ARIA ZERO TRUST PROTECT™

Autonomous inoculation
protection for IT & OT environments

Kernal Level driver approach - generically stops today's known and yet to be known attacks w/o updates

The Problem

Today's polymorphic zero-day attacks have outpaced traditional IOC based security methods and requires a different way of thinking. Most solutions try to stop attacks at the device or network level but are ill equipped at protecting the actual applications that run on them. The state of the ART NGAV looks for set IOC patterns to ID the attack and apply the appropriate block. However, today's latest attack can change/iterate the attack behaviors almost daily so that they are always one step ahead of the defender's ability to create new blocks. In addition, sophisticated attackers can get by NGAV and EDR approaches by exploiting application vulnerabilities as well as lever other sophisticated attack techniques once they have a foothold. Worse these solutions can be bypassed or turned off by sophisticated attackers.

The Solution

ARIA built a simpler generic approach to stopping these attacks by stopping the attacks as they try and execute in device memory, before ANY harm can be done. We start by locking down the applications running from adulteration by blocking code-based exploits of their vulnerabilities in real-time. Additionally, we watch for the techniques sophisticated cyber crime or nation state-based attackers use and block them as they go active. Finally, we can also lock the device down to only run known verified and approved applications. In this way we can stop any foreign code like zero-day malware/ransomware from executing, as well as stop the sophisticated attacks today's solutions can't easily detect let alone stop. Our goal was to create simple to operate fully automated Cybersecurity PROTECTION that anyone can use.

How it works

AZT is a lightweight, autonomous kernel level driver, that installs at Ring 0 in your Windows (XP- onward) or Linux systems. It's fully integrated into the operating system monitoring all activity of the programs running in device memory. Its design only allows verified and unadulterated applications or executables to run in memory starting at launch and monitored continuously through operation. Every other executable is denied. In addition, we watch for injection of new binaries in live memory, we watch the buffers for the appearance of unexpected shell code, attack processes and other techniques used by attackers to gain control. Our patented AI engine blocks these malicious techniques by applying the appropriate counter measures built into each agent, so nothing slips by. This is the most effective way to stop the sophisticated attacks including, imposter applications, zero-day malware,/ransomware (on day zero), fileless attacks, living off the land, supply chain, and even the obfuscated never seen before techniques- used by nation-state backed attacks.

Monitors & intercepts ALL exploits in MEMORY!

ARIA ZERO TRUST PROTECT™

Autonomous inoculation
protection for IT & OT environments

How it's Different

Kernal Level driver approach - generically stops today's known and yet to be known attacks w/o updates

	State of the Art	ARIA AZT
NGAV/EDR	Attempts to stop live attacks, misses those unseen before,. Can't stop Zero-days on day zero, nor stop supply chain/ nation state attacks. No air gapped network support. Can be turned off by sophisticated attackers. Does not support Legacy OS. Can affect application performance. Must be connected to Internet.	Prevents exploit of code –based application vulnerabilities (known and unknown) Stops zero days, stops supply chain and nation state backed attacks, for IT & OT, including air gapped networks. Works at Kernel level Ring zero can't be turned off. Works on 20-year-old legacy OS deployments without performance impact. Deploys without requiring a device reboot. Does not need an Internet connection
Patch/Vuln Management	Only stops known CVE's once patches are available often months after CVE published	Stop all code-based application exploits automatically (known or unknown) - security patch at your leisure
Allow Listing	Labor intensive, expensive, disruptive, looks once upon boot – never again while running, misses application adulterations process-based nation state-based attacks	Fully automated, watches applications continuously for adulterations. EZ install & management, AI based countermeasures catch the attacks including nation state backed.
Network based Security	Labor intensive up front/ongoing, capital expensive. Passive approach misses application-level, zero day and sophisticated attacks	Device level application protection installs on any IT OT device without performance hit, protection is fully automated no human effort.

Learn More: AZT Overview, AZT Case Study, AZT Whitepaper

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that true innovation starts with a smarter approach. Our customers rely on our solutions protect their most critical assets and applications. With a 50-year proven track record supporting the largest Govt and Enterprise to SMB, ARIA is committed to leading the way in cybersecurity success for everybody.

ARIA Cybersecurity Solutions • 175 Cabot St, Suite 210 • Lowell, MA O1854
Connect with Us: ariacybersecurity.com • ARIAsales@ariacybersecurity.com • 800.325.3110