Manufacturing | Global

A manufacturer cut unauthorized device movements out of its plants by 40%

A large manufacturer with several plants tagged laptops and equipment with RFID, put every device movement through approval, and discovered the devices on its network.



40%
fewer unauthorized device movements outside the facility

30%
more accurate device inventory

20%
faster approval of device movement requests

AT A GLANCE

INDUSTRY
Manufacturing

SIZE
Large

LOCATIONS
Multiple manufacturing facilities

PREVIOUSLY
No approval process for device movement

FEATURES USED
Connected | Site services | IT asset management | Insight

01 The client

The client is a large manufacturing company running several production facilities. Its laptops and equipment carry designs, process data and other intellectual property.

Devices moved in and out of the plants with no structured approval and no reliable list of what was connected to the network, which left the company exposed to IP theft and data breaches.

02 The challenge

Laptops and equipment could leave a facility without anyone approving it, and IT could not say with confidence which devices were on the network or where they were.

- No structured process to approve a device leaving a facility.
- Little visibility of IT assets, so unknown devices could sit on the network.
- Unauthorized movement raised the risk of IP theft and data breaches.
- No record of where a device had been or who had taken it.

03 What they set up in Asset Infinity

After a joint risk assessment, the client configured Asset Infinity for RFID-tagged devices, approved movements at the gate and regular network discovery.

Connected

RFID tags on laptops and equipment

Every laptop and piece of equipment carries an RFID tag, and fixed readers at doorways and gates record each move, so the register shows where a device last passed.

Site services

Approved movements at the gate

Taking a device out of a facility starts a gatehouse request that the right person must approve, and the gate checks the approval before the device leaves.

IT asset management

Network discovery

Regular discovery scans find the devices connected to the network and compare them with the register, so unknown devices stand out.

Insight

Movement and approval reports

Reports show which devices left, who approved them, how long approvals took and which devices moved without one.

04 How it works day to day

This is what happens now when an employee needs to take a laptop out of a plant.

EMPLOYEE
Requests the move
The employee raises a request to take the device out, naming the asset, the reason and the expected return date.

APPROVER
Reviews and approves
The request reaches the authorized approver, with a reminder if it waits. The approver accepts or rejects it with a note.

SECURITY GUARD
Checks at the gate
At the gatehouse the guard confirms the device matches an approved request before it leaves the facility.

SYSTEM
Records the move
The RFID reader at the exit records the device passing, and the move is written to the asset's history.

SECURITY TEAM
Follows up on exceptions
A device recorded leaving without a matching approval shows up in reports, so the team can follow it up.

IT TEAM
Runs network discovery
Scheduled discovery scans list the devices on the network. Any device missing from the register is investigated and added or removed.

IT MANAGER
Reviews the numbers
Dashboards show device movements, approval times and inventory accuracy across all facilities.

05 Before and after

	BEFORE	WITH ASSET INFINITY
Device leaving a facility	No structured approval	Approved request checked at the gate
Location of devices	Little visibility	RFID readers record each move
Devices on the network	Unknown devices possible	Regular discovery scans against the register
Approval time	No structured workflow	20% faster
Unauthorized movements	A constant IP risk	Down 40%
Inventory accuracy	Not dependable	Up 30%

06 How it rolled out

1

Risk assessment. The client and the Asset Infinity team reviewed device security risks, weak points and existing safeguards.

2

Devices tagged. RFID tags went on laptops and equipment, and readers were placed at the facility exits.

3

Approvals and scans set up. Approval steps for movement requests were configured, and network discovery scans were scheduled to run regularly.

07 The results

15% improvement in overall device security

- Every movement request reviewed and authorized by the right person
- Fewer unknown devices on the network
- A history of each device's movements for investigations and audits

08 Why it worked

Built on a risk assessment

The setup started from the client's own risks and safeguards, so controls went where exposure was highest.

Physical and network views together

RFID moves and network discovery both check against one register, so a device missing from either stands out.

Approvals people follow

A quick request with reminders meant staff used the process instead of working around it.

09 Looking ahead

With RFID tags, approved movements and network discovery working from one register, the manufacturer knows which devices it has, where they are and who allowed them to leave a plant.

The same register gives IT a dependable base for audits, replacements and software license counts as the device estate grows.

See it on your own assets

A 30-minute demo, set up for a manufacturer with sensitive IT equipment.

The client's name is withheld for confidentiality. Results are as reported by the client.

Book a demo

Start a 14-day free trial