aria CYBERSECURITY SOLUTIONS

# PARTNER SALES PRIMER

## Key Benefits

**AZT PROTECT™** employs a patented, innovative approach designed to safeguard Windows and Linux endpoints from the most sophisticated cyberattacks, including zero-day attacks, ransomware, advanced persistent threats (APTs) and nation-state attacks.

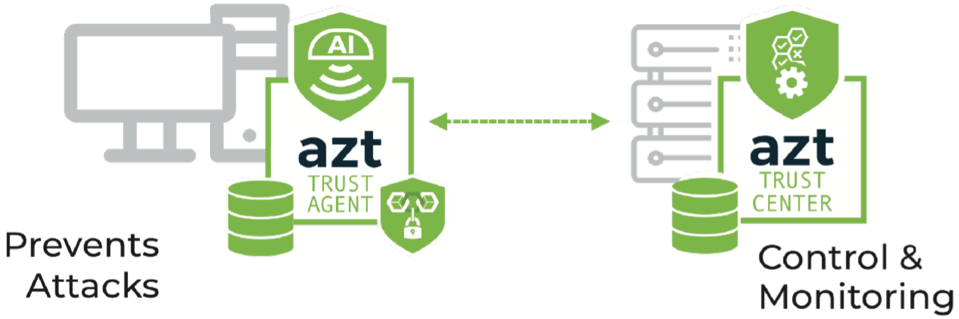
AZT uses reactive AI and kernel-level memory protection to instantly detect and block attack techniques on endpoints. Optimized for CPU and memory efficiency, it safeguards legacy applications on devices up to 20 years old without performance impact or system reboots.

- Automatically stops intruders and reduces code-based vulnerability exploits to near zero, minimizing the need for constant security patches.
- Delivers advanced application "allow-listing" that continuously locks down OT applications and hardens the systems OS.
- Easily installs within minutes, designed and built for Critical OT infrastructures.

There are two elements to the **AZT PROTECT** solution **Architecture:**

The **AZT Trust Agent** safeguards the OT network perimeter on all endpoint devices including desktops, laptops, and embedded devices. It occupies minimal space on a device, consuming **less than 2%** of CPU power.

The **AZT Trust Center** offers a comprehensive view of all endpoints and site locations, enabling seamless control and monitoring. It encompasses a range of functionalities, including policy and device management, application management, and alert monitoring.



## Solutions

| | |
|---|---|
| **AZT Endpoint Agent** | **SKU:** AZT-SW-AGNT-LIC |
| **AZT Trust Center** | **SKU:** AZT-SW-TC-LIC |

*Licensed on an Annual Subscription with Support SKUs* (All SW based, no HW required)*
*(Contact your Aria Regional Sales Director for the most up-to-date Promo's, Competitive Discounting & Licensing Offers.)

## Conversation Starters

- How do you secure Windows/Linux endpoints in your OT infrastructure (e.g., HMI's, SCADAs, maintenance laptops, control stations)?
- Do you run any legacy OS? If so, how do you mitigate risks without security patches?
- Have you experienced downtime due to cyberattacks?
- Do contractors or engineers remotely connect to the network?
- Are you facing cybersecurity insurance issues? High-premiums, loss of coverage or inability to get adequate coverage?
- Challenges with regulatory/compliance standards & guidelines (NIST, NERC CIP, ISA/IEC)? Pressure from the C-Suite, Board of Directors, etc. to secure the *Revenue* generating part of the business – OT.

## Tips, Hints & Talking Points

Concentrate on the primary concerns of OT and how addressing cybersecurity enhances **Overall Equipment Effectiveness** (OEE). (OT Security = Business continuity & stability: minimize change, maximize uptime)

Talk to:: Control Engineers, Automation Specialist, Plant Managers,etc. (Any OT Cybersecurity title/role when available e.g. OT Cybersecurity Architect, SCADA systems – Cybersecurity.) No cybersecurity expertise required—designed for OT staff.

AZT offers unparalleled protection against vulnerabilities and threats without administrative burden. **Simple** to secure critical endpoints, redirecting focus to operational efficiency and safety.

No other market solution offers this level of protection without updates, an internet connection, cloud connectivity, analytics, IoCs, or signatures.

aria CYBERSECURITY SOLUTIONS