DEVICE AUTHORITY

Discovery, Visibility & Risk Compliance

How KeyScaler Discovery strengthens IoT/OT security, visibility and compliance readiness

As enterprise IoT and OT environments continue to expand, organizations are struggling to maintain visibility over unmanaged devices, machine identities and hidden vulnerabilities. Device Authority's KeyScaler Discovery capability provides organizations with rapid visibility into connected assets, insecure services, open ports, certificate weaknesses and unmanaged endpoints across the network estate.

Combined with Device Authority's emerging Risk & Compliance functionality, organizations can move beyond simple discovery into continuous cyber resilience, policy alignment and compliance readiness.

Why Discovery Matters

Modern connected environments often contain unmanaged and undocumented devices that create operational and regulatory risk. Many organizations lack a complete inventory of IoT, OT and edge devices.

- Detect insecure or unauthorized endpoints
- Identify expired or weak TLS certificates
- Understand exposure to regulatory requirements
- Prioritize remediation activities
- Maintain Zero Trust architectures

KeyScaler Discovery Capabilities

KeyScaler Discovery enables organizations to identify and analyze unmanaged devices through an intuitive interface.

- IP addresses and MAC addresses
- Open ports and exposed services
- HTTP server visibility
- TLS certificate health and validity
- Devices lacking authentication or encryption
- Unknown or potentially vulnerable assets

Unlike passive scanning, which does not directly interrogate devices and can therefore miss critical information such as exposed services, certificate issues, software versions and dormant assets, KeyScaler Risk & Compliance uses active discovery techniques to build a much deeper understanding of connected-device risk and compliance posture.

KeyScaler Risk & Compliance can also ingest and enrich data from existing discovery and scanning tools, enabling organizations to leverage prior scans and generate detailed device intelligence, risk scoring and compliance insights without replacing existing security investments.

Connecting Discovery to Risk & Compliance

Discovery alone is not enough. Device Authority's Risk & Compliance capability extends visibility into actionable governance and cyber resilience workflows.

- Align IoT/OT environments with regulatory frameworks
- Monitor risk posture continuously
- Identify non-compliant devices and certificates
- Automate remediation and lifecycle management
- Support Zero Trust and audit readiness initiatives
-

Supporting Regulatory Readiness

Increasing regulatory pressure from frameworks such as CRA and NIS2 requires organizations to demonstrate stronger visibility and control.

- ·Understand where unmanaged devices exist
- ·Detect insecure configurations and outdated certificates
- ·Reduce human error through automation
- ·Improve audit and reporting readiness
- ·Strengthen cyber resilience across IoT and OT environments

From Visibility to Trust

Device Authority enables organizations to move from fragmented device visibility toward automated, identity-centric cyber resilience.

By combining KeyScaler Discovery with Risk & Compliance functionality, enterprises can gain the operational insight needed to secure unmanaged devices, improve compliance readiness and reduce exposure across modern connected environments.

Find out more about KeyScaler Risk & Compliance and Register Your Interest

DEVICE AUTHORITY
www.deviceauthority.com
contact@deviceauthority.com

UK Head Office
Level 2, Thames Tower
Station Road,
Reading,
RG1 1LX

Device Authority, Inc.
c/o Workbar
399 Boylston St fl. 6
Boston
MA 02116