SHIELDX

SOLUTION BRIEF

APEIRO™ Software-Defined Security

Segment and secure automatically and comprehensively with cloud scale and economics

Impacts of Breach

Had to Manage Public Scrutiny of a Security Breach

Experienced a Loss of Revenue

Experienced a Loss of Customers

Source: Cisco 2017 Security Capabilities Benchmark Study

Compatible with
VMware vSphere® 5.5-6.0, AWS EC2 and OpenStack® Mitaka

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

SOFTWARE-DEFINED SECURITY AT CLOUD SCALE

Security professionals have long known that a robust, multi-layered security posture is needed to effectively address the cyber kill chain, protect business-critical services, maintain compliance and avoid the wide-ranging impacts of a breach.

Their tools of choice typically span network, endpoint, and content security solutions, augmented by SIEMs, multiple threat feeds and security management applications to simplify operations across a myriad of products. Yet as reported by the Enterprise Strategy Group, as much as 74% of these same professionals abandon their traditional security controls because they are ineffective in the cloud environments* that most data centers and their services have migrated to. Most affected are monolithic, network security appliances that struggle to work efficiently across and within multi-cloud infrastructures.

Thus, practitioners are now investigating how to keep a multi-layered security approach, but as a part of an Adaptive Security Architecture that also supports:

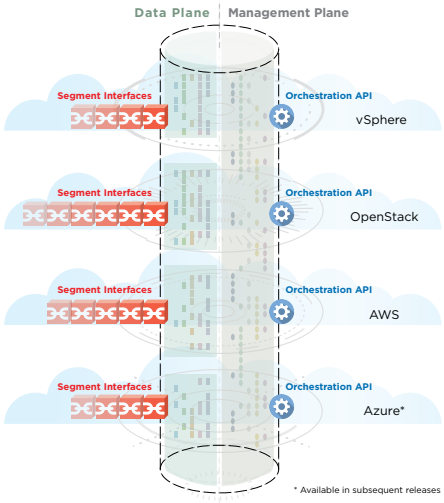
- **Advanced security** with in-depth, lateral visibility, continuous monitoring and advanced protection aligned to risk profiles, regardless of location
- **Cloud scale** that is elastic, ubiquitous, and automatically provisions, while sustaining performance across infrastructure and cloud-based workloads
- **Cloud economics** to empower operations staff to focus on threat research, policy creation, cost control, building with DevOps and maintaining SLAs

*Source: ESG Research Publication, ESG Infographic: *Cloud Security Requires New Processes and Controls*, November 2016

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.



ADVANCED SECURITY THAT'S UNCOMPROMISED

APEIRO is a network-based security platform and solution, offering the isolation, visibility and advanced security capabilities expected of a mature, network security product, but without the limitations or unacceptable compromises imposed by legacy architectures and technologies.

Deep Packet Inspection (DPI) and Visibility

- Full-flow inspection that is application, user*, content* and traffic-flow aware, including for highly secure, encrypted traffic
- Passive (tap) or active, inline modes
- Dynamic, ubiquitous deployment across clouds and along the highly-scaled, lateral ("East-West") axis of virtual infrastructure

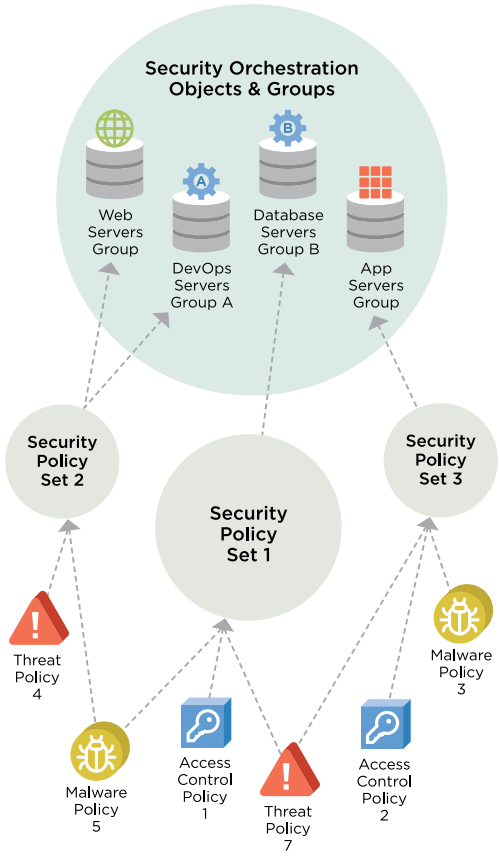


FIGURE 1: APEIRO SECURITY POLICY CONFIGURATION

Comprehensive 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

Intent-Based, Uniform Security Policy

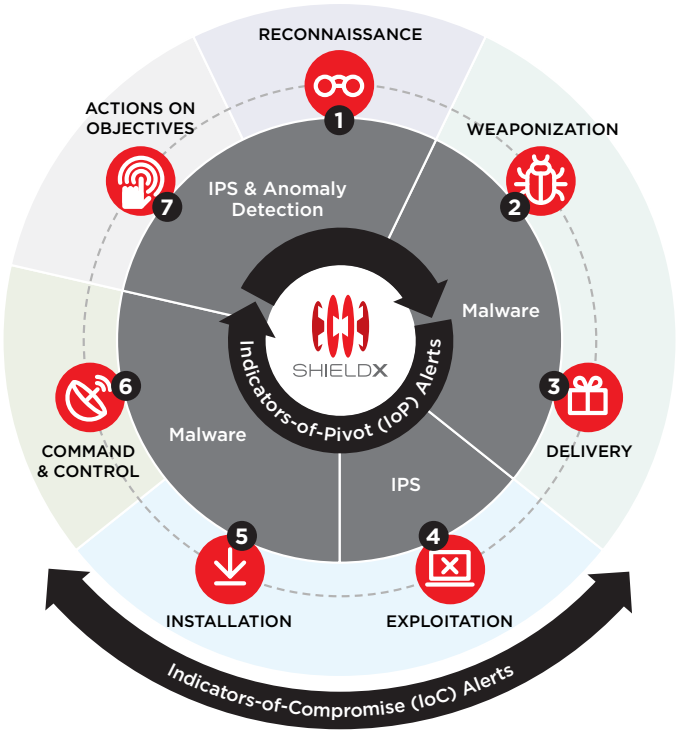
- Create security policies and sets for individual security controls, or collections of them according to security requirements
- Create security orchestration policies (SOPs) to identify objects to protect, then group them according to common security requirements
- Bind granular security policy sets to groups of objects to automatically express your security intent across the enterprise

Real-Time Analytics and APEIRO Indicators-of-Pivot (IoP)

To prevent, detect and remediate in real-time rather than after the fact, a solution needs to analyze large volumes of inline traffic with intelligent correlation. APEIRO analytics go beyond basic Indicators-of-Compromise (IoC) at the perimeter. It identifies individual stages of the kill chain, including the point where the attacker pivots and begins moving laterally within the data center, following an exposed path to critical assets to achieve service disruption or data exfiltration.

- Microservices-based, analytics engines deploy within the infrastructure for low latency and elastic, on-demand scale
- Multiple threat and reputation feeds continuously update and combine with APEIRO's intelligent, local profiling of traffic and anomalous activity
- Indicators-of-Pivot (IoP) alerts reduce false positives and help security analysts effectively identify and target threats much earlier in the kill chain

APEIRO in the Cyber Kill Chain



CLOUD SCALE THAT'S UNLIMITED

- Dynamically scales individual microservices, the components of the platform, according to security need and traffic volume
- Integrates with your infrastructure's orchestration platform for discovery and continuous monitoring, and self-orchestrates according to your deployment constraints
- Secures across multiple environments and virtual data centers up to multi-terabits of traffic, comprising a single, logical security system

CLOUD-PRINCIPLED

ECONOMICS THAT ARE UNPARALLELED

For IT teams looking to optimize their investments in the Cloud, APEIRO aligns with today's cloud principles by offering flexible licensing models* and significant reductions in infrastructure and operational costs.

For security teams, APEIRO also reduces TCO specific to security infrastructure management, with features such as:

- Security automation
- Centralized and role-based management
- Non-disruptive installation, upgrade, patch and removal
- API-first strategy for DevOps and integration
- Import of more intelligence feeds, or export of APEIRO data
- Rapid security time-to-service

OPS-ACCELERATING

SLA-READY

* Available in subsequent releases

Network-based Security

- App-aware micro-segmentation
- Threat detection and prevention
- Malware detection
- TLS decrypt/re-encrypt and termination
- URL classification and filtering
- Data Loss Prevention (DLP)*
- Real-time event correlation
- Threat intel feed import*
- Data export

*Available in subsequent releases

TSANET
Your Technology is Connected. Are you?

Support

ShieldX Networks is a member of the TSANet® alliance of computer manufacturers.

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

ShieldX Networks offers our customers annual subscriptions for global, 7x24 technical support.

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

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

www.shieldx.com

BETTER COMPLIANCE

With advanced micro-segmentation, organizations have the tools they need to provide separation within their highly-virtualized environments, while using policies powered by APEIRO DPI-based security controls to ensure that sensitive data is identified and protected against infiltration, exfiltration and improper access and use.

BETTER SECURITY OUTCOMES

ShieldX is committed to better security outcomes for our customers. Our goal is to offer a solution that provides the security that practitioners expect, while following the cloud principles they need.

In addition, ShieldX is committed to providing a security solution that is also secure:

- ShieldX follows SSDLC best practices, including for test and code analysis, and designs to the "defense-in-depth" concept
- APEIRO employs the "principle of least privilege", with each microservice given the lowest access level required to function
- Communication and storage of sensitive information by and between microservices employs authorization, authentication and multi-layer encryption techniques
- All virtual machine disk partitions are either read-only (e.g. for installation), or non-executable and encrypted for microservice data storage
- We maintain separation of management and data planes using a protocol barrier
- Our backup/restore process protects APEIRO configurations, but does not retain customer data, and all log file uploads are elective

BETTER BUSINESS OUTCOMES

With rapid security time-to-service at higher performance and lower cost, businesses and IT organizations are finally able to end unacceptable trade-offs, and move, securely, at the speed of digital and cloud-enabled business.

LEARN MORE

To learn more about APEIRO security features, please review our product documentation.

Or, experience it now. Evaluate APEIRO with our proof-of-value and beta programs by contacting ShieldX and our authorized Partners through our website at www.shieldx.com.

Updated August 2017