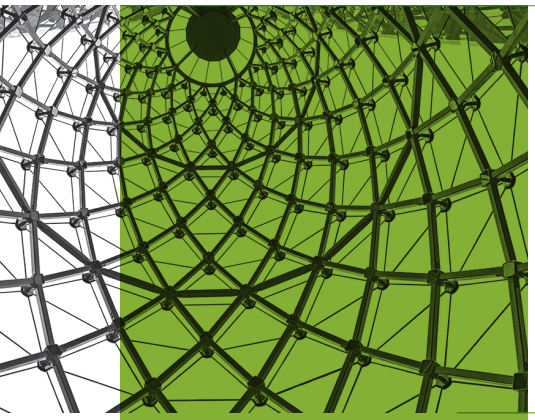

aria CYBERSECURITY SOLUTIONS

JUNIPER, ARIA JOINT SOLUTION PRIORITIZES EVENTS TO QUICKLY IDENTIFY ATTACKS

Challenges

Trying to collect the necessary logs and raw packet captures in large, complex networks, not to mention the challenge of reducing the signal-to-noise ratio, can be cumbersome for security operations center (SOC) teams.

Solution

Juniper Secure Analytics and ARIA Packet Intelligence allow SOC teams to focus on finding and stopping the spread of threats and the exfiltration of data within seconds of compromise.

Benefits

- *Reduces noise and potential false positives*
- *Provides quicker threat identification*
- *Detects network-borne threats and attacks that may have previously gone undetected*

Detecting and stopping cyberattacks as soon as possible is critical to minimizing damage. Network monitoring plays a critical role in the process, detecting compromise events before they have a chance to spread. With the joint Juniper Networks® Secure Analytics-ARIA Packet Intelligence solution, organizations can detect and mitigate threats faster than ever.

Successful threat detection requires the broadest possible network monitoring capabilities combined with advanced analytics. Just as important is the ability to work with existing infrastructures. Cybersecurity solutions that require rip-and-replace implementations fragment existing monitoring and event correlation capabilities, limiting their effectiveness. Juniper Secure Analytics and ARIA Packet Intelligence (PI) work together to help organizations rapidly detect threats by working with the infrastructure organizations already have in place.

The Challenge

Stopping attacks as soon as possible requires visibility not only into current compromise status, but an understanding of how these compromise events evolved. Log file analysis and packet capture give some visibility, but real-world deployments rarely cover enough of the network to provide the level of visibility required. Juniper Secure Analytics, working with ARIA Packet Intelligence (PI), gives organizations the tools they need to thwart modern threats.

Every device, application, operating system, agent, and security device produces logs that can be examined. Unfortunately, these raw logs include little data on threats, and on their own provide no context for tracking compromise events as they spread through the network. But adding this network data to the correlation of event sources allows organizations to detect threats at the earliest stages—potentially before any harm is done.

Giving SOCs the necessary visibility into the network requires more than simply sampling packets at the perimeter. Threats can and do emerge inside the corporate network. And unfortunately, today's networks are huge.

Collecting all necessary log files, along with the raw packet captures of all data flows, creates a substantial signal-to-noise ratio (SNR) problem. A lengthy list of data sources creates an ever-expanding haystack of information; keeping networks secure requires increasingly sophisticated techniques for finding the needles.

The SNR problem is exacerbated by the rise of lateral attacker movement, which requires examining all data flows within a data center. Far more traffic moves east-west in a data center than north-south, and this can dramatically increase the cost of network monitoring.

The logical approach to this problem—breaking up network monitoring to make it more manageable using traditional tools—isn't the answer. Without the ability to analyze all data, context is lost, preventing the full life cycle of a compromise event from ever being properly characterized.

Narrowly scoped network monitoring all too frequently results in gaps in coverage, or partial information that arrives well after the harm has already been done. This results in missed threats, or a lengthy resolution process that allows a minor compromise event to grow into something that threatens the entire company.

Data breaches are on the rise!

The lack of deep network visibility allows attackers to increase dwell time—that is, the time between initial compromise and threat isolation. According to the 2019 Ponemon Research Report:

- Breach life cycle grew noticeably between 2018 and 2019.
- Average time to identify a breach in 2019 was 206 days.
- Average time to contain a breach was 73 days.
- Average total dwell time was 279 days…a 4.9 percent increase over 2018!

Complicating matters are the twin problems of an ongoing shortage of qualified information security practitioners and the evolution of technology towards smaller, more numerous workloads that don't support traditional information security tools such as Endpoint Detection and Response (EDR). The proliferation of Internet of Things (IoT) devices, lightweight containerized workloads, and emerging technologies such as serverless have created new attack surfaces that traditional tools are ill-equipped to defend.

Defending the modern network requires the detection of—and action upon—threats as close to the point of compromise as possible. Achieving this requires deep network visibility and enforcement at every network connection point.

Juniper Secure Analytics and ARIA Packet Intelligence (PI) detect and verify threats as they transit the network, allowing organizations to identify threats early in the kill chain and giving SOCs a chance to deal with compromise events before any harm is done. Deep network visibility lets customers cost-effectively improve their cybersecurity preparedness while shrinking their attack surface. Additionally, the ARIA sensors used to monitor the network can also be used by the SOC to stop network-borne attacks as soon as they are detected.

Industry Best Practices

Network monitoring is part of virtually every cybersecurity standard. The importance of combating lateral movement has been highlighted in virtually all official government guidance around the world. In fact, east-west monitoring is now a standard part of today's most highly regarded cybersecurity frameworks.

These frameworks and governmental guidance documents are more than aspirational. They form the basis of numerous regulatory agencies and are used by the external security auditors that many of these agencies require.

While regulatory burdens vary greatly from vertical to vertical, industry best practices outlined in these documents impact both regulated and unregulated organizations. Official guidance documents—especially those published by the U.S. National Institute of Standards and Technology (NIST)—also inform how companies that offer cyber insurance assess risk and determine premiums.

Heavily regulated sectors—such as healthcare, defense, and government—are often legally required to follow industry best practices, including those that call for deep network visibility and multiple points of policy enforcement.

The importance of early detection

The NIST Framework for Improving Critical Infrastructure Cybersecurity consists of five concurrent and continuous functions: Identify, Protect, Detect, Respond, Recover. When taken together, these functions provide a strategic, high-level view of an organization's management of cybersecurity risk.

Detection is an important part of this framework. Organizations are encouraged to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. Examples of outcome categories within this detect function include Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

Implementing industry best practices for cybersecurity requires deep network visibility, specifically into east-west data flows in the data center. More than merely a compliance exercise, this type of monitoring represents a competitive advantage, as the consequences of neglecting it have proven disastrous for many well-known organizations.

The severity of 8 of the 10 worst data breaches in the past eight years was significantly exacerbated because attackers were able to spread laterally from the initial point of compromise, undetected and unchallenged. This led to massive amounts of compromised data from internal and external exfiltration, creating a perfect opportunity to spread malware and ransomware and establishing a foothold for future advanced persistent threats (APTs)[1].

The Juniper-ARIA Solution

Juniper Secure Analytics and ARIA PI let SOC teams focus on finding and stopping the spread of threats, as well as the exfiltration of data, within seconds of initial compromise. This solution allows SOC teams to prioritize events and quickly identify the critical attacks likely to do the most harm. Automation and orchestration integration also enable the immediate and automated quarantining of affected systems, speeding time to resolution.

To accomplish this, the ARIA PI application monitors all network traffic, efficiently feeding NetFlow metadata to the Juniper Secure Analytics solution to ensure complete network visibility.

ARIA PI generates a NetFlow record for every packet it sees. These records—approximately 1/1000th the size of the packets themselves—contain enough metadata to act upon. Integrated execution scripts provided by the ARIA PI application—combined with the metadata—allow Juniper Secure Analytics to efficiently detect threats.

Juniper Secure Analytics and ARIA PI also identify and classify threats such as ransomware, malware, botnets, data exfiltration, and even APTs as they traverse the internal network, letting IT teams act long before those threats have started sending data beyond the perimeter.

ARIA PI classifies all data flows so action can be taken to verify and stop attacks at a per-data traffic flow level. The ability to quarantine suspicious activity at a per-data flow level while allowing legitimate data flows to continue unimpeded allows organizations to maintain normal operations even when compromise events are underway.

The Juniper Secure Analytics and ARIA PI solution also allows organizations to record, store, and analyze network data via packet capture for specific network sessions, enabling the creation of a packet capture warehouse. Forensics teams can query and search captured network traffic when investigating a breach. The ability to sample both real-time and historic data is a critical advantage for forensics teams working to identify the nature, scope, and spread of compromise events.

Juniper Secure Analytics and ARIA PI solve the challenges of deep network visibility

ARIA PI provides NetFlow data on all network traffic, regardless of origin. Traffic can be collected from endpoints, servers, containers, VMs, IoT devices, or applications. This rich metadata provides Juniper Secure Analytics with more complete network visibility, lowering the number of false positives as well as allowing threats to be detected as close as possible to the initial point and time of compromise. This is accomplished by sending Juniper Secure Analytics metadata about data flows related to discovered threats, allowing the data to be correlated and verifying the threat.

ARIA PI allows Juniper Secure Analytics to operate with fewer log sources while improving its effectiveness by providing JSA with information about east-west data flows. This information can be correlated with other log sources, including applications, operating systems, and output from other security tools, allowing Juniper Secure Analytics to operate more efficiently and with increased performance. This means threats on large, high-traffic networks can be identified in seconds, rather than in minutes or hours.

ARIA PI uses open, RESTful APIs to integrate seamlessly with Juniper Secure Analytics and with other security orchestration, automation, and response (SOAR) security tools. This integration makes SOC teams more effective, giving them playbooks to follow and run in automated mode to find and stop the threats quickly.

Juniper Secure Analytics and ARIA PI give organizations a single management plane for monitoring the network and enforcing security policies.

For example, when Juniper Secure Analytics detects threats through ARIA-supplied metadata, further threat details—such as the type of ransomware, or what data is being impacted by a detected exfiltration—is desired. The SOC team can pivot, using the ARIA interface or its automated workflows to instruct ARIA PI instances to send copies of the complete matching packet streams to other devices, such as an intrusion detection system (IDS) and the ARIA Recorder.

[1]Source: ITRC Breach Reports, 2014 - 2019

Juniper Secure Analytics and ARIA Packet Intelligence Capabilities

The joint Juniper Secure Analytics-ARIA PI solution delivers the following capabilities for networks of all sizes.

1. Feed unsampled NetFlow data to Juniper Secure Analytics for better detection and rapid search functionality at lower ingestion costs:
   - Drastically reduce security information and event management (SIEM) indexer and search processing requirements compared to ingesting full packet capture, or additional device, application log output.
   - Detect network-borne threats and attacks that would previously be missed
   - Find threats faster, as they are happening
   - Reduce number of log sources requiring ingestion
   - Correlate with existing source log data and threat intelligence to enrich alerts and reduce false positives
   - Allow SIEM to see threats impacting IoT or critical production applications that cannot support an agent or full-blown EDR
   - Remove complexity around threat query string creation
2. Capture selective data conversations to provide "definitive" threat confirmation:
   - Eliminate the chance of false positives and provide more definitive proof
   - Improve the intermediate reach (IR) process by easily validating and identifying specific threat types
   - Minimize the ingestion of network data for detailed analysis
   - Eliminate the need and costs associated with other IR tools used to find this information
   - Assure compliance with increasingly stringent industry, federal (NIST, FISMA, HIPAA), and state regulations
   - Reduce the time and cost of audits and third-party investigative analysis
3. Automatically detect and stop threats immediately, without taking devices or applications offline:
   - Keep critical processes running while blocking the threat
   - Provide agentless threat containment for environments like IoT, VMs, and containers
   - Transparently detect IoT threats and block illegitimate conversations
   - Provide a surgical means for stopping threat conversations anywhere on network (north-south or east-west)
   - Stop threats upon detection
   - Provide a simple means to create and enforce network-based microsegmentation connectivity policies
4. Reduce data sets with filtering for improved results:
   - Reduce noise
   - Reduce false positives
   - Produce quicker search results
   - Implement more effective, lower cost IR processes
5. Verify and stop breaches when used in conjunction with the joint ARIA/SRX Series firewall solution:
   - Combines JSA, Juniper Networks SRX Series Services Gateways, ARIA Packet Intelligence, Automated Incident Response, Automated WorkFlow and Recorder applications
   - Detects, verifies, and stops data breaches while providing details on which files and records were exposed
   - Detects and stops critical data breaches in minutes rather than days or months, as is the norm today

Conclusion

Organizations of all sizes are struggling with detecting, quarantining, and resolving compromise events before they spread. With Juniper Secure Analytics and ARIA Packet Intelligence, it is now possible to identify and react to threats in seconds—a significant change from the minutes, days, or in some cases months that are the current industry norm.

This solution, unique to the market, combines Juniper Secure Analytics and ARIA Packet Intelligence capabilities to increase the detection of network-borne threats that are normally missed.

Juniper Secure Analytics and ARIA Packet Intelligence allows organizations to accomplish all this without requiring a rip-and-replace of existing cybersecurity capabilities. Building on the Juniper Connected Security strategy, this joint offering allows organizations to realize maximum value from their existing investments, improve their cybersecurity posture, and meet the most difficult regulatory requirements more cost-effectively than ever before.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

About ARIA Cybersecurity Solutions

ARIA Cybersecurity Solutions, a business of ARIof CSPi Inc.,recognizes that better, stronger, more effective cybersecurity starts with a smarter approach. Our solutions provide new ways to monitor internal traffic, while capturing and feeding the right mix of analytics to security tools like SIEMs or our ARIA ADR application to substantially improve threat detection and surgically disrupt cyberattacks and data exfiltrations. Customers in a range of industries rely on our solutions to improve their security posture—no matter their environment. ARIA Cybersecurity Solutions include ARIA Software-Defined Security (SDS), Myricom SmartNIC network adapters, and nVoy Security appliances. 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 to ensure cybersecurity success. Learn more at ARIACybersecurity.com

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

JUNIPER NETWORKS | Engineering Simplicity