Solution Overview

aria ZERO TRUST

ARIA Zero Trust PROTECT™

a Revolutionary New AI-driven Approach to OT Cybersecurity

aria CYBERSECURITY SOLUTIONS

INTRO / HIGHLIGHTS

ARIA Zero Trust PROTECT (AZT PROTECT™) is a new generation of endpoint security protection designed for critical operational technology (OT) environments. This unique patented solution protects all your endpoints from the full spectrum of cyberattacks and intrusion techniques, including the most advanced zero-day attacks, malware, ransomware, supply chain vulnerabilities – even those threats that are completely unknown to security teams. It proactively halts attacks before any damage occurs, ensuring seamless operations without disruption or downtime.

Delivering a revolutionary patented approach to OT endpoint cybersecurity, AZT PROTECT:

- Represents a great leap forward in the evolution of cybersecurity, surpassing anything available today.
- Requires no cybersecurity expertise and can be set up in minutes. It uses minimal computing power and does not impact critical devices or applications in any way.
- Keeps your production lines running and your critical systems safe, protecting your revenue and profitability.
- Lowers the risk of security vulnerability exploit on your endpoint device applications to near zero without the need for constant patching updates.

AZT PROTECT's unique capabilities

- Stops all attacks immediately as they try and execute on a protected device
- Stops attacks that leading cloud-based endpoint detection and response (EDRs) solutions do not: true never-seen-before zero days, supply chain, and nation-state backed attacks
- Understands known good applications and processes – and blocks the rest
- Provides a lightweight agent that can be rolled out on OT equipment with 20-year-old OS versions
- Makes each endpoint fully independent – no need for cloud updates to block new attacks
- Can run fully air-gapped and supports OT equipment with 20-year-old OS versions

A Purpose-built Solution for Protecting OT

AZT PROTECT was developed specifically to work within the constraints of an network environment. This means support for todays Linux and Windows OS as well as backward compatibility with legacy Windows operating systems – all the way back to Windows X. It works in real time, using distributed AI within each AZT endpoint agent to continually monitor for and prevent application modifications or changes in execution without the need for resource-intensive behavior analysis that risks producing false positives. Everything is either trusted or not trusted.

MARKET CONTEXT

Rapid digital transformation is blurring the boundaries between IT and Operational Technology. OT networks have traditionally been “air gapped” and kept isolated from the outside world, but this is no longer the case. Most OT networks are now connected to the internet and therefore increasingly vulnerable to cyberattack. A successful attack on critical infrastructure – launched by cybercriminals, hacktivists, or nation states – can have wide ranging repercussions, from operational disruption and revenue loss to major incidents that impact public safety. AZT PROTECT protects all industries that rely on business-critical OT networks, including pharmaceuticals, manufacturing, logistics, transportation, energy, and utilities.

Responding to high profile cyberattacks on critical infrastructure such as the Columbia Pipeline, the US Department of Homeland Security began issuing directives requiring OT networks to be continuously monitored and protected. Insurers are also demanding measures to protect critical OT devices from exploits and other attacks are implemented as a condition for providing business continuity insurance.

Simply placing OT devices under existing IT governance and monitoring processes to meet these new requirements does not go far enough. That’s because current IT best – practice processes, such as continuous patching, is not suitable for devices that can only be taken offline for a few times per year because of the criticality of their function and the massive dollar loss frequent shutdowns would have on reportable revenue. Nor do these processes scale to handle the increasing frequency and severity of new threats as cyberattackers take advantage of the latest advances in generative AI.

Most enterprises running OT networks lack the specialist skills and human resources to keep up to date with emerging threats. They also require the tools to protect both modern and decades old legacy systems from all forms of attack. AZT PROTECT is designed from the ground up to address all these challenges and keep your critical production facilities protected.

Utilities

Protect against outage, service disruption, and safety hazards by ensuring secure operation of systems such as electrical grids, water treatment plants, and oil and gas facilities.

Manufacturing

Protect production lines and processes, prevent disruptions and downtime, and safeguard supply chains.

Pharmaceutical

Protects critical research and development, and high value productionwithin a strict regulatory environment.

Bank and Finance

Protect critical backend servers and Cloud instances runing business critical applications.

Energy

Protect energy production based on oil, gas, nuclear, hydro, and renewables from disruption and safety risk.

Logistics

Protect transportation, inventory management, and supply chain systems; safeguard sensitive data, including shipping information and financial transactions.

Transportation

Protect the OT systems that are used by airplanes, airports, and railroads from disruption and dangerous attacks, including terrorism.

Autonomous Devices

Protect against application compromise, disruption, and loss of control of autonomous vehicles, ships, drones, and other robotic systems.

Hospital and Clinics

Protect PMS, Patient care systems as well as imaging systems with legacy OS.

HOW IT WORKS

"Set and Forget" – How AZT PROTECT Takes the Pain Out of OT Cybersecurity

AZT PROTECT is based on a lightweight AI-driven agent that is distributed to each device that needs protection and monitoring. The solution is designed to protect critical devices on OT and IT networks by neutralizing cyberattacks before they cause harm.

Protects ALL critical applications from being attacked

AZT PROTECT applies protection based on its ARIA TrustID, a binary code that uniquely identifies each application, executable process, and file. This patented process digitally analyzes code executing in memory in real time, instantly blocking any code that has a different digital pattern and memory footprint from the original source – without the need for sending and receiving data from third – party clouds. You set – up once and remain fully protected. The AI engine also detects and prevents attempted injections and other forms of modification that can fool even the best application control products. Once applications are locked down it does not matter if they have known or unknown vulnerabilities – AZT PROTECT protects them all from being exploited.

Deploys countermeasures to prevent fileless attacks

AZT PROTECT uses patented AI – driven countermeasures to stop the tactics used by sophisticated attackers to gain control of applications or devices. These countermeasures stop fileless attacks out of the box, by identifying the technique used by the attack such as a malicious script. Unlike many of today's EDRs, it will not result in a false positive that will shut down your production applications unnecessarily.

Uses AI to examine use of legitimate certificates

In the SolarWinds attack compromised code was pushed to SolarWinds' customers under legitimate software certificates. This case, alongside the Microsoft Exchange supply chain attack, forced the leading EDR and application control solution vendors to explain why they could not prevent this type of attack. AZT PROTECT's countermeasures detect and stop these attacks where other security vendors cannot, providing protection against the coming wave of AI-driven attacks.

Prevents privilege escalation

ARIA PROTECT prevents privilege escalation from “User” to “Admin” levels, preventing undesired device and application-level communication. It also includes measures to prevent the AZT PROTECT agent from being compromised, deactivated, or removed.

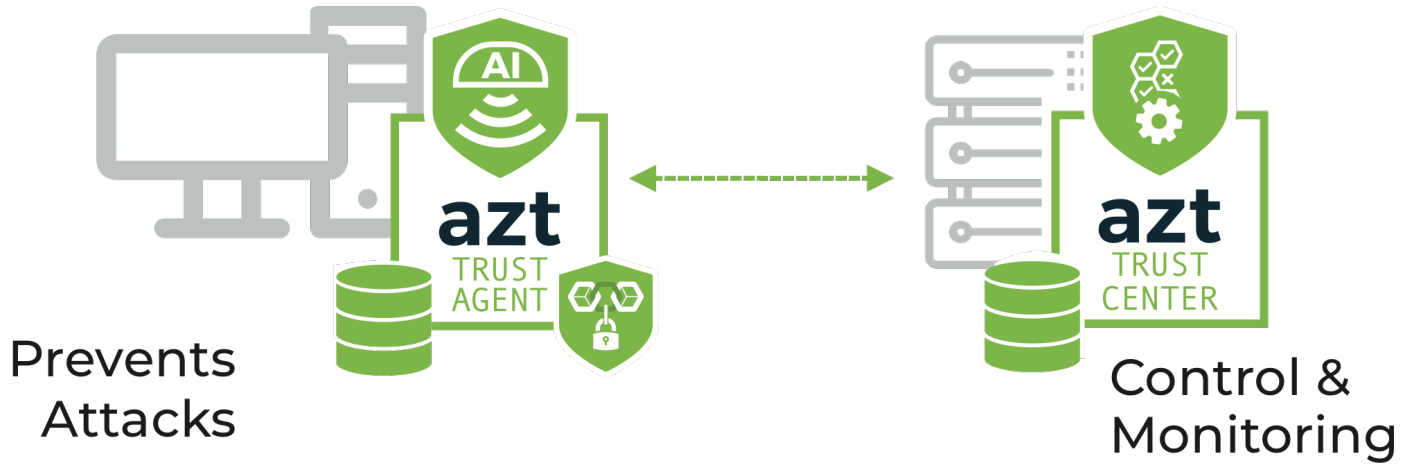
Ensures autonomous operation

AZT PROTECT is distributed to each device so that it works completely autonomously, avoiding the need for any centralized interaction that could allow harm to be done. There is no need to send suspect code and processes found on critical devices to a vendor’s cloud in an unknown location for analysis. And there is no need to receive fixes that are untested in your environment.

There are two elements to the AZT PROTECT solution architecture:

1. The **AZT Trust Agent** protects the OT network perimeter on all endpoint devices, spanning desktop, laptops, and embedded devices. It takes up minimal space on a device, consuming less than 2 percent of CPU even on legacy systems deployed decades ago. It does not require internet connectivity, making it suitable for fully air-gapped environments.

2. The **AZT Trust Center** provides a unified view of all endpoints and site locations for control and monitoring. This includes policy and device management, application management, and alert monitoring.



KEY BENEFITS

A Fully Featured, Customizable Cybersecurity Solution for All Types of OT Networks

Ten reasons AZT PROTECT is the most comprehensive OT cybersecurity solution available today:

1) **Breakthrough protection against the unknown**

AZT PROTECT's patented technology is the industry's only proven solution to protect against never – seen – before application and OS vulnerabilities—neutralizing attacks before they cause harm.

2) **Prevents even the most advanced zero-day attacks**

It takes time for security teams to respond to a zero-day exploit. There is no delay with AZT PROTECT. By automatically blocking every method, you're protected before Day Zero arrives.

3) **Works straight out of the box**

AZT PROTECT is up and running in minutes, requiring no specialist cybersecurity expertise or training. Its purpose-built AI does all the work.

4) **No need for cloud connectivity**

Your data does not need to be constantly exported to third-party clouds located who knows where. Nor do your systems need to download untested software updates from the cloud to stay protected.

5) **Ensures data sovereignty**

By never exporting your data to unknown or foreign locations, your valuable information never has to leave your premises.

6) **A super-lightweight endpoint agent**

AZT PROTECT uses an extremely low footprint on devices so there's no chance of disrupting your critical operations.

7) **Preserve your investments in legacy technology**

Protection for devices running Windows OS versions stretching back 20 years (to Windows XP). AZT PROTECT supports enterprise Linux as well.

8) **Support for the latest computing platforms**

AZT PROTECT offers full support for the latest processing architectures and is easily deployed on X86 and ARM-based devices, protecting all desktops, laptops, servers, and private cloud instances.

9) **Advanced firewalling within the same solution**

Avoid the complexity of isolating various parts of your network (micro-segmentation) by using AZT PROTECT's intelligent agent device-based firewalling capabilities that adapt to your network situation.

10) **Available as an outsourced service**

Implement the solution in the way that works for you, with the option to deploy as a managed service monitored daily by ARIA's US-based, US citizen-only Security Operations Center (SOC).

Contact Us to Schedule a Technical Demonstration or Arrange an Evaluation ARIAsales@ariacybersecurity.com

EFFECTIVE CYBERSECURITY STARTS WITH A TRUSTED PARTNER

ARIA Cybersecurity has been providing its customers with peace of mind for more than 50 years. We have provided security solutions to some of the most critical organizations in the world, including the US Department of Defense and other Western intelligence agencies.

Our cybersecurity experts work with you every step of the way. Contact us for more information on AZT PROTECT at info@ariacybersecurity.com or www.ariacybersecurity.com.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854

Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110
Follow Us: Linkedin • Facebook • Twitter • Blog