

ARIA AZT

REVOLUTIONIZING OT ICS PRODUCTION PROTECTION

DATA SHEET



Unplanned Updates, Rogue AI, and Attacks Threaten Uptime; Prevent Them with AZT PROTECT™

ARIA Cybersecurity's mission is to lock down critical devices, applications, and OS from disruptions of all kinds. This includes both Windows/Linux OT and IIoT devices used in production infrastructure across the globe.

Vulnerabilities grew over 1000% in each of the last 2 years on average, while over 900 reported ransomware attacks have targeted manufacturing supply chains, resulting in the loss of tens of billions in revenue over the last year. Rogue AI, where AI systems act against their intended purpose, is now acknowledged as a genuine threat by the leading model makers. At the same time, Dark AI attacks have surged over the past 18 months, using AI to discover and exploit undisclosed vulnerabilities before they are publicly known or patched. You care about keeping your production lines running and protecting your revenues. You can't allow the increased security risk to jeopardize critical production system output.

AZT PROTECT is an industry-proven lockdown solution built on a patented approach, developed with input from the NSA, which analyzes code as it executes in memory at runtime and blocks any code whose pattern or memory footprint differs from the trusted original. Next, it watches all known applications, including the OS as it runs to stop any attempt to adulterate the running code. Never-seen-before file-based and file-less attacks are stopped from doing harm. Application- and OS code level CVEs can't be exploited. Even unknown vulnerabilities can't be exploited. AZT is revolutionary in that it uses a set of countermeasures to take these actions and, as such- it NEVER needs updates to stop attacks. It's capable of running without ever requiring a network connection, supporting true air-gapped networks.

AZT PROTECT protects your devices (desktop, laptop, and servers as well as embedded devices, IoT/ARM core devices), including most OS versions from the latest and dating back to Windows XP, and enterprise Linux Kernels as far back as v3.10 running LSM. It does so by preventing malicious executables, scripts, injections, living off the land, remote code execution, privilege escalations, and other AI-generated attack attempts from executing on the device. When the integrity of an application is violated, AZT will stop the offending process and notify you of the prevented attack.

Over the past 4 years, AZT has been proven effective by successfully protecting over 1000 sites, while blocking 1000s of exploits. Customers who have chosen ARIA AZT will attest as to how simple it was to work with ARIA to deploy protection in their environments. See their [use cases](#), experience a demo, and even talk to them live.

KEY BENEFITS

- **Protects applications** by only allowing known-good applications to execute, while blocking any changes (exploits) to allowed applications as they run; includes the OS
- **Prevents advanced threats** including zero-days (blocked on day zero), APTs, and today's AI assaults
- **Protects endpoints** against all known and unknown application code-level CVE exploits
- **Protects legacy & embedded OS**, allows legacy OS to run safely. Automatically protects embedded IIoT without performance or cost impact
- **Never needs updates** – Unlike AV and EDRs; AZT requires no signatures or IOC updates, no false-positive-prone AI or ML, no cloud monitoring, and no risky, untested automatic updates that can reboot or blue screen your devices during production
- **Deploys in minutes**, fully protected Simple to deploy and operate; ideal for protecting OT environments, critical devices, and autonomous vehicles
- **Consumes less than 2% CPU usage**
No reboot/downtime on deployment
- **Stop security patching** – no need for continuous application patching and the risks and costs it brings to production
- **Supports air-gapped environments**
No external connection ever required
- **Improves plant operating margin**
Typically, from 1 to 4 percent



COMPONENTS AND SPECIFICATIONS

AZT Endpoint Agent

- **Host Machine OS:** Windows or Linux
- **Processors:** x86/x64 Intel/AMD 2 core or higher
- **Memory:** 100 MB available
- **Storage:** 200 MB
- **Networking:** 100 Mbps or Gbps, optional

AZT Trust Center

- **Host Machine:** ESXi 6.5+ or Hyper-V, Proxmox, Nutanix, and Cloud
- **Processors:** Intel/AMD 8-core or higher
- **Memory:** 16 GB
- **Storage:** 1 TB NVMe/SSD
- **Networking:** 1 Gbps

Advantages over the world's best EDRs

- Never needs updating
- Stops all attacks including Zero day and on day zero
- Works on Windows versions back to Windows XP
- Works fully air-gapped
- No need for untested updates
- Deploys live, no reboot required

Replaces need for security updates

- Works out of the box in minutes
- Protects OS's without the need for security patches
- Protects Applications as well
- Extends the life of EOS systems
- Deemed a compensating control to pass audits

Assists in Compliance

- ISA 95
- NIST CSF
- NERC CIP
- TSA, SEC
- IEC 62443
- NDIS 2

Improvement in Operating Margin

- AZT demonstrates an ability to improve margins 1-4%
- By improved production uptime
- Reduced patching costs
- Extended life of out of support endpoints

Instruction-level Methodology Conquers Current Industry Limitations

Protected by multiple patent filings, ARIA's TrustID™ methodology validates executable code by fingerprinting individual binaries with an immutable ID, while also protecting those applications as they run at the instruction level from adulteration. This secure technique avoids the high cost associated with daily security update computations of cryptographic signatures or lengthy IOCs at run-time. It also enables effective attack prevention at the device, regardless of its patching status.

This methodology enables "adaptive scrutiny" of all foreign code. AZT's Endpoint Agent identifies running software as trusted or untrusted without the resource-intensive, false-positive-prone behavioral-learning or AI techniques that rely on constant updates, all of which risk slowdowns or blue screens on underpowered production devices from resource starvation. Nor does it require a hole in your firewall back to a cloud monitoring service that constantly exports and analyzes your production code's behavior before flagging it as suspect and pushing blocking code down to endpoint agents, where it runs automatically and untested, and can shut down production, as happened in the July 2024 CrowdStrike incident that cost customers an estimated \$5.4 billion.

The Application Is the New Zero Trust Perimeter

With OT/IT integration, you can no longer trust a strong network defense to protect your production endpoints. What's worse is that friendly fire (mistakes that trigger unwanted updates during production) is 10 times more likely than an attack and just as harmful to your employees' safety as well as that of your consumers. AZT PROTECT has proven to block such updates that can take down production and create accidents or loss of the production process.

Unique Deterministic Detection

Continuous light-load AZT countermeasure computation is used to keep endpoints protected. AZT PROTECT lightweight endpoint agent delivers a simple approach to protection that does not need complex, resource-intensive, constant data collection nor updates of any kind. In fact, it can continuously protect without a network connection.

AZT™

PROTECT

SUPPORTED OS PLATFORMS

Microsoft (MS) Windows

- MS Windows Server 2003 SP2
- MS Windows Server 2008 (incl. R2)
- MS Windows Server 2012 (incl. R2)
- MS Windows Server 2016
- MS Windows Server 2019
- MS Windows Server 2022
- MS Windows Server 2025

Microsoft Windows Workstation & Embedded OS

- MS Windows XP SP2, SP3
- MS Windows 7
- MS Windows 10
- MS Windows 11

Linux (H1 2023)

- RedHat
- Ubuntu
- Debian
- Other upon request



State-of-the-art Attack Countermeasures

AZT PROTECT neutralizes the attack as it attempts to execute within the device's memory.

The specific patented method list includes:

- Heap Code Executions
- Unauthorized Functions
- Malicious Shellcode
- Reflective Injections
- Malicious Scripts
- JavaScript Injections
- Read Buffer Attacks
- Write Buffer Attacks
- Executable Tamper Attacks
- Privilege Escalations
- AZT Protection
- Unauthorized USB Connection
- Unauthorized device network connections

Multi-site Alert Monitoring & Control

The AZT Trust Center provides a unified view for data collected within/across multiple sites that are secured by AZT PROTECT. It allows individual devices, device groups or entire sites to send alerts upstream to a central or higher-level Trust Center. This provides a broader view of a large enterprise or global business that contains multiple business units or departments.

The AZT Trust Center provides reports and detailed forensics and analytics that can be imported into SIEMs such as Splunk or ARIA's own ADR for OT security, monitoring, compliance and the overall cybersecurity hygiene of the organization.

AZT Application Protection as a Service

AZT is also optionally provided as an application attack prevention service, where our 24x7 SOC staff monitor, and keep safe your production environment for you continuously as a service. This leverages our staff's expertise to provide you the peace of mind to protect your (or your customers') production OT environments without the need of trained skilled staff.

info@ariacybersecurity.com



www.ariacybersecurity.com