aria CYBERSECURITY

Preventing Steel Production Disruptions

Industry: Steel Manufacturing
Use Case: Lockdown of Critical Steel Mill Production Systems
Solution: AZT PROTECT™

The steel industry relies heavily on operational technology (OT) to manage material processing, furnaces, cranes, steel pouring and milling operations. Automated processes driven by industrial control systems (ICS) keep the mills efficient. Anything that disrupts these processes must be avoided at all costs. Taking down production unexpectedly at a steel mill not only costs 10s of thousands of dollars an hour, but it is also a huge high-risk human safety concern. The reliance on interconnected OT systems also creates new points of risk. This steel producer had one mill taken down by the spread of ransomware for multiple weeks and wanted to avoid this at all other mills.

Sophisticated attacks can shut down production, causing financial losses and ripple effects that impact customer projects. Traditional IT-style defenses, based on antivirus updates and frequent patching, are ill-suited for these types of industrial environments where uptime is critical. AV tools need daily security updates which risk application crashes, false positives, and costly production disruptions. None of these IT AV endpoint solutions were built to stop polymorphic ransomware attacks that have not yet been seen before. Unfortunately, these type of modern attacks have accounted for 800 such ransomware-based site shutdowns in 2024, according to the FBI.

All that aside, the most important protection is from friendly fire. Unintended, untested updates occurring outside of scheduled maintenance windows are just as disruptive to production than any attack. Unfortunately, according to the industry, unintended updates disrupt ICS production at least 10,000 times per year. **Such disruptions are an order of magnitude more frequent problem.**

Meanwhile, this customer had many of their mills running ICS Systems on Windows 10 and were mulling over the impact of massive upgrades to Windows 11 to prepare for Windows 10 end of support and further security patches in October of 2025. Both operating systems and any underlying equipment replacements are an ugly option when there is no ROI on the 1000s of dollars per system that such an upgrade would occur.

The Challenge

Our client, a leading U.S. Steel producer needed a solution that could lockdown a plant from unintended production disruptions as well as attacks.

Specifically, they required:

1. **Protection for a wide range of devices,** including Rockwell FactoryTalk and other ICS products, HMI's, data historians, and lab systems.
2. **A solution that could be deployed once and stay secure** without the need for ongoing security updates that disrupt production.
3. **Full lockdown of critical devices** to prevent unintended IT updates outside of approved maintenance windows.
4. **Coverage for legacy (Windows 10) devices** without forcing costly migrations or hardware refreshes.
5. **A simple install process** that allows plant operators to deploy without requiring specialized security training.
6. **Fully automated protection** that stops issues before they become problems.
7. **Simple monitoring** allows plant operators to spend only minutes a week reviewing issues

The Solution

The steel producer chose AZT PROTECT™ — purpose-built for OT environments, to ensure continuous protection and uptime without the need for IT oversight. AZT PROTECT automatically learned all ICS applications, even those not currently running and locked them against unauthorized changes. Operating at the OS kernel level, AZT PROTECT continuously monitors executables and processes, blocking anything malicious or unapproved before it can run. At the same time, it safeguards approved applications and the OS from adulteration by preventing exploitation of both known and yet-to-be-discovered vulnerabilities. Powered by the AI agent on each endpoint, AZT PROTECT also guards against application impersonation, version tampering, lateral movement, and privilege escalation.

The Steel producer selected AZT PROTECT for several reasons:

- **AI-driven Lockdown of production systems:** AZT PROTECT locked down the critical ICS systems. The deployment was timely. It had an OT network DMZ firewall update issue the first month after AZT was deployed. The concrete manufacturer had to reset the firewall rules to default in order to recover. Over 400 unintended and untested application updates flooded the OT network. AZT blocked each as it tried to update and reboot the production systems. The operator was extremely happy that a potential disaster was avoided.

- **Defense against zero-days:** AZT PROTECT neutralizes both zero-day attacks and vulnerability exploits before they can execute. This enables OT operators to safely delay OS and application patching until scheduled maintenance windows, reducing operational burden while keeping production running smoothly. It also allows the removal of legacy AV systems that were no longer effective, stopping today's ransomware attacks on ICS systems.

- **Fast, non-disruptive deployment:** AZT PROTECT installs in minutes without reboots, hardware changes, or complex configuration. Fully compatible with both modern and legacy systems, including Windows XP, 7, and 10, as well as critical unsupported applications — allowing production plants to extend the life of existing assets without costly migrations.

- **Built for operators, not IT:** Deployment requires no specialized security expertise and can be completed in three simple steps. Once installed, the solution runs silently in the background, providing protection without ongoing tuning or management.

- **Reduced reliance on patching:** By stopping exploits at the code execution level, AZT PROTECT eliminates the need for constant patching. This avoids patch-related crashes, freezes, or degraded performance — reducing both operational risk and staff workload.

The Solution

With AZT PROTECT, the steel manufacturer achieved permanent protection against unscheduled updates, ransomware, and advanced cyberattacks — all without the operational risks associated with constant security updates. The result: 1) production systems were shielded from disruption, ensuring uptime and safety in an industry where disruptions not only impact the bottom line, but they also put human lives in jeopardy; 2) reduced risk that directly impacts revenue, and infrastructure project contracts; 3) requires no ongoing tuning or IT oversight — a true one-time deployment that plant operators can rely on; 4) legacy Windows 10 systems remained secure, and production continuity was guaranteed. In summary, **AZT PROTECT a simple and cost-effective solution that protects production from the industry's highest risks of disruption.**

Effective Cybersecurity Starts with a Trusted Partner

For more than 50 years, ARIA Cybersecurity has delivered peace of mind to some of the world's most critical organizations — including the U.S. Department of Defense, Western intelligence agencies and large manufacturers. Our proven solutions and expert team are here to help you protect what matters most.

To learn more about AZT PROTECT, contact us at info@ariacybersecurity.com or visit https://www.ariacybersecurity.com/aria-azt-protect/

ARIA Cybersecurity Inc.
175 Cabot Street, Suite 210
Lowell, MA 01854
+1 800.325.3110