GUIDE

Onboarding the Future: Guide for Edge Deployment with FIDO Device Onboard

Why You Should Consider the FDO Standard for Zero-Trust Device Onboarding

Table of Contents

Executive Summary 2

What is Onboarding? 3

FDO Certified Products 7

On the Edge: The Urgency to Secure and Simplify Device Security 8

What Problems Does FDO Solve? 9

Benefits of FDO for Enterprises and Providers 10

How to Adopt FDO Today 11

Executive Summary

IoT and edge computing solutions are exploding as manufacturers are looking for new ways to modernize their operations and accelerate production. By 2025, over 75 billion IoT devices will be connected globally. The industrial IoT market, which spans industries like manufacturing, healthcare, and retail is valued at USD 194 billion in 2024 and is projected to reach USD 286 billion by 2029. This surge unlocks immense opportunities and innovation for businesses and manufacturers alike. However, keeping up with the pace of demand for these devices and deploying them sustainably has created unprecedented challenges.

Namely, two key factors have the potential to derail the edge revolution entirely:

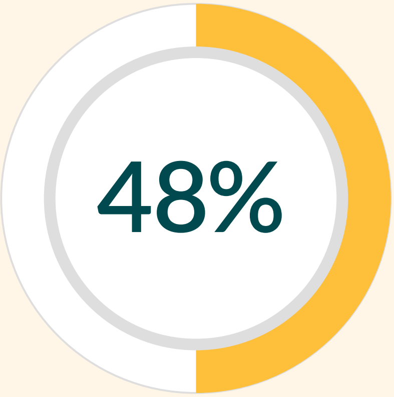
1. Costly and inefficient installation processes
2. Security vulnerabilities

What is Onboarding?

When an edge node or IoT device is installed in a facility, the device must be **onboarded** to its management platform hosted in the building or in the cloud.

The Onboarding Challenge

Device onboarding at scale is expensive and can introduce significant risks if not done properly. Meanwhile, typical manual onboarding processes and default passwords have created severe vulnerabilities, with [57% of IoT devices vulnerable to medium or high-severity attacks].



Nearly half (48%) of critical infrastructure security leaders reported experiencing at least one major security impact due to a compromised device within the last year.

What is FIDO Device Onboarding (FDO)?

FIDO Device Onboard (FDO) is a revolutionary standard designed to simplify, secure, and automate the onboarding process for IoT and edge devices. FDO simplifies device onboarding in edge and IoT computing environments with a plug and play, zero trust approach embedded in the specification. Developed by industry leaders like Arm, Amazon, Google, Intel, Microsoft and Qualcomm, the specification is one of the first openly available standards designed specifically to solve edge and IoT onboarding challenges: time-intensive, complex manual processes, high costs, and security vulnerabilities. It is targeted at industrial, medical, automotive, IT and retail use cases and is complemented by an independent certification program.

The Overlooked Opportunity and Risk

With the introduction of AI, a new layer of complexity was added to the edge challenge. Organizations are now hyper-focused on AI adoption and its promise of smarter, faster, and more efficient operations, but without addressing foundational IoT security, these ambitions are at risk of being undermined.

FIDO Alliance Device Onboard (FDO) provides the answer, offering a zero trust, plug and play standard that accelerates deployments while safeguarding infrastructure. In today's challenging economic climate, automating zero-touch device onboarding enables leaders to deliver ambitious digital transformation projects with limited resources and budgets, saving installation costs, accelerating time-to-value, and improving security. FDO is an open standard that allows users to innovate. FDO's zero-trust approach is an important piece of the IoT security puzzle and sets the stage for future AI updates inside protected enclaves.

Which industries benefit from FDO?

- Automotive
- Chemical
- Consumer goods
- Energy
- Education
- Manufacturing
- Enterprise and Networking
- Healthcare
- Oil and Gas
- Retail
- Telecommunications
- Supply chain and logistics

What Device Types Can Be Enabled with FDO?

Device Types	Examples
IoT sensors and devices	• Temperature sensors • Pressure sensors • Motion detectors • Water quality monitors • Smart thermostats • Connected industrial equipment
Smart cameras	• Wi-Fi-enabled cameras • Camera systems
Edge servers	• Edge servers • Mobile edge computing (MEC) servers
Networking equipment	• Routers • Switches • Gateways • 5G small cells
Industrial PCs and controllers	• Industrial PCs • Programmable logic controllers (PLCs) • Human-Machine Interfaces (HMIs)

Just as passkeys revolutionized user authentication, FDO is transforming device onboarding in edge computing and IoT environments.

The key features of FDO include:

LATE BINDING: Late binding saves money and time as FDO-enabled devices can be onboarded to any platform without the need for unique customization. This reduces the number of device SKUs needed versus other onboarding solutions. It ensures devices are authenticated and provisioned properly for the device recipient after ownership is verified.

PLUG AND PLAY: Whereas manual onboarding requires expensive, skilled technicians, FDO is highly automated, often allowing semi-skilled staff to carry out the installation. This is important in markets such as retail where FDO will allow the store manager to do the installation rather than needing to bring in an expensive IT expert.

OWNERSHIP VOUCHER: Device ownership is established and transferred securely in the supply chain with the "ownership voucher," which uses cryptographic authentication protocols in the FDO specification to verify the device recipient's physical and digital ownership.

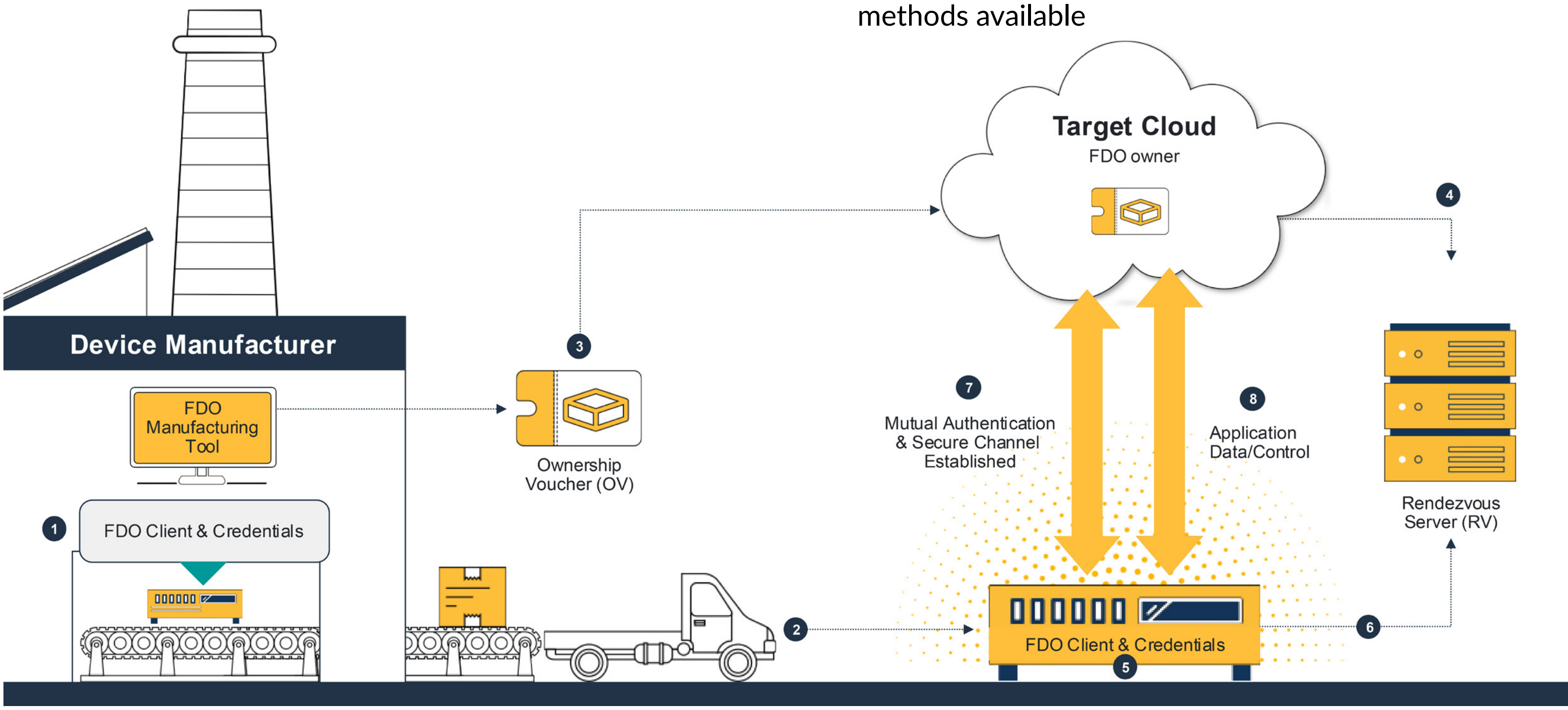
ZERO-TOUCH AND ZERO TRUST: Combined, these attributes establish a zero trust approach that covers end-to-end device onboarding using embedded, cryptographic protocols, and sequential processes to perform initial onboarding actions securely and quickly. The zero trust strategy covers both the device and the management platform during the onboarding process.

FDO for AI and Additional Features

FDO is designed to permit a secure subsystem to onboard independently and securely from the rest of the system. This makes FDO an excellent candidate for updating AI models deployed in edge secure enclaves from a cloud repository.

Additional features include:

- Interoperability with OPC Unified Architecture (OPC UA)
- Wi-Fi ready
- Flexible configurations for cloud, multi-cloud, and closed network environments with multi-tenant and cloud servers
- Multiple open source implementation methods available



FDO Certified Products

The FIDO Alliance is an open industry association with a mission to reduce the world's reliance on passwords. Consisting of the biggest global tech organizations and experts in cybersecurity, identity, and authentication, the alliance has a proven track record in transforming consumer authentication with passkeys.

In two years since the initial launch, passkeys have been enabled on 20% of the world's top 100 websites and over 15 billion accounts.

The FIDO Alliance has launched this complementary independent certification program that brings additional value to end users and solution providers alike. It assures that FDO certified solutions meet all the specifications, that devices comply with all security requirements, and have been tested for interoperability with other products.

>15 billion accounts

FDO Certified products bring considerable additional value to end users by offering:

- Guaranteed interoperability and security assurance
- Faster deployments and time to value
- Greater efficiencies
- Assures security and interoperability, eliminating the need for time-consuming vendor bake-offs with uncertified or home-brewed onboarding solutions

Now FIDO is applying this expertise to improve device authentication in industrial IoT and edge computing environments. FDO ensures devices and edge nodes can quickly and securely authenticate and connect online during initial deployment.

On the Edge: The Urgency to Secure and Simplify Device Security

Operational bottlenecks are a significant challenge in both industrial and commercial sectors. Manual, unsecured device onboarding not only consumes time and resources but also increases the risk of breaches. According to Microsoft's recent white paper, How to Scale Intelligent Factory Initiatives Through an Adaptive Cloud Approach, today's manufacturing leaders are burdened with *"technical sprawl and inefficiencies that create major obstacles to being able to scale solutions - including AI - to multiple production lines and geographically dispersed factories."*

This technical sprawl has led to data silos and management complexities, hindering global visibility and scalability. Ultimately, this prohibits the promise of connected devices from being realized in any industry.

$4.88 M

The average cost of a data breach in 2023 was $4.88 million (USD).

Edge implementations involve a lot of risk. Often these edge nodes are used in remote, precarious, and high-risk environments. Industries like healthcare, energy, and manufacturing face unique challenges and regulations, such as vulnerable patient monitoring systems, hazardous environments, and risks to complex supply chains. To make matters more complex, new threats are constantly emerging, such as the rise of quantum computing and zero-day exploits.

Some companies may feel that they can develop their own proprietary onboarding solution, but given today's economic pressures and the growing threat landscape, businesses often simply cannot afford to develop and maintain proprietary solutions or risk a preventable breach.

FDO and AI: A Symbiotic Future

Edge and IoT are also the "eyes and ears" of AI, collecting and transmitting data for analysis. There is a huge risk in overlooking IoT security and threats such as data poisoning, which can cripple AI models reliant on real-time data. Securing the foundation of edge and IoT is essential to unlock the full potential of AI.

AI systems depend on clean, reliable data streams. A compromised IoT device does not just threaten the device itself - it can corrupt AI models, disrupt decision-making, and open doors to adversarial attacks. FDO's zero trust onboarding ensures these vulnerabilities are eliminated from the start.

What Problems Does FDO Solve?

Human error:

34% of data breaches involve human error – FDO minimizes this with automation and a zero-touch approach.

Time-intensive and inefficient deployments:

FDO can deploy 10 times faster than manual methods. It dramatically reduces the time and budget needed to hire skilled technicians in high-risk environments, like oil rigs and factories. In some applications, such as retail, existing on-site staff can install FDO as it is plug and play technology.

Market speed to innovation:

Open standards help advance innovation and level the competitive playing field. By standardizing processes, providers can focus on truly adding value to their solutions. For customers, they can benefit from better solutions that are faster to deploy and more secure.

Device Security Risks – The Supply Chain Lifecycle

Stage 1: Manufacturing

Risk:
Supply chain compromises (for example, tampered devices)

FDO:
Establishes cryptographic ownership during manufacturing, ensuring device integrity

Stage 2: Shipment and storage

Risk:
Device ownership asset mismanagement

FDO:
Tracks and secures ownership transfers, maintaining a secure chain of custody

Stage 3: Onboarding and deployment

Risk:
Exposures from default passwords and manual installation errors

FDO:
Eliminates passwords and human errors with plug and play device onboarding and zero-touch automation

Stage 4: Operations

Risk:
Insecure data transmission, spoofing and infiltration

FDO:
Encrypts data exchanges and ensures ongoing device authentication

Benefits of FDO for Enterprises and Providers

Standards are vital to unlocking the full potential of any major global technology innovation. Global industry standard initiatives help remove huge amounts of waste, advance technology far more quickly, and increase market competitiveness. Standards also provide long-term security. As threats evolve, experts in the field continue to evolve the standards to keep up.

The FDO standard is also continuously improved within the FIDO Alliance. In the last two years, several Application Notes have been released to deal with implementation and other areas related to FDO 1.1. The newest version of the standard, FDO 1.2, is currently in development with new enterprise-ready features and is expected to be released in 2025.

The FDO standards have been developed and backed by the best companies in the industry, including Microsoft, Dell, and Intel. Experts from these organizations proactively work together to develop use cases and best practices for seamless and secure IoT device authentication, provisioning, and also support the adoption and implementation of the FDO standard.

Benefits for enterprises:

- Protect devices and supply chains with zero trust security.
- Integration is flexible with existing systems.
- Reduce the need to develop and manage your own testing requirements and protocols – buy with confidence with FDO certified products.
- Reduce time to market/deployment and increase value.

Benefits for providers:

- Leverage FDO certification as a competitive advantage. Ensure compatibility and earn customer trust with external independent validation. This becomes increasingly valuable as market adoption rises and FDO is increasingly referenced in Requests for Proposals (RFPs).
- Realize hardware efficiencies, simplify production, and reduce waste. As with FDO, operating systems can be deployed on-site and do not need to be hard programmed in. This capability is now part of an active workstream within the FDO Working Group called “Bare Metal Onboarding”.
- Fast-track solution development with confidence.
- Free engineer time to focus on higher value projects rather than waste time with manual or proprietary onboarding solutions. Offer a faster, more efficient solution to customers.

How to Adopt FDO Today

FDO offers a simple, secure, and scalable solution for enterprises and providers to accelerate edge computing and IoT device deployment at scale. With proven benefits like streamlined procurement, reduced costs, and enhanced security, FDO offers a clear path to efficiency and innovation – even in complex, high-risk, distributed environments.

Now is a perfect time to join industry leaders like Microsoft, Dell, Red Hat, and Intel in backing FDO and paving the way for wider adoption.

There are several ways to get involved with FDO with the FIDO Alliance:

Explore: Discover FIDO® Certified FDO products for seamless device onboarding.

Get Certified: Learn how to get FDO certified and demonstrate your products meet global security and interoperability standards.

Join the FIDO Alliance: Become a FIDO Alliance member and help shape the future of the FDO standard.

The technology, resources, and support are in place for FDO to transform the way leaders and teams deploy IoT devices at scale while managing edge security risks in today's fast-paced economy.

> **Deploying FDO has marked a pivotal shift for ASRock Industrial, establishing a new benchmark in secure, scalable onboarding for industrial edge IoT solutions. FDO's advanced security framework enables us to deliver unparalleled reliability and adaptability, empowering our clients to scale confidently in increasingly complex environments. This deployment cements ASRock Industrial's leadership in industrial computing security and sets the stage for us to shape the future of Industry 4.0 with solutions that are both resilient and future-ready".**
>
> **– Kenny Chang,**
> Vice President, ASRock Industries

References

Industrial IoT Market Forecast to 2029 Research and Markets Report. https://www.researchandmarkets.com/report/industrial-iot

Palo Alto Unit 42 IoT Report. https://start.paloaltonetworks.com/unit-42-iot-threat-report

Verizon 2024 Mobile Security Index. https://www.verizon.com/business/resources/reports/mobile-security-index/

Microsoft: How to Scale Intelligent Factory Initiatives Through an Adaptive Cloud Approach. https://clouddamcdnprodep.azureedge.net/gdc/gdcQIl0SB/original

IBM 2024 Cost of a Data Breach Report. https://www.ibm.com/reports/data-breach

Verizon 2024 Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/