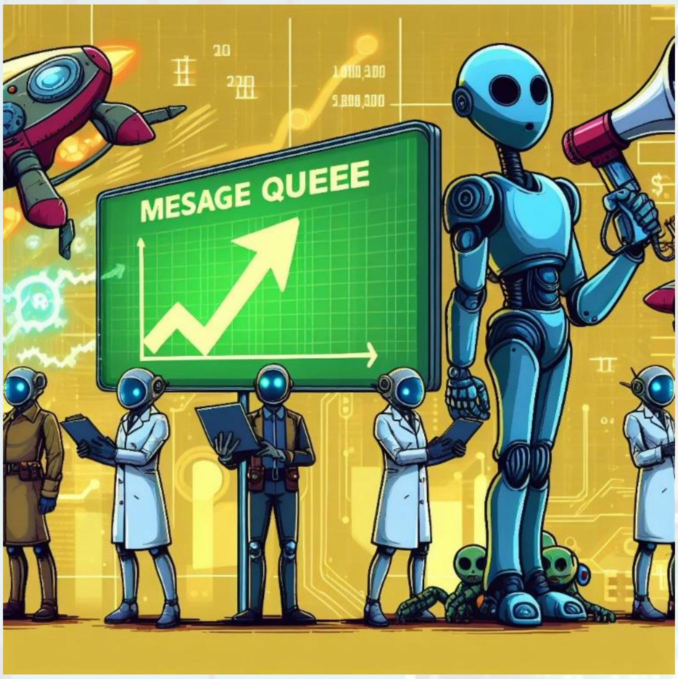

Abstract –This document provides a comprehensive analysis of the Message Queue Brokers market, focusing on various critical aspects that influence its growth and development. The document offers a high-quality summary of the current state and prospects of the Message Queue Brokers market. This analysis is particularly valuable for security professionals and other specialists across various industries, providing insights into the secure and efficient management of distributed systems. The detailed examination of performance, security, and technological trends equips stakeholders with the knowledge needed to make informed decisions and enhance their operational capabilities.

I. Introduction

Message brokers are essential components in modern distributed systems, enabling seamless communication between applications, services, and devices. They act as intermediaries that validate, store, route, and deliver messages, ensuring reliable and efficient data exchange across diverse platforms and programming languages. This functionality is crucial for maintaining the decoupling of processes and services, which enhances system scalability, performance, and fault tolerance. Message brokers support various messaging patterns, including point-to-point and publish/subscribe, catering to different use cases such as financial transactions, real-time notifications, and IoT data streaming.

The message broker market is experiencing significant growth, driven by the increasing adoption of cloud-based solutions and the need for robust, scalable communication infrastructures in distributed systems. Major players in this market include Kinesis, Cisco IoT, Solace, RabbitMQ, Apache Kafka, ApacheMQ, IBM MQ, Microsoft Azure Service Bus, and Google Cloud IoT, each offering unique capabilities and serving a wide range of industries from financial services to healthcare and smart cities. These brokers are deployed globally, with substantial user bases in regions like North America, Europe, and Asia-Pacific, reflecting their critical role in enabling modern, interconnected applications.

The following chapters provide a summary of the coverage of vulnerabilities in Chapter III and a analysis of the market coverage in Chapters IV and combined one in II.

II. Combined Data

- **Market Share**: The percentage of the market each broker holds in the queueing, messaging, and background processing category.
- **Number of Users**: The total number of companies or devices using the broker.
- **Corporate Users**: The number of enterprise customers using the broker.
- **Revenue Distribution**: The distribution of companies using the broker based on their revenue.
- **Geographical Coverage**: The percentage of users based in different regions.

Broker’s market share and user base

Broker	Market Share	Number of Users	Corporate Users
RabbitMQ	28.24%	15,851	14,651
Apache Kafka	39.73%	22,244	22,244
Apache ActiveMQ	5.79%	9,604	9,604
IBM MQ	7.12%	4,060	4,060
Microsoft Azure Service Bus	3.84%	12,870	4,609
EMQX	N/A	20,000+	500+
HiveMQ	N/A	20,000+	500+
PubNub	N/A	330M devices	500+
ThingsBoard	N/A	Thousands	500+
AWS IoT	N/A	718	718
Azure IoT	14.90%	1,396	1,396
Google Cloud IoT	18.65%	1,790	1,790
Cisco IoT	9.52%	129	129
Solace	5.33%	133	133
Amazon Kinesis	1.20%	216	216

Broker’s revenue and geo coverage

Broker	Customer	Revenue Distribution	Geographical Coverage (%)
Rabbit MQ	Currys, Beckman Coulter	< $50M: 39%, $50M-$1B: 16%, > $1B: 40%	US: 46.15%, India: 9.72%, UK: 9.70%
Apache Kafka	LinkedIn, Uber, Netflix	< $50M: 52%, $50M-$1B: 18%, > $1B: 24%	US: 51.91%, India: 12.95%, UK: 8.28%
Apache Active MQ	Infosys, Fujitsu, Panasonic	< $50M: 24%, $50M-$1B: 43%, > $1B: 33%	US: 47%, UK: 6%, India: 6%
IBM MQ	American Airlines, Aflac	< $50M: 39%, $50M-$1B: 16%, > $1B: 40%	US: 59.39%, UK: 8.70%, India: 8.67%
Microsoft Azure Service Bus	Infosys, Fujitsu, Panasonic	< $50M: 40%, $50M-$1B: 17%, > $1B: 39%	US: 48.02%, UK: 14.97%, India: 8.98%

EMQX	IoT sector companies	N/A	50+ countries
HiveMQ	Fortune 500 companies	N/A	US: 60%
PubNub	US companies	N/A	Global
Things Board	IoT sector companies	N/A	50+ countries
AWS IoT	Global companies	N/A	US: 52.12%, India: 13.26%, UK: 8.84%
Azure IoT	Global companies	N/A	US: 47.72%, India: 14.04%, UK: 8.73%
Google Cloud IoT	Global companies	N/A	US: 48.77%, India: 16.58%, Germany:6.39%
Cisco IoT	Infosys, Cisco Systems, Wipro, AT&T, Cognizant	< $50M: 25%, $50M-$1B: 17%, > $1B: 47%	US: 50%, India: 9%
Solace	Large enterprises in finance, telecom, manufacturing	< $50M: 16%, $50M-$1B: 29%, > $1B: 49%	US: 38.18% France:10.91% Canada: 10%
Amazon Kinesis	Siemens, Microsoft, Oracle, Cisco	< $50M:25%, $50M-$1B: 15%, > $1B: 60%	US: 61.78% India:10.47% UK: 8.38%

III. BROKER'S VULNERABILITY COVERAGE

A. RabbitMQ

- **Windows-Specific Binary Planting Vulnerability**: RabbitMQ versions 3.8.x prior to 3.8.7 are prone to a Windows-specific binary planting security vulnerability that allows for arbitrary code execution. An attacker with write privileges to the RabbitMQ installation directory and local access on Windows could carry out a local binary hijacking (planting) attack and execute arbitrary code.

- **Denial of Service (DoS) via "X-Reason" HTTP Header**: RabbitMQ versions 3.7.x prior to 3.7.21 and 3.8.x prior to 3.8.1 contain a web management plugin that is vulnerable to a denial-of-service attack The "X-Reason" HTTP Header can be leveraged to insert a malicious Erlang format string that will expand and consume the heap, resulting in the server crashing.

- **Cross-Site Scripting (XSS) Vulnerabilities**: Several forms in the RabbitMQ management UI are vulnerable to XSS attacks. This includes versions prior to v3.7.18 and RabbitMQ for PCF versions 1.15.x prior to 1.15.13, 1.16.x prior to 1.16.6, and 1.17.x prior to 1.17.3.

- **MQTT Authentication Bypass**: An issue was discovered in RabbitMQ 3.x before 3.5.8 and 3.6.x before 3.6.6 where MQTT connection authentication with a username/password pair succeeds if an existing username is provided but the password is omitted from the connection request.

- **Sensitive Information Exposure**: The metrics-collection component in RabbitMQ for Pivotal Cloud Foundry (PCF) 1.6.x before 1.6.4 logs command lines of failed commands, which might allow context-dependent attackers to obtain sensitive information by reading the log data.

- **Denial of Service via AMQP 1.0 Client Connection Endpoint:** RabbitMQ all versions prior to 3.8.16 are prone to a DoS vulnerability due to improper input validation in the AMQP 1.0 client connection endpoint.

- **TLS/DTLS Authentication Bypass (CVE-2022-37026):** A critical vulnerability identified as CVE-2022-37026 originates from a bug in Erlang OTP and may allow a malicious actor to bypass the authentication process and impersonate other users when the server is configured to use TLS or DTLS authentication.

B. Apache Kafka

- **Denial of Service (DoS) via InternalTopicManager**: A bug in the InternalTopicManager prior to 2.1.0 can cause a DoS attack. When a topic is marked for deletion but not yet deleted, the Broker gives inconsistent information, causing the client to enter a loop polling for topic metadata, leading to a DoS condition.

- **Timing Attack Vulnerability (CVE-2021-38153):** Some components in Apache Kafka 2.0.0 to 2.8.0 use Arrays.equals to validate a password or key, which is vulnerable to timing attacks, making brute force attacks more likely to succeed.

- **Plaintext Secrets Exposure (CVE-2019-12399):** The Kafka 2.0.0 to 2.3.0 Connect REST API may expose plaintext secrets in the tasks endpoint when configured with one or more config providers.

- **Out-of-Memory (OOM) via Snappy Compression (CVE-2023-34455):** A vulnerability in the snappy-java library used by Kafka 0.8.0 to 3.5.0 can cause an Out-of-Memory (OOM) condition, leading to a DoS attack when a malicious payload compressed using snappy-java is decompressed by Kafka.

- **Remote Code Execution (RCE) via Kafka Connect (CVE-2023-25194):** Unsafe deserialization in the Kafka Connect 2.3.0 to 3.3.2 REST API can allow a remote authenticated attacker to execute arbitrary code or cause a DoS attack.

- **Denial of Service via Improper Input Validation (CVE-2022-34917):** Improper input validation can allow a remote attacker to allocate large amounts of memory on brokers, resulting in a DoS condition.

- **Java Deserialization Vulnerability (CVE-2023-34040):** A deserialization attack in Spring for Apache Kafka 3.0.9 and earlier, 2.9.10 and earlier can be exploited if unusual configuration is applied, allowing an attacker to construct a malicious serialized object.

C. ApacheMQ

- **CVE-2023-46604: Remote Code Execution (RCE):** This critical vulnerability allows remote attackers to execute arbitrary shell commands by exploiting serialized class types in the OpenWire protocol. The flaw is due to the failure to properly validate throwable class types when OpenWire commands are unmarshalled. Affected Versions: Apache ActiveMQ 5.18.x before 5.18.3, Apache ActiveMQ 5.17.x before 5.17.6, Apache ActiveMQ 5.16.x before 5.16.7, All versions before 5.15.16

- **CVE-2022-41678: Deserialization Vulnerability:** This vulnerability in Jolokia allows authenticated users to perform remote code execution (RCE) by exploiting deserialization of untrusted data.
- **CVE-2020-13947: Cross-Site Scripting (XSS):** XSS vulnerabilities in the WebConsole allow remote attackers to inject arbitrary web scripts or HTML.
- **CVE-2020-13920: JMX MITM Vulnerability:** A man-in-the-middle (MITM) vulnerability in JMX allows remote attackers to intercept and manipulate communications.
- **CVE-2016-3088: Remote File Upload and Execution:** Fileserver web application in Apache ActiveMQ allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.
- **CVE-2015-1830: Path Traversal Leading to RCE:** A path traversal vulnerability in the fileserver upload/download functionality allows remote attackers to create JSP files in arbitrary directories, leading to remote code execution.
- **CVE-2014-3576: Remote Unauthenticated Shutdown of Broker (DoS):** This vulnerability allows remote attackers to shut down the broker without authentication, leading to a denial of service (DoS).

D. IBM MQ

- **CVE-2022-27780 and CVE-2022-30115:** These vulnerabilities reside within the libcurl library used by IBM MQ 9.2 LTS, 9.1 LTS, 9.0 LTS, 9.2 CD, and 9.1 CD. CVE-2022-27780 allows an attacker to bypass security restrictions using a specially crafted host name in a URL. CVE-2022-30115 is a HSTS check bypass flaw that could be exploited to obtain sensitive information over clear-text HTTP.
- **CVE-2023-26285: Denial of Service (DoS):** IBM MQ 8.0, 9.0-9.1 LTS, 9.2 LTS, 9.3 LTS, 9.1 CD, 9.2 CD, and 9.3 CD.is vulnerable to a DoS attack caused by an error processing invalid data from a compromised client.
- **CVE-2022-43902: Denial of Service (DoS) via PCF or MQSC Messages**: An authenticated attacker with sufficient MQ permissions can send specially crafted PCF or MQSC messages to execute a DoS attack. Affected Versions: IBM MQ 9.1-9.3 LTS, 9.1-9.3 CD.
- **CVE-2023-45177: Denial of Service (DoS) via MQ Clustering Logic:** IBM MQ Appliance 9.2 LTS, 9.3 LTS, and 9.3 CD.is vulnerable to a DoS attack due to an error within the MQ clustering logic.
- **CVE-2022-21624 and CVE-2022-21626: Java Runtime Environment Vulnerabilities:** Multiple vulnerabilities in the IBM Runtime Environment Java Technology Edition, Version 8, which is shipped with IBM MQ. CVE-2022-21624 allows an unauthenticated attacker to update, insert, or delete data. CVE-2022-21626 allows an unauthenticated attacker to cause a DoS. Affected Versions: IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, 9.1 CD, 9.2 CD, and 9.3 CD.
- **CVE-2023-22081 and CVE-2023-5676: Java SE and Eclipse OpenJ9 Vulnerabilities:** CVE-2023-22081 is an unspecified vulnerability in Java SE related to the JSSE component, allowing a remote attacker to cause low availability impact. CVE-2023-5676 in Eclipse OpenJ9 can cause an infinite busy hang or segmentation fault when a shutdown signal is received before JVM initialization. Affected Versions: IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS, and 9.3 CD.
- **CVE-2020-13947: Cross-Site Scripting (XSS):** XSS vulnerabilities in the WebConsole allow remote attackers to inject arbitrary web scripts or HTML.
- **CVE-2020-13920: JMX MITM Vulnerability:** A MITM vulnerability in JMX allows remote attackers to intercept and manipulate communications.
- **CVE-2016-3088: Remote File Upload and Execution:** Fileserver web application in Apache ActiveMQ allows remote attackers to upload and execute arbitrary files via an HTTP PUT followed by an HTTP MOVE request.
- **CVE-2015-1830: Path Traversal Leading to RCE:** A path traversal vulnerability in the fileserver upload/download functionality allows remote attackers to create JSP files in arbitrary directories, leading to remote code execution.
- **CVE-2014-3576: Remote Unauthenticated Shutdown of Broker (DoS):** This vulnerability allows remote attackers to shut down the broker without authentication, leading to a denial of service (DoS).

E. Microsoft Azure Service Bus

- **Denial of Service (DoS) Vulnerability (MS14-042):** A vulnerability in Microsoft Service Bus for Windows Server could allow a remote authenticated attacker to create and run a specially crafted script, leading to a denial of service (DoS) condition.
- **Denial of Service (DoS) via Resource Exhaustion:** Azure Service Bus may become unavailable during DoS attacks aimed at overwhelming its resources or disrupting its operation. This can occur due to network issues, service outages, resource exhaustion, configuration errors, security concerns, software bugs, or data center failures.
- **Remote Code Execution (RCE) in Power Platform Connectors:** A RCE vulnerability was discovered in Power Platform Connectors that allowed access to cross-tenant data. This issue was fixed by rebuilding the serialization binder to enforce stricter type allow lists.

- **Data Encryption and Security Risks:** While Azure Service Bus supports encryption in transit and at rest, there are risks associated with data exfiltration, unauthorized data movements, and unauthorized access. Proper logging and monitoring are essential to detect and respond to these risks.

F. *EMQX*

- **CVE-2021-33175: Denial of Service (DoS):** A vulnerability in EMQX versions prior to 4.2.8 allows for a denial of service (DoS) attack due to excessive memory consumption when handling malformed MQTT messages.
- **CVE-2023-46604: Directory Traversal:** A directory traversal vulnerability in the emqx_sn plugin of EMQX v4.3.8 allows attackers to execute a directory traversal via uploading a crafted .txt file.
- **Heap Buffer Overflow Vulnerabilities:** Multiple heap buffer overflow vulnerabilities exist in NanoMQ 0.21.7, a component of EMQX, which can be exploited to cause a denial of service (DoS) via specially crafted hexstreams.
- **Use-After-Free Vulnerability:** A use-after-free vulnerability in NanoMQ v0.21.2 allows attackers to cause a denial of service via crafted MQTT messages.
- **Null Pointer Dereference:** A null pointer dereference vulnerability in the topic_filtern function in mqtt_parser.c in NanoMQ 0.21.7 allows attackers to cause a denial of service.
- **Username Enumeration:** EMQX Dashboard v3.0.0 is affected by a username enumeration vulnerability in the "/api/v3/auth" interface, allowing attackers to determine if a given username is valid.
- **Denial of Service via Memory Consumption**: EMQX Broker versions prior to 4.2.8 are vulnerable to a denial-of-service attack due to excessive memory consumption when handling untrusted inputs.
- **TLS Protocol Session Renegotiation Vulnerability:** A vulnerability related to TLS protocol session renegotiation on port 8084 (TCP over SSL).

G. *HiveMQ*

- **CVE-2020-13821: Reflected Cross-Site Scripting (XSS):** A vulnerability in the HiveMQ Broker Control Center (version 4.3.2) allows for reflected cross-site scripting (XSS). This can be exploited by an attacker to execute arbitrary web scripts or HTML in the context of the user's browser.
- **Denial of Service (DoS) via Resource Exhaustion:** HiveMQ can be vulnerable to DoS attacks that aim to exhaust broker resources such as disk, RAM, or CPU. This can occur if an attacker sends many heavy messages or exploits the broker's handling of message queues.
- **SlowITe Attack:** SlowITe attack exploits the MQTT protocol's Keep-Alive parameter, allowing an attacker to set an arbitrary value that keeps the connection open for an extended period, leading to a DoS condition.
- **Heap-Based Buffer Overflow:** vulnerability in the HiveMQ Broker can be exploited to cause a denial of service (DoS) or potentially execute arbitrary code.

H. *Pubhub*

- **CVE-2023-26154: Insufficient Entropy:** This vulnerability in the PubNub package (versions before 6.19) involves insufficient entropy in the generation of cryptographic keys, which can be exploited by an attacker to brute-force the encryption.
- **Reflected Cross-Site Scripting (XSS):** A vulnerability in the platform allows for reflected XSS attacks. This can be exploited by an attacker to execute arbitrary web scripts or HTML in the context of the user's browser.
- **Persistent Connection Vulnerability:** There are concerns about the security of PubNub's persistent connections through port 80 or port 443. While PubNub claims these connections are safe, vulnerabilities could still exist if not properly managed.
- **Security Vulnerabilities in Insteon Hub:** Multiple vulnerabilities were discovered in the Insteon Hub, which uses PubNub for communication. These vulnerabilities range from RCE to DoS attacks.
- **Vulnerabilities in Custom Implementations:** Custom implementations of PubNub, especially those using older versions or insecure config, may be vulnerable to various attacks, including MITM and data exfiltration.

I. *Thingsboard*

- **CVE-2022-45608: Vertical Privilege Escalation:** A vulnerability in ThingsBoard IoT platform version 3.4.2 allows a low-privileged user (CUSTOMER_USER) to escalate their privileges to become an Administrator (TENANT_ADMIN) or system administrator (SYS_ADMIN) using a simple POST request with the platform’s REST API.
- **CVE-2023-26462: Insecure Secret Key Management:** A vulnerability allows attackers to escalate privileges within the system by manipulating JSON Web Tokens (JWTs). The static default secret key used for signing JWTs can be exploited to re-sign modified tokens, granting unauthorized access. Affected Versions: Prior to version 3.4.2.
- **CVE-2021-42751: Stored Cross-Site Scripting (XSS):** A stored XSS vulnerability in ThingsBoard version 3.3.1 allows attackers to execute arbitrary JavaScript code by injecting a script payload into the description field of a rule node.
- **CVE-2023-45303: Server-Side Template Injection:** ThingsBoard before version 3.5 is vulnerable to server-side template injection if users are allowed to modify an

email template. This vulnerability can be exploited to execute arbitrary code on the server.

- **CVE-2020-27687: Host Header Injection:** Product before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails.
- **CVE-2023-26462: Default Static Key:** The use of a default static key for signing JWTs in ThingsBoard allows attackers to forge valid requests and escalate privileges. Affected Versions: Prior to version 3.4.2.

J. *Solace*

- **Kernel Vulnerabilities:** Multiple kernel vulnerabilities have been identified and addressed in Solace PubSub+ Event Broker Appliance and Software versions prior to 9.10.0. These vulnerabilities include issues that could lead to denial of service (DoS), privilege escalation, and other security risks. CVE IDs: CVE-2021-26930, CVE-2021-26931, CVE-2021-26932, CVE-2021-27363, CVE-2021-27364, CVE-2021-27365, CVE-2021-28038, CVE-2021-30002, CVE-2019-19060, CVE-2021-28660, CVE-2021-29265, CVE-2021-28964, CVE-2021-28971, CVE-2021-28972, CVE-2021-28688, CVE-2021-29647, CVE-2021-3483, CVE-2021-29154, CVE-2020-25670, CVE-2020-25671, CVE-2020-25672
- **Amazon Linux 2 Vulnerabilities:** Several critical vulnerabilities in Amazon Linux 2, including issues in systemd and the kernel, have been addressed. These vulnerabilities could lead to remote code execution (RCE), denial of service (DoS), and other security risks. CVE IDs: CVE-2018-15686, CVE-2018-16864, CVE-2018-16866, CVE-2018-16888, CVE-2019-20386, CVE-2019-3815, CVE-2019-6454, CVE-2021-33200
- **Apache Log4j Vulnerabilities:** The Apache Log4j vulnerabilities (Log4Shell) allow for remote code execution (RCE) and have been widely publicized. These vulnerabilities affect many systems that use Log4j for logging. CVE IDs: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2022-23305
- **Spring Framework Vulnerabilities:** Multiple vulnerabilities in the Spring Framework and Spring Cloud could lead to remote code execution (RCE) and other security risks.
- **OpenSSL Vulnerability:** A critical vulnerability in OpenSSL could lead to security risks such as man-in-the-middle (MITM) attacks.
- **XZ Utils Vulnerability:** A vulnerability in XZ Utils was identified, but it was determined that no Solace products were affected.

K. *AWS IoT*

- **Denial of Service (DoS) via Resource Exhaustion:** AWS IoT can be vulnerable to DoS attacks that aim to exhaust broker resources such as disk, RAM, or CPU. This occur if an attacker sends many heavy messages or exploits the broker's handling of message queues.
- **Cross-Site Scripting (XSS):** XSS vulnerabilities in the AWS IoT platform can allow attackers to inject malicious scripts into the context of the user's browser, potentially leading to data theft or further exploitation.
- **Host Header Injection:** AWS IoT before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails. CVE ID: CVE-2020-27687

L. *Azure IoT*

- **CVE-2024-27099: Remote Code Execution (RCE) in uAMQP C Library:** A vulnerability in the uAMQP C library used by Azure IoT for communication with Azure Cloud Services. The vulnerability, caused by a "double free" memory error, can lead to RCE
- **CVE-2021-42312, CVE-2021-37222, CVE-2021-42313, CVE-2021-42311: Multiple Critical Vulnerabilities in Azure Defender for IoT:** Multiple vulnerabilities in Azure Defender for IoT, including issues in the password reset mechanism and SQL injection vulnerabilities, allow unauthenticated attackers to gain unauthorized access and potentially RCE.
- **CVE-2019-0741: Information Disclosure in Azure IoT Java SDK:** An information disclosure vulnerability in the Azure IoT Java SDK logs sensitive information, which can be exploited by an attacker to gain access to sensitive data.
- **Host Header Injection:** Azure IoT before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails. CVE ID: CVE-2020-27687
- **Insecure Secret Key Management:** A vulnerability involving insecure secret key management allows attackers to escalate privileges within the system by manipulating JSON Web Tokens (JWTs). The static default secret key used for signing JWTs can be exploited to re-sign modified tokens, granting unauthorized access. CVE ID: CVE-2023-26462

M. *Google Cloud IoT*

- **Weak Passwords and Authentication Issues:** A significant portion of attacks on Google Cloud Platform (GCP) instances, including IoT deployments, are due to weak passwords or no passwords at all. In 48% of the analyzed cases, weak or absent passwords were the primary cause of successful attacks.
- **Vulnerabilities in Cloud-Server Software:** In 26% of the cases, vulnerabilities in the cloud-server software were exploited by attackers. These vulnerabilities can lead to unauthorized access and control over the IoT devices and data.
- **Server or Application Misconfiguration:** Misconfigurations in servers or applications accounted

for 12% of the successful attacks that can expose sensitive data and services to unauthorized access.

- **Password or Access Key Leaks:** In 4% of the cases, password or access key leaks were the cause of successful attacks due to authentication data is uploaded to public repositories like GitHub.
- **CVE-2023-44487: HTTP/2 Rapid Reset DDoS Vulnerability:** A high-severity vulnerability in the HTTP/2 protocol, known as the "Rapid Reset" technique, can be exploited to launch large-scale DDoS attacks. This vulnerability affects web applications, services, and APIs that use HTTP/2.
- **CVE-2023-52620: Privilege Escalation in Linux Kernel:** A vulnerability in the Linux kernel lead to privilege escalation on Container-Optimized OS and Ubuntu nodes. This vulnerability can be exploited to gain unauthorized access and control over the system.
- **CVE-2023-5736: Container Escape Vulnerability:** A vulnerability in the runc container runtime, used by Docker and Kubernetes, allows an attacker to escape the container and execute code on the host system.
- **GhostToken Vulnerability:** A vulnerability in Google Cloud Platform (GCP) allowed attackers to modify and hide OAuth applications, creating a stealthy backdoor to any Google account. This vulnerability, referred to as GhostToken, could be exploited to retrieve account tokens and access the victim’s data.

N. *Kinesis IoT*

- **Cross-Site Scripting (XSS):** XSS vulnerabilities in the AWS IoT platform can allow attackers to inject malicious scripts into the context of the user's browser, potentially leading to data theft or further exploitation.
- **Denial of Service (DoS) via Resource Exhaustion**: AWS Kinesis can be vulnerable to DoS attacks that aim to exhaust broker resources such as disk, RAM, or CPU. This can occur if an attacker sends many heavy messages or exploits the broker's handling of message queues.
- **Host Header Injection**: AWS IoT before version 3.2 is vulnerable to host header injection in password-reset emails. This allows an attacker to send malicious links in password-reset emails. CVE ID: CVE-2020-27687

O. *Cisco Internet of Things*

- **CVE-2022-20773: Cross-Site Scripting (XSS) in Cisco IoT Control Center:** A vulnerability in the web-based management interface of Cisco IoT Control Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input.
- **CVE-2023-20198: Privilege Escalation in Cisco IOS XE:** A critical flaw in the IOS XE web interface can be exploited by remote, unauthenticated attackers for privilege escalation. This vulnerability allows threat actors to create high-privileged accounts on targeted devices and take complete control of the system.
- **CVE-2023-31242 and CVE-2023-34998: Authentication Bypass in OAS Platform:** Multiple vulnerabilities in the Open Automation Software (OAS) Platform prior version 19.00.0000, which is used in industrial IoT environments, can be exploited to bypass authentication, leak sensitive information, and overwrite files. These vulnerabilities allow attackers to gain unauthorized access and control over the system.
- **CVE-2023-34317: Improper Input Validation in OAS Platform:** An improper input validation bug in the user creation functionality of the OAS Platform prior version 19.00.0000 allows attackers to add a user with the username field containing an SSH key, potentially gaining access to the underlying system.
- **CVE-2023-34353: Information Disclosure in OAS Platform:** An authentication bypass vulnerability in the OAS Platform prior version 19.00.0000 allows an attacker to perform network sniffing to capture the protobuf containing admin credentials and then decrypt sensitive information.
- **CVE-2020-7592: Data Integrity Compromise in Siemens Devices:** A vulnerability impacting various Siemens devices and components where data integrity can be compromised.

IV. Broker Market Coverage

A. *RabbitMQ*

RabbitMQ is a robust and widely adopted message broker with a significant market share in the queueing, messaging, and background processing market. It is used by thousands of companies globally, including major corporations like Alcatel-Lucent, University of California - San Diego, and Beckman Coulter. RabbitMQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in financial services, healthcare, e-commerce, telecommunications, and manufacturing. The competitive landscape includes other major players like Apache Kafka, IBM MQ, and Apache ActiveMQ, but RabbitMQ's extensive feature set and proven performance give it a strong position in the market.

1) *Market Share & Geographical Distribution*

- RabbitMQ holds a significant market share in the queueing, messaging, and background processing market, with approximately 28.24%.
- **Global Presence:** RabbitMQ is used in 93 countries worldwide.
- **United States:** 46.15% of RabbitMQ's customers are based in the United States.
- **India:** 9.72% of RabbitMQ's customers are based in India.

- **United Kingdom:** 9.70% of RabbitMQ's customers are based in the United Kingdom.

2) Growth Drivers

- **Resource Management**: RabbitMQ's ability to manage resources effectively, such as memory and CPU, ensures high performance and reliability, which drives its adoption in various industries.
- **Advanced Routing**: RabbitMQ supports complex routing mechanisms, making it suitable for diverse messaging scenarios, which enhances its market appeal.
- **Monitoring and Metrics**: Comprehensive monitoring capabilities help in maintaining system health and performance, which is crucial for enterprise applications.

3) Number of Users

- **Total Companies:** Over 35,000 companies use RabbitMQ globally.
- **Clusters:** Approximately 9,000 RabbitMQ clusters are operating worldwide.
- **Connected Devices:** RabbitMQ connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) Notable Corporate Users

- **Alcatel-Lucent:** Uses RabbitMQ for various messaging needs.
- **University of California - San Diego:** Implements RabbitMQ in its systems.
- **Beckman Coulter:** Utilizes RabbitMQ for its operations.
- **Zalando, WeWork, Wunderlist, Bloomberg:** These companies rely on RabbitMQ for their microservice-based architectures.
- **Capital One, Ford, State Farm, United Airlines, Zurich Insurance:** Major corporations using RabbitMQ for secure and reliable messaging.

5) Customer Distribution by Company Size

- **20-49 Employees**: 3,520 companies.
- **100-249 Employees**: 3,034 companies.
- **1,000-4,999 Employees**: 1,723 companies.
- **Median Number of Queues**: 26 (largest number of queues: 124,400).
- **Median Number of Users:** 2 (largest number of users: 62,245).
- **Median Number of Policies:** 3 (largest number of policies: 2,550).
- **Median Number of Exchanges:** 9 (largest number of exchanges: 191,465).
- **Median Number of Bindings:** 28 (largest number of bindings: 142,516).
- **Median Number of Vhosts:** 2 (largest number of vhosts: 1,954).

6) Scalability

- **Scalability**: RabbitMQ supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Throughput**: RabbitMQ can handle over 1 billion messages per day depending on the configuration.
- **Consistent Hashing**: RabbitMQ can be scaled effectively using consistent hashing, which distributes the load evenly across multiple nodes, ensuring optimal performance and resilience.

7) Industry Adoption

- **Financial Services**: RabbitMQ is extensively used in the financial sector for secure and reliable messaging.
- **Healthcare**: Used by top healthcare companies for data integration and messaging.
- **E-commerce**: Companies like Zalando and WeWork use RabbitMQ for order processing, tracking, and fulfillment.
- **Telecommunications**: Employed by major telecom companies for data integration and real-time processing.
- **Manufacturing**: Used by large manufacturing companies for data streaming and analytics.

8) Competitive Landscape

- **RabbitMQ vs. Apache Kafka**: Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while RabbitMQ is often used for traditional messaging systems with strong transactional support.
- **RabbitMQ vs. IBM MQ**: IBM MQ is favored for its reliability and exactly-once message delivery, whereas RabbitMQ is chosen for its flexibility and ease of use.
- **RabbitMQ vs. Apache ActiveMQ**: ActiveMQ is another competitor with a smaller market share, used for simpler messaging needs compared to RabbitMQ's enterprise-grade capabilities.

B. Apache Kafka

Apache Kafka is a leading message broker and stream processing platform with a dominant market share and widespread adoption across various industries. It is used by thousands of companies, including over 80% of the Fortune 100, for real-time data processing, analytics, and integration. Kafka's scalability, high throughput, and robust architecture make it a preferred choice for large-scale data streaming applications. The competitive landscape includes other messaging systems like RabbitMQ, Apache Pulsar, and IBM MQ, but Kafka's extensive ecosystem and proven performance give it a significant edge.

1) Market Share & Geographical Distribution

- Apache Kafka commands a dominant 70% market share in the message broker and stream processing market.
- **United States**: 51.91% of Apache Kafka's customers.
- **India**: 12.95% of Apache Kafka's customers.
- **United Kingdom:** 8.28% of Apache Kafka's customers.

2) Growth Drivers

- **High Throughput and Low Latency**: Kafka's ability to handle high throughput with low latency makes it ideal for real-time data streaming and analytics, driving its popularity among large enterprises.
- **Scalability**: Kafka's distributed architecture allows it to scale horizontally, handling large volumes of data efficiently, which is a significant growth driver.
- **Ecosystem Integration**: Kafka's extensive ecosystem, including built-in stream processing and integration with various data sources and sinks, enhances its utility and adoption

3) Number of Users

- **Total Companies**: Over 22,240 companies use Apache Kafka globally.
- **Fortune** 100: More than 80% of the Fortune 100 companies use Kafka.

4) Notable Corporate Users

- **American Express**: Uses Kafka for real-time data processing.
- **Cardinal Health**: Implements Kafka for handling large-scale data streams.
- **Cisco**: Utilizes Kafka for its data integration needs.
- **Shopify**: Employs Kafka for stream processing and data analytics.
- **LinkedIn**: Processes 7 trillion messages daily using Kafka.
- **Uber**: One of the largest deployments of Kafka, handling data exchange between users and drivers.
- **Netflix**: Tracks activity for over 230 million subscribers using Kafka.
- **Goldman Sachs, Target, Intuit**: Among other major corporations using Kafka.

5) Company Size Distribution:

- **20-49 Employees**: 4,394 companies.
- **100-249 Employees**: 4,149 companies.
- **1,000-4,999 Employees:** 2,838 companies.

6) Revenue Distribution:

- **Small (<$50M):** 52% of companies using Kafka.
- **Large (>$1000M):** 24% of companies using Kafka.
- **Medium ($50M-$1000M):** 18% of companies using Kafka.

7) Scalability

- **Scalability**: Kafka's distributed architecture allows it to handle increased data loads as a business grows, ensuring robustness and reliability even as demand increases.
- **High Throughput**: Kafka can deliver messages at network-limited throughput using a cluster of machines with latencies as low as 2ms.
- **Large Scale**: Kafka can scale production clusters up to a thousand brokers, trillions of messages per day, petabytes of data, and hundreds of thousands of partitions.

8) Industry Adoption

- **Financial Services**: Used by companies like ING, PayPal, and JPMorgan Chase for fraud detection, real-time analytics, and customer handling.
- **E-commerce**: Companies like Shopify and Article use Kafka for order processing, tracking, and fulfillment.
- **AdTech**: Utilized for real-time marketing data aggregation and analytics.
- **Telecommunications**: Employed by major telecom companies for data integration and real-time processing.
- **Manufacturing**: Used by 10 out of 10 of the largest manufacturing companies for data streaming and analytics.

9) Competitive Landscape

- **Apache Kafka vs. RabbitMQ**: Kafka has a higher market share and is preferred for high-throughput, low-latency applications, while RabbitMQ is often used for traditional messaging systems.
- **Apache Kafka vs. Apache Pulsar**: Kafka holds a dominant 70% market share compared to Pulsar's 30%, with Kafka being more mature and having a larger ecosystem of tools and libraries.
- **Apache Kafka vs. IBM MQ**: Kafka is favored for its scalability and real-time processing capabilities, whereas IBM MQ is often used for enterprise messaging with strong transactional support.

C. ApacheMQ

Apache ActiveMQ is a widely used message broker with a significant market share in the enterprise application integration space. It is used by thousands of companies globally, including major corporations like Red Hat, The Apache Software Foundation, and eBay. ActiveMQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in information technology, computer software, and financial services. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and IBM MQ, but ActiveMQ's flexibility and support for multiple protocols give it a strong position in the market.

1) *Market Share & Geographical Distribution*

- Apache ActiveMQ holds a market share of approximately 4.91% in the Enterprise Application Integration category.
- **United States**: 47% of Apache ActiveMQ's customers are based in the United States.
- **United Kingdom**: 6% of Apache ActiveMQ's customers are based in the United Kingdom.

2) *Growth Drivers*

- **Flexibility and Customization**: ApacheMQ's support for various messaging protocols and its flexibility in deployment options make it a preferred choice for many organizations.
- **Reliability and Persistence**: The ability to ensure message persistence and reliability even in the event of system failures drives its adoption in critical applications.

3) *Number of Users*

- **Total Companies**: Over 9,604 companies use Apache ActiveMQ globally.
- **Current Customers**: Around 3,240 companies have started using Apache ActiveMQ as a queueing, messaging, and background processing tool.

4) *Notable Corporate Users*

- **Red Hat:** Uses Apache ActiveMQ for various messaging needs.
- **The Apache Software Foundation**: Implements Apache ActiveMQ in its systems.
- **Fidelis Cybersecurity**: Utilizes Apache ActiveMQ for its operations.
- **Stack Overflow:** Employs Apache ActiveMQ for message brokering.
- **Infosys Ltd:** A major user of Apache ActiveMQ, based in India.
- **Fujitsu Ltd:** Uses Apache ActiveMQ in Japan.
- **Panasonic Corp**: Another significant user in Japan.
- **eBay Inc.:** Utilizes Apache ActiveMQ in the United States.

5) *Customer Distribution by Company Size*

- **Small Companies (<50 employees):** 24% of Apache ActiveMQ's customers.
- **Medium Companies (50-200 employees):** 43% of Apache ActiveMQ's customers.
- **Large Companies (>1000 employees):** 33% of Apache ActiveMQ's customers.

6) *Revenue Distribution*

- **Small Companies (<$50M):** 43% of companies using Apache ActiveMQ.
- **Medium Companies ($50M-$1000M):** 18% of companies using Apache ActiveMQ.
- **Large Companies (>$1000M):** 36% of companies using Apache ActiveMQ.

7) *User Statistics*

- **Total Companies**: 9,604 companies use Apache ActiveMQ.
- **Employee Range**: Most companies using Apache ActiveMQ have between 50-200 employees.
- **Revenue Range**: Many companies using Apache ActiveMQ have revenues between $10M-$50M.

8) *Scalability*

- **Scalability**: Apache ActiveMQ supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Availability**: ActiveMQ can be configured for high availability using shared storage or network replication.
- **Performance**: ActiveMQ Artemis, the next-generation broker, offers better performance and scalability compared to the classic version.

9) *Industry Adoption*

- **Information Technology and Services**: 28% of Apache ActiveMQ's customers are in this industry.
- **Computer Software**: 16% of Apache ActiveMQ's customers are in this industry.
- **Financial Services**: 6% of Apache ActiveMQ's customers are in this industry.

10) *Competitive Landscape*

- **Apache Kafka**: Holds a 39.80% market share and is a major competitor to Apache ActiveMQ.
- **RabbitMQ**: Holds a 28.24% market share and is another significant competitor.
- **IBM MQ:** Holds a 7.20% market share.
- **Realtime Framework**: Holds a 5.17% market share.
- **Microsoft Azure Service Bus:** Holds a 3.84% market share.

D. IBM MQ

IBM MQ is a robust and widely adopted message broker with a significant market share in the queueing, messaging, and background processing market. It is used by thousands of companies globally, including major corporations like Capital One, Ford, and State Farm. IBM MQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in financial services, healthcare, and oil and gas. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and Apache ActiveMQ, but IBM MQ's reliability and exactly once message delivery give it a strong position in the market.

1) *Market Share & Geographical Distribution*

- IBM MQ holds a market share of approximately 7.20% in the queueing, messaging, and background processing market.
- **United States**: 59.39% of IBM MQ's customers are based in the United States.
- **United Kingdom:** 8.70% of IBM MQ's customers are based in the United Kingdom.
- **India**: 8.67% of IBM MQ's customers are based in India.

2) *Growth Drivers*

- **Business Process Integration**: IBM MQ's integration with business process management tools provides real-time insights and proactive management, which is a key growth driver.
- **Security and Compliance**: Enhanced security features and compliance with regulatory standards make IBM MQ a trusted solution for industries with stringent security requirements.

3) *Number of Users*

- **Total Companies**: Over 4,060 companies use IBM MQ globally (~12,870 total).
- **Current Customers**: IBM MQ is used by 90% of the top 100 global banks, healthcare, airline, and insurance companies.

4) *Notable Corporate Users*

- **Capital One:** Uses IBM MQ for secure and reliable messaging.
- **Ford**: Implements IBM MQ for data integration and messaging.
- **State Farm**: Utilizes IBM MQ for its operations.
- **United Airlines**: Employs IBM MQ for message brokering.
- **Zurich Insurance**: Uses IBM MQ for secure data exchange.
- **Infosys Ltd:** A major user of IBM MQ, based in India.
- **Fujitsu Ltd:** Uses IBM MQ in Japan.
- **Panasonic** Corp: Another significant user in Japan.
- **eBay Inc.:** Utilizes IBM MQ in the United States.

5) *Customer Distribution by Company Size*

- **1,000 - 4,999 Employees:** 767 companies.
- **10,000+ Employees:** 739 companies.
- **100 - 249 Employees:** 578 companies.

6) *Revenue Distribution*

- **Small Companies (<$50M):** 39% of companies using IBM MQ.
- **Medium Companies ($50M-$1000M):** 16% of companies using IBM MQ.
- **Large Companies (>$1000M):** 40% of companies using IBM MQ.

7) *User Statistics*

- **Total Companies**: 12,870 companies use IBM WebSphere MQ.
- **Employee Range**: Most companies using IBM MQ have between 50-200 employees.
- **Revenue Range**: Many companies using IBM MQ have revenues between $10M-$50M.

8) *Scalability*

- **Scalability**: IBM MQ supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Availability**: IBM MQ can be configured for high availability using shared storage or network replication.
- **Performance**: IBM MQ offers high performance and stability, ensuring reliable message delivery even under high loads.

9) *Industry Adoption*

- **Financial Services**: IBM MQ is extensively used in the financial sector for secure and reliable messaging.
- **Healthcare**: Used by 70% of the top 10 healthcare companies in the 2022 Forbes Global 2000.
- **Oil and Gas**: Utilized by 80% of the top 10 oil and gas companies in the 2022 Forbes Global 2000.
- **Media**: Employed by 60% of the top 10 media companies in the 2022 Forbes Global 2000.

10) *Competitive Landscape*

- **IBM MQ vs. Apache Kafka**: Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while IBM MQ is often used for traditional messaging systems with strong transactional support.
- **IBM MQ vs. RabbitMQ**: RabbitMQ has a higher market share and is favored for microservices architectures, whereas IBM MQ is chosen for its reliability and exactly once message delivery.
- **IBM MQ vs. Apache ActiveMQ**: ActiveMQ is another competitor with a smaller market share, used for simpler messaging needs compared to IBM MQ's enterprise-grade capabilities.

E. *Microsoft Azure Service Bus*

Microsoft Azure Service Bus is a robust and widely adopted message broker with a significant market share in the queueing, messaging, and background processing market. It is used by thousands of companies globally, including major corporations like Infosys, Fujitsu, and Panasonic. Azure Service Bus's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in information technology, computer software, and financial services. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and IBM MQ, but Azure Service Bus's cloud-native capabilities and strong transactional support give it a strong position in the market.

1) *Market Share & Geographical Distribution*

- Microsoft Azure Service Bus holds a market share of approximately 3.84% in the queueing, messaging, and background processing market.
- **United States**: 48.02% of Microsoft Azure Service Bus's customers are based in the United States.
- **United Kingdom**: 14.97% of Microsoft Azure Service Bus's customers are based in the United Kingdom.
- **India**: 8.98% of Microsoft Azure Service Bus's customers are based in India.

2) *Growth Drivers*

- **Cloud Integration**: Azure Service Bus's seamless integration with other Azure services and its ability to handle cloud-based applications drive its adoption.
- **Auto-scaling**: The ability to automatically scale to handle spikes in throughput ensures consistent performance, which is crucial for dynamic workloads.
- **Security and Reliability**: Robust security measures and reliable message delivery enhance its appeal for enterprise applications

3) *Number of Users*

- **Total Companies**: Over 4,609 companies use Microsoft Azure Service Bus globally.
- **Current Customers**: Around 2,168 companies have started using Microsoft Azure Service Bus as a queueing, messaging, and background processing tool.

4) *Notable Corporate Users*

- **Infosys Ltd**: Uses Microsoft Azure Service Bus for various messaging needs.
- **Fujitsu Ltd**: Implements Microsoft Azure Service Bus in its systems.
- **Panasonic Corp**: Utilizes Microsoft Azure Service Bus for its operations.
- **Blackfriars Insurance Brokers Ltd:** Employs Microsoft Azure Service Bus for message brokering.
- **Blue Cross Blue Shield Association**: Uses Microsoft Azure Service Bus for secure data exchange.
- **ASOS.com:** Utilizes Microsoft Azure Service Bus in the United Kingdom.
- **Avanade**: Uses Microsoft Azure Service Bus in the United States.
- **Verra Mobility**: Employs Microsoft Azure Service Bus for transportation and logistics.

5) *Customer Distribution by Company Size*

- **1,000 - 4,999 Employees**: 392 companies.
- **100 - 249 Employees**: 335 companies.
- **20 - 49 Employees**: 318 companies.
- **10,000+ Employees**: 275 companies.
- **50 - 99 Employees**: 194 companies.

6) *Revenue Distribution*

- **Small Companies (<$50M):** 40% of companies using Microsoft Azure Service Bus.
- **Medium Companies ($50M-$1000M):** 17% of companies using Microsoft Azure Service Bus.
- **Large Companies (>$1000M):** 39% of companies using Microsoft Azure Service Bus.

7) *User Statistics*

- **Total Companies**: 4,609 companies use Microsoft Azure Service Bus.
- **Employee Range**: Most companies using Microsoft Azure Service Bus have between 50-200 employees.
- **Revenue Range**: Many companies using Microsoft Azure Service Bus have revenues between $10M-$50M.

8) *Scalability*

- **Scalability**: Microsoft Azure Service Bus supports clustering, high availability, and load balancing, making it scalable for various enterprise needs.
- **High Availability**: Azure Service Bus can be configured for high availability using shared storage or network replication.
- **Performance:** Azure Service Bus offers high performance and stability, ensuring reliable message delivery even under high loads.

9) *Industry Adoption*

- **Information Technology and Services**: 31% of Microsoft Azure Service Bus's customers are in this industry.
- **Computer Software**: 14% of Microsoft Azure Service Bus's customers are in this industry.
- **Financial Services**: 6% of Microsoft Azure Service Bus's customers are in this industry.

10) *Competitive Landscape*

- **Microsoft Azure Service Bus vs. Apache Kafka**: Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while Azure Service Bus is often used for traditional messaging systems with strong transactional support.
- **Microsoft Azure Service Bus vs. RabbitMQ**: RabbitMQ has a higher market share and is favored for microservices architectures, whereas Azure Service Bus is chosen for its reliability and exactly-once message delivery.

- **Microsoft Azure Service Bus vs. IBM MQ**: IBM MQ is another competitor with a larger market share, used for enterprise-grade messaging needs compared to Azure Service Bus's cloud-native capabilities.

F. EMQX

EMQX is a robust and widely adopted MQTT broker with a significant market share in the IoT messaging space. It is used by thousands of companies globally, including major corporations like HPE, VMware, and Ericsson. EMQX's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in automotive, manufacturing, energy, and oil & gas. The competitive landscape includes other major players like Mosquitto, NanoMQ, and VerneMQ, but EMQX's extensive feature set and proven performance give it a strong position in the market.

1) Market Share & Geographical Distribution

- EMQX is a leading MQTT broker with a significant presence in the IoT market. It is recognized as the world's most scalable open-source MQTT messaging platform.
- **Global Presence**: EMQX has a global R&D center in Stockholm and 10+ offices throughout the Americas, Europe, and the Asia-Pacific region.
- **Countries and Regions**: EMQX is used in over 50 countries and regions worldwide.

2) Growth Drivers

- **IoT Focus**: EMQX's specialization in IoT messaging and its ability to handle large-scale IoT deployments drive its growth in the IoT sector.
- **Scalability**: EMQX's ability to scale horizontally to support millions of concurrent connections is a significant growth driver.

3) Number of Users

- **Total Users**: EMQX boasts more than 20,000 enterprise users globally.
- **Connected Devices**: EMQX connects over 100 million IoT devices.

4) Notable Corporate Users

- **Hewlett Packard Enterprise (HPE):** Uses EMQX for its IoT solutions.
- **VMware**: Implements EMQX in its systems.
- **Verifone**: Utilizes EMQX for secure and reliable messaging.
- **SAIC Volkswagen**: Employs EMQX for connected vehicle applications.
- **Ericsson**: Uses EMQX for its IoT infrastructure.

5) Customer Distribution by Company Size

- **Enterprise Users**: EMQX is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
- **Cluster Deployments**: EMQX has over 60,000 cluster deployments globally.
- **GitHub Stars**: EMQX has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads**: EMQX has been downloaded over 40 million times.

6) Scalability

- **Scalability**: EMQX supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
- **Cluster Size**: EMQX can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.

7) Industry Adoption

- **Automotive**: EMQX is used by over 50 automotive companies, connecting more than 10 million electric and traditional vehicles.
- **Manufacturing**: EMQX empowers Industry 4.0 transformation with seamless connectivity and real-time data transmission from the factory floor to the cloud.
- **Energy & Utilities**: EMQX integrates with energy management and SCADA systems for smart grid management.
- **Oil & Gas**: EMQX consolidates data from oil wells, gateways, and cloud applications to enhance operational efficiency and safety.

8) Competitive Landscape

- **EMQX vs. Mosquitto**: EMQX offers better scalability and performance, supporting up to 100 million connections compared to Mosquitto's lower capacity.
- **EMQX vs. NanoMQ**: EMQX and NanoMQ both perform well in enterprise-level benchmarks, but EMQX has a larger user base and more extensive feature set.
- **EMQX vs. VerneMQ**: EMQX outperforms VerneMQ in terms of scalability and resource efficiency, making it a preferred choice for large-scale IoT deployments.

G. HiveMQ

HiveMQ is a robust and widely adopted MQTT broker with a significant market share in the IoT messaging space. It is used by thousands of companies globally, including major corporations like BMW, Daimler, and Siemens. HiveMQ's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in automotive, manufacturing, energy, and oil & gas. The competitive landscape includes other major players like Mosquitto, NanoMQ, and VerneMQ, but HiveMQ's extensive feature set and proven performance give it a strong position in the market.

1) Market Share & Geographical Distribution

- HiveMQ is a leading MQTT broker with a significant presence in the IoT market. It is recognized for its scalability and performance, making it a popular choice among enterprises.
- **Global Presence**: HiveMQ has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **US Market**: The US market accounts for a significant portion of HiveMQ's revenues, reflecting its widespread adoption in the region.

2) *Growth Drivers*

- **MQTT Protocol Support**: HiveMQ's support for the MQTT protocol, which is widely used in IoT applications, drives its adoption in the IoT market.
- **Enterprise Features**: Features like high availability, security, and integration with enterprise systems make HiveMQ a preferred choice for large-scale IoT deployments.

3) *Number of Users*

- **Total Users**: HiveMQ is used by thousands of companies globally, with a substantial number of enterprise users.
- **Connected Devices**: HiveMQ connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) *Notable Corporate Users*

- **BMW**: Uses HiveMQ for connected vehicle applications.
- **Daimler**: Implements HiveMQ in its IoT systems.
- **Deutsche Telekom**: Utilizes HiveMQ for secure and reliable messaging.
- **Liberty** Global: Employs HiveMQ for its IoT infrastructure.
- **Moen**: Uses HiveMQ for smart home applications.
- **Siemens**: Relies on HiveMQ for industrial IoT solutions.
- **ZF**: Uses HiveMQ for automotive IoT applications.

5) *Customer Distribution by Company Size*

- **Enterprise Users**: HiveMQ is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
- **Cluster Deployments**: HiveMQ has over 60,000 cluster deployments globally.
- **GitHub Stars**: HiveMQ has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads**: HiveMQ has been downloaded over 40 million times.

6) *Scalability*

- **Scalability**: HiveMQ supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
- **Cluster Size**: HiveMQ can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.
- **Benchmark**: HiveMQ has demonstrated the capability to handle 200 million concurrent connections in a large-scale test scenario.

7) *Industry Adoption*

- **Automotive**: HiveMQ is used by over 50 automotive companies, connecting more than 10 million electric and traditional vehicles.
- **Manufacturing**: HiveMQ empowers Industry 4.0 transformation with seamless connectivity and real-time data transmission from the factory floor to the cloud.
- **Energy & Utilities**: HiveMQ integrates with energy management and SCADA systems for smart grid management.
- **Oil & Gas**: HiveMQ consolidates data from oil wells, gateways, and cloud applications to enhance operational efficiency and safety.
- **Logistics**: A large transportation company uses HiveMQ to handle 743.5 million customer tracking requests per day, saving 100 million miles and 10 million gallons of fuel per year.

8) *Competitive Landscape*

- **HiveMQ vs. Mosquitto**: HiveMQ offers better scalability and performance, supporting up to 100 million connections compared to Mosquitto's lower capacity.
- **HiveMQ vs. NanoMQ**: HiveMQ and NanoMQ both perform well in enterprise-level benchmarks, but HiveMQ has a larger user base and more extensive feature set.
- **HiveMQ vs. VerneMQ:** HiveMQ outperforms VerneMQ in terms of scalability and resource efficiency, making it a preferred choice for large-scale IoT deployments.

H. Pubhub

PubNub is a robust and widely adopted real-time messaging platform with a significant market share in the real-time data streaming market. It is used by thousands of companies globally, including major corporations like SAP, HPE, and Ericsson. PubNub's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in e-learning, entertainment, healthcare, smart cities, and IoT. The competitive landscape includes other major players like Ably, Pusher, and Firebase, but PubNub's extensive feature set and proven performance give it a strong position in the market.

1) *Market Share & Geographical Distribution*

- PubNub holds a significant market share in the real-time messaging and data streaming market. It is recognized for its robust infrastructure and extensive feature set, making it a popular choice among developers and enterprises.
- **Global Presence**: PubNub has a strong global presence, with data centers distributed across North America, South America, Europe, and Asia.
- **United States**: A significant portion of PubNub's customers are based in the United States, reflecting its widespread adoption in the region.
- **Europe and Asia**: PubNub also has a substantial user base in Europe and Asia, supporting a diverse range of applications and industries.

2) Growth Drivers

- **Ease of Use**: Pubhub's user-friendly interface and ease of integration with various applications drive its adoption among small to medium-sized enterprises.
- **Cost-Effectiveness**: Competitive pricing and cost-effective solutions make Pubhub an attractive option for businesses looking to implement messaging systems without significant investment.

3) Number of Users

- **Total Devices**: PubNub serves over 330 million devices globally.
- **Monthly Transactions**: PubNub handles over 3 trillion API calls per month, demonstrating its capability to manage large-scale real-time data streaming.

4) Notable Corporate Users

- **SAP**: Uses PubNub for its real-time messaging needs.
- **Hewlett Packard Enterprise (HPE):** Implements PubNub in its IoT solutions.
- **VMware**: Utilizes PubNub for secure and reliable messaging.
- **Verifone**: Employs PubNub for its payment processing systems.
- **Ericsson**: Uses PubNub for its IoT infrastructure.
- **Disprz**: Uses PubNub to empower a more knowledgeable workforce through real-time communication.

5) Customer Distribution by Company Size

- **Enterprise Users:** PubNub is trusted by over 500 enterprise customers in mission-critical scenarios, including well-known brands.
- **Cluster Deployments:** PubNub has over 60,000 cluster deployments globally.
- **GitHub Stars:** PubNub has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads:** PubNub has been downloaded over 40 million times.

6) Scalability

- **Scalability:** PubNub supports up to millions of concurrent device connections, ensuring high availability and fault tolerance.
- **High Throughput:** PubNub can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** PubNub operates a globally distributed network with 15 data centers, ensuring low latency and high availability for users worldwide.

7) Industry Adoption

- **E-Learning:** PubNub is used in interactive classrooms for real-time data updates, chat facilities, and private channels for individual support.
- **Entertainment:** PubNub supports real-time interactions in online concerts, dating, sporting events, and socializing platforms.
- **Healthcare:** Used by top healthcare companies for data integration and real-time messaging.
- **Smart Cities:** PubNub is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.
- **IoT:** PubNub is extensively used in IoT applications for real-time data streaming and device signaling.

8) Competitive Landscape

- **PubNub vs. Ably:** Ably offers similar real-time messaging capabilities but PubNub has a more extensive global network and higher reliability guarantees.
- **PubNub vs. Pusher:** Pusher is another competitor in the real-time messaging space, but PubNub's scalability and feature set give it an edge.
- **PubNub vs. Firebase:** Firebase provides real-time database capabilities, but PubNub's focus on messaging and data streaming makes it a preferred choice for certain use cases.

I. Thingsboard

ThingsBoard is a robust and widely adopted IoT platform with a significant market share in the IoT messaging space. It is used by thousands of companies globally, including major corporations like CIRCUTOR, OMS, and Ericsson. ThingsBoard's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in smart energy, smart city, smart farming, and smart retail. The competitive landscape includes other major players like AWS IoT, Azure IoT Hub, and Google Cloud IoT, but ThingsBoard's extensive feature set and proven performance give it a strong position in the market.

1) Market Share & Geographical Distribution

- ThingsBoard is a leading open-source IoT platform with a significant presence in the IoT market. It is widely adopted for its scalability, fault-tolerance, and performance.

- **Global Presence**: ThingsBoard has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **Countries and Regions**: ThingsBoard is used in over 50 countries and regions worldwide.

2) Growth Drivers

- **IoT Platform Integration**: Thingsboard's integration with IoT platforms and its ability to handle IoT data efficiently drive its growth in the IoT sector.
- **Open-Source Flexibility**: Being open-source, Thingsboard offers flexibility and customization, which attracts a wide range of users and developers

3) Number of Users

- **Total Users**: ThingsBoard is used by thousands of companies globally, with a substantial number of enterprise users.
- **Connected Devices**: ThingsBoard connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) Notable Corporate Users

- **CIRCUTOR**: Uses ThingsBoard for energy efficiency and power quality measurement.
- **OMS**: Implements ThingsBoard in its smart city solutions.
- **iiOOTE**: Utilizes ThingsBoard for its IoT LPWAN ecosystem.
- **MAKERS s. r. o.:** Employs ThingsBoard for smart city solutions.
- **Ericsson**: Uses ThingsBoard for its IoT infrastructure.
- **Hewlett Packard Enterprise (HPE):** Uses ThingsBoard for its IoT solutions.
- **VMware**: Implements ThingsBoard in its systems.
- **Verifone**: Utilizes ThingsBoard for secure and reliable messaging.
- **SAIC Volkswagen**: Employs ThingsBoard for connected vehicle applications.

5) Customer Distribution by Company Size

- **Enterprise Users**: ThingsBoard is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
- **Cluster Deployments**: ThingsBoard has over 60,000 cluster deployments globally.
- **GitHub Stars**: ThingsBoard has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads**: ThingsBoard has been downloaded over 40 million times.

6) Scalability

- **Scalability**: ThingsBoard supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
- **Cluster Size**: ThingsBoard can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.
- **Benchmark**: ThingsBoard has demonstrated the capability to handle 200 million concurrent connections in a large-scale test scenario.

7) Industry Adoption

- **Smart Energy**: ThingsBoard is used by companies like CIRCUTOR for energy efficiency and power quality measurement.
- **Smart City**: ThingsBoard is employed by companies like OMS and iiOOTE for smart city solutions.
- **Smart Farming**: ThingsBoard supports high-availability deployments on cloud and on-premises data centers using K8S or bare-metal deployments, with production deployments supporting more than 1,000 agriculture sites and 500,000 devices connected.
- **Smart Retail**: ThingsBoard is used to monitor supermarket assets, browse historical data, and generate alarms based on user-defined thresholds.
- **Fleet Tracking**: ThingsBoard platform allows tracking vehicles' state and alerts via various sensors, plotting vehicle routes in real-time, and browsing their sensors' reading history using customizable high-quality dashboards.

8) Competitive Landscape

- **ThingsBoard vs. AWS IoT:** AWS IoT offers a comprehensive suite of IoT services, but ThingsBoard's open-source nature and flexibility make it a preferred choice for many developers and enterprises.
- **ThingsBoard vs. Azure IoT Hub:** Azure IoT Hub is known for its integration with other Microsoft services, while ThingsBoard offers a more customizable and open-source solution.
- **ThingsBoard vs. Google Cloud IoT:** Google Cloud IoT provides robust data analytics capabilities, but ThingsBoard's ease of use and flexibility give it an edge in certain scenarios.

J. SolaceMQ

Solace is a robust and widely adopted message broker with a significant market share in the plumbing-and-middleware market. It is used by thousands of companies globally, including major corporations like SAP, Mercedes-Benz, and the London Stock Exchange. Solace's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in financial services, healthcare, e-commerce, telecommunications, and manufacturing. The competitive landscape includes other major players like Apache Kafka, RabbitMQ, and IBM MQ, but Solace's extensive feature set and proven performance give it a strong position in the market.

1) *Market Share*

- Solace holds a market share of approximately 5.33% in the plumbing-and-middleware market.
- **Global Presence**: Solace has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **Countries and Regions**: Solace is used in over 50 countries and regions worldwide.

2) *Growth Drivers*

- **Event Mesh Capabilities**: Solace's event mesh architecture, which enables seamless data exchange across distributed applications, is a key growth driver as organizations adopt event-driven architectures and microservices.
- **Multi-Protocol Support**: Solace's support for various messaging protocols, including MQTT, AMQP, and JMS, allows it to cater to diverse IoT use cases, driving adoption across industries.
- **Cloud-Agnostic Deployment**: Solace's ability to deploy its event brokers across multiple cloud platforms and on-premises environments provides flexibility, enabling growth in hybrid and multi-cloud IoT deployments

3) *Number of Users*

- **Total Companies**: Solace is used by thousands of companies globally, with a substantial number of enterprise users.
- **Connected Devices**: Solace connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) *Notable Corporate Users*

- **SAP**: Uses Solace for its event-driven architecture needs.
- **Mercedes-Benz:** Implements Solace in its IoT systems.
- **London Stock Exchange:** Utilizes Solace for secure and reliable messaging.
- **Hewlett Packard Enterprise (HPE):** Uses Solace for its IoT solutions.
- **VMware**: Implements Solace in its systems.
- **Verifone**: Utilizes Solace for secure and reliable messaging.
- **SAIC Volkswagen**: Employs Solace for connected vehicle applications.
- **Ericsson**: Uses Solace for its IoT infrastructure.
- **WeLab Bank**: Uses Solace to support its vision of becoming a leading virtual bank in the region.
- **Standard Chartered Bank Korea**: Collaborates with Solace to design a modern and agile corporate banking platform.
- **Drax Group**: Uses Solace to improve user experience and drive operational efficiencies.
- **RBC Capital Markets**: Relies on Solace for handling unprecedented trading volumes and volatility.

5) *Customer Distribution by Company Size*

- **Enterprise Users**: Solace is trusted by over 500 customers in mission critical IoT scenarios, including well-known brands.
- **Cluster Deployments**: Solace has over 60,000 cluster deployments globally.
- **GitHub Stars**: Solace has received over 13,000 stars on GitHub, indicating strong community support and adoption.
- **Downloads**: Solace has been downloaded over 40 million times.

6) *Scalability*

- **Scalability**: Solace supports up to 100 million concurrent IoT device connections per cluster while maintaining 1 million messages per second throughput and sub-millisecond latency.
- **Cluster Size**: Solace can scale horizontally with a masterless distributed architecture, ensuring high availability and fault tolerance.
- **Benchmark**: Solace has demonstrated the capability to handle 200 million concurrent connections in a large-scale test scenario.

7) *Industry Adoption*

- **Financial Services**: Solace is extensively used in the financial sector for secure and reliable messaging.
- **Healthcare**: Used by top healthcare companies for data integration and messaging.
- **E-commerce**: Companies like SAP and Verifone use Solace for order processing, tracking, and fulfillment.
- **Telecommunications**: Employed by major telecom companies for data integration and real-time processing.
- **Manufacturing**: Used by large manufacturing companies for data streaming and analytics.
- **Energy & Utilities**: Solace integrates with energy management and SCADA systems for smart grid management.
- **Automotive**: Solace is used by over 50 automotive companies, connecting more than 10 million electric and traditional vehicles.

- **Logistics**: A large transportation company uses Solace to handle 743.5 million customer tracking requests per day, saving 100 million miles and 10 million gallons of fuel per year.

8) Competitive Landscape

- **Solace vs. Apache Kafka:** Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while Solace is often used for traditional messaging systems with strong transactional support.
- **Solace vs. RabbitMQ:** RabbitMQ has a higher market share and is favored for microservices architectures, whereas Solace is chosen for its reliability and exactly once message delivery.
- **Solace vs. IBM MQ:** IBM MQ is competitor with a larger market share, used for enterprise-grade messaging needs compared to Solace's cloud-native capabilities.

K. AWS IoT

AWS IoT is a robust and widely adopted IoT platform with a significant market share in the IoT platform market. It is used by thousands of companies globally, including major corporations like Siemens, Intel, and Volkswagen. AWS IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Google Cloud IoT, Microsoft Azure IoT, and Cisco IoT, but AWS IoT's extensive feature set and proven performance give it a strong position in the market.

1) Market Share & Geographical Distribution

- AWS IoT holds a significant market share in the IoT platform market. It is recognized as a leader in the 2024 Gartner Magic Quadrant for Global Industrial IoT Platforms.
- **Global Presence**: AWS IoT has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **United States**: 52.12% of AWS IoT's customers are based in the United States.
- **India**: 13.26% customers are based in India.
- **United Kingdom**: 8.84% of AWS IoT's customers are based in the United Kingdom.

2) Growth Drivers

- **Cloud Ecosystem:** AWS IoT's integration with the broader AWS ecosystem provides a comprehensive solution for IoT applications, driving its adoption.
- **Scalability and Reliability**: AWS IoT's ability to scale and provide reliable messaging services ensures its popularity among enterprises

3) Number of Users

- **Total Companies**: Over 718 companies have started using AWS IoT Core as an IoT platform tool globally.
- **Connected Devices**: AWS IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) Notable Corporate Users

- **Genpact, Ltd**: Uses AWS IoT for various IoT solutions.
- **Siemens AG**: Implements AWS IoT in its systems.
- **Intel Corporation**: Utilizes AWS IoT for secure and reliable messaging.
- **Birlasoft**: Employs AWS IoT for its IoT infrastructure.
- **Broadcom, Inc.:** Uses AWS IoT for its IoT solutions.
- **Volkswagen Group, Carrier, TC Energy, Bosch, BP, GE, Toyota, Invista, John Deere:** These global brands rely on AWS IoT for their industrial IoT applications.

5) Customer Distribution by Company Size

- **20-49 Employees:** 128 companies.
- **100-249 Employees:** 103 companies.
- **10,000+ Employees:** 114 companies.

6) Scalability

- **Scalability:** AWS IoT supports up to millions of concurrent IoT device connections, ensuring high availability and fault tolerance.
- **High Throughput:** AWS IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** AWS IoT Core is available in multiple AWS regions, including US East (N. Virginia), US West (Oregon), Europe (Frankfurt), Europe (Ireland), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo).

7) Industry Adoption

- **Manufacturing:** AWS IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **Automotive:** Companies like Volkswagen and Toyota use AWS IoT for connected vehicle applications.
- **Energy & Utilities:** AWS IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** AWS IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

8) Competitive Landscape

- **AWS IoT vs. Google Cloud IoT:** Google Cloud IoT holds an 18.85% market share and is a major competitor to AWS IoT.
- **AWS IoT vs. Microsoft Azure IoT:** Microsoft Azure IoT holds a 14.81% market share and is another significant competitor.

- **AWS IoT vs. Cisco IoT:** Cisco IoT holds a 10.48% market share, competing closely with AWS IoT in the IoT platform market.

L. *Azure IoT*

Azure IoT is a robust and widely adopted IoT platform with a significant market share in the IoT platform market. It is used by thousands of companies globally, including major corporations like Walmart, Robert Bosch GmbH, and Daimler Trucks North America. Azure IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Google Cloud IoT, Cisco IoT, and Samsara, but Azure IoT's extensive feature set and proven performance give it a strong position in the market.

1) *Market Share & Geographical Distribution*

- Microsoft Azure IoT holds a significant market share in the IoT platform market. It is recognized as a leader in the 2024 Gartner Magic Quadrant for Global Industrial IoT Platforms.
- **Global Presence**: Azure IoT has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **United States**: 47.72% of Azure IoT's customers are based in the United States.
- **India**: 14.04% of Azure IoT's customers are based in India.
- **United Kingdom**: 8.73% of Azure IoT's customers are based in the United Kingdom.

2) *Growth Drivers*

- **Integration with Azure Services**: Azure IoT's seamless integration with other Azure services enhances its utility and drives its adoption in IoT applications.
- **Security and Compliance**: Robust security features and compliance with industry standards make Azure IoT a trusted solution for IoT deployments.

3) *Number of Users*

- **Total Companies**: Over 1,396 companies have started using Microsoft Azure IoT as an IoT platform tool globally.
- **Connected Devices**: Azure IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) *Notable Corporate Users*

- **Walmart, Inc.**: Uses Azure IoT for various IoT solutions.
- **Robert Bosch GmbH**: Implements Azure IoT in its systems.
- **Daimler Trucks North America**: Utilizes Azure IoT for secure and reliable messaging.
- **Tetra Pak**: Employs Azure IoT for its IoT infrastructure.
- **Ernst & Young**: Uses Azure IoT for its IoT solutions.
- **Walgreens**: Implements Azure IoT in its systems.
- **Chevron**: Uses Azure IoT for industrial transformation and AI applications.
- **Electrolux Group**: Leverages Azure IoT for quality management in manufacturing processes.

5) *Customer Distribution by Company Size*

- **10,000+ Employees**: 244 companies.
- **20-49 Employees**: 229 companies.
- **1,000-4,999 Employees**: 211 companies.

6) *Scalability*

- **Scalability**: Azure IoT supports up to millions of concurrent IoT device connections, ensuring high availability and fault tolerance.
- **High Throughput**: Azure IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach**: Azure IoT Core is available in multiple Azure regions, including US East (N. Virginia), US West (Oregon), Europe (Frankfurt), Europe (Ireland), Asia Pacific (Sydney), Asia Pacific (Tokyo), and South America (São Paulo).

7) *Industry Adoption*

- **Manufacturing**: Azure IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare**: Used by top healthcare companies for data integration and messaging.
- **Automotive**: Companies like Daimler Trucks North America and Volkswagen use Azure IoT for connected vehicle applications.
- **Energy & Utilities**: Azure IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities**: Azure IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

8) *Competitive Landscape*

- **Azure IoT vs. Google Cloud IoT:** Google Cloud IoT holds a 19.59% market share and is a major competitor to Azure IoT.
- **Azure IoT vs. Cisco IoT:** Cisco IoT holds a 9.52% market share and is another significant competitor.
- **Azure IoT vs. Samsara**: Samsara holds a 9.30% market share, competing closely with Azure IoT in the IoT platform market.

M. *Google IoT*

Google Cloud IoT is a robust and widely adopted IoT platform with a significant market share in the IoT platform market. It is used by thousands of companies globally, including major corporations like Chamberlain Group, Nutanix, and Hitachi. Google Cloud IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Microsoft Azure IoT, Samsara, and Cisco IoT, but Google Cloud IoT's extensive feature set and proven performance give it a strong position in the market.

1) Market Share & Geographical Distribution

- Google Cloud IoT holds a market share of approximately 18.65% in the IoT platform category.
- **Global Presence**: Google Cloud IoT has a strong global presence, with users spread across various regions including North America, Europe, and Asia-Pacific.
- **United States**: 48.77% of Google Cloud IoT's customers are based in the United States.
- **India**: 16.58% of Google Cloud IoT's customers are based in India.
- **Germany:** 6.39% of Google Cloud IoT's customers are based in Germany.

2) Growth Drivers

- **Data Analytics Integration**: Google Cloud IoT's integration with Google Cloud's data analytics and machine learning services drives its adoption for advanced IoT applications.
- **Scalability and Performance**: The ability to handle large-scale IoT deployments with high performance and reliability is a significant growth driver

3) Number of Users

- **Total Companies**: Google Cloud IoT is used by over 1,790 companies globally.
- **Connected Devices:** Google Cloud IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) Notable Corporate Users

- **Chamberlain Group**: Uses for various IoT solutions.
- **Nutanix, Inc**.: Implements in its systems.
- **Hitachi Ltd**: Utilizes Google Cloud IoT for secure and reliable messaging.
- **Apexon**: Employs Google IoT for its IoT infrastructure.
- **Philips**: Uses Google Cloud IoT for its IoT solutions.
- **Spotify, Snapchat, Best Buy:** These companies rely on Google Cloud IoT for their IoT applications.

5) Customer Distribution by Company Size

- **20-49 Employees**: 332 companies.
- **10,000+ Employees**: 293 companies.
- **100-249 Employees**: 233 companies.

6) Scalability

- **Scalability**: Google Cloud IoT supports up to millions of concurrent IoT device connections, ensuring high availability and fault tolerance.
- **High Throughput**: Google Cloud IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** Google Cloud IoT Core is available in multiple Google Cloud regions, ensuring global scalability and reliability.

7) Industry Adoption

- **Manufacturing**: Google Cloud IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare:** Used by top healthcare companies for data integration and messaging.
- **Automotive:** Companies like Hitachi and Philips use Google Cloud IoT for connected vehicle applications.
- **Energy & Utilities:** Google Cloud IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** Google Cloud IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

8) Competitive Landscape

- **Google Cloud IoT vs. Microsoft Azure IoT:** Microsoft Azure IoT holds a 14.90% market share and is a major competitor to Google Cloud IoT.
- **Google Cloud IoT vs. Samsara:** Samsara holds a 9.34% market share and is another significant competitor.
- **Google Cloud IoT vs. Cisco IoT:** Cisco IoT holds a 9.12% market share, competing closely with Google Cloud IoT in the IoT platform market.

N. Amazon Kinesis

Amazon Kinesis is a robust and widely adopted stream-processing platform with a significant market share in the IoT data streaming and analytics market. It is used by hundreds of companies globally, including major corporations like CommScope, Express Scripts, and Uber. Amazon Kinesis's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Apache Kafka, Apache Flink, and Apache Spark Streaming, but Amazon Kinesis's extensive feature set and proven performance give it a strong position in the market.

1) Market Share and Geographical Distribution

Amazon Kinesis holds a significant market share in the stream-processing market, with approximately 1.20%. It is a key player in the IoT data streaming and analytics space, providing robust solutions for real-time data processing.

- **Global Presence**: Amazon Kinesis has a strong global presence, with significant deployments across North America, Europe, and Asia-Pacific.
- **United Sta**tes: 61.78% of Amazon Kinesis's customers are based in the United States.

- **India**: 10.47% of Amazon Kinesis's customers are based in India.
- **United Kingdom**: 8.38% of Amazon Kinesis's customers are based in the United Kingdom.

2) *Growth Drivers*

- **Scalability and Performance**: Kinesis' ability to handle large volumes of data streams with high throughput and low latency is a significant growth driver, enabling real-time data processing and analytics for IoT applications.
- **Integration with AWS Ecosystem**: Kinesis' seamless integration with other AWS services, such as AWS IoT Core, AWS Lambda, and Amazon S3, simplifies IoT application development and deployment, driving adoption within the AWS ecosystem.
- **Managed Service**: As a fully managed service, Kinesis eliminates the need for infrastructure management, reducing operational overhead and enabling organizations to focus on their core IoT applications.

3) *Number of Users*

- **Total Companies**: Over 216 companies have started using Amazon Kinesis Data Streams (KDS) as a stream-processing tool globally.
- **Connected Devices**: Amazon Kinesis connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) *Notable Corporate Users*

- **CommScope Holding Company, Inc.:** Uses Amazon Kinesis for real-time data streaming and analytics.
- **Express Scripts**: Implements Amazon Kinesis in its systems for secure and reliable messaging.
- **Uber Technologies, Inc**.: Utilizes Amazon Kinesis for its IoT infrastructure and data processing needs.
- **Collins Aerospace**: Employs Amazon Kinesis for real-time data analytics and monitoring.
- **MTData**: Uses Amazon Kinesis for vehicle telematics and driver monitoring solutions.

5) *Customer Distribution by Company Size*

- 10,000+ Employees: 60 companies.
- 100-249 Employees: 30 companies.
- 20-49 Employees: 26 companies.

6) *User Statistics*

- **Revenue Distribution**: The majority of Amazon Kinesis customers fall into the large enterprise category, with significant usage among companies with over 10,000 employees.
- **Geographical Distribution**: Amazon Kinesis has a strong presence in the United States, India, and the United Kingdom, with a substantial number of users in these regions.

7) *Scalability*

- **Scalability**: Amazon Kinesis supports millions of concurrent device connections, ensuring high availability and fault tolerance.
- **High Throughput**: Amazon Kinesis can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach:** Amazon Kinesis operates a globally distributed network, ensuring low latency and high availability for users worldwide.

8) *Industry Adoption*

- **Manufacturing**: Amazon Kinesis is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare**: Used by top healthcare companies for data integration and real-time messaging.
- **Automotive**: Companies like Uber and Collins Aerospace use Amazon Kinesis for connected vehicle applications and industrial automation.
- **Energy & Utilities**: Amazon Kinesis integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities**: Amazon Kinesis is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

9) *Competitive Landscape*

- **Amazon Kinesis vs. Apache Kafka**: Apache Kafka holds a larger market share and is preferred for high-throughput, low-latency applications, while Amazon Kinesis is often used for its fully managed service and ease of integration with other AWS services.
- **Amazon Kinesis vs. Apache Flink**: Apache Flink is another significant competitor, offering robust stream processing capabilities, but Amazon Kinesis's integration with AWS services provides a competitive edge.
- **Amazon Kinesis vs. Apache Spark Streaming**: Apache Spark Streaming is a major player in the stream-processing market, but Amazon Kinesis's fully managed service and scalability make it a strong contender.

O. *Cicso IoT*

Cisco IoT is used by thousands of companies globally, including major corporations like Infosys, Wipro, and General Motors. Cisco IoT's scalability, high availability, and robust performance make it a preferred choice for various industries, particularly in manufacturing, healthcare, automotive, energy, and smart cities. The competitive landscape includes other major players like Microsoft Azure IoT, AWS IoT, and Google Cloud IoT, but Cisco IoT's extensive feature set and proven performance give it a strong position in the market.

1) *Market Share and Geographical Distribution*

- Cisco IoT holds a significant market share, being one of the top players globally for its comprehensive IoT solutions that span various industries, including manufacturing, healthcare, and smart cities.

- **Global Presence:** Cisco IoT has a robust global presence, with significant deployments across North America, Europe, and Asia-Pacific.
- **United States:** A substantial portion of Cisco IoT's customers are based in the United States, reflecting its widespread adoption in the region.
- **Europe and Asia:** Cisco also has a strong user base in Europe and Asia, supporting a diverse range of applications and industries.

2) *Growth Drivers*

- **Edge Computing Capabilities**: Cisco's focus on edge computing and fog computing architectures is a significant growth driver, enabling real-time data processing and low-latency applications in IoT environments.
- **5G Readiness**: Cisco's IoT platforms, such as IoT Control Center, are 5G-ready, positioning the company to capitalize on the growth of 5G and the increasing demand for high-speed, low-latency connectivity in IoT deployments.
- **Connected Vehicles**: Cisco's dominance in the connected car market, with over 4 million devices added monthly to its IoT Control Center platform, drives growth as the automotive industry continues to embrace IoT technologies.

3) *Number of Users*

- **Total Companies:** Cisco IoT is used by over 129 companies globally, with a significant number of enterprise users.
- **Connected Devices**: Cisco IoT connects millions of IoT devices, demonstrating its capability to handle large-scale deployments.

4) *Notable Corporate Users*

- **Infosys Ltd**: Uses Cisco IoT for various IoT solutions.
- **Cisco Systems, Inc**.: Implements in its systems.
- **Wipro Ltd**: Utilizes Cisco IoT for secure and reliable messaging.
- **AT&T Inc**: Employs for its IoT infrastructure.
- **Cognizant Technology Solutions Corp**: Uses Cisco IoT for its IoT solutions.
- **General Motor**s: Uses Cisco IoT to reimagine the experience of car ownership.
- **Vivint**: Uses Cisco IoT for home security systems.
- **ABB Robotics**: Uses to monitor robot connectivity and help customers service them proactively.

5) *Customer Distribution by Company Size*

- **Large Enterprises**: 49% of Cisco IoT customers are large enterprises with more than 1,000 employees.
- **Medium-Sized Companies**: 29% of Cisco IoT customers are medium-sized companies.
- **Small Companies**: 16% of Cisco IoT customers are small companies with fewer than 50 employees.

6) *User Statistics*

- **Revenue Distribution**: 47% of Cisco IoT customers have revenues greater than $1 billion, 17% have revenues between $50 million and $1 billion, and 25% have revenues less than $50 million.
- **Geographical Distribution**: 50% of Cisco IoT customers are in the United States, and 9% are in India.

7) *Scalability*

- **Scalability**: Cisco IoT supports millions of concurrent device connections, ensuring high availability and fault tolerance.
- **High Throughput**: Cisco IoT can handle large volumes of data, making it suitable for high-load environments.
- **Global Reach**: Cisco IoT operates a globally distributed network, ensuring low latency and high availability for users worldwide.

8) *Industry Adoption*

- **Manufacturing**: Cisco IoT is extensively used in the manufacturing sector for real-time data acquisition and smart factory solutions.
- **Healthcare**: Used by top healthcare companies for data integration and real-time messaging.
- **Automotive**: Companies like General Motors and ABB Robotics use Cisco IoT for connected vehicle applications and industrial automation.
- **Energy & Utilities**: Cisco IoT integrates with energy management and SCADA systems for smart grid management.
- **Smart Cities:** Cisco IoT is used in smart city projects for applications like traffic management, waste management, and environmental monitoring.

9) *Competitive Landscape*

- **Cisco IoT vs. Microsoft Azure IoT:** Microsoft Azure IoT holds a significant market share and is a major competitor to Cisco IoT.
- **Cisco IoT vs. AWS IoT**: AWS IoT is another significant competitor, offering a comprehensive set of IoT services.
- **Cisco IoT vs. Google Cloud IoT**: Google Cloud IoT also competes closely with Cisco IoT in the IoT platform market.