

Transform device cybersecurity from a product liability into a high-margin competitive advantage. By embedding ARIA AZT PROTECT™ directly into your Operational Technology (OT), Industrial Control Systems (ICS), or medical devices, you lock down the operating system (OS) and applications, neutralizing cyberattacks and undesired updates before they can execute.

## 1. The Premium Monetization Strategy for OEMs

In today’s threat landscape, end users are hyper-focused on supply chain vulnerabilities and ransomware campaigns that target physical processes. Standard firewalls and reactive agent software are bypassed daily. By integrating ARIA AZT PROTECT™, you introduce a premium cyber-hardened tier to your product roadmap.

Premium Tier Upsell

+15% to +25%

Average margin expansion achieved by branding devices as “Zero-Trust Protected” and completely immune to binary exploits or zero-day script injections.

Competitive Win-Rate Acceleration

+38%

Outperform competitors in strict utility, defense, pharmaceutical, and critical infrastructure RFPs requiring rigorous compliance and active validation.

### Differentiated Value Realization

Zero-Trust Realized

Automatically profiles acceptable process parameters, locking application executables, scripts, and memory space against unauthorized drift.

Zero-Day Neutralization

Stops sophisticated malware, such as ransomware and advanced memory injections, without requiring any threat signatures or persistent internet-dependent cloud connectivity.

Instant Compliance

Satisfy compliance mandates including NERC CIP, NIST SP 800-82, IEC 62443, and NIS 2 straight out of the box.

## 2. Delivering Quantifiable Value to Your End Customers

When selling an AZT-embedded device, your sales force shifts the conversation from a cost-per-unit negotiation to a total cost of ownership (TCO) protection model. You provide a self-defending asset that guarantees operational continuity and uptime.

| Protection Feature           | Operational Benefit to Customer                                                                                              | Estimated Financial Value                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Application Lockdown         | Blocks arbitrary executable files, unauthorized updates, and malicious payloads from launching on the local host controller. | \$45,000+ saved per incident                                                                                           |
| OS and Application Hardening | Inhibits operational drift. Stops attacks targeting critical applications and embedded OS functions.                         | \$12,000 saved per asset per year                                                                                      |
| Memory Injection Shielding   | Defeats fileless, in-memory exploits seeking to hijack active, running trusted device processes.                             | Prevents catastrophic failures costing millions of dollars                                                             |
| Total Combined Impact        | Guarantees 99.99% production uptime against threat vectors with autonomous protection.                                       | Est. \$189,000 TCO savings<br>Based on 1 incident (\$45,000) plus 4 assets over 3 years (\$12,000 per asset per year). |

Securing the device doesn't just drive top-line revenue; it aggressively insulates your bottom-line engineering and support ecosystem. Unsanctioned device alterations, unexpected malware contamination, and field environment changes create astronomical costs.

### 3. Drastic Reduction in Warranty, Support, and Replacement Liability

Historically, up to 40% of standard OEM technical support incidents stem from unsanctioned changes, rogue applications, unintended operator errors, or opportunistic malware introduced via customer IT updates and USB drives. ARIA AZT PROTECT™ eliminates these issues by locking the device into its golden state.

#### Key Areas of Cost Mitigation

- **Fewer Truck Rolls:** Preventing application and OS corruption reduces the need for field service deployments to re-image devices.
- **Deflection of Warranty Disputes:** Because the application state is cryptographically locked down, unauthorized field manipulations are blocked, eradicating "gray area" liability disputes.
- **Elimination of Emergency Patch Cycles:** Protects OEM software running on Windows, Windows Embedded, Linux, and embedded Linux operating systems without requiring urgent code rewrites or emergency patches once vulnerabilities are found.

#### Support Ticket Drop

**65% Reduction**

Average decrease in high-tier technical support cases involving software anomalies or corrupted runtimes.

#### Field Replacement Savings

**\$4,500+**

Saved per field instance by avoiding emergency device replacement logistics, travel, and custom engineer hours.

### 4. The OEM Financial Impact Model (Per 1,000 Shipped Devices)

The following financial projection models the direct internal operational cost savings an OEM can expect over a standard 3-year support cycle after embedding ARIA AZT PROTECT™.

| Expense Category                                                                                                        | Legacy Device Model | AZT Embedded Model | OEM Bottom-Line Savings |
|-------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------|-------------------------|
| <b>Tier-3 Escalated Cyber/OS Support Tickets</b><br>Est. \$250 per incident handling cost                               | 450 tickets         | 158 tickets        | \$73,000                |
| <b>Emergency Field Dispatch and Truck Rolls</b><br>Est. \$3,500 per field deployment                                    | 35 deployments      | 7 deployments      | \$98,000                |
| <b>Unwarranted Hardware Returns (aka RMA)</b><br>Logistics, teardown, and bench testing. Est. \$2,400 per unit returned | 22 units            | 4 units            | \$43,200                |
| <b>Emergency Security Patch Engineering</b><br>Dev cycle, QA, regression testing, and release                           | 4 cycles per year   | 0 cycles required  | \$375,000               |
| <b>Total Operational Capital Reclaimed</b>                                                                              | n/a                 | n/a                | <b>\$589,200</b>        |

### Strategic Summary

Embedding ARIA AZT PROTECT™ transforms your device ecosystem. On the front end, it acts as a high-margin monetization engine, allowing sales teams to capture higher pricing tiers and achieve increased win rates. On the back end, it operates as a structural protection layer, deflecting more than half of your typical support engineering costs, reducing field interventions, and maximizing corporate profitability.