

BOOK TWO | A LEADER'S GUIDE

When the Supply Chain Stops.

Securing the connected devices behind warehouses, distribution, and production.

Eldad Matityahu

Founder and CEO, NetOps IQ

Published September 7, 2026

ILLUSTRATIVE

2:17 a.m.



A camera in the loading yard starts talking to a stranger.

Forty trucks arrive at six.

CONTENTS

Inside

Nine short chapters. One idea: stop the attack without stopping the work.

A letter before we begin 4

01 The Warehouse Is a Computer Now 6

02 When the Shelves Start to Empty 9

03 The Real Cost Is the Work That Stops 13

04 Seven Doors Into the Operation 17

05 See Without Stopping the Shift 22

06 Three Questions Before You Touch Anything 25

07 Stop the Attack Without Stopping the Operation 28

08 The Cold Chain Can't Wait 33

09 Ten Minutes With the COO 36

A closing word 39

A LETTER BEFORE WE BEGIN

To the people who keep goods moving.

ILLUSTRATIVE

2:17 a.m.

A camera in the loading yard of a distribution center does something new. It has watched the same patch of asphalt for six years. Tonight it starts talking to a stranger on the internet.

That camera shares a network with the gate readers, the dock doors, and the system that tells forty trucks where to go at 6 a.m.

The person on call has one question to answer before sunrise. Can we cut this camera off without stopping the trucks?

Many companies can't answer it. Their people are smart. They just never got a map. Often, nobody knows what that camera can reach, who owns it, or what breaks if you pull the plug.

This book is for the people who keep goods moving.

Warehouses, distribution centers, and plants are now networks of connected physical systems. Security often sees only part of that environment, while operations depends on all of it working.

You'll meet four companies that lost weeks of business when their systems went dark: a grocery distributor, a retailer, a carmaker, and a medical supplier. None of these attacks is known to have started with a camera. They're in this book because of what happened next. The systems stopped. Then the trucks stopped. The shelves emptied. And the money walked out the door.

Then I'll show you how to find the quiet devices in your own operation, decide which ones matter, and shut down an attack without shutting down the shift.

One promise before we start. I'll always tell you what kind of evidence you're reading. You'll see three labels. Observed means we saw it ourselves in a NetOps IQ engagement, with the customer's name removed. A small number after a sentence means independent evidence, and the source is in the notes at the back. Illustrative means an example built to show how something works, like the camera above.

Let's go find your blind spots.

Eldad Matityahu

Founder and CEO, NetOps IQ

THE FOUR IDEAS THIS BOOK HANGS ON

Start with the trunk.

Every story and number in this book is a branch off four ideas. Hold these, and the details have somewhere to hang.

01 The warehouse is a computer you can drive a truck into.

Cameras, gate readers, RFID readers, scanners, and conveyor controls all have software, a login, and a network connection.

02 When a device belongs to four teams, nobody owns its risk.

Facilities, operations, vendors, and IT each hold a piece. Attackers live in the gaps.

03 The real cost is the work that stops.

The biggest losses come from trucks, shifts, and shelves standing still while the systems are dark.

04 Contain the device, not the building.

Cut off the one device. Then prove two things: the door is closed, and the work goes on.

How the book follows them. Chapter 1 shows the first two ideas. Chapters 2 and 3 show the third. Chapters 4 to 9 show the method that delivers the fourth, and what it's worth.

CHAPTER

01

The Warehouse Is a Computer Now

Hundreds of small machines run your building. Few people are watching them.



Walk into a modern distribution center and listen.

You hear forklifts. Conveyors. A truck backing up to dock seven. What you don't hear is the conversation happening over your head and under your feet. Hundreds, sometimes thousands, of small machines, talking all day long.

The camera over the dock door. The reader that opens the gate when a driver taps a badge. The RFID reader that counts every pallet that rolls past. The scanner in a worker's hand. The Wi-Fi access point bolted to a steel beam. The controller that runs the conveyor. The sensor that reports the temperature in cold storage. The heating and cooling system. The cellular modem a vendor installed so they could fix the dock doors from three states away.

Each one is a small computer. Each one has software, a login, and a connection to your network.

Twenty years ago, a warehouse was a building full of shelves. Today it's a computer you can drive a truck into.

Now the hard truth. Your security team didn't buy most of those computers. Facilities bought the cameras and the heating. Operations bought the scanners and the conveyor controls. A vendor installed the dock doors and kept a key to get back in. IT runs the network they all share. Four teams. Four budgets. Four sets of priorities.

Today it's a computer you
can drive a truck into.

When a device belongs to four teams, nobody really owns its risk. The gaps fall between them. That's where attackers live.

Your office security tools are nearly blind here. You can't install protection software on a gate reader. A conveyor controller doesn't send the kind of logs your security team reads every morning. Many of these devices can't be updated without a vendor visit and a weekend shutdown. Some can't be updated at all.

So they sit there. Always on. Rarely watched. Often on the same network as the systems that run your orders, your inventory, and your trucks.

I call this the warehouse blind spot. Many buildings that move goods have one. The only question is whether you find yours before someone else does.

Try this in your own operation. Could your team list every connected device in one building by tomorrow? Do you know who owns the dock doors, the gate readers, and the cold storage sensors from a security point of view? Do you know which of them can reach your warehouse management system?

OUT OF STOCK

CHAPTER

02

When the Shelves Start to Empty

A grocery giant took its systems offline. Then the shelves started to empty.



In June 2025, a New York grocery chain started running out of yogurt and sparkling water. A bakery couldn't get flour.

Their customers had probably never heard of the company behind the problem.

It was United Natural Foods, or UNFI. You may never have seen its name, but you've probably eaten food it delivered. It is the main distributor for Whole Foods and supplies thousands of other grocery stores across North America.

On June 5, 2025, UNFI spotted unauthorized activity on its computer systems. It did what a responsible company does. It took systems offline to contain the threat.¹

And then the trucks stopped making sense.

In its own filing, UNFI said the attack temporarily hurt its ability to fulfill and distribute customer orders.¹ Deliveries were missed. Stores and bakeries scrambled to find other suppliers.²

A month later, UNFI put a price on it. It expected to lose \$350 to \$400 million in sales that year.²

Think about that. The attackers didn't steal that money. It vanished because the business couldn't do its job while the systems were dark.

The attackers didn't steal that money.

That's this whole book in one story. A cyberattack turns into a supply chain problem the moment the systems that move goods go quiet. Ordering. Picking. Shipping. Receiving. When those stop, every truck, every worker, and every store down the line feels it.

One thing to be clear about. Nothing made public ties a camera or a gate reader to the UNFI attack, and I'm not claiming Findavi would have stopped it.

I'm telling the story because of what it shows. Security now has to reach past the office. Every device on the floor, every reader on the gate, every sensor in the cooler is part of the chain. If any link can be used as a way in, the whole chain can stop.

Try this in your own operation. If your ordering and shipping systems went offline tomorrow morning, how many hours could you keep trucks moving? Who would decide what to shut down, and how would they know what's safe to leave running?

UNITED NATURAL FOODS, 2025

Up to \$400 million.

The sales UNFI expected to lose in a single year after an attack forced it to take systems offline.

Source: UNFI earnings release, Form 8-K, July 16, 2025. Note 2.

CHAPTER

03

The Real Cost Is the Work That Stops

The biggest bill comes from the work that can't happen.

ORDERS SHIPPED



For 46 days, one of Britain's best-known retailers couldn't take a single online order for clothes.

It started on April 25, 2025. Marks & Spencer stopped taking clothing and home orders on its website and app after a cyberattack.³

Inside the company, people did what good people do in a crisis. They kept the business alive by hand. M&S switched to manual processes to keep stock moving. It worked, but it was slow and expensive. The company reported extra waste and logistics costs, and food shelves in some stores ran thin.⁴

Then came the bill. M&S expected the attack to cut about £300 million from its operating profit that year.⁴

Think about where that money went. Some of it went to investigators, lawyers, and consultants. But much of it was simply the work that couldn't happen. Orders nobody could place. Stock that sat in the wrong place. Food that spoiled before it reached a shelf. Hours of people doing by hand what machines used to do in seconds.

Running a business by hand is heroic. It's also a slow leak. It buys you days, not months, and every day costs more than the last.

A few months later, the same lesson hit a factory floor.

Running a business by hand is heroic. It's also a slow leak.

In late August 2025, Jaguar Land Rover was hit by a cyberattack. It shut down its systems and stopped building cars around the world. Its big UK plants went quiet. A company that normally builds about 1,000 cars a day built none. The shutdown lasted about five weeks.⁵

And the damage didn't stay inside the company. The smaller firms that make JLR's parts had nowhere to send them. The pain spread down the supply chain. An independent group, the Cyber Monitoring Centre, estimated the total hit to the UK economy at about £1.9 billion, affecting more than 5,000 UK organizations.⁵ That is an outside estimate, not a JLR number. JLR's own numbers were bad enough: a £485 million loss before tax and one-off items for July to September, plus £196 million in one-off costs from the attack.⁵

Five weeks. A thousand cars a day. More than five thousand organizations. That is what a stopped supply chain looks like. One company goes dark, and the suppliers, the workers, and the paychecks down the line go dark with it.

Most leaders are worried enough already. I share these stories for a different reason. They change the question your company should be asking.

The old question was: how do we keep attackers out of our servers?

The new question is: if something on our network is taken over tonight, can we stop it without stopping the operation?

The rest of this book answers it.

Try this in your own operation. If you had to run one building by hand tomorrow, which tasks would stop first? What would a day of that cost you? Do you know which connected devices those tasks depend on?

JAGUAR LAND ROVER, 2025

Five weeks.

A thousand cars a day, not built. More than 5,000 UK organizations hit.
An independent estimate of £1.9 billion in damage to the UK economy.

Sources: Cyber Monitoring Centre, October 22, 2025; PA Media, September 16, 2025. Note 5.

CHAPTER

04

Seven Doors Into the Operation

Attackers take the easiest way in. In most buildings, there are seven.



Attackers are practical people. They don't pick the hardest way in. They pick the easiest one. In a warehouse, a plant, or a distribution center, the easiest ways in tend to be the same seven doors. Here they are, with the answer to each.

Door one: the factory password. Cameras, gate readers, and controllers often still use the login they shipped with, or one password shared across a whole fleet. Attackers keep lists of these. The answer: know every device you have, give each one its own login, and get an alert when someone keeps guessing.

Door two: old software. Many floor devices run software that's years out of date, with weaknesses anyone can look up. Updating means a vendor visit and downtime, so it waits. The answer: track the software on every device, update what can reach important systems first, and fence off what you can't update yet.

Door three: one big flat network. The yard camera and the shipping system sit on the same network. Get into one, and you can see the other. The answer: separate the floor devices from the systems that run the business, and be ready to cut off a single device the moment it misbehaves.

Is the door closed? And does the device still do its job?

Door four: the vendor who never left. The company that installed your dock doors, conveyor, or refrigeration often keeps a permanent remote connection. Handy for repairs. Also an open door into your building, day and night. The answer: see every vendor session as it happens, allow it only when you've approved it, and question anything unexpected.

Door five: the control panel anyone can open. The setup page for a camera or controller is often reachable from the guest Wi-Fi, or even the internet. The answer: find every one of them and close it.

Door six: the radio nobody watches. RFID readers, handheld scanners, wireless links, and cellular modems all talk over the air. Most security teams rarely look at that traffic. The answer: treat wireless and radio links as part of your network, and watch them like you watch everything else.

Door seven: the fix nobody checked. This one is new, and it's the sneakiest. Your team changes a password or blocks a connection, and the attacker is out. Good. But nobody checked whether the scanner still scans or the gate still opens. Monday morning, trucks line up at a gate that won't move. The answer: every fix gets two checks. Is the door closed? And does the device still do its job?

Look at the pattern. Every answer comes down to three moves. **See** the device. **Prove** what risk it carries. **Control** it quickly, with a person in charge and proof that both the security and the service are intact. That's the method. The next three chapters show you how.

Try this in your own operation. Which of these seven doors would your team bet is closed in every building? Which one are you least sure about?

Seven doors in.

And how to shut each one.

01

The factory password

Give every device its own login.

02

Old software

Track it. Fix what reaches the most.

03

One big flat network

Separate the floor from the business.

04

The vendor who never left

See every session. Allow it on your terms.

05

The open control panel

Find them. Close them.

06

The radio nobody watches

Watch the airwaves like the wires.

07

The fix nobody checked

Check the door. Then check the device.

The method

**See. Prove.
Control.**

THE METHOD IN THIS BOOK

See. Prove. Control.

Three questions every operations leader should be able to answer.

See

THE LEADER'S QUESTION

What devices and connections are really on the floor?

WHAT FINDAVI DELIVERS

A live, listen-only map of every device and everything it talks to.

Prove

THE LEADER'S QUESTION

Which paths could stop shipping, safety, or temperature?

WHAT FINDAVI DELIVERS

Evidence, reach, ownership, and a plan ranked by impact on the operation.

Control

THE LEADER'S QUESTION

Can we cut off one device and prove the work goes on?

WHAT FINDAVI DELIVERS

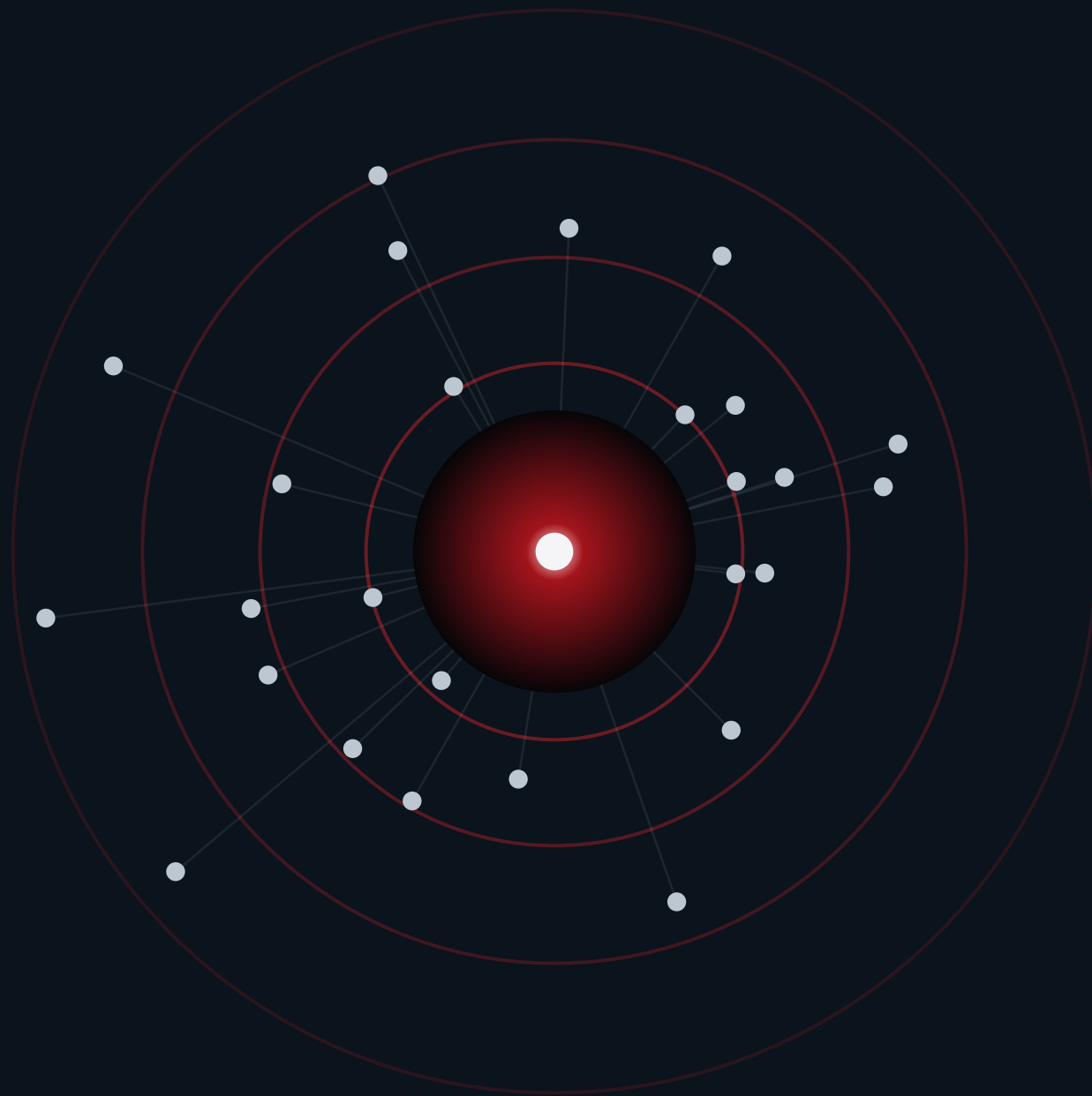
An approved action, a recorded decision, a security check, and a service check.

CHAPTER

05

See Without Stopping the Shift

You can't protect what you can't see. But looking too hard can break things.



ILLUSTRATIVE

It's the week before a holiday. The distribution center is running at full speed. Someone from security walks onto the floor and says, "We'd like to scan the network today."

The operations manager doesn't even look up. "Not this week."

She's right to say no. Some older or sensitive devices don't handle active scanning well. A scan can slow them down, confuse them, or in some cases make them restart. A frozen scanner in peak season is a missed truck.

That's the puzzle. You can't protect what you can't see. But looking too hard can break the very things you're trying to protect.

The answer is simple. Listen. Don't poke.

Every device in your building is already talking. The camera sends video to its recorder. The gate reader checks badges with a server. The RFID reader reports every pallet it counts. All of that traffic flows across your network all day long.

Listen. Don't poke.

If you connect a listening device to a special monitoring port on the network, you can hear all of it without sending a single thing to any device. Nothing gets scanned. Nothing gets probed. The shift doesn't notice.

From that traffic alone, you learn a lot. What each device is. Who made it. Often what software it runs. And most important of all, who it talks to.

That last part is where attacks give themselves away. A yard camera should talk to its video recorder, and that's about it. If it suddenly starts talking to the shipping system, or to an address on the other side of the world, something is wrong. You don't need a long list of known threats to spot that. You just need to know what normal looks like.

I'll be honest about the limits, because you should demand that of any vendor. Listening only shows you what crosses the part of the network you're watching. A device that stays silent can hide. That's why a good assessment starts with a clear scope, one building or one part of the network, and tells you exactly what it can and can't see.

This is how we built Findavi, our platform. It plugs into a monitoring port on your network and listens. It doesn't scan. It doesn't probe. The AI runs on a small box inside your building, and your data stays on your network.

What you get is something most operations have never had: a living map of every connected device on the floor that updates itself as things are added or moved. Spreadsheets go stale the week someone finishes them. This one doesn't.

Try this in your own operation. When was your last device inventory done, and how old is it now? Would your operations team agree to a method that only listens?

CHAPTER

06

Three Questions Before You Touch Anything

Hundreds of devices. One busy team. Three questions decide what comes first.

FIX FIRST

01

Can reach your order systems



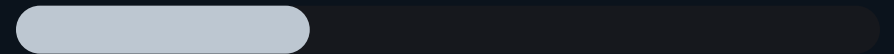
02

Stops shipping if it fails



03

Fenced in, low impact



The first time you see every device in a building, it's a shock. Hundreds of them. Some you didn't know existed. A long list of problems, and a team that's already busy.

The instinct is to sort the list by how scary each problem sounds. Resist it. A frightening technical label on a device that can't reach anything important is a distraction. A dull-sounding problem on the gate reader that controls your yard can cost you a day of shipping.

Instead, ask three questions about every device.

What can it reach? A camera that only talks to its own recorder is a small problem. A camera on the same network as your warehouse management system is a big one, because it's a stepping stone to the system that runs your orders.

What breaks if it fails? Follow the device to the work it supports. If the gate reader goes down, can trucks get in? If the RFID reader at dock four goes down, can you receive inventory? If the temperature sensor in cold storage goes quiet, would anyone notice before the product spoils? The closer a device sits to safety, shipping, inventory, or temperature, the higher it goes on the list.

A list tells you what's wrong. A plan tells you what to do on Monday.

Can we safely change it today? Some fixes take five minutes and nobody notices, like changing a factory password during a quiet hour. Others need the vendor, a part, and a weekend shutdown. A dangerous device with an easy, safe fix goes straight to the top. A lot of risk can disappear in the first week.

For the problems you can't fix yet, don't just leave them sitting there. Fence them in. If an old conveyor controller can't be updated until the next shutdown, limit it so it can only talk to the one system it needs. That buys you time without leaving the door open.

This is what we mean by **Prove**. You end up with a short, ranked plan, built on evidence from your own building, that says what to fix first and why. A list tells you what's wrong. A plan tells you what to do on Monday.

And it gives you something every operations leader needs: a reason your team can defend. When someone asks why you fixed the gate reader before the lobby camera, you can show them.

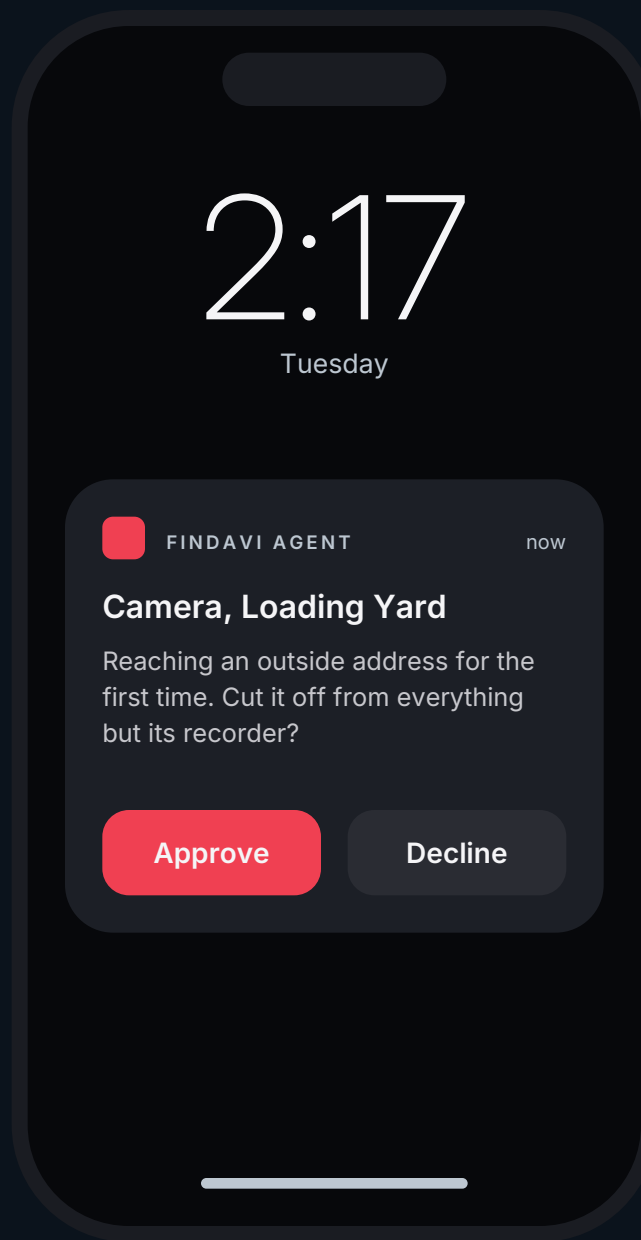
Try this in your own operation. Which five devices in your busiest building would stop the most work if they failed? Which of them could you safely improve this week?

CHAPTER

07

Stop the Attack Without Stopping the Operation

Stop the attack, and you stop the operation. Unless you can cut off just one device.



In May 2026, West Pharmaceutical Services faced the choice every leader dreads.

West makes components that drug and vaccine makers depend on. On May 4, the company detected an intrusion. Within days it knew data had been taken and some systems had been locked up by the attackers.⁶

So West did the responsible thing. It took systems offline around the world to contain the attack.⁶ That stopped the spread. It also meant manufacturing, receiving, and shipping had to restart site by site as systems came back. By May 20, the company said it was fully operational again across its manufacturing, supply chain, and commercial sites.⁷

West handled a hard situation well, and it was back to full operation in about two weeks. But look at the tool it had to reach for. When you can't tell which systems are safe, the safest move is often to pull the plug on everything.

That's the trade many companies are stuck with today. Stop the attack, and you stop the operation. Keep the operation running, and you leave the door open.

I started NetOps IQ to break that trade.

Let's go back to the camera in the loading yard. 2:17 a.m.

Contain the device, not
the building.

ILLUSTRATIVE

Findavi has been listening to that camera for months. It knows what normal looks like: video to the recorder, nothing else. Tonight the camera reaches for an outside address. That's new.

What happens next takes seven steps.

First, Findavi spots the change and checks it against what the camera has always done. Second, it checks your rules. Is this a device you've agreed can be isolated at night without a phone call? Third, if the rules say ask, it sends the on-call person a clear recommendation: cut this camera off from everything except its video recorder. One tap to approve.

Fourth, it acts. Fifth, it checks that the door is really closed, and the camera can no longer reach anything it shouldn't.

Sixth, and this is the step that often gets skipped, it checks that the camera still works. Is video still reaching the approved recorder? Is the yard still being watched? A fix that blinds your yard is just a different kind of problem.

Seventh, it writes everything down. What it saw. What it recommended. Who approved it. What changed. The proof that the path is closed. The proof that the service still works. And anything left to do in the morning.

At 6 a.m., the trucks roll in. Nobody on the dock knows anything happened.

That's the whole idea. Contain the device, not the building.

You choose how Findavi responds.

Observe: it finds problems and recommends what to do, without changing anything. Approve: a person says yes before each action runs. Autonomous: it acts only within the device types and actions your team approved in advance.

A word on what this takes, because you should hear it straight. Findavi can block a device, isolate a port, or push a configuration change. It does this only for the device types, models, and software versions we support, through integrations you approve, and under your rules. We confirm what's supported at your site before anything is switched on. Nothing happens without someone saying yes, or without a rule you approved in advance. And you can stop, undo, or switch off any agent at any time.

OBSERVED IN A NETOPS IQ DEMONSTRATION

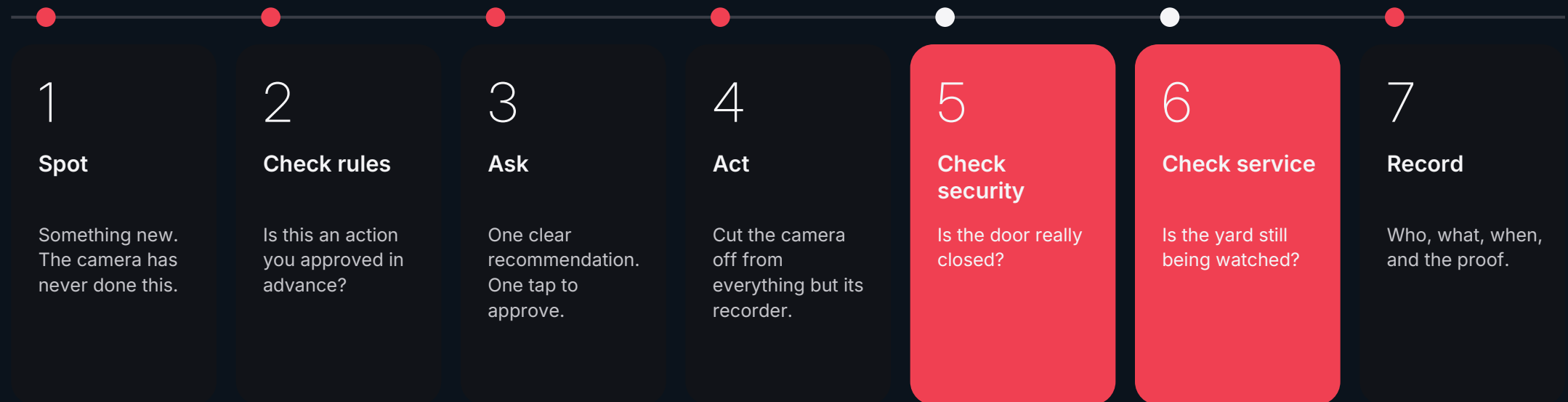
We have shown this in a controlled demonstration on a real operator's equipment. For a company that runs RFID infrastructure, Findavi detected and stopped a test attack on the RFID system, then a second test attack on the building's heating and cooling controls. These were demonstrations, not live incidents.

Questions for your team

If one device in your busiest building were taken over tonight, could you cut off just that device? Or would your only option be to shut down much more? Who would approve it, and how would you prove the operation still works?

Contain the device, not the building.

ILLUSTRATIVE: THE YARD CAMERA AT 2:17 A.M.



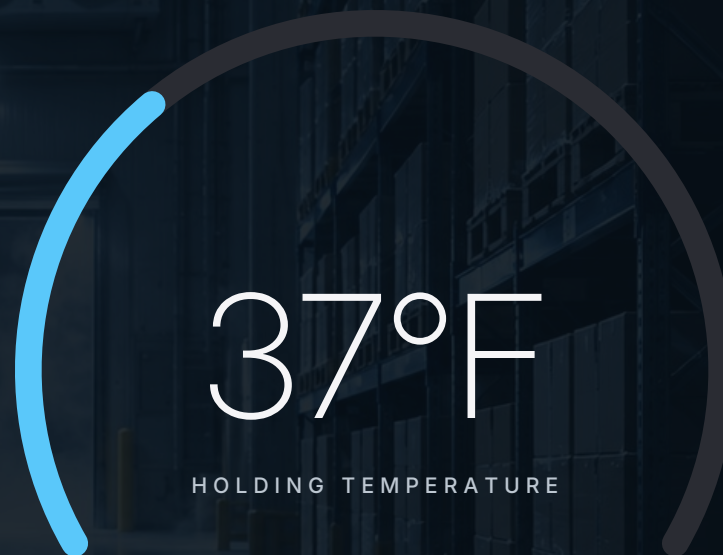
Two checks before the job counts as done: the door is closed, and the device still works.

CHAPTER

08

The Cold Chain Can't Wait

In a cold chain, closing the door is only half the job.



Path closed



Cooling still works

ILLUSTRATIVE

A refrigerated warehouse holds a full load of vaccines, or frozen food, or fresh produce headed to a few hundred stores. The product inside is only good as long as the temperature stays right. A few hours out of range can turn a truckload of value into a truckload of waste.

Now picture the sensors that report that temperature going quiet.

Maybe someone tampered with them. Maybe a well-meaning fix cut them off from the monitoring system. Either way, the screen in the control room still shows the last good reading. Everything looks fine. It isn't.

Cold storage is already a target. In April 2023, Americold, a major operator of temperature-controlled warehouses, found a cyberattack on its network and took operations offline to secure its systems.⁸ Nothing public says its cooling failed. But it shows that the buildings keeping food and medicine cold are on attackers' lists too.

Nothing shows the big idea of this book better than the cold chain. In most of security, closing the door is the finish line. In a cold chain, it's only half the job.

You've traded one problem for another, and this one melts.

Say Findavi spots something wrong with a refrigeration controller and, with your approval, cuts it off from everything it shouldn't be talking to. The attacker is out. Good. But the next question matters just as much. Is the controller still holding temperature? Are the sensors still reporting to the monitoring system? Will the alarm still sound if something drifts?

If the answer to any of those is no, you've traded one problem for another, and this one melts.

That's why Findavi checks each action twice: one for security and one for service. The path is closed, and the cooling, the monitoring, and the alarms all still work. Both have to pass before the job counts as done.

The issue stays open.

If we can't show the controller is still holding temperature, or that the monitoring system is still getting its data, the issue stays open. Cutting off the attacker is not the finish line.

The same goes beyond refrigeration. A pharmaceutical distributor, a food wholesaler, a biotech freezer farm. Anywhere the product depends on a controlled environment, the devices running that environment deserve the same attention as the computers in the office. Usually more.

Questions for your team

If the temperature sensors in your cold storage stopped reporting, how long before someone noticed? Do your security and facilities teams agree on who gets that call?

CHAPTER

09

Ten Minutes With the COO

The COO thinks in trucks, shifts, and service levels.
Speak that language.

01

Found

Facts from your building

02

Saved

Hours given back

03

Avoided

Downtime, estimated

The COO doesn't think in firewalls and passwords. The COO thinks in trucks, shifts, and service levels. So if you want ten minutes of real attention, speak that language.

Start with the stories. A grocery distributor that expected to lose \$350 to \$400 million in sales.² A retailer that ran on manual workarounds for weeks and expected to lose about £300 million in profit.⁴ A carmaker that stopped building cars for about five weeks, in an attack an independent group says cost the UK economy about £1.9 billion.⁵

Then bring it home. Ask the COO what one day of downtime in your busiest building would cost. Missed shipments. Trucks waiting at the gate. Workers standing idle. Food or medicine that spoils. Penalties in customer contracts. The customer who quietly moves to a competitor. Many COOs can answer that faster than their security team can.

Now show what you'd measure, in three levels, and be clear about which is which.

Level one is what you found. Hard facts from your own building. How many connected devices nobody had on a list. How many still had factory passwords. How many could reach the systems that run your orders. How many attack paths you closed, with proof they stayed closed.

Pick the spot that worries you most.

Level two is the time you saved. How many hours your team used to spend hunting for devices, chasing vendors, or checking alerts by hand, and how many it takes now. Multiply by what those people actually cost.

Level three is the downtime you avoided. This one is an estimate, so say so. Show your assumptions and let the COO challenge them. Being honest about this number is what makes the first two believable.

Then make one small, clear ask.

Findavi Operational Blind-Spot Assessment

A scoped, on-site assessment of connected devices, exposed paths, accountable owners, and supported response options.

Don't start with the whole company. Start with one place. One warehouse, distribution center, camera fleet, RF environment, or cold-storage zone. Pick the spot that worries you most.

We ship you a small box with Findavi already loaded. It plugs into a monitoring port, listens without touching anything, and keeps your data on your own network.

You get a report you can act on: every connected device we found, the paths an attacker could use, who owns each problem, what to fix first ranked by impact on the operation, the safe ways to fix it, and what the security check and the service check will each confirm.

That's it. One site, real evidence, and a plan your operations team can live with.

Questions for your team

Which single building would hurt most if it stopped for a day? That's your first site.

A CLOSING WORD

Forty trucks. Right on time.

Nobody on the dock knew anything had happened.

ILLUSTRATIVE



Go back to the camera in the loading yard. The one from the first page.

At 2:17 a.m., it reached for the outside world. By sunrise, it was cut off from everything except its own recorder, the yard was still being watched, and forty trucks rolled in on time. Nobody on the dock knew anything had happened.

That's the future I want for every building that moves goods. Attacks will still happen. But an attack on a single device stays a single-device problem.

The warehouses of the next ten years will run on even more machines talking to machines. Robots picking orders. Self-driving yard trucks. Sensors on every pallet. Every one of them will be either a helper or a way in. Someone has to make sure they stay helpers. That's why we built Findavi.

Security and operations both remain intact.

A supply chain does not stop only when a server goes down. It stops when the connected devices behind gates, docks, scanners, cameras, refrigeration, and controls cannot be trusted to keep doing their jobs. Findavi helps teams contain the specific exposure, under their rules, and prove that security and operations both remain intact.

You don't have to do it all at once. Start with one building. Find out what's really there. Then decide.

If you'd like help with that first step, I'd be glad to talk. e-Mail: info@netopsiq.com.

Eldad Matityahu

Founder and CEO, NetOps IQ

Sources, by chapter

CHAPTER 2

- 1 United Natural Foods detected unauthorized activity on June 5, 2025, took systems offline, and said the incident temporarily affected its ability to fulfill and distribute customer orders. [UNFI Form 8-K, June 2025](#).
- 2 Missed deliveries and shortages at a New York grocery chain and at bakeries; UNFI's estimate that the incident would cut fiscal 2025 net sales by about \$350 to \$400 million. [FOX 13 Tampa Bay, June 10, 2025](#). [UNFI earnings release, Form 8-K, July 16, 2025](#).

CHAPTER 3

- 3 Marks & Spencer paused online clothing and home orders on April 25, 2025 and resumed after 46 days. [Reuters via StreetInsider, June 10, 2025](#).
- 4 M&S's manual processes, additional waste and logistics costs, reduced food availability, and an estimated impact of around £300 million on Group operating profit for 2025/26 before mitigation. [Marks & Spencer Group plc, full year results, May 21, 2025](#).
- 5 UK production suspended for about five weeks, phased restart from October 8, 2025, and a modelled UK financial impact of £1.9 billion (range £1.6 to £2.1 billion) across more than 5,000 UK organizations. An independent estimate of the wider UK impact, not JLR's own loss. JLR's £485 million loss before tax and exceptional items for the quarter to September 30, 2025, and £196 million of costs relating to the cyber incident. Normal output of about 1,000 cars a day. [Cyber Monitoring Centre, October 22, 2025](#). [JLR Q2 FY26 results, November 14, 2025](#). [PA Media via Express & Star, September 16, 2025](#).

CHAPTER 7

- 6 West Pharmaceutical Services detected an intrusion on May 4, 2026, found that certain data was exfiltrated and certain systems encrypted, and took systems offline globally for containment. [West Form 8-K, May 11, 2026](#).
- 7 West reported that it was fully operational across manufacturing, supply chain, and commercial sites. [West Form 8-K/A, May 20, 2026](#).

CHAPTER 8

- 8 Americold began receiving evidence of a cybersecurity incident on April 26, 2023, and took operations offline to secure its systems. [Americold Form 8-K, May 1, 2023](#).

CHAPTER 9

Chapter 9 repeats figures from notes 2, 4, and 5.

All sources checked October 10, 2026. Red footnote numbers in the text link to the source.

TAKE THE NEXT STEP

Findavi Operational Blind-Spot Assessment

A scoped, on-site assessment of connected devices, exposed paths, accountable owners, and supported response options.

One warehouse, distribution center, camera fleet, RF environment, or cold-storage zone.

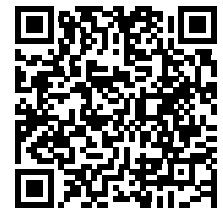
We ship you a small box with Findavi, our platform, already loaded. It plugs into a monitoring port, listens without touching anything, and keeps your data on your own network. You get a report you can act on: every connected device we found, the paths an attacker could use, who owns each problem, what to fix first, and how each fix will be checked for both security and service.

info@netopsiq.com

+1 (408) 621-5500

Listens only. On site. Your data stays home.

Scan to request
an assessment



The blind spot, secured.

NetOpsIQ™

FINDAVI PLATFORM



netopsiq.com
