



BOOK ONE | A HOSPITAL LEADER'S GUIDE

The Blind Spot.

Securing the devices your IT security can't reach.

Eldad Matityahu

Founder and CEO, NetOps IQ

Published September 1, 2026



Eleven minutes.

That's all it took to almost reach the heart of a hospital.



CONTENTS

Inside

A letter before we begin 4

01 The Camera in the Ceiling 6

02 Eleven Minutes 11

03 This Was Never About Data. It's About Patients. 17

04 See: The Stethoscope, Not the Scalpel 22

05 Prove: Trade Your Hunch for Evidence 25

06 Triage: Chest Pain Before Sprained Ankles 28

07 Control: 2:47 A.M. 31

08 Where Does Our Data Go? 35

09 Ten Minutes With the Board 39

A closing word 44

To the people who keep hospitals running.

Eleven minutes.

That's how long someone spent trying to break into a hospital's network through a security camera, during one of our pilots, while doctors and nurses worked just a few feet away. This was a real attempt, not a drill and not a test.

Our system was only watching at the time. It saw every move. When the team switched our agents on, the attempt stopped cold at the camera. Doctors kept seeing patients. Nurses kept doing their rounds. Outside the security team, nobody ever knew it happened.

I think about that camera a lot. It wasn't on anyone's list of risks. Facilities had installed it years ago. The software inside it had never been updated. And it sat on a part of the network that everyone assumed was walled off from the clinical side. It wasn't.

That camera is what I call a blind spot. And here's the hard truth I've learned talking with hospital security leaders: most hospitals have far more of them than anyone realizes.

I started NetOps IQ because the security tools most hospitals own were built for laptops, servers, and the cloud. They do that job well. But the devices that actually run the building were left out. I mean the cameras, door readers, heating and cooling systems, nurse call, and asset trackers. They can't run security software. They rarely get updates. And very few people are watching them.

This book is for the person who has to answer for all of that. Maybe you're a CISO, a CIO, or the person in clinical engineering or facilities who keeps getting pulled into security meetings. You don't need another brochure. You need a clear way to think about the problem and a practical plan you can start on Monday.

That's what I've tried to write. I'll be straight with you throughout. When something has been measured, I'll say so. When something is an estimate, I'll show you how we got there.

How to read the evidence in this book. Every story and number here is one of three kinds, and I'll always tell you which.

Observed means we saw it ourselves in a NetOps IQ pilot or assessment, with the customer's details removed. A small number after a sentence means **independent evidence**, and you'll find the source in the notes at the back, listed by chapter.

Illustrative means an example scenario that shows how something works, not a report of a specific event.

Let's start by looking at the parts of your hospital that nobody is looking at.

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 building is the new front door.

Cameras, door readers, heating and cooling, and nurse call are all small computers sitting on your network.

02 Nobody owns them, so nobody watches them.

Facilities, vendors, clinical engineering, and IT each own a piece. The risk falls in between.

03 Every cyber risk is a patient risk.

When a device fails or gets taken over, a real person in a bed feels it.

04 See. Prove. Control. Then prove it worked.

Find every device, rank what matters, act with a person in charge, and confirm the door is closed and the device still does its job.

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

CHAPTER

01

The Camera in the Ceiling

The easiest way into your hospital might be hanging in the hallway.



Ask a hospital security leader how an attacker would break in, and most will mention a phishing email or a stolen password. Fair enough. But the attackers I worry about are looking somewhere else. They're looking up at the ceiling, at the little camera in the corner of the hallway. That camera might be the easiest way into your hospital, and there's a good chance nobody in IT has ever put it on a list.

Walk through any hospital and count what's connected. There's a camera in every hallway and parking level. There's a badge reader on every staff door. The heating and cooling system talks to a controller in the basement. Nurse call buttons sit beside every bed. Refrigerators in the pharmacy and lab report their temperatures. Tags on wheelchairs and infusion pumps tell staff where equipment is. Elevators, digital signs, and parking gates are all on the network too.

Each of these is a small computer. Each one has software inside it, a login, and a connection to your network. And almost none of them were bought by the security team.

The building has become
the new front door.

The math is uncomfortable. Your security program was built to protect the computers on desks. But in a modern hospital, a growing share of the computers sit in the walls, ceilings, and basements instead. Those are the ones nobody is watching.

That's the heart of the problem. In most hospitals, these devices are owned by several groups at once. Facilities installed the cameras. A vendor manages the building controls. Clinical engineering looks after anything near a patient. IT runs the network they all plug into. When a device belongs to four teams, ownership of its risk gets split four ways, and the gaps fall in between.

Your regular security tools can't help much here either. The protection software you put on laptops and servers can't be installed on a camera or a door controller. These devices don't send the logs your security team is used to reading. Many can't be patched without a vendor visit, and some can't be patched at all.

So they sit there, year after year, quietly connected. To an attacker, that makes them perfect. They're always on. They're rarely watched. And they often sit on the same network as systems that hold patient records or support care.

Picture a Friday morning in May 2021. It's five o'clock, and someone at Colonial Pipeline finds a ransom note on a company computer. Colonial carries about 45 percent of the gasoline the East Coast runs on. Within the hour, they shut the whole pipeline down.

The attackers never touched the pipeline itself. They logged in through an old remote access account that nobody was using anymore. It had no second check at the door, so one password was enough. When Colonial's CEO testified to the Senate a month later, he said the company still didn't know how the attackers got that password.¹ They only reached the office side of the network. But nobody could say for sure where the office ended and the pipeline began. So everything stopped.

For nearly a week, fuel stopped flowing. People lined up with gas cans. More than 9,500 gas stations ran dry, from Washington, D.C., to Florida. Colonial paid the hackers \$4.4 million.²

One password. One forgotten account. Nearly half the East Coast's gasoline.

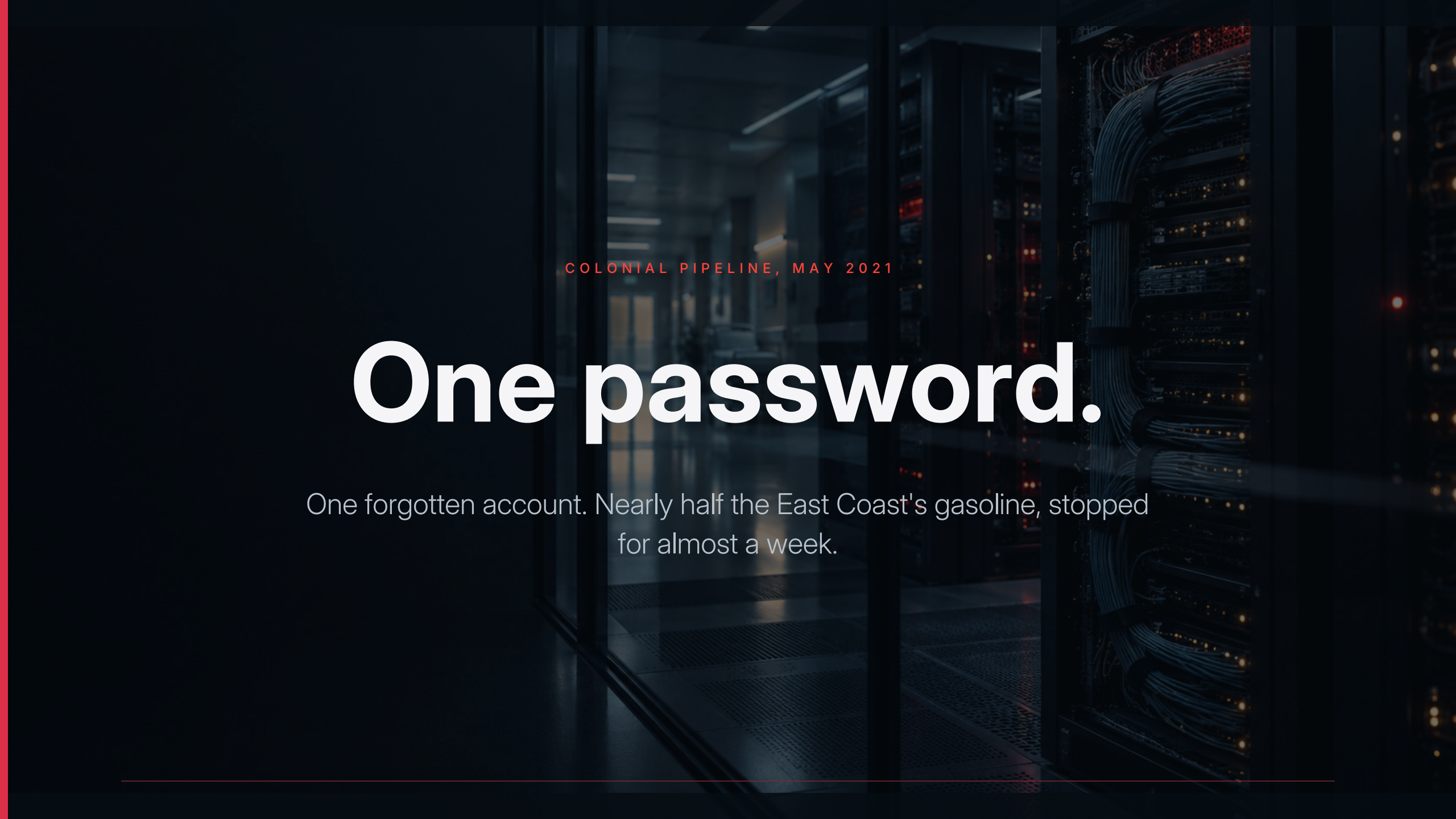
Now ask yourself the question I ask every hospital leader I meet. If someone broke into the office side of your hospital tonight, could your team say for certain where it ends and patient care begins?

I like to say the building has become the new front door. You've spent years putting strong locks on the main entrance. Meanwhile, the side doors were left open because nobody thought of them as doors.

Try this on your own hospital. Could your team produce a complete list of every connected device in your hospital by tomorrow? Do you know who owns the cameras and building controls from a security point of view? Do you know which of those devices can reach your clinical systems?

If any answer is "I'm not sure," you're not alone. Almost every hospital leader I talk to says the same thing. The rest of this book is about changing that answer.





COLONIAL PIPELINE, MAY 2021

One password.

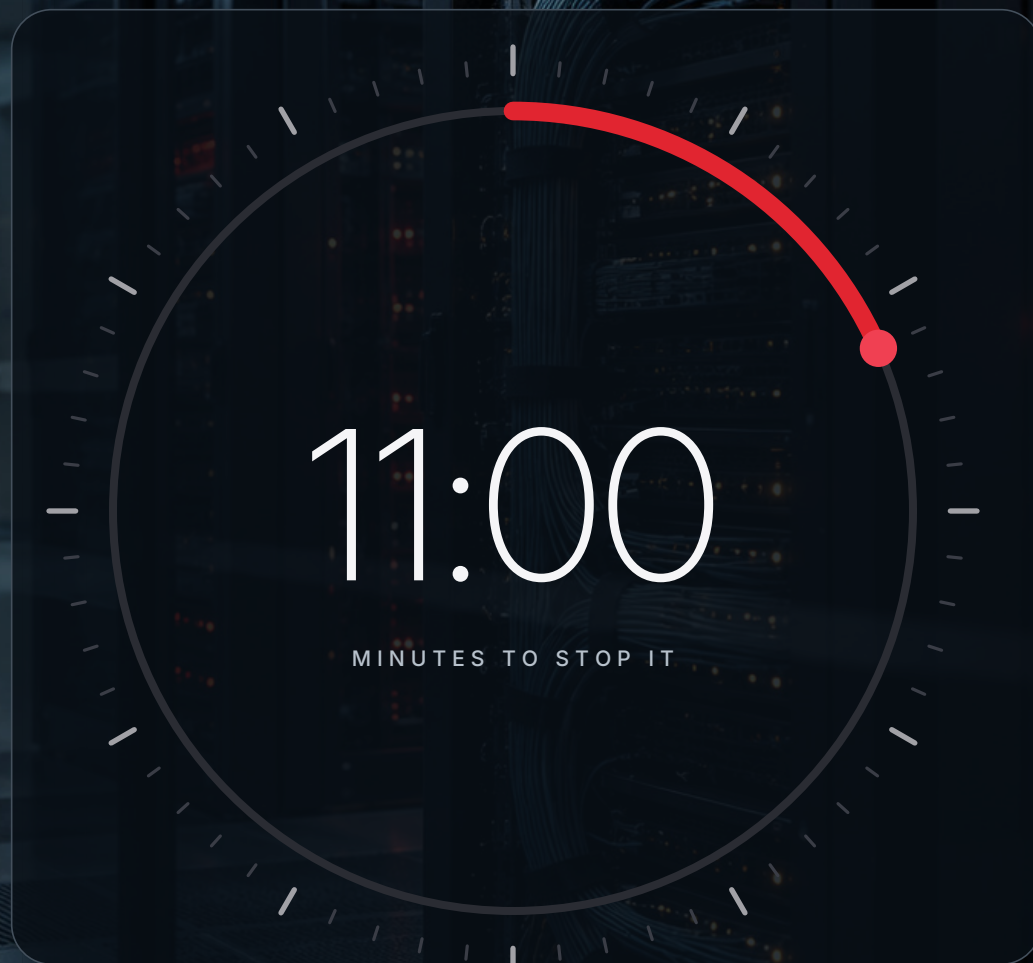
One forgotten account. Nearly half the East Coast's gasoline, stopped for almost a week.

CHAPTER

02

Eleven Minutes: How Hackers Get In, and the Answer

The attacker didn't need to be a genius. They just needed a camera.



The attacker didn't need to be a genius. They just needed a camera.

OBSERVED IN A NETOPS IQ PILOT

They found a camera that could be reached and started testing it. Once they had a foothold, they began looking around, trying to see what else that camera could talk to. That is the whole game. The camera itself isn't the prize. It's a stepping stone toward the systems that matter: patient records, clinical applications, and the controls that keep the building running.

It took about eleven minutes from the first touch to the moment it was stopped. That's the part I want every hospital leader to remember. These attacks don't take weeks to unfold. They move fast, and they move quietly. If nothing is watching the traffic coming out of your devices, eleven minutes is more than enough.

In this case, something was watching. Our system saw the camera behaving in a way it never had before. When the team turned on our agents, the camera was cut off from the rest of the network, and the attacker had nowhere left to go. Patient care never paused.

So how do hackers get in? After many assessments, we see the same handful of paths again and again. Here they are in plain terms, along with the answer to each.

The camera itself isn't the prize. It's a stepping stone.

Factory passwords. Many cameras, door readers, and building controllers still use the login they came with from the factory, or one shared password across hundreds of devices. Attackers know these passwords and try them first. The answer is to know every device you have, give each one its own strong password, and get an alert when someone keeps trying to log in.

Old software. These devices often run software that is years out of date, with weaknesses that are publicly known. Updating them usually means calling a vendor and scheduling downtime, so it gets put off. The answer is to track the software version on every device, fix the ones that can reach important systems first, and wall off the ones you can't update yet.

Flat networks. In many hospitals, a camera or heating controller sits on the same network as clinical systems. Once an attacker is inside one device, they can reach almost anything. The answer is to separate building devices from clinical systems, and to be ready to cut off a single device the moment it starts acting strangely.

Vendor remote access. Many building systems have a permanent remote connection so the vendor can service them. That's convenient, but it's also a standing door into your hospital. The answer is to see every vendor connection as it happens, allow it only during approved times, and question anything unexpected.

Exposed control panels. The setup pages for many devices can be reached from guest Wi-Fi or even the internet. The answer is to find every one of them and close it off.

Quiet calls home. A device that has been taken over may start sending data out or be used to relay an attack. Nobody notices because nobody knows what normal looks like for that device. The answer is to learn each device's normal behavior so anything new stands out right away.

Tampering with the building itself. Some attackers go after the heating and cooling commands, door access, or tracking tags to disrupt operations or open doors. The answer is to watch the control traffic for commands that don't make sense and stop them before they take effect.

You may have noticed a pattern. Every answer comes down to three things. First, you have to see the device. Then you have to prove what risk it carries. Then you have to be able to control it quickly. I call this **See, Prove, Control**, and the next chapters walk through each part.



CHAPTER 02 IN ONE PAGE

Seven ways in.

And the answer to each.

01

Factory passwords

Give every device its own login.

02

Old software

Track it. Fix what reaches the most.

03

Flat networks

Separate the building from the clinic.

04

Vendor remote access

See every session. Allow it on your terms.

05

Exposed control panels

Find them. Close them.

06

Quiet calls home

Know normal. Flag anything new.

07

Building tampering

Watch the commands. Stop the strange ones.

The method

**See. Prove.
Control.**

THE METHOD IN THIS BOOK

See. Prove. Control.

Three questions every hospital leader should be able to answer.

See

THE LEADER'S QUESTION

What devices and connections are actually there?

WHAT FINDAVI DELIVERS

A live, passive view of every device and everything it talks to.

Prove

THE LEADER'S QUESTION

Which paths put patients or operations at risk?

WHAT FINDAVI DELIVERS

Evidence, reachability, ownership, and priorities ranked by impact.

Control

THE LEADER'S QUESTION

Can we stop the path safely and prove it stayed closed?

WHAT FINDAVI DELIVERS

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

CHAPTER

03

This Was Never About Data. It's About Patients.

In most businesses, a cyberattack is a money problem. In a hospital, it's a patient problem.



In most businesses, a cyberattack is a money problem. In a hospital, it's a patient problem.

You know how this story goes. A hospital gets hit, and suddenly ambulances are sent elsewhere. Surgeries are pushed back. Staff go back to paper charts and handwritten orders. Lab results take hours instead of minutes. Every one of those delays lands on a real person in a bed.

In February 2024, that story went national. On February 12, attackers typed a stolen password into a remote login page at Change Healthcare. Most people had never heard of Change. But it sits quietly in the middle of American healthcare, handling billing, payments, and pharmacy claims. That login page had no second check. One password was enough.³

For nine days, the attackers moved around inside. Then they set off the ransomware.

Pharmacies struggled to fill prescriptions. Doctors' offices and hospitals went weeks without the payments they live on. A month in, the American Hospital Association heard from nearly 1,000 hospitals. Seventy-four percent said the attack was directly affecting patient care. Ninety-four percent said it was hurting them financially. And among hospitals with cash flow problems, more than a third said over half of their revenue was affected.⁴

If this device were taken over tonight, what would happen to the people in our beds tomorrow morning?



The numbers kept climbing for more than a year. In April 2024, UnitedHealth, Change's parent company, estimated the attack would cost it up to \$1.6 billion that year, and it had already advanced billions of dollars to providers to keep them going.⁵ By October 2024, the estimate had grown to \$2.87 billion.⁶ The count of people whose data was caught up in it grew too: an estimated 190 million in January 2025,⁷ and a final count of 192.7 million in July 2025.⁸ That's more than half the country.

That's what happens when a critical partner goes down. Change wasn't a hospital. Most patients had never heard its name. But because it sat in the middle of claims and payments, its outage became everyone's outage, at providers and pharmacies that were never attacked themselves.

Notice something about Colonial and Change Healthcare. Neither attack started with a camera or some brilliant piece of code. Both started with one door that had only one lock. Two stories, one lesson. Attackers don't need the front door. They need any door nobody is guarding closely. And in most hospitals, the least guarded doors are the devices nobody has even put on a list.

It's easy to think of cameras and building systems as "not clinical," and so not urgent. But think about what happens when they fail or get taken over. If door access goes down, staff can't move freely between units, or the wrong people can get in. If the pharmacy refrigerator stops reporting its temperature, medicines can spoil without anyone knowing. If the heating and cooling system is tampered with, operating rooms and isolation rooms lose the conditions they depend on. If nurse call stops working, a patient presses a button and nobody comes.

And as we saw in the last chapter, a camera that nobody watches can be the first step toward the systems that hold patient records and run clinical care.

This changes how you should talk about the problem. When you go to your board or your clinical leaders, don't lead with technical terms. Lead with patients. Ask the question this way: if this device were taken over tonight, what would happen to the people in our beds tomorrow morning?

That question gets attention, and it should. It also helps you decide what to fix first, which we'll come back to in Chapter 6.

It's also worth looking at your downtime plans with fresh eyes. Most hospitals have careful plans for when the electronic health record goes down. Far fewer have thought through what happens when the building systems, door access, or cameras go down at the same time. Bring your facilities and clinical engineering teams into that conversation. They know these systems better than anyone, and they'll be your best partners in protecting them.

Try this on your own hospital. Do your downtime plans cover building and physical security systems, not only clinical software? Could you explain the risk of an unprotected camera in terms of patient safety? Are facilities and clinical engineering part of your security planning today?





CHANGE HEALTHCARE, FEBRUARY 2024

192.7 million people.

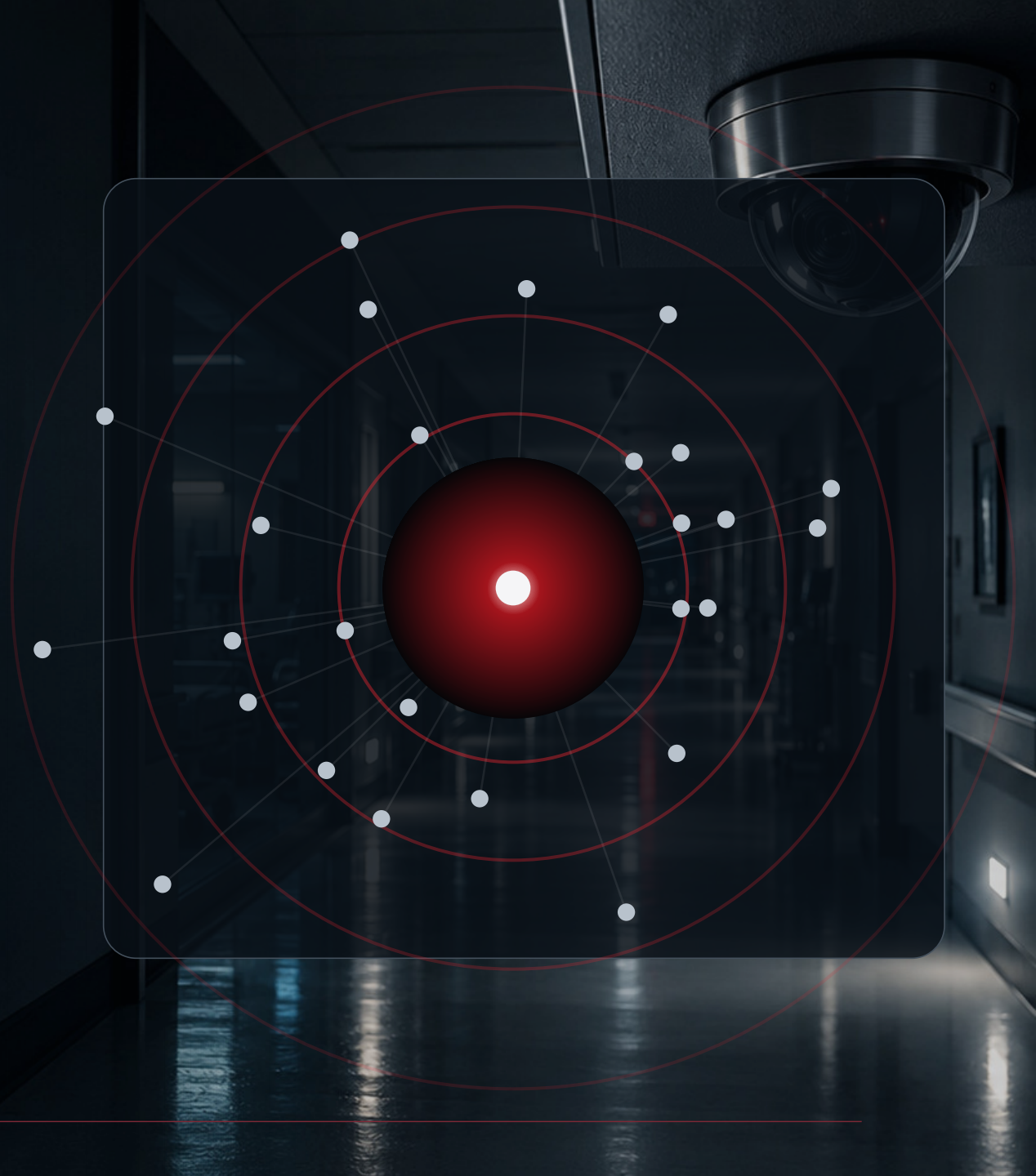
UnitedHealth's final count of people whose data was affected, reported in July 2025. It started with one stolen password.

CHAPTER

04

See: The Stethoscope, Not the Scalpel

You can find every device in your hospital without touching a single one.



ILLUSTRATIVE

Ask a veteran clinical engineer about network scans and watch their face. Some of them have a story like this one. Security runs a routine scan. Within minutes, the phones start ringing because equipment on a patient unit has frozen or restarted. Nobody gets hurt, but nobody forgets it either. From then on, clinical engineering has one word whenever security wants to scan anything near a patient: no.

So here'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 good news is there's a way to find every connected device in your hospital without poking at a single one of them. You do it by listening.

The usual way to find devices is to scan the network, which means sending out probes and seeing what answers. That works fine on laptops and servers. But some older or sensitive medical and building devices don't handle active probing well. A scan can slow them down, confuse them, or in some cases make them restart. That's why many clinical engineering teams push back when security wants to run a scan near patient equipment. They're right to be careful.

Listening is different. Instead of sending anything to the devices, you connect to a special monitoring port on the network and quietly watch the traffic that's already flowing. Think of it like a doctor using a stethoscope instead of surgery. You learn a great deal, and the patient never feels a thing.

Think of it like a doctor
using a stethoscope
instead of surgery.

From that traffic alone, you can learn what each device is, who made it, and often what software version it's running. More important, you learn who it talks to. A camera should send video to its recording server, and that's about it. If that same camera starts reaching out to a records system or an address overseas, you know something is wrong.

This is also how you build something most hospitals have never had: a true, living list of every connected device, updated on its own as things are added or moved. No spreadsheets that go stale the week after they're finished. No relying on what vendors remember to tell you.

People often ask me how long this takes. In most cases, a useful picture starts to form within hours, and a full picture within days, because devices reveal themselves as they go about their normal work. And since nothing is sent to the devices, there's no change window to schedule and no risk to patient care.

That's how our own appliance at NetOps IQ is designed to work. It connects through a passive monitoring port. It listens. It doesn't probe or scan. That design choice came straight from conversations with hospital teams who told us, very clearly, that anything they connect must not put patients at risk.

Try this on your own hospital. Has anyone on your team ever had a device freeze or reboot during a scan? Do you have a complete, current list of connected devices today? Would your clinical engineering team support a method that only listens?

CHAPTER

05

Prove: Trade Your Hunch for Evidence

A hunch won't get you a budget. Proof will.



Every hospital leader I meet has a hunch. "I'm pretty sure our cameras are a mess," they'll say, or "I bet half those building controllers still have the factory password." They're usually right. But a hunch won't get you a budget, and it won't get a vendor to show up on a Saturday. Proof will.

A focused device assessment is how you get that proof. It turns "we think we're exposed" into "here are the exact devices, here's what's wrong with each one, and here's what to fix first." Suddenly you're not asking for faith. You're showing facts.

We've done these assessments in hospitals, including reviews of camera systems spread across several sites. I can't name the hospitals, but I can tell you the kinds of things we tend to find, because they show up almost everywhere.

We find devices still using factory passwords, or one password shared across an entire fleet. We find software that hasn't been updated in years. We find cameras and building controllers sitting on the same network as clinical systems, with nothing between them. We find setup pages that anyone on the guest network could open. And we often find devices sending traffic to places they have no business talking to.

That's the difference
between a list and a plan.

None of this means anyone did a bad job. These devices were installed by different teams over many years, usually with the goal of getting them working, not locking them down. The assessment simply shows you the truth of where things stand today.

A good assessment report should do four things. It should list every finding with real evidence, not guesses. It should explain what each finding means in plain language, including what an attacker could reach from there. It should rank the findings so you know where to start. And it should tell you how to fix each one, or how to contain it if a fix isn't possible yet.

There's one more thing that matters a lot. A device assessment is not the same as a regular vulnerability scan. A scan gives you a long list of technical issues, often thousands of them, with little sense of which ones matter. A device assessment looks at how each device is actually connected and what it could lead to. That's the difference between a list and a plan.

At NetOps IQ, we deliver our assessment on a small appliance that we prepare and ship to you. It connects through the listening approach from the last chapter, so nothing is disrupted while the evidence is gathered.

Try this on your own hospital. If your board asked tomorrow which devices are your biggest risk, could you show them evidence? Do you know how many of your devices still use factory passwords? Has anyone ever reviewed your camera fleet from a security point of view?

CHAPTER

06

Triage: Chest Pain Before Sprained Ankles

Your hospital already knows how to decide what comes first.

FIX FIRST

01

Can reach patient records



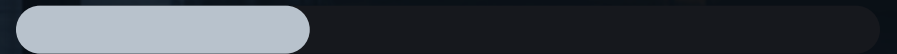
02

Affects care if it goes down



03

Isolated, low impact



ILLUSTRATIVE

Picture Monday morning. The assessment report lands in your inbox. You open it, scroll, and keep scrolling. There are hundreds of findings. Maybe more. Your team is already stretched thin, and now you're holding a list that could keep them busy for two years.

Where do you start?

Your hospital already knows the answer. It's called triage. When the emergency department fills up, nobody treats patients in the order they walked in. They treat the person who is in the most danger first. A sprained ankle waits. Chest pain doesn't.

Device security works the same way. The mistake most teams make is sorting findings by how scary the technical label sounds. That's like triaging by how loud someone is yelling. Instead, ask three simple questions about every device.

First, what can it reach? A camera that can only talk to its own video recorder is a sprained ankle. A camera that sits on the same network as your patient records is chest pain.

Second, what happens to patients if it's taken over? A lobby sign showing the wrong message is embarrassing. A pharmacy refrigerator that stops reporting its temperature is dangerous.



A sprained ankle waits.
Chest pain doesn't.

Third, how hard is it to fix? Some problems take five minutes, like changing a factory password. Others need a vendor, a budget line, and a weekend outage. Quick fixes on high-risk devices go to the top of the list. You'll be amazed how much risk disappears in the first two weeks.

For the problems you can't fix right away, don't just leave them sitting there. Contain them. If an old controller can't be updated until next year, wall it off so it can only talk to the one system it needs. That buys you time without leaving the door open.

There's a bonus, too, and it makes all of this much easier to sell inside your hospital. Almost everything you find maps neatly to the rules and frameworks you already report against. That includes the HIPAA Security Rule, the HHS 405(d) Health Industry Cybersecurity Practices, the NIST Cybersecurity Framework, and the CIS Controls. When you show your compliance team that fixing a camera password also closes a gap they've been asked about, you gain a powerful ally.

Try this on your own hospital. Is your team sorting findings by technical score or by patient impact? Which five devices on your network would hurt patients most if they were taken over? What could you fix this week in under an hour?

CHAPTER

07

Control: 2:47 A.M.

A camera starts doing something it has never done.
Who's awake to notice?

2:47

Thursday



FINDAVI AGENT

now

Camera, Floor 4

Trying to reach a finance server. It has never done this before. Isolate this camera?

Approve

Decline

ILLUSTRATIVE

It's 2:47 in the morning. A camera on the fourth floor, the one outside the pediatric unit, suddenly starts trying to reach a server in the finance department. It has never done that before. Not once.

Who's awake to notice?

In most hospitals, the honest answer is nobody. The security team is small. They're asleep, like they should be. By the time someone reads the alert over coffee, the attacker has had five hours to explore.

This is where most security leaders feel stuck. They know they need to respond faster than humans can. But they're nervous, and rightly so, about letting software make changes on a hospital network all by itself. One wrong move could cut off a device that's supporting a patient.

There's a middle path, and it's the one I believe in. Use smart software agents that do the watching, figure out what's wrong, and prepare the fix. Then have them ask a person before anything happens.

One tap to approve. The camera is cut off. The rest of the hospital keeps running.

Now replay 2:47 a.m. with agents on watch. The agent spots the strange behavior. It checks what the camera normally does and what it's trying to reach now. It prepares a clear recommendation: isolate this one camera from the rest of the network. Then it sends that recommendation to the on-call person's phone. One tap to approve. The camera is cut off. The rest of the hospital keeps running. The whole thing takes minutes, not hours.

But stopping it isn't the end of the story. The next morning, someone will ask the question that really matters: are you sure it's closed? Maybe it's your CIO. Maybe it's an auditor. Maybe it's a board member who read about Colonial Pipeline. "We think so" is not an answer you want to give.

So Findavi, our platform, answers before anyone asks. After the camera is isolated, it checks that the path the attacker was using is truly shut. Then it writes it all down: what it saw, what it recommended, who approved it, what changed, and the check that confirmed the door is closed. You don't walk into that meeting with a promise. You walk in with proof.

It checks one more thing, and in a hospital it matters just as much. Is the camera still doing its job? Findavi confirms the camera can still reach its approved video recording system and is still sending video. Shutting the attacker out is only half the work. A fix that breaks the service is just a different kind of outage.

Control is finished only when you can prove it. The door is closed, the proof is on file, and the hospital never stopped running.

For supported device types and approved integrations, our agents can do three kinds of things. They can block a device, isolate a single network port, or push a configuration change. Every one of those workflows is set up with your team before it's ever switched on. None of it happens without someone saying yes. Every action is recorded, so you can always see who approved what and when. And you can stop, undo, or switch off any agent at any time. You stay in charge.

In a hospital, there's one more step that matters. Before you ever cut off a device that might be near a patient, make sure clinical engineering and facilities are part of the approval path. Agree ahead of time on which devices can be isolated instantly and which need a quick phone call first. Do that planning on a calm Tuesday afternoon, not in the middle of the night.

When this is set up well, your security team changes jobs without changing seats. They stop spending their days chasing alerts. Instead, they become the ones giving the orders, reviewing what the agents found and deciding what to do. Small teams start to perform like big ones.

Try this on your own hospital. If a device started acting strangely at 3 a.m. tonight, how long before someone acted? Which devices could you safely isolate in seconds, and which need a call first? Who in your hospital should approve actions on building and clinical devices?



CHAPTER

08

Where Does Our Data Go?

Six questions for any vendor. Including us.

YOUR NETWORK



There's a moment in almost every first meeting I have with a hospital. The CISO is interested. The demo went well. Then the privacy officer leans forward and asks, "So where does our data go?"

Good. That's the right question. In fact, it's the question that should stop any security vendor in its tracks if they can't answer it clearly.

There's an irony here. You're bringing in a tool to make your hospital safer. But that tool sits on your network, sees your traffic, and in some cases can make changes. If it isn't built carefully, the cure becomes a new disease. So before you connect anything, from us or anyone else, ask these six questions and insist on clear answers in writing.

One. What will the report actually show me? You want real findings with evidence, an explanation of what each one means, and a clear order for what to fix first. If a vendor can't show you a sample report, be cautious.

Two. Is the value measured or estimated? Plenty of vendors promise huge savings. Ask which numbers come from your own network and which are guesses. Good vendors keep the two apart and show you their assumptions.

Three. What exactly does the device do when I plug it in? Does it only listen, or does it send anything out onto your network? Does it scan? Can it make changes on its own?

If it isn't built carefully, the cure becomes a new disease.

Four. Where does my data go? What does it collect, where is it stored, how long is it kept, who can see it, and does anything leave the building? Does it rely on an outside AI service in the cloud?

Five. What are its own risks, and what has been independently checked? Every product has weak points. Ask what they are and how they're protected. And make the vendor separate the certifications they actually hold from features that merely help you meet a standard.

Six. How much control do I keep? Can it act without permission? Is every action recorded? Can you stop it, undo it, or shut it off whenever you want?

I'd be a hypocrite to ask those questions without answering them myself. So this is how NetOps IQ answers. Our appliance connects through a passive port and only listens by default. The AI analysis runs entirely on the device itself. We don't send your traffic to an outside AI service. Your data is stored on the appliance, inside your network, not in our cloud. Nothing changes on your network unless a person approves it, and every action is recorded. We're working toward formal security certifications, and until we have them, we'll tell you so and show you exactly how the product is built instead.

That's the standard I'd want if I were sitting in your chair.

Try this on your own hospital. Have you asked these six questions of the security tools already on your network? Does your privacy officer know which of your vendors send data off site? Which of your current tools could make changes without asking?

BEFORE YOU CONNECT ANYTHING

Six questions.

Ask every vendor. Including us.

- 1 What will the report actually show me?
- 2 Is the value measured or estimated?
- 3 What does the device do when I plug it in?
- 4 Where does my data go?
- 5 What are its own risks, and what has been checked?
- 6 How much control do I keep?

CHAPTER

09

Ten Minutes With the Board

How to make a tired boardroom care about cameras and door readers.

01

Measured

What you found

02

Saved

Hours given back

03

Reduced

Risk, estimated

You have ten minutes on the board agenda. Right after the quarterly finance update and right before a discussion about the new parking garage. The room is tired. Half the members are checking their phones.

How do you get them to care about cameras and door readers?

Not with technical charts. Board members have seen a hundred slides full of red and yellow warnings. They've learned to nod and move on. What gets their attention is a simple story with honest numbers behind it.

Every board member understands one kind of story: money walking out the door. MGM is that story. In September 2023, MGM Resorts shut down computer systems across its properties after a cyberattack. For ten days, guests couldn't get into their hotel rooms. Some couldn't pay by card or pull cash from an ATM. Reservations broke. MGM later said the attack would cost it more than \$100 million in lost earnings. The cleanup itself, the lawyers and the consultants, came to less than \$10 million of that.⁹

Boards like to say yes to clear, sensible requests backed by real evidence.

Look at those two numbers side by side. The repairs were the small part. The big cost was all the business that simply couldn't happen while the systems were down. A hospital works the same way. Every hour of downtime means procedures that don't happen, beds that don't turn over, and patients sent somewhere else.

If your board wants one number, give them this one. IBM's 2025 study put the average cost of a data breach in the United States at \$10.22 million, the highest it has ever been. Healthcare has been the most expensive industry in that study for fourteen years in a row, and hospital breaches take an average of 279 days to find and contain.¹⁰ Numbers like that belong in the boardroom, right next to the finance update.

Start with the story. Tell them about the camera. Tell them how a device nobody was watching gave an attacker a path toward patient systems, and how long it took to stop. Make it real. Then show them where your own hospital stands.

For the numbers, I suggest splitting the value into three levels, and being very clear about which is which.

Level one is what you measured. These are the hard facts from your own network. How many devices you found that nobody knew about. How many still had factory passwords. How many could reach clinical systems. How many attack paths you closed, with proof that they stayed closed. Nobody can argue with these, because they came from your hospital, not a sales brochure.

Level two is the time you saved. How many hours did your team used to spend chasing down devices, building inventories by hand, or investigating alerts? How many hours does it take now? Multiply by what your own staff actually cost. This is still measured, just in a different way.

Level three is the risk you reduced. This one is an estimate, so say so out loud. Show the assumptions you used and let the board question them. You might estimate what a day of diversion or downtime would cost your hospital, and how much more likely that day was before you closed these gaps. Being honest about this number makes the first two levels even more believable.

The same evidence also does double duty. The facts that convince your board are the same facts your auditors and compliance team want to see. You build it once and use it everywhere.

End your ten minutes with one clear ask. Not a vague request for "more security." Something specific, like approval to assess every site by the end of the quarter, or to bring building devices under the same monitoring as everything else. Boards like to say yes to clear, sensible requests backed by real evidence.

Try this on your own hospital. Could you tell the story of your biggest device risk in two minutes? Which of your numbers are measured and which are estimates? What is the one specific thing you want your board to approve?



IBM COST OF A DATA BREACH, 2025

\$10.22 million.

The average cost of a breach in the United States. Healthcare has been the costliest industry for fourteen years straight.

A CLOSING WORD

That night, nothing bad happened.

Somebody was finally watching.



Go back for a moment to that camera in the hospital hallway. The one from the very first page.

That night, nothing bad happened. No patient was harmed. No records were stolen. No ambulance was turned away. And the reason was simple. Somebody was finally watching the part of the hospital that nobody used to watch.

This whole book comes down to three moves. See every device. Prove which ones put your patients at risk. Control them quickly, with a person always in charge. None of it requires ripping out what you have. None of it requires putting patient care on hold. It just requires deciding that the side doors matter as much as the front one.

And this is only the beginning. The hospital of the next ten years will be run more and more by machines talking to machines. Smart beds, robots delivering medicine, buildings that adjust themselves, sensors in every room. That future is coming whether security is ready or not. Every one of those machines will be either a helper or a way in. I started NetOps IQ because I believe someone has to make sure they stay on our side.

You don't have to do it all at once. Start with one site. Start with one camera fleet. Start with one honest list of what's really on your network. Every blind spot you close is one less path to the people who trust your hospital with their lives.

If you'd like help taking that first step, we'd be glad to talk.

Sources, by chapter

CHAPTER 1

- 1 Colonial Pipeline CEO Joseph Blount's Senate testimony: the legacy VPN account had no multifactor authentication, and the company did not know how the password was obtained. Dark Reading, June 2021. darkreading.com/cyberattacks-data-breaches/colonial-pipeline-ceo-ransomware-attack-started-via-pilfered-legacy-vpn-account
- 2 Colonial's share of East Coast fuel, the shutdown, more than 9,500 stations out of fuel, and the \$4.4 million ransom. Associated Press via WEAR-TV, May 19, 2021. weartv.com/news/nation-world/colonial-pipeline-confirms-it-paid-44m-to-hackers

CHAPTER 3

- 3 Change Healthcare entry on February 12, 2024 through a remote access portal without multifactor authentication, and ransomware nine days later, from CEO Andrew Witty's congressional testimony. TechTarget, April 30, 2024. techtarget.com/cybersecurity/news/366582824/Change-Healthcare-breached-via-Citrix-portal-with-no-MFA
- 4 AHA survey of nearly 1,000 hospitals, responses March 9 to 12, 2024. American Hospital Association, March 15, 2024, as reported by Becker's Hospital Review. aha.org/node/692736 and beckershospitalreview.com/finance/94-of-hospitals-take-financial-hit-from-change-hack-aha-survey.html
- 5 UnitedHealth's first 2024 estimate of up to \$1.6 billion and more than \$6 billion in advance funding to providers. Business Insurance, April 17, 2024. businessinsurance.com/unitedhealth-estimates-16-billion-loss-from-change-cyberattack

- 6 UnitedHealth's revised full-year 2024 estimate of \$2.87 billion, in its third-quarter 2024 results. Becker's Payer Issues, October 15, 2024. beckerspayer.com/payer/unitedhealth-posts-6-1b-profit-in-q3
- 7 Estimate of 190 million people affected. Fierce Healthcare, January 24, 2025. fiercehealthcare.com/payers/unitedhealth-estimates-190m-people-impacted-change-healthcare-cyberattack
- 8 Final count of 192.7 million people, from UnitedHealth Group's July 31, 2025 letter to state regulators. Healthcare IT News, August 6, 2025. healthcareitnews.com/news/new-numbers-change-healthcare-data-breach-193-million-affected

CHAPTER 9

- 9 MGM Resorts' ten-day shutdown, guest impact, and estimate of more than \$100 million in lost earnings. Associated Press via KSAT, October 6, 2023. ksat.com/business/2023/10/06/cyberattack-at-mgm-resorts-expected-to-cost-casino-giant-100-million
- 10 IBM Cost of a Data Breach Report 2025: \$10.22 million U.S. average, healthcare the costliest industry for fourteen years, and a 279-day healthcare breach lifecycle. HIPAA Journal, 2025. hipaajournal.com/average-cost-of-a-healthcare-data-breach-2025

TAKE THE NEXT STEP

NetOpsIQ™

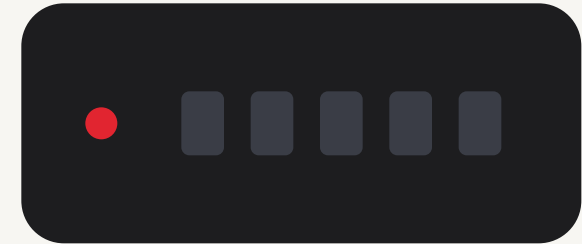
See what's really on your network.

The NetOps IQ Blind Spot Assessment gives you a clear, evidence-based picture of the devices on your hospital network that your current security tools can't reach. We ship you a small appliance with Findavi, our platform, already loaded. It connects through a passive port, listens without disturbing anything, and keeps all of your data on your own network. Start as small as you like: one hospital, one building, one camera fleet, or one type of device. You'll receive a prioritized report of the devices we found, the paths an attacker could use, the actions we recommend, and the evidence behind each one.

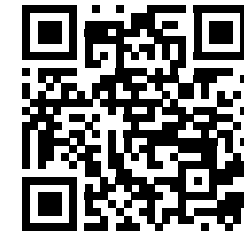
info@netopsiq.com

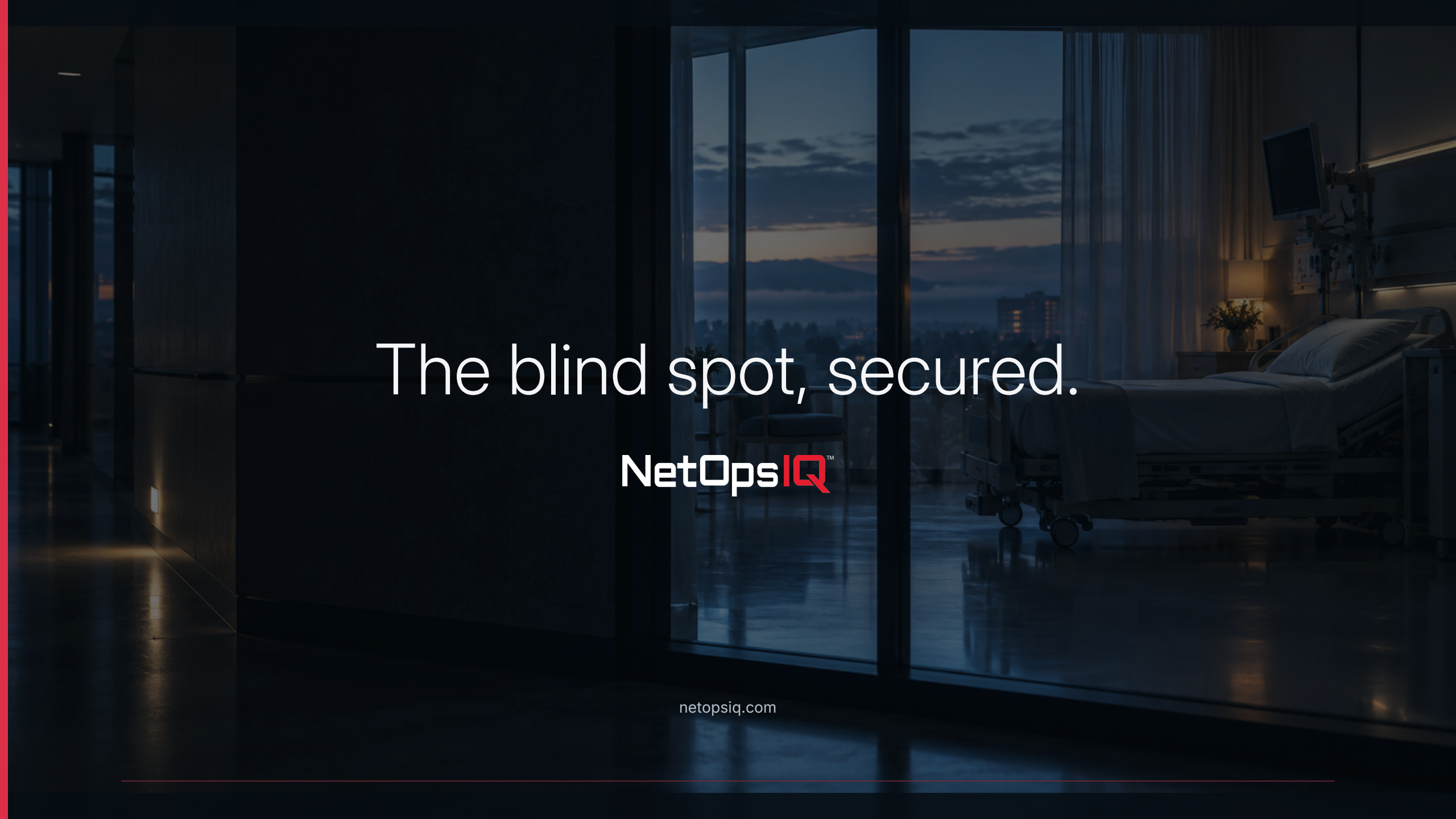
+1 (408) 621-5500

FINDAVI PLATFORM



Passive. On site. Your data stays home.





The blind spot, secured.

NetOpsIQ™

netopsiq.com