aria CYBERSECURITY SOLUTIONS

INDUSTRY BRIEF

Better Cybersecurity for SD-WAN

PROBLEM: Software-defined wide area network (SD-WAN) services are strategically valuable to enterprises in their efforts to consolidate and upgrade WAN services. However, they require 100% uptime and protection from cyberattacks. Yet today's SD-WAN appliances and applications do not provide much more than simple distributed firewall services in the way of security. They do little to protect from threats like ransomware, malware, advanced persistent threats (APTs), or intrusions that could lead to data breaches. A better approach is needed to stop these types of malicious attacks.

A broad market is positioned to deploy SD-WAN. Healthcare, state and local government and education (SLED), and regional banks and credit unions are all ready to embrace SD-WAN to upgrade their WAN services. These organizations expect not only improved application performance in a secure environment, but also at a lower cost.

The service provider that inherits the challenge of deploying the new SD-WAN solution also assumes the responsibility of securing the new infrastructure.

Today's approach to SD-WAN security seems straightforward, but unfortunately it is flawed; because in most cases it only includes:

- Adding simple distributed firewalls to uCPE devices
- Centrally routing and monitoring all traffic to and from the internet through unified threat management (UTM) firewalls

At best, these methods only protect the high-speed internet underlay service from known attacks coming through the internet perimeter. They do nothing to stop attacks once they have broken through and are spreading through the environment.

Cybersecurity protection is required from the most harmful and prevalent threats such as:

- Ransomware
- Malware
- APTs
- Intrusions leading to data breaches and exfiltration

These threats may come from infected devices that connect to the customer's internal network, spearfishing, or vulnerable IIoT (Industrial Internet of Things) devices.

SOLUTION: ARIA Cybersecurity Solution's ARIA SDS Packet Intelligence (PI) application can be positioned within the SD-WAN. It may sit transparently and cost-effectively in the uCPE, on the backhaul, or within the core network of data centers. The application monitors and classifies every packet of information, as well as it ensures that the proper security policies and controls are enforced. It monitors traffic to detect threats and attacks. Actions can be taken by the application to stop attacks, at the threat conversation level, without disrupting business processes. It may also perform analytics on the customer's network traffic, delivering valuable information for a multitude of uses.

Why do we need something other than what exists now?

Most cyber-attacks today often get missed once they get inside an enterprise's internal network. Let's look at two attacks of high concern:

- Ransomware that spreads internally like an epidemic once it gets a foothold
- Data breaches resulting from intrusions into critical devices that can go undetected for long periods of time. Once they get past the perimeter, this can lead to exfiltrated data.

Both types of attacks are very different. Ransomware moves fast in order to do the most damage and maximize its impact. Many regional hospitals, municipal governments, and agencies have been completely paralyzed by ransomware in a matter of 48 hours.

Data breach attacks, on the other hand, tend to move slower as hackers look to find and access valuable information. According to Ponemon Research, the time span between when a data breach incident occurs to when it is finally contained is 279 days. Some of the worst breaches occurred at Target, Equifax, and Anthem. They were so effective because undetected lateral movement was able to occur until hackers discovered the right devices with valuable information.

However, what is common between both types of attacks is the lateral spread techniques used to access other network devices, VMs, and containers. What is also common is that traditional threat detection techniques don't have a network visibility component, and don't work to find these threats in time. This is why these types of cyberattacks are most harmful and costly.

How does the ARIA PI application find and stop attacks?

The ARIA PI application sits within the SD-WAN service and generates the type of information needed for threat detection tools to find attacks early in the kill chain – before harm is done. We deploy our solution within the SD-WAN network infrastructure to feed tools like security information and event management (SIEMs) with visibility into all SD-WAN traffic. This technique discovers threats that typically go unnoticed, especially malicious activity in east-west traffic. Examples of this traffic include intra-VLAN, between VMs or containers, and inside IoT environments.

This gives your SD-WAN service the unique ability to help find the critical attacks your customers may be missing today. It allows the SD-WAN provider to offer customers a simple reference design to detect and stop such threats using the intelligence provided by ARIA PI solution, which are fed into the customer's SIEMs and security operations center (SOC) processes. It makes these tools and processes much more efficient and effective at finding and stopping harmful attacks.

What's truly unique is that the ARIA SDS solution, when deployed within the SD-WAN, it can contain attacks at the network-conversation level while leaving business-critical applications online and unaffected. ARIA PI application is capable of automatically shutting down attacks when using automated workflow tools. Customers may manage these automated functions via APIs which enable integrations with third-party SOAR tools (such as Demisto, LogRhythm, and Splunk) and allows for a broad set of integrations that offer further process automations.

How does it work with existing SD-WAN applications and implementations?

All the leading SD-WAN providers allow for service chaining easily enabling ARIA PI to fit within. It effectively steers specific or all traffic to it for analytics generation and classification. This can be done locally at the uCPE or deeper within the provider's infrastructure.

The ARIA PI application generates metadata from the traffic, which is used to find threats and specific traffic. Once detected, this information is sent directly to a central location for further analysis. Any traffic conversations of interest, after the metadata threat detection occurs, can be delivered via the APIs for further analysis. Such traffic can be sent to tools within a central data center to verify a potential threat. These can be the provider's, or your customer's tools, depending on your business model. Once a threat is verified, it can be acted upon locally at the source of the traffic.

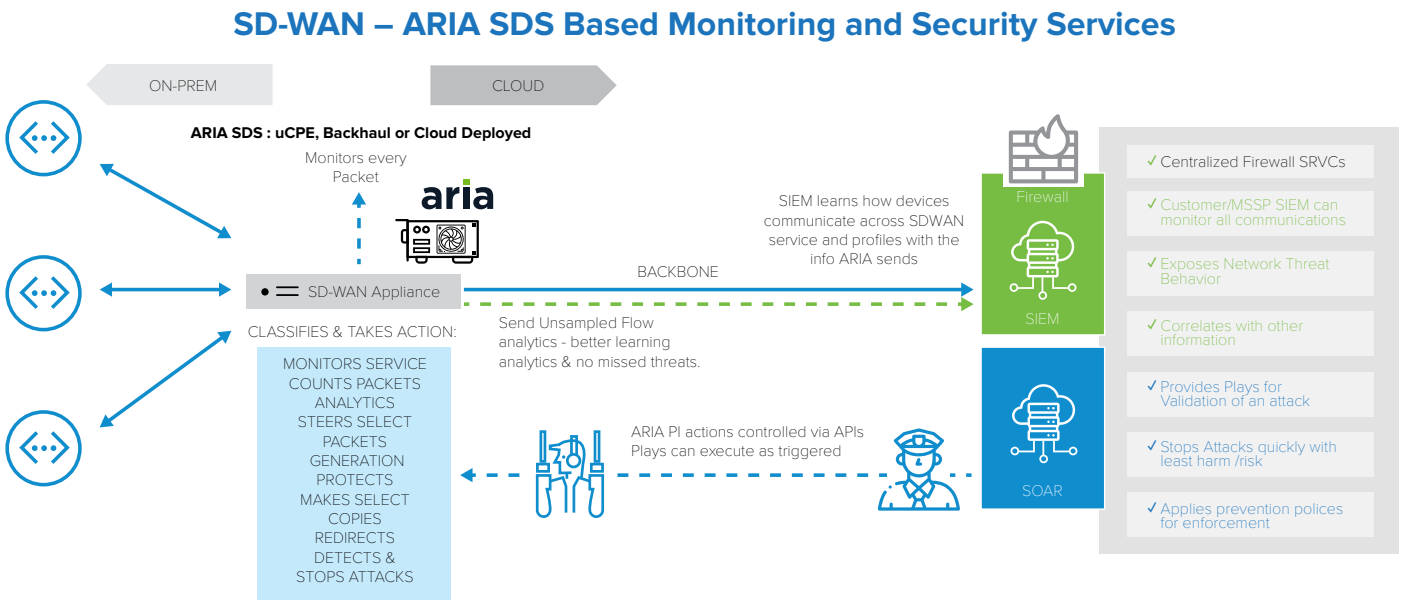
How is ARIA SDS unique?

CAPABILITY	ARIA	WITH TODAY'S SD-WAN
Intra-VLAN protection	Y	N
VM-to-VM protection	Y	N
Container protection	Y	N
IoT protection	Y	N
Monitors every packet	Y	N
Ransomware within the network	Y	N*
Malware within the network	Y	N*
Exfiltration resulting from lateral spread	Y	N
Enforces connection policy within network	Y	N

**Only if coming in from known bad internet sites and known signatures – not the case for a vast majority of infections*

How will it work within co-managed services models?

The open nature of the ARIA SDS platform makes it easy for any service provider to add security features. Its APIs can be accessed by the customer, as well as by the provider. The APIs can be used to obtain specific metadata and traffic packets. Based on this information, action may be taken on particular traffic conversations within each customer's individual service. The service provider controls the licensing set-up and SD-WAN security services.



The ARIA PI application:

- Monitors, classifies and counts every packet
- Counts packets
- Provides analytics
- Steers select packets
- Creates NetFlow metadata to find threats in motion via modern SIEM integration
- Discovers, verifies, and stops threats – while avoiding false positives

These actions are fully automated via open APIs that allow the application to be driven by SOC scripts or SOAR playbooks. 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.

All ARIA SDS applications can be deployed:

- With zero-touch provisioning
- In-line
- Co-residing with the SD-WAN application in the uCPE
- On ARIA's secure, high-performance probes (as pictured above)
- Within the provider's cloud as a software instance in their data center
- On Secure Intelligent Adapters deployed in critical data center application servers

RESULTS: 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 enterprise networks – modernizing wide area networking while safeguarding critical processes and information in a simple and affordable way. All on a software-defined delivery platform with fully open APIs and zero-touch provisioning to work within the customer's operational environment.

BENEFITS: With ARIA SDS organizations can now:

- Deliver missing high-value threat and attack detection coverage for SD-WAN services
- Provide enhanced security for IIoT, VM, and container environments
- Surgically contain threats without taking infected devices offline
- Automatically stop data breach and exfiltration utilizing recorded network data
- Easily add network-based policy enforcement to internal processes

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

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

ABOUT ARIA CYBERSECURITY SOLUTIONS

ARIA Cybersecurity Solutions recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor all internal network traffic, while capturing and feeding the right data to existing security tools to improve threat detection and surgically disrupt intrusions. Customers in a range of industries rely on our solutions each and every day to accelerate incident response, automate breach detection, and protect their most critical assets and applications. With a proven track record supporting the Department of Defense and many intelligence agencies in their war on terror, and an award-winning portfolio of security solutions, ARIA Cybersecurity Solutions is committed to leading the way in cybersecurity success.

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

aria CYBERSECURITY SOLUTIONS ariaSDS nVoy SECURITY APPLIANCES