NEW FOR 2025

Guide To IOT/OT Visibility and Control

The Importance of Machine Identity Automation for Device Security

DEVICE AUTHORITY™

Contents

Introduction

As the digital landscape continues to evolve at an unprecedented pace, the traditional security perimeter has all but vanished. Today, as organizations increasingly rely on diverse digital entities to operate efficiently and securely, identity —both human and non-human in various forms— has become the new frontier in cybersecurity. The explosive growth in machine identities, particularly machine identities tied to unmanaged devices in IoT and OT environments, has introduced new layers of complexity and risk. In this rapidly changing world where adversaries utilize AI to accelerate the speed and sophistication of attacks, safeguarding these identities has become paramount and is a core pillar of Zero Trust upon which other security solutions rely.

In this latest guide focused on the current and future trends in identity-based security for devices, we will explore how forward-thinking organizations can adapt to these emerging cybersecurity challenges and employ currently available solutions to protect their device estate.

STATE OF THE MARKET

a) Identity: The New Security Perimeter

With the rise of cloud computing, mobile devices, converged OT and IoT ecosystems, and remote workforces, the once-clear boundaries of the corporate network are fading. No longer confined to physical locations or data centers, today's heterogeneous environments extend into the cloud and beyond. This shift has led to a critical realization: identity—not the network edge—is now the primary line of defense.

In 2024, identity-related attacks grew into one of the most prevalent cyber threats, with 90% of organizations having experienced at least one breach, and 84% of those causing direct business impact[1]. Organizations must now treat identities, whether human or machine, as the core assets to protect, ensuring that each entity is authenticated, authorized, and continuously secure in its interactions.

b) The Exponential Growth of Identities

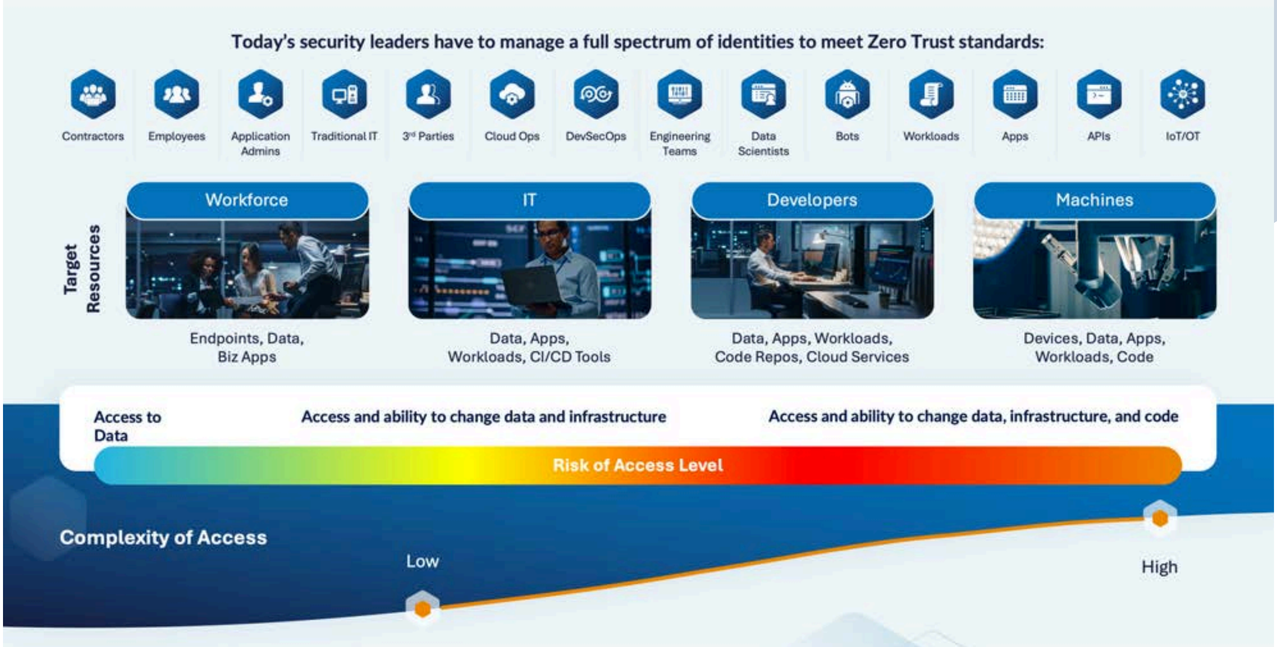
The rapid growth in machine identities has added immense complexity to cybersecurity strategies. CyberArk states that machine identities outnumber human identities in organizations worldwide by at least 82 to 1[2] with each organization managing an average of 45,000 machine identities. This surge includes devices, workloads, applications, and APIs, all of which are integral to modern digital infrastructures.

Unlike human identities, which are typically tied to individuals and can be managed with relative stability, machine identities are dynamic and multiply with the adoption of automation, IoT, and digital transformation initiatives. Each new microservice, IoT device, or cloud workload introduces additional machine identities that requires diligent management, and adherence to corporate security policy.

c) Machine Identities: Devices are a Major Vulnerability

While machine identities span several categories, including workloads, APIs, and applications, connected devices represent the largest and most vulnerable segment. In 2024 alone, over 18 billion IoT devices were connected to the internet, and this number is expected to more than double to 39.6 billion by 2033[3] with particular growth in critical infrastructure, transportation and government. With such growth comes increased risk. According to CyberArk, 42% of machine identities have access to sensitive data (vs 37% of human identities) and 90% of organizations have experienced an identity related breach in the last 12 months[4]. The number of attempted attacks has also increased significantly, with organizations facing an average of 53 IoT exploit attempts per week in 2024 which is a 46% increase on the previous year[5].

[1] 2024 Trends in Identity Security, IDSA
[2] 2025 Identity Security Landscape, CyberArk
[3] Statista
[4] 2025 Identity Security Landscape, CyberArk
[5] Check Point Software Technologies


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

The challenge is that many connected devices lack the security mechanisms of traditional IT assets, making them easier targets for attackers. Many can be legacy devices that have not kept pace with the rapidly changing threat landscape and can also be located remotely with infrequent connectivity, compounding the problem. Whether they are deployed in industrial settings, healthcare environments, or smart cities, the stakes are high. Compromised devices can serve as entry points into broader networks, enabling lateral movement by attackers and increasing the risk of operational disruption, data breaches, or even physical harm.

Compounding this issue is the reality that IoT devices rarely operate in static environments. They are frequently reconfigured, redeployed, or retired. If these stages are not secured with the same rigor as initial deployment, organizations face significant and avoidable risks, including unauthorized reuse of credentials, lingering privileged access to critical systems, and exposure to unpatched vulnerabilities. As these environments grow, managing machine identities becomes infinitely more complex and special attention must be paid to each stage of the life cycle.

A holistic approach that covers the full device journey: establishing initial trust, automated onboarding, identity lifecycle management, enterprise integration, decommissioning, and recommissioning - is vital to maintaining the integrity of connected ecosystems.

DEFINING THE MARKET

a) A Fragmented Market Struggling to Keep Up

The exponential growth in connected devices and the increasing attack surface means that the cybersecurity market is undergoing a fundamental transformation in an attempt to keep up. Fragmented, siloed solutions have dominated in the past, but these are proving inadequate in the face of rapidly evolving cyber threats, particularly in the context of connected device identities. AI-based attacks for example have the ability to rapidly move across these siloes evading detection or making it difficult to respond before the damage has already been done.

The existing fragmentation in the market results from many vendors focusing on niche solutions that address only one aspect of the broader problem. Traditionally, identity and access management (IAM) has focused on human identities, which are relatively straightforward to manage using credentials, multi-factor authentication (MFA), and role-based access controls. But with the rise of automation, cloud services, and the proliferation of connected devices, this narrow focus has become insufficient.

While many solutions focus heavily on Detect and Respond capabilities, the evolving threat landscape and regulatory pressure highlight the need to shift security left—starting with Identity. The February 2024 update to the NIST Cybersecurity Framework (CSF 2.0) reinforces this by placing greater emphasis on the "Identify" function as foundational to all other security activities. For IoT and edge environments, establishing strong device identity is not optional—it's the critical first step to ensuring visibility, trust, and control across the entire ecosystem. Without verified identities, detection and response efforts are undermined before they even begin.

However, many organizations continue to rely on fragmented solutions that fail to integrate human, machine, and IoT identities under a single security framework. This disjointed approach leaves critical gaps in security, making it easier for attackers to exploit vulnerabilities and harder for organizations to maintain comprehensive visibility and control.

b) The Two Identity Categories: Human Vs Non Human

In the evolving cybersecurity landscape, identities can be divided into two main categories: human and non-human, a sub-set of which is machine identities which includes IoT/OT devices. Each category presents its own unique challenges and requires tailored security solutions to ensure comprehensive protection.

i) Human Identities

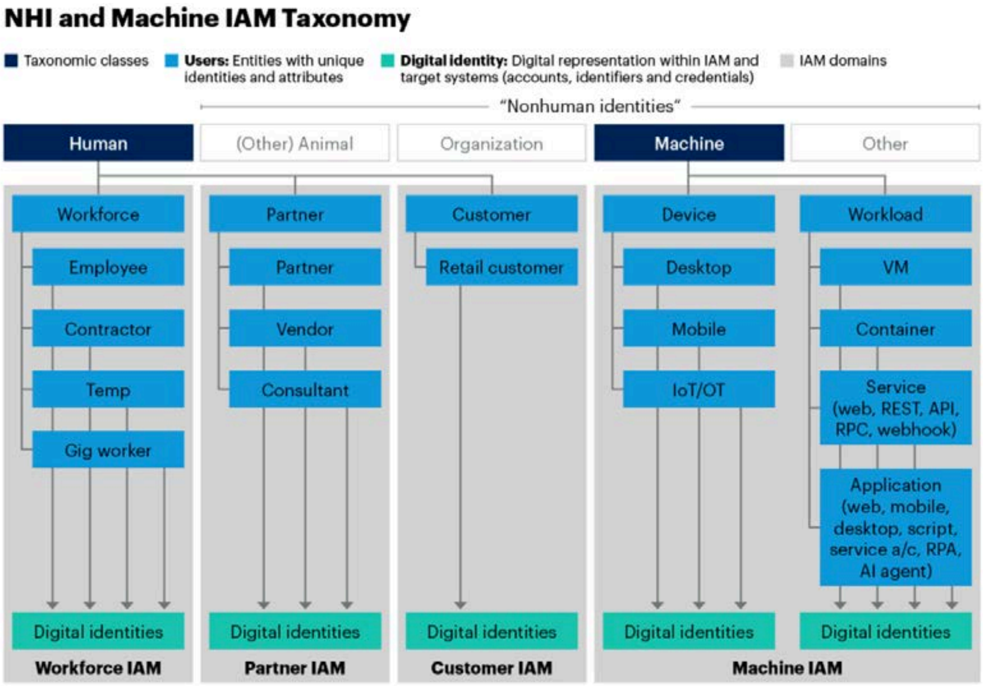
Human identities remain a cornerstone of identity management. These identities are linked to individuals—employees, contractors, customers, or partners—who require access to an organization’s resources. Traditional IAM solutions are designed to manage human identities, offering controls such as password management, MFA, single sign-on (SSO), and privileged access management (PAM).

While human identities are still a major focus of security efforts, they no longer represent the majority of identities within modern organizations. However, the human element continues to be a key attack vector, particularly through social engineering, phishing, and credential theft. Therefore, securing human identities with strong authentication and access controls remains critical, but it must be part of a broader identity-based security strategy that accounts for the growing number of machine identities.

ii) Non-Human Identities

Non-human identities (NHI) refer to any identity that is not human, including devices, software, legal entities, and even animals. While all machine identities fall under the broader category of NHI, not all NHIs are machine identities.

The concepts of machine identity and identity and access management (IAM) for nonhumans aren't new, but what's changing is how vendors now position machine IAM capabilities under the NHI banner—driven by the rapid proliferation of machine identities in digital environments.



Gartner, 2025

- **Machine Identities**

Machine identities encompass any digital entity that interacts with other systems, networks, or users. These include workloads, applications, containers, virtual machines, APIs, and bots. As automation increases and cloud adoption accelerates, machine identities have proliferated, often outstripping human identities in both number and complexity, and today are estimated to outnumber human identities 85:1.

Managing machine identities requires a fundamentally different approach than managing human identities. Machine identities are often ephemeral, being created and destroyed as workloads spin up and down in cloud environments. They require cryptographic keys, certificates, and other forms of secure authentication to interact with other systems. Yet many organizations lack the necessary infrastructure to manage these identities effectively, leaving them vulnerable to attacks such as credential stuffing, API exploitation, and certificate misuse.

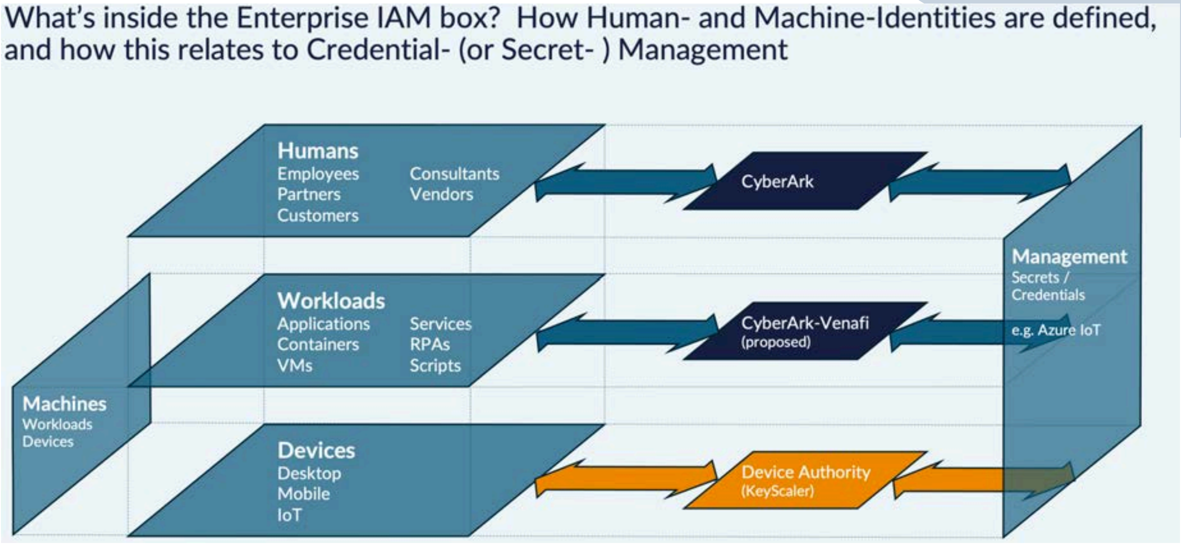
The rise of machine identities has expanded the attack surface, making it essential for organizations to deploy automated solutions that can manage and secure these identities at scale. However, most organizations are still playing catch-up, relying on manual processes or point solutions that cannot keep pace with the dynamic nature of machine identities.

- **IoT/OT Devices**

IoT and OT devices represent an important sub-set of machine identities and they are perhaps the most challenging to secure. These devices are often deployed in environments where traditional IT security controls are difficult to implement, such as industrial settings, critical infrastructure, healthcare, and smart cities. Unlike human or machine identities, IoT and OT devices often lack the computing power and security capabilities to support robust identity management practices.

oT/OT devices are also diverse, ranging from simple sensors and actuators to complex industrial machinery and connected medical devices. This diversity makes it difficult to implement a one-size-fits-all security solution. However, attackers are increasingly targeting these devices as they are often the weakest link in an organization’s security chain. For example, an unsecured IoT device could be used to launch a Distributed Denial of Service (DDoS) attack or serve as a gateway for lateral movement within a network.

The diagram below demonstrates how the different types of identities create opportunities for attackers to exploit the gaps in an incomplete identity security strategy.



c) Redefining IoT: A More Nuanced Approach

As the IoT ecosystem continues to expand, the need for a more nuanced definition of IoT is becoming clear. The traditional view of IoT as a homogenous collection of connected devices no longer reflects the diversity of use cases and environments in which these devices operate. To address this, we propose a new classification system that divides IoT into three categories: consumer, corporate, and enterprise/industrial devices.

i) Consumer IoT

Consumer IoT devices are those used in homes and personal environments. These include smart home devices such as thermostats, security cameras, wearable technology, and voice-activated assistants. While the security of consumer IoT devices is a growing concern, particularly with the rise of smart home ecosystems, these devices are generally outside the control of corporate security teams. However, their widespread adoption creates new risks, especially when employees connect these devices to corporate networks.

ii) Corporate IoT

Corporate IoT devices are used in business environments and are typically managed by IT teams. These devices include connected printers, office security systems, smart lighting, and conference room equipment. While corporate IoT devices are subject to some level of security management, they are often overlooked in broader cybersecurity strategies, leading to potential vulnerabilities. For example, a compromised smart printer could be used as a pivot point for a larger network attack.

iii) Enterprise/Industrial IoT

The final category encompasses enterprise and industrial IoT devices, also referred to as OT devices or unmanaged devices. These are deployed in critical infrastructure, manufacturing facilities, healthcare settings, and other industrial environments. These devices are often the most difficult to secure due to their complexity, reliance on legacy systems, the need for continuous operation, and the lack of visibility of these devices by IT-focused security teams. However, they represent some of the most significant cybersecurity risks. A compromised industrial IoT device could lead to operational disruption, lost productivity, physical damage, or even harm to human life.

LOOKING AHEAD

The Need for an Integrated Approach

The current market for identity-based security is struggling to keep up with the pace of change. Fragmented solutions that treat human, machine, and IoT identities separately are no longer sufficient. To address the growing threat landscape, organizations must adopt an integrated approach that unifies the management of all identity types under a single security framework. Larger vendors are making steps towards consolidating the market and adopting a ‘Prescribe rather than describe’ approach in the form of reference architectures. These architectures, produced by Microsoft among others, provide a ready made, integrated eco-system of vendors and solutions that make it easier to achieve the desired security outcome.

By recognizing the unique challenges posed by machine and IoT/OT identities and implementing robust, automated solutions, organizations can better protect themselves against the evolving threats of the modern digital world.

Following is an example of how technology leaders like Microsoft are creating industry-specific reference architectures with security as a critical component, helping customers build resilience into their operations and reduce some of the most common threats to machine identity security, from devops all the way through the supply chain.

SOLVING IOT SECURITY CHALLENGES WITH CLOUD-DELIVERED SOLUTIONS

The growth of IoT devices presents both incredible opportunities and significant security risks for organizations. Managing device identities, automating secure provisioning, and enforcing policies across increasingly complex IoT environments can overwhelm traditional security solutions and organizations are under increasing pressure to maintain consistent, policy-driven security across diverse and distributed device environments.

A cloud-based Software-as-a-Service (SaaS) model offers significant advantages for meeting these challenges—providing the scale, speed, and flexibility needed to manage device identity and security at enterprise levels without the overhead of costly infrastructure. Here are some of the main drivers for organizations adopting a cloud-based approach to security:

- **The Modern Regulatory Landscape Necessitates a New Approach**

New and emerging regulations—such as the EU Cyber Resilience Act, the U.S. Cyber Trust Mark, EO14028, and national critical infrastructure mandates—require continuous, demonstrable security controls over IoT assets. These regulations are not one-time compliance checkboxes; they demand ongoing visibility, integrity assurance, and proof of control. SaaS-based security platforms enable centralized policy management, real-time auditing, and consistent enforcement across geographic regions and device types—critical for achieving and maintaining compliance.

- **Addressing the Security Skills Gap**

Organizations globally are facing a shortage of skilled cybersecurity professionals, and the specialized nature of IoT security—particularly identity, PKI, and secure provisioning—makes this shortage even more acute. According to Boston Consulting Group, the global security workforce reached 7.1million in 2024 but a further 2.8million jobs remain unfilled. SaaS solutions abstract much of the underlying complexity, providing simplified workflows, pre-configured security templates, and automated policy enforcement. This reduces dependency on scarce expertise and enables broader IT and operations teams to take secure action with confidence.

- **Reducing Risk from Human Error**

Manual processes introduce risk, especially when managing thousands (or millions) of devices across various lifecycles and environments. Misconfigured certificates, missed updates, and inconsistent policies can all lead to exposure. A cloud-native platform automates critical operations - such as device onboarding, identity binding, certificate rotation, and revocation - ensuring consistency, reducing missteps, and accelerating response when issues arise.

- **Enabling Scale with Automation and Intelligence**

In highly distributed IoT environments, manual approaches simply do not scale. Cloud-based SaaS platforms are built to support large, dynamic device fleets—enabling policy-based automation for identity provisioning, authentication, encryption, and access control. By combining automation with threat intelligence and contextual awareness, SaaS solutions enable real-time security decisions without human intervention, aligning with Zero Trust principles such as "never trust, always verify."

- **Future-Proofing with Continuous Innovation**

Finally, a SaaS delivery model ensures customers benefit from continuous updates, the latest security innovations, and evolving compliance support—without the overhead of maintaining infrastructure or patching software. This agility is essential in an era where threats evolve faster than traditional IT cycles can adapt.

PRODUCT SPOTLIGHT

To address these challenges, KeyScaler-as-a-Service (KSaaS) offers a cutting-edge, cloud-native solution that simplifies and strengthens IoT security at scale.

What is KSaaS?

KSaaS is a fully hosted, cloud-delivered version of Device Authority's award-winning KeyScaler platform. It provides a seamless, scalable approach to managing device identities and automating critical IoT security processes. By leveraging KSaaS, organizations can secure their IoT infrastructure without the need for costly, on-premises hardware or complex manual processes.

Core Features of KSaaS

1. **Automated Device Identity Management:**
   - KSaaS establishes trusted identities for IoT devices through automated provisioning of digital certificates and cryptographic keys.
   - Supports secure device onboarding within seconds, reducing manual intervention and eliminating the risk of configuration errors.
2. **Dynamic Policy-Driven Security:**
   - Enforces security policies dynamically across the entire device lifecycle, including onboarding, authentication, updates, and decommissioning.
   - Ensures real-time compliance with organizational security requirements and industry regulations.
3. **Integration with Enterprise Applications:**
   - Seamlessly connects with existing enterprise applications, including Microsoft Azure, AWS IoT, and VMware, ensuring a unified security framework.
   - Simplifies the integration of IoT security into broader IT operations without disrupting workflows.
4. **End-to-End Automation with PKI:**
   - Automates Public Key Infrastructure (PKI) processes such as certificate issuance, renewal, and revocation.
   - Reduces administrative overhead while maintaining high levels of trust and security.
   - Supports integration with existing Public and Private PKI services, including BYOK (Bring Your Own Key) model
5. **Scalable and Flexible Architecture:**
   - Built to support organizations of any size, KSaaS scales effortlessly as IoT networks grow.
   - Provides flexibility to adapt to the unique needs of diverse industries, from healthcare and manufacturing to critical infrastructure.
6. **Real-Time Visibility and Insights:**
   - Offers centralized visibility into device trust and security posture across all connected devices.
   - Enables proactive security management through detailed logs, reports, and analytics.

Click or scan for more information about KSaaS

Benefits of KSaaS

1. **Enhanced Security at Scale:**
   - By automating identity and security processes, KSaaS reduces vulnerabilities and strengthens the overall security posture of IoT networks.
   - Eliminates the risk of credential misuse, unauthorized access, and supply chain attacks.
2. **Cost and Resource Efficiency:**
   - Avoids the need for on-premises hardware and reduces operational costs by delivering a cloud-based, fully managed solution.
   - Frees up IT and security teams to focus on higher-value activities, as routine processes are handled automatically.
3. **Faster Time to Value:**
   - KSaaS enables rapid deployment, allowing organizations to secure their IoT environments without delays associated with traditional solutions.
   - Accelerates ROI by simplifying the setup and ongoing management of device security.
4. **Regulatory Compliance Made Easy:**
   - KSaaS supports compliance with industry regulations (e.g., GDPR, NIST, ISO 27001) by enforcing robust authentication, encryption, and policy management standards.
   - Reduces the complexity of meeting audit and reporting requirements.
5. **Future-Ready IoT Security:**
   - Designed to evolve with emerging IoT technologies and security trends, KSaaS ensures that organizations remain protected as their IoT ecosystems grow.
   - Supports integration with advanced technologies like AI, machine learning, and blockchain to enhance security further.

LOOKING AHEAD

Security support for agentless devices at the Edge will continue to grow in importance because many of the connected systems in industrial, healthcare, and critical infrastructure environments are not designed to run security agents. These devices—such as sensors, programmable logic controllers (PLCs), and legacy embedded systems—often operate with limited compute resources, real-time constraints, or vendor restrictions that prevent the installation of traditional security software.

As organizations push computing and intelligence closer to where data is generated—at the Edge—the attack surface widens dramatically. Agentless devices may still handle sensitive data, control critical operations, or serve as potential entry points for lateral attacks. Without native agent support, they often lack basic visibility, policy enforcement, and threat detection, creating blind spots in an organization’s security posture.

ENHANCING CYBER RESILIENCE AND COMPLIANCE THROUGH DEVICE DISCOVERY AND VISIBILITY

In today's complex and interconnected enterprise environments, Chief Information Security Officers (CISOs) face the critical challenge of maintaining comprehensive visibility over all devices within their networks. This visibility is fundamental to strengthening cyber resilience and ensuring compliance with regulatory standards.

The Imperative of Device Discovery and Visibility

Complete visibility into the network's attack surface enables organizations to proactively identify vulnerabilities and weaknesses within their infrastructure. By understanding their digital footprint, organizations can prioritize security measures, allocate resources effectively, and mitigate risks associated with cyber-attacks. However, many threats originate outside of the traditional network boundaries through unknown or undocumented assets.

As an example, OT environments are often opaque, containing legacy and proprietary systems with minimal documentation and visibility within IT systems. Without a clear understanding of all connected devices, organizations risk leaving vulnerabilities unaddressed, which can be exploited by malicious actors, leading to data breaches, operational disruptions, and non-compliance with industry regulations.

Active vs Passive Scanning

In securing IoT environments, both active and passive scanning play crucial roles—each with distinct benefits. Whilst passive scanning observes device traffic without direct interaction, active scanning involves directly probing devices to gather information such as open ports, protocols, and firmware details, which enables faster detection of misconfigurations, outdated software, and known vulnerabilities. Although passive methods reduce the risk of device disruption and, for that reason, are often favoured by IT teams, a combination of active and passive approaches will provide a more complete, low-risk view of the IoT threat landscape—balancing thoroughness with operational safety.

As an example, when combined with a Software Bill of Materials (SBOM), a detailed list of all software components in a device, active scanning of devices enables organizations to quickly and precisely identify and respond to vulnerabilities, reducing risk.

Active scanning also plays a key role in PQ readiness where OT environments with devices that may operate for decades need long-term cryptographic resilience. In order to achieve this certificate visibility is critical, both to be aware of certificates and algorithms used across all devices but also to identify legacy or hardcoded certificates that are static or weak and difficult to update.

Planning for Safe Device Discovery

To avoid operational disruptions:

- Map the Network: Understand zones, conduits, and communication flows.
- Leverage OT-Aware Tools: Use discovery platforms designed for industrial protocols and systems.
- Engage OT Stakeholders: Coordinate with engineers and operators to define scanning windows and asset sensitivity.
- Throttle Interactions: Control probing frequency and depth when using non-intrusive active methods.

A careful, layered approach to device discovery ensures visibility without jeopardizing system uptime or safety.

PRODUCT SPOTLIGHT

KeyScaler Discovery

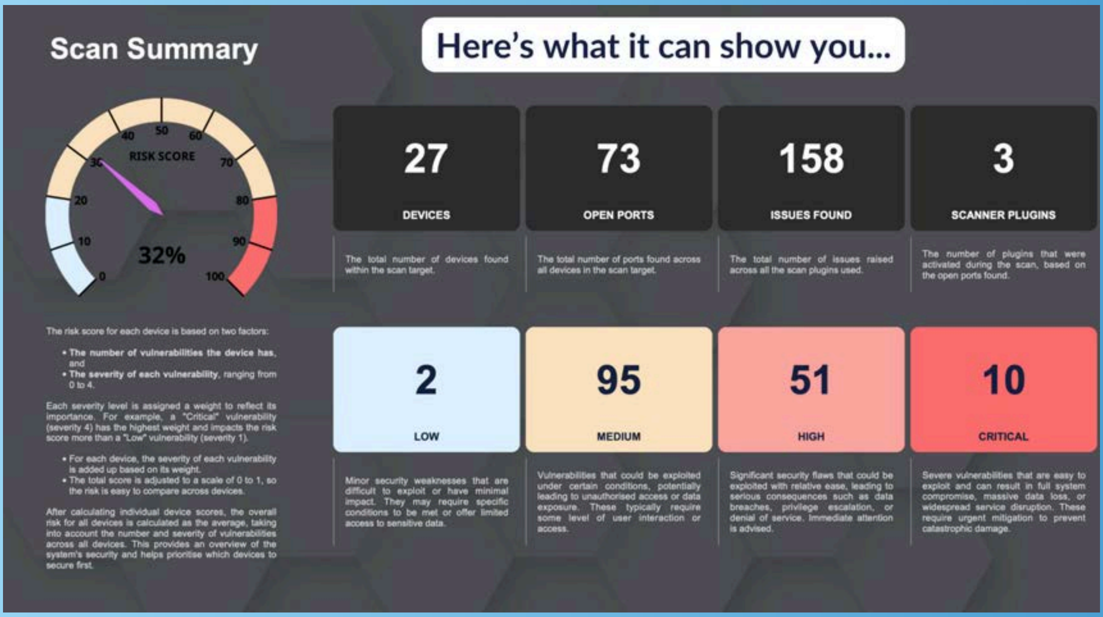
Introducing KeyScaler Discovery

To assist enterprises in achieving comprehensive device visibility, Device Authority has developed a Discovery Tool—a user-friendly solution designed to transform how organizations secure their IoT networks.

Key Features of KeyScaler Discovery:

- Comprehensive Device Identification: The tool scans specified IP ranges to identify devices, providing details such as IP addresses, MAC addresses, operating system information, and open ports.
- Vulnerability Detection: It highlights potential security risks, including expired or long-duration TLS certificates and unmanaged devices, which could pose threats to the network.

- Actionable Reporting: Generates clear, professional reports that guide IT teams through the process of addressing identified vulnerabilities, facilitating swift remediation.
- User-Friendly Interface: Designed for ease of use, ensuring that IT teams of all skill levels can effectively implement and utilize the tool.



Scan Summary

Here’s what it can show you...

The risk score for each device is based on two factors:

- **The number of vulnerabilities the device has**, and
- **The severity of each vulnerability**, ranging from 0 to 4.

Each severity level is assigned a weight to reflect its importance. For example, a "Critical" vulnerability (severity 4) has the highest weight and impacts the risk score more than a "Low" vulnerability (severity 1).

- For each device, the severity of each vulnerability is added up based on its weight.
- The total score is adjusted to a scale of 0 to 1, so the risk is easy to compare across devices.

After calculating individual device scores, the overall risk for all devices is calculated as the average, taking into account the number and severity of vulnerabilities across all devices. This provides an overview of the system's security and helps prioritise which devices to secure first.

27
DEVICES
The total number of devices found within the scan target.

73
OPEN PORTS
The total number of ports found across all devices in the scan target.

158
ISSUES FOUND
The total number of issues raised across all the scan plugins used.

3
SCANNER PLUGINS
The number of plugins that were activated during the scan, based on the open ports found.

2
LOW
Minor security weaknesses that are difficult to exploit or have minimal impact. They may require specific conditions to be met or offer limited access to sensitive data.

95
MEDIUM
Vulnerabilities that could be exploited under certain conditions, potentially leading to unauthorised access or data exposure. These typically require some level of user interaction or access.

51
HIGH
Significant security flaws that could be exploited with relative ease, leading to serious consequences such as data breaches, privilege escalation, or denial of service. Immediate attention is advised.

10
CRITICAL
Severe vulnerabilities that are easy to exploit and can result in full system compromise, massive data loss, or widespread service disruption. These require urgent mitigation to prevent catastrophic damage.

Benefits for CISOs:

- Enhanced Cyber Resilience: By identifying and addressing vulnerabilities proactively, organizations can strengthen their defenses against potential cyber threats.
- Improved Compliance: Comprehensive device visibility aids in meeting regulatory requirements by ensuring that all devices adhere to security policies and standards.
- Efficient Resource Allocation: Actionable insights enable IT teams to prioritize remediation efforts, focusing resources on the most critical vulnerabilities.

Incorporating Device Authority's Discovery Tool into an organization's security strategy empowers CISOs to gain the necessary visibility to manage device security proactively. This foundational step is crucial for achieving a zero-trust security model and enhancing the organization's overall cyber resilience.

Click or scan for more information about KeyScaler Discovery

LOOKING AHEAD

Real-time data visibility and dashboards will continue to be vitally important to CISOs as they manage thousands – or even millions – of distributed connected devices. Dashboards that consolidate device identities, access logs, vulnerability exposure, and policy compliance (more on that later) into a single pane of glass empower CISOs to make faster, more informed decisions. Indicators of compromise (IOCs) that feature on these dashboards will also broaden to include factors such as anomalous behaviour detection as an indicator of risk. This visibility is crucial not only for proactive threat detection and incident response, but also for maintaining regulatory compliance, justifying security investments, and reporting risk posture to executive stakeholders.

As cyber threats grow more dynamic and regulations become more stringent, automated, AI-enhanced dashboards that surface actionable insights will be indispensable to maintaining trust, resilience, and accountability in IoT environments (See Section 6 for more on AI)

CHALLENGES PRESENTED BY AI

As artificial intelligence (AI) becomes embedded into connected systems, it introduces not only new capabilities but also novel security challenges. These challenges are further amplified by the emergence of Agentic AI—autonomous agents capable of making decisions, executing tasks, and initiating communications across distributed environments without human intervention. When operating across critical systems, from industrial control networks to healthcare infrastructure, the implications for security and trust are profound.

a) The Role of Automation in the AI Era

In today’s AI-driven threat landscape, automation is no longer optional—it is imperative. The speed and sophistication of modern cyberattacks far outpace what manual processes can effectively address. Without automated identity and security lifecycle management, organizations are exposed to unacceptable risks, including delayed response to threats, human error, and inconsistent policy enforcement.

The increased adoption of AI by adversaries demands an equally sophisticated and automated defense strategy. This is particularly true in IoT environments, where devices can number in the thousands or even millions and operate in distributed, resource-constrained conditions. Manual or semi-manual methods for identity provisioning, certificate rotation, or trust recovery simply cannot keep pace.

- **Loss of Determinism in Behavior**

Traditional security models rely on predictable device behavior. Agentic AI, however, introduces dynamic and evolving behavior based on continuous learning, context, and goals. This non-determinism makes it harder to:

a. Establish clear behavioral baselines.
b. Detect anomalies in real time.
c. Define static policies for authorization and access control.

As a result, security teams must adapt to monitoring and assessing trust in systems that "learn and change" autonomously, potentially acting outside pre-defined boundaries.

- **Identity Ambiguity and Role Fluidity**

Agentic agents can operate across multiple domains, assume different roles, and interact with diverse systems and datasets. This fluid identity model breaks conventional approaches to device identity, which typically assume a static role or context.

This means that accurately identifying and authenticating agentic agents—and managing their role-based access—requires dynamic and context-aware identity management, not just static certificates or pre-assigned roles.

- **Data Integrity and Provenance Risks**

Autonomous agents often generate, transform, or consume data as part of decision-making loops. Without strong cryptographic guarantees, the authenticity and integrity of this data can be compromised—or worse, manipulated by malicious agents.

This makes the verification of data provenance and ensuring the trustworthiness of data from autonomous sources critical to preventing poisoned inputs, model manipulation, or misinformed decision-making.

- **Compromised AI Supply Chain**

Agentic systems often rely on external models, APIs, datasets, and firmware updates. These dependencies introduce AI-specific supply chain risks, including:

  - Deployment of tampered or malicious models.
  - Use of third-party data sets with embedded biases or vulnerabilities.
  - Hardcoded AI behaviors that are difficult to audit.

As a result, securing the full lifecycle of AI components—including model updates, data ingestion, and runtime configuration—is necessary to prevent covert attacks and maintain control.

- **Autonomous Policy Violations and Overreach**

Agentic agents may take initiative that violates policy—either through misaligned goals, adversarial manipulation, or unforeseen interactions with the environment.

This means that establishing effective policy constraints, implementing runtime enforcement, and enabling real-time override mechanisms are vital to prevent harmful or unauthorized actions.

- **Trust Calibration and Explainability**

Organizations must be able to quantify and calibrate trust in agents and their actions. Yet, many AI systems—particularly black-box models—lack transparency.

As a result, security teams struggle to evaluate the trustworthiness of AI decisions without explainability, increasing risk in high-assurance environments such as defense, healthcare, or critical infrastructure.

PRODUCT SPOTLIGHT

Device Authority's KeyScaler platform addresses these challenges by anchoring identity at the hardware and cryptographic level, ensuring that every AI agent—autonomous or not—can be authenticated, authorized, and continuously monitored. Through features like:

- Dynamic policy enforcement.
- Certificate-backed device identity.
- Real-time risk assessment via SBOM and threat intel integration.
- AI-assisted threat response (via KeyScaler's Microsoft Copilot integration).

KeyScaler ensures that even as AI systems become more autonomous and distributed, they remain secure, accountable, and aligned with organizational controls.

Click or scan for more information about KeyScaler

THE VALUE OF AI IN CONNECTED DEVICE SECURITY

The rapid expansion of the Internet of Things (IoT) and Operational Technology (OT) has transformed industries, enabling automation, efficiency, and real-time data insights. However, this growth has also introduced significant security challenges, including increased attack surfaces, complex device ecosystems, and evolving cyber threats. Traditional security approaches struggle to keep pace with the scale and sophistication of modern threats, making Artificial Intelligence (AI) an essential component of IoT and OT cybersecurity strategies.

AI-driven security solutions offer the ability to analyze vast amounts of device data, detect anomalies, and enforce dynamic, risk-based security policies in real time. By leveraging AI, organizations can enhance explicit device trust, automate security decisions, and proactively mitigate threats before they impact operations.

a) **The Business Benefits**

- **Enhanced Threat Detection:** AI identifies subtle behavioral anomalies that traditional security measures might miss.
- **Scalability & Automation:** AI-powered security scales effortlessly with IoT growth, reducing operational overhead.
- **Faster Incident Response:** Continuous monitoring and real-time anomaly detection accelerate threat mitigation.
- **Improved Regulatory Compliance:** AI-driven policy enforcement ensures adherence to cybersecurity standards.

As IoT and OT ecosystems continue to expand, AI-powered security solutions provide the intelligence, automation, and adaptability needed to establish explicit device trust and proactively defend against emerging threats. By integrating AI into IoT security frameworks, organizations can achieve a higher level of cyber resilience while maintaining operational efficiency.

PRODUCT SPOTLIGHT

KeyScaler AI™

KeyScaler AI: AI-Powered Trust, Anomaly Detection and Adaptive Security

Device Authority's KeyScaler AI is an advanced AI/ML module designed to bring intelligence and automation to IoT security. By integrating machine learning algorithms, KeyScaler AI continuously analyzes device behavior, enforces adaptive security policies, and detects anomalies that could indicate threats.

Key Capabilities of KeyScaler AI

- **Frictionless Device Onboarding**
  - Uses AI-driven pattern recognition to validate new devices against known, trusted device behaviors.
  - Automates secure onboarding, reducing manual intervention and enhancing security at scale.
- **Adaptive, Policy-Driven Security**
  - Continuously learns from device activity to refine and update security policies dynamically.
  - Enforces granular, context-aware access controls based on real-time risk assessments.
- **Anomalous Device Behavior Detection**
  - Monitors device activity and flags deviations from normal behavior patterns.
  - Enables rapid detection and response to potential security threats before they escalate.
- **Automated Compliance and Risk Management**
  - Helps organizations align with Zero Trust principles by ensuring continuous authorization and verification.
  - Supports compliance with industry security standards (e.g., NIST, ISO 27001, and GDPR) by proactively addressing vulnerabilities.
- **Microsoft CoPilot Integration**
  - Enables discovery of critical identity security data using natural language prompts (e.g. How many vulnerabilities did my devices have yesterday?)
  - Provides actionable recommendations in already familiar productivity tools like Microsoft Teams

Microsoft Copilot Integration

KeyScaler's integration with Microsoft Copilot helps organizations respond faster to threats and reduce the manual workload on stretched security teams by analysing real-time device information, including Software Bills of Materials (SBOMs) and external vulnerability databases like CVE repositories to identify weaknesses faster and take targeted action with greater confidence .

Designed for users of Microsoft's productivity suite, this virtual security assistant accelerates decision-making and improves visibility across large, complex fleets of connected devices, where delays or errors can carry significant operational risk and cost.

The integration extends access to KeyScaler AI and surfaces its rich device identity data into familiar tools like Microsoft Teams. Instead of spending hours sifting through code, vulnerability descriptions, or third-party resources, security professionals are presented with AI-curated threat summaries and recommended next steps through natural language prompts. This reduces investigation time and supports faster remediation—without sacrificing accuracy or control.

Key Benefits of Copilot Integration in KeyScaler:

- **Improved Visibility Across eco-systems:** AI-enhanced insights give a clearer picture of the security posture of every connected device, from edge sensors to core infrastructure.
- **Accelerated Threat Response:** Copilot interprets CVEs and associated data to prioritise the most urgent risks and recommend relevant mitigation strategies.
- **Reduced Manual Workload:** By automating risk assessments and information gathering, Copilot alleviates pressure on overstretched security teams and Security Operations Centers (SOCs).
- **Operational Resilience:** Faster decision-making and fewer false positives help avoid unnecessary system downtime, supporting business continuity.
- **Consistent Protection:** The AI engine ensures a scalable, repeatable approach to securing IoT/OT estates—regardless of complexity or size.

As cybersecurity threats become more distributed and adaptive, embedding AI into device identity management becomes essential. KeyScaler's Copilot integration represents the next step in autonomous, intelligent IoT security—bringing speed, scale, and precision to identity protection when it matters most.

Click or scan for more information about KeyScaler AI

LOOKING AHEAD

As AI becomes increasingly integrated into IoT security platforms, its role is also likely to expand from reactive threat detection to proactive regulatory alignment and risk forecasting. Future AI capabilities will continuously assess an organization’s IoT and device estate against evolving, unstructured policy documents and regulatory frameworks, automatically mapping device configurations, software components, and cryptographic usage to regulatory requirements. By analyzing SBOMs, certificate lifecycles, access controls, and telemetry data in real time, AI combined with Machine Learning (ML) and Large Language Models (LLMs) will expose non-compliant assets, highlight policy violations, and identify vulnerabilities that may trigger audit failures or fines. This continuous compliance assessment will enable security teams to prioritize remediation, reduce regulatory risk, and maintain a state of audit-readiness across complex, distributed environments.

ESTABLISHING TRUST AT ONBOARDING WITH DYNAMIC DEVICE KEY GENERATION (DDKG)

The foundation of any secure IoT ecosystem begins with establishing trust in the identity of each device. Before a certificate can be issued, before a device can be authenticated or authorized, its origin and integrity must be verified. Device Authority's Dynamic Device Key Generation (DDKG) capability is designed to solve this critical first challenge: how to onboard devices securely at scale and with confidence.

a) What is DDKG?

DDKG enables devices to generate unique cryptographically secure identities at the point of onboarding—either at manufacturing, first boot, or initial network connection. Unlike static credentials or pre-provisioned keys, DDKG ensures that keys are created securely on the device itself and are bound to that device's unique identity. These keys form the basis for a secure and immutable root of trust, paving the way for issuing certificates and enabling secure communications throughout the device's lifecycle.

b) Why It Matters

- Zero Trust Starts at Zero Touch: In modern Zero Trust environments, no device should be implicitly trusted. DDKG establishes identity from the start, creating a strong cryptographic anchor without requiring human intervention.
- Security Without Supply Chain Risk: Since keys are generated on-device, there's no risk of exposure or tampering during manufacturing, shipping, or staging—eliminating one of the most common vulnerabilities in connected ecosystems.
- Accelerated Onboarding at Scale: DDKG supports automated, policy-driven onboarding for millions of heterogeneous devices, reducing provisioning overhead and minimizing configuration errors.

c) Value to Our Partner Ecosystem

DDKG is not only a security enabler—it's a business enabler. For our technology and integration partners, it provides a trusted mechanism to streamline onboarding workflows, reduce complexity, and align with modern compliance requirements. Whether partners are deploying connected medical devices, vehicles, smart grids, or industrial controllers, DDKG lays a reliable foundation for identity issuance and lifecycle management.

By embedding trust at the very first step, Device Authority helps partners and customers eliminate identity gaps, reduce operational friction, and build secure, scalable IoT systems from the ground up.

EVOLVING FRAMEWORKS AND COMPLIANCE IN IOT/OT SECURITY

As connected devices become foundational to critical infrastructure, regulators and industry bodies are strengthening expectations around device security, trust, and lifecycle management. For organizations operating in regulated sectors or global markets, compliance is no longer a checkbox—it is a strategic imperative that protects customer trust, operational continuity, and brand integrity.

a) The Expanding Landscape of IoT/OT Security Regulations

Governments and standards bodies worldwide are introducing new laws and frameworks to enforce stronger security practices across IoT/OT ecosystems. Key developments include:

- **EU Cyber Resilience Act (CRA):** Requires manufacturers to implement secure-by-design principles and maintain ongoing security updates and vulnerability handling.
- **U.S. Executive Order 14028 & NIST IoT Frameworks:** Emphasizes supply chain security, SBOM transparency, and zero-trust architecture for federal and critical infrastructure systems.
- **UK PSTI Act (Product Security and Telecommunications Infrastructure):** Mandates basic security features such as unique passwords, vulnerability disclosure processes, and update transparency for consumer-connected products.
- **ETSI EN 303 645:** A leading baseline for IoT cybersecurity, adopted globally as a best practice framework.
- **IEC 62443:** Widely used in industrial environments, with an emphasis on secure system design and component certification.

These frameworks and laws increasingly demand proof of compliance across the entire device lifecycle—from onboarding and provisioning to software updates and certificate renewal.

NIST is also approaching the five year revision of its IoT security guidelines (2025). Its recent approach has focused on a risk-based, outcome-driven framework placing increased emphasis on governance, asset identification, and integration with broader organizational security strategies. It also positions device identity and trust as essential building blocks and a foundational step before organizations can effectively protect, detect, respond to, or recover from cyber threats in IoT ecosystems.

From its early workshops, the revision process looks set to include greater consideration for Industrial IoT, the relationship between privacy considerations and IoT security and consideration for the maintenance, repair and end of life of connected devices. It also identified key challenges and opportunities around three key themes:

1. **Lifecycle-Centric Security:** Addressing cybersecurity throughout the IoT product lifecycle with transparency, traceability, and the consideration of evolving demands.
2. **Risk Visibility and Evaluation:** Tackling challenges from limited visibility, unforeseen use cases, and unexpected environments, with an emphasis on assessing the scale of impacts.
3. **Effective Communication**: Bridging gaps between manufacturers and customers during pre-market and post-market phases to improve alignment and sustain cybersecurity.[6]

b) Why Automation is Essential for Sustained Compliance

Given the scale and complexity of modern IoT deployments, maintaining compliance manually is not practical. Compliance obligations often include:

1. Secure onboarding and credential issuance
2. Ongoing certificate rotation and expiry management
3. Audit trails and proof of identity/access control
4. Real-time vulnerability management and response

Without automation, these tasks become a significant burden on already-stretched security teams—raising the risk of missed deadlines, overlooked vulnerabilities, or non-conformance during audits.

LOOKING AHEAD

As regulatory frameworks around IoT and device security continue to evolve, maintaining compliance will be an ongoing central priority for organizations. Continuous compliance assessment enables organizations to align device configurations, software components, cryptographic protocols, and access controls with current regulatory standards. By mapping assets to requirements and monitoring elements such as SBOMs, certificate lifecycles, and telemetry data in real time, security teams can identify non-compliant assets, enforce policy adherence, and address vulnerabilities before they lead to audit failures or penalties. This proactive approach ensures audit readiness, reduces regulatory risk, and supports efficient remediation workflows—especially in complex, distributed IoT environments. While advanced technologies such as AI and ML enhance this process (see section 6), the foundational goal remains clear: sustained compliance through visibility, automation, and continuous alignment.

[6] https://www.nist.gov/blogs/cybersecurity-insights/five-years-later-evolving-iot-cybersecurity-guidelines#:~:text=Lifecycle%2DCentric%20Security:%20Addressing%20cybersecurity,improve%20alignment%20and%20sustain%20cybersecurity.

PRODUCT SPOTLIGHT

KeyScaler™

How KeyScaler Supports Compliance with Confidence

Device Authority’s KeyScaler platform provides the critical automation and intelligence needed to meet evolving regulatory demands across connected ecosystems. It aligns with core compliance requirements in the following ways:

Automated Identity Lifecycle Management

KeyScaler ensures secure, policy-driven onboarding, credential issuance, and lifecycle automation—including certificate rotation, revocation, and renewal—based on device behavior and risk.

Audit-Ready Logging and Evidence

All actions performed by KeyScaler are logged and verifiable, providing a strong audit trail to support conformance with regulatory reporting and incident investigation requirements.

SBOM and Vulnerability Integration

With SBOM insights and live threat intelligence integration, KeyScaler identifies devices at risk from newly disclosed CVEs and supports timely remediation—addressing NIST and CRA expectations for vulnerability management.

Policy Enforcement at Scale

Security and compliance policies can be enforced consistently across thousands (or millions) of devices, ensuring uniform protection, even in highly distributed or hybrid environments.

Standards-Aligned Architecture

KeyScaler’s architecture is compatible with NIST, ETSI, and IEC 62443 recommendations, helping customers align with globally recognized best practices.

A Foundation for Regulatory Confidence

In today’s regulatory climate, compliance is dynamic, not static. Frameworks will continue to evolve alongside the threat landscape—and organizations must adopt platforms that evolve with them.

By automating complex compliance tasks and enabling security-by-design at scale, Device Authority’s KeyScaler empowers customers and partners to stay ahead of evolving legislation while building a strong, evidence-based security posture across their connected ecosystems.

Click or scan for more information about KeyScaler

10

CONCLUSION

The recent publications of NIST 1800-36B and IR 8259 Rev 1 highlight a positive trend toward standardizing automated machine identity lifecycle management for IoT/OT devices.

However it is important to focus on a few fundamental requirements to making this a reality: automation, full lifecycle management, software based delivery, and where appropriate agent-based controls to enable security at the edge where many devices operate.

First, automation is essential—not just to scale identity provisioning and renewal across millions of devices, but to enable real-time responses to changes in risk posture. Full lifecycle management is equally important, encompassing not only onboarding and certification but also rotation, revocation, and decommissioning.

Equally critical is the adoption of software-based delivery models, such as SaaS, which provide the agility and scalability required to stay ahead of evolving threats and regulations. This model also enables consistent policy enforcement and faster integration with broader security operations.

Visibility is another foundational pillar. Organizations must be able to continuously discover and monitor all devices—especially unmanaged or agentless ones—and map their configurations, credentials, and vulnerabilities. This insight enables security teams to identify risks before they are exploited and to maintain an accurate compliance posture.

Artificial Intelligence is emerging as a powerful force multiplier in this space. By leveraging AI and Machine Learning, organizations can analyze vast amounts of telemetry, detect non-compliant behavior, and forecast regulatory gaps or security weaknesses before they impact operations.

In today's regulatory and threat landscape, achieving strong device identity security is no longer optional—it's a prerequisite for Zero Trust, compliance, and operational resilience. Organizations that embrace automation, visibility, AI, and comprehensive lifecycle management will be best positioned to protect their assets, meet audit requirements, and confidently scale their digital transformation.

Get In Touch

www.deviceauthority.com

contact@deviceauthority.com

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

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