AV-Comparatives Publishes Operational Technology (OT) Security Test of ARIA AZT PROTECT™

AV-Comparatives has published the results of a test evaluating security products in air-gapped Operational Technology (OT) environments.

INNSBRUCK, LOWELL MA, MA, UNITED STATES, July 11, 2025 /EINPresswire.com/ -- AV-Comparatives, the leading independent testing organisation for cybersecurity solutions, has published the results of a test evaluating endpoint security products in air-gapped Operational Technology (OT) environments. The test focused on one of the most demanding and under-tested threat models in industrial cybersecurity: offline, post-breach attack scenarios in fully isolated systems.

Logo ARIA Cybersecurity

Download the Full Report here: https://www.av-comparatives.org/reports/aria-zero-trust-protect-operational-technology-ot-test/

OT security refers to the protection of hardware and software systems used to control industrial operations, including those in:

> “Testing in true offline conditions is often neglected in security evaluations. This report highlights how solutions like ARIA AZT PROTECT can enforce strong execution control in OT environments.”
> *said Peter Stelzhammer, co-founder of AV-Comparatives.*

- Manufacturing
- Energy and utilities (e.g., power plants, water treatment)
- Transportation (e.g., railway systems, airports)
- Critical infrastructure (e.g., oil pipelines, industrial robots)

Examples of OT systems:

- SCADA (Supervisory Control and Data Acquisition)
- PLC (Programmable Logic Controllers)
- DCS (Distributed Control Systems)

The evaluation tested ARIA AZT PROTECT alongside two other enterprise-grade endpoint security

platforms, examining each product's ability to prevent execution of untrusted binaries in fully offline conditions. All systems were evaluated in simulated post-breach environments, with test cases including code injection, binary impersonation, DLL sideloading, and supply chain tampering.

Logo AV-Comparatives

ARIA Expert Reviewing AI-driven Defense System

The test was conducted using a controlled, air-gapped lab setup. All products were installed on isolated Windows 10 systems and tested without internet connectivity. An application update test was also included to assess the ability of each solution to distinguish between malicious and legitimate software activity in an offline context.

ARIA AZT PROTECT successfully blocked all malicious execution attempts across five attack scenarios. After a configuration adjustment consistent with its OT enforcement model, the product also permitted a legitimate software update to complete without issue. ARIA's approach relies on strict trust enforcement at the kernel level, making it well-suited for high-security environments where internet connectivity is restricted or unavailable.

"Testing in true offline conditions is often neglected in security evaluations," said Peter Stelzhammer, co-founder of AV-Comparatives. "This report highlights how solutions like ARIA AZT PROTECT can enforce strong execution control in OT environments, even without cloud intelligence or behavioural learning."

"AZT PROTECT as a 4th generation endpoint protection platform was created to stop today's sophisticated attacks on OT Endpoints as well as prevent nation-state attackers from turning protection off which is an industry problem," said Gary Southwell President of ARIA Cybersecurity. "AV-Comparatives is respected in the industry for its ability to take on difficult testing challenges and provide simple to understand comparisons. AV-Comparatives confirmation that ARIA's AZT PROTECT works well to PROTECT OT environments provides the industry assurance their production endpoints can be fully protected even if no further security patches are available for out of support applications."

About ARIA AZT PROTECT
ARIA AZT PROTECT is an endpoint protection platform built specifically for OT environments. Operating at the kernel level (Ring 0), the solution enforces binary-level trust policies, allowing only explicitly approved executables to run. It is designed to work in fully offline environments, including legacy systems where cloud access or regular patching is not feasible. The product can operate standalone or in conjunction with traditional endpoint protection platforms.

About AV-Comparatives
AV-Comparatives is an internationally recognised independent testing lab based in Innsbruck, Austria. The organization performs regular public and commissioned evaluations of cybersecurity solutions across categories such as endpoint protection, anti-malware, mobile security, and advanced threat protection. This offline OT evaluation reflects AV-Comparatives' ongoing commitment to supporting cybersecurity decisions in critical infrastructure sectors.

Download the Full Report here: https://www.av-comparatives.org/reports/aria-zero-trust-protect-operational-technology-ot-test/

Peter Stelzhammer
AV-Comparatives
+43 512 287788
email us here
Visit us on social media:
LinkedIn
Facebook
X