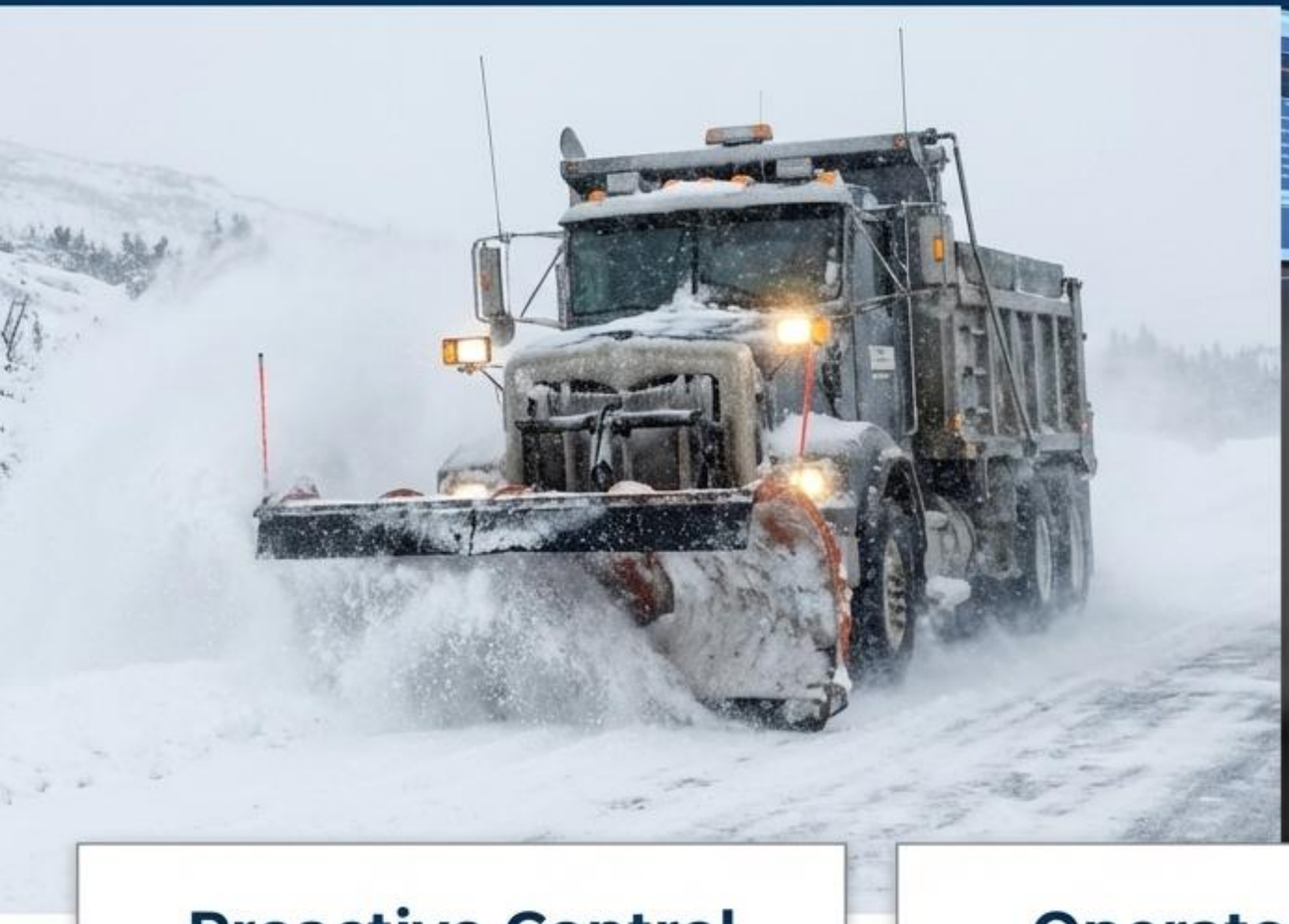

cahill
TECHNICAL
NotebookLM

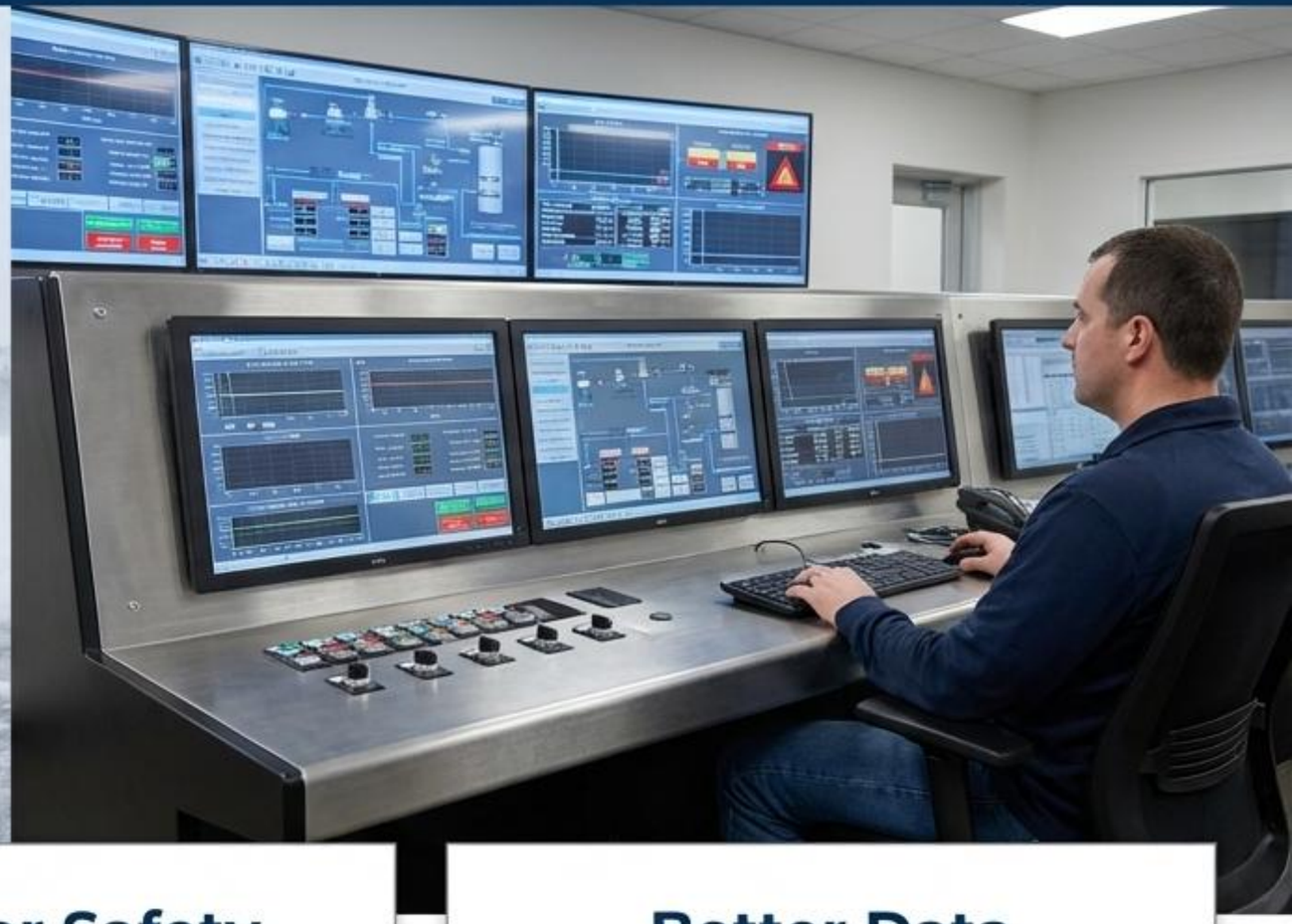
Operator to Operator: Operational Integrity

A Guide to SCADA Cybersecurity for NL Water & Wastewater

cahill TECHNICAL

SCADA helps us run better plants with small crews.





Proactive Control

Alarms and trends catch issues before they turn into a mess.

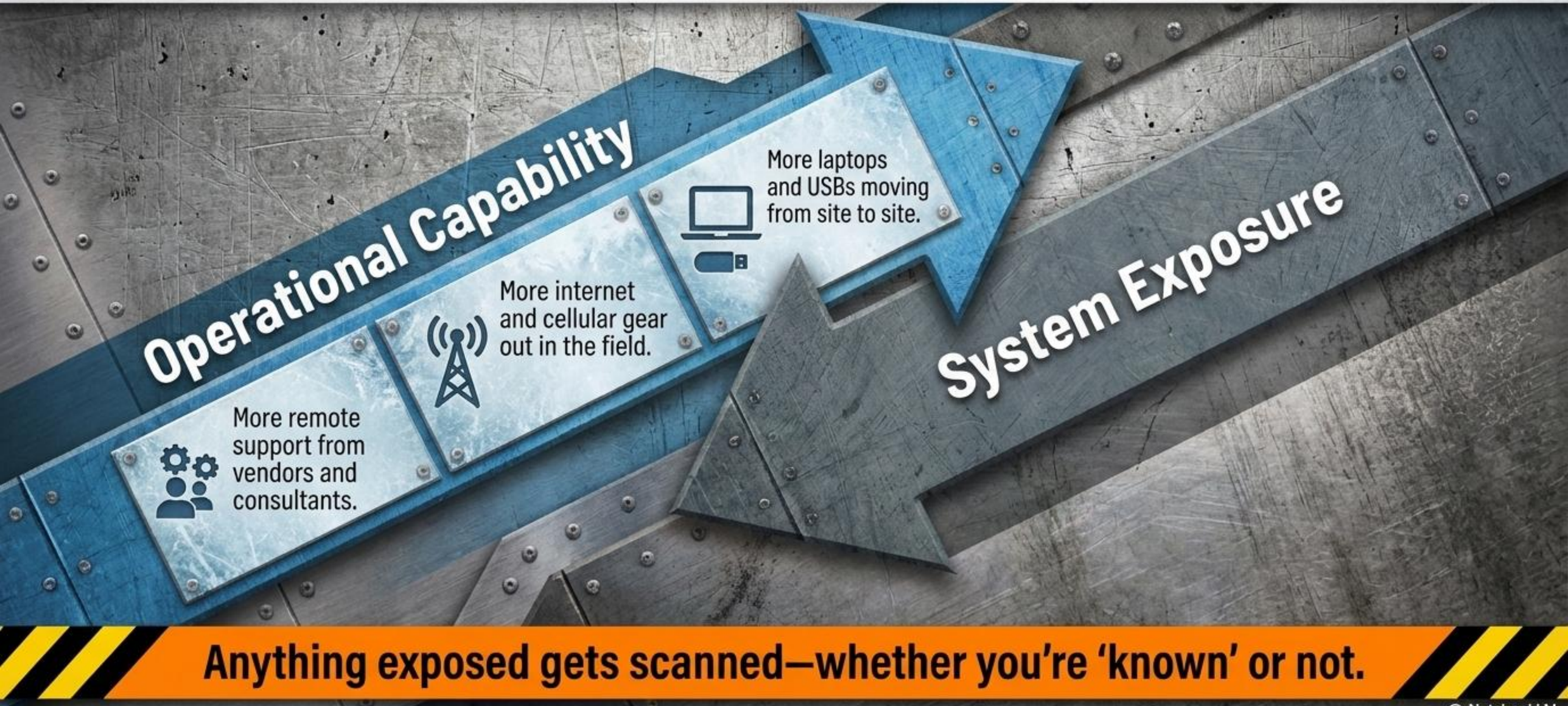
Operator Safety

Less driving in ugly weather and fewer risky callouts.

Better Data

Cleaner records for compliance and faster troubleshooting.

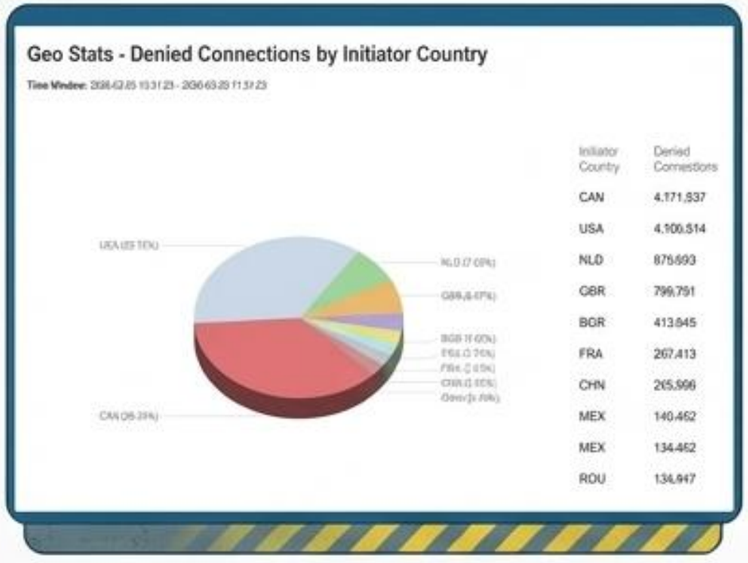
What Changed Over the Last Few Years



Anything exposed gets scanned—whether you're 'known' or not.

Canada is not immune—it's just quieter.

The Constant Storm



Over 4 million denied connections from scanning bots.

Municipal Impact (Feb 2024)

City of Hamilton water system incident.

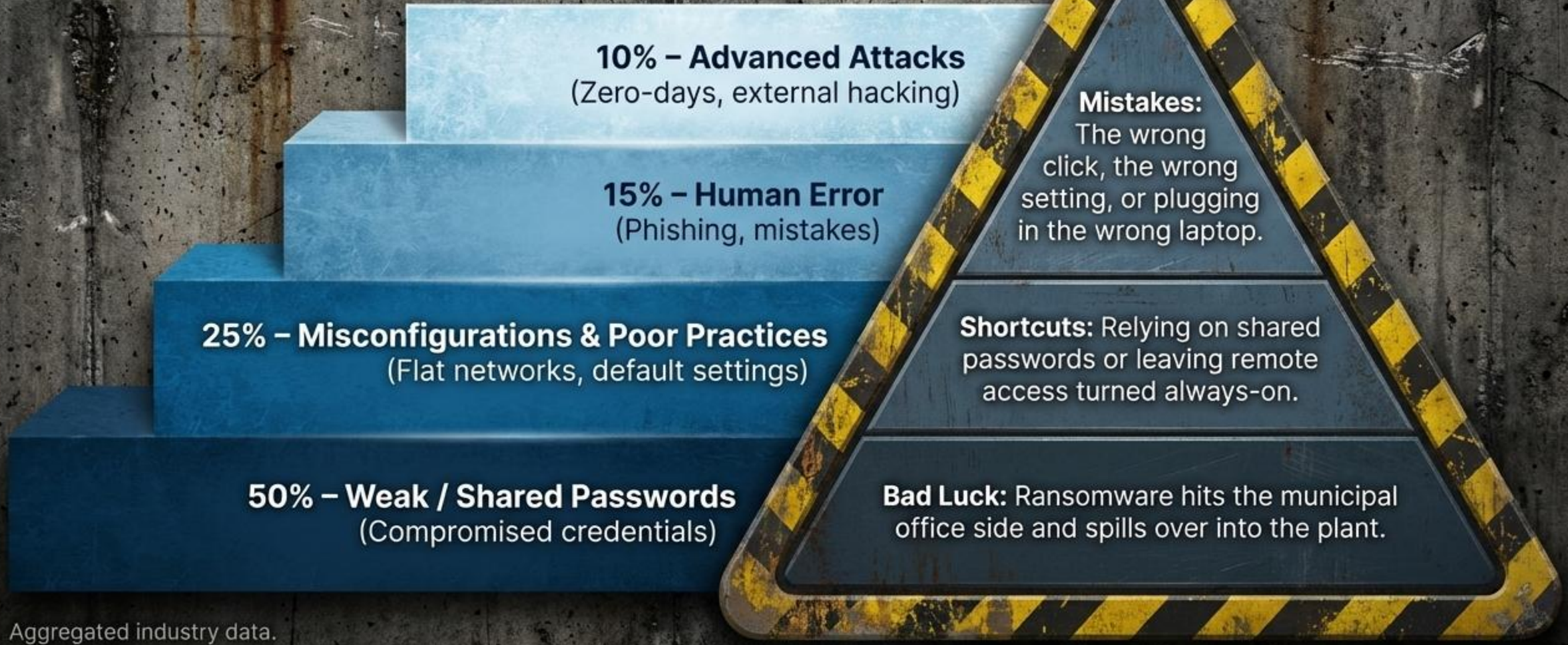
Result: Proactive system shutdown, forced shift to manual operations to contain the issue.

Regional Impact (Nov 2021)

Newfoundland & Labrador Hydro ransomware event.

Result: Impacted corporate IT, causing operational disruptions and forcing manual processes. Even when OT isn't directly hit, IT disruption affects operations.

How Plants Actually Get Burned



Aggregated industry data.

Cybersecurity is just good operating practice.

It requires the exact same mindset as lockout/tagout and pre-start checks.
Fixing the basics means fewer emergencies.

Access:
Control exactly who can touch the system.

Hygiene:
Keep field tools clean and updated.

Autonomy:
Make sure you're not stuck waiting on someone else to fix a problem.

Shared Logins vs. Unique Identity

The Hazard: The Shared Login

- You can’t tell who did what.
- If the password leaks once, the entire plant is exposed.
- When people leave the company, their access stays active.

The Control: The Unique Login

- Person-by-person accounts.
- Clear logs of who made changes.
- Turn off access instantly when the work is done.

Don’t let the vendor hold the only keys.

The Reality:
If something goes sideways at 2 a.m., you need access right now. The vendor might be on another job, on a plane, or offline.

The Rule of Two:
Always maintain at least two independent municipal admin accounts.

The Break-Glass Protocol:
Keep an emergency break-glass process—a sealed and documented way to regain total control of your system if locked out.

Remote Access: Great When Done Right

The Truth: Remote support saves incredible amounts of time—no question.

The Trap: 'Always-on' remote access gets forgotten and leaves a permanent open door.

The Standard: Managed Remote Access

- Must be an approved method.
- Turned ON only when needed, OFF when the job is done.
- Log every instance: Who connected, when, and why.

How trouble travels on laptops and USBs.

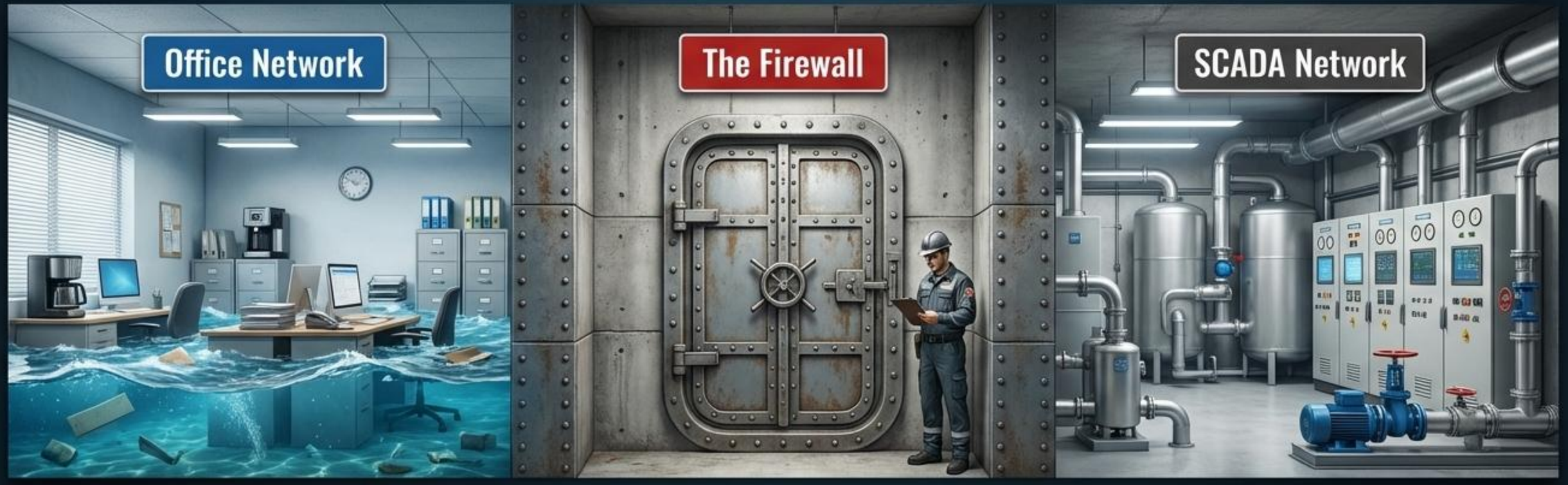
The Risk:

- Laptops hop from plant to plant constantly.
- They don't always get security updates or run active antivirus.
- USB sticks are easy to use, but act as direct carriers for trouble.

Fix Action Box

Set a strict minimum standard for ANY laptop or drive that touches your SCADA system.

Firewalls & Segmentation: Keep Office Problems Out



Core Rule:

The office network and the SCADA network should not be one big open space.

Firewalls:

Act like the physical gate and the security log book. They dictate exactly what traffic can pass.

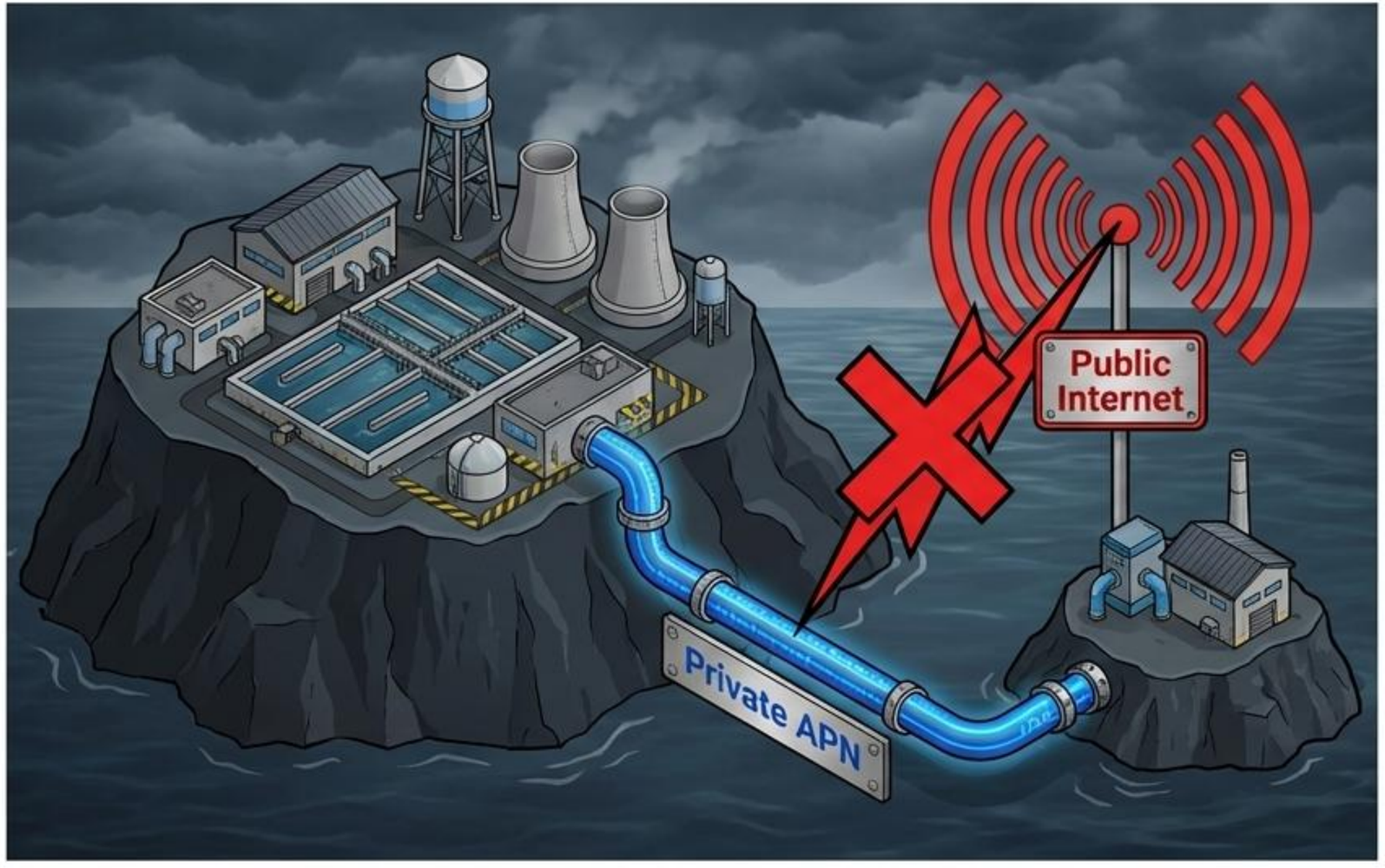
Segmentation:

Acts like bulkheads on a ship—limiting the damage and keeping the plant running even if the office side gets hit with a problem.

Action Plan:

Start simple. Separate, restrict, and monitor.

APN (Private Cellular): A Safer Way for Remote Sites



The Challenge:

Remote assets are spread out. Lift stations, water towers, and pump houses rely on cellular connections.

The Solution:

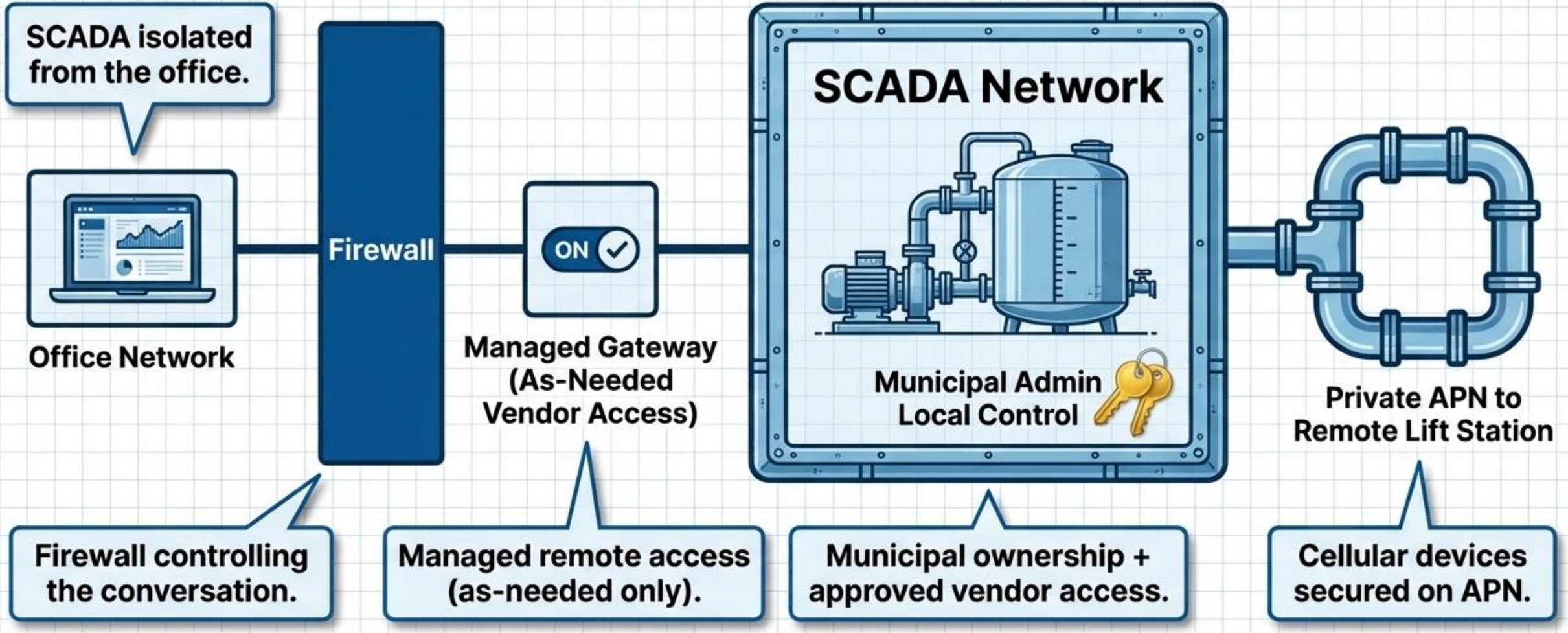
A Private APN keeps operational traffic completely off the public internet.

The Result:

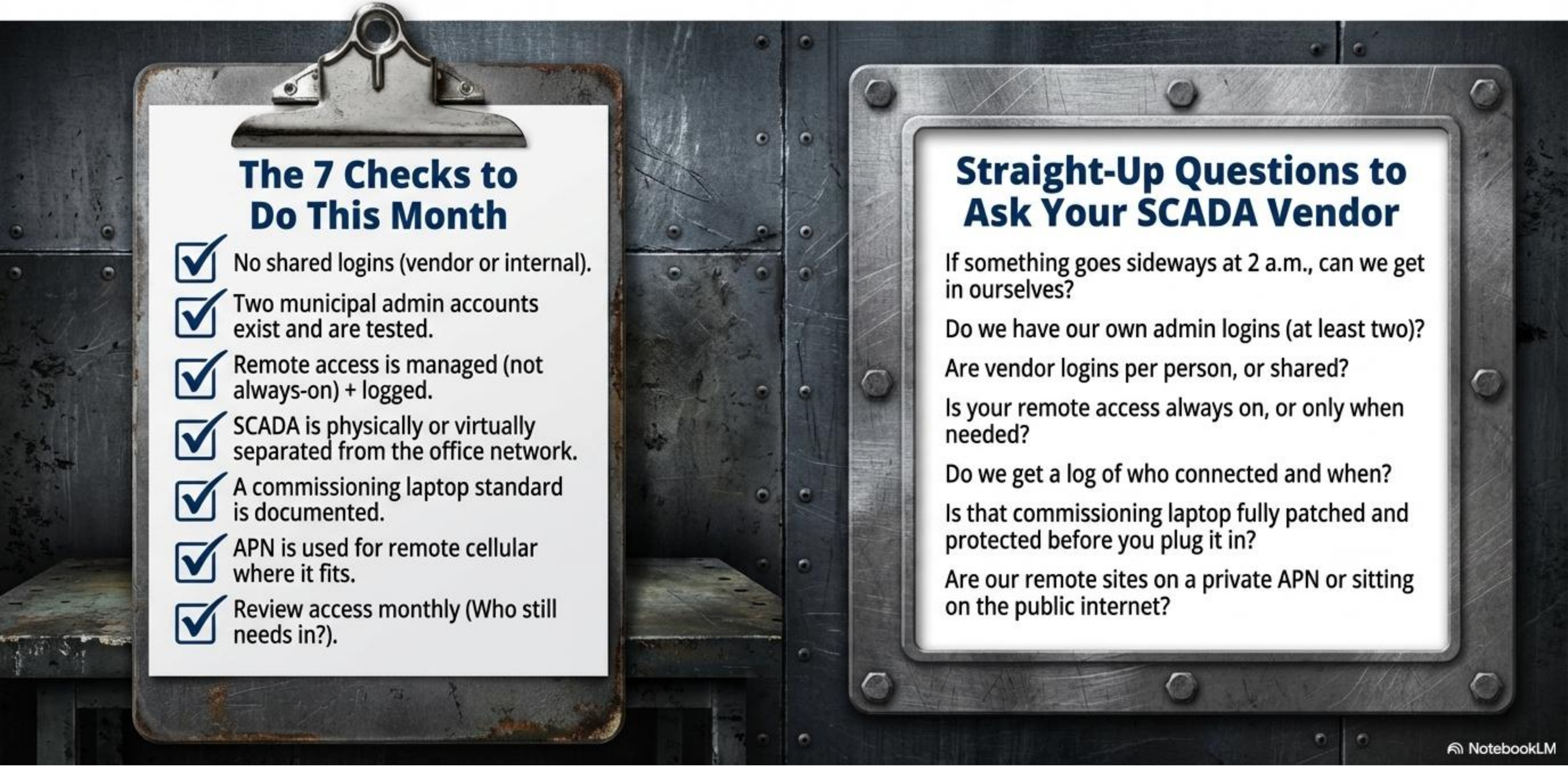
Less exposure to scanning, tighter control. Best when combined with strict firewall rules.

A Practical Setup That Works in Real Life

The Ultimate Practical Blueprint



Straight-Up Questions & The 7 Checks to Do This Month



The 7 Checks to Do This Month

- ☑ No shared logins (vendor or internal).
- ☑ Two municipal admin accounts exist and are tested.
- ☑ Remote access is managed (not always-on) + logged.
- ☑ SCADA is physically or virtually separated from the office network.
- ☑ A commissioning laptop standard is documented.
- ☑ APN is used for remote cellular where it fits.
- ☑ Review access monthly (Who still needs in?).

Straight-Up Questions to Ask Your SCADA Vendor

If something goes sideways at 2 a.m., can we get in ourselves?

Do we have our own admin logins (at least two)?

Are vendor logins per person, or shared?

Is your remote access always on, or only when needed?

Do we get a log of who connected and when?

Is that commissioning laptop fully patched and protected before you plug it in?

Are our remote sites on a private APN or sitting on the public internet?


Keep the Water Flowing.
SCADA is essential for our communities. Connectivity naturally creates operational risk. Simple, routine practices reduce that risk.
cahill
TECHNICAL
NotebookLM

cahill
TECHNICAL

ENGINEERING

Precision-led design tailored for demanding environmental and operational conditions.

INDUSTRIAL SOLUTIONS

Scalable, high-fidelity technical systems engineered for maximum resilience and control.

FIELD EXECUTION

Uncompromising on-site implementation driven by profound local expertise and global standards.