aria | CYBERSECURITY

AZT™ Embedded Protection: IOT

The Need: Fill the gap in protecting the Internet of Things
Use Case: Lockdown IoT endpoint systems to prevent service disruption
Solution: AZT PROTECT™

Requirements & Challenges

Today's next generation of services infrastructure relies on intelligent edge services devices. These edge devices are designed to be low cost and compute resource optimized to meet the commercial requirements of scale. Protection of these devices was never even considered an option because today's protection does not run on these devices or was thought to be commercially unviable. Protection was therefore treated by the cyber industry as "a best effort", left to network level protections. Such efforts have been proven to be entirely inadequate to cover this decade's needs.

The IoT services infrastructure requires 2 forms of protection:

1. **A means to lock down devices from unapproved updates, applications, and other undesired executables.** The idea is to maintain up time by minimizing the chance of disruption. Seeing as device resources are often constrained, adding new or updated applications must be well tested to be sure they are optimized to consume the fixed device resources. These devices are often difficult/expensive to replace and truck rolls need to be avoided. Unapproved updates, or unknown applications can also be a risk to the services being run or to the accessible data.

2. **A means to block cyberattacks.** Today's attacks are increasingly being engineered to attack IoT devices with malicious polymorphic code. Traditional Anti-Virus (AV) requires continuous connectivity, large amounts of computer and memory resources when processing updates for the latest leaned attacks. In most cases they cannot stop sophisticated supply chains or nation state backed attacks. In either case these protections typically were not designed to run on ARM core-based technology or require more resources when actively updating and scanning that hobble device performance and may require frequent device reboots. False positives are also an issue when an attack pattern mimics a production application - therefore these solutions must be actively monitored by a SoC team to maintain proper operation which adds significant operational costs**.**

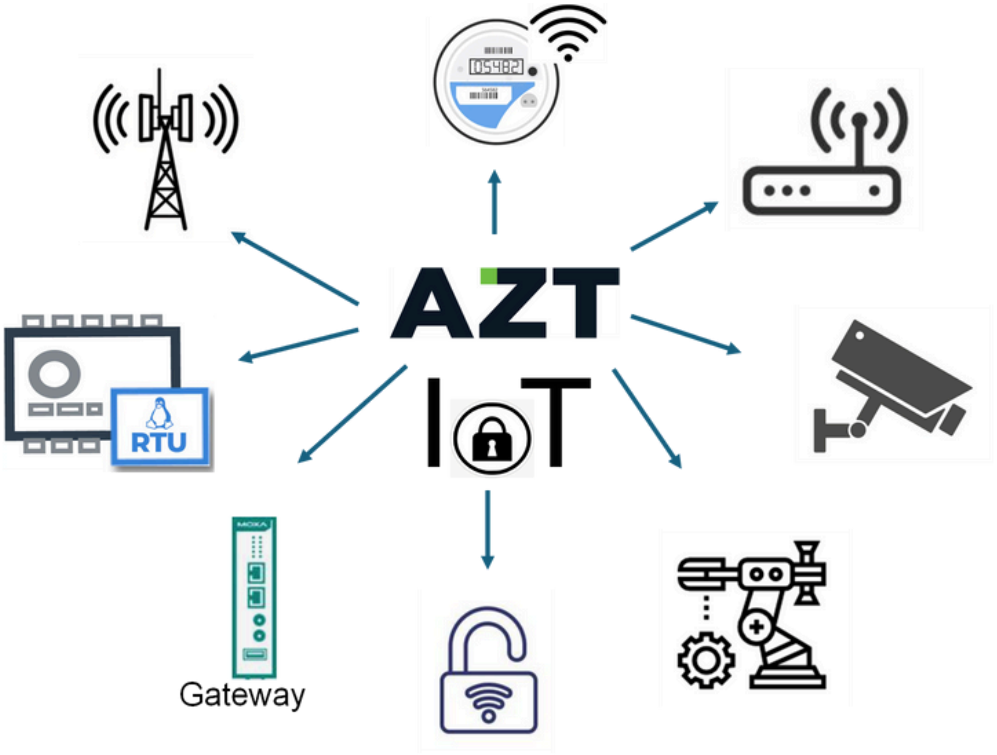
The Solution

ARIA AZT PROTECT™ solves all these issues with an effective protection solution that addresses both needs. A solution that can be quickly embedded by the device manufacturers or the solution vendors that provide these devices and their application suites.

How AZT’s Patented Approach Works

- Connects in as a Windows or Linux OS kernel level driver at Ring Zero
- See what is coming down the memory stack as it’s about to execute
- Stops unauthorized updates and attacks before they can execute
- Blocks application code-level vulnerability exploits
- AI driven fully automated generic form of protection.
- Never needs security updates, and can run forever network disconnected
- Removes need for OS security patch updates
- Ideal for “out of support” OS embedded versions.
- Stops the endless need for system reboots for patching
- Maximizes uptime impact, reduces risk, while ensuring compliance

IoT Protected devices and service examples:



Benefits:

- **AI-driven Lockdown of production systems:** AZT PROTECT locks down the critical IoT systems. Stopping unintended and untested application updates flooded into the IoT network. AZT blocks each as it tries to update and reboot the production applications. Allows updates to be managed to meet commercial operation SLAs with minimal disruption and uptime risk.

- **Defense against Zero-day, Supply Chain and Nation State attacks:** AZT PROTECT neutralizes both zero-day attacks and vulnerability exploits before they can execute. This enables IoT operators to safely delay OS and application patching until scheduled maintenance windows if ever, reducing operational burden while keeping production running smoothly. Effective at stopping today's ransomware attacks. Blocking supply chain vulnerabilities. Neutralizing nation state attacks.

- **Fast, non-disruptive deployment:** AZT PROTECT installs in minutes without reboots, hardware changes, or complex configuration. Fully compatible with both modern embedded and legacy systems—including Windows 10 back to XP, as well as critical unsupported applications—extending the life of existing IoT assets without costly migrations.

- **Built for operators, not IT:** Deployment requires no specialized security expertise and can be completed in one simple step. Once installed, the solution runs silently in the background, providing protection without ongoing tuning or management. Can be deployed/run of fully air gapped devices.

- **Reduced reliance on patching:** By stopping exploits at the code execution level, AZT PROTECT eliminates the need for constant patching. This avoids patch-related crashes, freezes, or degraded performance—reducing operational risk and workload.

- **Optimized to run on IoT:** NEVER utilizes more than 2% of CPU nor more than a few 10s of Megabytes of memory. Ensuring your applications run performance is optimized even when under stress.

- **ARIA backed from integration to deployment support, to monitoring 24x7:** ARIA's team is there every step of the way. Capable with assisting in turn-key integration and deployment

If your IOT solutions require protection, ARIA AZT PROTECT is built from the ground up to meet your needs.

aria
ZERO TRUST
PROTECT

Effective Cybersecurity Starts With a Trusted Partner

For more than 50 years, ARIA Cybersecurity has delivered peace of mind to some of the world's most critical organizations—including the U.S. Department of Defense and other Western intelligence agencies. Our proven solutions and expert team are here to help you protect what matters most.

To learn more about AZT PROTECT, contact us at info@ariacybersecurity.com or visit https://www.ariacybersecurity.com/aria-azt-protect/

ARIA Cybersecurity
175 Cabot Street, Suite210
Lowell,MA 01854
+1 800.325.3110