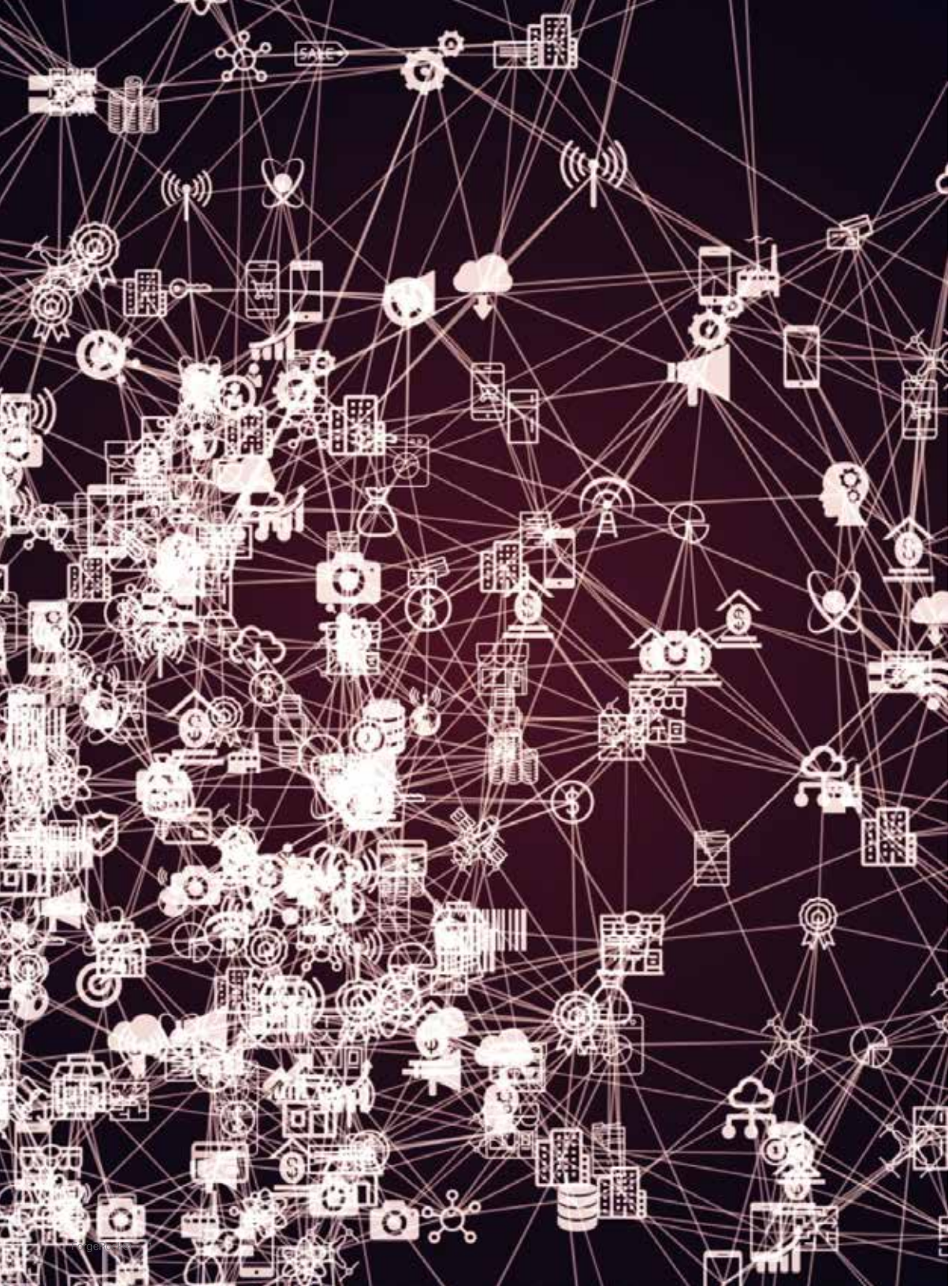


Your Guide to the Identity of Things

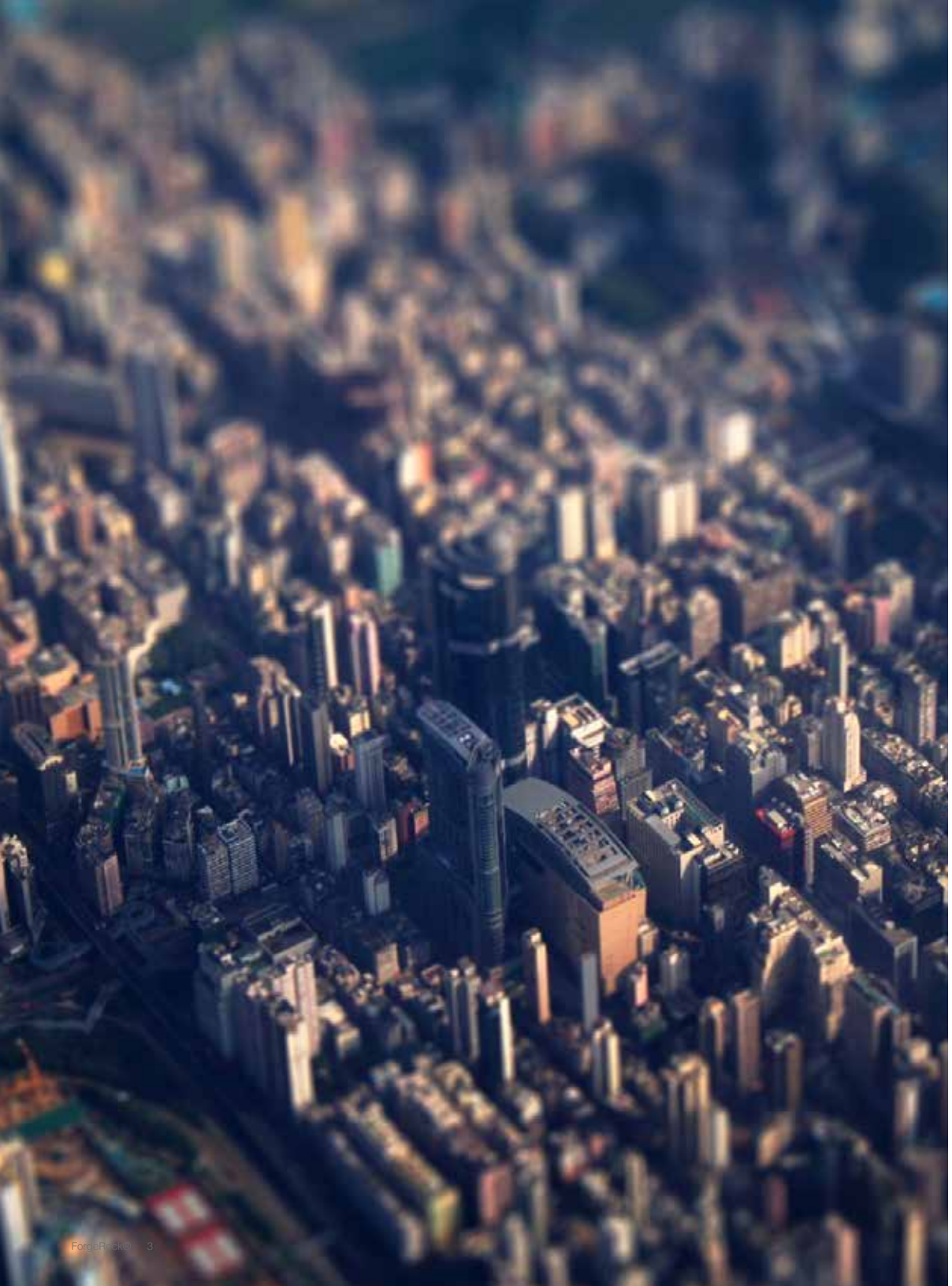
The Top 12 Considerations for an IoT Ready Identity and Access Management Platform

FORGEROCK

Is Your IAM Platform IoT Ready?

Organizations that introduce millions of new devices and billions of new relationships into their digital ecosystems must select an Identity & Access Management (IAM) solution that can handle the massive scale, complexity, and challenges of the Internet of Things (IoT). Here are the requirements and features you should keep in mind when evaluating an IoT ready IAM system.

- ☐ IoT Scale
- ☐ High Performance
- ☐ Flexible Architecture
- ☐ Standards Based
- ☐ Continuous, Contextual Security
- ☐ Easy Device Registration & Authorization
- ☐ Adaptive Authentication
- ☐ Identity Relationship Visualization
- ☐ Privacy and Consent Tools
- ☐ Single View of Customers via Devices
- ☐ API Protection
- ☐ Unified, Comprehensive Platform



1

IoT Scale

Organizations require an IAM system that can operate at massive scale. Legacy IAM platforms were not built to handle hundreds of millions of identities from a registration, login and ongoing session validation perspective. Modern platforms need to handle thousands of login or access validation actions per second, often based on stateless token architectures.

By 2020, the IoT will be made up of more than 20 billion connected "things", contributing to a global economic impact of $2 trillion

SOURCE: GARTNER RESEARCH

2

High Performance

An IoT ready platform should support:

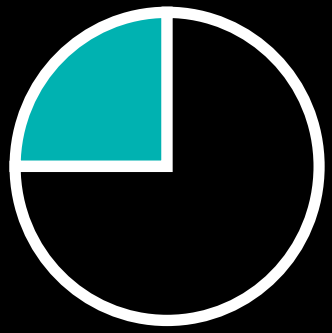
- Upwards of 15,000 transactions per second for login and token validations to ensure uninterrupted access to resources
- Out of the box high availability deploymentswith N-way multi-master replication, including data centers with geographic separation formanaging failover and disaster recovery
- Rapid instantiation of new node instances to manage load bursts
- Seamless tear down of existing nodes due to load reduction
- The ability to make modern web services multi-node and multi-site to ensure 24x7x365 availability across multiple geolocations
- Redundancy across all services, agents, APIs, instances, in all locations
- Session failover and verification by any node to provide optimal load balancing and token validation

24 / 7 / 365

3

Flexible Architecture

A common REST API framework across all services in the device lifecycle provides the flexibility to build a range of mashup services and applications on any platform or language. The device lifecycle will include everything from device creation, update and deletion, right through to device authentication and authorization. A common programmatic way is needed to interact with those services, accelerate integration time and reduce the cost of learning new technology. Most importantly, it makes it simple to connect the platform to any digital thing, from mobile devices and cars to set-top boxes and machines across a range of languages and platforms.



25%+

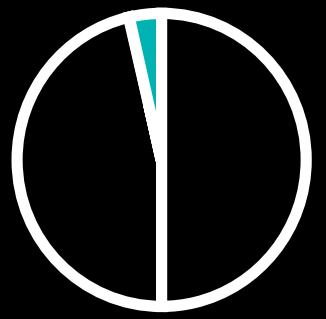
“

By 2020, more than 25 percent of identified attacks in enterprises will involve IoT, although IoT will account for less than 10 percent of IT security budgets

Gartner Research

”

>10%

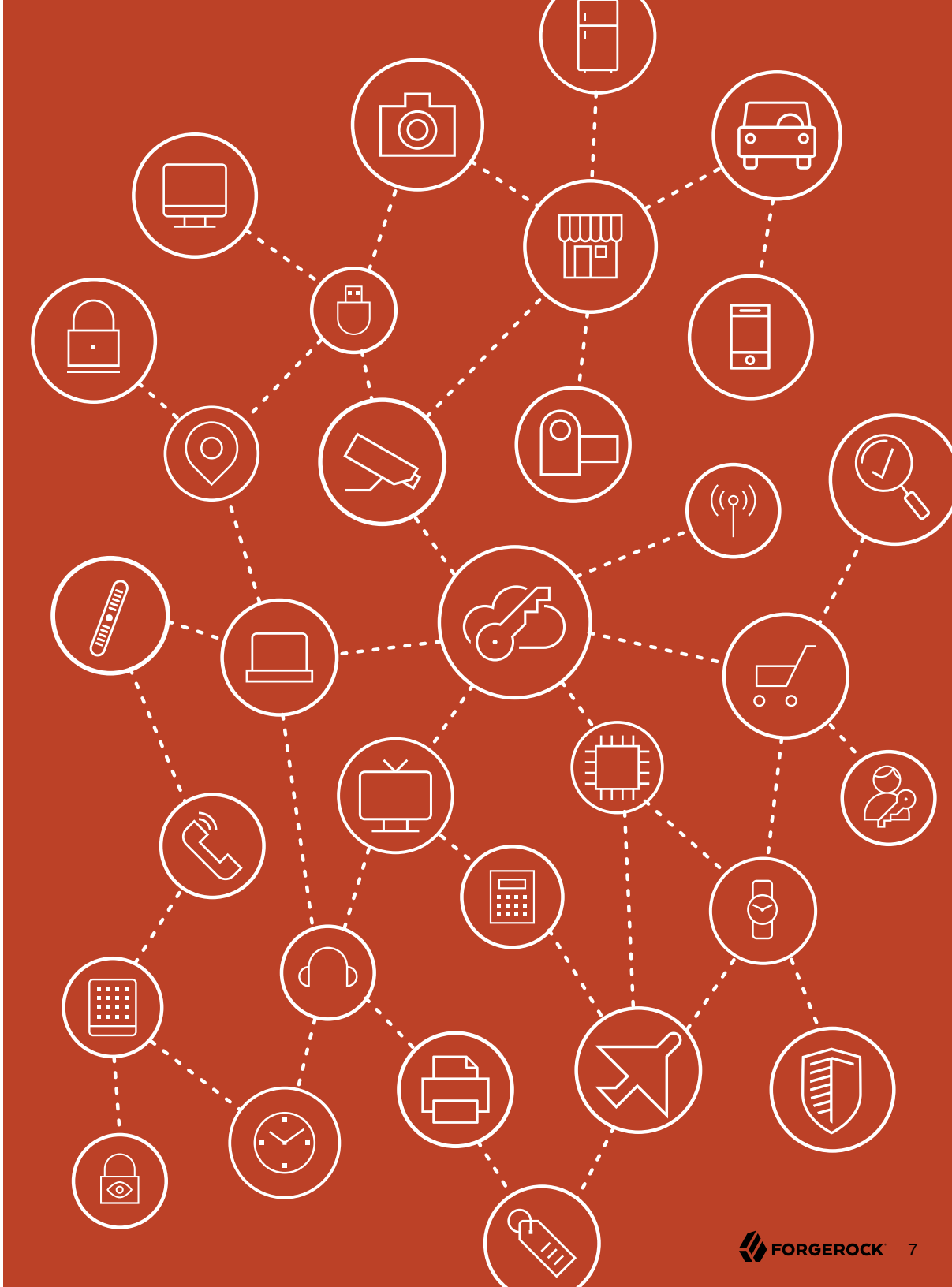


4

Standards Based

Open standards provide a safety net for deployers, as they provide an independently designed, non-proprietary and well documented way to integrate applications and devices. Identity and access management services, like encryption, should not be homegrown, due to the complexity and skills required to make them stable and secure. There are many identity and access related standards that should be supported in any IoT identity platform including:

- OAuth2,
- OpenID Connect
- JWT
- JOSE
- User Managed Access



5

Continuous, Contextual Security

Connected devices represent a new opportunity, not only for digital businesses, but for hackers and malicious actors as well. From DDoS botnets to compromised blood pumps and connected cars, IoT devices can be used to cause great harm. Context based security for users and devices will be critical in securing IoT. Using contextual cues like geographic location,IP address, time of day, and device profile, organizations can generate a real-time risk score and prompt an appropriate level of authentication be that email, security question, or biometric.

Most IAM solutions only protect at initial authentication. Greater security is required for IoT. Apply contextual identity, adaptive risk, and multi-factor authentication at the time of authentication as well as at any point during a digital session for increased security. The continuous security approach ensures authenticity of users, devices, things, and services at all times and can mitigate risk whenever an anomaly is detected, even during existing sessions. Features like single sign-on, social login, device to device passwordless login, and biometrics can all help organization to deliver a frictionless user experience (especially in customer-facing use cases).

6

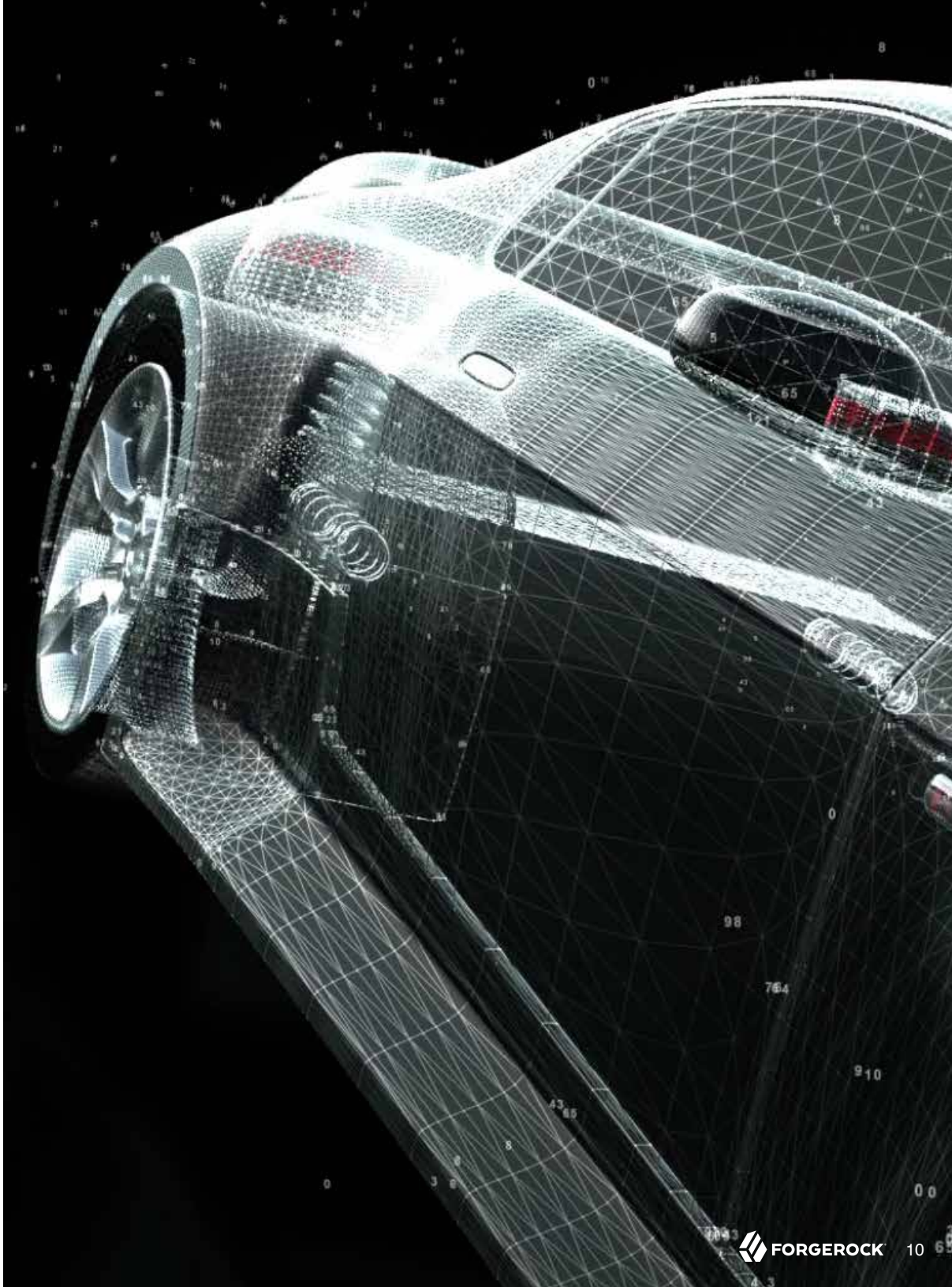
Easy Device Registration and Authorization

Introducing millions of connected devices requires repeatable, standards based processes for registering, provisioning, pairing, maintaining, and de-provisioning devices. IoT device lifecycle management should be easy, automated, and scalable. A simple approach to device to identity registration and pairing is to use standards like OAuth2. This allows for a device to gain the necessary permissions it needs to represent the user to internal and 3rd party APIs and cloud services. Simple revocation, by invalidating the assigned OAuth2 access and refresh tokens provides a simple “kill-switch” style approach to removing access if the device is sold, stolen or lost.

7

Adaptive Authentication

When managing millions of diverse IoT devices that vary in sophistication, connectivity, and power requirements, there must be authentication methods that can support them. Requirements differ from basic sensors to smart refrigerators and smart cars. An IAM solution for IoT should be flexible to support adaptive authentication for different devices in different scenarios and varying levels of complexity and security requirements.



8

Identity Relationship Visualization

With billions of relationships being made between connected devices and users, IAM platforms for IoT need to provide administrators with a simple way to manage connections and data at scale. Identity relationship visualization is a way to quickly notice anomalies, eliminate potential issues, and provide updates to identities.

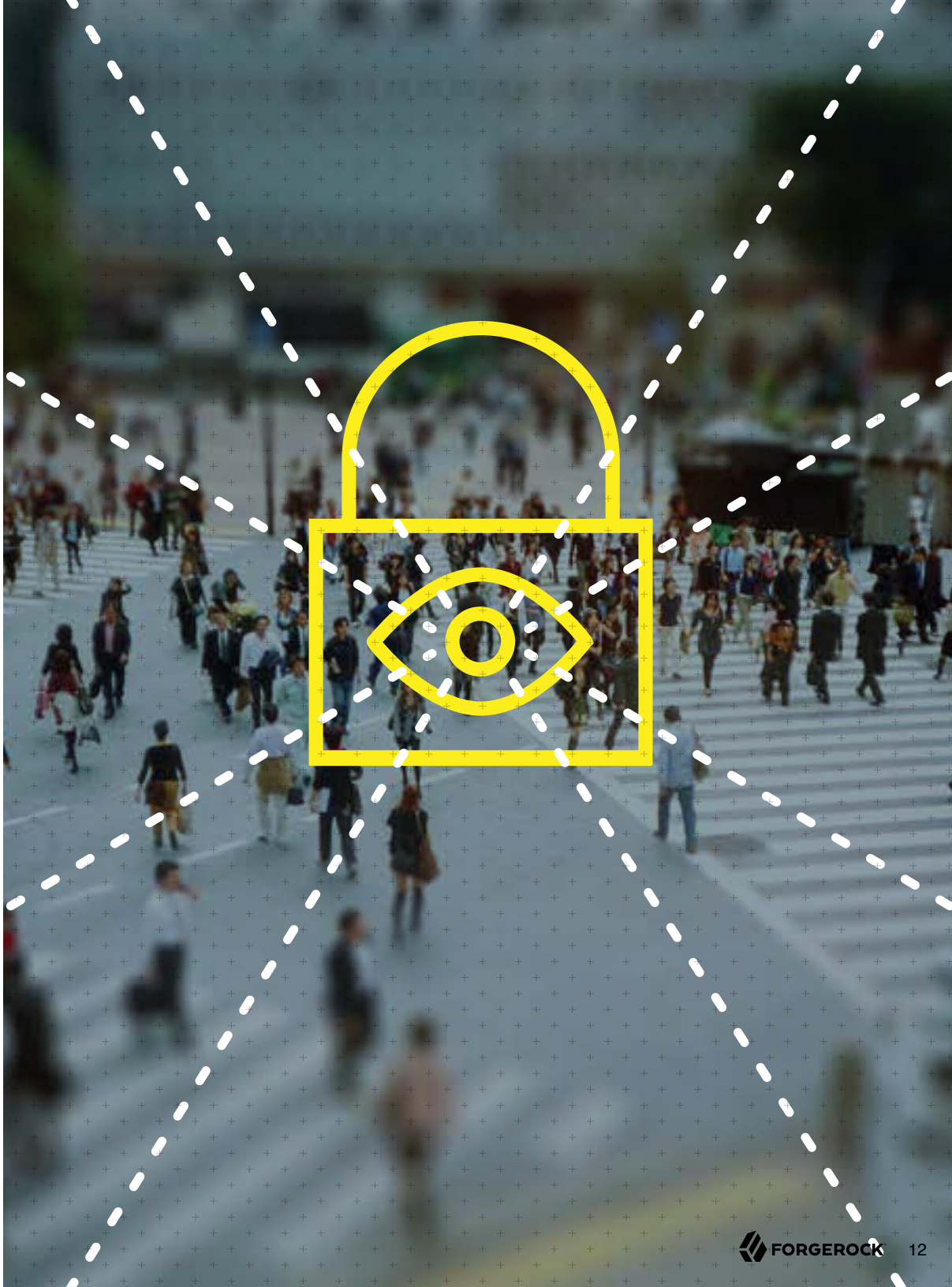
9

Privacy and Consent Tools

IoT devices gather massive amounts of data. Customers as well as regulators are concerned about how this data is shared and used. In order to build trusted relationships with users and enable the sharing of valuable customer information (user history, preferences, etc) that is key to delivering personalized experiences, privacy must be prioritized. To address privacy concerns that could slow adoption of IoT, an IAM platform should give customers the ability to manage privacy preferences and consent to data sharing. Privacy tools like User-Managed Access (UMA) give users control over what devices, cloud services, and users can access their data, for how long, and under what conditions.

Only 9% of IT professionals believe that current data privacy tools will be able to adapt to the needs of the emerging digital economy

Source: ForgeRock Privacy Survey



10

Single View of Customers via Devices

IAM for IoT should enable organizations to unify user identities, devices, and data in order to deliver consistent, personalized customer experiences on every channel to increase loyalty and revenue.

11

API Protection

APIs are the cornerstone for connecting users, devices, and things to applications and services. APIs enable smart devices to communicate with other devices and leverage a variety of complementary applications. As IoT is a complex mashup of users, devices, things, services, and applications, all with varied relationships, it will require a high level of security and scalability for these APIs. Identity-enable applications and services for seamless engagement across any user, device, or thing.

UNIFIED PLATFORM

DISPARATE PRODUCTS

12

Unified, Comprehensive Platform

Identity for IoT should not be an afterthought, purchased to supplement existing employee or customer identity systems. Organizations require an IAM solution that is purpose built for IoT, capable of defining and managing the identities of people, devices, and things.

By the end of 2020, 40% of IAM vendors will require complete redesigns of their IAM solution to work with the Internet of Things (IoT), up from 5% today.

Source: Gartner Research

About ForgeRock

ForgeRock® is the digital identity management company transforming the way organizations interact securely with customers, employees, devices, and things. Organizations adopt the ForgeRock Identity Platform™ as their digital identity system of record to monetize customer relationships, address stringent regulations for privacy and consent (GDPR, HIPAA, FCC privacy, etc.), and leverage the internet of things. ForgeRock serves hundreds of brands, including Morningstar, Vodafone, GEICO, Toyota, TomTom, and Pearson, as well as governments like Norway, Canada, and Belgium, securing billions of identities worldwide. ForgeRock has offices across Europe, the USA, and Asia.

For more information and free downloads visit http://www.forgerock.com.
Follow us on Twitter @ForgeRock