CASE STUDY 2025

EVIDENCE BACKED

THIRD PARTY TESTING PROVES ARIA AZT PROTECT BLOCKS EVERY ATTACK!

Contact: Peter Moore | Sales and Technical Director

Email: pmoore@logitech.com.au

Contact: Ben Kirk | Business Development Manager

Email: bkirk@logitech.com.au

logi-tech PARA BELLUM SOLUTIONS aria CYBERSECURITY

ARIA CASE STUDY 2025

About Logi-Tech

Logi-Tech provides comprehensive cybersecurity services designed to help clients understand and strengthen their security posture. In addition to technical solutions, Logi-Tech offers strategic guidance on policy and governance to reduce human error and support compliance with frameworks such as the Payment Card Industry Data Security Standard (PCI DSS), the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the Australian Cyber Security Centre (ACSC) Essential Eight.

Key services include continuous asset validation through automated penetration testing and a full Security Operations Centre (SOC) as a service.
This includes:

- Security Information and Event Management (SIEM)
- Security Orchestration, Automation and Response (SOAR)
- Endpoint Detection and Response (EDR)
- Network Traffic Analysis (NTA)
- User and Entity Behaviour Analytics (UEBA)
- Artificial Intelligence (AI) and Machine Learning (ML)
- Ransomware protection
- Application allow listing
- Email filtering and phishing detection
- Staff education and awareness tools

Logi-Tech also provides expert advice and tools for business continuity and disaster recovery, supported by experienced professionals who can implement and maintain these solutions.
Additional capabilities include:

- Leading the design and management of security strategies
- Incident management and response
- Automating risk profiling, asset inventory, and security operations
- Conducting cybersecurity, regulatory, and risk management reviews
- Delivering phishing simulations and targeted staff training
- Investigating security incidents
- Threat containment and eradication
- Business continuity planning
- Disaster recovery strategy
- Testing operational and executive response plans
- Designing and implementing cybersecurity architectures
- Deploying firewalls and Intrusion Prevention Systems (IPS)
- Endpoint security solutions
- Identity and Access Management (IAM)
- Attack surface management
- Threat detection and prevention
- Intrusion Detection Systems (IDS)
- Vulnerability scanning
- Penetration testing
- SIEM deployment and monitoring

These integrated services provide real-time insights and measurable outcomes, protecting even legacy operating systems and operational technology (OT) environments from modern threats, including zero-day vulnerabilities.

Evidence Backed – Third Party Testing Proves ARIA AZT PROTECT Blocks Every Attack!

In an increasingly interconnected world, Operational Technology (OT) networks face unprecedented cyber threats. Unlike traditional IT systems, critical OT devices, which often underpin essential services and industrial processes, cannot tolerate frequent downtime for security patches. This inherent fragility, coupled with escalating regulatory demands and insurer requirements, has created an urgent need for specialized and robust OT cybersecurity solutions.

Enter ARIA Zero Trust PROTECT™ (AZT PROTECT), a groundbreaking endpoint security solution engineered specifically for the unique demands of critical OT environments. Heralded as a revolutionary AI-driven approach, AZT PROTECT operates on a fundamental principle: it inherently understands and permits only "known good" applications and processes, effectively blocking everything else. Its lightweight agent can be deployed even on legacy OT equipment running operating systems decades old, ensuring each endpoint is autonomously protected without relying on constant cloud updates. This design prioritizes keeping production lines operational and critical systems secure, directly safeguarding revenue and profitability.

But how does AZT PROTECT truly stand up against real-world threats? Two independent assessments provide compelling evidence of its impressive capabilities.

Secure Network Technologies (SNT) Assessment: Comprehensive Prevention Proven

In April 2025, Secure Network Technologies (SNT) conducted an assessment for Aria Cybersecurity, evaluating ARIA Zero Trust Protect (AZT) application version 1.15.8.13. The primary objective was to determine AZT PROTECT's efficacy in preventing common threat actor techniques from deploying or injecting malware on Windows hosts.

SNT's methodology meticulously replicated real-world attack paths using consistent and reproducible Techniques, Tactics, and Procedures (TTPs) favoured by threat actors. The testing environment mirrored a standard enterprise setup, including Windows 10, Windows Server 2008 R2, and Windows Server 2019 64-bit virtual machines, loaded with typical applications like Microsoft Office and Visual Studio Code. Attackers utilized Cobalt Strike, a tool frequently employed by Crimeware and Advanced Persistent Threats (APTs), to generate diverse malicious payloads across various file types, including .exe, .pif, .xll, .mdb, .xlsm, .hta, .cpl, .scr, .node, and .dll.

The assessment revealed AZT PROTECT's comprehensive prevention capabilities across a wide spectrum of sophisticated threat vectors, demonstrating key strengths:

- Prevention of Unsigned Executable Filetype Execution: AZT PROTECT successfully blocked unsigned malicious executables, even those employing spoofed certificate signing and packed within common archive formats like .zip, .7z, and .ISO.
- Prevention of Office Macro Droppers: Malicious macro-enabled Office files designed to drop executables were effectively neutralized.
- Prevention of AppDomain Hijacking: This technique, which leverages the .NET framework to load malicious code within a trusted context—often bypassing EDRs and application whitelisting—was successfully blocked by AZT PROTECT.

- Prevention of DLL Loading and Node Sideloading: AZT PROTECT thwarted malicious DLL execution via rundll32.exe and prevented Node sideloading attacks that exploit applications built using the Electron framework.
- Prevention of Advanced Non-Paged Memory Pool Injection Techniques: AZT PROTECT detected and neutralized sophisticated memory-based threats, including the "PoolParty" injection technique, which targets non-paged memory pools in the Windows kernel.

Prevention of DLL Loading and Node Sideloading: AZT PROTECT thwarted malicious DLL execution via rundll32.exe and prevented Node sideloading attacks that exploit applications built using the Electron framework.

Prevention of Advanced Non-Paged Memory Pool Injection Techniques: AZT PROTECT detected and neutralized sophisticated memory-based threats, including the "PoolParty" injection technique, which targets non-paged memory pools in the Windows kernel.

OTIFYD Efficacy Testing: Blocking Every Attack

A subsequent evaluation by OTIFYD in November 2024 (with the report issued in June 2025) further validated AZT PROTECT's effectiveness. This test, conducted on ARIA Zero Trust Agent version 1.16.0.7 on Windows Server 2016, aimed to demonstrate its capability in preventing malware execution and mitigating advanced attacks through the use of live malware samples and proof-of-concept exploits.

OTIFYD's efficacy test comprised three stages: baseline environment analysis, simulated adversary execution, and evasion technique analysis.

The results were conclusive: AZT PROTECT exhibited strong defensive capabilities, successfully preventing every tested attack and malware execution.

- Live Malware Neutralization: In Test Case 1, live malware samples, including various WannaCry and WannaCrypt0r ransomware variants, as well as Ransomware RATs (like Jalapeno RAT) and Kryptik Ransomware, were successfully stopped at detonation by AZT PROTECT's "No Trust" countermeasure when configured in "Prevent" mode. These are types of malware known for their ability to encrypt entire systems.

- Blocking Proof-of-Concept Process Injection Attacks: Test Case 2 showcased AZT PROTECT's ability to block process injection attacks designed to exploit legitimate processes such as cmd.exe, wordpad.exe, and regedit.exe. These included advanced techniques like MSBuild iTask Shellcode Injection, PROPAgate Shellcode Injection, APC Process Injection, Listplanting Process Injection, and Oleum Process Injection. None of these sophisticated attacks succeeded.

These tests unequivocally underscore AZT PROTECT’s effectiveness in stopping both malicious software and exploit attempts, positioning it as a highly reliable tool for defending against a broad range of threats.

A New Standard in OT Cybersecurity

The findings from both the SNT and OTIFYD assessments emphatically demonstrate that ARIA AZT PROTECT represents a significant advancement in cybersecurity.

It offers breakthrough protection against unknown threats, including the most advanced zero-day attacks, and operates effectively "out of the box."

Its patented technology and unique capabilities enable it to halt attacks immediately upon attempted execution. Furthermore, AZT PROTECT is meticulously designed to meet the unique constraints of OT networks.
It supports modern Linux and Windows operating systems, while also providing backward compatibility with legacy Windows versions all the way back to Windows XP.

Crucially, it demands minimal computing power, consuming less than 2 percent of CPU even on decades-old legacy systems, ensuring no adverse impact on critical devices or applications.

Its ability to run fully air-gapped and enable each endpoint to be completely independent eliminates the need for constant patching updates or cloud connectivity.

By preventing even the most advanced TTPs that bypass leading EDRs and application whitelisting solutions, AZT PROTECT offers a robust, defence-in-depth architecture capable of addressing both conventional malware and highly evasive adversary tradecraft.

It truly delivers a "set and forget" approach to OT cybersecurity, ensuring seamless operations without disruption or downtime.

Contact: Peter Moore | Sales and Technical Director

Email: pmoore@logitech.com.au

Contact: Ben Kirk | Business Development Manager

Email: bkirk@logitech.com.au

Contact us today!

Since 1986

logitech.com.au
sales@logitech.com.au