SOLUTION BRIEF

APCON
Solutions for Networks

Eliminate Security Risks with Superior Cloud Network Visibility

Moving Workloads to the Cloud Introduces Visibility Gaps that can Seriously Jeopardize IT Security and Operations

Cloud Landscape

Gartner predicts spending in public cloud services will increase by 15.8% to $227.8 billion in 2019 and another 16.9% to $266.4 billion in 2020.[1]

As more organizations move workloads to the cloud they struggle to maintain the same level of visibility in the cloud that they have in their on-premises data centers.

This lack of visibility in the cloud is a risk companies can't afford. According to 2019 Cloud Security Report by Cybersecurity Insiders, 93% of organizations are moderately to extremely concerned about security in the public cloud.[2]

ENTERPRISES ARE RESPONSIBLE FOR PUBLIC CLOUD SECURITY,

public cloud providers are only responsible for the security of the cloud infrastructure. Security of the cloud data and applications along with organizational and regulatory compliance rest on the IT security operations of the organizations. The key challenge is that tradition security solutions that enterprises are familiar with have limited functionality or do not work at all in cloud environments.

Zero Visibility Zero Protection

In any IT environment there is an essential question: "which users, machines and applications are communicating with each other?" Companies need to see what is occurring across their infrastructure in order to quickly identify and prioritize issues and trace them back to their origin. This enhanced visibility can lower the mean time to fix problems for end users, as well as reduce detection times of security threats. Visibility is crucial for both security and operations teams. However, moving workloads to the cloud often significantly reduces the overall effectiveness of existing security and monitoring tools, hindering IT and security operations staff from addressing problems.

This is not a new issue. Even traditional data center environments struggle with blind spots. Tools historically used to monitor for issues and threats at network tap points cannot track all east-west traffic within the virtual data centers. In addition, these monitoring points certainly can't provide the data needed to link network issues back to specific devices, applications and processes. The **visibility these traditional monitoring points do provide is lost** especially when machines, applications and network elements are moved to cloud services such as AWS.

Cloud Visibility Drives Better Operations

The Improvement starts with your security operations team: comprehensive cloud monitoring accelerates security posture improvements, threat hunting, threat detection and threat elimination. You should be leveraging cloud-native tools available on AWS such as CloudTrail, CloudWatch, GuardDuty and VPC flow logs. These are great initial steps that give you some basic functionality however it is limited. A best-practices approach integrates a solution that provides **packet-level visibility within the cloud**, allowing security and operations teams to spend more time applying their expertise to mission critical activity.

The benefits carry over to adjacent areas such as IT operations, including hardware, applications and network teams as well as compliance and risk professional and DevOps teams. In many cases the person who initially finds a problem may not completely understand the issue or be the one to solve it.

The APCON Solution

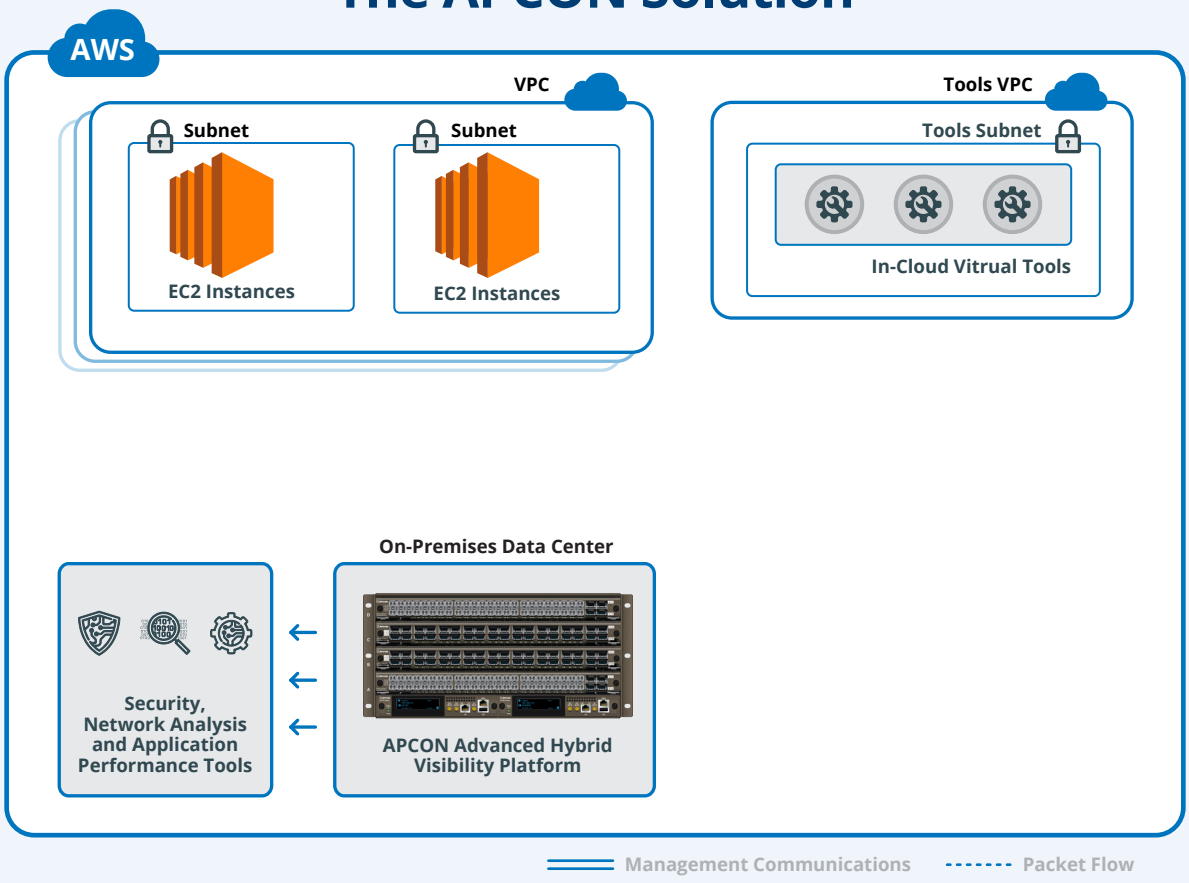
APCON's **IntellaCloud** feeds a common baseline of information into their existing security and system management tools, enabling better cooperation across teams. APCON helps you find threatening applications that attempt outbound connections to command-and-control networks by **monitoring network activity from cloud-based endpoints (VMs and containers)** and correlating all the network communications. APCON's solution creates a unique ability for IT and security administrators to see specific network threats.

REFERENCES

1 Gartner Forecast: Public Cloud Services, Worldwide, 2018-2022, November 2019

2 2019 Cloud Security Report: Cybersecurity Insiders

The APCON Solution



IntellaCloud Solution Capabilities

COLLECTION

Light Weight Agent

Deployed to each instance to be monitored. The agent can copy all traffic or just look for specific types of traffic, applying filters and performing packet slicing.

COMMUNICATION

Virtual Controller

The virtual controller initiates tunnels and delivers copied traffic to in-cloud or on-premise endpoints for further analysis.

VISUALIZATION

APCON Management Interface

From the user interface, maintain control over your visibility platform and enable dynamic monitoring by subnet or tags.

Top Features

- Scales with Your Elastic Cloud Environment
- Capture and Filter Cloud Network Traffic
- Cloud-Native Microservices Architecture
- Deliver Traffic to On-Premises or Cloud Endpoints
- Container Visibility and Multi-Region Support
- Dynamic Monitoring by Subnet or Tag
- Reduce Data-Transfer Fees with Packet Slicing

Benefits

Eliminate Cloud Blind Spots

Access, capture and monitor cloud network traffic

Deep Visibility that Scales

Elastic monitoring enables auto-scaling to maintain visibility

Connect Anywhere for Hybrid Security

Deliver optimized traffic to security tools on-premises or within cloud environments

Optimize Security & Performance

Easy-to-use UI, container and multi-region support for complete visibility and security

The APCON Difference

APCON leverages its proprietary IP and deep expertise to provide flexible, focused solutions across the

- **Government**
- **Healthcare**
- **Financial Services**
- **Manufacturing**
- **Telecommunications**
- **Higher Education**

APCON solutions provide the flexibility and means to gain visibility to their data more efficiently, resulting in savings across the board – including time, resources and maintenance.

Service and Support

APCON's professional services team of certified engineers have years of experience optimizing network visibility strategies for businesses across the globe. In addition to providing installation assistance of existing analysis tools, this team proudly provides around the clock troubleshooting services and support.

About APCON

A privately held corporation, APCON is headquartered near Portland, Oregon, where it has operated since 1993. APCON's in-house staff manages product design and development, manufacturing, quality assurance and final testing, customer training and long-term servicing of its solutions – whether for a system with a single switch or a global installation that spans across multiple geographical or cloud locations.

APCON
Solutions for Networks

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

19054-0120