

When the Water System Loses Sight.

How utilities can secure connected controls without interrupting essential service.

Eldad Matityahu

Founder and CEO, NetOps IQ

Published September 13, 2026





ILLUSTRATIVE

3:14 a.m.

A pump station controller gets a command it has never seen.

By sunrise, the town needs answers.

CONTENTS

Inside

Nine short chapters. One idea: cut off the attacker, keep the water flowing.

A letter before we begin 4

01 The Pump Station Nobody Was Watching 6

02 When the Operator Loses the Screen 9

03 Every Pump Has a Password 13

04 Five Doors Into the Control Room 16

05 See the Controller Without Touching It 21

06 Which Change Could Affect the Water? 24

07 Contain the Connection, Keep the Pump Running 27

08 The Alarm Has to Work Too 32

09 Ten Minutes With the Utility Board 36

A closing word 39

A LETTER BEFORE WE BEGIN

To the people who keep the water running.

ILLUSTRATIVE

3:14 a.m.

The pump station sits at the edge of town, behind a chain-link fence and a padlock. Nobody has been inside since Tuesday. Nobody needs to. A small computer runs it. It has run it for eleven years.

Tonight that computer gets a command it has never seen before.

The pumps keep humming. No siren. No smoke. Nothing a passing police car would notice. But by sunrise, someone in that town will need three answers. Is the water still flowing? Do the alarms still work? Does our operator still have control?

Many towns can't answer those questions fast. Their people are good. Their budgets are thin. And their pumps, valves, and tanks are spread across miles of quiet roads, each one watched by a screen that someone, somewhere, can reach.

Water is different from everything else in this series. You can delay a shipment. You can reschedule a surgery. You can't pause clean water. **Water has no undo button.**

In the summer of 2026, that stopped being a thought experiment. In one night, attackers reached more than 30 community water systems in a single state. Within days, the FBI and EPA warned that utilities in at least seven states had been hit. Some towns ran their plants by hand. Some issued boil-water notices.^{1 2}

This book is not about who did it. People are still arguing about that, and I'll leave the arguing to them. This book is about what a utility can do on its own equipment, starting tomorrow morning.

One promise before we start. I'll always tell you what kind of evidence you're reading. **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 pump station above.

Let's go find out who's really watching your pumps.

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 Water runs on small computers in places nobody visits.

Wells, pump stations, towers, and lift stations each have a controller, a screen, and a link back to the plant.

02 Remote access built a road from the internet to the pump.

Exposed screens, factory passwords, and vendor links left doors open, with a few busy operators to watch them.

03 Water has no undo button.

Shut down the wrong thing and you cause the outage the attacker wanted. Every fix has to be narrow.

04 Done means two checks pass.

The door is closed. The pump still answers the operator, and the alarm still sounds.

How the book follows them. Chapters 1 to 4 show the first two ideas. Chapters 5 and 6 show where the third one bites. Chapters 7 to 9 show the method that delivers the fourth, and what it's worth.



CHAPTER 01

The Pump Station Nobody Was Watching

A town's water runs on small computers in places
nobody visits.

Turn on your kitchen tap and think about what just happened.

Somewhere, a pump started. A valve opened. A sensor checked the pressure. Another one checked the chlorine. A tank on a hill sent its level back to a screen in a control room, maybe a few miles away, maybe in the next county.

You didn't see any of it. That's the point. Water is the one service we only notice when it stops.

Most people never picture this part. A town's water system is a scatter of small sites. Wells in a field. Pump stations by the road. Water towers. Lift stations that push wastewater uphill. A treatment plant in the middle of it all. Some systems have dozens of these sites, and a handful of operators to cover every one.

Each site has a small computer that runs it. A controller turns the pumps on and off. A screen lets the operator see the levels and change the settings. A modem or radio link sends it all back to the plant.

Twenty years ago, an operator drove to each site to check it. Today, most of that driving is gone. Remote access made the job possible with a tiny crew. It also did something nobody planned for. It made the pump station reachable from far beyond the fence.

The padlock still works. It just guards the wrong door.

The padlock still works. It just guards the wrong door.

And the people watching? They're the same few operators who are also fixing a main break, reading the meters, and answering the board's questions. Security is one more job on a list that was already too long. There's often no security team at all. There's Dave, and Dave is very busy.

That is the water blind spot. It's a missing pair of eyes.

The rest of this book is about getting those eyes back, without asking an exhausted crew to do more.

Try this in your own utility. Can you list every site where a controller or screen can be reached from outside the plant? Who would notice tonight if one of them started acting strangely?

When the Operator Loses the Screen

In July 2026, more than 30 Minnesota water systems were hit in one night.

On the night of July 26, 2026, a lot of small towns in Minnesota went to bed with working water systems. By morning, more than 30 of them had been hit.¹

Dozens of small break-ins, all in the same night.

In Braham, the attack shut down the operating controls and took the well and the water treatment plant offline. In Plymouth, it hit communications at two water towers and several lift stations. In South St. Paul, it reached the automated controls of the water system. In Maple Plain, the mayor declared a local state of emergency.¹

The good news came fast, and it matters. Officials said the drinking water stayed safe. No water advisories were issued. Braham's plant was back online and treating water by Monday morning.¹ Operators did what operators do. They got in their trucks and kept the water running.

But look at what they lost, even for a few hours. They lost sight.

Somebody walked in and changed the locks from the inside.

Four days later, the FBI and the EPA warned utilities across the country. At least seven states had reported attacks that week. The pattern was simple and ugly. Attackers found devices that could be reached from the internet. They changed the passwords. They changed the network settings. And the people who run the water lost the ability to monitor and control their own equipment.²

The FBI had a name for what that does to equipment: "a loss of view."² That's where this book gets its title. Notice how ordinary the rest of it sounds. The warning describes open doors and changed locks. **Somebody walked in and changed the locks from the inside.**

The federal warning said some of the activity degraded water operations. CISA said some of the larger attacks led to boil-water notices and sustained manual operations.² That means people in real towns boiled their water, and real operators ran their plants by hand, hour after hour.

That's the lesson of this chapter, and of the whole book. The scariest moment in a water attack often comes when the operator looks at the screen and can no longer trust it. Or can't reach it at all.

A quick word on restraint. Nothing public tells us which device or path was used in each town, and I won't guess. Nothing public names the attacker either, and that question has turned political. This book stays out of it. What matters for you is the pattern, because the pattern can reach any utility.

Try this in your own utility. If your operators lost every screen tonight, how long could you run every site by hand? Who would drive where first?

FBI AND EPA WARNING, JULY 30, 2026

"A loss of view."

What attackers caused at water utilities in at least seven states, by changing passwords and network settings on controllers they could reach from the internet.

Source: FBI and EPA Public Service Announcement, July 30, 2026. Note 2.

Every Pump Has a Password

The attack doesn't need to be clever when the door is open.



A water controller is built to last. Twenty years is normal. Some run longer than the careers of the people who installed them.

That's wonderful for the budget. It's terrible for security.

Think about the phone you carried in 2006. Now imagine it still runs part of your town, still on its original software, and still answers anyone who knows where to call. That's a fair picture of a lot of water equipment today.

Most of it was designed for a closed world. The controller talked to the screen. The screen talked to the operator. Nobody outside was supposed to be listening, so nobody built much of a lock.

Then the world opened up. A vendor needed to fix something without driving three hours, so a remote connection went in. A board wanted to cut overtime, so operators got access from home. A remote site had no cable, so somebody added a cellular modem. Every one of those choices made sense on the day it was made.

Together, they built a road from the internet to the pump.

Together, they built a road from the internet to the pump.

And at the end of that road, too often, sits a login that has never changed. The password it shipped with. Or one password shared across every site, written on a sticky note inside the control panel door, known to three retired operators and one vendor who went out of business.

Attackers know this. They don't need to be brilliant when the door is unlocked. They need a list of addresses and a little patience.

Small teams make it harder. A big city might have a security group. A town of 5,000 has an operator, a part-time IT contractor, and a vendor's phone number. Nobody is careless. Everybody is stretched.

So stop asking "Are we a target?" Everyone with a pump is. Ask a simpler question. How many of our doors are still open, and do we even know where they are?

Try this in your own utility. Which of your controllers and screens still use the password they shipped with? When was the last time anyone changed the shared one?

Five Doors Into the Control Room

Attackers take the easy way in. In water, there are five.

Attackers are lazy in the most practical way. They don't pick the hardest way in. They pick the easiest one. In a water system, the easy ways in tend to be the same five doors. These are the five, and how to shut each one.

Door one: the screen on the internet. An operator screen that anyone can reach from anywhere. It was set up for convenience, years ago, and nobody remembers it's out there. The answer: find every screen and controller that can be reached from outside, and take them off the open internet. If someone needs remote access, give them a locked, watched way in.

Door two: the factory password. The login the device shipped with, or one password shared across every site. The answer: a unique login on every device, changed when people leave, and an alert when someone keeps guessing.

Door three: the vendor who never left. The company that installed your controls kept a permanent connection to fix things from afar. Handy. Also open all night, every night. The answer: see every vendor session as it happens, allow it only when you've approved it, and close it when the work is done.

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

Door four: the radio at the remote site. Cellular modems and radio links connect the far-off sites. Many of them skip your network completely, so your network tools never see them. The answer: treat the airwaves as part of your network, and watch them the same way.

Door five: the fix nobody checked. This one surprises people. Your team changes a password or blocks a connection. The attacker is out. But nobody checked whether the alarm still reports or the tank level still reaches the screen. Next week, the tank overflows and nobody hears about it. The answer: every fix gets two checks. Is the door closed? And does the equipment still do its job?

Look at the five answers together and you'll see a pattern. **See** every device. **Prove** which ones put the water at risk. **Control** them quickly, with a person in charge and proof that the security and the service both work. That's the method. The next three chapters show how.

Try this in your own utility. Which of these five doors would your team bet is closed at every site? Which one are you least sure about?

Five doors in.

And how to shut each one.

01

The screen on the internet

Take it off the open internet.

02

The factory password

A unique login on every device.

03

The vendor who never left

See every session. Close it after.

04

The radio at the remote site

Watch the airwaves like the wires.

05

The fix nobody checked

Check the door. Then check the pump.

The method

See. Prove. Control.

THE METHOD IN THIS BOOK

See. Prove. Control.

Three questions every utility leader should be able to answer.

See

THE LEADER'S QUESTION

What controllers, screens, and links are really out there?

WHAT FINDAVI DELIVERS

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

Prove

THE LEADER'S QUESTION

Which paths could touch water quality, pressure, or alarms?

WHAT FINDAVI DELIVERS

Evidence, reach, ownership, and a plan ranked by what it means for the water.

Control

THE LEADER'S QUESTION

Can we cut off one connection and prove the pump still runs?

WHAT FINDAVI DELIVERS

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

See the Controller Without Touching It

In a water plant, a careless scan can do the attacker's job for him.

ILLUSTRATIVE

A security consultant walks into a treatment plant with a laptop and a big smile. "We'll just run a quick scan of the network."

The chief operator puts down his coffee. "Not on my plant, you won't."

He's right to say no. Some older controllers don't handle active scanning well. A scan pokes every device to see what answers. Most devices shrug it off. A few get confused, freeze, or restart. In an office, a frozen printer is a nuisance. In a water plant, a frozen controller can stop a pump.

In a water plant, a careless scan can do the attacker's job for him.

So how do you see what's on the network without poking it?

You listen.

Every device in a water system is already talking. The controller reports tank levels to the screen. The screen sends commands back. The remote site checks in with the plant. All day, all night, the network carries a running conversation.

You listen.

Connect a listening device to a monitoring port on the network, and you can hear that whole conversation without sending a single thing to any device. Nothing gets scanned. Nothing gets poked. The pumps never notice.

From listening alone, you learn a lot. What each device is. Who made it. Often what software it runs. And most important, who it talks to and how often.

That last part is where trouble shows itself. A pump controller should talk to its screen, and that's about it. If it suddenly starts talking to an address on the other side of the world, or takes a command at 3:14 a.m. that it has never taken before, something is wrong. You don't need a giant list of known threats to spot that. You need to know what normal looks like.

I'll be honest about the limits, because you should demand that from any vendor. Listening only shows what crosses the part of the network you're watching. A device that never talks can hide. A remote site on its own cellular link won't show up on your wired network at all. That's exactly why Door four matters. A good assessment starts with a clear scope and tells you what it can and can't see.

This is how we built Findavi. It plugs into a monitoring port and listens. It doesn't scan. It doesn't probe. Where your sites use radio or cellular links, it can watch those too, through an RF switch that connects it to the radio side of your sites. The AI runs on a small box inside your plant, and your data stays on your network.

What you get is something most utilities have never had: a living map of every controller, screen, and link, updated on its own as things change. The spreadsheet in the shared drive from 2019 can finally retire.

Try this in your own utility. When did anyone last list every controller at every remote site? Would your operators agree to a method that only listens?

Which Change Could Affect the Water?

Some fixes are free. Some could change the water.

The first time a utility sees every connected device across all its sites, the reaction is usually the same. A long silence. Then: "We have how many?"

Then comes the list of problems. Old software here. A factory password there. A modem nobody remembers buying. The instinct is to start at the top and fix everything, fast.

Resist it. In water, a rushed fix can hurt more than the problem it fixes.

Some changes are free. Changing the password on a screen that only shows reports, during a quiet afternoon, with the operator watching. Nobody notices, and the risk goes down.

Some changes can touch the water itself. Anything near chemical dosing. Anything near pressure control. Anything that decides when a pump runs or a valve opens. Get those wrong, and you can cause the very outage you were trying to prevent.

So before you touch anything, ask three questions about every device.

What can it reach? A screen that only displays levels is a small problem. A screen that can send commands to the pumps is a big one. Follow the wires and the radio links, and find out what an attacker could do from that device.

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

What happens to the water if it fails? Follow the device to the job it does. If this controller stops, does a tank overflow? Does pressure drop? Does a dose go wrong? Does an alarm go quiet? The closer a device sits to water quality, pressure, or public safety, the higher it goes on the list.

Can we change it safely right now? Some fixes take five minutes during a quiet hour. Others need the vendor, a maintenance window, and an operator standing next to the equipment. A dangerous device with an easy, safe fix goes straight to the top. A dangerous device with a hard fix gets fenced in first, so it can only talk to the one thing it needs, while you plan the real fix.

That's what we mean by **Prove**. You end up with a short, ranked plan built on evidence from your own system. A list tells you what's wrong. A plan tells you what to do on Monday, and what to leave alone until Thursday's maintenance window.

It also gives your operators something they deserve: a say. The people who run the water know exactly which changes could hurt the water. Their answer to question two is worth more than any score a tool can produce.

Try this in your own utility. Which five devices, if they failed, would affect water quality or pressure first? Which of them could you safely improve this week?

Contain the Connection, Keep the Pump Running

Cut off the attacker. Keep the water flowing.

When most organizations spot an attack, they reach for the biggest switch they have. Unplug it. Shut it all down. Sort it out later.

In an office, that works. Laptops can wait.

In a water system, the big switch has a cost. Shut down the controls and an operator has to drive to every site and run it by hand. Lose the screens and you lose sight of every tank and pump at once. Pull the plug in the wrong place and you can create the outage the attacker was hoping for.

So water needs a smaller, smarter move. Cut off the attacker. Leave the pump alone.

Let's go back to the pump station at the edge of town. 3:14 a.m.

ILLUSTRATIVE

Findavi has been listening to that controller for months. It knows the controller's normal day: level readings to the screen, commands from the plant, nothing else. Tonight, a command arrives from a connection it has never seen. That's new.

What happens next takes seven steps.

Contain the connection,
not the town.

First, Findavi spots the change and compares it with everything the controller has done before. Second, it checks your rules. Is this a device your team has agreed it can protect on its own, or does a person need to say yes? Third, if the rules say ask, it sends the on-call operator a clear message: block this connection and isolate the port it came through, and leave the controller running. One tap to approve.

Fourth, it acts. Fifth, it checks that the door is really closed, and the unknown connection can no longer reach the controller.

Sixth, and this is the step that matters most in water, it checks that the pump still works. Does the controller still answer the operator's screen? Are the tank levels still coming in? Does the pump still start when it should?

Seventh, it writes everything down. What it saw, what it recommended, who approved it, what changed, and the proof from both checks.

At 6 a.m., the town wakes up and turns on the coffee. Nobody knows anything happened. That's the goal. Contain the connection, not the town.

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.

For water, I'll be direct. Start with Observe or Approve. Keep Autonomous for narrow, low-risk actions your operators have signed off on, like blocking a connection that should never exist. Anything that could change how water is treated or moved should wait for a human.

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. Those changes cover the connections and devices around your controls, like passwords and network access. Findavi doesn't change how your pumps run. Process control and safety decisions stay with your operators and engineers. You can stop, undo, or switch off any agent at any time, and every action is recorded so you can audit it.

OBSERVED IN A NETOPS IQ PILOT

We have seen this work on real water equipment. During a pilot at a live water site, our team ran a simulated attack on the plant's controller screens. Findavi blocked the attacking connection and isolated the port it came through. Then it ran both checks. The door was closed, and the controls kept running for the operator the whole time. Both checks passed. This was a test during a pilot, not a real attack, and the site is unnamed.

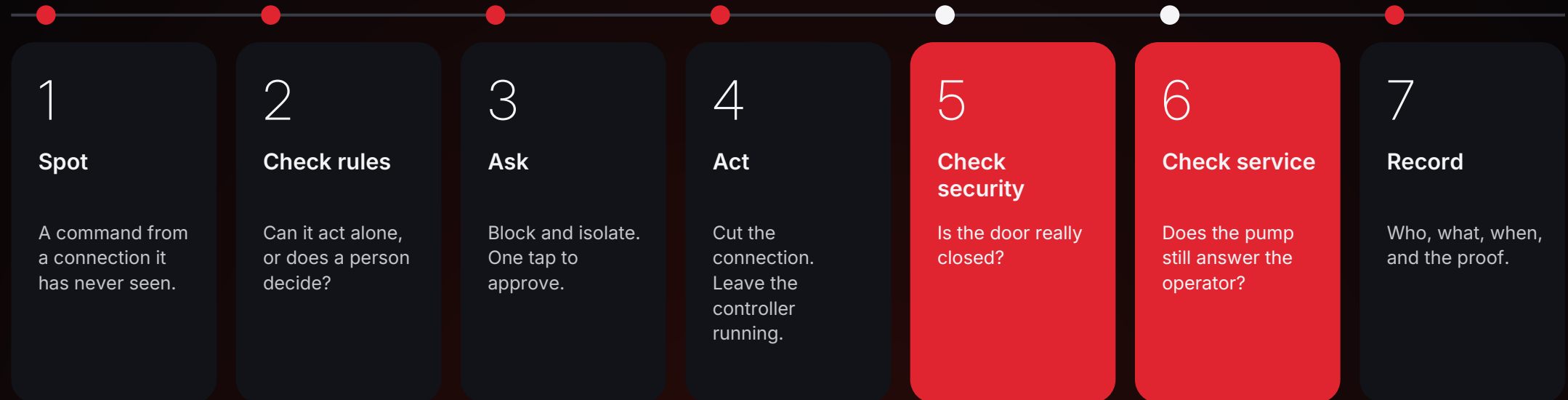
OBSERVED IN AN AUTHORIZED TEST, POWER GENERATION

In an authorized test at a power-generation facility, NetOps IQ recorded a blocked connection and an available camera feed. The notes do not confirm uninterrupted service or successful recording. This result covers the equipment and scope tested.

Try this in your own utility. If one controller were taken over tonight, could you cut off just that connection? Or would your only option be to shut down far more? Who would approve it at 3 a.m., and how would you prove the pumps still work?

Contain the connection, not the town.

ILLUSTRATIVE: THE PUMP STATION AT 3:14 A.M.



Two checks before the job counts as done: the door is closed, and the pump still answers the operator.

The Alarm Has to Work Too

Kicking out the attacker is only half the job.

An alarm is a promise. It says: if something goes wrong, you'll hear about it.

Now imagine someone quietly breaks that promise and doesn't tell you.

In late August 2026, attackers reached two small, privately owned water utilities in Colorado. Each one serves fewer than 200 people. According to the governor's office, the attackers changed equipment settings, disabled remote access and alarms, and changed the pumping cycles.³

The ending was a good one. The state said the disruptions were brief, and that there were no known impacts on water treatment, water quality, or public safety.³ Somebody noticed. Somebody fixed it.

But look at the list of what the attackers touched. Settings. Remote access. Alarms. Pumping cycles. Each one is a different way of losing sight. Change the settings, and the equipment does something the operator didn't choose. Kill remote access, and the operator has to drive out to see. Silence the alarms, and the system stops telling anyone when something drifts. Change the pumping cycles, and the water moves on someone else's schedule.

That's why, in water, kicking out the attacker is only half the job.

An alarm is a promise.

Say Findavi spots trouble at a pump station and, with the operator's approval, blocks the bad connection. The attacker is out. Good. Now the real questions start. Are the settings back to what the operator chose? Does remote access work for the people who should have it? Will the alarm sound if the tank runs low? Is the pump running on the right schedule?

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

If we can't show the alarm will still sound, or that the operator can still see and control the site, the issue stays open. Cutting off the attacker is not the finish line.

This is the same idea at the heart of this whole series, and water is where it matters most. An attack you stop but can't verify is just a quieter problem.

Try this in your own utility. When did someone last test that each alarm actually reaches a human? If an attacker silenced one tonight, how would you know?

COLORADO, AUGUST 2026

Alarms off.

Attackers changed settings, disabled remote access and alarms, and changed pumping cycles at two small water utilities. The state said water quality was not affected.

Source: Governor's office, as reported by Axios, September 18, 2026. Note 3.

Ten Minutes With the Utility Board

Boards think in safe water, steady service, and public trust. Speak that language.

A utility board doesn't think in ports and passwords. It thinks in three things: safe water, steady service, and the public's trust. If you want ten minutes of real attention, speak that language.

Start with the summer of 2026. More than 30 water systems hit in one state in one night.¹ Utilities in at least seven states reporting attacks within days, some running their plants by hand, some issuing boil-water notices.² Two tiny utilities with their alarms switched off.³ None of these were big cities. And that matters. Smaller systems often have the fewest people watching.

Then bring it home. Ask the board one question: what would a single boil-water notice cost us? Count the overtime for operators running sites by hand. The calls from residents. The local news crew in the parking lot. The questions from regulators. The trust that took years to build. Many boards can answer that faster than any security vendor.

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 system. How many controllers and screens could be reached from outside. How many still had factory passwords. How many remote sites talk over links nobody watches. How many doors 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 operators used to spend driving to sites, chasing vendors, or checking things by hand, and how many it takes now. Multiply by what those hours actually cost.

Level three is the trouble you avoided. This one is an estimate, so say so. Show your assumptions and let the board push back. Being honest about this number is what makes the first two believable.

And before anyone says there's no budget, check whether your state, your water association, or a federal program offers help paying for cybersecurity work. It's worth one phone call.

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.

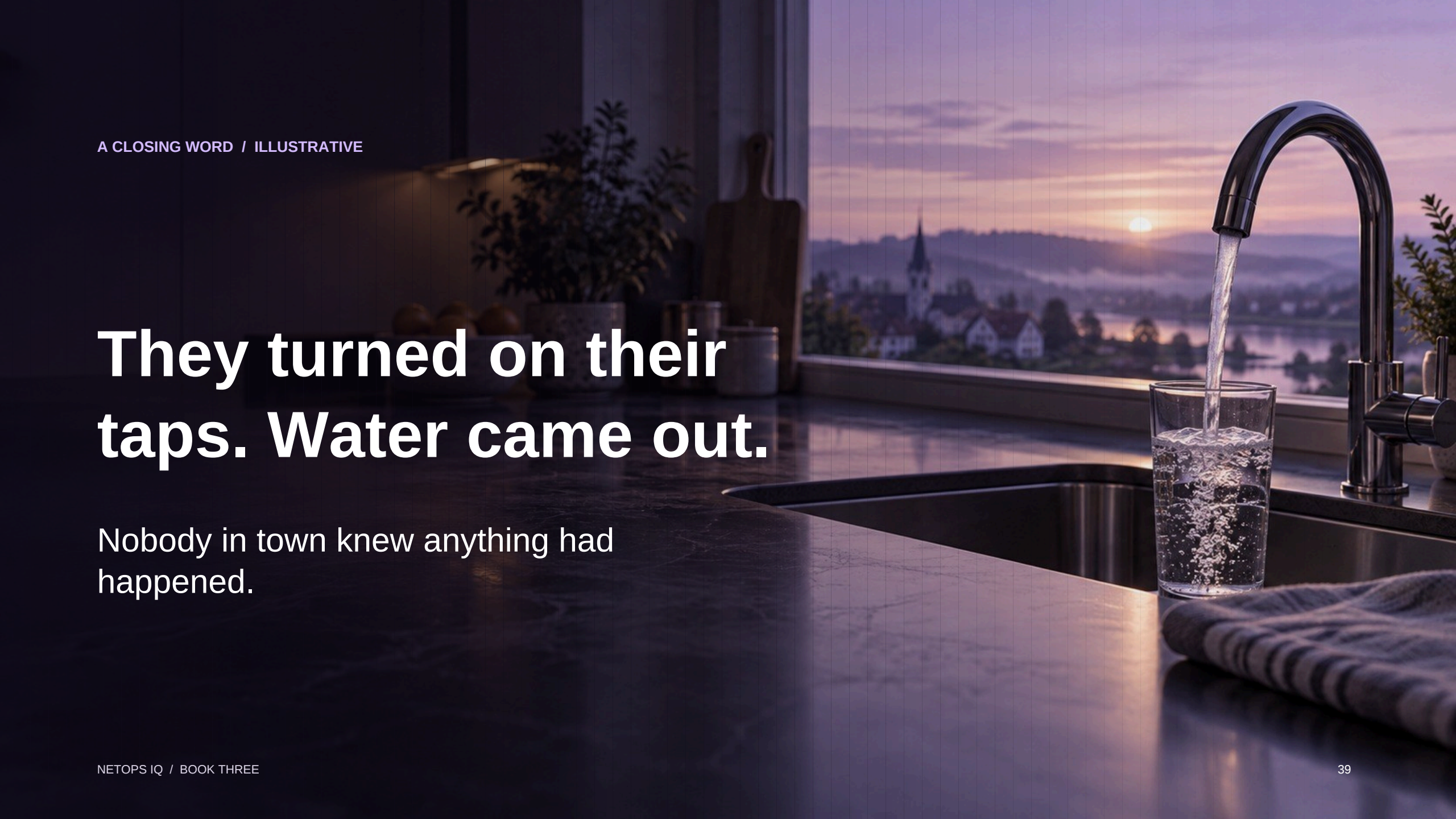
Don't start with the whole system. Start with one place. One treatment plant. One set of remote pump stations. One radio network. Pick the spot that worries you most.

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 what it means for the water, the safe ways to fix it, and what the security check and the service check will each confirm.

One site. Real evidence. A plan your operators can live with.

Try this in your own utility. Which single site would hurt most if your operators lost sight of it for a day? That's your first site.

A photograph of a modern kitchen sink with a sleek, curved faucet. Water is flowing from the faucet into a clear glass. The sink is set into a dark, polished countertop. In the background, a large window offers a view of a town at sunset, with a church spire visible on the horizon. A potted plant and a wooden cutting board are on the counter to the left of the sink.

A CLOSING WORD / ILLUSTRATIVE

They turned on their taps. Water came out.

Nobody in town knew anything had happened.

ILLUSTRATIVE

Go back to the pump station at the edge of town. The one from the first page.

At 3:14 a.m., a stranger tried to give it orders. By 3:20, that connection was cut off and the port it came through was closed. The pump kept running. The alarm still worked. The operator still had control. At sunrise, the night operator read the record over a cup of coffee and signed off on it.

Nobody in town knew anything had happened. They turned on their taps, and water came out. That's the best ending a water story can have.

That's the future I want for every utility. Attacks will still come. But an attack on one controller stays a problem with one controller, and the town never feels it.

A water system doesn't fail only when a server goes down. It fails when nobody can trust what the controllers are doing. Findavi helps utilities contain the specific threat, under their own rules, and prove that both security and service are still intact.

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

NOTES

Sources, by chapter

LETTER, CHAPTERS 2 AND 9

- 1 More than 30 Minnesota community water systems hit by a coordinated cyberattack on operational technology on July 26 and 27, 2026; the Minnesota Department of Health worked with the affected systems, with no requests for residents to change their drinking water use. Details for Braham, Plymouth, South St. Paul, and Maple Plain, and Braham's plant back online by Monday, from local reporting. [Minnesota IT Services release, July 28, 2026](#). [Valley News Live, July 28, 2026](#).
- 2 Since July 27, 2026, water and wastewater utilities in at least seven states reported incidents to the FBI, and some activity degraded water operations; actors remotely accessed internet-facing controllers and changed IP addresses and passwords, causing a loss of monitoring and control and "a loss of view, and in some cases function, of connected equipment." CISA said the activity "has resulted in boil water notices and sustained manual operations." [FBI and EPA PSA I-073026-PSA, July 30, 2026](#). [CISA alert, July 30, 2026](#).

CHAPTERS 8 AND 9

- 3 Two small privately owned Colorado water utilities, each serving fewer than 200 people, breached in late August 2026; attackers altered equipment settings, disabled remote access and alarms, and changed pumping cycles. Governor Jared Polis's office said disruptions were brief, with no known impacts on water treatment, water quality, or public safety, and state health officials confirmed the problems were resolved. [Axios Denver, September 18, 2026](#).

References dated through 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, listen-only assessment of connected devices, exposed paths, accountable owners, and supported response options.

Pick your first site: one treatment plant, one set of remote pump stations, or one radio network. 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.

A typical assessment takes a few days, depending on the size of the site.

e-Mail: info@netopsiq.com

+1 (408) 621-5500

Listens only. On site. Your data stays home.



**Request an
assessment**

Scan or click



The blind spot, secured.

netopsiq.com

