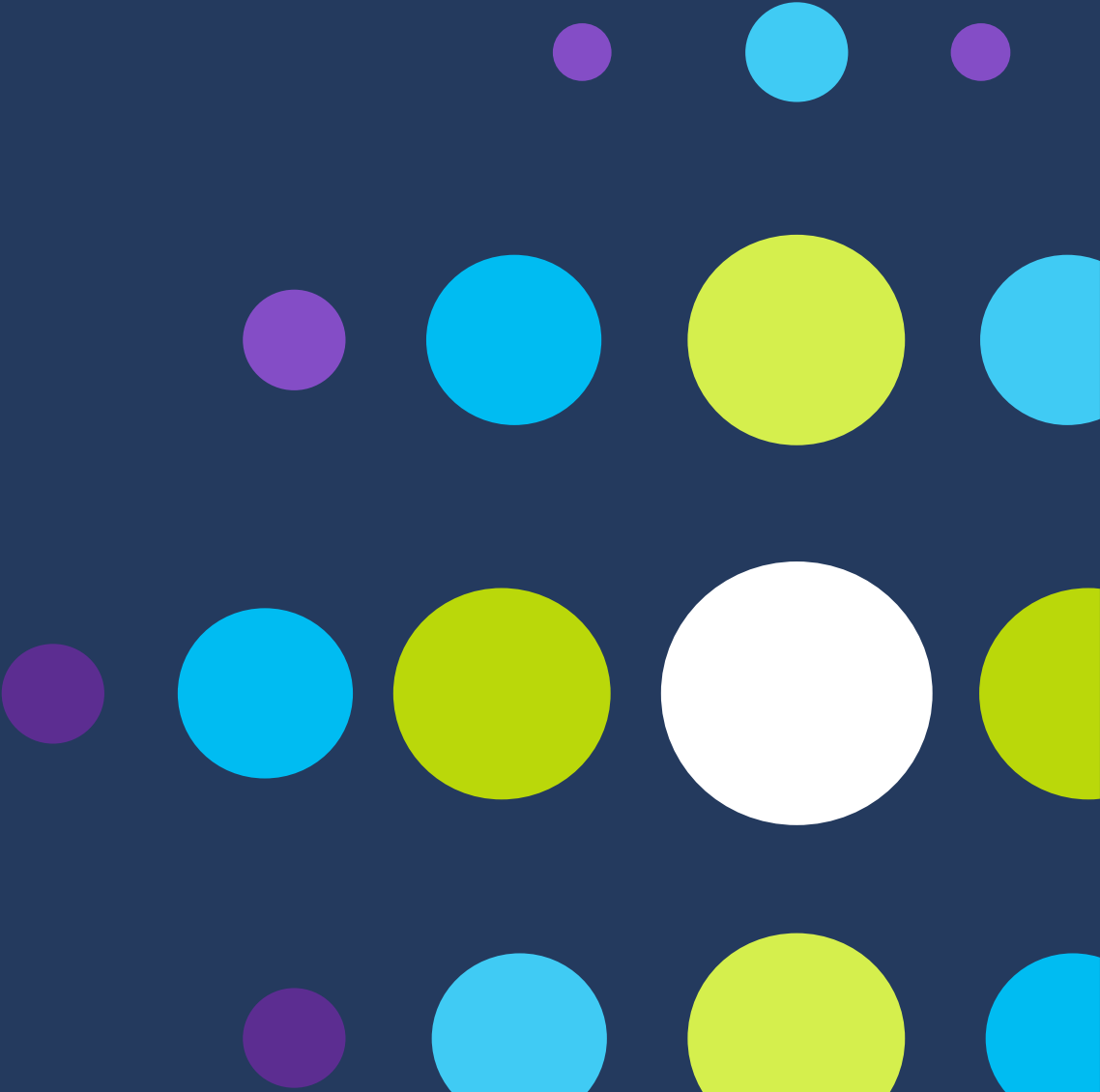
## [참고] Availability Zone (가용성 영역)

### 고가용성 지원을 위해 리전 수준으로 이중화 구성하기

- 가용성 영역은 리전 내 각각 독립적인 위치에 존재
- 각 영역은 하나 이상의 독립적인 전원, 공조, 네트워크 기능을 가진 데이터 센터 내에 구성
- 가용성 영역에서는 VM 간 대기 시간이 2ms를 넘지 않도록 설계



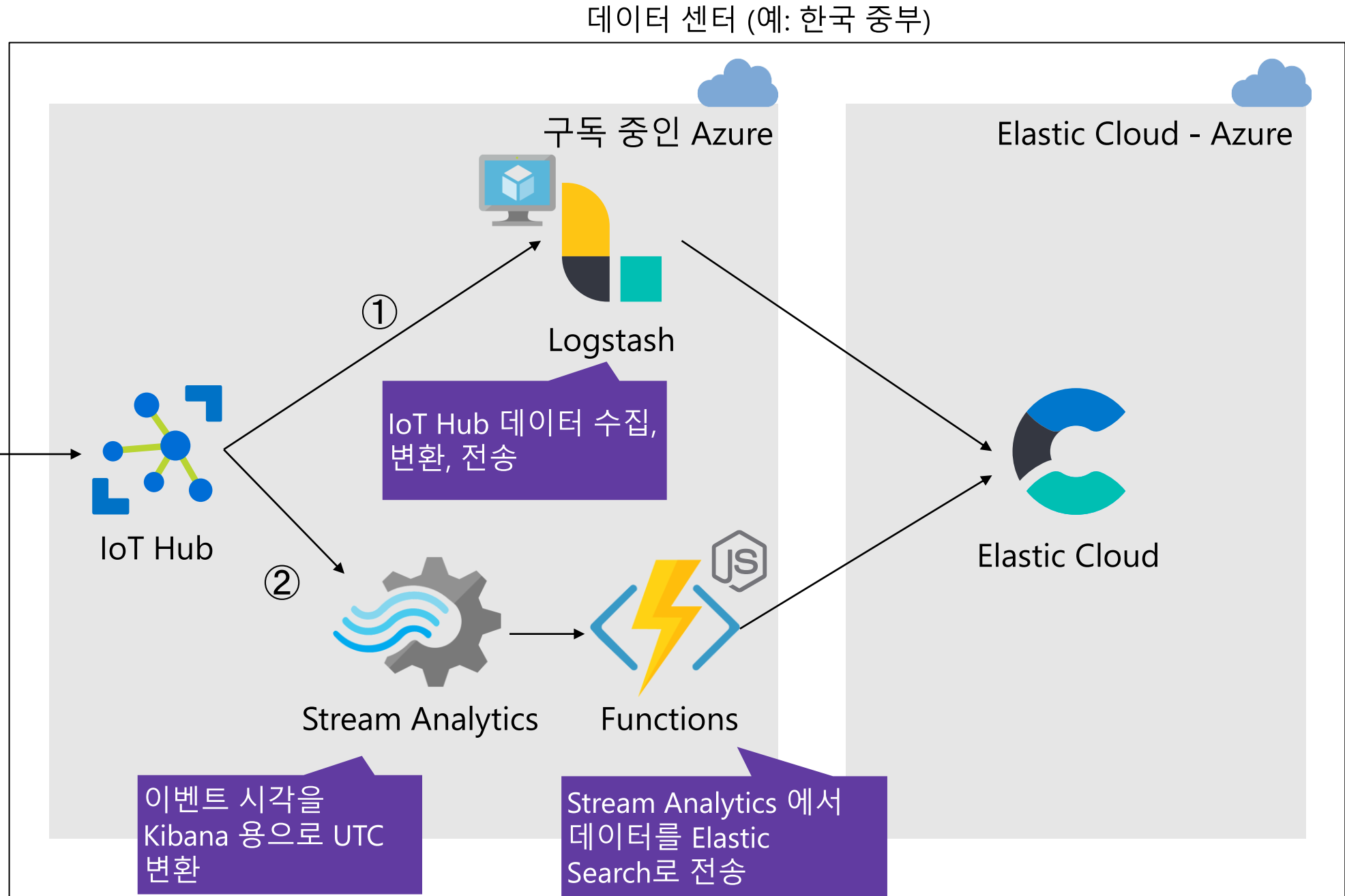
DEMO



# DEMO 구성



PC (시뮬레이터)



# IoT Hub / Event Hub 를 위한 Logstash 에서 살펴볼 점

Config file for IoT Hub

```
input {  
  azure_event_hubs {  
    event_hub_connections => ["Endpoint=sb://*****"]  
    threads => 8  
    decorate_events => true  
    consumer_group => "logstash"  
    storage_connection => "DefaultEndpointsProtocol=https;AccountName=*****"  
  }  
}
```

Azure\_event\_hubs input plugin 에서 IoT Hub 에도 연결 가능

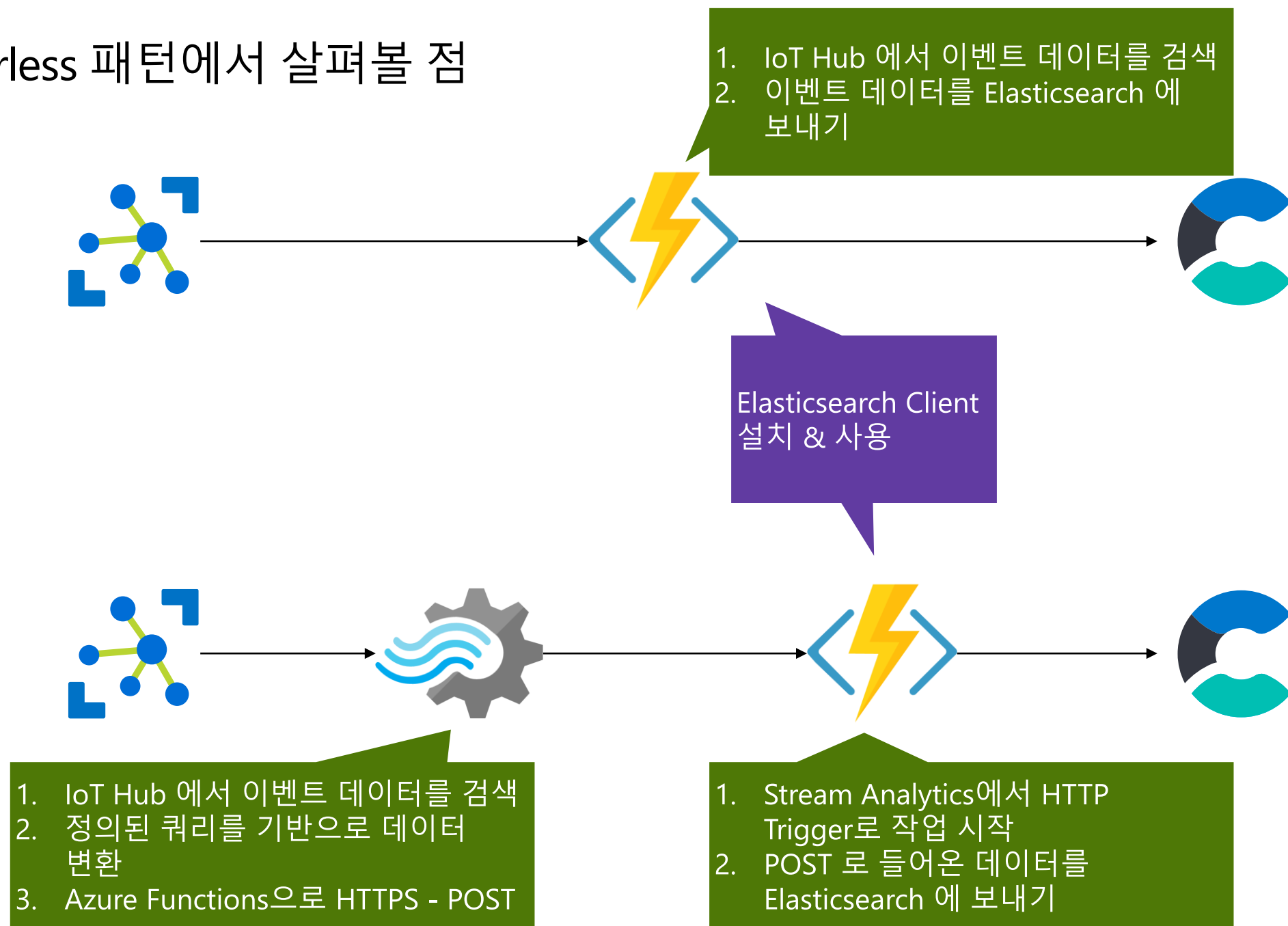
- Input / Output plugins 에서 다양한 데이터와 연계 가능
- Filter plugin 에서 유연하게 데이터 변환 가능



Event Hub / IoT Hub 를 위한 플러그인이 사전 설치되어 있어 바로 연결 가능

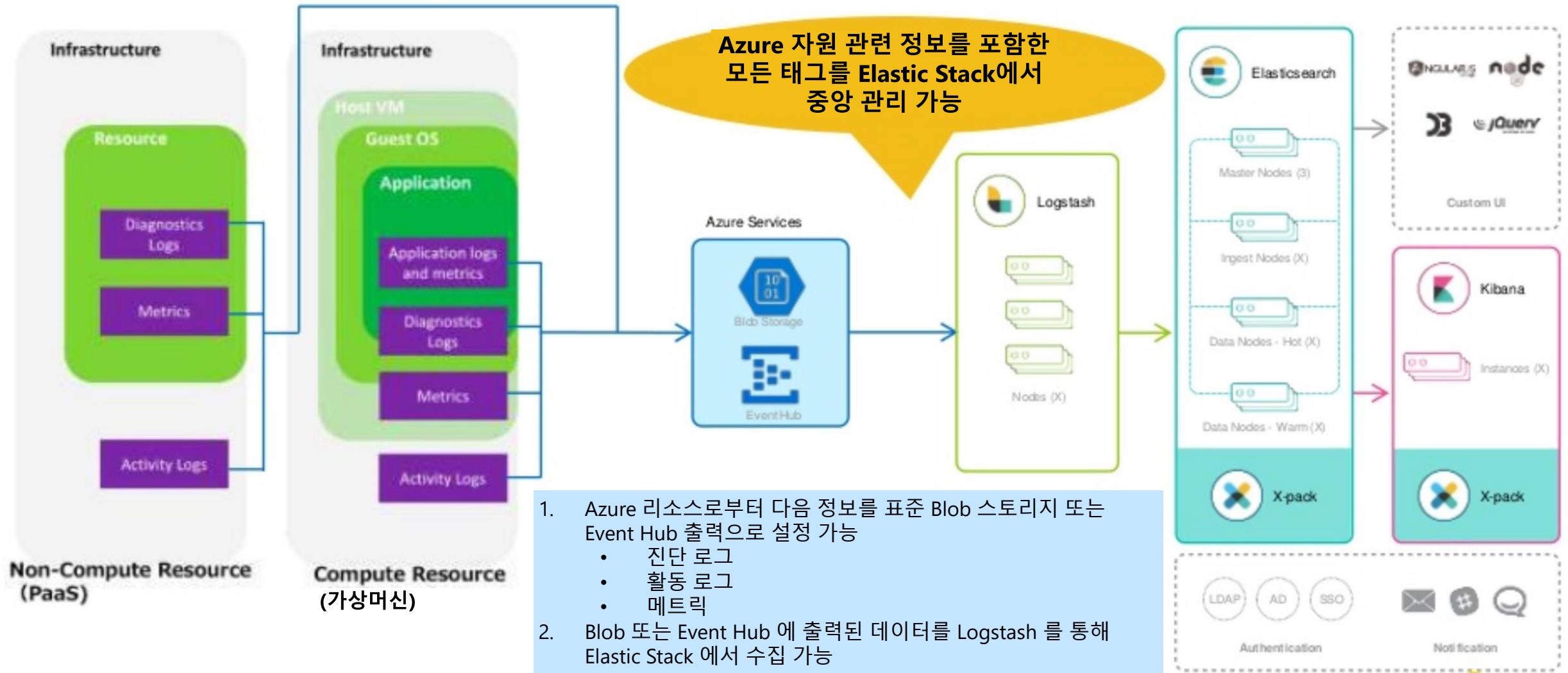


## Serverless 패턴에서 살펴볼 점

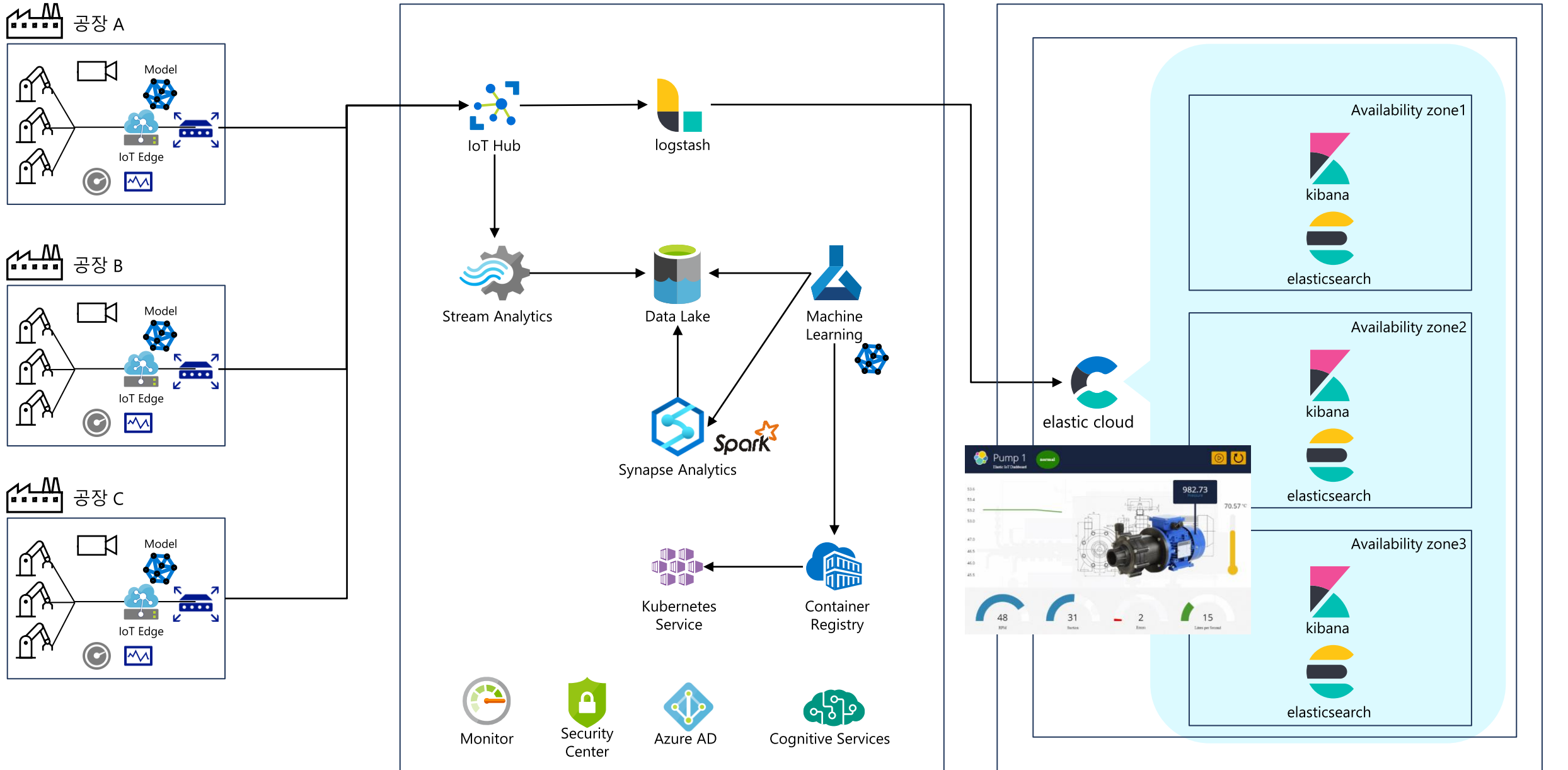


# [시나리오 1] Azure 리소스 로그 및 통계 수집 구성

Azure 진단 로그, 작업 로그, 메트릭에 대한 Elastic Stack 에서 수집



# [시나리오 2] IoT 구성



## 요약 & 정리

- ✓ Elasticsearch Service on Azure: SaaS 형태로 사용 가능하며, IaaS 기반은 마켓플레이스에서 검색 & 사용 가능
- ✓ Elastic Cloud 및 고객 Azure 환경을 활용한 안전하고 빠른 데이터 연동
- ✓ Azure 에서 다양한 서비스와 연계하여 다양한 시나리오에 적용 가능

# References

Elasticsearch Service Documentation

<https://www.elastic.co/guide/en/cloud/current/index.html>

Logstash Azure Event Hubs plugin

[https://www.elastic.co/guide/en/logstash/current/plugins-inputs-azure\\_event\\_hubs.html](https://www.elastic.co/guide/en/logstash/current/plugins-inputs-azure_event_hubs.html)

Elasticsearch Node.js client

<https://www.elastic.co/guide/en/elasticsearch/client/javascript-api/current/index.html>

Azure IoT Hub

<https://docs.microsoft.com/ja-jp/azure/iot-hub/about-iot-hub>

자습서: Azure Stream Analytics 작업에서 Azure Functions 실행하기

<https://docs.microsoft.com/ko-kr/azure/stream-analytics/stream-analytics-with-azure-functions>

DEMO: Azure Functions 샘플 코드

<https://github.com/hidwatanabe/functions-nodejs-samples/tree/master/stream-analytics-http-trigger-elastic-cloud>

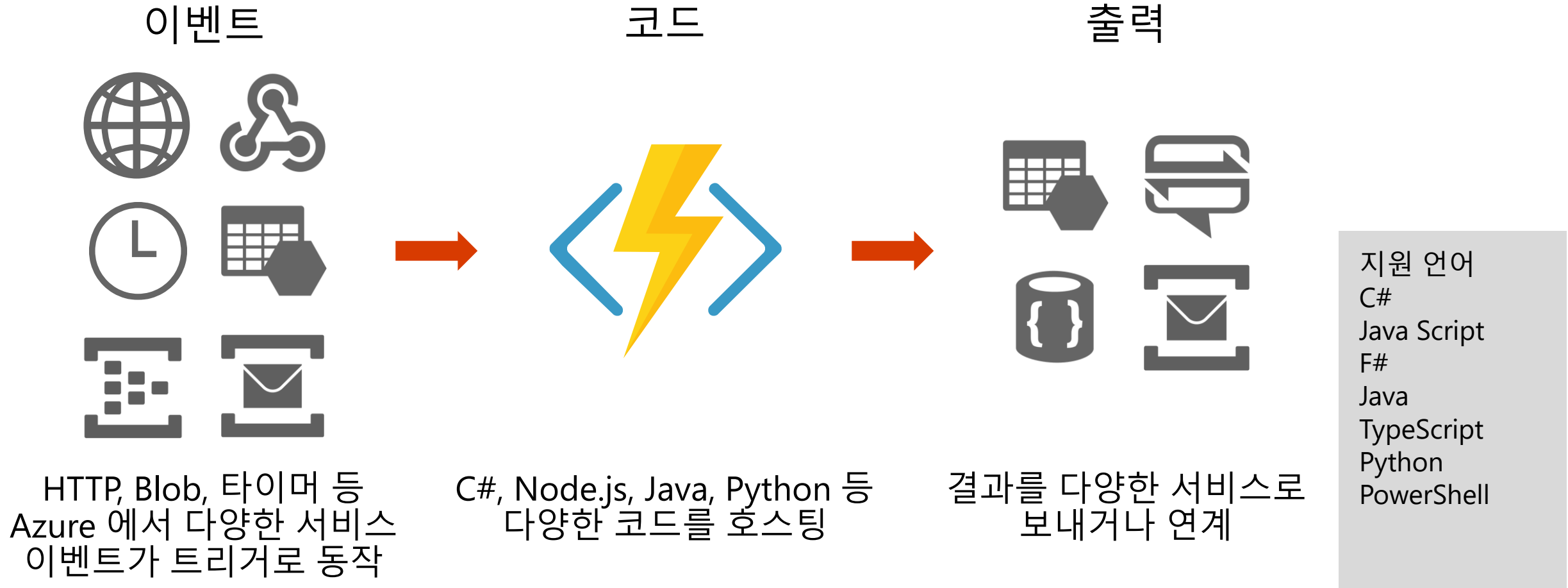


Thank you!



# [참고] Azure Functions 이란

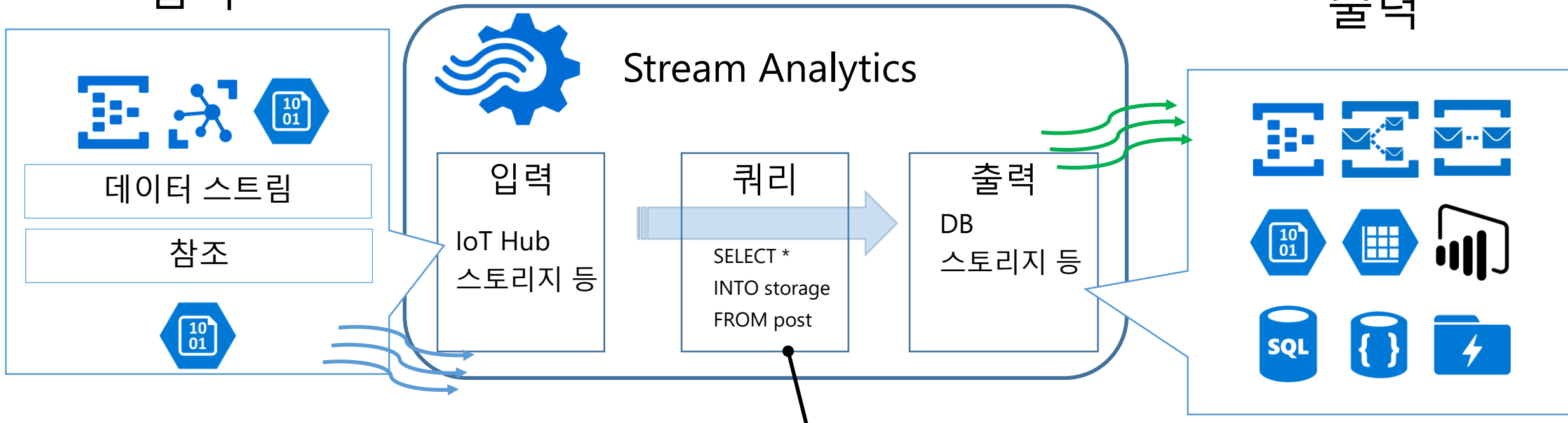
## 이벤트 기반 (Event-driven) 서버리스 컴퓨팅



## [참고] Stream Analytics 이란

스트림 데이터에 대한 전체적인 관리 & 처리를 위한 서비스

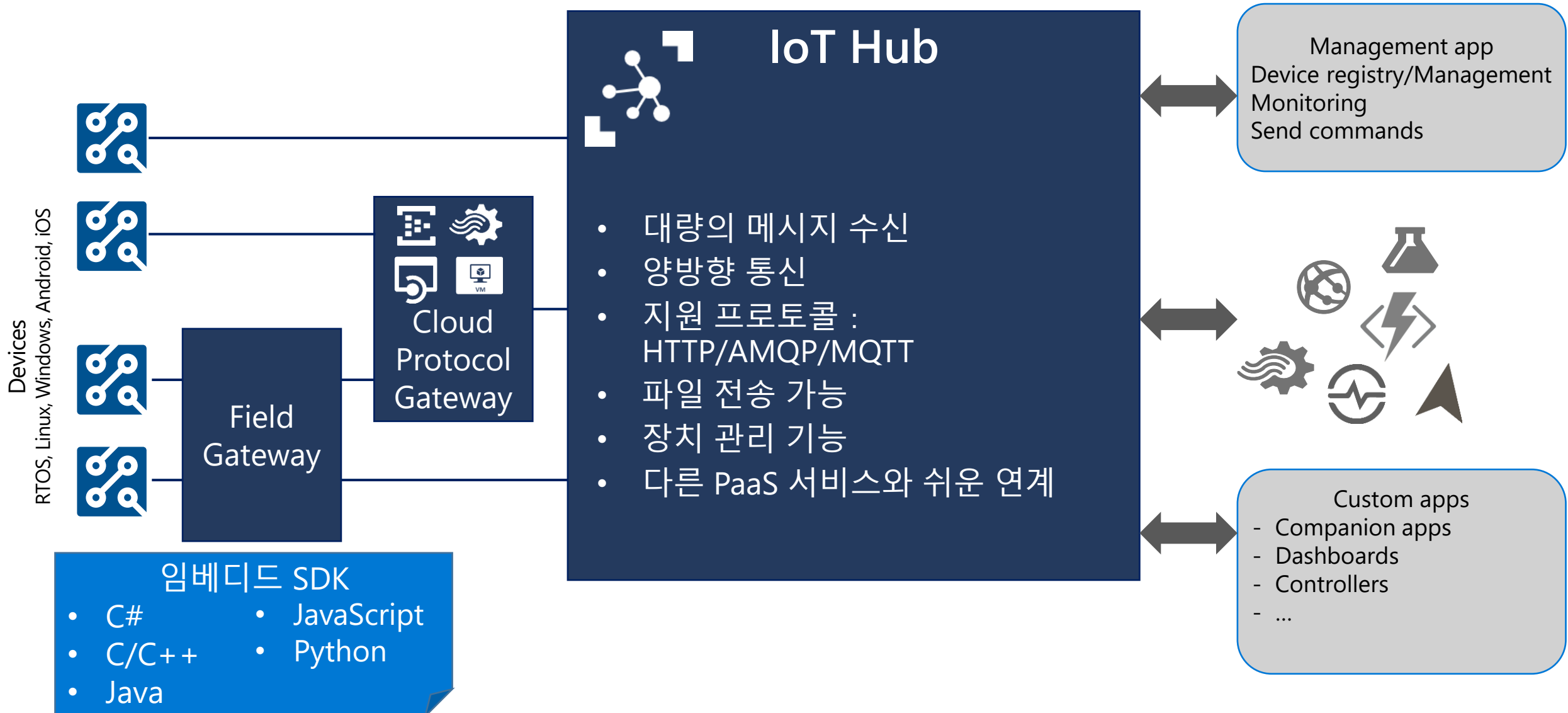
입력



SQL을 기반으로 확장된  
스크립트 언어로, 실시간  
데이터를 분석 및 처리

## [참고] Azure IoT Hub 에 대해

### 기기로부터 대량의 스트림 데이터를 수신하는 Message Queueing 서비스



# [참고] Azure IoT Edge 에 대해

## IoT Edge 모듈

클라우드 측에서 개발한 다양한 로직을 실행  
AI, AzureML, Stream Analytics, Functions,  
SQL, 사용자 정의 코드 등

## 보안

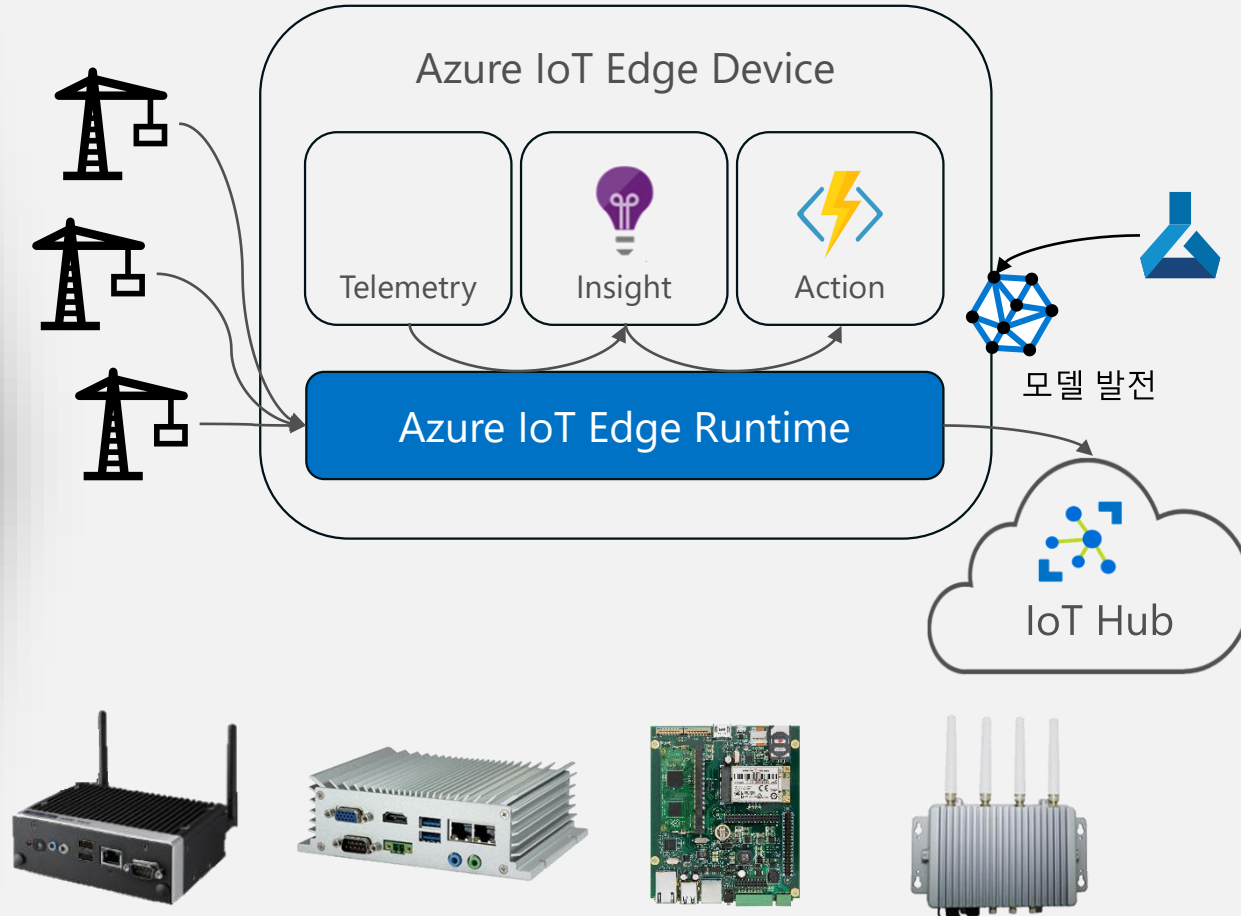
기초부터 탄탄하게 설계된 보안 및 인증 받은  
보안 장치

## 오픈 소스 및 크로스플랫폼

오픈 소스로 제공 - Linux, Windows를 비롯한  
다양한 OS 지원

## 클라우드에서 관리

원격 구성, 업데이트, 모니터링 및 관리 가능



장치에서 실행 가능한 PaaS

Azure IoT Hub, Stream Analytics, Azure Machine Learning, Azure Functions, SQL Server