APCON & RSA SECURITY ANALYTICS

Network Performance Monitoring and Analysis

APCON Product
IntellaFlex Series 3000 Monitoring Platform

RSA Product
RSA Security Analytics

PROBLEM OVERVIEW

With today's rapidly evolving threat environment, one of the keys to securing your organization is the ability to see and understand everything that is happening on your network. Real-time visibility and high-powered analytics along with long-term data retention are required to fulfill detection, investigation, analysis, forensic, and compliance needs. The RSA Security Analytics solution makes this a reality with two primary infrastructure elements: the capture infrastructure and the analysis and retention infrastructure.

The cornerstone of the RSA Security Analytics capture architecture is the decoder, a highly configurable appliance that enables the real-time collection, filtering, enrichment, and analysis of network packets as well as log data. For network packet analysis, it is essential for the decoder to have complete visibility throughout the network – typically by tapping crucial links and collecting mirrored data from SPAN ports. These datastreams may need to be aggregated together, de-duplicated, filtered, and load-balanced to maximize decoder efficiency.

The APCON IntellaFlex Series 3000 intelligent network monitoring switch is the solution to enterprise-grade requirements in the data center. With up to 288 non-blocking ports of fully aggregatable IntellaFlex 10G Ethernet in a single 8RU chassis, APCON provides both data throughput capacity and chassis port density.

By combining APCON's IntellaFlex Platform with RSA's Security Analytics, you empower network forensic and packet capture devices by providing customized data streams aggregated from multiple points on the production network. Advantages include preventing data loss, collecting more relevant data per packet capture, de-duplication for tool optimization and packet slicing to address compliance concerns.

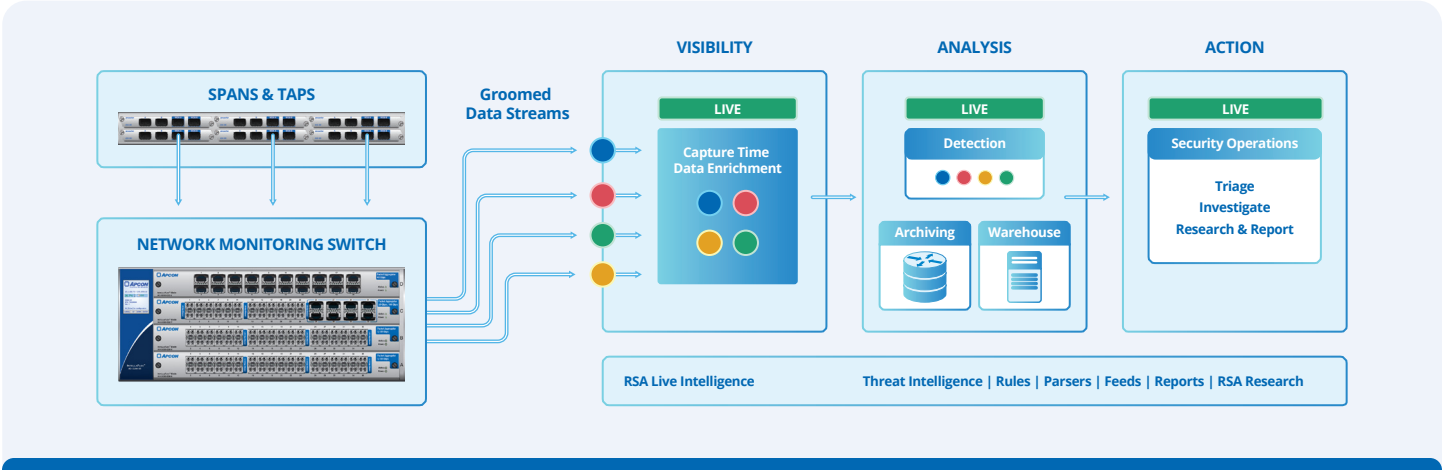

Figure 1 | APCON's network monitoring switch provides visibility and maximizes efficiency of the RSA Security Analytics infrastructure.

RSA SECURITY ANALYTICS

GAIN COMPLETE VISIBILITY – Eliminate blind spots with visibility across logs, networks, and endpoints. Inspect every network, packet session, and log event for threat indicators at the time of collection with Capture Time Data Enrichment.

DETECT AND ANALYZE – Discover attacks missed by traditional SIEM and signature-based tools by correlating network packets, endpoints, and logs. Identify high-risk indicators of compromise by harnessing the power of Big Data and data science techniques.

TAKE TARGETED ACTION – Prioritize investigations and streamline multiple analysis workflows in one tool. Instantly pivot from incidents into deep endpoint and network packet detail to understand the true nature and scope of the issue.

THE APCON SOLUTION

The APCON solution enables the aggregation of packets from multiple mission-critical monitoring points. Utilizing APCON's IntellaFlex solution, users can then manipulate, filter, and load balance this traffic to the appropriate monitoring tool.

Enterprise-grade data center monitoring switches must have the ability to bond several disparate data streams from external-facing, DMZ, and internal switches, and route all this data to the RSA Security Analytics decoders, as well as other network data monitoring tools. Key features provided by the APCON switch include:

- Packet Aggregation – merge many data input sources
- Multicast the merged stream to multiple output ports
- Apply egress filters to customize each data stream
- Reduce packet size with packet slicing
- Remove duplicate copies of packets

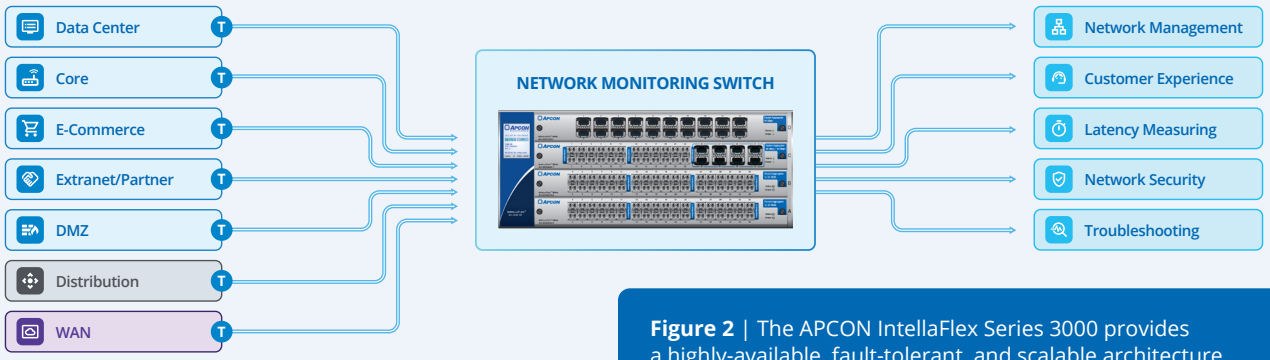

Figure 2 | The APCON IntellaFlex Series 3000 provides a highly-available, fault-tolerant, and scalable architecture suitable for use in a production data center employing the RSA Security Analytics infrastructure and other network data monitoring applications.

SOLUTION: APCON AND RSA SECURITY ANALYTICS

APCON's enterprise-grade intelligent network monitoring switch solution is certified for use with the RSA Security Analytics infrastructure, and provides the port density, overall port count and throughput capacity, and high availability to handle the volume of data generated in a modern data center.

APCON also provides the ability to eliminate duplicate packets, slice packets at the header, and filter packets on any criteria. This allows network engineers to bring together data inputs from any point on the network, aggregate and manipulate the data at the packet level, and then direct those data flows to the RSA Security Analytics decoders for analysis.

ABOUT APCON – APCON develops scalable network switching solutions for enterprise data centers worldwide. APCON intelligent network monitoring switches and TAPs provide complete network visibility, improve network security, and optimize monitoring tool efficiency. APCON's filtering and aggregation technology and multi-switch management software minimize network downtime and maximize monitoring tool investments.

ABOUT RSA – RSA is a global leader laser-focused on identity and access management, reflecting the company's belief that assuring digital identities throughout their lifecycle is of preeminent importance in cybersecurity. RSA focuses on serving the planet's most security-sensitive organizations, with specialties in federal government, financial services, healthcare, energy and technology services.

APCON Solutions for Networks

APCON, Inc. ▪ 9255 SW Pioneer Court, Wilsonville, Oregon 97070
+1–503–682–4050 ▪ 1–800–624–6808 ▪ **apcon.com**

14074-0822