

Your Firewall Can't Hear Radio

The modems, badge readers and wireless links that walk right around your security.



ILLUSTRATIVE

4:12 a.m.

A pump controller at a remote station drops off the network.

Everyone assumes it went quiet.

It didn't. It's still talking. Just not on the network you're watching.

CONTENTS

What's inside.

A Letter From Eldad	4
How to Read the Stories	5
Three Ideas	6
01 Your Firewall Can't Hear Radio	7
02 The Modem Nobody Listed	9
03 Five Ways In Through the Air	11
04 Listen Before You Touch	15

05 Three Questions Before You Cut a Path	18
06 Close the Path. Keep the Door Working.	20
07 Ten Minutes With Security and Facilities	23
Closing: Something Is Listening	26
Sources	27
Start With One Blind Spot	28

Security used to mean watching the wire.

For most of my career, that was the whole job. If you could see every packet, you could protect the network.

Not anymore.

Walk through any hospital, warehouse, water plant or office tower and look for the things that talk through the air. The badge reader at the front door. The emergency phone in the elevator. The alarm panel with a cellular backup. The pump controller with a 4G modem a vendor installed to skip a two-hour drive. The wireless sensors on the chillers.

Not one of them asks your firewall for permission. Many of them never touch it.

This book isn't against wireless. Radio is cheaper than cable. It reaches places cable can't. It keeps working when the network goes down. That's exactly why it's everywhere.

It's a case for three simple rules. Every connection has an owner. Every connection has a reason. And someone is paying attention.

Like the four books before it, this one labels every story, so you always know what kind of evidence you're reading. It's short on purpose. Seven chapters. One idea.

Your firewall guards the wires. Someone has to watch the air.

Eldad Matityahu

Founder and CEO, NetOps IQ

Three labels. No guessing.

OBSERVED

We saw it.

Something our team saw during a NetOps IQ assessment, pilot or controlled demonstration. We don't publish customer names, device identifiers or dates.

SOURCED

Someone else reported it.

Public reporting or research from a named outside source. The links are in the notes at the back.

ILLUSTRATIVE

We built it to explain.

A realistic scenario that shows how the problem works. It's not a real incident, and we never pretend it is.

One more rule. When we describe a real attack or a real finding, we tell you what we saw and what we didn't. We'd rather undersell than oversell.

Start with three ideas.

Every story in this book grows from one of these.

01

Your firewall guards the wires. Radio goes around it.

Cellular modems, badge readers and wireless links can reach your operation without ever passing through the firewall.

02

A connection nobody owns is a door nobody locks.

Every radio link needs an owner, a reason, and someone who notices when it changes.

03

Done means two checks pass.

The risky path is closed. And the device still does its job. The door still opens. The alarm still calls out.



Badge reader at the entrance

CHAPTER 01

Your Firewall Can't Hear Radio

It guards the wires. The air goes around it.

Take a slow walk around one of your sites. Skip the server room. Look at everything else.

At the front door, a badge reader checks every card that taps it. Over radio. In the elevator, an emergency phone waits to call out over a cellular line. In a utility closet, the alarm panel has a cellular backup in case the phone lines die. On the roof, wireless sensors report from the chillers. In a pump room at the edge of the property, a controller has a small 4G modem with an antenna screwed on top.

Every one of those devices is doing its job. And every one of them can talk without asking your firewall.

A guard at the front door

Your firewall is a good guard. It checks everything that comes through the front door of your network. Keep it.

But a guard at the front door can't see the window around back. A cellular modem is a window. So is a wireless gateway. So is a radio tucked inside equipment nobody listed when it showed up.

Traffic on those paths can skip the firewall completely. It may never show up in your logs. Your tools aren't broken. They're watching the wires, and this traffic isn't on the wires.

The device was never on the network map. It still had a way in.

This isn't a war on wireless

Radio is how modern buildings work. It's cheaper than cable, it reaches places cable can't, and it keeps working when the network goes down. That's why alarm panels and elevator phones depend on it.

The risk isn't radio. The risk is a radio link that's unknown, unowned, unneeded or acting strange. That's a blind spot. Attackers love blind spots.

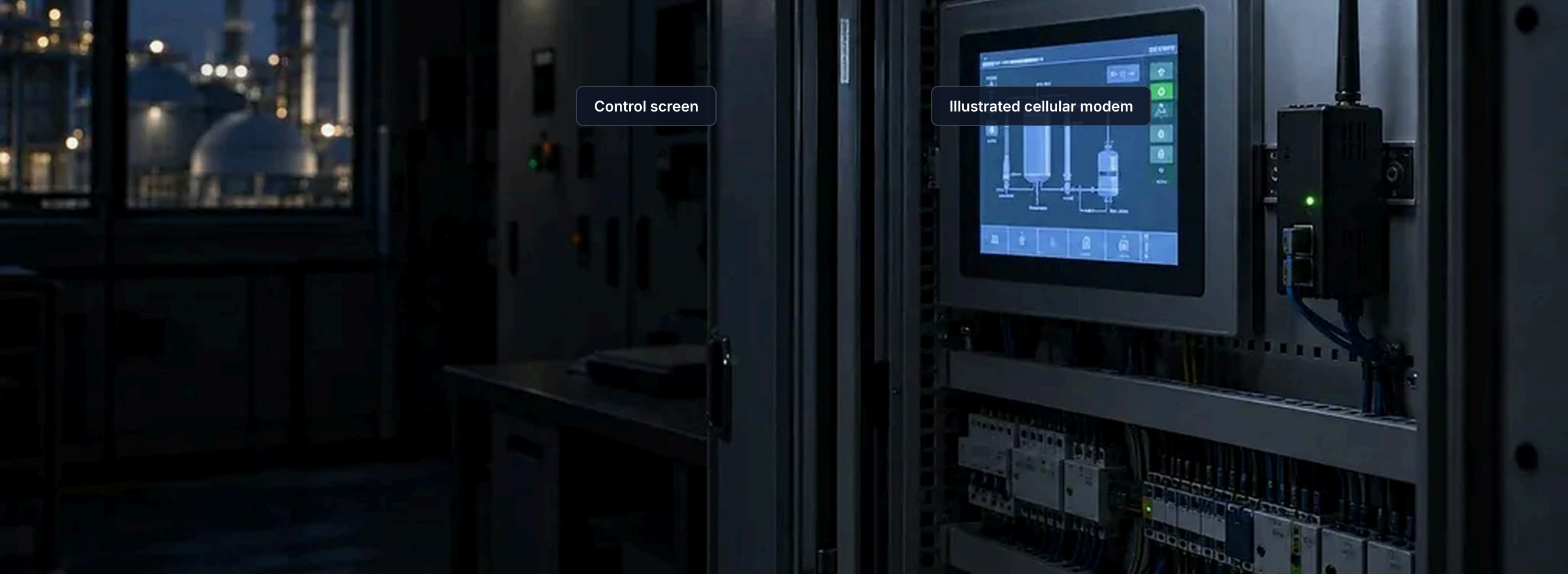
Who owns the modem?

Ask three teams who owns the 4G modem in the pump room. IT says facilities. Facilities says the vendor. The vendor says it's yours now. Everyone is right. Nobody is watching.

That gap is where this book lives.

TRY THIS

Could your team name every device at one site with a cellular modem, an RFID reader, a wireless link or a built-in radio? If not, you just found your first blind spot.



Control screen

Illustrated cellular modem

CHAPTER 02

The Modem Nobody Listed

The connection nobody wrote down becomes the door nobody locks.

Illustrative installation. Verify the cable path, modem setup and owner on site.

OBSERVED

During an assessment at an energy campus, our team walked the site and found a 4G modem wired into a control screen. It gave that screen its own way to the outside world, one that never touched the site's network. A back door. On the same site, we also found remote-access tools open to the internet.²

We won't name the site, and we won't tell you more than we saw. The point is simple. The modem was there, and nothing on the network had flagged it.

How a modem ends up there

Modems like this usually show up for a good reason. A vendor wants to support equipment without sending a technician. A contractor needs remote access during commissioning. A remote site has no other way to report.

Then the project ends. The people move on. The modem stays. It keeps its connection, its default settings and its quiet path to the outside, long after anyone remembers why it's there.

One small modem. One unseen path.

It isn't only modems someone added

SOURCED

In 2025, Reuters reported that undocumented communication devices had been found in some solar power inverters, and cellular radios in some batteries.¹ Equipment can arrive with radios nobody wrote down.

Your inventory is built from what you bought and what you installed. A radio nobody listed isn't in it. You can't secure a connection you don't know exists.

| A firewall can't control a connection that never passes through it.

Not every modem is a threat

Plenty of radio links are legitimate. Some are essential. The question isn't whether the modem should exist. It's whether it's known, approved, owned, and limited to the job it was put there to do.

TRY THIS

Who approved the last cellular modem installed at your busiest site? Who would notice if it started acting differently tonight?



CHAPTER 03

Five Ways In Through the Air

The easiest way around your firewall may already be bolted to the wall.

YOUR FIREWALL CAN'T HEAR RADIO

Attackers don't need a new trick when an old door is open. In public reporting and in our own field work, the same five weak spots keep coming up. None of them needs an exotic attack. All of them can be fixed.

1. The factory password

A controller, camera, gateway or reader still uses the password it shipped with. Or one password covers the whole fleet. Anyone who knows the default knows the way in.

Safer: find it, give it a unique credential, and check the device still works afterward.

2. The screen anyone can reach

SOURCED

In July 2026, the FBI and EPA reported attacks on internet-facing controllers at water and wastewater systems in at least seven states. Some disrupted operations.³ That was an exposed-network problem, not a radio one. But the lesson travels: a control screen anyone can reach is an open door, however the path gets there.

Safer: remove direct exposure. Allow access only through approved routes.

3. The modem a vendor left behind

Remote support was set up for one project and never taken down. It still works. It still goes around your network.

Safer: give it an owner and a purpose. Remove what nobody needs. Limit what stays.

Old doors are the easiest ones to walk through. Nobody remembers to lock them.

4. The radio nobody watches

SOURCED

In April 2026, Toronto Police reported more than 13 million network disruptions linked to devices posing as cell towers.⁴ Phones are the obvious victims. But alarm panels, elevator phones and sensors that rely on cellular need a working radio link too.

A device that suddenly goes quiet, connects somewhere new or starts behaving differently is telling you something. If nobody is listening, nobody hears it.

Safer: learn what normal looks like for each device, and chase down the changes that matter.

5. The fix nobody checked

Someone blocks a suspicious connection in a hurry. The threat stops. So do the badge reads, the alarm reporting or the sensor data the operation runs on. Nobody notices until morning.

Safer: no fix is finished until two checks pass. The risky path is closed. The service still works.

Hear the signal. Prove the risk. Control the path. Then check the service.

TRY THIS

Which of these five are you least sure about at your most important site?

Hear. Prove. Control.

Three questions every leader should be able to answer about the air around one site.

Hear.

What's talking over the air at this site?

A record of the devices and radio activity in the areas we monitor, side by side with what's happening on the network.

Prove.

Which path could hurt access, alarms, safety or operations?

The evidence, the owner, what the device can reach, and a ranked plan.

Control.

Can we close one risky path without breaking the service?

Act inside your rules. Then record the security check and the service check.

Then check two things: the risky path is closed, and the service still works.

Listen Before You Touch

You can't protect a radio link by ignoring it.



Conceptual information flow, not a wiring diagram or product screenshot. Interfaces, radio types and coverage must be confirmed for each deployment.

Here's how Findavi listens at your site, in plain terms.

One box, two ways to listen

Findavi runs on a small appliance at your site.

- **The wires.** A network mirror port gives Findavi a passive copy of the traffic in the areas you approve. It listens. It never probes your devices.
- **The air.** Findavi connects to an RF switch, which picks up the Wi-Fi and RFID side of your site.

With both, your team sees the wires and the air of one site in one place. A badge reader or wireless device that shows up where none was listed stops being invisible.

| You can't secure what you can't hear. So listen first.

What it listens to

- **Cellular modems and routers.** When a controller, alarm panel or kiosk with a cellular modem is also on your network, Findavi sees it there. It alerts your team when the device drops off or acts differently, and it can cut the device off from the rest of your network.
- **RFID badges and door readers.** Findavi protects supported RFID systems and checks that real employee badges and tag reads keep working.
- **Wireless links and gateways.** The links that carry data from sensors, meters and building systems. Findavi learns their normal activity and flags new devices, connections and changes.
- **Wireless devices nobody listed.** Findavi flags Wi-Fi and RFID devices that show up where none were approved, including equipment missing from your inventory.

What it doesn't do

It doesn't jam. Findavi listens. It doesn't jam or block the radio signals your devices depend on.

It doesn't hear cellular. A modem that talks straight to a cell tower and never touches your network is out of Findavi's view. We say so up front. Then we find those modems the reliable way: we walk the site, check the hardware and give every modem an owner.

It doesn't see everywhere. Findavi hears the areas it's connected to. Range and radio types depend on the RF switch at your site. We confirm coverage during planning and tell you what's out of view.

It doesn't send your data away. Findavi's AI runs on the appliance itself. The network data it collects never leaves your site.

Listening finds what alerts miss

OBSERVED

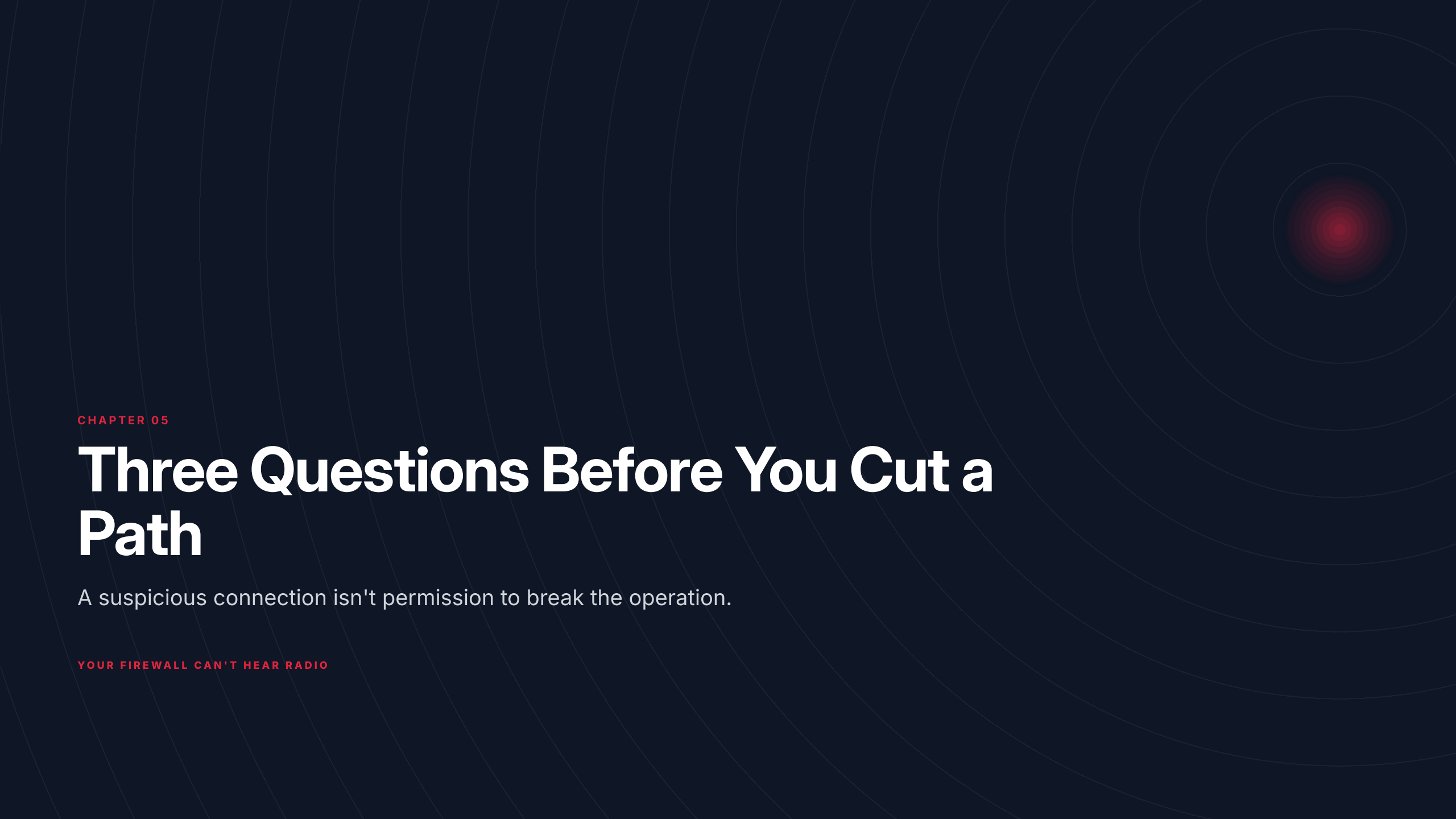
At a transport site we assessed, an unauthorized device scanned the network. The existing security tools raised zero alerts. Our assessment caught it.⁵

That was on the wires, where tools were already watching. Now ask who would notice something in the air.

Listen first. Learn what normal looks like. Change nothing until your team agrees on what matters.

TRY THIS

At one site, can your security, facilities and network teams look at radio activity and network activity in the same investigation?

The background features a series of concentric circles that originate from a point in the upper right quadrant. This point is surrounded by a red, glowing, concentric pattern, resembling a signal source or a target. The circles are thin and light gray, fading out as they move towards the left and bottom edges of the frame.

CHAPTER 05

Three Questions Before You Cut a Path

A suspicious connection isn't permission to break the operation.

YOUR FIREWALL CAN'T HEAR RADIO

When a radio-connected device does something strange at night, the instinct is to cut it off. Sometimes that's right. Sometimes it locks a door that needed to open, or silences an alarm that needed to ring. Ask three questions first.

1. What can it reach?

A control screen? The building management system? The access-control server? A vendor outside? The internet? A zone it has no business talking to? The more it can reach, the faster you move.

2. What depends on it?

A door or gate, a camera, an alarm, an elevator phone, a sensor, a controller, an RFID workflow, a remote site, an emergency process? The more that depends on it, the more careful you are.

3. Can we change it safely, right now?

Is this device and this action supported? Who owns the service? Is the device in Observe, Approve or Autonomous mode? What's the way back if something breaks? What has to keep working afterward?

Three modes. Your call.

- **Observe.** Findavi watches, learns and reports. It changes nothing. Most sites start here.
- **Approve.** Findavi recommends one specific action, with evidence. A named person says yes or no.
- **Autonomous.** For narrow situations you approved in advance, Findavi acts on its own, then runs both checks and reports.

A parking-lot camera might run in Autonomous. A badge reader on an emergency exit might stay in Approve for a long time. Both are good answers. You decide, device by device.

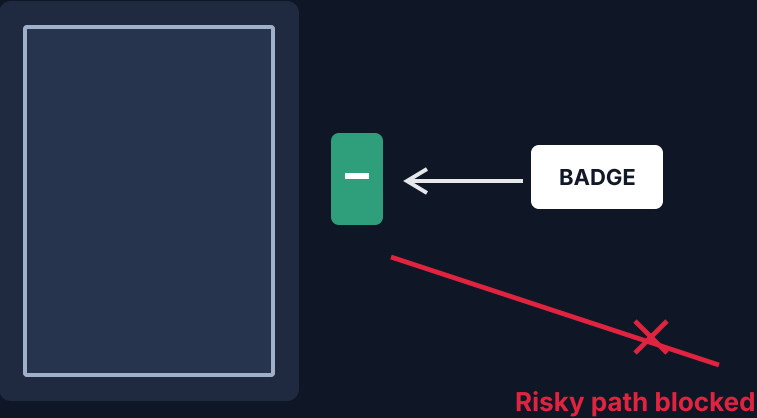
The right response is the smallest approved action that closes the risky path and keeps the service running.

TRY THIS

If a badge reader acted strangely tonight, who could approve a response?
And who would confirm the door still opens?

Close the Path. Keep the Door Working.

Contain the risky path, not the building.



Authorized access continues

Illustrated result only.
A live change needs both checks shown here.

SAMPLE EVIDENCE RECORD

Example scenario, not a measured result.

DEVICE / FINDING

Badge reader contacting an unapproved destination.

APPROVAL

The owner, the agreed change and the time it was approved.

SECURITY CHECK

The unapproved destination can't be reached.

SERVICE CHECK

A real employee badge still opens the door.

RECORD

Before and after evidence, time and the way back.

ILLUSTRATIVE

It's 11:48 p.m. The badge reader on a side entrance has a normal routine that Findavi learned over weeks: badge events, and conversations with one access-control server. Tonight it starts talking to an address it has never contacted.

- **Spot.** Findavi sees traffic outside the reader's normal pattern.
- **Check.** It looks up the device, its owner, the risk and the response rules your team approved.
- **Ask.** The reader is in Approve mode, so the on-call manager gets one narrow recommendation: limit the reader to its approved server.
- **Act.** She says yes. Findavi applies the supported action.
- **Check security.** The unknown address can no longer be reached.

- **Check service.** Real employee badges still open the door.
- **Record.** The alert, the approval, the action and both results are kept together for the morning.

Notice what didn't happen. Nobody jammed a radio. Nobody shut the building. One path closed, and the door kept working.

| **Closing the path is half the job. The door still has to open.**

Tested on an operator's equipment

OBSERVED

In a controlled demonstration on an operator's equipment, Findavi detected and stopped a test attack on the RFID system, then a separate test attack on heating and cooling controls.⁶ These were demonstrations, not live incidents. We report them as exactly that.

Every badge system is different

SOURCED

Wireless access deserves its own checks. Testing by Germany's ADAC shows that relaying the signal between some keyless cars and their keys can let a thief open and start the car.⁷ Badges aren't car keys, and badge systems don't all use the same protections. That's the point: each system has to be checked on its own. We confirm coverage for your readers, badges and setup before Findavi acts on them.

Two checks. Both must pass.

After this action	Security check	Service check
Restrict a badge reader	The unknown path can't be reached	Real badges still open the door
Remove an unneeded vendor modem	The unapproved remote access is gone	Required readings still report
Change a gateway's factory password	The old password no longer works	Sensor data still reaches its system
Isolate a remote sensor	It can't reach other zones	Monitoring and alarms still report

If either check fails, or can't be proven, the issue stays open.

When silence is the alarm

Sometimes the warning sign isn't a new connection. It's a missing one. An alarm panel that stops checking in. A sensor that goes quiet.

A quiet device isn't a fixed device. It may be the first sign you've lost the service it provides. Findavi alerts your team when a device drops off your network or its activity changes, so silence gets a human answer.

CHAPTER 07

Ten Minutes With Security and Facilities

The blind spot exists because the job is split.

YOUR FIREWALL CAN'T HEAR RADIO

Radio links fall between teams. Nobody did anything wrong. The org chart just has a gap in it.

Team	Usually cares about
Security	Exposure, unauthorized access, evidence
IT and network	Connectivity, segmentation, device identity
Facilities and engineering	Uptime, maintenance, service vendors
Physical security	Doors, readers, cameras, visitor access
Operations	Continuity, safety, response time

Put them in one room for ten minutes. Ask three questions.

- Which devices at this site use cellular, RFID or another radio?
 - Which of them would hurt access, alarms, monitoring or operations if they went quiet or acted strange?
- Who approves a response, and who confirms the service still works?

If the room goes quiet, you've found your blind spot. That isn't a failure. It's a starting point.

Start with one blind spot

You don't have to fix every site. Start with one area you can understand completely: one badge-reader environment, one group of cellular controllers, one remote site, one wireless sensor network, or the modems your vendors installed.

The Findavi RF Blind Spot Assessment listens through a passive network port and the RF switch, in Observe mode. Our team walks the site to find the modems Findavi can't hear. Nothing changes. At the end, you get:

- The devices, radio activity and modems we found in the area you picked
- Which ones are exposed, and why

- Who owns each one
- Prioritized findings and next steps
- The security and service checks each action would need

TRY THIS

Which one site would hurt most if its hidden wireless connections failed, changed or were used by someone else? Start there.

Something is listening.

ILLUSTRATIVE

Back to 4:12 a.m.

The pump controller was still talking, through a modem nobody had listed. But this time, someone was paying attention. Findavi saw the controller go quiet on the network and raised the alarm. Silence was the signal.

The engineer on call pulled up the record. The last walk-through had already found the modem. It was on the list, waiting for an owner.

She approved one narrow action: the controller could talk only to the operator's screen. The modem could still reach the controller, but nothing beyond it. Two checks ran. The path into the rest of the site was closed. The operator's screen still reached the controller.

Nobody drove two hours to a pump station. Nobody shut down the site. By morning, the modem had an owner, a reason and a ticket to remove it.

That's what good security sounds like. Quiet.

Your firewall can't hear radio. So make sure someone is listening.

Eldad Matityahu

Founder and CEO, NetOps IQ

SOURCES

Sources, by chapter.

NetOps IQ observations are anonymized. Customer names, device identifiers and dates are not published.

Chapter 2 / The Modem Nobody Listed

1. Rogue communication devices found in some Chinese solar inverters, and cellular radios in some batteries.

Reuters, May 14, 2025

<https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/>

2. Energy campus: a 4G modem wired into a control screen, found during a site walk-through, plus remote-access tools open to the internet. Anonymized site assessment.

NetOps IQ field results

<https://www.netopsiq.com/proof.html#additional-field-results>

Chapter 3 / Five Ways In Through the Air

3. Malicious cyber actors targeting internet-facing programmable logic controllers in the water and wastewater sector, causing operational disruptions.

FBI and EPA alert, July 2026

<https://www.fbi.gov/investigate/cyber/alerts/2026/malicious-cyber-actors-targeting-water-and-wastewater-sector-inter-net--facing-programmable-logic-controllers-causing-operational-disruptions>

4. Arrests linked to devices imitating cell towers; more than 13 million network disruptions. The figure counts disruptions, not individual victims.

Toronto Police Service, April 2026

<https://www.tps.ca/media-centre/stories/unprecedented-sms-blast-arrests/>

Chapter 4 / Listen Before You Touch

5. Transport site: an unauthorized device scanned the network while existing tools raised zero alerts. Anonymized NetOps IQ assessment.

NetOps IQ field results

<https://www.netopsiq.com/proof.html#additional-field-results>

Chapter 6 / Close the Path. Keep the Door Working.

6. Controlled demonstration on an operator's equipment: Findavi detected and stopped test attacks on an RFID system and on heating and cooling controls. Not live incidents.

NetOps IQ field results

<https://www.netopsiq.com/proof.html#rfid-hvac-demonstration>

7. Keyless-system testing: relaying the signal between some cars and their keys can let a thief open and start the vehicle.

ADAC, August 2026

<https://www.adac.de/rund-ums-fahrzeug/ausstattung-technik-zubehoer/assistenzsyste/keyless/>

START WITH ONE BLIND SPOT

Start with one blind spot.

Securing the air around every site starts with one area you understand completely.

The **Findavi RF Blind Spot Assessment** looks at one tightly scoped area. One badge-reader environment. One group of cellular controllers. One remote site. One wireless sensor network. The modems your vendors installed. You pick.

Findavi listens through a passive network port and the RF switch, in Observe mode, and our team walks the site to find the modems Findavi can't hear. It changes nothing.

At the end, you get a record of the devices, radio activity and modems in scope, which ones are exposed and why, who owns them, and a prioritized plan. For every action we propose, you get the security check and the service check that would prove it worked.

Then you decide what moves to Approve, and what might one day run in Autonomous.

NetOpsIQ™



Visit netopsiq.com

Scan or click

Request an assessment

netopsiq.com/assessment

info@netopsiq.com

The blind spot, secured.



netopsiq.com