aria
CYBERSECURITY

ARIA ZERO TRUST PROTECT™ (AZT)

SECURING WINDOWS END OF LIFE MACHINES IN OT ENVIRONMENTS

A SIMPLE APPROACH TO: **Protect Vulnerable Endpoints without Patching or System Updates**

Aria Zero Trust Protect™ (AZT) is an advanced endpoint protection solution designed specifically for **Operational Technology (OT) environments.** With many industry systems relying on **Windows 10 or older machine operating systems (OS's) at End -of-Life (EOL),** ARIA AZT Protect ensures these systems remain **secure and operational** without requiring disruptive updates or expensive upgrades. It doesn't require a reboot! This includes Windows embedded machines which can't easily be upgraded once deployed.

▶ **Why spend 1,000's per device upgrading - keep what you have and be more secure!**

WHY CHOOSE ARIA AZT FOR WINDOWS EOL MACHINES?

▶ **Agent- Based Protection:** Lightweight agent deployed on Windows endpoints, adding Zero Trust Security without impacting system performance- (Less than 2% CPU utilization)

▶ **No Patching Required:** Instantly protects machines that no longer receive security updates from Microsoft or your application vendors

▶ **Purpose-Built for OT:** Works in **air-gapped** environments and legacy systems, without requiring Internet connectivity

▶ **Threat Prevention & Containment:** Detects and blocks All malware, ransomware, and unauthorized applications before execution

▶ **Seamless Deployment:** Easily integrates into existing OT Environments without disrupting operations

▶ **Compliance Ready:** Maintain Cyber-insurance policy requirements while supporting regulatory requirements like **NERC CIP, IEC 62443 and CISA guidance**

UNIQUE VALUE PROPOSITION

ARIA AZT is the **only solution purpose built** to provide **Zero Trust endpoint protection for unpatched, legacy window machines -** a critical gap in industrial cybersecurity strategies. With ARIA AZT, organizations can extend the life of their OT systems while meeting modern cybersecurity requirements.

HOW IT WORKS

1. Deploy lightweight AZT agent to Windows endpoints.
2. Instantly block unauthorized applications including updates, and attempted exploits.
3. Continuously monitor for threats without performance impact.
4. Automatically prevent malware execution - no signature updates required.

KEY BENEFITS

▶ No dependency on **signature-based detection**, **IoCs, manual whitelisting/blacklisting, etc.**
▶ Protects **Windows 10**, **7, XP, and Server 2003/2008 machines**
▶ Reduces risk of ransomware, supply chain attacks, and unapproved OS/Application updates to **keep production running**
▶ Quick deployment with **minimal resource footprint**
▶ Maintains **system uptime and performance**

Prevents Attacks

Control & Monitoring