Safeguarding Concrete Production from Disruption

Industry: Concrete Manufacturing
Use Case: OT Endpoint Protection for Critical Production Systems
Solution: AZT PROTECT™

The concrete production industry relies heavily on operational technology (OT) to manage crushing, grinding, mixing, preheating, calcination, final processing, and batching for large-scale delivery. Automated processes driven by SCADA systems keep plants efficient, but this reliance on interconnected OT systems also creates new points of vulnerability. Concrete producers are increasingly being targeted by organized crime groups and nation-state attackers aiming to disrupt operations and extort ransom payments.

These sophisticated attacks can shut down production, causing massive financial losses and ripple effects that impact customer projects. Reliance on firewalls alone is not working. Attacks are circumventing firewalls via the supply chain and other paths to land on industrial automation production systems. Another layer of protection is needed for these systems.

Traditional IT- style defenses, based on antivirus updates and frequent patching, are ill-suited for these types of industrial environments where uptime is critical; their need for daily security updates risks application crashes, false positives, and costly delays. None of these IT endpoint solutions were built to stop the sophisticated nation-state–sponsored attacks that now account for 17 percent of OT attacks in the US, according to the FBI.

Meanwhile, many facilities still depend on legacy systems and unsupported applications that can no longer receive security patches, significantly increasing risk. But complete equipment and system replacements are not an option in environments where infrastructure investments can take up to 10 years to recoup.

The Challenge

Our client—a major U.S. concrete company needed a solution that could protect its concrete plant from cyberattacks without disrupting operations.

1. **Protection for a wide range of devices**, including factory servers running Rockwell FactoryTalk and other DCS products, HMIs, data historians, and maintenance laptops.
2. **A solution that could be deployed once and stay secured** 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 devices and unsupported applications** without forcing costly migrations or hardware refreshes.
5. **A simple install process** that allows plant operators to deploy without requiring specialized security training.

The Solution

The concrete 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 concrete producer selected AZT PROTECT for several reasons:

- **AI-driven defense against zero-days:** AZT PROTECT locks down critical ICS applications and neutralizes both zero-day and unknown threats before they can execute. This enables OT operators to safely delay OS patching until scheduled maintenance windows, reducing operational burden while keeping production running smoothly.

- **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 Results

With AZT PROTECT, the concrete producer achieved permanent protection against ransomware, advanced cyberattacks, and unscheduled updates—without the operational risks associated with constant updates. Production systems are shielded from tampering, ensuring uptime and safety in an industry where delays directly impact revenue, supply chains, and infrastructure projects. Most importantly, the solution requires no ongoing tuning or IT resources—a true one-time deployment that plant operators can rely on. Legacy systems remain secure, and production continuity is guaranteed. In summary, a simple and cost-effective means of providing defense in depth for their OT environment from all forms of disruption.

aria
ZERO TRUST
PROTECT

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