aria CYBERSECURITY SOLUTIONS

Cybersecurity for Industrial and Utility Networks

PROBLEM: Industrial and utility networks incorporate many different forms of industrial internet of things (IIoT) that were not designed with security in mind. IIoT devices like industrial controls, sensors, automation, and HVAC, along with critical system control applications running on VMs, all need 100% uptime and protection from attacks.

SOLUTION: ARIA Cybersecurity Solutions' ARIA Software-Defined Security (SDS) helps find and eliminate threats at the network conversation level to stop attacks and leave critical Industrial Control System (ICS) devices online. Most of these devices are exposed because they don't generate the right type of information to feed threat detection tools in order to effectively do their job. Other approaches like EDRs and agents typically doesn't work on this type of equipment because of device constraints. We deploy the ARIA SDS solution within the network to provide the visibility to detect threats and attacks within the data conversations to and from IIoT devices as well as VMs and containers. ARIA finds threats you're missing today and automatically shuts them down.

PLATFORM: The ARIA SDS cybersecurity platform was purpose built to automate the capture, generation, recording, and blocking of network packet and flow information to your threat detection tools and processes. We've reduced the complexity and cost of doing this by combining the best elements of a packet broker and a packet recorder, and added them all to the industry's first intelligent automated threat containment system. All on a software-defined delivery platform with fully open APIs to work in any environment.

You can now:

- Provide enhanced security for IIoT, VM, and container environments without agents or EDRs
- Surgically contain threats without taking infected devices offline to remediate
- Provide missing threat detection coverage for IIoT by sending network data to your security tools
- Automatically stop data breaches and exfiltration utilizing recorded network data
- Easily add network-based microsegmentation to your IR process

"Utilities are expected to increase their security spend.

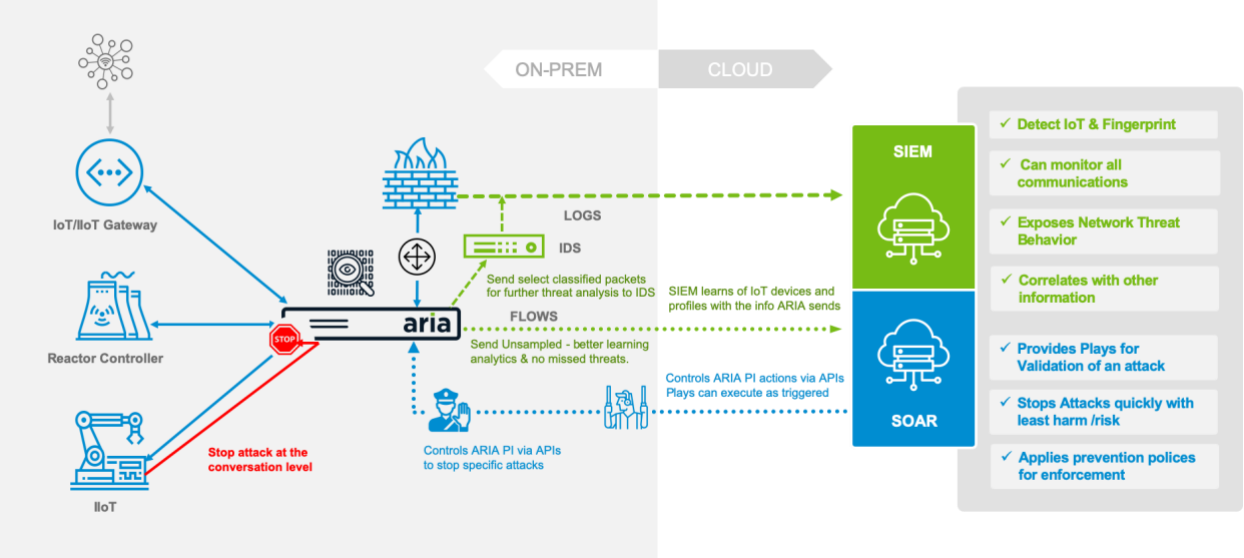
Unfortunately, only 55% of total spend in the next five years will be spent in smart infrastructure."

ABI RESEARCH

ARIA SDS makes it simple and extremely cost-effective to secure your smart IIoT infrastructure along with your enterprise network, without touching your devices.

ARIA SDS SOLUTION DEPLOYMENT

IIoT Threat detection/surgical containment and prevention



With ARIA SDS's Packet Intelligence (PI) application, we see and classify every packet, create NetFlow metadata to find threats in motion via modern SIEM integration, and allow action to be taken to interrogate certain packet data conversations to find and verify threats to avoid false positives. The actions are fully automated via open APIs that allow ARIA PI to be driven by your SOC's scripts or SOAR plays.

This is important as ARIA SDS can be controlled programmatically to surgically stop attacks at the conversation level, keeping critical devices and processes online even if compromised. ARIA SDS applications can be deployed in-line either on our secure, high performance probes (as pictured above), via smart NICs deployed in your critical application servers, or within the public cloud as a software instance.

The result: ARIA SDS provides complete network threat surface coverage and delivers a better approach to finding and stopping attacks. This helps fulfill the ultimate goal facing todays industrial networks – modernizing existing infrastructure while safeguarding critical processes, controls, and information in a much simpler and affordable way.

Learn more about our approach to Enhanced Network Security and Accelerating Incident Response.

Contact Us Today: sales@ariacybersecurity.com