50 Years of Growth, Innovation and Leadership

IoT Data Security Market Watch: Solutions to Address the Key Industry Requirements

Responsive, Upgradeable and Easy-to-Use Data Security is Essential for the IoT

A Frost & Sullivan White Paper

FROST & SULLIVAN

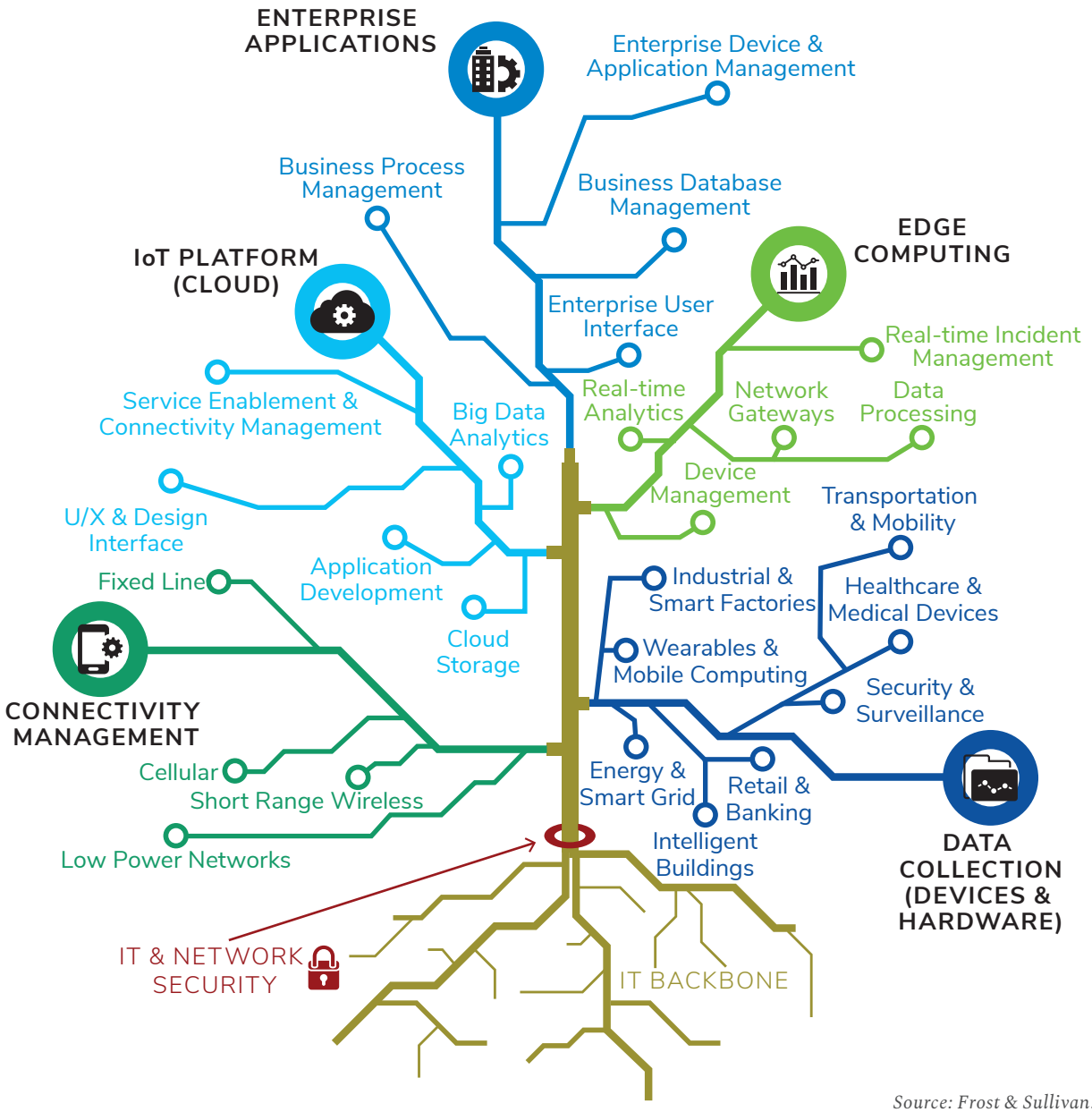
CONTENTS

INTRODUCTION AND OVERVIEW

This Frost & Sullivan white paper describes the key requirements in the Internet of Things (IoT) data security market and highlights how Sixgill—a leading provider of IoT data services—addresses these requirements. Frost & Sullivan also provides perspectives on the growth drivers for the IoT data security market.

IoT Market Growth

EXHIBIT 1: IoT ECOSYSTEM COMPONENTS, GLOBAL, 2019



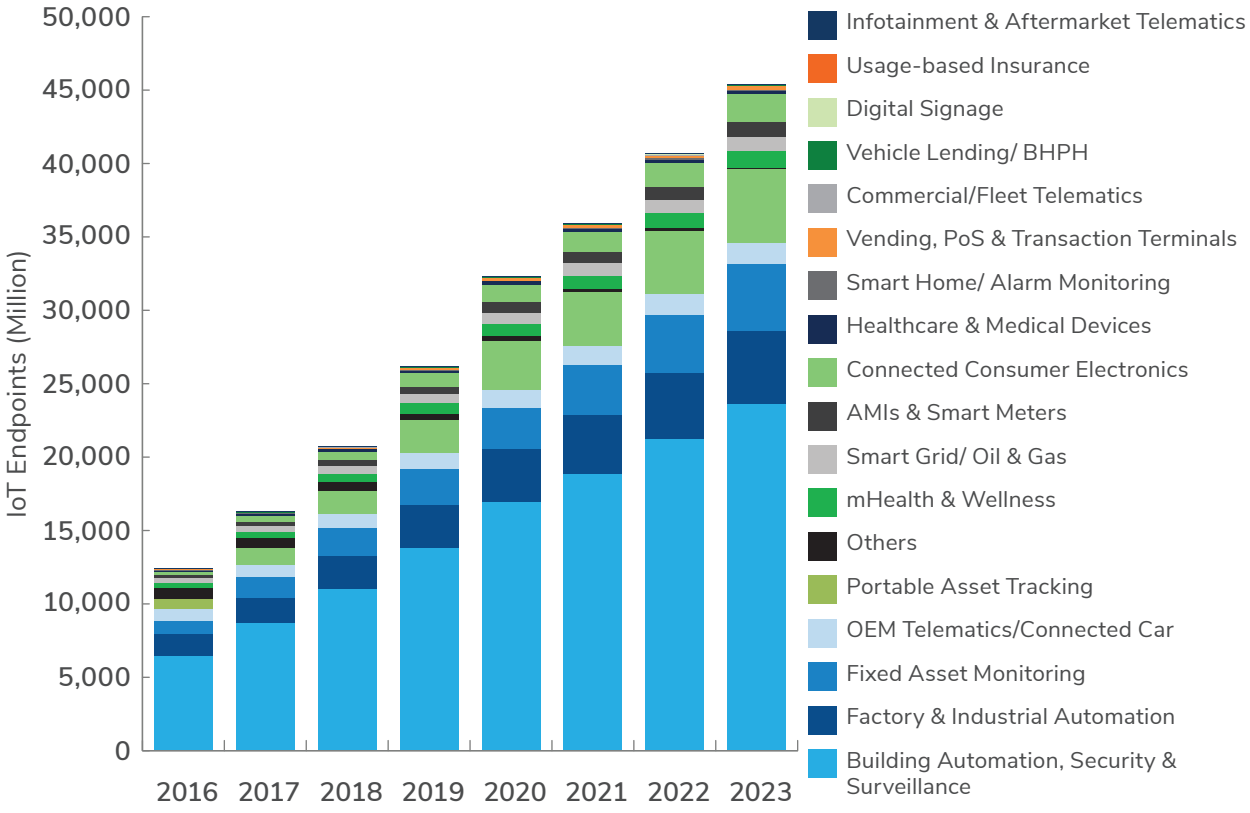
Source: Frost & Sullivan.

EXHIBIT 2: MAJOR GROWTH OPPORTUNITIES IN IoT, GLOBAL, 2019

Connected Car	Connected Spaces	Smart Grid and Utilities	Fleet Telematics	Industrial Automation
Consumer telematics and vehicle diagnostics	Connected smart building and automation deployments	Demand response, automated meter reading, efficient infrastructure management	Managing fleets and commercial vehicles	Smart manufacturing, and industrial process control environments
Internet connectivity and media in vehicles	Security and monitoring deployments in connected buildings	Monitoring pipelines and upstream, midstream, and downstream operations	Autonomous vehicle operations	Supply chain, logistics and quality control, predictive and preventative maintenance
Vehicle-to-vehicle communications			Regulatory compliance and vehicle diagnostics	

Source: Frost & Sullivan.

EXHIBIT 3: IoT CONNECTIONS FORECAST, GLOBAL, 2016–2023



Note: All figures are rounded, the base year is 2017.
Source: Frost & Sullivan.

Frost & Sullivan expects the total number of IoT devices to grow from approximately 12.4 billion devices in 2016 to over 45.4 billion devices in 2023, at a global compound annual growth rate (CAGR) of 18.6%. Building automation systems and security systems are expected to account for over 50% of all IoT devices over the forecast period. Other leading verticals for IoT include connected transport, manufacturing, fixed asset tracking, smart grid, oil and gas, and smart utilities.

Emerging Trends in IoT Data Security

EXHIBIT 4: KEY EMERGING TRENDS IN IoT DATA SECURITY, GLOBAL, 2019

1 **Blockchain for IoT Data Security***	Blockchain-based implementations continue to see greater use in the IoT data security markets. The various applications of distributed ledger technologies in blockchain include secure firmware updates, secure data communication through tight integration with PKI technologies, and data integrity and lifecycle management.
2 **Integrated IT, IoT and OT Security****	The convergence of IT, IoT and OT networks is driving the need for integrated connected devices security. Support for heterogeneous environments across customers' extended enterprise—including campus, data center, public cloud, private cloud, and OT—through integrated solutions is an important trend.
3 **IoT Risk Management**	IoT Risk Management comprised of functions such as assisting customers with defining key risks, understanding their probability and impact on business processes, identifying anomalous processes and entity behaviors and developing response strategies is an important need of the IoT industry.
4 **Security for Microservices**	Given that containers are expected to be the next generation of virtualization platforms in IoT, solutions to secure individual containers are an emerging need for IoT data security. Providers must focus on implementing very specific technologies, such as edge ID orchestration, to secure IoT microservices.
5 **Security by Design in IoT**	Security-by-design continues to remain the fundamental requirement in IoT. Implementations that can help secure IoT devices during the product development phase are essential to secure the IoT. Close integration between DevOps and SecOps is also a much-needed requirement for IoT data security.

*For additional information on this trend, please read the Frost & Sullivan deliverable: **IoT Cybersecurity Analysis—Blockchain-enabled IoT Cybersecurity Market, 2018** Implementing New Service Models through Distributed Ledger Technologies

** For additional information on this trend, please read the Stratecast/Frost & Sullivan deliverable: **IT and OT Silos are Breaking Down; Network Access Control 2.0+ Smooths Transition** NAC Foundational Device Visibility and Control for IT/OT Convergence

Source: Frost & Sullivan.

Ensuing end-to-end IoT security requires a combination of technologies, processes, and systems. For example, a Trusted Execution Environment (TEE) for critical low-level software operations can be used for data security enablement. A TEE is an environment within the main processor on a device which enables a secure operating system (OS), and allows Trusted Applications (TAs) to run on it. This secure

OS runs alongside the normal OS (e.g. Android). Partitioning the software into normal code and a small protected trusted code base for security sensitive operations enables protection with hardware-level isolation. This architecture has been successfully used in the mobile computing space to deliver robust protection against common security threats. Applying the proven security advancements of mobile computing to IoT can be a sensible and practical approach to delivering scalable IoT solutions.

It is also imperative for the IoT stakeholders to invest in post-deployment monitoring technologies that can identify anomalies by comparing network configurations and traffic patterns with validated baseline configurations. Adopting a multi-layered data security strategy, focused on deep network indexing along with blockchain, AI and ML can help deliver strong data security in IoT. Providers must evaluate the number and types of protocols that they examine or monitor in the network and focus on understanding the interplay between these to generate maximum visibility.

COMPANY PROFILE: SIXGILL SENSE™ DATA SERVICES PLATFORM[1]

Key IoT Data Security Market Need: Unified, Programmatic and Secure Sensor Data Processing for the IoT

With the growth of microelectronics, ubiquitous connectivity, and predictive computing, IoT is poised for rapid growth. Security is essential for reliable operations of IoT. Malfunctioning or 'compromised' IoT devices, whether malicious or accidental, can pose significant risks to consumers, businesses and societies. In fact, Frost & Sullivan research indicates that more than 70% of organizations currently believe security is a top consideration in IoT purchase decisions. This statistic is only expected to accelerate in the coming years.

As IoT matures, the emphasis will be on implementing approaches that enable IoT devices to interact with—and learn from—other IoT endpoints and data sources to enable proactive decision making without human intervention. In order to maximize the value of connected intelligence, a wide range of industries must unify and manage the collection of streaming data from disparate sensor sources to enable context-driven decision making. With an increased emphasis on data-driven consumer and business operations facilitated through IoT, the amount of data generated from IoT deployments has continued to increase rapidly. For example, it is estimated that autonomous vehicles will generate several Terabytes (TB) of data. As IoT enters this era of the "sensing applications" supported by sensors, machine data and data processing software, there is a clear need for platform solutions that can provide large-scale data acquisition, storage and analysis capabilities to manage the large amounts of time-series data generated by IoT deployments.

Relying on even slightly corrupted data streams to support real-world operations can have disastrous consequences in this era of hyper-connectivity. Therefore, IoT data platform solutions and associated data security implementations must ensure that emitted, transmitted, ingested and stored sensor

1 Profile Source: Sixgill, Frost & Sullivan

data is authentic. While encryption technologies are critical for securing the data, it may not always be possible to verify that the data chain has not been compromised by using encryption only. Therefore, in addition to encryption, platform implementations must also have the required capabilities to ensure that data being processed, stored, automated and shared in not modified or changed in an unauthorized manner.

EXHIBIT 5: KEY MARKET NEEDS FOR IoT DATA SECURITY, GLOBAL, 2019

Data Management

Data lifecycle management for next-generation IoT

Unified, high-performance platform solutions designed to programmatically manage IoT data lifecycle and enable automated decision making are essential for IoT value delivery

Data Integrity

Ensuring IoT data integrity is maintained at all times

Addressing real-world operating problems through IoT requires that data integrity to be maintained at all times during the data creation, transport, storage and analysis stages

Real-time Performance

Speed & responsiveness of IoT data operations

Data operations, including securing, transmission, reformatting and normalization, and analytics must be completed within the latency requirements of IoT vertical applications

Source: Frost & Sullivan.

Sixgill Sense™ Data Services for the Internet of Everything

Sixgill, LLC provides universal sensor data automation services that enable organizations to govern Internet-of-Everything (IoE) assets—people, places and things. The company offers the Sixgill Sense 2.0 platform to enable IoT developers to easily acquire, analyze and act on any sensor-generated data—at any velocity or scale—in a rules-based and machine learning environment. Sense can be used on a PaaS basis, installed on-premise, deployed on the Edge, or hybrid configurations. With features such as:

1. micro services-based architecture to enable support for unrestricted sensors and stream data types,
2. advanced plug-and-play modules to shorten programming for IoT use cases,
3. sophisticated IoT edge computing agents with Machine Learning, Rule Processing, and Blockchain compatibility; and
4. an expanding list of partners and channel alliances, the Sixgill Sense platform supports high-performance, data-driven IoT applications.

Enterprise customers can ingest new sensors and stream data types quickly in the Sixgill Sense platform, and combine sensor data with contextual data to correlate among various streaming and static data sources for generating relevant and actionable insights. The platform uniquely addresses

the need for cross-enterprise data knowledge and handling as well, which is an important benefit. A range of other features, including centralized administration and monitoring, and dedicated support and service help Sense deliver the key functionality for efficiently aggregating data from various connected endpoints and relevant third-party sources.

Sixgill Sense includes built in security controls for secure communication, access control and sensor data processing and storage. Sixgill has also developed the distributed ledger technology (DLT)-based Sixgill Integrity™ solution for addressing the essential data integrity requirements of secure IoT data operations such as safeguarding data veracity, validating device authenticity and providing immutable auditability for data-driven operations. A device- and ledger-agnostic solution, Sixgill Integrity is designed from the ground up to solve the fundamental need for an end-to-end, real-time sensor data authenticity system. The tamper-proof nature of distributed ledgers ensures that data emitted, transmitted and ingested remains unchanged and is auditable. By leveraging the existing infrastructure of public blockchains, there is no need to build separate mining resources to guarantee that transactions are valid. Sixgill Integrity can be deployed independently of Sixgill Sense, to provide blockchain data authenticity for any data stream.

It is important to note that Sixgill Integrity employs a hybrid architecture approach by combining the immutability of public blockchains with an off-chain data layer to deliver data integrity and real-time performance at scale. In doing so, Sixgill Integrity also promises to overcome the limitations of centralized cloud resources used for IoT data management. Sixgill also employs edge computing which, when combined with the Sixgill Integrity solution, significantly reduces opportunities for data interception and overcomes limitations in bandwidth by reducing communication latency to maintain real-time performance. With Sixgill working on various enhancements focused on increasing the data management efficiency, scalability, collaboration and security capabilities in its solutions, the company will have an attractive offering for IoT sensor data acquisition, aggregation and processing in North America.

EXHIBIT 6: HIGHLIGHTS OF SIXGILL'S IoT SOLUTIONS, 2019

Unified Data Platform	Next-generation IoT Data Security	Strategic Partnerships and Product Roadmap
Sixgill Sense™ brings the ability to identify actionable exception events from noisy sensor data streams and **trigger programmatic responses reliably and at scale**. It includes responsive edge capabilities to preserve functionality during connectivity interruptions, attack network latency, and optimize data transfers to the cloud.	Sixgill Integrity provides a **strong foundation for IoT data security**. By deploying a hybrid blockchain-based architecture, and by combining it with various edge computing innovations, Sixgill provides a unique, effective solution to ensure complete IoT data integrity protection.	Sixgill employs a **vigorous partners and channel strategy** to support its product integration and distribution efforts. The company has ambitious plans for new product enhancements to deliver greater customer value. Sixgill is also expected to introduce an IoT developer and ecosystem collaboration program.

Source: Sixgill, Frost & Sullivan.

Analyst Perspectives

Sophisticated technical capabilities, product modularity, open architecture, and ease of use are among the key differentiators for the Sixgill Sense platform. The challenge for Sixgill would be to execute on its product enhancement strategy by acquiring the required resources to help develop new product features. Even though Sixgill offers highly agile and modern implementations, the significant marketing resources of competing industry solution providers have enabled them to capture a greater mind share among the key decision makers for IoT deployments within the large enterprises. However, in industries such as critical infrastructure, connected manufacturing and smart construction, customer references also matter during the pre-sales process. This should help companies such as Sixgill that have adopted a focused approach to addressing the time-series data management requirements of IoT and have been trusted by reputed brands for their IoT deployment initiatives.

THE LAST WORD

The criticality of deploying secure systems in the IoT cannot be overstated. Existing security technologies and mechanisms can be adapted for IoT data security. However, a range of specialized solutions must also be offered to cater to the unique operating requirements of the IoT. Data security implementations must deliver real-time protection without impacting the speed of operations and increasing device costs. Ability to upgrade data security capabilities during the lifecycle of IoT deployments is also essential. Frost & Sullivan observes increased focus on vertical prioritization among leading industry ecosystem participants. This trend is driven by the differences in privacy and compliance requirements between different industry verticals, usage of proprietary technologies across verticals, and market maturity levels in various verticals. Frost & Sullivan expects the global IoT data security market to grow significantly in the next five years due to:

1. the growing awareness of the need to secure connected deployments,
2. increasing regulatory oversight in critical industries, and
3. continued focus of the industry solution providers in deploying easy to use IoT data security solutions.

Vikrant Gandhi

Industry Director—IoT & Digital Transformation (ICT)
Frost & Sullivan
vgandhi@frost.com

Brent Iadarola

Vice President—Mobile & Wireless Communications
Frost & Sullivan
biadarola@frost.com

FROST & SULLIVAN

SILICON VALLEY | 3211 Scott Blvd, Santa Clara, CA 95054
Tel +1 650.475.4500 | Fax +1 650.475.1571

SAN ANTONIO | 7550 West Interstate 10, Suite 400, San Antonio, Texas 78229-5616
Tel +1 210.348.1000 | Fax +1 210.348.1003

LONDON | Floor 3 - Building 5, Chiswick Business Park, 566 Chiswick High Road, London W4 5YF
TEL +44 (0)20 8996 8500 | FAX +44 (0)20 8994 1389

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?