SHIELDX

DATASHEET

# APEIRO™

The first containerized, microservices platform for agentless, multi-cloud security

## Automate orchestrated micro-segmentation with full-flow traffic inspection and policy enforcement while elastically scaling to multi-terabit speeds at a fraction of the cost.

Compatible with
**VMware vSphere® 5.5-6.x, OpenStack® Mitaka, AWS EC2® and Microsoft® Azure®**

**Uncompromised Security**

- Micro-segment and secure in minutes at scale
- Unlock lateral traffic visibility
- Inspect and protect in depth with DPI
- Detect earlier via analytics and Indicator of Pivot (IoP)
- 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
- Deploy over your infrastructure
- Manage multi-cloud and multi-site

**Unparalleled Economics**

- Save time with automation
- Empower DevOps with APIs
- Maintain SLAs with high availability
- Save costs at only 2-4 cores/microservice and public cloud "lights off" removal
- Save your budget with cloud-friendly licensing at a fraction of the TCO and price

## SECURE YOUR BUSINESS WITHIN THE MULTI-CLOUD

To contain risk and maintain compliance in today's complex, mixed legacy and multi-cloud environments, IT organizations like yours must collaborate across Infrastructure, Security and DevOps teams to ensure rapid and secure IT service turn-up.

You need a flexible solution that can effectively segment and secure, especially for new attack surfaces that have become targets for advanced attacks and APTs, propagated via lateral movement. This requires extending beyond basic role-based management, perimeter security and access control. It requires a solution that offers deep packet inspection and the visibility, policy management and enforcement you expect of an enterprise-class security system. And one that aligns with your infrastructure, working natively and uniformly at scale and across environments, without forcing you to compromise your business with unacceptable trade-offs between performance, cost and risk.

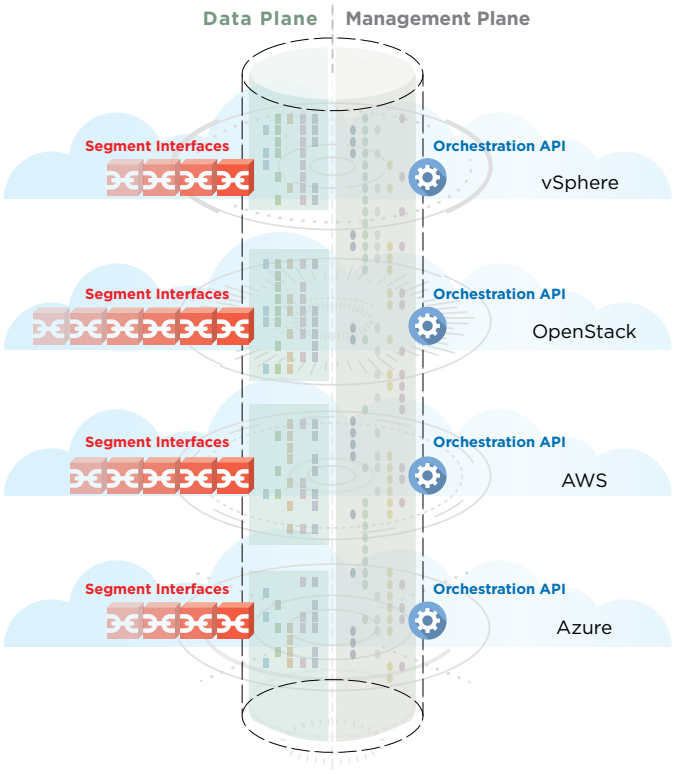
## INTRODUCING APEIRO

- Automate security insertion, orchestration and inspection elastically to multi-terabit scale across both physical and virtualized environments such as VMware vSphere®, OpenStack®, Amazon Web Services® and Microsoft® Azure®.

- Manage and implement uniform security policy on demand and at scale with enhanced micro-segmentation, TLS decryption, full-flow threat prevention, malware detection and data loss prevention*.

- Deploy over your existing, commodity infrastructure within 15 minutes and within your preferred OpEx or CapEx-based financial model. Improve operations with APEIRO automation, high availability, and API-first strategy that supports integration with DevOps-oriented processes.

*Available in subsequent releases




## NEW MODEL, UNCONVENTIONAL SOLUTION

APEIRO is a complete rebuild of traditional, network-based security.

APEIRO is true Software-Defined Security, built on a containerized, microservices-based architecture. We've deconstructed the monolithic, appliance-based solutions of yesteryear into their component microservices, or xServices, and packaged them natively within individual containers.

These containers auto-detect each environment to replicate, distribute and communicate between each other and form a single logical unit, or Virtual Chassis. The Virtual Chassis dynamically inserts, orchestrates and elastically scales out across and over your commodity infrastructure and public cloud services according to your security intent, the constraints you provide, and the policies you configure.

## FEATURES + SPECIFICATIONS

### Uncompromised Security

APEIRO allows you to create and implement uniform security policy, enforcement and micro-segmentation via security controls and functions that are application, user*, content* and traffic flow-aware. Its dynamic insertion combined with deep packet inspection and real-time analytics offers exceptional visibility and detection of Indicators of Pivot (IoP), helping analysts reduce false positives and identify attacks earlier in the kill chain.

TABLE 1: APEIRO Security Controls

| | |
|---|---|
| **MICRO-SEGMENTATION** | Access control policies that are application-aware for over 5000 applications |
| **THREAT DETECTION AND PREVENTION** | Employs behavioral, reputation, anomaly and signature-based techniques with over 10,000 threat definitions and intelligent correlation (IoP) |
| **MALWARE DETECTION** | Cloud-based sandboxing and advanced integration with FireEye™ AX-series appliances and Helix Cloud |
| **TLS DECRYPTION AND TERMINATION** | Full network-based decryption, re-encryption and termination where it's needed and at the scale and cost you determine |
| **URL CLASSIFICATION AND FILTERING** | Validates safety of external connections and locations and enhances granularity of security policy, detection, and enforcement |
| **NETWORK-BASED DLP*** | Provides inspection of data at rest and in-motion to identify locations and flows for policy and micro-segmentation that is risk-profile aware |

*Available in subsequent releases

## Unlimited Scale

While APEIRO uses containers to enable automatic insertion into multiple environments, its microservices-based architecture allows for dynamic, elastic and essentially unlimited scale of any component within its management and data planes in response to changes in your traffic flows, and according to the resources you allocate. APEIRO consumes only the resources it needs, when it needs them, removing security as your infrastructure and service performance bottleneck, and over-provisioned cost.

TABLE 2: APEIRO Supported Environments and Requirements

### VMware vSphere® 5.5-6.0, OpenStack® Mitaka and later

**HARDWARE COMPATIBILITY**

- Optimized for Intel® Xeon®, Sandy Bridge or later for on-premises, hosted or colocation environments

**BASE CONFIGURATION REQUIREMENTS (PER XSERVICE) PER SHIELDX VIRTUAL CHASSIS**

- Management plane: Total minimum xServices – 16 vCores, 32GB RAM, 500 GB storage per 40Gbps traffic inspection
- Segment interface: 2 vCores, 2GB RAM, 2GB storage per 10Gbps traffic inspection
- Flow and inspection: 4 vCores, 6GB RAM, 12 GB storage per 2Gbps traffic inspection
- SSL/TLS decryption: 2 vCores, 3 GB RAM, 6GB storage per 0.5Gbps encrypted traffic inspection

### Amazon EC2

**BASE CONFIGURATION XSERVICES REQUIREMENTS PER SHIELDX VIRTUAL CHASSIS**

- Management plane: 1 x m4.4xlarge per 40Gbps traffic inspection
- Segment interface flow and inspection: 2 x m4.xlarge per 1Gbps inspected traffic
- SSL/TLS decryption: 1 x m4.xlarge per 0.5Gbps encrypted traffic inspection

### Microsoft Azure

**BASE CONFIGURTION XSERVICES REQUIREMENTS PER SHIELDX VIRTUAL CHASSIS**

- Management plane: 1 x DS13_V2 Promo per 40Gbps traffic inspection
- Segment interface flow and inspection: 2 x F4S Standard per 1Gbps inspected traffic
- SSL/TLS decryption: 1 x F8S Standard per 0.5 Gbps encrypted traffic inspection

vmware READY APPLICATION SOFTWARE

openstack. COMPATIBLE

powered by amazon web services

Azure

TSANET
Your Technology is Connected. Are you?

**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, and is a member of the TSANet® alliance of computer manufacturers.

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

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

www.shieldx.com

## Unparalleled Economics

As 100% cloud-native software, APEIRO is based on cloud principles, technologies and economics. APEIRO can drive a revolution in the way infrastructure and security organizations purchase and operationalize security within their organizations, at up to 50% less than comparable solutions.

### CLOUD-PRINCIPLED

- Flexible, transparent purchase models for CapEx or OpEx budgets
- Easy, inspection-based, all-inclusive licensing
- Elastic, multi-tenant scale at 2-4 commodity cores per microservice

### OPS-ACCELERATING

- Segment and secure Terabits of traffic in less than 15 minutes
- Improve productivity with real-time analytics and automation
- Visualize, import/export, report, integrate or control with REST-APIs

### SLA-READY

- Maintain business performance, security, and compliance
- Highly available with non-disruptive install, upgrade and removal
- Role-based access separates duties with logging for audit trails

## 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.