FIAM: Frontline Identity, Access, and Management

Enforcing Zero Trust for the Frontline with 42Gears

Executive Summary

For years, organizations have relied on traditional Mobile Device Management (MDM) to secure and manage their devices. While MDM has been effective for basic control, it was never designed for today's frontline reality—shared devices, high user turnover, rugged environments, and constant pressure to balance security with speed.

The truth is clear : a managed device is not a fully secure device.

Modern IT teams face two critical and growing challenges:

- **Building a robust security defence** against breaches, credential misuse, and lateral network movement.
- **Reducing operational complexity** caused by fragmented identity, access, and device management tools.

To address these challenges, 42Gears introduces **FIAM – Frontline Identity, Access, and Management.** FIAM is the industry's first unified platform designed to **natively enforce a Zero Trust framework across the entire enterprise ecosystem**—from shared frontline and rugged devices to corporate endpoints and IoT.

FIAM transforms frontline security by unifying **device trust, user identity, and least-privilege access** into a single, cohesive platform.

The Frontline Security Reality: Why Traditional MDM Falls Short

Traditional IT solutions were built for desk-bound knowledge workers using personal laptops and phones. When these same tools are applied to frontline environments—warehouses, retail floors, manufacturing plants, healthcare facilities—they introduce serious security and compliance gaps.

The Core Issue: Managed Devices Without Identity Context

MDM answers only one question:

Is the device managed?

It does **not** answer:

- Who is using the device right now?
- Are they authorized for this application?
- Should they have access to the wider network?

This lack of identity and access context creates significant risk.

1. From Device Management to True Frontline Security

FIAM is built specifically to close the most dangerous gaps created by legacy device-centric security models.

Problem 1: Identity Blindness & Audit Risk

The Pain Point

One shared device is used by multiple workers across shifts.

Why It Fails

Traditional MDM is blind to user identity on shared devices. This leads to:

- Shared passwords
- Lack of user-level audit trails
- Compliance and investigation failures

The FIAM Solution

SureIdP verifies the specific user every time they access a device or application. This enables:

- Individual accountability
- Complete audit trails showing who accessed what, when
  Strong identity assurance on shared devices

Problem 2: Unworkable Authentication for the Frontline

The Pain Point

Frontline workers often operate with gloves, limited time, and varying technical skill levels.

Why It Fails

Passwords and traditional MFA are:

- Slow and disruptive
- Error-prone
- Unrealistic in high-turnover, shift-based environments

The FIAM Solution

SureIdP enables **fast, passwordless authentication,** including:

- NFC badge tap
- QR code scan

This dramatically reduces login time, improves adoption, and boosts productivity—without compromising security.

Problem 3: Access Overkill & Network Exposure

The Pain Point

Frontline users typically need access to *one application*, not the entire corporate network.

Why It Fails

Traditional VPNs grant broad network access, increasing the blast radius of:

- Compromised credentials
- Infected devices

The FIAM Solution

SureAccess enforces **least-privilege access** using **Per-App VPN micro-tunnels:**

- Users can access only the specific app they are authorized for
- No visibility into the rest of the network
- Dramatically reduced attack surface

2. A Unified Zero Trust Platform for the Frontline

FIAM is designed from the ground up around Zero Trust principles:

Never trust. Always verify. Enforce least privilege.

Instead of stitching together multiple tools, FIAM unifies all frontline security requirements into a single platform.

The Three Pillars of FIAM

Pillar 1: Device Trust

42Gears Product: SureMDM

What It Solves:

The challenge of a so-called "managed device" that may still be compromised or misconfigured.

Capabilities Include:

- Kiosk mode for task-focused usage
- Continuous device compliance checks
- OS patching and updates
- Threat defense and policy enforcement

Business Benefit:

Only healthy, compliant devices are allowed to access corporate resources.

Pillar 2: User Identity

42Gears Product: SureIdP

What It Solves:

Identity blindness on shared and frontline devices.

Capabilities Include:

- Passwordless authentication (NFC / QR)
- Rapid shift handovers
- Strong user verification without friction

Business Benefit:

Eliminates password fatigue while ensuring full accountability and audit readiness.

Pillar 3: Least-Privilege Access

42Gears Product: SureAccess

What It Solves:

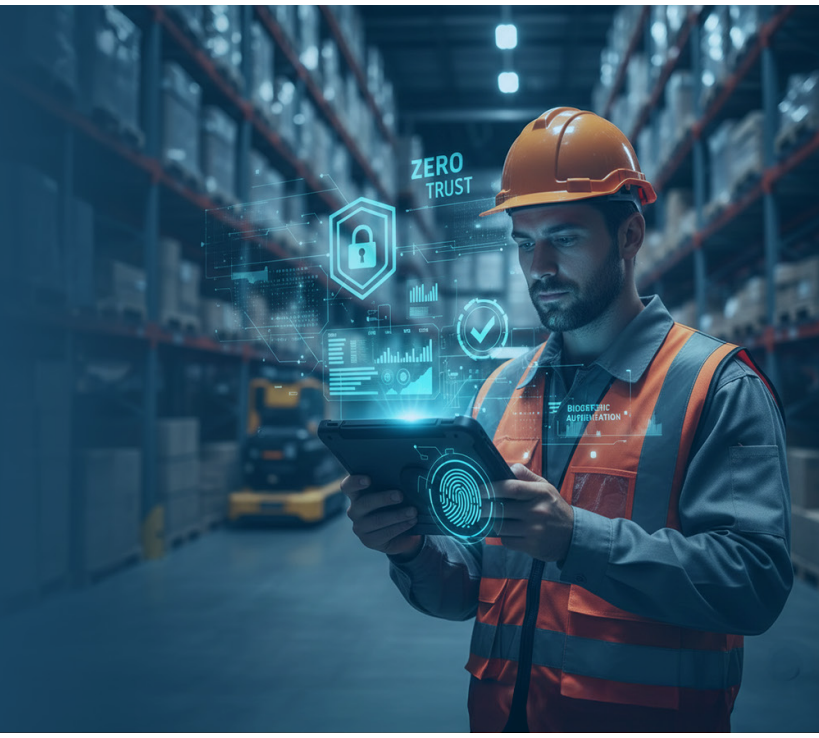
Over-permissioned access and unnecessary network exposure.

Capabilities Include:

- Per-App VPN micro-tunnels
- Context-aware access control
- No full-network VPNs

Business Benefit:

Reduces the attack surface dramatically while maintaining a seamless user experience.



3. From Frontline to Enterprise: A Unified Security Platform

FIAM is not just a frontline solution—it is a strategic platform aligned with the CIO's goal of consolidation and simplification.

One Platform, Multiple Endpoint Types

Frontline & Shared Devices

- Frontline Identity, Access, and Management (FIAM)
- Secure shared usage
- Full audit visibility
- Higher productivity with zero trust enforcement

Knowledge Worker Devices

- Comprehensive Unified Endpoint Management (UEM)
- Company-owned phones, tablets, and laptops
- Single dashboard for policy, compliance, and security

IoT & Things

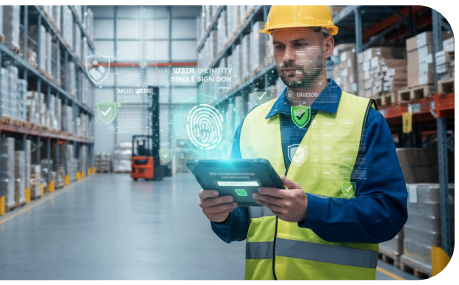
- Expanded management for non-mobile endpoints
- Printers, RFID readers, rugged scanners, and more
- Centralised visibility and control

Impact

- Fewer tools
- Lower operational overhead
- Consistent security posture across the enterprise

Why CIOs Are Standardizing on FIAM

As enterprises expand frontline operations and adopt Zero Trust, CIOs are reassessing fragmented endpoint and security strategies. FIAM addresses the three outcomes that matter most at the executive level: security assurance, workforce productivity, and platform consolidation.



Establish a Defensible Security Posture

Move beyond device management to provable security. By tightly linking user identity with real-time device posture, FIAM eliminates identity blind spots common in shared-device environments. Every access is attributable—clearly answering who accessed which application, on which device, and when—closing audit gaps and reducing credential-related risk.

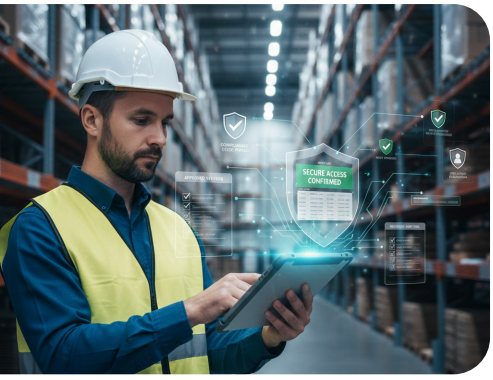
Enable Productivity Without Compromising Security

Security should never slow down frontline operations. FIAM's passwordless authentication workflows, including NFC badge taps and QR-based access, are purpose-built for rugged, high-turnover environments. Workers are productive from their first minute on shift, without sacrificing identity assurance or compliance.

Reduce Complexity Through Platform Consolidation

CIOs are under pressure to simplify sprawling IT environments. FIAM replaces disconnected tools with a single, unified control plane—managing mobile devices, rugged handhelds, printers, RFID readers, and IoT endpoints from one platform. The result is fewer vendors, lower operational overhead, and a consistent security posture across the enterprise.

Built for Compliance, Scale, and Real-World Operations



Audit and Compliance Readiness by Design

Regulated industries demand verifiable controls, not assumptions. FIAM supports audit and compliance initiatives by providing:

- User-level access logs for shared devices
- Clear separation of user identity, device posture, and application access
- Centralized policy enforcement across all endpoints

This reduces the effort required for audits and strengthens compliance with internal security policies and industry regulations.

Designed for High-Turnover, Shared-Device Environments

Frontline environments are defined by shift work, device sharing, and rapid onboarding. FIAM is optimised for this reality, enabling:

- Instant user onboarding and offboarding
- Secure shift handovers without reconfiguration
- Consistent user experience across locations and device types

Measurable Operational and Cost Benefits

By consolidating endpoint, identity, and access management into a single platform, organisations can:

- Reduce the number of security and management tools
- Lower administrative overhead for IT teams
- Minimise downtime caused by authentication friction or misconfigured access

The outcome is a stronger security posture delivered with lower total cost of ownership.

Conclusion: Redefining Frontline Security with FIAM

Frontline environments demand a fundamentally different approach to security—one that recognises shared usage, operational speed, and minimal access requirements.

With FIAM, 42Gears delivers:

- True Zero Trust enforcement
- Identity-aware security for shared devices
- Least-privilege access by design

A unified platform that scales from the frontline to IoT

The result is stronger security, simpler management, and a frontline workforce that stays productive without compromise.

42Gears FIAM: Because managing devices is no longer enough.

Take the next step toward Zero Trust for the frontline with 42Gears FIAM.