SHIELDX

SOLUTION BRIEF

APEIRO™ + Amazon Web Services®

Comprehensive, uniform security policy with cloud scale and economics

RightScale 2017
State of the Cloud Report

Work with **Cloud** | Adoption of **Public Cloud** | Strategy for **Multi-Cloud**

powered by amazon web services

Compatible with
Amazon EC2

Uncompromised Security

- Secure in minutes at scale
- Unlock traffic visibility
- Inspect and protect in depth with DPI
- Detect earlier via analytics
- Protect more with uniform policy
- Align to risk and compliance

Unlimited Scale

- Scale-out and back-in elastically, up to multi-terabits of inspection
- Automate, insert and orchestrate
- Manage multi-cloud and multi-site
- Deploy over your infrastructure

Unparalleled Economics

- Save time with automation
- Empower DevOps with APIs
- Maintain SLAs with high availability
- Save costs with "lights off" removal
- Save your budget with cloud-friendly licensing at a fraction of the TCO and price

THE CALL TO NEW CLOUD SECURITY ECONOMICS

According to RightScale*, the past couple of years have seen enterprise progression along the Cloud Maturity Model. With public cloud adoption acting as a strong driver toward hybrid and multi-cloud strategies, 41% of respondents report workloads running within a public cloud. Of these deployments, the RightScale report depicts AWS as the top provider at 57%.

In the same report, RightScale also illustrates a transition in perceived cloud challenges. We now see a more balanced view with an "expertise, security and spend tie for #1." Essentially, IT organizations are concerned with optimizing the service and talent resources which they have invested in, while maintaining a robust security posture within a complex environment.

In this context, when evaluating both traditional and emerging cloud-based security solutions, IT teams are faced with critical questions such as:

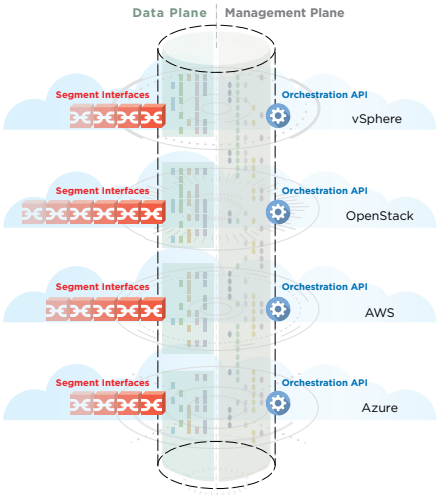
- Can this solution provide uniform, automated policy, protection and compliance across lateral attack surfaces and multiple environments?
- Do we have to disruptively touch every guest or hypervisor to deploy? Will an endpoint-based solution provide true isolation and network visibility?
- If we employ a network-based approach, can we practically operationalize a virtual network security appliance in our AWS instances?
- Does this solution allow us to optimize our security resources and investments in a public/hybrid/multi-cloud strategy?

*RightScale 2017 State of the Cloud Report

INTRODUCING APEIRO MULTI-CLOUD SECURITY

APEIRO is the first containerized, microservices platform for multi-cloud security.

Natively software-defined and enabled by its uniquely distributed and elastic architecture, APEIRO provides deep packet inspection (DPI) and network-based security automatically and on-demand, across multiple environments, at logically unlimited scale.



Security Controls —Network-based and Full-Flow

- Threat detection and prevention
- Malware detection
- TLS decryption and termination
- URL classification and filtering
- Real-time event correlation
- Threat intel feed import
- Data export
- App-aware microsegmentation*
- Data Loss Prevention (DLP)*

*Available in subsequent releases

Support

Our goal is to help enterprises maximize the value and benefits of their infrastructure automation, virtualization and security investments.

ShieldX Networks offers customers global, 7x24 technical support included with their subscription.

Contact Us
ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110

+1 408-758-9400
info@shieldx.com

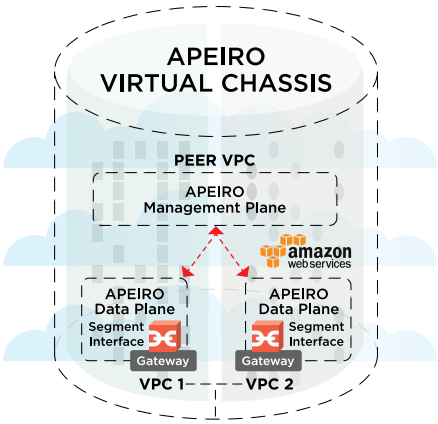
www.shieldx.com

USING APEIRO TO SECURE AWS ENVIRONMENTS

Advanced Security Orchestrated in Public Cloud in Minutes

Expand your existing APEIRO deployment, or start with AWS. Simply instantiate the APEIRO .ami file, login, configure with EC2 credentials, and start managing. APEIRO will automatically insert and dynamically scale out and in, according to your security, traffic and budget needs.

Each APEIRO Virtual Chassis has a single management plane, and one or more data planes. The management plane can manage across VPCs and non-AWS environments and can be located within a peer VPC, another connected environment, or across multiple environments.



Optimize Your Investments and Your Infrastructure

- Automate security insertion into the service chain “on-the-fly”
- Create intent-based security policy deployed within context and enforced uniformly across VPCs, AWS instances, or even many clouds
- Visualize traffic and understand attack behavior
- Meet compliance requirements and maintain business performance with scalable, enterprise-grade security
- Reduce operations costs through automation, self-orchestration and lower infrastructure resource requirements than comparable solutions

Requirements and Costs Over Your AWS Infrastructure

COMPATIBILITY

- Services: Amazon EC2

BASE CONFIGURATION (per license and traffic inspection rate)

MANAGEMENT PLANE (if AWS only)	SEGMENT INTERFACE, FLOW & INSPECTION	SSL/TLS DECRYPTION (Optional)
• 1 x m4.4xlarge per 40Gbps inspection	• 2 x m4.xlarge per 1Gbps inspected traffic	• 1 x m4.xlarge per 0.5Gbps encrypted inspection

LEARN MORE

Experience it now. Evaluate APEIRO with our proof-of-value program by contacting ShieldX or our authorized Partners through our website at www.shieldx.com.

Updated December 2017