DEVICE AUTHORITY

January 2026

Tern Investor Presentation

Discovery, Automation, Compliance

Darron Antill, CEO

About Device Authority

Device Authority's KeyScaler platform automates the full identity lifecycle of unmanaged IoT/OT devices from discovery and machine identity management, to AI-based risk assessment and compliance readiness.

Background

Device Authority is a UK Limited Company

- Team 25 Employees
- Raised $7m 2023 led by 1011 Ventures
- Launched KeyScaler 2018, 11 Patents
- KSaaS launched October 2022

Team

Locations:

- Reading, UK
- Boston, US
- Bangalore, India

Details

- Rich Ecosystem of Strategic Partners
- Recognized by independent analysts as a leader in IoT device security and data encryption
- Proven success with top global companies in Automotive, Medical, & Industrial IoT sectors

KSaaS KeyScaler as a Service

KeyScaler AI™

KeyScaler Central™

KeyScaler Edge™

Investors

TENELEVEN

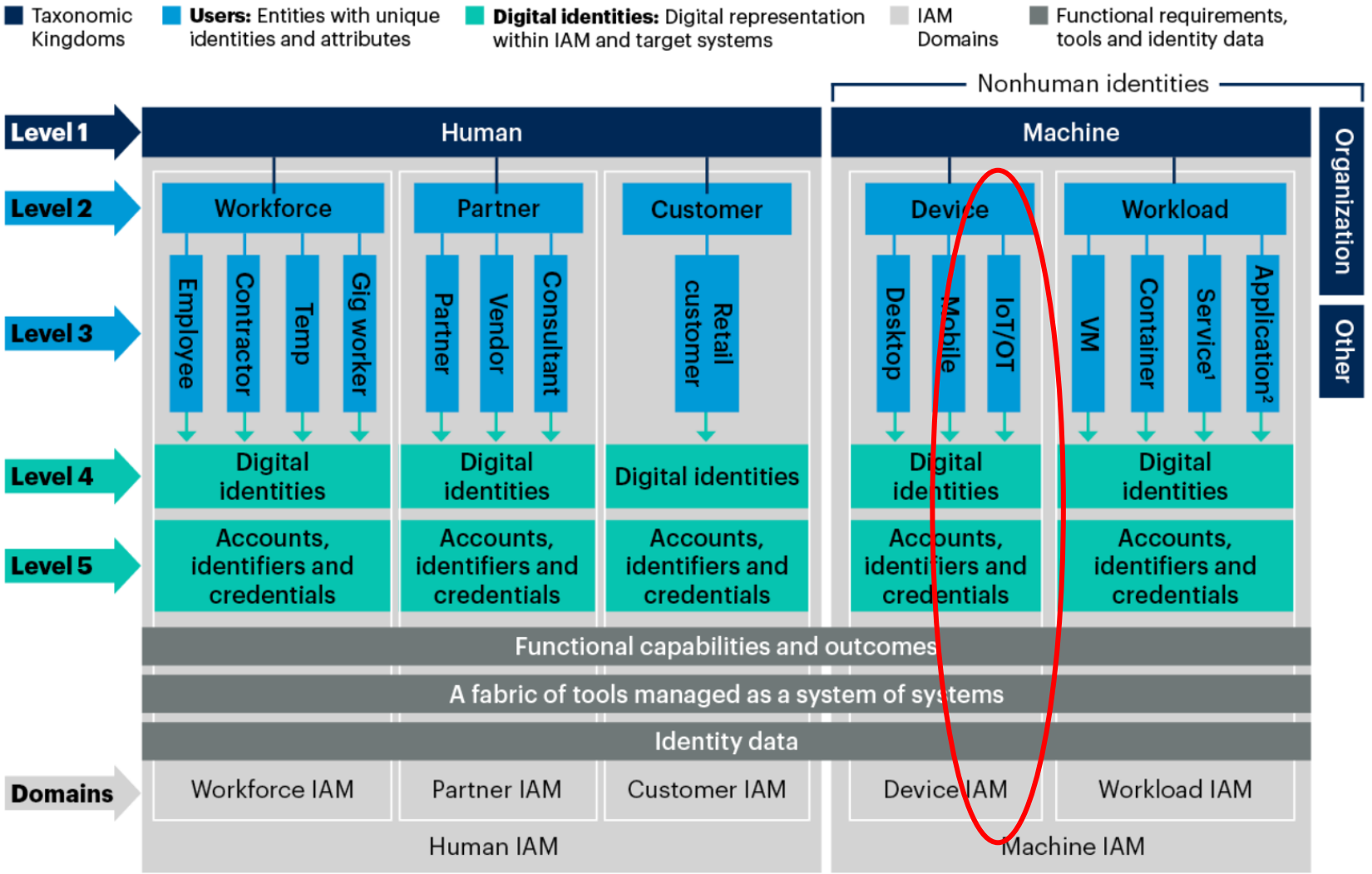
tern

ALSOP LOUIE PARTNERS

CYBERARK

VICTOR CHARLIE PARTNERS

The IAM Taxonomy



[1] = web, REST, API, RPC, webhook
[2] = web, native, script, service, RPA, AI agent

Source: Gartner

Note: IAM = identity and access management; IoT = Internet of Things; OT = operational technology; VM = virtual machine; RPC = remote procedure call; RPA = robotic process automation

832903_C

Device Authority KeyScaler at a Glance

30+ Million
SaaS Device Transactions

60+ Million
Keys Provisioned

30+
Integrations

59
Connected Countries

<10 seconds
To Securely Register & Get Cert

$1.5M
2025 ARR

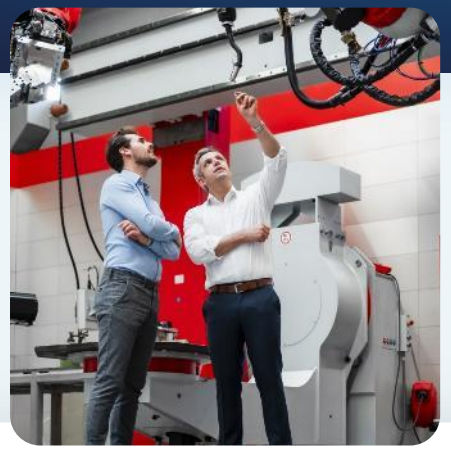
138%
Net Retention Rate (‘23-’25 average)

278%
Customer ROI Case Study

Slide Data is unaudited.

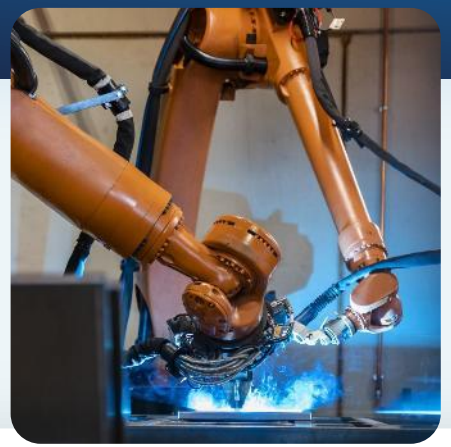
A Strategic Shift in Medical, Automotive and Industrial Manufacturing: Identities are the New Perimeter.

Compliance Risk



60% of companies report compliance issues tied to machine identities (e.g., certificates, keys) and 59% say auditing machine identities is harder than auditing human identities.

Cyber-attack Exposure



50% of organisations reported a security incident or breach linked to compromised machine identities in the past year, & 43% suffered unauthorized access to sensitive systems/data via machine-identity compromises. The average cost of a healthcare data breach is $10.9m

AI & Machine Identity Growth

81% of security leaders believe securing machine identities is vital to protecting the future of AI & 72% have experienced a certificate-related outage, underscoring the link between machine identities and AI /automation risk.

Need For Automation

66% of surveyed security professionals say machine-identity management requires more manual processes than managing human identities — pointing to a costly automation gap.

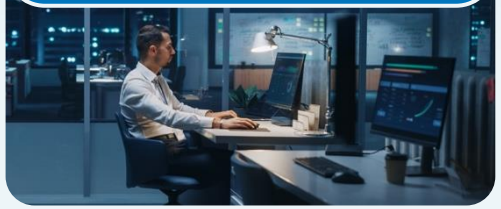
Sources : CyberArk, Sailpoint and H-ISAC, 2025

DEVICE AUTHORITY

Today's security leaders have to manage a full spectrum of identities to meet Zero Trust standards:

Contractors | Employees | Application Admins | Traditional IT | 3rd Parties | Cloud Ops | DevSecOps | Engineering Teams | Data Scientists | Bots | Workloads | Apps | APIs | IoT/OT

Target Resources

Workforce	IT	Developers	Machines
			
Endpoints, Data, Biz Apps	Data, Apps, Workloads, CI/CD Tools	Data, Apps, Workloads, Code Repos, Cloud Services	Devices, Data, Apps, Workloads, Code

Access to Data

Access and ability to change data and infrastructure

Access and ability to change data, infrastructure, and code

Risk of Access Level

Complexity of Access

Low

High

DEVICE AUTHORITY

Which Translate into 3 Broad Management Strategies:

Human Identities
augmented by Multi-Factor Auth

Machine Identities
using keys and certificates

IoT/OT Device Identities
requiring Zero-Touch Automation

Complexity of Access X Volume of Identities = **Potential for Human Error**

DEVICE AUTHORITY

Device Authority Value Proposition to Customers

The purpose-built solution for addressing the full identity lifecycle of OT/IoT Devices from discovery to compliance

Market Drivers

1. **Expanding Attack Surface:** Growth of IoT/OT fleets, legacy brownfield devices, and supply chain complexity increase cyber risk.
2. **Operational Burden:** Manual key and certificate management at scale is costly, error-prone, and unsustainable.
3. **Regulatory Pressure:** Compliance mandates like EU CRA, NIS2, AIS-189, and UN R155/156 demand provable device identity and auditability.

Device Authority Solution

1. **Active Discovery:** Continuous detection and visibility of new and legacy devices with automated onboarding, provisioning, and policy enforcement.
2. **Automated Lifecycle Management:** End-to-end identity provisioning, renewal, and retirement across mixed IoT/OT environments including Edge.
3. **Compliance Intelligence:** AI-driven risk scoring mapped to regulatory frameworks, with continuous compliance visibility.

Customer Value

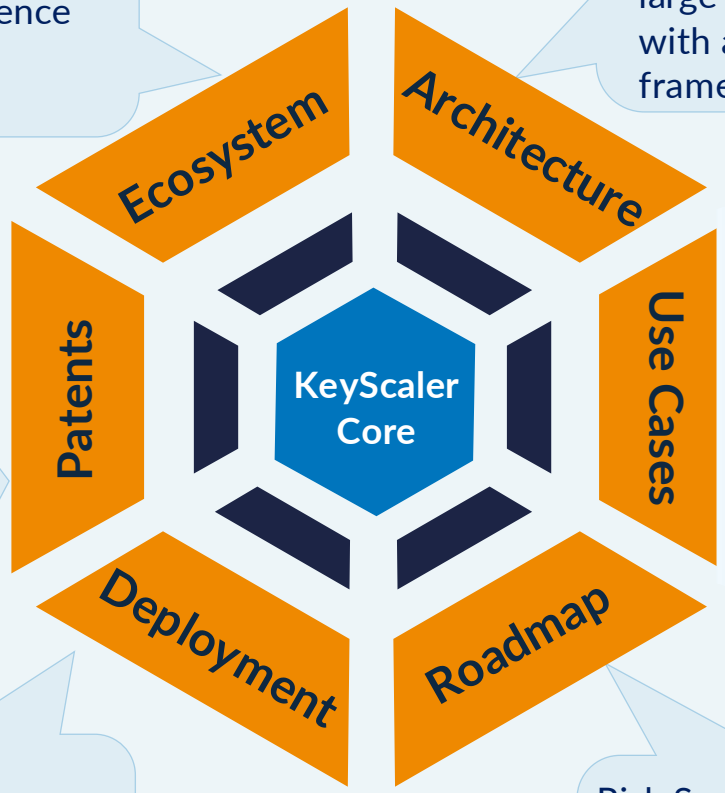
1. **Reduced Risk Exposure:** Stronger protection against cyberattacks and compromised devices through automated policy enforcement.
2. **Lower Operational Costs:** Automation eliminates manual effort and human error, reducing total cost of ownership.
3. **Proven Compliance Readiness:** Continuous, auditable assurance of regulatory alignment and crypto-agility according to evolving standards.

KeyScaler Platform Overview

Connectors with top IoT Platforms, CA's, HSM's, and Threat Intelligence Platforms

Flexible, multitenant cloud-native platform built to scale out with large device deployments with alignment to NIST framework

Patents with focus on systems and processes for securing IoT devices - DDKG



Private cloud, or infrastructure-free SaaS options for fast time to value - KSaaS

Risk Scoring & Compliance, Comprehensive Edge Management, Rich Data Visualization w/AI-driven Analytics, Discovery

- Key Management Service (KMS)
- Automated Lifecycle Management
- AI-Driven Risk Scoring & Compliance Readiness
- End to End Data Encryption
- Anomalous Device Behavior Detection
- Code Signing & OTA Updates
- PKI for IoT
- Brownfield Device Attestation w/DDKG
- Offline Device Policy Enforcement

Automotive	Energy
Medical Device Mfr.	Connected Agriculture
Industrial	Gov/Critical Infrastructure

DEVICE AUTHORITY

5 Ways KeyScaler Delivers Key Market Value

1. Device Authority's KeyScaler® platform **transforms OT/IoT device trust data into actionable intelligence.**

2. KeyScaler **turns manual and costly processes into 100% automation,** enabling organizations to manage millions of identities simultaneously, free up operational resources, and minimize breaches due to human error.

3. KeyScaler uses **active discovery, automated identity lifecycle management, and AI-driven risk scoring** to assess IoT/OT device vulnerabilities and align with compliance standards like the EU CRA, NIS2, and UN R155/156.

4. KeyScaler gives each device a provable trusted identity, and gives enterprises the ability to **quantify risk, prioritize remediation, and demonstrate compliance readiness** in real time meeting Zero Trust standards.

5. KeyScaler enables **easy integration with major enterprise applications** to enable complete security of large scale, IoT/OT device deployments with accelerated deployment and reduced management burden.

KeyScaler as a Service (KSaaS): Cloud-Native Device Identity Automation and Full Lifecycle Management Across the Ecosystem

DEVICE AUTHORITY

01 Automated Registration

02 Device Authentication

03 Policy Management

04 Certificate & Key Management

05 APIs

06 Security Events, Alarms, Logs

07 Service Connectors

KSaaS®
KeyScaler as a Service

PAM for IoT/OT
CYBERARK
BeyondTrust

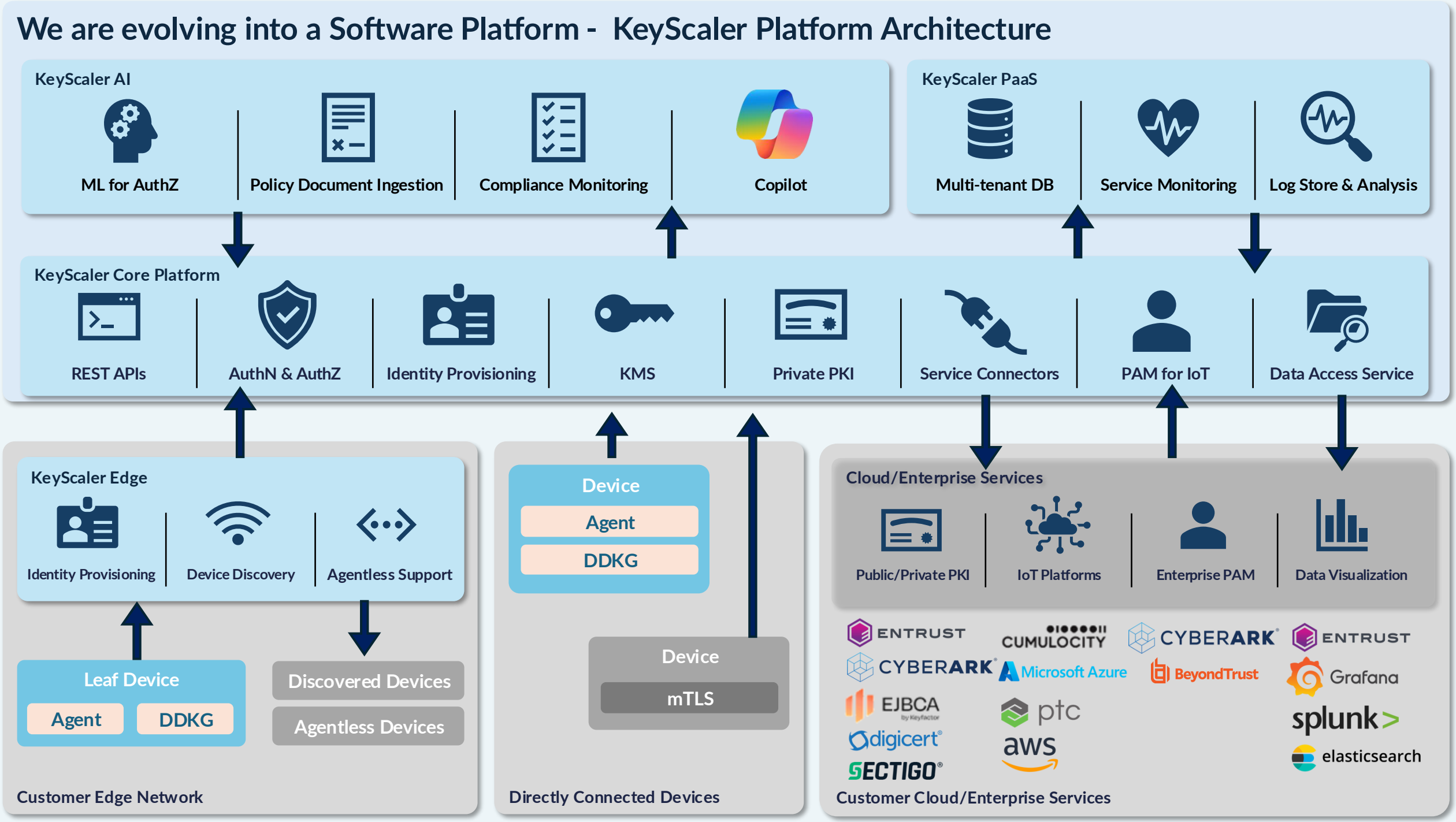
IoT/OT Devices

CA/Machine Identity Provider
CYBERARK
ENTRUST
EJBCA by Keyfactor
SECTIGO
digicert

Enterprise Apps
Microsoft Azure
aws
ptc
CUMULOCITY

Secure Connection

We are evolving into a Software Platform - KeyScaler Platform Architecture



KeyScaler® Compliance - transforms device trust into actionable intelligence—discovering devices, automating identity lifecycles, and applying AI-driven risk & compliance scoring to meet frameworks like EU CRA, NIS2, and UN R155/156.

Discovery → Automation → Compliance → Visualization

Device Discovery & Identity Lifecycle Management

Advanced Automation & AI

Trust Scoring & Compliance Readiness

Compliance Dashboard

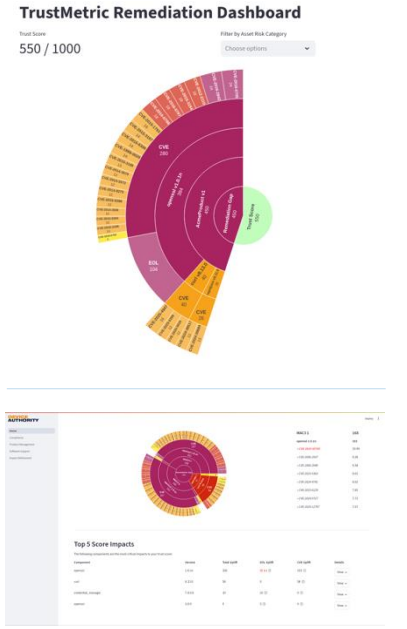
- Discovery
- Device Authentication
- Automated Onboarding
- Policy Management
- API Services
- Data Security
- Cert. & Key Management

KeyScaler Platform

- Device Authority Engine
- Key Management Service

KeyScaler AI

- Data Analysis & Agentic Enrichment
- Trust Scoring Engine



- Microsoft Azure
- Copilot
- Power BI
- Microsoft Sentinel
- ENTRUST
- splunk>

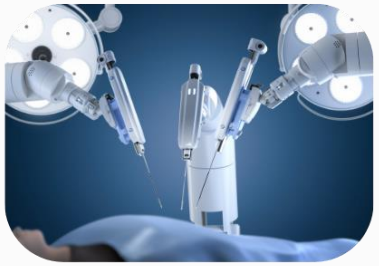
DEVICE AUTHORITY

Go To Market Strategy - Channels For Scale And Reach

Vertical Markets

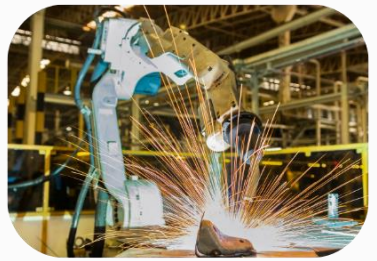
AUTOMOTIVE

MEDICAL



PUBLIC SECTOR

INDUSTRIAL MFR.



Partnerships & Channels

System Integrators/MSP's

Azure/AWS Marketplace

SI/MSP Partners

avanade

accenture

OPTIV

IoT Applications

Microsoft Azure

CUMULOCITY

amazon web services

ptc

Identity Partners

CYBERARK The Identity Security Company

ENTRUST

Microsoft Cosell

Microsoft

Market Drivers

AI Adoption

Compliance

Identity Lifecycle for OT/IoT

CYBER RESILIENCE ACT

FDA

THE WHITE HOUSE

UNECE WP.29

NIST 800-53

DEVICE AUTHORITY

Device Transaction Automation Calculator

What does it show?

The calculator represents the number of customer device transactions automated by KeyScaler (on-premise and KSaaS)

What kinds of transactions does it include?

- "Device Provisioned"
- "Successful device authentication"
- "Device Registration"
- "Device deprovisioned"
- "Device Removed"
- "License notification"
- "Device integrity tested"
- "Certificate Provisioned"
- "Certificate Revoked"
- "Successful device password rotation"
- "Invalid Key"
- "Authorization id added to device"
- "Device quarantined"
- "Device blacklisted"
- "Device state success"

How & When is it updated?

- The calculator is updated manually to allow us to gather the data from on-premise customers
- It is now being updated on a monthly basis

DEVICE AUTHORITY