IOT Needs CIAM

The Importance of Centralized IAM in a Growing IoT Ecosystem

ADITYA KUMAR

IOT LEAD SOLUTION DESIGNER

VODAFONE IOT



Agenda

- **Internet of Things**
  - What is IoT?
  - Vodafone IoT
  - Risk of IoT
- **IAM in IOT**
  - Role of CIAM in IOT
- **Challenges in Implementation**
- **Strategy**
- **Solution**
- **Benefits**
- **Future**

Internet of Things



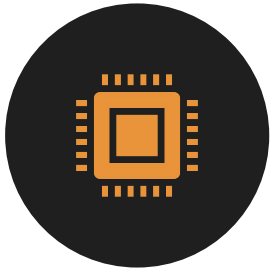
What is IoT?



The Internet of Things (IoT) refers to a network of interconnected devices, machines, objects, and even living beings that possess unique identifiers (UIDs).



In Internet of Things (IoT), a "***thing***" can refer to various entities, such as a person wearing a smartwatch, livestock fitted with RFID transponders, or vehicles such as cars, trucks or motorbikes with tracking devices.



Any object, whether natural or man-made, can be assigned an Internet Protocol (IP) address and possess the capability to transmit data over a network.



This interconnectedness enables seamless communication and data exchange, enhancing monitoring, control, and functionality across a wide range of applications.

Vodafone IOT

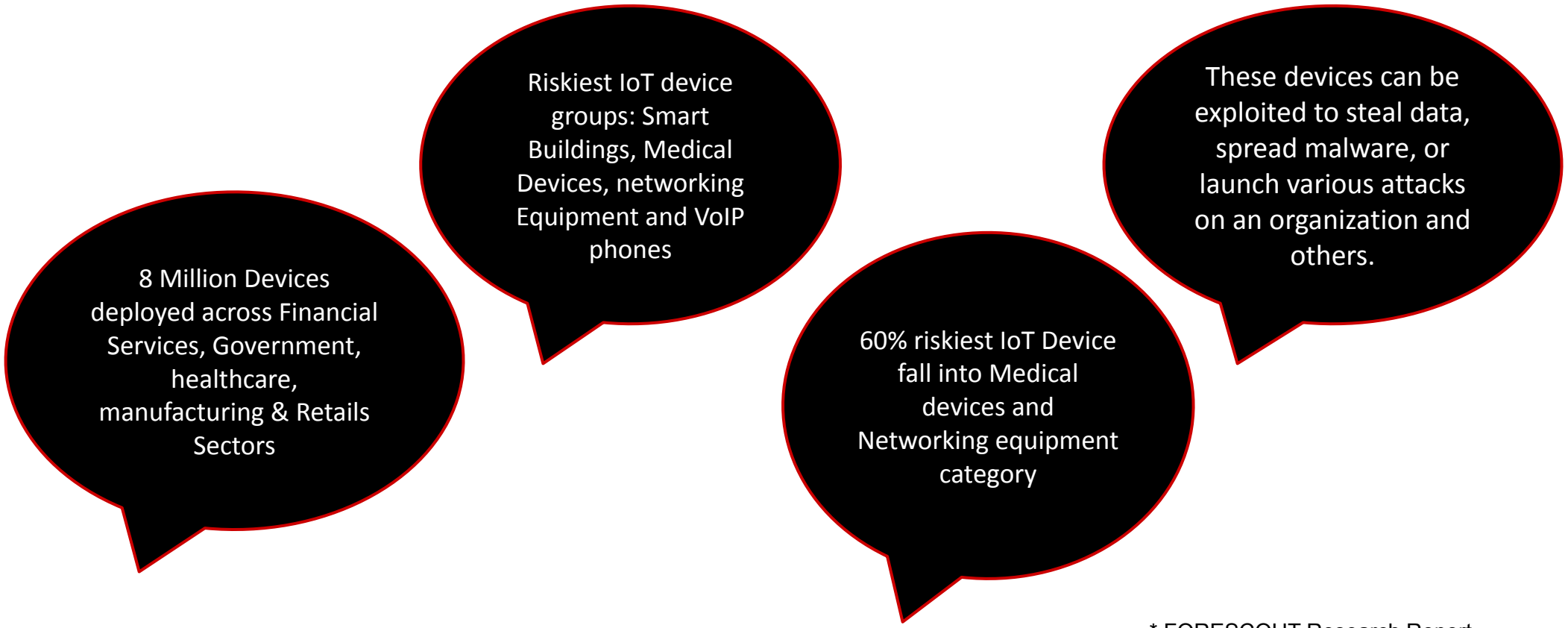
- IoT Connectivity : 175 Million
- Monthly Data Usage (IOT Sims) : 5.0Million GB
- Biggest Live Customer : 15 Million Sims



vodafone

Risk of IoT

Key Findings based on the Enterprise of Things Security Report*



* FORESCOUT Research Report

IoT Security Attacks

- Limited Compute & Hardware
- Weak/Hardcoded passwords
- Insecure Networks
- Insecure Ecosystem Interfaces
- Insecure Update Mechanisms
- Insecure or Outdated Components
- Insure Data Transfer and Storage
- Improper Device Management
- Vulnerable Components
- Lack of Physical hardening
- Open-Source Code Vulnerabilities
- Unencrypted Data

Introspection



Identity Management – IOT



Role of Customer Identity & Access Management (CIAM) on the Internet of Things

User Experience



SINGLE
SIGN-ON



PERSONALIZED
EXPERIENCE

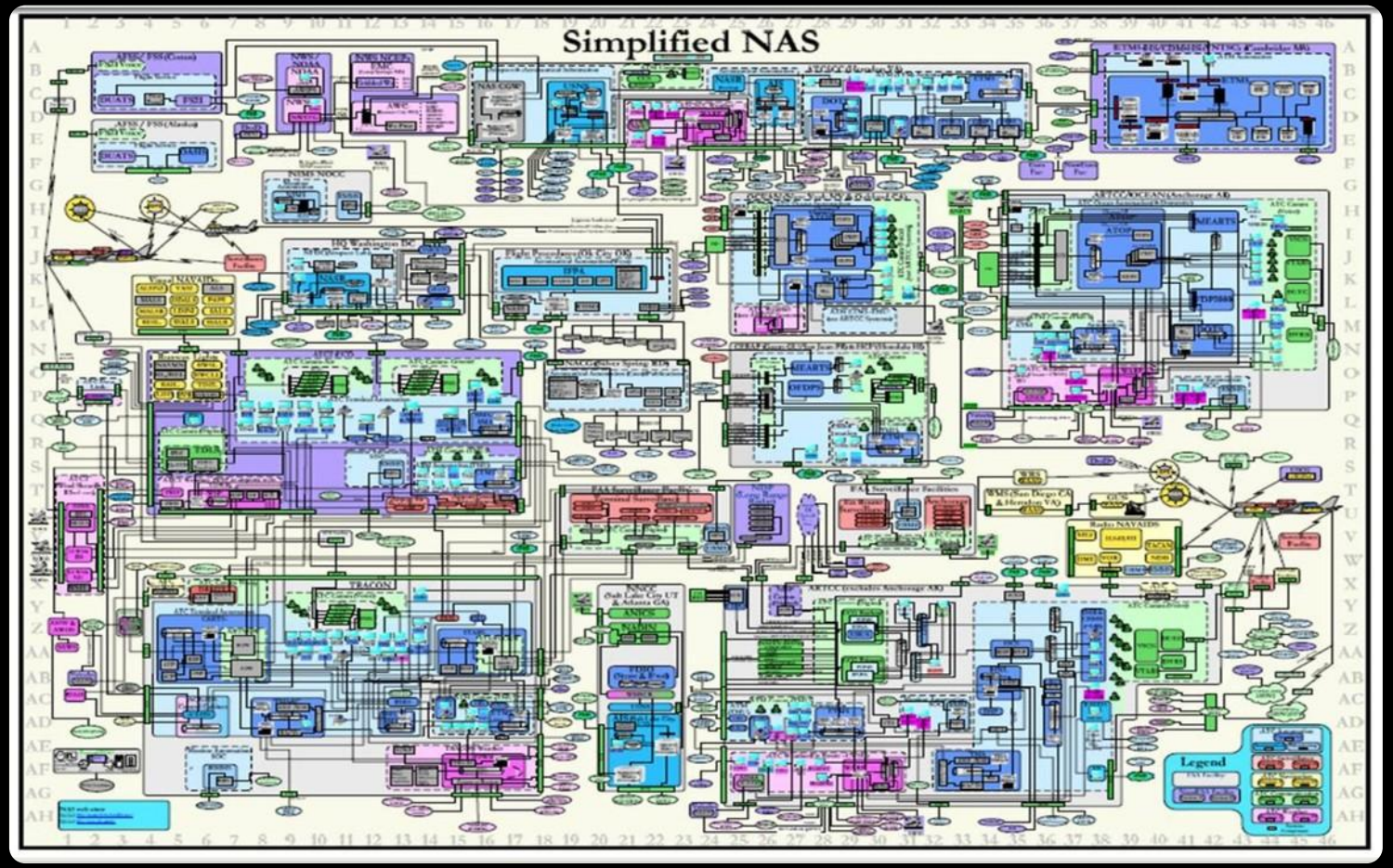


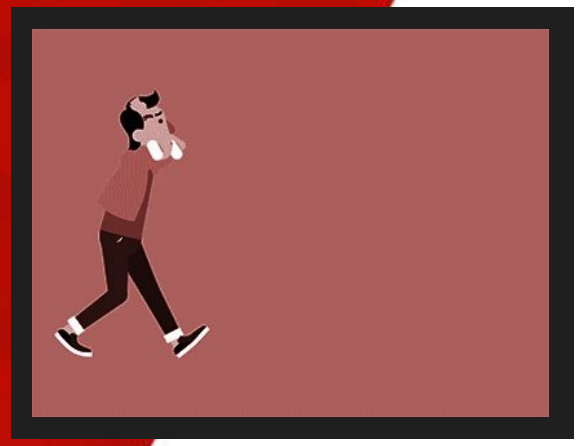
PRIVACY
MANAGEMENT

Security

- Authentication & Authorization
- Mutli-Factor Authentication
- Risk-Based Authentication
- Device identity Management

Legacy System





Challenges

- 10+ years old Platform
- Continuous Addition of new features
- Local Authentication by each component
- Different Solution with different Authentication
- Individual & Independent Authorization Models
- No Federation
- No Single Sign-ON



Strategy

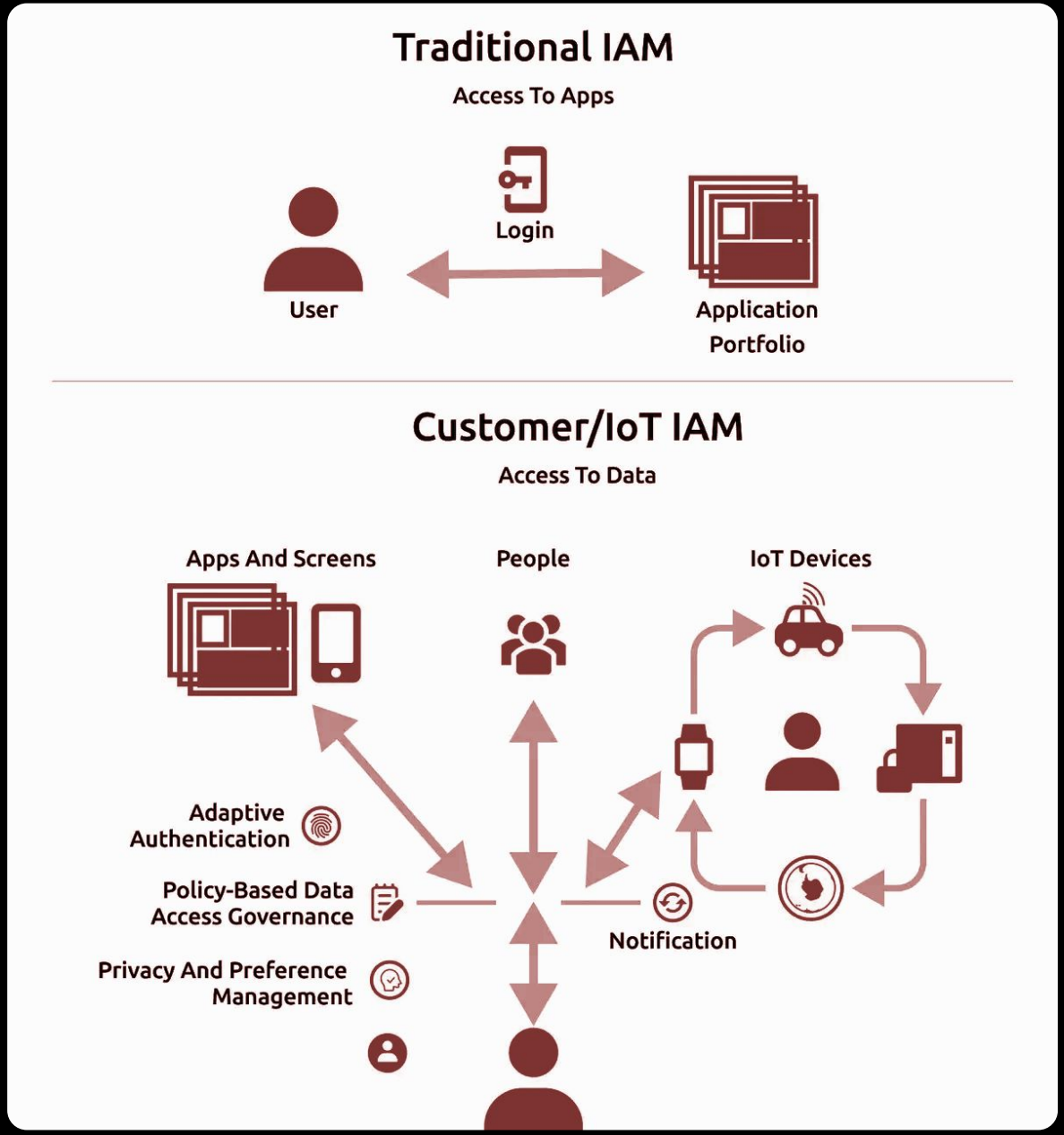
- Identify an Identity Service provider!!
  - To enforce User identity and Authorization end-to-end across all channels
  - All the different Components to use IDM as master for user identity/preferences/permission
  - To Introduce a centralized Authentication and Authorization solution where all the User identity and their associated roles/functions/permissions are centrally managed within IDM.
  - Simplifies SSO and federation against the service providers
- Created a Roadmap of 3 years
  - Well Achieved

Solution

Created a Centralized IAM by refactoring of the existing IoT Platform to centralize Identity and Access Management

- Identity and Access Management Architectural Framework.
- Authentication to support protocols like SAML, OAuth2, OIDC.
- Multi Factor Authentication (Adaptive Authentication).
- Identity Federation
- Single Sign ON
- Centralized Authorization Model
- Geo-Redundant IAM Solution
- 3rd party Federation with Consumer Like (OEM Car Manufacturers)
- Different Application Integrated

IoT Device Security



Benefits/Success Factors



Improved Security



OEM Car Manufacturers



Reduced Compliance Risk

Journey Ahead

- Align with Cloud-Native Architecture and Ecosystem
- OEM Integrations – Federation with IDPs
- Risk based authentication using AI/ML

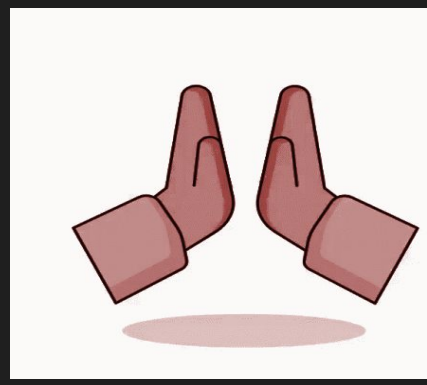
IAM Philosophy

It's not the destination, it's the journey

Ralph Waldo Emerson

IAM is not a destination, it is a journey

Anonymous



THANK YOU