aria
CYBERSECURITY

ICS LOCKDOWN:

Protecting Production Systems

The FBI reported 800 ICS organizations incurred site shutdowns in 2024 due to cyber-attacks. Yet the industry estimates 10,000 instances of unapproved OS/application updates bring ICS systems down during production each year **- an order of magnitude larger problem.** ARIA AZT PROTECT™ is the only AI-powered solution designed first and foremost to lock down your devices to prevent unapproved updates as well as stop cyberattacks. AZT delivers unparalleled protection—**Maximizing system uptime.**

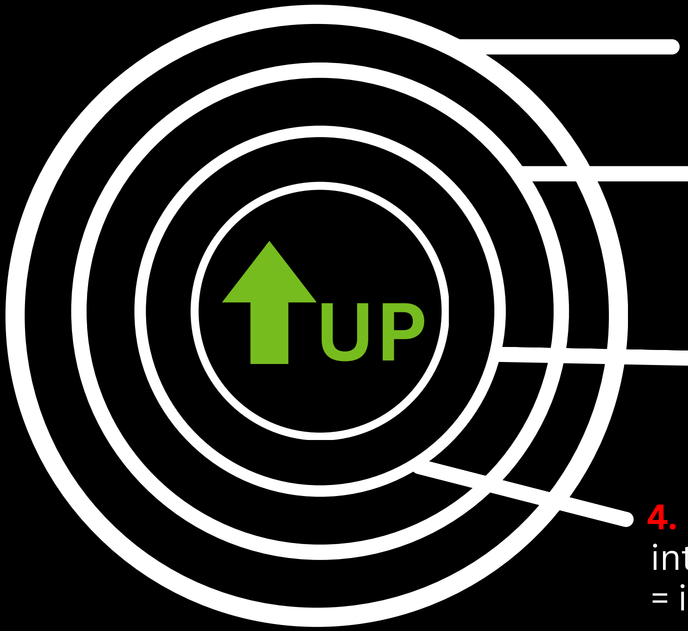
Straight-forward Value Proposition: Stops production disruption and reduces safety risks. Pushes out the need to perform patches and updates. Extends the life of out of support applications while being protected. AZT Protect removes the recurring risk of security update bluescreens, freezes and associated production downtime.

aria
ZERO TRUST
PROTECT

AZT PROTECT's Unique Advantages

- **Automated Lockdown Protection:** Automatically deploys on active production systems— learns your applications, running or not, and locks them down from further update. Checks them continuously and blocks any attempted version changes, adulterations or impersonations. Ensuring continuous uptime.
- **Real-time, Autonomous Defense:** AI-powered neutralization of attacks—including zero-day and unknown attacks—before they can impact operations. Allows production teams to put off patching until desired, if ever.
- **No Downtime, No Disruption:** Deploys in minutes, requires no re-boot. Set once and never touch again. Your systems stay up and running, always.
- **The Only Solution for Blocking Vulnerabilities:** AZT PROTECT's unique approach can stop code level vulnerability exploits. No patches required! Increase production time while reducing your operations risk and effort.
- **Legacy Operating System Support:** AZT PROTECT is the only AI solution that protects out of support applications back to Windows XP.
- **Zero Trust, Zero Hassle:** Delivers ironclad lock down without complex operations or the need for application expertise - making it easy for you to deploy and operate.
- **Protects What Others Can't:** Shields Windows & Linux OS including embedded systems. Works on legacy out of support systems. Deploys on X86 and ARM Core based platforms. Works in fully air-gapped network environments.

AZT PROTECT™: The 4 Circles of Production Uptime



1. ICS Lockdown: Stop "friendly-fire" unintended & untested updates that take systems down

2. Zero-Day Defense: Stop the Ransomware & Malware without risky updates = false positives that cause production application shutdowns

3. Exploit Shielding: Stops exploits of known yet known application vulnerabilities- without risky updates = Block code level exploits w/o waiting defenseless for security patches

4. Nation State Shutdown: Stop sophisticated intrusions & living off the land techniques = intercept and silently stop

LEARN MORE:

AZT™
PROTECT