Entrust Datacard Emerged as 2019 Technology Leader in the SPARK Matrix Analysis of IoT IAM Market

KNOWLEDGE BRIEF

BY

Quadrant
Knowledge Solutions

Entrust Datacard Emerged as 2019 Technology Leader in the SPARK Matrix Analysis of IoT IAM Market

Driven by industry 4.0 and digital transformation trends across consumer, healthcare, manufacturing, and infrastructure, organizations are increasingly adopting smart IoT, cloud, and advanced analytics solutions to improve operational performance, customer experience, and overall business growth. The scale of IoT devices, applications, and data continue to grow significantly, and thereby, IoT solutions are increasingly becoming an integral part of business and industrial operations. Advancements of networking technologies, including LPWAN, LTE, and 5G, is further driving the adoption of smart IoT solutions.

Widespread adoption of IoT devices is significantly increasing the attack surface and the number of potential threats. A growing number and frequency of IoT-specific cyber-attacks, such as DDoS, malware, spoofing, data breach, and others are significantly raising the security concerns of IoT devices. Growing security concern has emerged as the most significant barrier in the adoption of IoT devices for industrial applications since a compromise in IoT security can have far more devastating consequences from monetary loss, data loss, to the life-threatening impact.

Quadrant Knowledge Solutions recent analysis of the global IoT IAM market "*Market Outlook: IoT Identity & Access Management (IoT IAM), 2019-2024, Worldwide*" provides strategic information to the technology vendors in formulating their growth strategies and users in evaluating different vendors capabilities, competitive differentiation, and market position. The research includes SPARK Matrix™ analysis of major IoT IAM vendors evaluating their technology capabilities, market presence, and overall value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall IoT IAM market.

IoT Identity & Access Management (IoT IAM) market consists of vendors that offer a scalable solution for deploying and managing security keys and certificates to enable device identity and integrity to be cryptographically proven and validated throughout its lifecycle. Securing IoT devices require a purpose-built device-centric IAM solution as traditional employee-centric IAM or customer IAM (CIAM) solutions are not capable of addressing IoT-specific challenges. Traditional IAM systems were designed to enforce access control policies for the users and their access to enterprise networks, applications and data. These systems are not capable of handling billions of IoT devices, their identities, and communications with other entities, including other devices, people, and applications on the network. A purpose-built IoT IAM solution capabilities, include 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.

SPARK Matrix™ Analysis of the Global IoT IAM Market
*Entrust Datacard has emerged as 2019 Technology Leader in the Global IoT IAM Market*

Quadrant Knowledge Solutions conducted an in-depth analysis of the major IoT IAM vendors by evaluating their product portfolio, market presence, and value proposition. The IoT IAM market outlook provides competitive analysis and a ranking of the leading vendors in the form of proprietary SPARK Matrix™. SPARK Matrix™ analysis provides a snapshot of key market participants and a visual representation of market participants and provides strategic insights on how each vendor ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall IoT IAM 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 IAM market, Entrust Datacard, with its sophisticated ioTrust™ security platform has secured strong ratings for the overall parameters of technology excellence and customer impact. Entrust Datacard has been positioned as the clear technology leader in the 2019 SPARK Matrix™ of the global IoT IAM market.

"Entrust Datacard ioTrust™ security platform provides sophisticated functional capabilities to enable organizations to build a trusted foundation for operational infrastructure, supply chain integrity, and data security from sensors to the enterprise cloud platforms. The ioTrust™ security solution portfolio is well-positioned to help organizations in implementing secure by design strategies by establishing a root-of-trust throughout the device lifecycle," according to Piyush Dewangan, Industry Research Manager at Quadrant Knowledge Solutions. "Entrust Datacard, with a continued focus on technology innovation, industry-specific expertise, and a strong partner ecosystem can acquire significant market share in the global IoT IAM market," adds Dewangan.

Figure: 2019 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
IoT Identity & Access Management (IoT IAM) Market
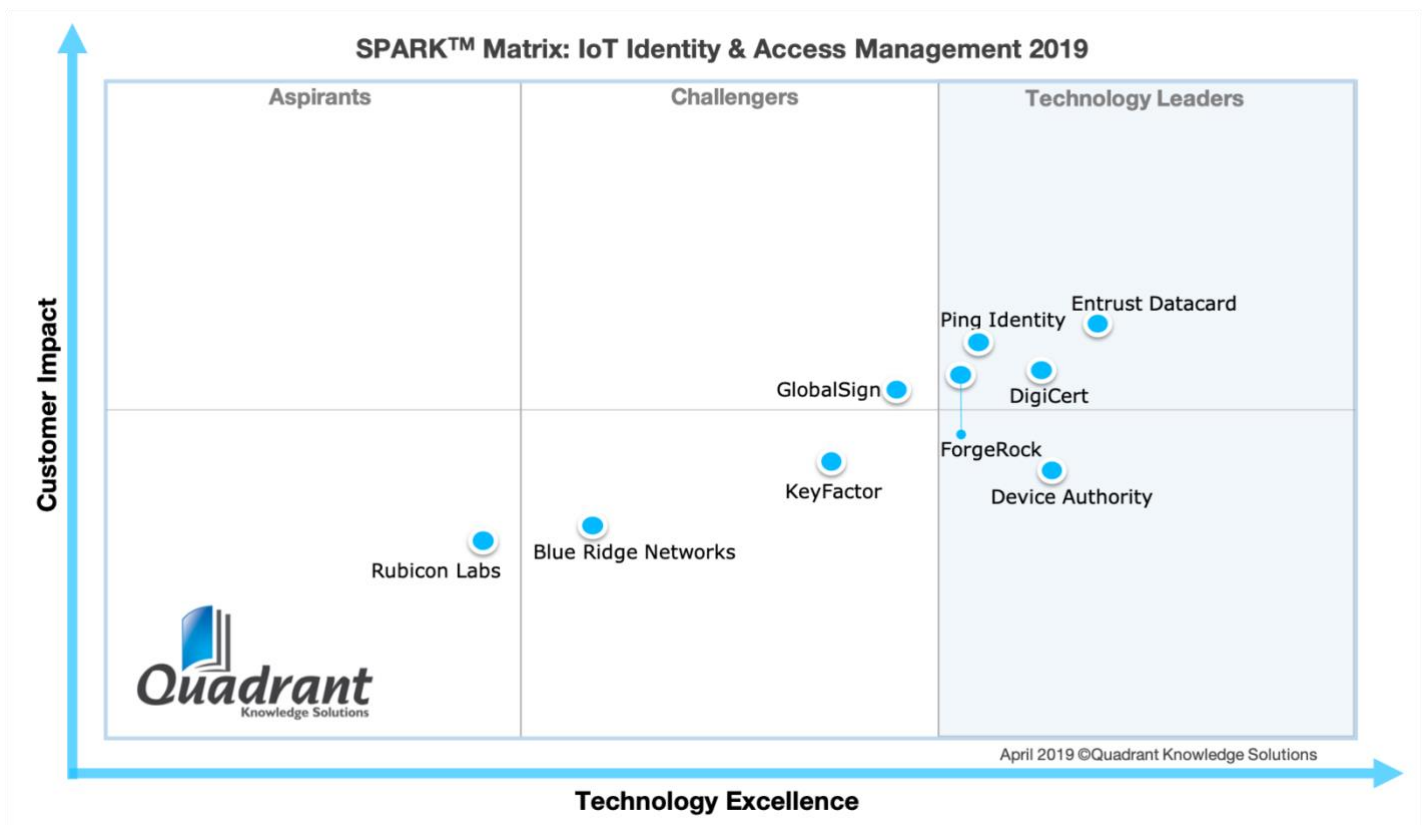
Entrust Datacard's Capabilities in the Global IoT Identity & Access Management (IoT IAM) Market

Entrust Datacard offers ioTrust™ security solution into three distinct tiers from identity provisioning during device manufacturing for establishing a root-of-trust to addressing operational security by providing strong authentication and authorization, data integrity, and identity lifecycle management solution. The solution is technology agnostic and enables easy integration with both brownfield and greenfield IT/OT infrastructure. ioTrust™ solution supports deployments over on-premise appliances, software license, and managed cloud services.

- ◆ **ioTrust™ Identity Issuance**: Leveraging 20+ years of PKI and cryptographic technology, the Identity Issuance solution helps in establishing a root of trust by provisioning trusted identities to IoT devices during its manufacturing enabling organizations to validate device authenticity, federate device ownership, and allow fast enrollment of devices in the supply chain ecosystem. Organizations can uniquely identify each device during its lifecycle, thereby enhancing supply chain visibility and facilitating enablement of operational services. The solution enables bulk and on-demand issuance of devices identities to support manufacturing scalability.

- ◆ **ioTrust™ Identity Management**: ioTrust™ includes identity lifecycle management for IoT devices, including enrollment, renew, suspend, and termination of device identities in real-time to address operational security requirements. Identity Management solution offers strong authentication and authorization policy management to secure device-to-device and device-to-application communications. Vital validation services for IoT certificates are baked into the core solution with embedded CRL publishing and an OCSP Responder within the solution's Service(cloud) Gateway. ioTrust™ includes a web-based management console for provisioning managed identities, real-time monitoring of IoT infrastructure, and visibility into the operational environment from the sensor level to the enterprise data hub via a managed and secured MQTT telemetry stream. The solution helps organizations in improving the operationalization of IoT devices into their connected ecosystem.

- ◆ **ioTrust™ Identity and Data Security**: The solution allows organizations to enforce granular controls over data acquisition, access to data streams, and command execution. It helps organizations to improve supply chain integrity, device visibility and provides an ability to track the security history of the IoT devices from its manufacturing through the entire lifecycle.   Easy to use

libraries and APIs allow customers to leverage managed identities with their existing toolchains.

♦ **ioTrust™ Security Solutions for Industries**: A robust IoT security strategy is fundamental to the success of digital transformation use cases, such as connected industries, connected infrastructure, connected vehicles, and connected ecosystem. Entrust Datacard offers industry-specific capabilities for industrial verticals (energy, utility, chemical, and manufacturing), automotive, and telecom sectors. The ioTrust™ security solution is compatible with various industrial protocol and secures both greenfield and existing brownfield IoT devices in the industrial environment. It helps in connecting remotely deployed industrial IoT devices into an enterprise data hub to securely collect operational data for reporting and analytics. ioTrust™ security solution for automotive helps in building a trusted foundation for secure communication, command and control of connected vehicles and helps in mitigating emerging risk. ioTrust™ security solution helps automotive companies in implementing IoT security strategy by embedding trusted managed identities early from component supply chain to vehicle manufacturing, to initial ownership and the entire lifecycle of the vehicles. It offers a trusted automotive ecosystem for service delivery and secures vehicle-to-vehicle and vehicle-to-infrastructure communications. ioTrust™ solutions help telecom companies in leveraging IoT opportunities and expanding their revenue streams beyond connectivity to provide end-to-end content-based service delivery. ioTrust™ security solution helps telecom companies in creating a trusted IoT ecosystem by providing trusted device identities across the network, secure gateways, and data encryption to ensure data is accessed only by authorized devices, applications, and people. Telecom companies can securely collect data and create dynamic analytic insights from millions of connected devices to provide value-added services to their customers.

♦ **Competitive Differentiation**: Entrust Datacard key differentiator is primarily attributed to its comprehensive device-centric functional IAM capabilities to secure complete device lifecycle from establishing a root-of-trust to ensure security throughout its operational lifespan. ioTrust™ solution for supply chain integrity, trusted infrastructure and secure data acquisition management helps to establish a trusted digital ecosystem to secure complex interaction between connected systems, users, and things. Entrust Datacard has demonstrated a robust implementation of ioTrust™ solution in the energy & utility industry along with growing installed base in the automotive, industrial manufacturing, medical devices, transportation, and telecom sectors. Entrust Datacard brings strong industry experience in the authentication and identity

management segment and is expected to post significant revenue growth in the next four to five years.

The Last Word

Founded in 1969 and with over 2000 employees in 34 worldwide locations, Entrust Datacard is a well-recognized vendor in the trusted identity and secure transaction technologies market. Entrust Datacard ioTrust™ platform includes comprehensive capabilities for scalable enrollment and provisioning of trusted identities, identity lifecycle management, centralized management console, authentication, policy-based authorization, and granular access control. Additionally, leveraging enterprise-grade encryption technologies, ioTrust™ provides end-to-end data encryption to secure data transmission from the field to the enterprise data hubs. Driven by the highest overall ratings across technology excellence and customer impact, Entrust Datacard has been positioned as the 2019 technology leader in the SPARK Matrix™ evaluation of the global IoT IAM market.