ARIA SDS
Packet Intelligence
Application

CSPi's ARIA SDS Packet Intelligence (PI) application enhances an organization's existing network security capabilities by enabling the monitoring of all network communications, including east-west traffic, throughout an enterprise.

Using the ARIA PI application, flow-level metadata can be created for all packet traffic and directed to existing security tools like SIEMs or UEBA solutions. By feeding a steady stream of data to these devices, it is more likely that the algorithms will find network-born threats. Enabling the correlation of this data with other sources can improve threat detection effectiveness by 80% while also lowering the number of false positives. In addition, the ARIA PI application can be programmed to send certain packet-level traffic streams, such as "send all conversations to and from SQL databases in this subnet to this group of devices," to threat detection tools, including IDS or SIEMs.

If a threat is detected, and the detection tool has the appropriate built-in automation, it can tell the ARIA PI instances to send conversations, in their entirety, for further analysis. Security tools that support automated workflows can communicate via APIs to the ARIA PI application to take one, or multiple actions, against suspect traffic conversations. In real time, ARIA can generate as many copies of specific traffic streams as needed and enable multiple workflows to occur independently and in parallel. The result is enhanced speed and effectiveness of a broad array of tools, as well as the security team members' success detecting network-born attacks.

This can be thought of as a passive approach to threat detection. Passive in that the PI application will typically run out-of-band through the use of network taps or switch/v-switch span ports. In such an implementation, threats can be detected but not directly acted upon.

FEATURES

Benefits:

- Helps detect and automatically stops network-born threats.
- Runs wire rate at 10 or up to 25G without impact to network or application performance.
- Performs full network monitoring of all critical assets and application data, including lateral traffic flows.
- Gives many flexible deployment options: out-of-band for passive monitoring or inline (in-band) for automatic traffic filtering ranging from network policy enforcement, to dropping and/or redirecting threat traffic streams for further analysis.
- Leverages and improves effectiveness of existing security tools including SIEMs, UEBA, IDS/IPS, DLP, and forensic packet recorders.
- Delivers UI or APIdriven options for automatic disruption of network threats immediately upon detection. Works with SOAR tools. Ideal for MDR services deployment.
- Provides four deployment options optimized to meet variety of security requirements: threat analytics, passive protection, active protection or complete, out-of-the box turnkey protection.

However, the PI application can also take active measures to prevent and/or stop detected network-born threats. If deployed in-band, or "in-line", the PI application can classify traffic in real time while also applying a set of rules to that live traffic as it passes through network. This approach can stop threats in four ways:

1. Network Policy Enforcement – Create, apply, and enforce microsgementation rules to determine which set of devices, groups, or applications within these groups can talk to each other outside the group. All of this occurs inside the network, including between the on-premises networks and the public cloud, as well as microservices running within and between applications.
2. Pre-specified Investigation Analysis – Redirect traffic stream conversations as specified by policy or dynamically; such as directing certain file transfers and/or email traffic streams through a DLP system to identify and stop data leaks.
3. Dynamic Redirect – Leverage workflow automation tools to dynamically redirect particular traffic stream conversations for additional investigation; such as upon API instruction send all traffic from a potentially malware-infected device group through an extensive IPS rule set, while also sending a copy of the traffic to a packet recorder for forensic analysis and future audit.
4. Network Based Remediation – Through the ARIA UI, stop specified conversations as identified by the security team, or automatically through including scripts/API commands from third-party threat detection tools.

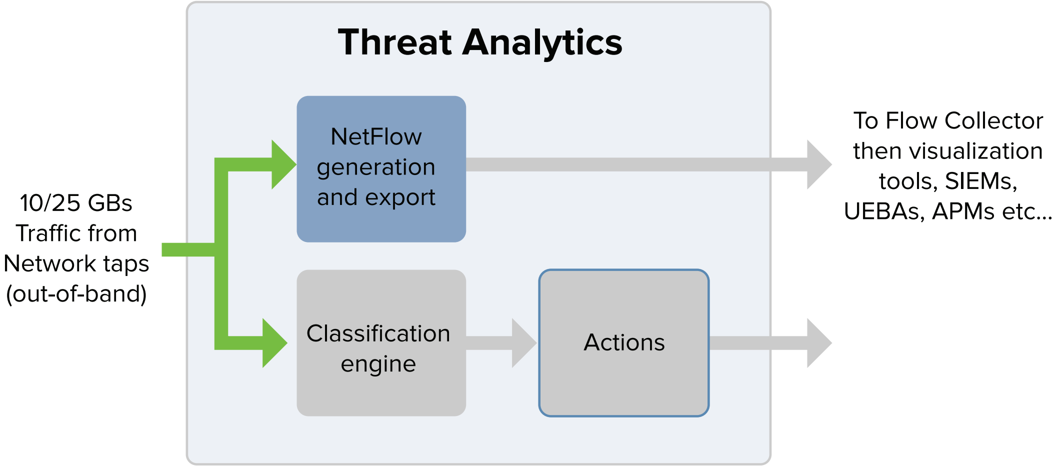
When used in any of these manners, the ARIA PI application enables the real-time automatic execution of preventative actions on specified traffic flows. Another benefit of the PI application is that it executes at full line-rate, up to 25G, without affecting application performance. For organizations that desire data protection capabilities, ARIA PI can direct traffic to additional ARIA applications to provide crypto services.

The ARIA SDS Platform solution simplifies and automates the deployment, and provisioning of the ARIA PI application. This make it as easy to deploy and run one or hundreds of instances across a wide-spread organization.

The ARIA PI solution is offered in four configurations, each designed to meet a variety of security needs:

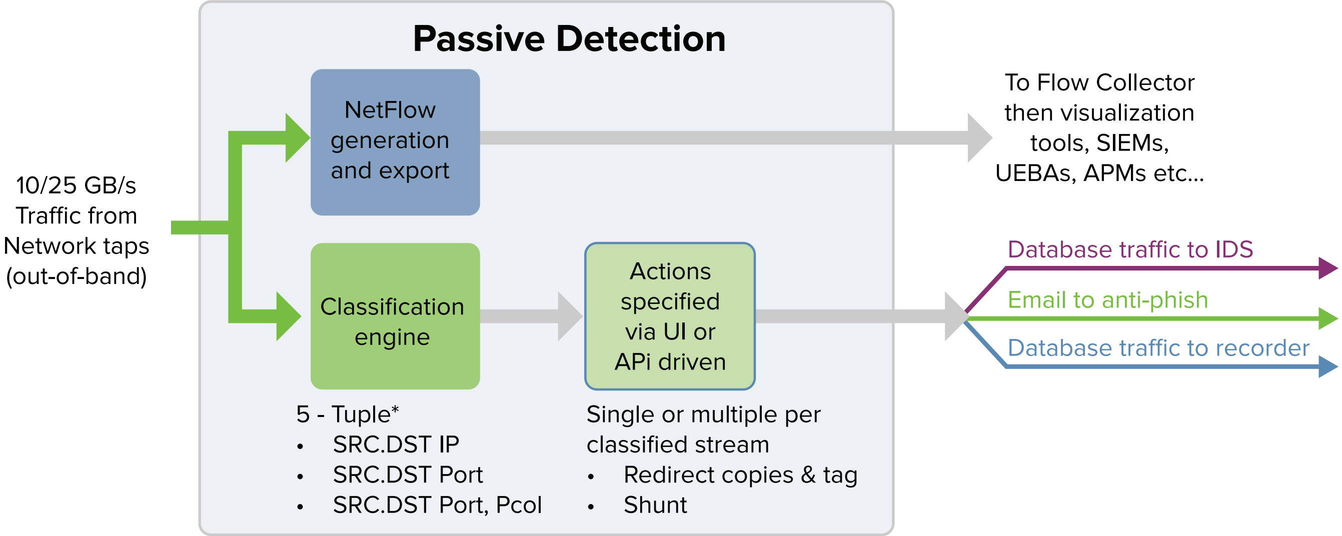
Threat Analytics:

Provides a simple, low-cost approach to improve the visibility and intelligence gathering of network communications. This fully automated solution identifies and classifies all network traffic at full line rates of 10G or 25G with no loss of application performance. The PI Threat Analytics configuration improves network visibility by providing Netflow metadata (v5, v9 or IPFIX format) and/or provides application identification information for each traffic stream. This "meta information", provided to new or existing tool sets, allows for quicker identification of threats.


Threat Analytics
10/25 GBs Traffic from Network taps (out-of-band)
NetFlow generation and export
Classification engine
Actions
To Flow Collector then visualization tools, SIEMs, UEBAs, APMs etc...

Passive Detection:

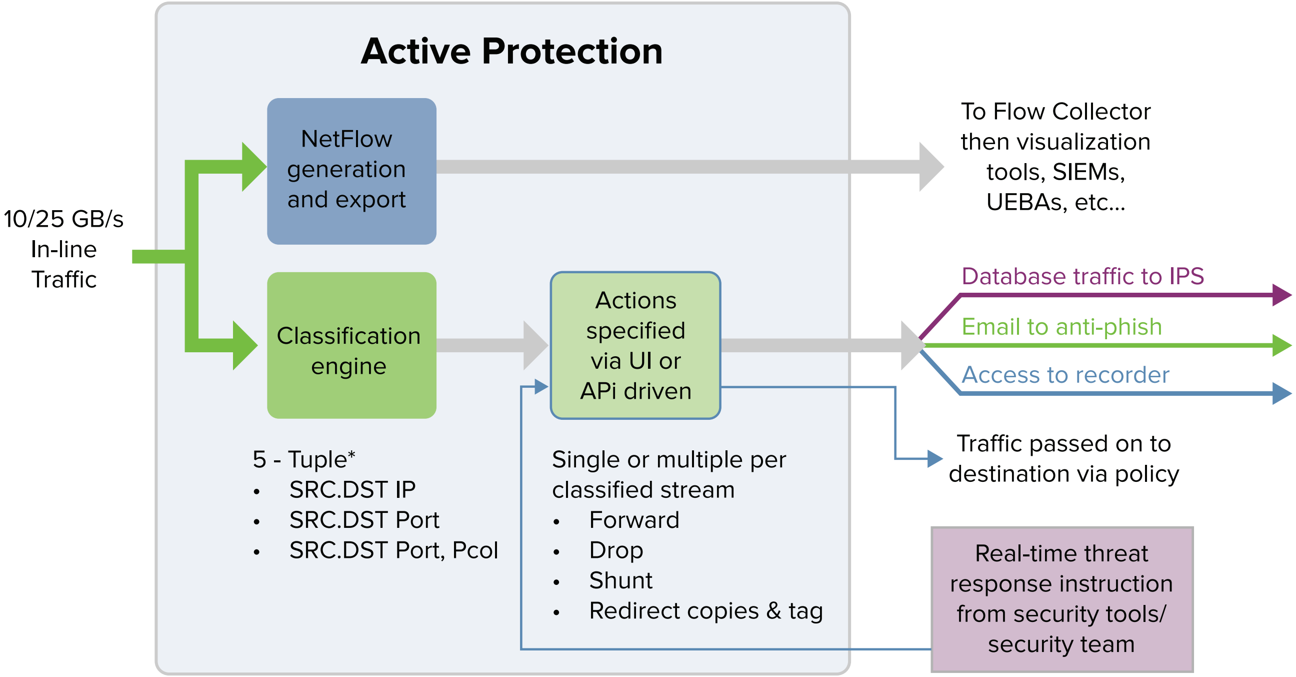
The passive network detection configuration deployed either through tap or switch span directs the appropriate classified traffic streams to security toolsets, including SIEMs, IDS, UEBA, and DLP for further analysis. This intelligent filter capability redirects specific flows to each tool as specified. It also can shunt certain flows, such as streaming video and audio-only, sending a specified number of bytes. Such adaptive filtering allows detection tools to operate more effectively by only analyzing the most relevant traffic. For SIEMs like Splunk and QRadar that charge by ingested bit, this translates into dramatic cost savings.


Passive Detection
10/25 GB/s Traffic from Network taps (out-of-band)
NetFlow generation and export
Classification engine
Actions specified via UI or APi driven
To Flow Collector then visualization tools, SIEMs, UEBAs, APMs etc...
Database traffic to IDS
Email to anti-phish
Database traffic to recorder
5 - Tuple*
• SRC.DST IP
• SRC.DST Port
• SRC.DST Port, Pcol
Single or multiple per classified stream
• Redirect copies & tag
• Shunt

Active Protection:

The in-band deployment of CSPi's packet intelligence active solution not only provides the same level of automated network monitoring capabilities as found in passive offerings (Threat Analytics and Passive Detection), but it also enables the real-time ability to stop network threats, as well as perform network policy enforcement. It works with third-party tools that support Security Orchestration, Automation, and Response (SOAR) solutions, and or automated scripts and workflows that allow such tools to communicate with ARIA to stop the threats as they are detected.

This greatly increases an organization's ability to take the appropriate actions against certain traffic streams, including forward, drop, replicate, redirect, shunt, and alert. Dynamic interaction directly or via automated workflow APIs gets the specified suspect traffic conversation streams to the right tool sets for proper analysis. Additionally, the active protection configuration is centrally managed, through a UI, and once set-up, eliminates the manual effort and potential errors when managing a complex environment. For organizations that have requirements around redundancy and resiliency, there are options for high availability.


Active Protection
10/25 GB/s
In-line
Traffic
NetFlow generation and export
Classification engine
Actions specified via UI or APi driven
To Flow Collector then visualization tools, SIEMs, UEBAs, etc...
Database traffic to IPS
Email to anti-phish
Access to recorder
Traffic passed on to destination via policy
5 - Tuple*
SRC.DST IP
SRC.DST Port
SRC.DST Port, Pcol
Single or multiple per classified stream
Forward
Drop
Shunt
Redirect copies & tag
Real-time threat response instruction from security tools/ security team

Turnkey Protection:

The last and most robust packet intelligence configuration is a complete turnkey approach to full network-based threat detection or protection. CSPi's Packet Intelligence solution integrates third-party security tools, such as IDS tools, to detect threats and, IPS to detect and to take automatic, actions to stop or disrupt threats once detected. This preconfigured solution gives organizations a centralized and orchestrated way to secure their environment, as well as the right data needed for security team resources to identify and stop potentially destructive network activity.

Feature	Threat Analytics	Passive Detection	Active Protection	Turnkey Protection
NetFlow analytics	✓	✓	✓	✓
App ID analytics	✓	✓	✓	✓
Creates analytics for every packet	✓	✓	✓	✓
Classifies traffic flows	✓	✓	✓	✓
Sends copies of flows to tools	✓	✓	✓	✓
Performs multiple operations/ traffic flow	✓	✓	✓	✓
Does not impact traffic performance	✓	✓	✓	✓
Deploys passively	✓	✓		
Passively detects threats		✓		
Dynamic Redirect		✓	✓	✓
Deploys actively			✓	✓
Redirects traffic flows to prevention tools			✓	✓
Enforces connectivity policy			✓	✓
Performs micro-segmentation			✓	✓
API Driven to stop threat traffic			✓	✓
Network based remediation			✓	✓
Automated deployment	✓	✓	✓	✓
Set and forget configuration	✓	✓	✓	✓
High Availability option		✓	✓	✓
Traffic decryption option		✓	✓	✓
IDS or IPS integrated option				✓
Email anti-phish option				✓

About CSPi

CSPi (NASDAQ: CSPi) is a global technology innovator driven by a long history of business ingenuity and technical expertise. A market leader since 1968, we are committed to helping our customers meet the demanding performance, availability, and security requirements of their complex network, applications and services that drive success.

CSPi Corporate Headquarters
175 Cabot Street - Suite 210
Lowell, MA 01854
800.325.3110 (US & Canada)

CSPi High Performance Products
800.325.3110 (US & Canada)
us-hpp-sales@cspi.com

CSPi Technology Solutions
800.940.1111
us-ts-sales@cspi.com

www.linkedin.com/company/csp-inc

@ThisIsCSPi

us-hpp-sales@cspi.com

www.cspi.com

All companies and logos mentioned herein may be trademarks and/or registered trademarks of their respective companies.

MYRICOM Network Products