

Your Quickest and Safest Route to IoT Device Trust

How our managed service platform, KSaaS, can secure your IoT ecosystem without the burden of infrastructure or dedicated resources





Why is the industry moving to SaaS for IoT Security?



Achieving Zero Trust in IoT requires a focused approach



Managing machine identities for IoT is complex



Simplify deployments & responsibilities



Op-ex model scales with your business



Less infrastructure means less overhead



Consistent and predictable performance



Considerations for a new Software Platform

- Do you have the operational and technical skills required?
- Can you gain a market advantage through “Buy” not “Build”?
- Do you have critical regulatory or compliance requirements that SaaS will help satisfy?
- Are you vulnerable to key skillsets and knowledge leaving the business?



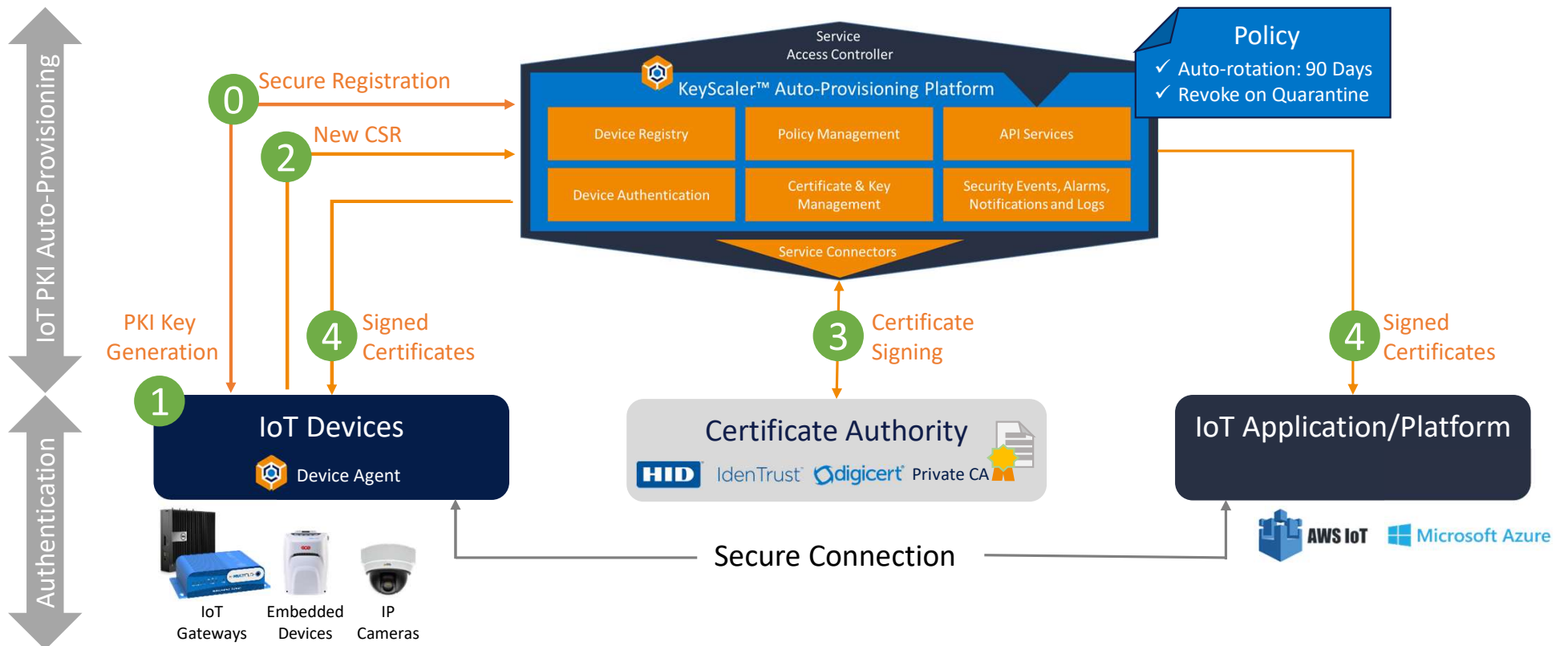
What is KeyScaler?

- KeyScaler is the first IAM platform that can manage and deliver identity and trust at the edge, securing device trust from day 1 to day done
- Fully automated and driven by group policy frameworks, KeyScaler integrates to your existing processes and services - delivering a real-time view of your asset landscape
- Able to scale from 10 to 10,000,000 devices and beyond

KeyScaler™ IoT PKI Automation in Action:



Device-bound, Policy-driven Key Provisioning & Rotation



Platform Delivery



ON-PREMISE / VPC



- **Download and Install the full KeyScaler technology stack**
- **Configure server-side software packages**
- **Deploy into own data center or Private Cloud**

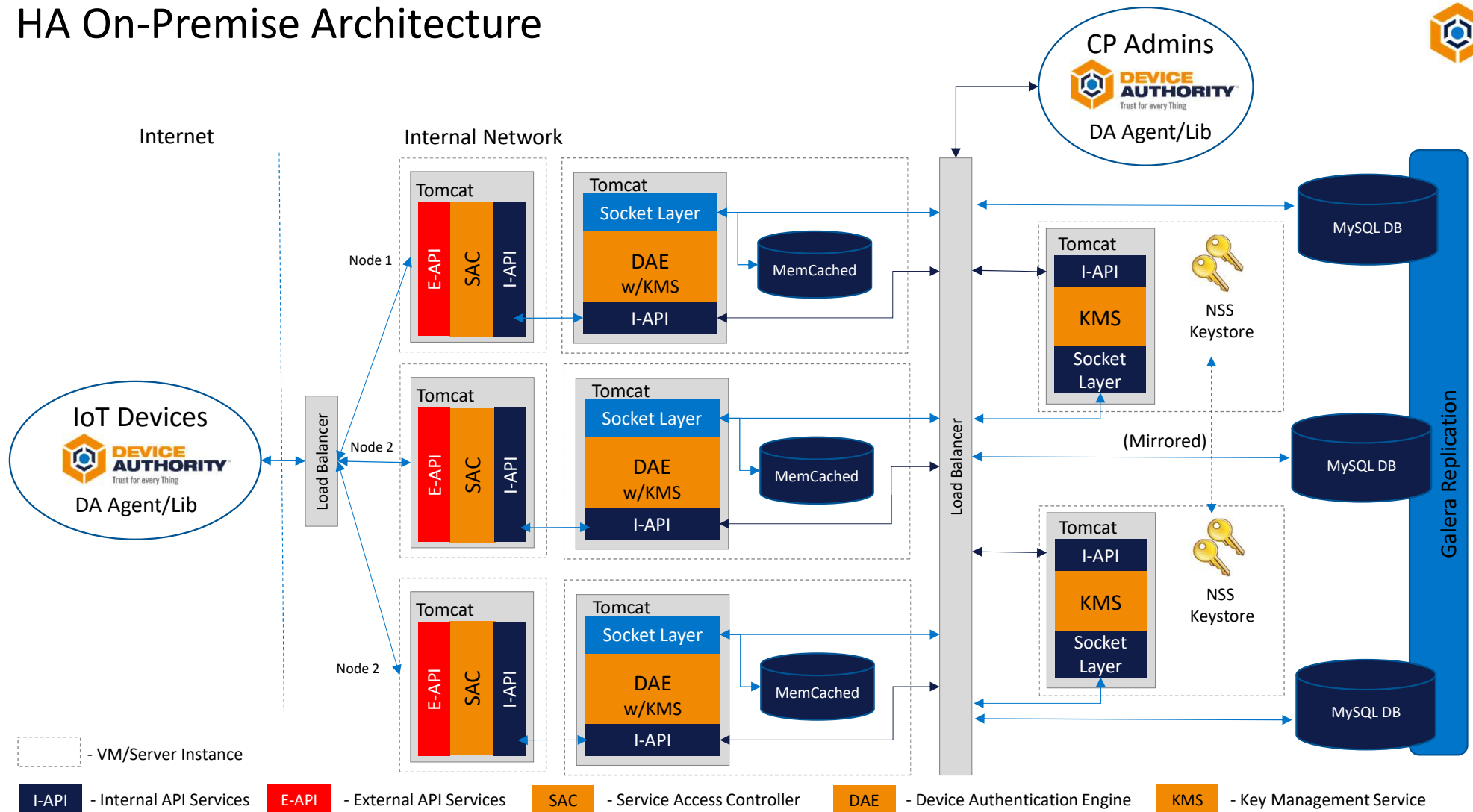
OR

MANAGED SERVICE



- **Subscribe to hosted KeyScaler service**
- **No infrastructure deployment or running costs**

HA On-Premise Architecture





On Premise Challenges



People



Deployment and maintenance



Infrastructure



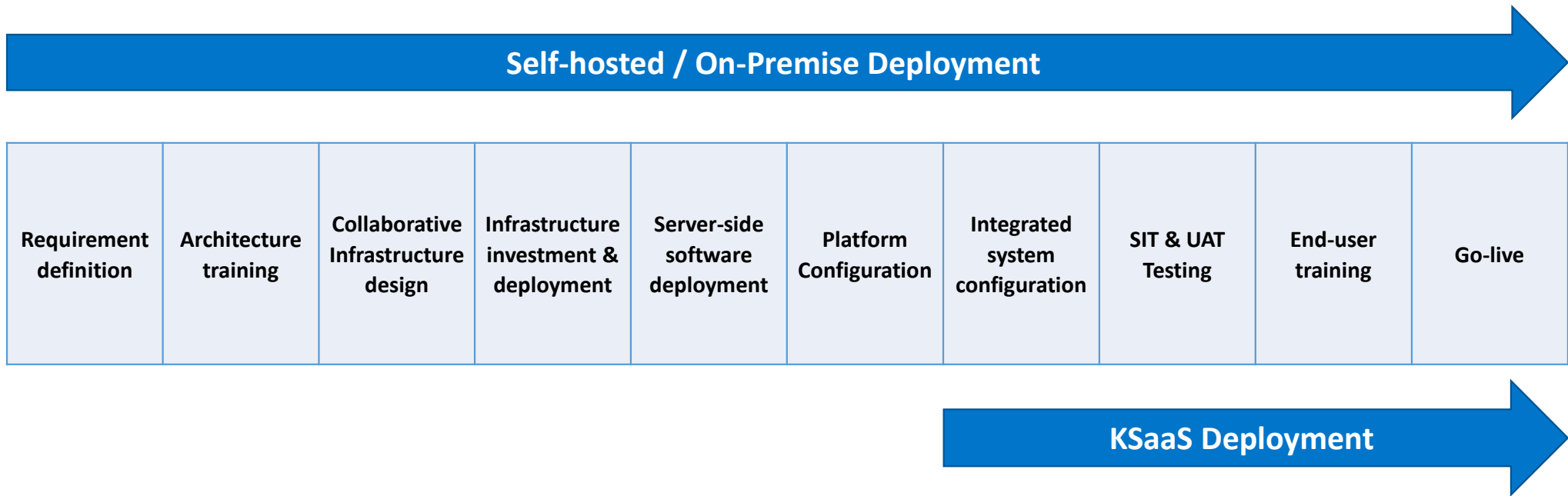
Training



KeyScaler as a Service

- Fully managed, hosted solution
- Secure multi-tenant architecture
- Infinitely Scalable
- Transparent managed updates
- Industry standard approach

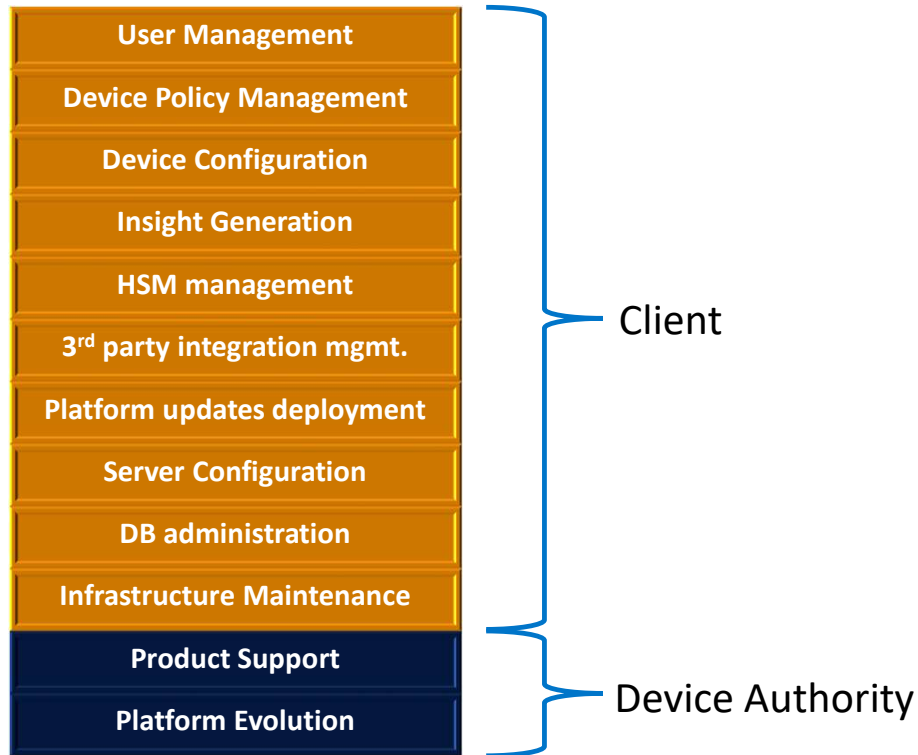
Deployment path Comparison



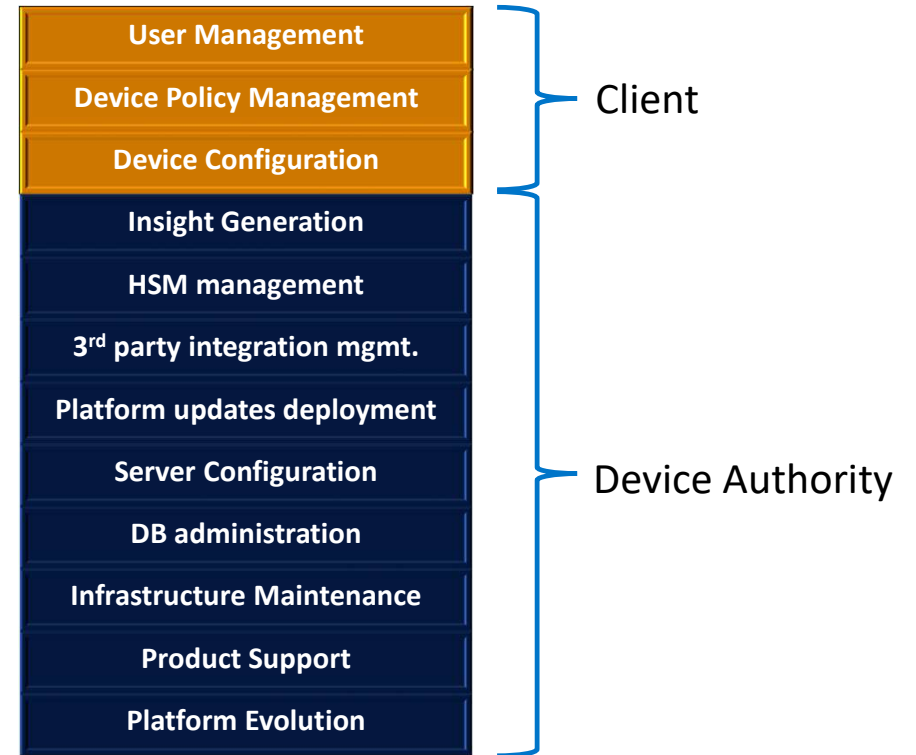


In-life Roles & Responsibilities

On-Premise / Private Cloud



KeyScaler-as-a-Service



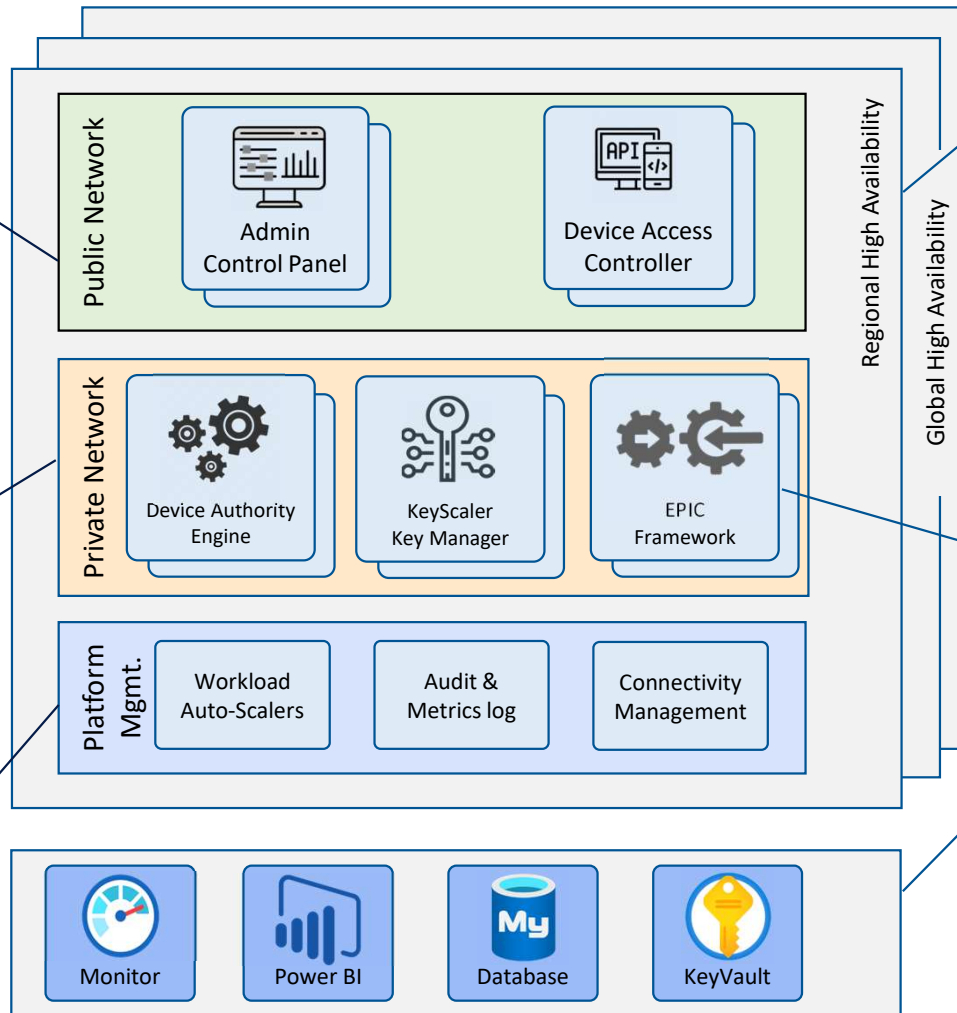
KSaaS Global Architecture



Highly Available Public Access Points
 The Control Panel and Device API both auto-scale to ensure consistent and reliable performance. IP Whitelisting is available, if desired.

Private Internal Network
 The core KeyScaler components reside in a secure private network, and auto-scale to ensure consistent and reliable performance. All internal network traffic is cryptographically bound to a private tenant, making inter-tenant contamination impossible.

Platform Management
 The KeyScaler components are constantly monitored, and deploy more horsepower, where it's needed, within seconds. All running components report to a centralized Audit Log, to know exactly when and where a device has been connected.



Global, or Regional Deployment
 Azure Global traffic management directs network traffic to the closest, or most performant KeyScaler cluster around the globe. KSaaS Tenants can be configured to geofence data to a single region, if desired, while still retaining high availability and redundancy.

Highly Flexible Integration Framework
 The KeyScaler EPIC (Enhanced Platform Integration Connector) framework allows the secure integration of almost any 3rd party platform. From HSMs to Analytics Dashboards, EPIC provides a simple means to integrate with any stage of the KeyScaler workflow.

Highly Available Managed IaaS
 Using Managed IaaS services allows us to capitalize on the High Availability and Robustness of the Azure Platform, whilst maintaining the highest level of security and privacy. All managed Services are isolated and have no external connections. Private Endpoints within the KeyScaler Cluster facilitate secure internal communication.

KSaaS Benefits



Time to Production



Scale with your Business



People and Skillsets



Robust and Reliable



Preview: The Value of Scale

- Aggregated anonymised device data
 - Industry benchmark reports
- Device misbehaviour analysis
 - Semi-supervised AI to recommend the next best action
 - ML techniques to automate misbehaviour prevention
 - Predictive analysis notifications



Try it today – at www.deviceauthority.com

The screenshot shows the Device Authority website landing page. At the top left is the Device Authority logo. The navigation menu includes links for About Us, Platform, Solutions, Industries, Partners, Resources, and Contact Us. On the right side of the navigation bar are two buttons: "Free Trial" (blue) and "Book a Demo" (orange). The main content area features a large 3D padlock icon in the center, surrounded by various IoT-related icons like a smartphone, a camera, and a sensor. To the left of the padlock, the text reads: "Protect your reputation and revenue from malicious IoT attacks" followed by "Protecting connected things, applications, and data against security threats with Edge to Enterprise IoT security solutions." Below this text is a form with a grey input field labeled "Enter email address" and an orange "Book a Demo" button.



Thank you

Ben Benson

VP. Technical Operations

Ben.Benson@deviceauthority.com