

The Green Light Has a Password

Securing the connected controllers behind
safe streets.



Eldad Matityahu

Founder and CEO, NetOps IQ

Published October 13, 2026



Thirty.

That's how many traffic signal controllers one security researcher found sitting on the open internet in 2024.

No password needed. Anyone who found one could change how long the lights stay green, load new settings, or throw the whole intersection into flashing red.

A city can cut those controllers off in a minute.

But will the intersection still work when it does?

Nine short chapters. One idea.

Close the unsafe path and keep the street moving.

A letter before we begin	04	6 Three Questions Before You Touch Anything	16
Start with the trunk	05	7 The Fix That Breaks the Street	17
1 The Street Has a Network	06	8 The Intersection Still Has to Work	20
2 A Computer With a Green Light	08	9 Ten Minutes With the Traffic Engineer	23
3 The Threat Had a Badge	10	Closing word. Back at Main and 5th	25
4 Six Doors Into the Intersection	12	Notes	26
5 Listen First	15		

A letter before we begin

To the people who keep traffic moving.

Nobody thanks a traffic light.

It turns green. You go. It turns red. You stop. The school bus gets through. The ambulance gets through. Nobody gives it a second thought, and that's exactly how it should be.

But the light on the pole is the simple part. The real work happens in a gray metal cabinet on the corner. Inside that cabinet is a computer. It decides who goes and who waits. It talks to the traffic center. It shares a network switch with cameras, radios and sensors. Many of them can be reached from miles away, so an engineer doesn't have to drive out to every corner.

That convenience is a gift. It's also an open door if nobody is watching it.

This book is about those cabinets and the computers inside them. It's for the people who answer for them: traffic engineers, IT and security teams, signal technicians, the contractors who maintain the gear, and the leaders who sign off on all of it.

It makes one promise. When something goes wrong at one controller, you should be able to shut down that one problem and leave the rest of the corridor running.

Then you should be able to prove two things. The unsafe path is closed. And the intersection still works.

Every story in this book carries one of three labels.

OBSERVED We saw it ourselves, at a real site, with customer details removed.

INDEPENDENT EVIDENCE It comes from a public record you can check in the notes.

ILLUSTRATIVE We built the scenario to show how a response works.

You'll find all three. You'll always know which is which.

Eldad Matityahu Founder and CEO, NetOps IQ

Four ideas hold this book up.

Remember these and the rest is detail.

1. A traffic signal is a computer standing on a street corner.
2. Whoever can reach the controller can run the intersection.
3. Flashing red is safe. The street still has to move.
4. Close the path. Keep the street moving.

Chapters 1 and 2 prove the first idea. Chapters 3 and 4 prove the second. Chapters 5 to 9 show the third and fourth at work.

01 The Street Has a Network



Kuan-yu Huang / Pexels · Illustrative photograph

The light is what you see. The computer is what runs it.

Next time you're stopped at a red, look at the corner. There's a gray metal cabinet, about the size of a refrigerator. Most people think it holds wires.

Open the door and you'll find a small data center.

The controller sits in the middle. It reads the sensors and decides when each light changes. Next to it is a network switch. A radio on the pole above links the cabinet to the next intersection, or back to the traffic center. A camera on the mast arm sends live video so engineers can watch the corner from their desks. Loops cut into the pavement, or video detectors, tell the controller a car is waiting. A receiver listens for fire trucks and ambulances so it can turn their light green.

And there's one more board, the quiet hero of the cabinet. It's a safety unit wired into the hardware. If the controller ever tries to give green to two directions that would collide, this board overrides it and drops the whole intersection into flashing red.

Count them up. Controller, switch, radio, camera, detectors, emergency receiver. That's six computers or more on one corner. Multiply by every signal in your city.

Now ask who owns them.

Traffic engineering owns the timing. IT may own the network, or may not even know it exists. Signal technicians own the hardware. A contractor installed half of it and still holds the passwords. The vendor has a remote login for support. Each one touches the cabinet. Nobody owns the risk of the whole cabinet.

That gap is where attackers like to work.

Ask your team: Could you list every connected controller, radio, camera and vendor login in one traffic corridor by tomorrow morning?

02 A Computer With a Green Light

If someone can reach the controller, they can run the corner.

A traffic controller has software, a login and a network connection. That makes it a computer. It just happens to run an intersection.

Researchers have shown what that means. Twice.

INDEPENDENT EVIDENCE

In 2014, a team at the University of Michigan worked with a road agency in Michigan that ran just under 100 traffic signals. With the agency's permission, they tested the system. The radios linking the intersections sent everything unencrypted. The radios, the network switch and the controller still used factory default usernames and passwords. From more than half a mile away, the team joined the network and changed the lights at a real intersection on command.



When they told the controller's maker, the company answered that it followed the industry standard, and that the standard didn't cover security.

In July 2024, a security researcher disclosed a flaw in one maker's line of traffic controllers. The controller's web page could be opened without a password. Anyone who reached it could change light timing, load new settings, or put the intersection into four-way flash. He found about 30 of these controllers reachable from the open internet. The maker said these were older products and asked customers to contact it for guidance. In April 2025, step-by-step instructions for the attack were posted publicly.

One caution. Neither record describes a criminal taking over a city's signals. Nobody has shown that anyone abused the 2024 flaw. What these records show is simple. The door was open, and the people responsible didn't know it.

There's good news too. Remember the safety board in the cabinet? The Michigan team found it did its job. It blocks any attempt to give green to two directions that would collide. So the movie version, where hackers turn every light green, mostly stays in the movies.

But the researchers found a catch. An attacker could trip that safety board on purpose from far away. The intersection would drop into flashing red. And it stays that way until a technician drives out and resets it by hand. Do that across a city at rush hour and you can break signals faster than crews can fix them.

Core idea: A traffic signal is a computer standing on a street corner.

Ask your team: Which of our controllers, radios or cameras can be reached from somewhere other than the traffic center?

03 The Threat Had a Badge

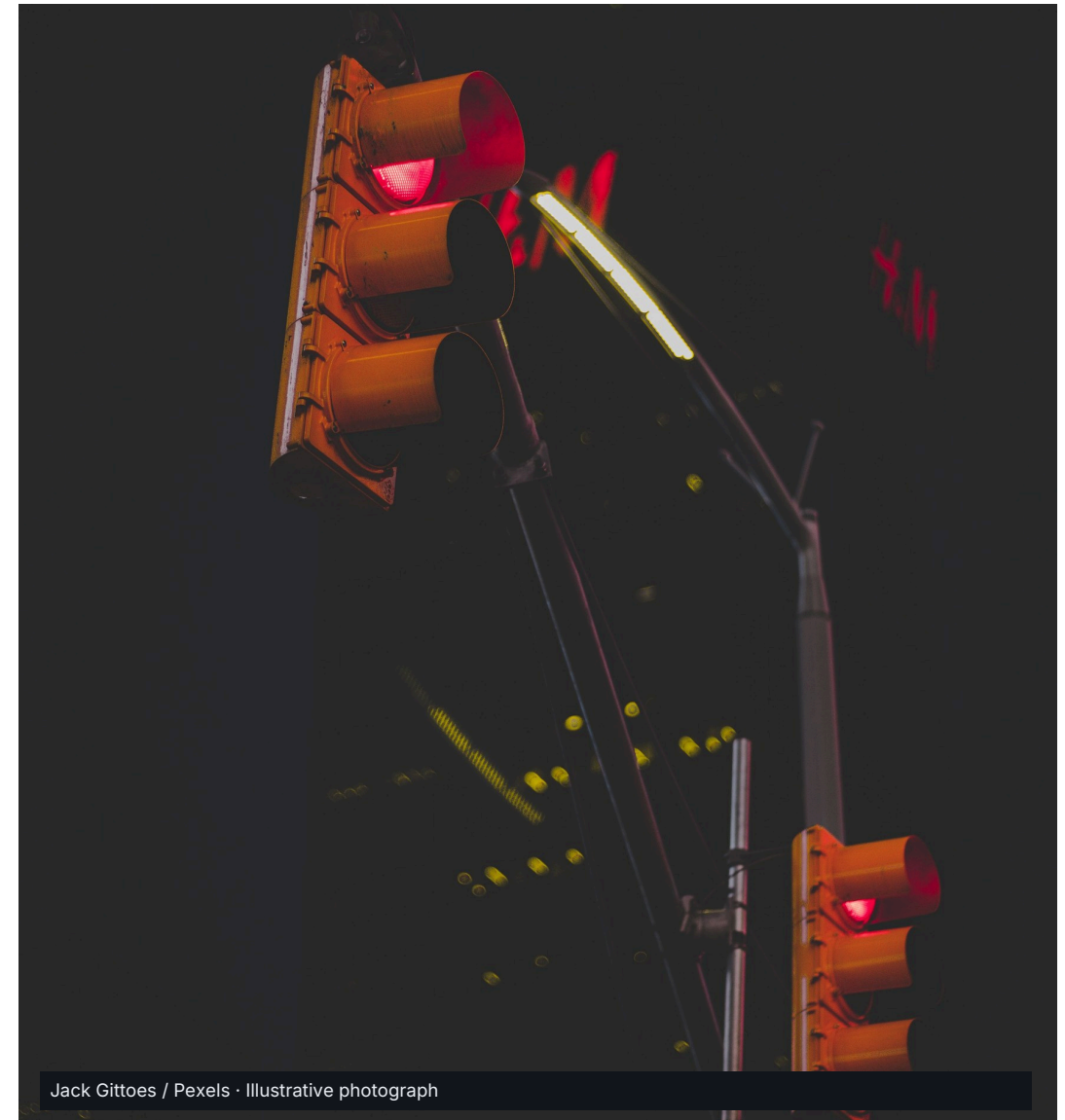
Sometimes the person with the keys is the problem.

Most people picture a stranger in a hoodie. One of the best-known traffic signal attacks on record came from inside the building.

INDEPENDENT EVIDENCE

In August 2006, the City of Los Angeles was bracing for a labor action by its traffic engineers. Managers planned to block engineers from making changes to the traffic system while it lasted.

It didn't work. On the night of August 21, hours before the action began, two senior engineers at the city's traffic control center logged in and sent commands that disconnected the signal boxes at four busy intersections. One was near Los Angeles International Airport. Prosecutors said the pair used a supervisor's login and changed the codes so nobody else could undo the damage.



It took four days to get the system fully working again. No accidents were reported. In 2008, both engineers pleaded guilty to a felony charge of illegally accessing a city computer.

No hacker broke in. No password was cracked. Two people with real access used it in a way nobody planned for.

Now look at your own corridor. Who can reach your controllers today? Your engineers, yes. But also the contractor who installed the new signals three years ago. The vendor with a support login. The technician who left last spring. The laptop that plugs into the cabinet on maintenance day.

Every one of those is a door. Some should be open. Some should have closed a long time ago. Most agencies can't say which is which, because nobody keeps that list in one place.

Core idea: Whoever can reach the controller can run the intersection.

Ask your team: If someone who left our agency last year still had a working login to our signal system, how would we find out?

04 Six Doors Into the Intersection

Attackers look for the device someone forgot to own.

An attacker doesn't need your best-protected controller. They only need the one nobody checked. Once they're on the signal network at one point, they may be able to reach every intersection on it. The Michigan researchers said it plainly: an attacker only has to beat the weakest link.

In a traffic system, there are six usual ways in.

Door	What it looks like	How you shut it
1. The factory password	A controller, radio or switch still uses the login it shipped with, or one login shared across the whole corridor	Give each device its own login, then check it still does its job
2. The open control screen	A controller's web page or management port can be reached from the internet or from a network that has no business seeing it	Close the outside access and allow only approved paths
3. The flat cabinet	The controller, camera, radio and every other device share one switch with no rules between them	Let each device talk only to what it needs

Door	What it looks like	How you shut it
4. The login that never left	A contractor, vendor or former employee still has working access	See every login and session, approve what's needed, remove what isn't
5. The radio nobody watches	Radio links between intersections, or cellular modems in the cabinet, carry traffic nobody inspects	Treat the airwaves around the corridor as part of the network
6. The fix nobody checked	A security change cuts off the attacker and also cuts the controller off from the traffic center, or trips it into flash	Require a security check and a service check before calling it done

The first five doors are about how attackers get in. The sixth is about how defenders hurt themselves on the way out. It's the one most agencies never measure.

Ask your team: Which of these six doors would you be least comfortable swearing is shut on every corridor?

See. Prove. Control.

Three questions every traffic leader should be able to answer.

Step	The leader's question	What Findavi delivers
See	What devices and connections actually run our intersections?	A listen-only map of the devices in scope and who they talk to
Prove	Which paths could change timing, knock out monitoring or break emergency priority?	The evidence, the owner, what each device can reach and a ranked plan
Control	Can we close one dangerous path and prove the intersection still works?	An approved action, a record of the decision, a security check and a service check

05 Listen First

Poke an old controller too hard and you can knock out the corner you came to protect.

ILLUSTRATIVE

The security team wants to scan the signal network to see what's on it. The signal operations manager asks one fair question.

"What happens if a controller doesn't like being scanned?"

Nobody in the room has a good answer.

She's right to ask. Many controllers in the field are ten or twenty years old. They were built to run lights, not to handle a flood of probes from a security tool. An aggressive scan can freeze one, or trip it into flash. The very act of checking for risk becomes the risk.

So Findavi starts by listening.

The Findavi appliance sits where your signal network comes together, often at the traffic center, and connects to a port that copies the network traffic you approve. It sends nothing to your controllers, radios or cameras. It hears what they already say to each other every day and builds a picture from that.

From listening alone, it can tell a lot. Which devices are on the network. What they are. Who each one talks to. Which ones still use default logins or send passwords in the clear. Which ones can be reached from places they shouldn't. Which ones are suddenly talking somewhere new.

The AI that does this runs on the appliance itself. No outside AI. The network data never leaves your agency.

The Findavi appliance can hear the radio too. Connected to an RF switch, it can watch wireless activity in range of that switch.

One honest limit. Findavi sees only the parts of the network it's connected to. A corridor whose traffic never passes the appliance is still invisible. Every assessment says plainly what it covered and what it didn't.

Coming next: a guard inside the box. We're building a small sensor that sits in the signal cabinet itself and watches the controller's traffic right at the corner. It only listens. It can't send commands, change settings or block anything, so it adds no new way in.

Ask your team: When did someone last check our list of controllers, radios and cameras against what's actually plugged in?

06 Three Questions Before You Touch Anything

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

The first look at a signal network usually turns up a long list. Default logins. Old firmware. A contractor account nobody remembers. A camera that can reach the internet. A radio link with no encryption.

The list feels urgent. It's also useless until you decide what comes first. Severity scores help, but they don't know your streets. A critical flaw on a controller at a quiet rural crossing can wait a week. A medium flaw on the controller outside the hospital can't.

Three questions sort the list.

1. What can it reach?

Can this device reach the traffic center? Other intersections? A vendor's network? The internet? A device that can reach the whole corridor moves to the top. A device boxed into its own corner moves down.

2. What breaks if it fails?

Would a busy corridor drop into flash at rush hour? Would fire trucks lose their green light? Would a school crossing stop working? Would the traffic center go blind on a dozen intersections? The bigger the answer, the more care the fix needs.

3. Can we change it safely today?

Is the fix one Findavi supports for this device? Has the traffic engineer said yes? Is there a quiet window, say two in the morning, to make the change? Is there a way back if it goes wrong? Do we know exactly how we'll check that the unsafe path is closed and the intersection still works?

If any answer is no, the fix waits. The device can still be watched and walled off in the meantime.

Core idea: Severity tells you something is wrong. What breaks if it fails tells you what comes first.

Ask your team: Which five intersections would cause the most trouble if their controllers went dark today?

07 The Fix That Breaks the Street

Shut down the problem. Keep the corner running.

ILLUSTRATIVE · A COMPOSITE SCENE, NOT A REAL EVENT

School just let out. A mom in a gray minivan waits at Main and 5th. Behind her, a fire truck is trying to get through.

The light goes red. Then all four directions start flashing.

Nobody hacked anything to make it happen. Somebody fixed something.

Ten minutes earlier, the city's security team found a controller at that corner talking to the open internet. They did the right thing. They cut it off.

They cut off a little too much. The controller lost its link to the traffic center and fell back to flashing red, in every direction, at the busiest hour of the day.



Yura Forrat / Pexels · Illustrative photograph

The security ticket says: Resolved.

The street says otherwise.

So two people stand in the same room and ask two different questions.

The security lead asks: "Is the door closed?"

The traffic engineer asks: "Is the street still working?"

Most tools only answer the first one.

OBSERVED · CUSTOMER DETAILS REMOVED

This book has no traffic agency result to share yet. The closest proof we can publish comes from another place where a controller runs something people depend on: a water plant.

During a pilot at a live water site, the team ran a simulated attack on the screens operators use to control the plant. Findavi blocked the attacking connection and isolated a port. Then it ran two checks. The way in was closed. And the controls kept running for the operator.

The attacker lost. The plant never stopped.

Seven steps, every time

1. Spot. See behavior that doesn't fit the device.

2. Check the rules. Is this action allowed for this device, at this time?

3. Ask. If a person must approve, send one clear recommendation and wait.

4. Act. Block the device, isolate a port, push a configuration change, or push a block rule to your firewall, for supported devices only. Findavi never writes new signal timing.

5. Check security. Test the path again. Is it closed?

6. Check service. Is the device still doing its job?

7. Record. Keep the finding, the approval, the action and both results in one place.

You decide how much Findavi does on its own

Observe	Approve	Autonomous
Findavi finds problems and recommends fixes. It changes nothing.	Findavi proposes the fix. A person says yes before it runs.	Findavi acts on its own, within limits your team set in advance.

You choose the mode for each device and each action. For signal controllers, we recommend starting in Observe or Approve. Your team can stop or switch off any Findavi agent at any time, and every action is recorded.

Core idea: Close the path. Keep the street moving.

Ask your team: If one controller acted strangely tonight, could we cut off just that controller? Or would we have to take down the whole corridor to be safe?

08 The Intersection Still Has to Work

Blocking the attacker is only half the job.

Too many security teams call it a win the moment the bad connection is blocked. On a city street, that's halftime.

A controller can be safe and cut off from the traffic center. A camera can be locked down and no longer feed detection. An emergency receiver can be protected and no longer turn the light green for the fire truck. A radio link can be secured and the next three intersections can go dark.

Each of those failures is quiet. Nobody notices until someone needs the thing that broke.

So Findavi runs two checks after every action.

Device	Security check	Service check
Signal controller	The unapproved path is closed. The old login fails.	The controller still reports to the traffic center and runs its approved timing plan.
Detection camera	The risky connection is blocked.	Video and vehicle detection still reach the controller and the traffic center.
Emergency vehicle priority	The unexpected connection is closed.	A technician confirms a test call still turns the light green.

Device	Security check	Service check
Radio link or cellular modem	Unknown devices are off the link.	The link to the next intersection and the traffic center stays up.
Cabinet network switch	The risky port is isolated.	Every approved device in the cabinet still talks to what it needs.

Notice who does what. Findavi checks what it can see on the network: the path is closed, the controller reports in, the video arrives. Some checks need a person on the street. Only someone standing at the corner can confirm the fire truck got its green. Findavi records those checks too, and keeps the issue open until they're done.

If either check fails, the issue stays open. Somebody gets told. If Findavi made the move on its own, it undoes it on its own. Putting a controller's settings back always waits for a person. Nobody gets a green checkmark for a dark intersection.

Two checks. One human.

And if the service check fails?

Findavi shows your engineer what changed and what the last approved settings looked like. One person reviews it at the traffic center console. One person approves it. Then Findavi puts the settings back.

One honest limit. Findavi restores settings. It doesn't reinstall firmware. If the controller's own software has been tampered with, a restore won't clean it. That job belongs to your technicians and the equipment maker.

A human presses undo. Findavi makes undo possible.

You set the rules. Always.

Core idea: If the path is closed but the intersection isn't proven, the job isn't done.

Ask your team: After our last change to a controller or signal network, what proved nothing quietly broke?

09 Ten Minutes With the Traffic Engineer

He thinks in corridors, travel times and how fast the fire truck gets through.

The traffic engineer's questions are simple. Will the corridor run on plan at rush hour? Will emergency vehicles get their green? Will the traffic center see every intersection it's supposed to see? Will we be fixing a problem at two in the morning, or answering complaints at nine?

If you have ten minutes with him, talk in those terms. Then show results he can check, in three levels.

Level	What it shows
Found	Devices missing from the inventory. Default and shared logins. Controllers reachable from places they shouldn't be. Contractor and vendor logins nobody owns. Devices talking somewhere new.
Saved	Hours your team no longer spends hunting for devices, chasing vendors, driving to cabinets and checking fixes by hand, priced at your own labor rates.
Estimated	The disruption you likely avoided, with every assumption shown so your team can change it.

Keep those three apart. Found is measured. Saved is measured against your own numbers. Estimated is a judgment, and it should look like one.

Then make one small ask. Start with one corridor.

Pick the place where trouble would hurt most. The corridor outside the hospital. The route to the airport. The school zone. One radio network. One contractor's remote login.

The Blind Spot Assessment puts a Findavi appliance on that one part of your signal network and listens. At the end, your team gets five things.

1. A map of the devices in scope and who they talk to.
2. Evidence of each exposure, with an owner named for it.
3. A plan ranked by what breaks if each device fails.
4. The fixes Findavi can make under your approval rules.
5. The security check and service check for every proposed change.

Ask your team: Which single corridor would cause the biggest problem for the public if its signals failed for a day? Start there.

Back at Main and 5th

ILLUSTRATIVE

Same corner. Same school bell. Different ending.

Findavi spots the controller at Main and 5th answering to an address outside the city. It sends the on-call engineer one recommendation: block the outside path and turn off the controller's open web page.

She says yes.

The security check passes. The outside path is closed.

The service check fails. The controller stopped reporting to the traffic center.

Findavi flags it and shows her what changed. She checks it at the traffic center console and approves a restore of the last approved settings. The outside path stays blocked at the network. The controller reports in again.

Both checks pass. The lights stay on plan. The minivan goes. The fire truck goes.

The issue stays open, flagged for the team in the morning, so they can find a safer way to close that web page for good.

Nobody on that corner ever knows anything happened.

That's what good security looks like on a city street. The threat is contained. The proof is on record. And the light turns green when it should.



Kateryna Hnidash / Pexels · Illustrative photograph

Sources

All sources checked October 12, 2026.

OPENING AND CHAPTER 2

1. NIST National Vulnerability Database, CVE-2024-38944, published July 22, 2024. Unauthenticated remote access to a traffic controller's web interface. nvd.nist.gov
2. TechSpot, "Traffic light vulnerability could let hackers cause massive gridlocks, study finds," July 19, 2024. Around 30 exposed controllers found; the maker said the affected controllers had not been produced for almost 10 years and asked customers to reach out for guidance. techspot.com
3. Exploit Database, entry 52151, April 9, 2025. Public write-up of the attack, including changing light sequences and forcing four-way flash. exploit-db.com
4. Ghena, Beyer, Hillaker, Pevarnek and Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," USENIX Workshop on Offensive Technologies, 2014. Road agency with just under 100 signals; unencrypted radios; default credentials; remote light control demonstrated with the agency's cooperation; safety unit blocks conflicting greens but can be tripped remotely and needs a manual reset. usenix.org

CHAPTER 1

5. Same paper as note 4, section 2, for the parts of a traffic cabinet: controller, switch, radio, camera, detection and malfunction management unit.

CHAPTER 3

6. The Register, report on the charges, January 10, 2007. Charges, the supervisor login, and the four intersections. theregister.com
7. Planetizen, summarizing the Los Angeles Times, November 6, 2008. Guilty pleas to a felony count; four days to restore the system. planetizen.com

CHAPTER 7

8. Observed story: a NetOps IQ pilot at a live water site, simulated attack. Details confirmed by NetOps IQ's CTO. Customer details withheld.

CHAPTERS 5, 7 AND 8 (FINDAVI CAPABILITIES)

9. NetOps IQ, Findavi platform page: on-site appliance, AI on the box, supported actions, Observe, Approve and Autonomous modes, separate security and service checks. Settings restore and the cabinet sensor confirmed by NetOps IQ's CTO, October 2026. netopsiq.com

© 2026 NetOps IQ Inc. NetOps IQ™ and Findavi™ are trademarks of NetOps IQ Inc.

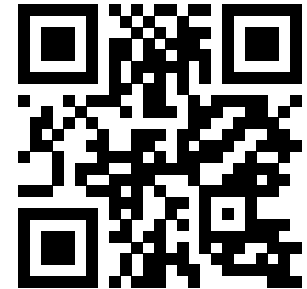
Pick your first corridor.

Start with one corridor, one controller fleet, one radio network or one contractor login.

Listens first. Acts only when you say. Your data stays on site.

You set the rules. Always.

netopsiq.com



The photographs.

Illustrative photographs. They do not show the reported attacks, Main and 5th, or a Findavi customer deployment. No endorsement is implied.

Traffic signals in rain

Blue Ox Studio / Pexels

Intersection light trails

Kuan-yu Huang / Pexels

Green signal hardware

Paul Lichtblau / Pexels

Red signals at night, New York

Jack Gittoes / Pexels

Emergency vehicle at night

Yura Forrat / Pexels

Pedestrians at a night intersection

Kateryna Hnidash / Pexels

Photographs used under the Pexels License. Each image appears once.

Close the path. Keep the street moving.



netopsiq.com