

OEMs: SECURE BY DESIGN STARTS HERE.

AZT™

PROTECT

Adding ARIA AZT PROTECT™ to your packaged software stack differentiates your solution. AZT locks down your stack, preventing attacks and preserving performance while maximizing uptime for your customers.



AZT integrates easily into your software stack, locking down the OS and application layer, without disrupting either.

Your customers don't run your systems in isolation. One unauthorized (untested) OS update can change the tuned system performance which turns into your **warranty support escalations**. An infection on a single unit can cascade into **protracted downtime** on a customer line, **with stranded customers calling your support lines** for help.

AZT stops both situations before they start!

Improves Profitability & Market Share

- Adds **15–25% in increased gross margin** due to the value provided
- Improves RFP selection due to the value of a **built-in, instantly secured solution**

How: AZT prevents harm from attacks while locking the solution down to stop unauthorized updates that can disrupt production. AZT prevents safety issues, addresses compliance requirements, and reduces risk.

Reduces Warranty & Support Costs

- Reduction in the number of tickets and remote support cases
- Reduction in RMAs

How: AZT locks down the system to prevent undesired or untested OS updates that can impact performance. It keeps the device in a safe, known-good state, so you're not on the hook to diagnose cyber infections or customer-inflicted issues.

AZT generates \$100s in revenue and saves up to \$1,000s per device over its lifetime.

See our OEM Solution Lock-Down business case for the full financial breakdown.

[Learn more about AZT](#)

aria

CYBERSECURITY