proarch

OT Security Best Practices

For Power & Energy Operations

Table of Contents

Introduction

Industrial operations run on systems like SCADA, PLCs, DCSs, RTUs, and HMIs—which are built for uptime, not cybersecurity. But as connectivity increases, so does exposure.

Legacy infrastructure, third-party access, and undocumented changes have created environments with limited visibility and fragmented control. In many cases, risks remain hidden until they trigger downtime, safety incidents, or regulatory fallout.

OT security is no longer optional. It's essential for protecting critical infrastructure.

This guide shares four proven best practices to help you regain control, reduce risk, and secure OT systems that were never designed to face today's threats.

What is OT?

OT (Operational Technology) refers to the hardware and software systems that monitor & control physical devices, processes, and infrastructure in industrial environments.

Unlike IT (Information Technology), which manages data and digital systems, OT deals with the real-world operations—like controlling machinery on a factory floor, regulating power grids, managing HVAC systems in large facilities, or running automated production ines.

A Letter from ProArch's VP of Industry Solution

Luke Bixby

Vice President of Industry Solutions @ ProArch,

Operational Technology (OT) is no longer isolated behind air gaps and legacy assumptions. In reality, it hasn't been a long time. Over the past decade, OT has steadily become more connected, embedding digital intelligence directly into mechanical systems. That connectivity enabled smart feedback loops, automated controls, and real-time visibility that improved reliability and efficiency.

Industrial OT is the unseen foundation of the digital economy, powering data centers, enabling AI, and sustaining modern business. Without resilient, high-performing OT at the source, none of it functions.

In conversations with plant leaders and operations executives, the pressures are consistent. They are being asked to modernize faster, connect more systems, enable remote operations, and extract more value from existing assets. AI initiatives are accelerating this shift,
reaching deeper into plants and into systems once considered isolated.

In OT, we don't have the option to patch first and fix later. Downtime isn't acceptable, and safety can't be compromised. Yet the same challenges persist, limited asset visibility, unmanaged third-party access, unvalidated backups, and patching decisions made without operational context. The issue isn't connectivity. OT should be connected. The question is whether these environments are being secured in a way that respects how they actually operate.

This guide is built with that reality in mind, I focus on practical, operations-first OT security that strengthens reliability, resilience, and trust.

Why OT Security Can't Be an After thought

OT environments are no longer isolated. They're connected to IT, cloud platforms, and third-party vendors— expanding the attack surface. Traditional IT security doesn't fit OT, where uptime, safety, and legacy systems dominate.

21%

According to a study released by Black Kite, the manufacturing sector accounts for 21% of ransomware attacks & placesmanufacturing " entities at a significantly high risk, making them more than three times as likely to suffer a ransomware attack.

Darkreading.com

Why OT is Exposed

→ Limited Asset Visibility

→ Unmanaged Third-Party Access

→ Delayed Patching & Legacy Systems

→ Uptime vs. Security Conflicts

Why it's Non-egotiable

→ 26% now have basic OT visibility (up from 20%)

→ Outages impacting revenue dropped from 52% to 42%

→ Yet nearly 1 in 2 organizations still face intrusions

Impact

→ **Power & Utilities**

Grid stability, compliance, secure SCADA/DCS visibility

→ **Manufacturing**

Reduced downtime, legacy asset monitoring, faster response

So How Do You Secure OT Without Breaking It?

Start with OT Security Best Practices

Operational technology (OT) environments face growing pressure as legacy systems, complex supply chains, and increased connectivity expand the attack surface.

The risks are no longer theoretical. Cyber incidents can lead to downtime, safety events, and compliance failures. As threats evolve and regulations tighten, OT security requires a structured, operationally aware approach. The following OT security best practices provide a practical starting point.

4 OT Security Best Practices

1. OT Patching:
A Risk-Aware Operation,
Not a Routine Task.

Read More →

2. OT Visibility:
See Everything.
Miss Nothing.

Read More →

3. OT Backup Is
More Than Storage, It's
Operational Insurance.

Read More →

4. Third-Party Access:
Vendors Can Be Your
Weakest Link.

Read More →

1

OT Patching: A Risk-Aware Operation, Not a Routine Task

OT patching is a controlled operational decision, not routine IT maintenance. Every patch carries real-world risk. A mistimed update can disrupt operations, violate regulatory limits, or impact safety. Unlike IT, OT systems control physical processes where uptime and compliance are non-negotiable.

That's why our approach focuses on visibility, validation, and system awareness, not one-size-fits-all patch schedules.

OT Patching Best Practices

→ **Validated Asset Inventory**

Confirm what's active, supported, and safe to change, no assumptions.

→ **Backup & Recovery Readiness**

Systems are backed up & recovery plans validated before any update.

→ **Isolated Patch Testing**

Patches are tested in sandboxed environments, especially for high-risk or delayed updates.

→ **Phased, Risk-based Deployment**

Low-risk systems first, with monitoring before touching critical assets.

→ **OEM-aligned Execution**

Patching follows vendor guidance, with compensating controls where support gaps exist.

✓ OT Patching: A Risk-Aware Operation, Not a Routine Task
○ OT Visibility: See Everything. Miss Nothing.
○ OT Backup Is More Than Storage, It's OperationalInsurance
○ Third-Party Access: Vendors Can Be Your Weakest Link

2

OT Visibility: See Everything. Miss Nothing.

OT visibility requires a strategic approach. You can't protect what you can't see. OT environments are full of legacy infrastructure, specialized protocols, and unmanaged edge devices, blindspots are common. Misconfigured SPAN ports, unmanaged switches, and assumptions from IT-only experience lead to missed data, noise, and exposure. Real visibility steams a foundation to act faster, plan smarter, and secure what matters.

Best Practices for OT Visibility

→ Full OT Mapping

Identify every OT asset from SCADA and PLCs to legacy & isolated systems using OT-aware discovery.

→ Precision Monitoring

Configure network visibility to eliminate blind spots without flooding teams with noise.

→ Zero Trust Baseline

Establish clear asset and communication baselines so only expected OT traffic is trusted.

→ Non-Intrusive Discovery

Use passive techniques to surface unmanaged assets without disrupting operations.

→ Unified IT, OT View

Centralize OT and IT visibility on a single platform, enabling faster detection and coordinated response.

○ OT Patching:
A Risk-Aware Operation,
Not a Routine Task

✓ OT Visibility:
See Everything. Miss
Nothing.

○ OT Backup Is
More Than Storage, It's
OperationalInsurance

○ Third-Party Access:
Vendors Can Be Your
Weakest Link

3

OT Backup Is More Than Storage, It’s Operation al Insurance

Backup failures in OT can halt production, cause compliance violations, or even impact safety. Unlike IT, OT systems often lack redundancy, run on legacy infrastructure, and can’t tolerate downtime. You’re not just backing up files; you’re preserving control logic, SCADA configs, and HMI state. Without tested, offline, and targeted backups, you’re not protected. You’re just hoping.

How to Get OT Backups Right

→ Define RTO/RPO by System Impact

Use system criticality to set Recovery Time and Point Objectives. Not every system needs the same standard.

→ Air-Gap, Encrypt, & Lock Backups

Keep backups offline (air-gapped), immutable, and encrypted to prevent ransomware spread.

→ Follow 3-2-1, Plus Real Testing

Three copies, two media types, one offsite, and only count backups you've tested.

→ Know Where the Critical Data Lives

Back up PLC programs, SCADA configs, HMI images—not just general system files.

→ Automate, but Verify

Automation saves time, but regular manual verification ensures reliability.

○ OT Patching: A Risk-Aware Operation, Not a Routine Task
○ OT Visibility: See Everything. Miss Nothing.
✓ OT Backup Is More Than Storage, It’s OperationalInsurance
○ Third-Party Access: Vendors Can Be Your Weakest Link

4

Third-Party Access Vendors Can Be Your Weakest Link

Third-party vendors often need deep access to OT environments to support operations and system changes. Without clearboundaries and ongoing oversight, this access can introduce serious risk.

In our assessments, we've seen common shortcuts, like unmanaged remote tools or overly permissive firewall rules create vulnerabilities that remained hidden until visibility was enforced.

How to Manage OT Third-Party Access

→ **Defined Network Boundaries**

Strict segmentation between OT systems and vendor access zones.

→ **Controlled Access Paths**

Vendor access flows through monitored electronic security perimeters.

→ **OT-Aware Vendor Selection**

Partners are chosen based on real OT operational experience.

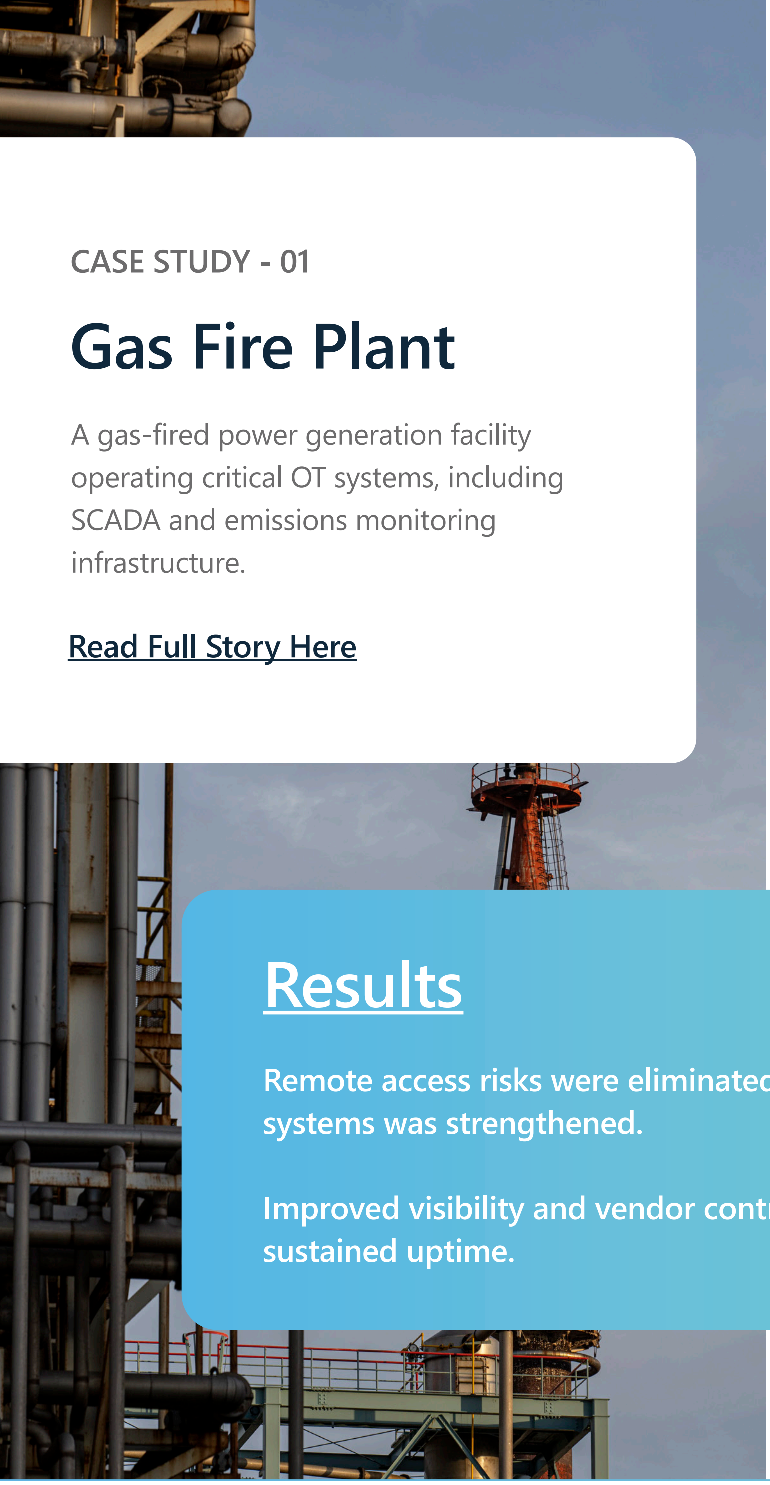
→ **Continuous Activity Monitoring**

Vendor behavior is monitored to detect shadow access and anomalies.

→ **Zero Trust Enforcement**

Access is isolated, time-bound, and limited to least privilege.

○ OT Patching: A Risk-Aware Operation, Not a Routine Task
○ OT Visibility: See Everything. Miss Nothing.
○ OT Backup Is More Than Storage, It's OperationalInsurance
✓ Third-Party Access: Vendors Can Be Your Weakest Link



CASE STUDY - 01

Gas Fire Plant

A gas-fired power generation facility operating critical OT systems, including SCADA and emissions monitoring infrastructure.

Read Full Story Here

Challenge

An unapproved third-party remote access tool created an unmonitored connection into the SCADA network.

This exposed the OT environment to lateral movement and potential operational risk.

Solution

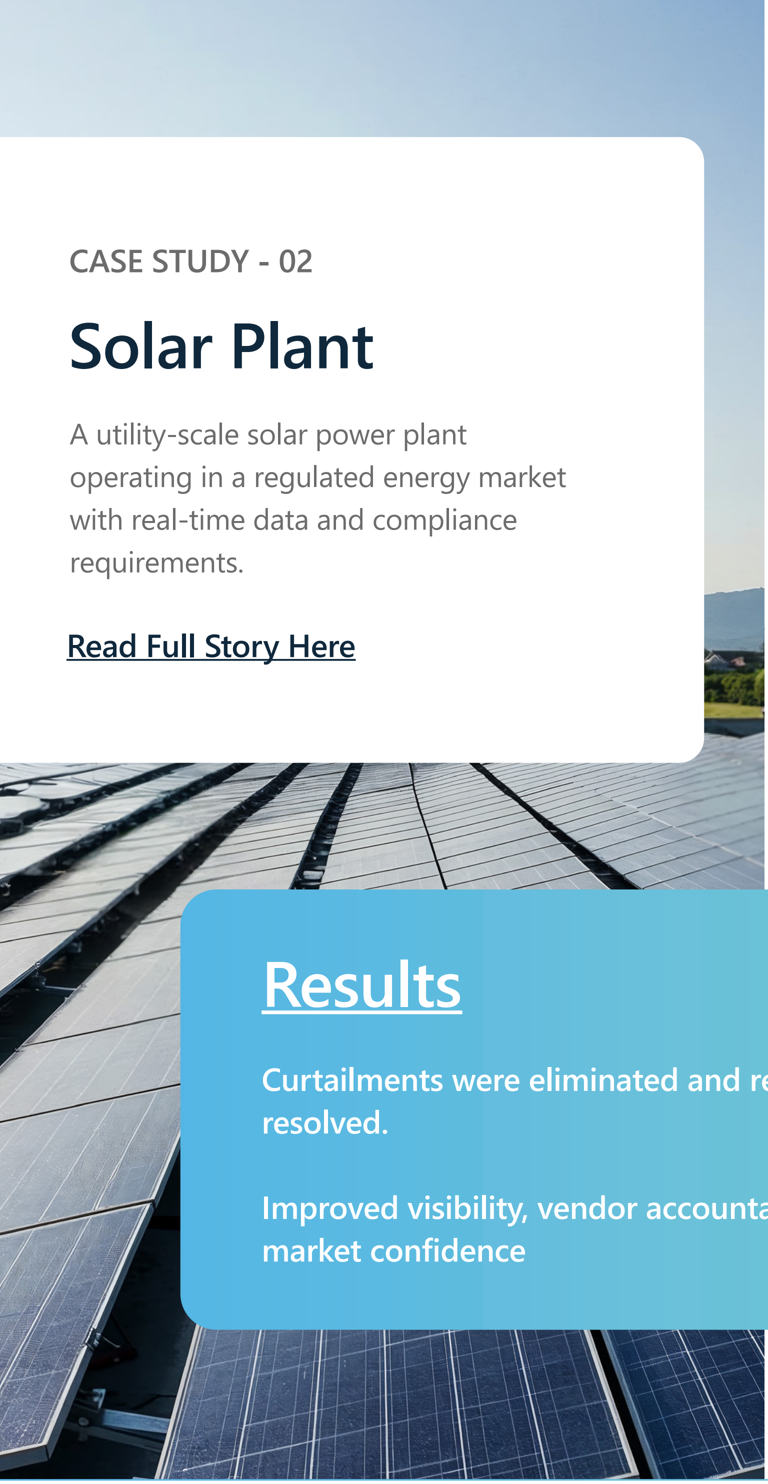
ProArch's OT Insights & Managed Services (OTIMS) detected the anomaly through continuous monitoring.

Remote access was disabled and segmented vendor access controls were enforced.

Results

Remote access risks were eliminated and cyber resilience across OT systems was strengthened.

Improved visibility and vendor controls ensured secure operations and sustained uptime.



CASE STUDY - 02

Solar Plant

A utility-scale solar power plant operating in a regulated energy market with real-time data and compliance requirements.

Read Full Story Here

Challenge

Unreliable SCADA and market data caused repeated curtailments and revenue loss.

Lack of system visibility and unclear vendor ownership delayed resolution.

Solution

ProArch’s OT Insights & Managed Services (OTIMS) assessed data flows and identified failure points.

Vendors were aligned and a tested failover strategy was implemented to stabilize market data.

Results

Curtailments were eliminated and revenue-impacting data issues were resolved.

Improved visibility, vendor accountability, and reliable reporting restored market confidence

Choosing The Right Provider

As the line between IT and OT continues to blur, the need for cybersecurity partners with deep expertise in both domains has become critical.

Through its OT Managed Services and Insights, ProArch provides 24x7x365 monitoring, vendor-agnostic support across ICS and control systems, and standardized security aligned to the Purdue Model. Continuous visibility, tested backups, asset discovery, and compliance support help organizations maintain resilience across their entire technology landscape.

87%

of industrial respondents believe that Zero Trust is the right approach to securing OT Environments.

Paloal Networks

ProArch’s OT Capabilities

We provide integrated IT and OT services to help industrial organizations improve operational visibility, security, and resilience. Our capabilities are built to support critical infrastructure environments with continuous monitoring, risk reduction, and operational insight.

OT Managed Services & Insights →

We provide continuous monitoring, operational insights, and managed support for OT environments. Our services help organizations gain real-time visibility into OT networks, detect issues early, and maintain reliable operations.

OT Security Services →

We provide OT-focused cybersecurity services designed to protect industrial environments without disrupting operations. Our approach helps reduce cyber risk, improve threat detection and response, and support compliance across ICS and SCADA systems.

IT and OT Services for Power & Utilities →

We provide IT and OT services tailored for power and utility organizations. Our capabilities support secure operations, improved asset visibility, and reliable delivery of critical services across complex infrastructure environments.

IT and OT Services for Manufacturing →

We provide IT and OT services for manufacturing organizations to improve production visibility, reduce downtime, and strengthen security across connected plant systems and operations.

proarch

ProArch is a Data and AI–first consulting and implementation partner, helping organizations harness cloud, cybersecurity, compliance, and software development to achieve their vision. We believe the future belongs to businesses that embed Data Governance, AI Adoption, and Responsible AI Innovation into the way they grow.

Our expertise spans Data Governance, AI Security, Microsoft Ecosystem, Agent Development, and GenAI testing—empowering organizations to innovate responsibly while ensuring security, compliance, and scalability.

Contact us to learn how ProArch can help you design, build, and test Responsible and Secure AI solutions.

✉ letstalk@proarch.com   🌐 proarch.com