

Validated, documented, and unpatched

Four questions every life sciences manufacturing site should be able to answer.

In May, West Pharmaceutical Services took systems offline globally after an attacker exfiltrated data and encrypted parts of its infrastructure. The company disclosed the event in an SEC filing as material, engaged outside incident response, and worked through a phased recovery before declaring its manufacturing, supply chain, and commercial sites fully operational roughly two weeks later.

West makes stoppers, seals, and containment components used by most of the industry. Which is the part worth sitting with: the disruption did not need to reach your site to reach your schedule.

But the more useful detail is what recovery looked like. A pharmaceutical or device manufacturer cannot simply restore from backup and resume. Processes

are validated. Changes are documented. Before production restarts, the compliance obligations have to be satisfied — which means the recovery clock in a regulated environment runs on a different scale than it does anywhere else.

That asymmetry is the whole problem, and it starts long before an incident.

01

The paradox of a validated system

Validation exists to produce control. Documented configurations, controlled change, auditable history. In every respect that matters to product quality, a validated system is the most rigorously governed asset on the floor.

It is also, frequently, the least patched.

The reason is not carelessness. Patching a validated system triggers change control, impact assessment, and some level of requalification. That work has a

cost, and in most capital and operating budgets it was never scoped. So the patch waits for the next planned campaign, which slips, and the system continues running a firmware or OS version that stopped receiving security attention years ago — fully documented, fully compliant, and fully exposed.

The same discipline that makes the environment auditable is what makes it slow to defend. Any vendor who does not understand that tension will propose remediation your quality organization cannot accept.

Fully documented, fully compliant, and fully exposed.

02

Where the exposure actually sits

Most life sciences sites share a recognizable profile:

Vendor remote access that never got the validation treatment. OEM service agreements on filling lines, lyophilizers, autoclaves, chromatography skids, and isolators frequently include remote support. Those connections are commissioned by equipment vendors, are often not documented in the same system inventory as the equipment itself, and in many cases remain live years after the service contract lapsed. Industry surveys on third-party OT risk have repeatedly found that many manufacturers do not formally vet vendor security practices.

The IT-to-OT boundary. The common attack path is not a direct assault on a PLC. It is a corporate credential or an unpatched internet-facing service, followed by lateral movement to the manufacturing boundary and then into MES and batch management.

Batch systems as a pressure point. Ransomware operators understand the economics. A batch in progress represents significant work in process, and biologics and cell therapy products have process windows that cannot be extended. The urgency is structural, and adversaries price it.

Quiet exfiltration. Not every intrusion announces itself. Access to laboratory data systems, batch records, and formulation databases can produce sustained IP theft with no ransom note, no downtime, and no obvious indicator — detectable only through monitoring of data access patterns, not perimeter defense.

CMO, CDMO, and tech transfer relationships. Multi-party access to process data and recipes, frequently governed by agreements written before anyone was thinking about OT segmentation.

The four questions

Before evaluating any tool or service, a site should be able to answer these with evidence rather than assumption:

- 1** Can you produce a current inventory of every device on your OT and manufacturing network — including equipment under vendor service agreements — and identify which are reachable from outside your perimeter?
- 2** Do you know every active remote access path into your control and manufacturing systems, who owns each one, and whether any still use default or shared credentials?
- 3** If controller logic or a batch record were modified at 2:00 a.m. on a Sunday, how long would it take you to know?
- 4** Which of your validated systems are running unpatched because requalification was never scoped into anyone's budget?

A site that cannot answer all four does not have a technology problem yet. It has a visibility problem, and visibility is what an assessment is for.

Note what question three implies in a GxP context. An unauthorized modification to a record is not only a security event. It is a data integrity event, and it lands in a different part of the organization with a different set of consequences.

Start with CISA. It costs nothing.

Before spending a dollar with anyone, enroll in CISA's Cyber Hygiene Services. Life sciences manufacturers qualify as critical infrastructure, the service is free, and there is no good argument against being subscribed.

What it provides is real: continuous automated scanning of internet-facing assets, identification of Known Exploited Vulnerabilities and the exposed services commonly used for initial access, and recurring reports with mitigation recommendations.

Where the free scan stops

Two limitations matter more in a regulated manufacturing environment than almost anywhere else.

LIMIT 1

It is external only.

By CISA's own description, the scanning is a non-intrusive review of internet-accessible systems. It does not reach inside the private network and it cannot change anything. In a life sciences plant that means it sees nothing about segmentation between the business network and the manufacturing layer, nothing about credentials on a validated HMI that is not internet-facing, nothing about the OEM support tunnel into a filling line, and nothing about who can reach the MES. Nearly every finding that would matter most on a GxP floor sits inside that blind spot.

LIMIT 2

It produces findings, not fixes.

This is the harder limit. In a validated environment, acting on a finding means change control, impact assessment, a qualified maintenance window, and documentation that will survive an inspection. CISA is not staffed for that and does not claim to be. The distance between receiving a report and closing a finding is measured differently here — and that distance is where the risk actually lives.

From findings to fixed

Whether findings originate in a CISA scan or a full IEC 62443-aligned assessment, remediation on a regulated manufacturing site generally means:

- ▲ Removing or properly brokering internet-exposed assets that were never meant to be reachable
- ▲ Inventorying every vendor and OEM remote-access path, assigning an owner, and terminating what has outlived its contract
- ▲ Replacing default, shared, and legacy credentials across controllers, HMIs, historians, and engineering workstations
- ▲ Establishing real segmentation between business systems, the manufacturing layer, and safety systems
- ▲ Correcting firewall rule sets accumulated across years of project and tech transfer work
- ▲ Building a patch and requalification pathway so that security updates have a route to production instead of waiting indefinitely
- ▲ Standing up detection and response, so question three has an answer measured in minutes

Each item has to be sequenced around production schedules, change control, and a quality organization that will reasonably resist anything undocumented.

That sequencing is the actual deliverable. It is also the reason generic IT security firms struggle here.

APPLIES TO DEVICE & COMBINATION PRODUCT MANUFACTURERS

A note on FDA's Computer Software Assurance guidance

FDA's Computer Software Assurance guidance was finalized in September 2025 and superseded by an updated final version in February 2026, aligned to the Quality Management System Regulation. The current version adds explicit expectations around cybersecurity evidence and expands the treatment of vendor oversight, encouraging assessment of vendor cybersecurity posture through mechanisms such as SOC reports and software bills of materials.

If your supplier qualification process does not currently produce that evidence, it is worth knowing that the expectation is now written down.

INFLEXIONPOINT

We work with life sciences manufacturers on the part that comes after the findings.

We conduct vendor-neutral OT cybersecurity risk assessments aligned to IEC 62443, scoped for validated environments — and we remediate what gets identified, whether the source is our assessment or a CISA scan you are already receiving.

We are not reselling a security product, and we do not hand over a report and leave. As an Operating Partner, we stay in the environment: monitoring, hardening, and working inside your change control rather than around it.

Enroll with CISA regardless of what you do next. Then let's talk about closing what it finds, and what it cannot see.

[Request an assessment](#)