Knowledge Brief

Quadrant Knowledge Solutions

Device Authority is Leader in SPARK Matrix: IoT Identity & Access Management (IoT IAM), 2021

Quadrant
Knowledge Solutions

2021
SPARK MATRIX
LEADER

IoT Identity & Access
Management Market

An Excerpt from Quadrant Knowledge Solutions
"SPARK Matrix: IoT Identity & Access Management (IoT IAM), 2021"

Device Authority is Leader in SPARK Matrix: IoT Identity & Access Management, 2021

Advent of the internet of things technologies and its widespread adoption in various sectors, including consumer sector, businesses, industrial, energy & utility, building & facilities, mobility, infrastructure, and such others, are significantly transforming the way people, processes, and technologies are converging and driving improvements. However, the increasing adoption of smart technologies also means increasing concern for security. Driven by the increased adoption of internet of things technologies, the scope of Identity and Access Management technologies is no longer confined to just people. IoT has emerged as a popular trend that is transforming IAM technologies. IAM solutions in their current form cannot handle the complexity of the internet of things due to various factors listed below.

In IoT, devices act as identifiers and have a unique attribute in a particular domain. This should not be confused with the device address, as there is a fundamental difference between an identifier and an address of a device. For instance, while connecting to the internet, a device may use an IP address, which can change if used on a different network. In the absence of a specific identity, the devices may connect with other entities inadvertently and can put an organization's data security at risk.

It is challenging to implement application development in IoT as devices tend to have different protocols. A touch screen sensor has a different protocol than that of a video monitor. It includes people, devices, and applications – the entities – which will have the same requirements to interact with each other. Authentication is another big challenge in implementing IoT. Usual IAM measures like multi-factor authentication or even classic authentication methods like user ids/passwords may not directly work with it.

A purpose-built IoT IAM solution capability includes massive scalability & availability to handle a wide variety and volume of IoT devices, secure device registration & provisioning, end-to-end data encryption, device authentication, compliance management, and centralized policy management, identity & device lifecycle management, certificates and key management, API management and security.

This research service includes a detailed analysis of the global IoT Identity & Access Management (IoT IAM) solution market dynamics, major trends, vendor landscape, and competitive positioning analysis. The study provides a comprehensive competition analysis and ranking of the leading IoT IAM vendors in the form of the SPARK Matrix. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities, competitive differentiation, and market position.

SPARK Matrix includes ranking and positioning of IoT Identity & Access Management (IoT IAM) vendors, with a global impact. The SPARK Matrix includes analysis of vendors, including Blue Ridge Networks, Device Authority, DigiCert, Entrust, ForgeRock, GlobalSign, Keyfactor, Mocana, Okta, Ping Identity, Rambus, and Sectigo.

Market Dynamics and Trends

The following are the key research findings of Quadrant Knowledge Solutions IoT Identity & Access Management research:

- Organizations are embracing security-by-design philosophies to secure IoT devices, which means security is built in from the start to add trust to the devices rather than after an attack. IoT security vendors are progressively collaborating with device manufacturers to guarantee that security keys and certificates are provisioned during the manufacturing process, ensuring a robust root of trust. These security keys and certificates can be used for secure and automated registration and onboarding of IoT devices, as well as secure operation. IoT IAM vendors are working on providing end-to-end data encryption in IoT devices and securing data-at-rest and data-in-transit between devices and users. IoT security vendors are focusing on integrated features to ensure data security and privacy are effectively connected with device identification and root-of-trust to enable end-to-end IoT security.

- IAM systems are evolving to accommodate Identity of Things. IAM vendors are constantly working on adding device centric capabilities into their existing IAM solutions to address IoT-specific challenges. IAM vendors are reorganizing their solution portfolio to offer unified IAM solution including an integrated solution for employee IAM, customer IAM and IoT IAM solution. With the advent of several device centric IAM providers and predicted mergers and acquisitions in this field, market dynamics and technology evolution is expected to evolve.

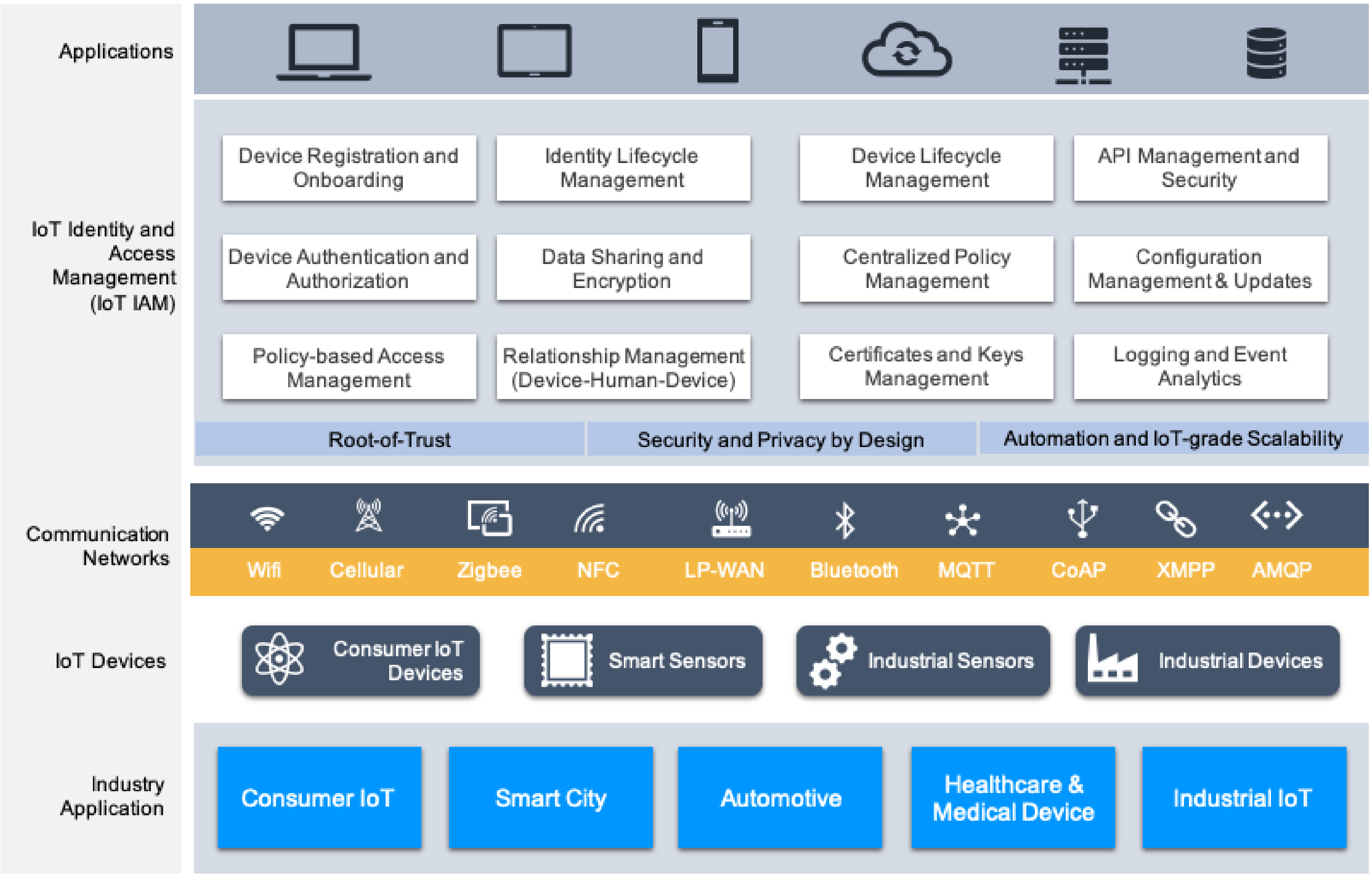
- The increasing frequency, sophistication, and complexity of IoT-based cybersecurity attacks leveraging a large number of unsecured IoT devices is significantly expanding the organization's risk exposure. With the rapid and widespread adoption of IoT devices, practically every industry sector is exposed to IoT botnet-based cybersecurity threats. The continued disruption happening in the technology landscape is driving a wave of advanced network and cybersecurity attacks, with attackers using sophisticated tools leveraging automation, artificial intelligence, and machine learning.

- The global regulatory compliance requirements and scrutiny of auditors continue to become stringent with numerous compliance frameworks and emergence of strict data privacy regulation driven by GDPR, CCPA, and others. With organizations increasingly investing in modern security solutions to improve their overall security strategy, an effective IoT security strategy can significantly help organizations to ensure adherence to an ever-changing industry and regulatory compliance specifications.

- Other factors fueling the growth of the IoT IAM market include, continued emphasis and investments on digital transformation projects across industry sectors and geographical regions, and growing popularity of next generation of wireless technologies, such as LP WAN, 5G, and Gigabit LTE.

- IoT IAM market is still in the nascent stage with the presence of multiple vendors reorganizing their unified IAM solutions to support the requirement of IoT IAM solution. Additionally, the specialized IoT IAM vendors are engaging with numerous small scale and pilot projects to establish the authenticity and effectiveness of a purpose-built IoT IAM solution. IoT IAM market is expected to evolve towards an integrated IoT security solution to include the integrated solution for root-of-trust, device-centric identity and access management, end-to-end data security, comprehensive device visibility and granular access control, and such others.

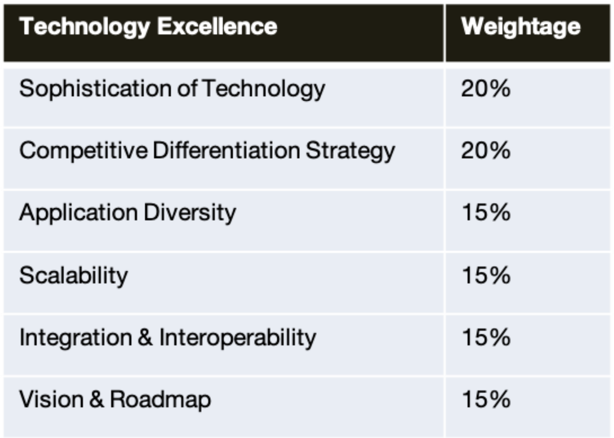
Figure: IoT IAM Solution and Capabilities


Applications
IoT Identity and Access Management (IoT IAM)
Device Registration and Onboarding
Identity Lifecycle Management
Device Lifecycle Management
API Management and Security
Device Authentication and Authorization
Data Sharing and Encryption
Centralized Policy Management
Configuration Management & Updates
Policy-based Access Management
Relationship Management (Device-Human-Device)
Certificates and Keys Management
Logging and Event Analytics
Root-of-Trust
Security and Privacy by Design
Automation and IoT-grade Scalability
Communication Networks
Wifi
Cellular
Zigbee
NFC
LP-WAN
Bluetooth
MQTT
CoAP
XMPP
AMQP
IoT Devices
Consumer IoT Devices
Smart Sensors
Industrial Sensors
Industrial Devices
Industry Application
Consumer IoT
Smart City
Automotive
Healthcare & Medical Device
Industrial IoT

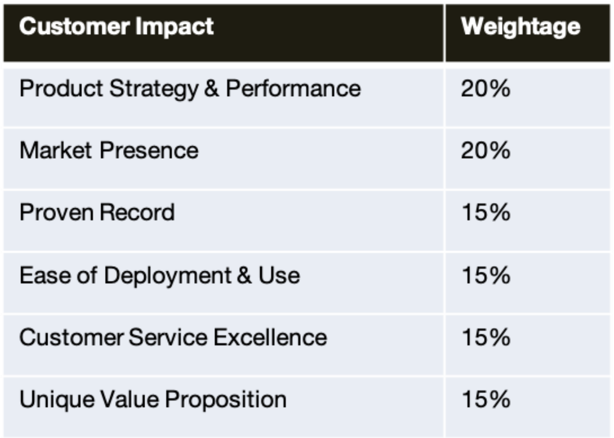
Source: Quadrant Knowledge Solutions

SPARK Matrix Analysis of the IoT Identity & Access Management Market

Quadrant Knowledge Solutions conducted an in-depth analysis of the major IoT Identity & Access Management vendors by evaluating their product portfolio, market presence, and customer value proposition. IoT Identity & Access Management market outlook provides competitive analysis and a ranking of the leading vendors in the form of a proprietary SPARK Matrix™. SPARK Matrix analysis provides a snapshot of key market participants and a visual representation of market participants. It provides strategic insights on how each vendor ranks related to their competitors based on their respective technology excellence and customer impact parameters. The evaluation is based on the primary research including expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall IoT Identity & Access Management market.



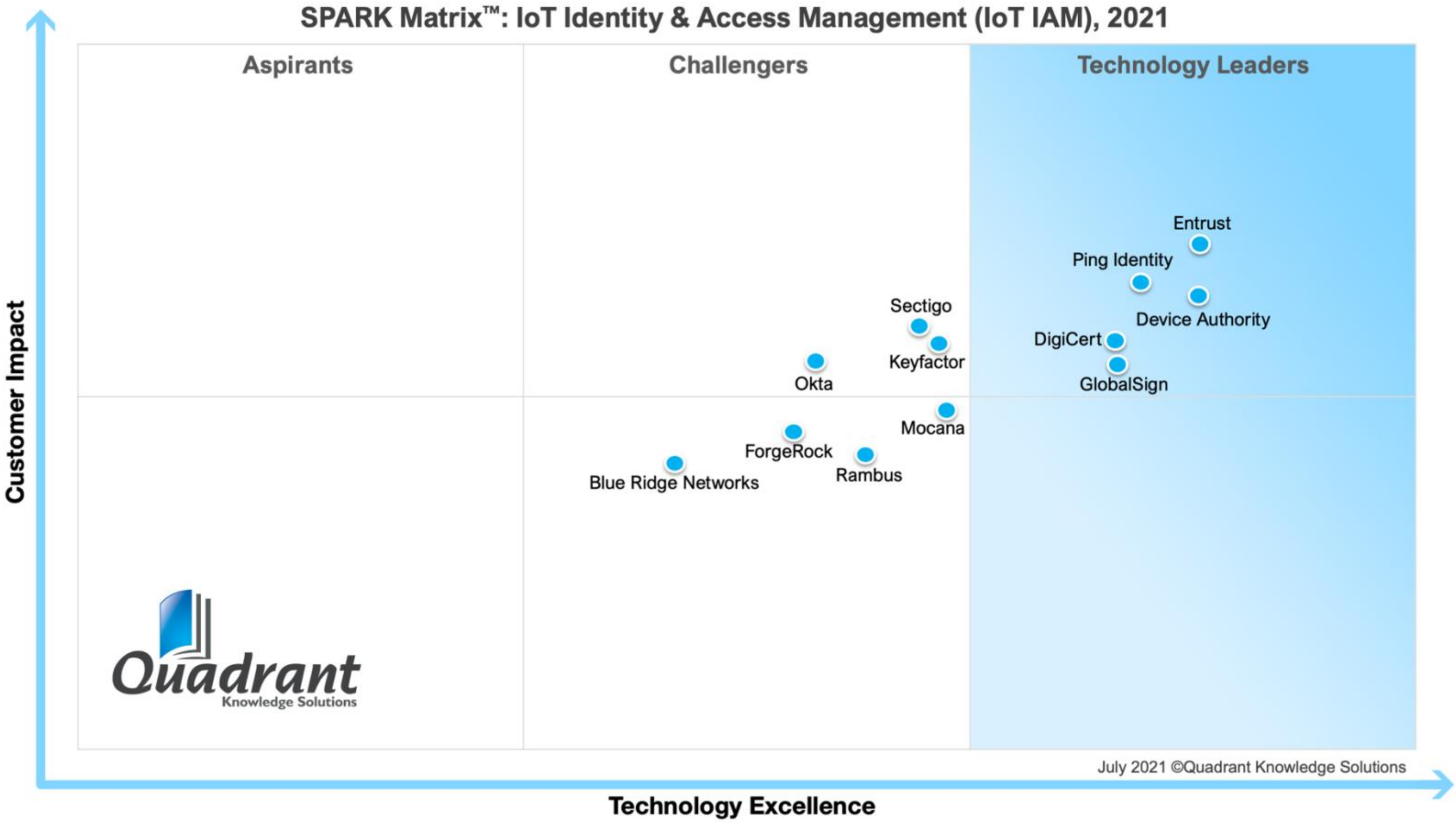
Technology Excellence	Weightage
Sophistication of Technology	20%
Competitive Differentiation Strategy	20%
Application Diversity	15%
Scalability	15%
Integration & Interoperability	15%
Vision & Roadmap	15%



Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

According to the SPARK Matrix analysis of the global IoT Identity & Access Management market, “Device Authority, with a robust functional capability of its product - ‘KeyScaler’, has secured strong ratings across the performance parameters of technology excellence and customer impact, and has been positioned amongst the technology leaders in the 2021 SPARK Matrix of the IoT Identity & Access Management market.”

Figure: 2021 SPARK Matrix
(Strategic Performance Assessment and Ranking)
IoT IAM Market



Device Authority Capabilities in the Global IoT Identity & Access Management Market

Founded in 2016 and headquartered in Reading, UK, Device Authority is a provider of identity and access management solutions for the Internet of Things (IoT). KeyScaler is the device-centric IAM platform from Device Authority that offers device-bound data security for IoT devices.

KeyScaler offers comprehensive IoT security solutions to encapsulate “Security by design”, “privacy by design”, “simplicity by design”, and “trust by design”. The solutions offer capabilities that deliver Security Lifecycle Management & Orchestration, including secure device registration and provisioning, end-to-end data encryption, automated certificate lifecycle management, automated password management, tokenized authentication, secure updates of software and firmware on IoT devices, network access control functionality, and such others. KeyScaler provides secure & automated provisioning and onboarding of IoT devices through establishing a strong Root of Trust (RoT) utilizing bootstrap keys and certificates and patented Dynamic Device Key Generation (DDKG) technology. KeyScaler provides policy-driven end-to-end data encryption for secure delivery and storage of data. KeyScaler ensures IoT device certificates and keys are securely generated, provisioned, managed, and signed through policy-driven automation. It also includes an optional feature “Secure Soft Storage” to store certificates and the associated keys encrypted in the device for additional security against theft and unauthorized use.

KeyScaler provides tokenized security for policy driven IoT security operations through Delegated Security Management (DSM). DSM provides device makers and IoT applications with a turnkey, plug-and-play IoT security suite that is easy to deploy & manage and provides policy-driven automation for scalability. The comprehensive out-of-the-box security suites for Microsoft Azure and PTC ThingWorx allow customers to quickly implement, accelerate deployment and leverage their existing investments in Microsoft and PTC infrastructure. KeyScaler platform helps in preventing unauthorized software and firmware updates on IoT devices. The platform provides a Code-signing and Secure Update delivery solution to ensure software updates are securely deployed to authorized devices.

KeyScaler platform includes Edge based deployment support, where a lightweight version of KeyScaler has been created specifically for Edge nodes, with the ability to register, authenticate, and provision certificates & tokens to devices in the local network, independent of an available internet connection. This enables customers to provide Security Lifecycle Management functionalities for private local network deployments for applications such as retail, industrial and factory. As more and more IoT use cases are at the edge, there are significant security risks due to limited security management resources. The edge security model needs to accommodate offline devices, constrained devices, and data privacy without much overhead or human intervention. KeyScaler platform’s core design principles of simplicity, interoperability, privacy, and trust are extended to Edge now making it the only solution when customers care about unified device and data trust in one platform at scale for edge use cases.

KeyScaler platform includes Automated Password Management (APM) solution that enables organizations to set and manage local account password on IoT devices at scale. APM significantly helps to reduce the attack surface by enforcing password rotation policies on the devices.

Backed by the company's flexible device interface protocol, KeyScaler offers three alternatives for device authentication: patented Dynamic Device Key Generation (available as an SDK, or Agent), and agentless PKI Signature+ or mutual TLS utilizing a bootstrap device certificates and standards-based communications, providing flexibility for a wide range of device types and capability. KeyScaler's Enhanced Platform Integration Connector (EPIC) allows for easy integration with any external platforms and services. KeyScaler also provides configurable service connectors for AWS IoT services, and interoperability with public certificate authorities (CA), such as IdenTrust (part of HID Global) or DigiCert. KeyScaler platform includes a Hardware Security Modules (HSM) Access Controller for secure and easy integration of applications, services, and devices with off-the-shelf HSMs, via a standard set of RESTful APIs.

KeyScaler platform includes Network Access Control (NAC) functionalities suitable for IoT environment. KeyScaler platform leverages PKI certificates to authorize specific devices to register into the network. The platform can automate the process of managing device identity, device registration & onboarding, PKI lifecycle management for devices, and also provides integration with Microsoft Active Directory for validation during the network authentication process.

Device Authority has partnered with leading IoT platforms including Azure IoT, PTC ThingWorx and AWS IoT and utilizing KeyScaler’s EPIC framework can integrate to Any IoT Application e.g., Google IoT Core; HSM products including Entrust and Thales (Gemalto); certificate authorities including IdenTrust (part of HID Global) and DigiCert. Built on a service-oriented architecture, KeyScaler offers multiple deployment options like on-premise, SaaS, or as multi-tenant service platform for cloud and service providers.

Analyst Perspective

Following is the analysis of the Device Authority capabilities in the IoT IAM market:

- Device Authority KeyScaler platform offers robust IoT security solution through a unified trust model by combining device, data trust and operationalizing trust at scale. KeyScaler IoT IAM platform provides sophisticated functionalities to deploy and manage PKI for IoT devices at scale through automated device onboarding, zero-touch provisioning, authentication, credential management, secure updates solutions and end-to-end policy defined data encryption. Additionally, it helps to protect, accelerate, and manage IoT solutions with its Highly flexible Life Cycle Management solution.

- Security by design, privacy by design, simplicity by design and trust by design are all approaches the ecosystem is now considering to solve IoT use cases, ensuring initial security, the lifecycle is managed securely and people safety is maintained. The KeyScaler platform encapsulates these concepts and really embraces simplicity by design to make IoT Deployments work. A good example of this is KeyScaler's recent innovation for Edge capabilities, where localised private "offline" security management capability is required for a broad range of IoT use cases i.e. Industrial, Factory, Medical. These use cases cannot rely on having an internet connection, they need to be isolated, so cannot connect to cloud hosted services, PKI vendors, 3rd party CAs etc. they must operate within their own environments but still offer the same security management capabilities.

- KeyScaler is device and platform-independent, with features like "secure by design", patented DDKG for robust authentication, device-bound identity and data security, security suites for IoT platforms for easy integration such as Azure IoT, ThingWorx and AWS IoT. Device Authority's Enhanced Platform Interface Connector (EPIC) enables a flexible and seamless approach to interfacing to Any IoT Application or service e.g. Google IoT Core. HSM Access Controller and a strong partner ecosystem. The device-bound identity and data security model is unique for this platform and helps to meet the unified security requirements for critical IoT use cases.

- Device Authority KeyScaler provides device-bound identity, authentication and data security, device and data trust at the application layer, code signing and security updates, zero-touch provisioning, and operational security. Additionally, it allows to easily integrate with cloud platforms, enterprise infrastructure, and PKI trust infrastructure like HSMs, Cas.

- Geographically, Device Authority has a strong presence in the USA and Europe. From the industry vertical perspective, the company has a presence across a wide variety of industry verticals including healthcare & life sciences, manufacturing, energy & utilities, transport (Automotive & Marine), retail & eCommerce, govt & public sectors, and IT & telecom. From a use case perspective, Device Authority has deployed many solutions across a wide range of use cases including surgical robots in hospital theatres, outpatient medical monitoring, sterilization and surgical products, identity and key management for oil/gas infrastructure and monitoring, identity management for automotive & marine, automotive secure factory environments, key management and provisioning on production lines, and security lifecycle management for PKI.

- The primary challenges before Device Authority include the competition from vendors with traditional technology offerings aligned to enterprise use cases, where these vendors attempt to pivot and position themselves into IoT, where these vendors claim to offer IoT Solutions but in reality, do not solve the fundamental problems. These vendors have successfully gained a strong market position with increased penetration amongst small to mid-market organizations and are amongst the primary targets for mergers and acquisitions. Device Authority may face challenges in expanding its market presence in Canada, Latin America, Asia Pacific, and Middle East & Africa region. However, Device Authority, with its sophisticated technology platform, comprehensive functional capabilities, compelling customer references, wide set of use cases, and robust customer value proposition, is well-positioned as the leader to maintain and grow its market share in the IoT IAM market.

- Responding to customer demand and a shift to the Edge, Device Authority is innovating in new KeyScaler Edge technology which provides IoT IAM directly within the localized ecosystem at the edge. Additionally, the company is focusing on improving their platform by enhancing AI/ML-based authorization, Blockchain identity and access management, user-managed access, and 5G.