

# The Internet of Things

As seen at Matrix IoT



What we intend to do?

**Internet connectivity**

**+ digital intelligence**



01

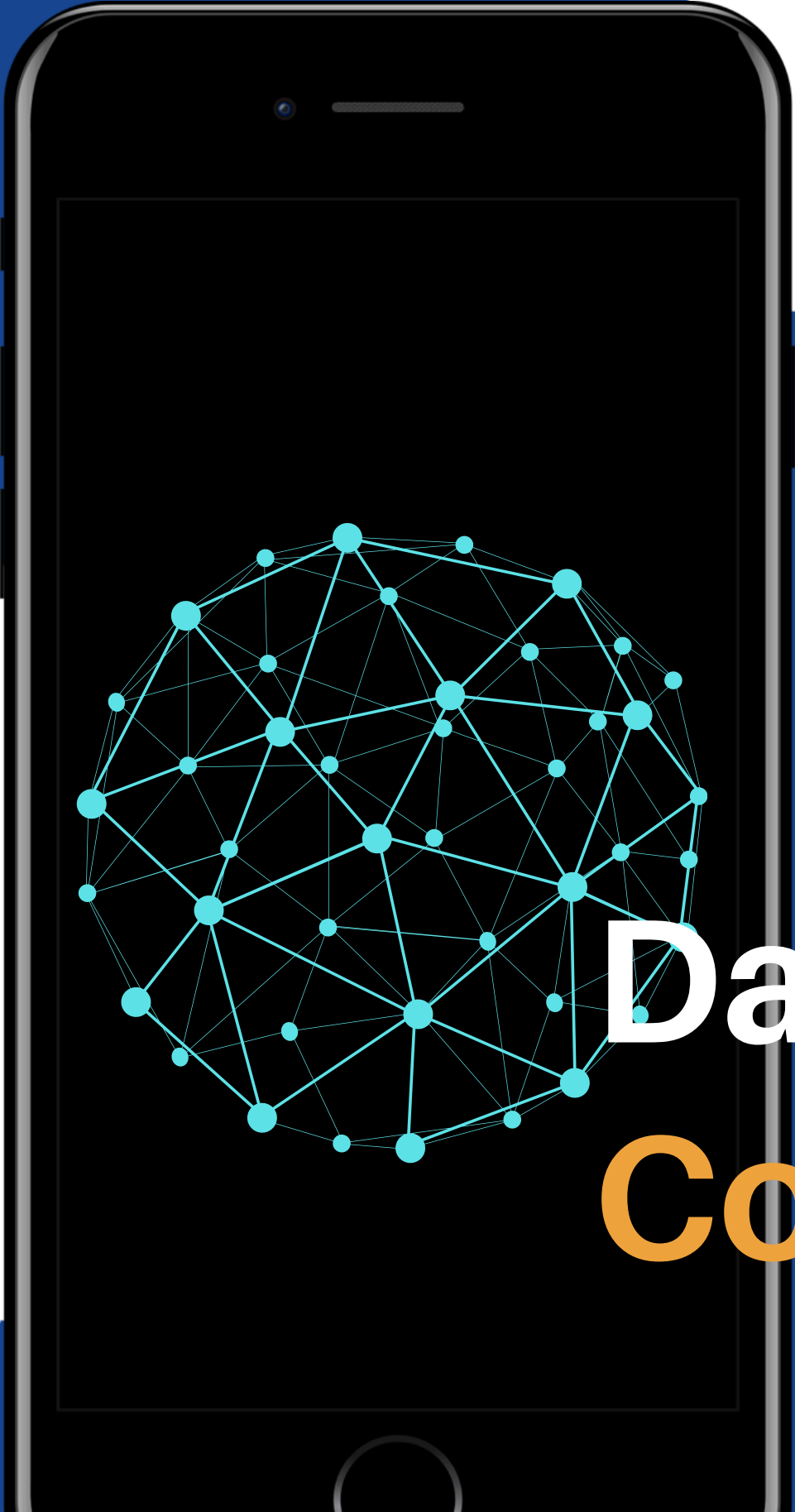
The **Challenges**  
of the Internet  
of Things

# Common Factors in IoT Sensors

- **Communication/Connectivity.**
- Storage
- **Security**

**Matrix intends to address Communication/Connectivity and Security, as security is our core competence and connectivity is an important factor.**

50% of IoT  
implementations  
struggle with  
connectivity



**Data**  
**Connectivity**

02

# Problems in Communication/Connectivity

- **Significant Impact:** A large percentage of IoT projects experience some form of connectivity challenges. Surveys often cite figures where over 50% of IoT implementations struggle with connectivity.
- **Top Business Challenge:** Data connectivity consistently ranks among the primary concerns for businesses and organizations working with IoT systems.

**Matrix IoT would like to address Device Compatibility for different standards, which helps the following issues:**

- Fragmentation in connectivity protocols
- Issues with seamless integration of devices from different manufacturers.

# Our Solution - Mat Ensemble

Securing Your IoT Ecosystem with Confidence

## The Challenge:

The Internet of Things (IoT) promises unprecedented connectivity and efficiency, but it also introduces significant security vulnerabilities.

Unprotected devices, weak authentication, and mishandled data can expose businesses and individuals to risk.

## Mat Ensemble's Solution:

Mat Ensemble is not just a product suite, but a comprehensive approach to IoT security. We tailor our solutions to your specific needs, balancing robust protection with practicality.



# Core Components of Mat Ensemble:

**Data Encryption:** We encrypt data both at rest and in transit, ensuring confidentiality and integrity even if a breach occurs.

**Regulatory Compliance:** Mat Ensemble is designed with privacy regulations like GDPR 2.0 in mind, giving you peace of mind.



**Hardware Security Modules (HSMs):** We integrate HSMs directly into your IoT devices, providing a secure foundation for encryption, key management, and authentication.

**Secure Key Management:** Our solutions follow industry best practices for key generation, storage, and rotation, minimizing the risk of compromise.

**Biometric Authentication:** Our advanced face recognition software adds an extra layer of user verification, making unauthorized access significantly more difficult.



## Key Considerations Addressed by Mat Ensemble

**Cost/Complexity:** We understand budget constraints. Mat Ensemble offers modular options, allowing you to select the level of security that fits your needs and budget. Our experienced team streamlines integration to minimize disruption.

**Power Consumption:** We recognize the importance of battery life for IoT devices. Mat Ensemble incorporates energy-efficient algorithms, ensuring that security doesn't drain your resources.

**Biometric Accuracy:** Our face recognition software boasts exceptional accuracy (FAR 99.99%, FRR 96%).

**Privacy:** We take data protection seriously. Mat Ensemble adheres to strict privacy principles, employing strong encryption and secure storage practices.

**Regulations:** We prioritize compliance. Mat Ensemble is built to meet or exceed the requirements of privacy regulations like GDPR 2.0, protecting you from legal and reputational risks.

# Why Choose Mat Ensemble?

- Proven Expertise: Our team has extensive experience in IoT security, having successfully deployed solutions across diverse industries.
- Customizable Solutions: We don't believe in one-size-fits-all. We tailor Mat Ensemble to your specific environment, ensuring maximum effectiveness.
- Ongoing Support: Our commitment doesn't end with implementation. We provide continuous monitoring, updates, and support to keep your IoT ecosystem secure.

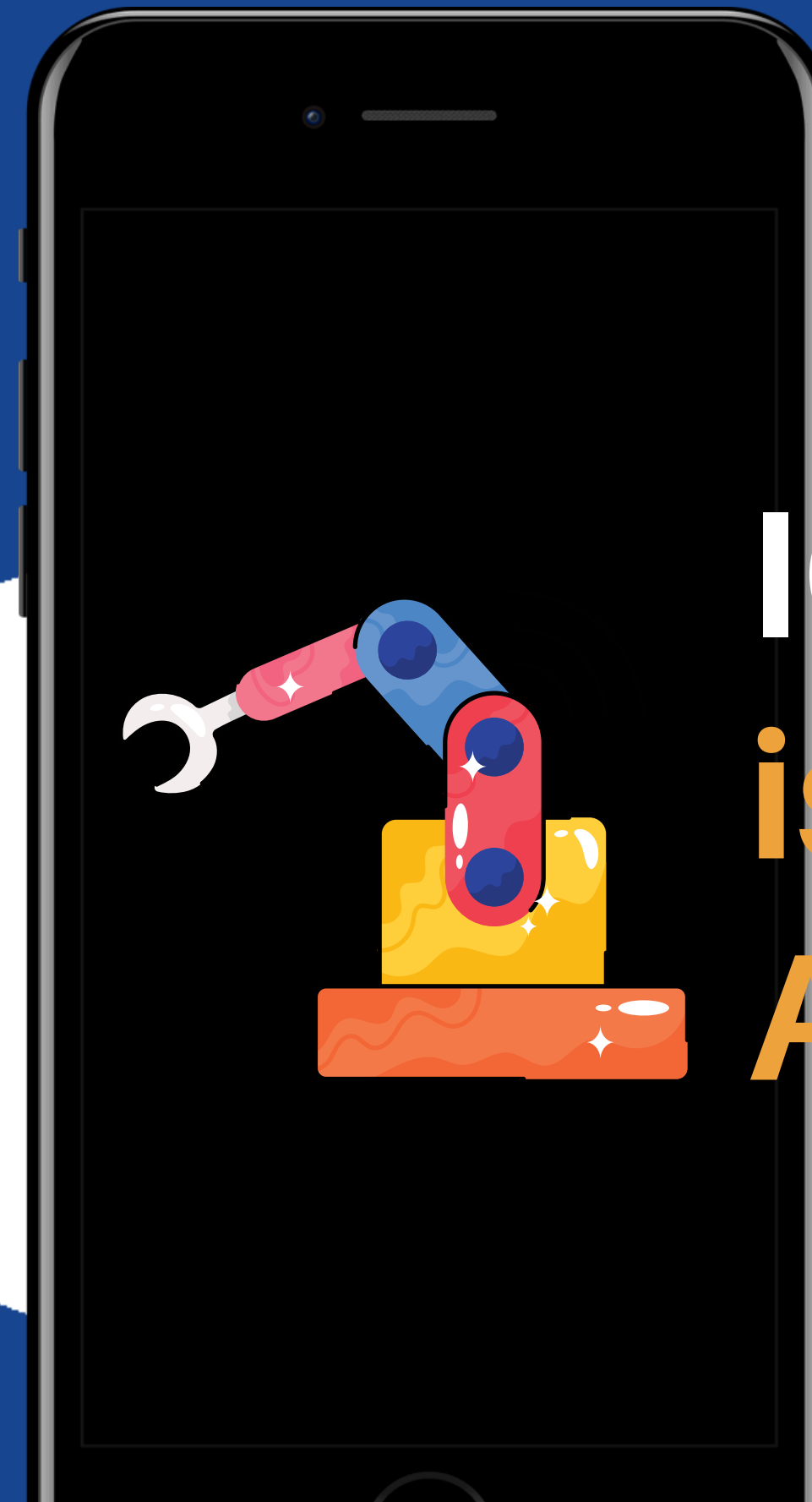
Mat Ensemble

Massive Growth = Massive Risk:  
The number of active IoT devices  
is predicted to surpass 25.4 billion  
globally by 2030 . This massive  
scale directly increases the attack  
surface for hackers.

Source:

(<https://iot-analytics.com/number-connected-iot-devices/>)

04



IOT  
is the  
Answer

# Enhancing IoT Security with Biometrics, 2FA and 3FA

## 2FA/3FA with TPM:

- Password + TPM-secured Key: The TPM can store a cryptographic key that is released only after successful password entry, providing the second authentication factor.
- Biometrics + TPM: The biometric template is stored in the TPM. During authentication, the live biometric scan is compared to the template within the secure environment of the TPM.

**Secure Boot:** Use Face recognition while the system is booting after the password authentication (1:1) or with finger authentication using webcam/QR Code. (Authenticate QR Code with a known device)

**We have developed a unique “Seamless authentication of face”. It is both Hardware and Software Based, which can be used with a server.**

**For More Details Contact**

# **Matrix IOT Solutions Sdn. Bhd.**

Co Number : 202101027697 (1427997-T)

Email : [support@matrix-iot.com](mailto:support@matrix-iot.com)

Phone : 603 7660 4280

Mobile : +60 16 217 7753/+60 16 266 3851

Website : [www.matrix-iot.com](http://www.matrix-iot.com)

