TECHNOLOGY PAPER

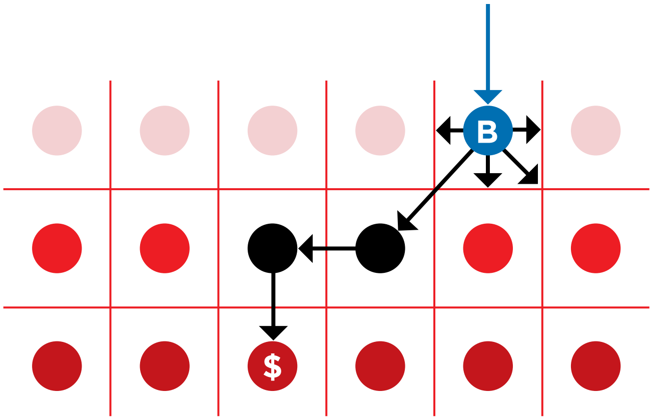
ShieldX APEIRO Technology Paper

EXECUTIVE SUMMARY

Technology infrastructure is evolving quickly and changing everything. DevOps and cloud architectures (Software as a Service (SaaS) and Infrastructure as a Service (IaaS)) have started to show the cracks in the existing security foundation. Historically security was done mostly by fortifying the perimeter of the network, assuming that the adversaries were largely external. That architecture is no longer effective, as there is an incongruity between the physical datacenter boundary and virtual perimeters. Those new perimeters can take up any size and shape and change at cloud speeds making it impossible for traditional security to keep pace. Additionally, the security controls offered by cloud vendors are less mature than traditional options and are often no match against advanced attacks hindering secure cloud adoption.

ShieldX's APEIRO platform addresses these issues by providing a scalable and flexible multi-cloud security platform for highly-virtualized data center and IaaS networks. Featuring an elastic micro-services-based technology that doesn't require agents, enterprises can automatically define and enforce a full-stack security strategy for multi-cloud or virtualized environments regardless of size.

ShieldX is the answer to network security both today and for the future.



THE CHALLENGE

The strategic technology initiatives of enterprises, including application modernization and adoption of cloud technologies, result in challenges to deliver agile IT without compromising on enterprise security risk. Between a multi-platform architecture and the dozens of solutions within data centers, this creates a complicated situation to manage as perimeter-centric security has proven insufficient to protect critical data. This creates a number of challenges:

- **Current security architecture assumes external adversaries.** Every time a new attack appears a new control emerges requiring implementation of another device on the perimeter. Over years of this approach, many organizations struggle with security appliance sprawl, each requiring management and subscriptions to keep the devices current—consuming significant time and money and adversely impacting the return on investment (ROI) of the solution.
- **Attack vectors continue to change due to consistent innovation by the adversaries, who now undertake sophisticated campaigns involving compromising many devices.** Typically, they initially gain presence by compromising a low-value device and then move laterally until they reach their goal. These well-funded and sophisticated attackers hide in plain sight by being patient and encrypting traffic to obfuscate malicious activity.

- **The imminent redefinition of the *data center* further complicates protecting networks.** Critical data increasingly resides within a combination of highly-virtualized data centers and Infrastructure as a Service (IaaS) providers, potentially in multiple cloud environments. This requires the ability to securely interconnect these various data centers, enforce security controls based upon the nature of the data, and substantiate security controls for compliance purposes.
- **The existing approach of routing all traffic through inspection points in the cloud isn't a viable approach moving forward.** It's inefficient and ineffective forcing enterprises to think differently to protect multi-cloud and highly virtualized networks. The next iteration of security will not just be cloud-friendly, but cloud-native, to leverage the unique capabilities of the cloud while recognizing the need to provide consistent controls across network interconnects and within virtualized data centers.

NEW NETWORK SECURITY REQUIREMENTS

Reflecting on the challenges facing security professionals, a set of clear requirements emerge regarding how to protect highly virtualized data centers and critical data residing on cloud platforms. To protect applications and ensure attackers cannot compromise an entire data center by compromising one device (control blast radius), tighter segmentation must be embraced by organizations wherever their data resides.

Commonly known as micro-segmentation, this involves defining a set of policies defining and enforcing access control for every resource on the network. As mentioned above, today's attacks involve significant lateral movement to move from the initial entry point to the sensitive data underscoring the mission. This "east-west" traffic requires a different set of controls and enforcement points than the traditional firewall used for "north-south" access control. Thus, a modern network security offering delivers flexible and policy-based micro-segmentation to limit the east-west traffic.

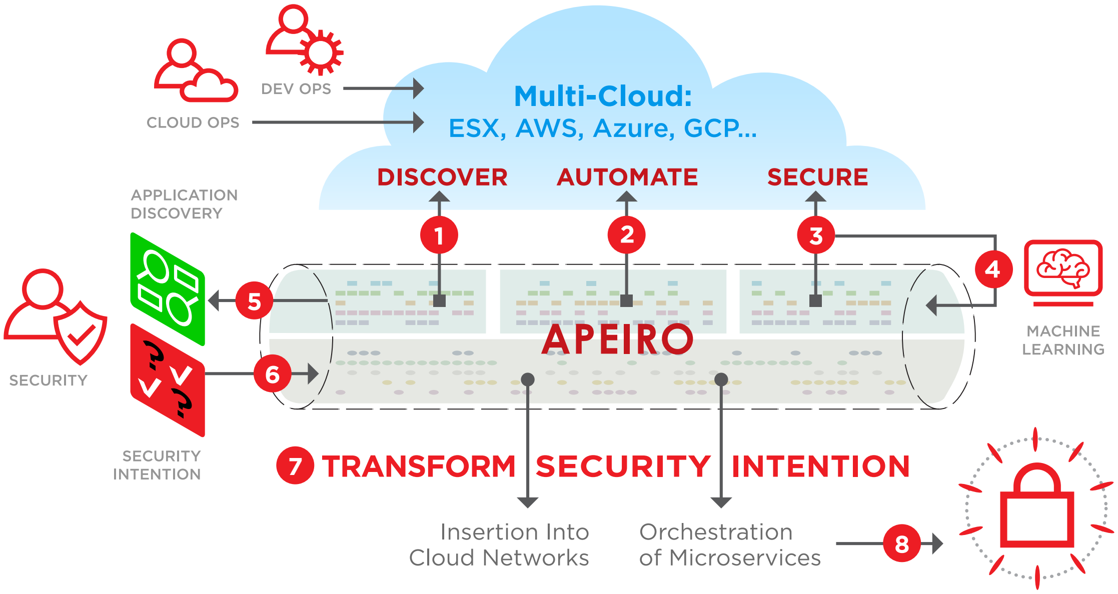
Next, a modern solution features a cloud-native architecture, which supports multi-cloud environments, including support for private cloud technologies (VMware ESX) and multiple public clouds since the goal remains to enforce a consistent security policy, regardless of where the data resides. Traditional security architectures involving firewalls (even of the next generation variety) require an inline deployment to provide visibility and enforcement. An inline deployment doesn't fit most cloud architectures requiring an agent on each cloud instance to implement the security policy. This approach creates friction with cloud operations teams that don't want to add more technologies and complexities to their technology stacks. Thus, a modern network security offering cannot require agents or inline virtual appliances to enforce security policies.

The next requirement addresses the need for policy-based, comprehensive security going beyond micro-segmentation, which is necessary, but not sufficient to deal with emerging attacks. Comprehensive security requires deep packet inspection at wire speed, which enables SSL decryption, firewall/access control, threat detection, intrusion prevention, URL filtering, and DLP at scale. Additionally, the use of security controls should be contextual and application-centric, allowing enforcement of different security policies for various applications, different cloud providers, and different geographies. An approach like this requires the flexibility to add and change security controls on the fly, without adding new appliances.

Finally, new network security offerings must provide sufficient scale to grow in step with the enterprise network. Organizations need to start small, given protecting the entire enterprise network in one fell swoop is unrealistic. As the technology stacks grow and potentially move to various cloud providers, network security needs to scale out without requiring forklift upgrades or appliance replacement.

INTRODUCING APEIRO

ShieldX's APEIRO allows enterprises to implement microsegmentation with DPI that configures automatically and provides full stack analysis to protect against lateral movement and data center threats. APEIRO applies comprehensive security, including firewall, threat detection, DLP, URL filtering and more, allowing organizations to consolidate their security infrastructure, reducing management complexity and cost.



ShieldX deploys quickly by analyzing multi-cloud environments to self-provision a comprehensive security stack that autonomously right-sizes and reacts at cloud-speed. Protecting against the new vector of cloud-based attacks such as crypto-jacking, cross workload, cross-cloud and other emerging tactics, APEIRO's visibility across the entire network reduces the effort required for compliance monitoring.

Discover

ShieldX continuously discovers and catalogs assets to provide visibility across cloud environments and within virtualized data centers. Then, using machine learning, ShieldX leverages internal and external intelligence to automatically define and implement security policies at the perimeter and within the data center. APEIRO provides situational awareness about applications running in the dark corners of your virtualized data centers that you didn't know about without introducing new load on existing security tools.

Modern networks are dynamic, which means you don't have time to discover everything in your environment and by the time you do, it has changed. APEIRO addresses this challenge by using its infrastructure connector to discover exiting infrastructure. The infrastructure connector leverages the APIs provided by the cloud providers (AWS, Azure, GCP, VMware) to normalize the activity accessible via these standard interfaces.

Intelligence is used to apply tags, grouping resources and other objects of interest based on servers terminating connections and clients initiating connections. Leveraging ShieldX's deep packet inspection capabilities, APEIRO also gains context about the application components in use. Once the data is captured and normalized, APEIRO maps the topology of the networks and identifies application dependencies across highly-virtualized data centers and public cloud providers, offering an end to end view of all of an organization's resources.

Machine learning is then used to quickly and effectively model relationships and entities to produce a visual application connectivity graph, allowing administrators to have a clear picture of their traffic dynamics over time to pinpoint potential issues. APEIRO then suggests a security policy based on the application connectivity model, which administrators can change and tune. The policy recommendation streamlines the time to value for APEIRO, allowing organizations to get value in hours, not weeks.

A strength of APEIRO, security policy definition and enforcement offers organizations the ability to granularly group workloads into resource groups (Web group, App group, DB group, etc.) while decoupling the policy layer from the enforcement layer. Separating policy from enforcement enables the policy to be defined based on intent and enforced based on available controls that can change dynamically based on the situation.

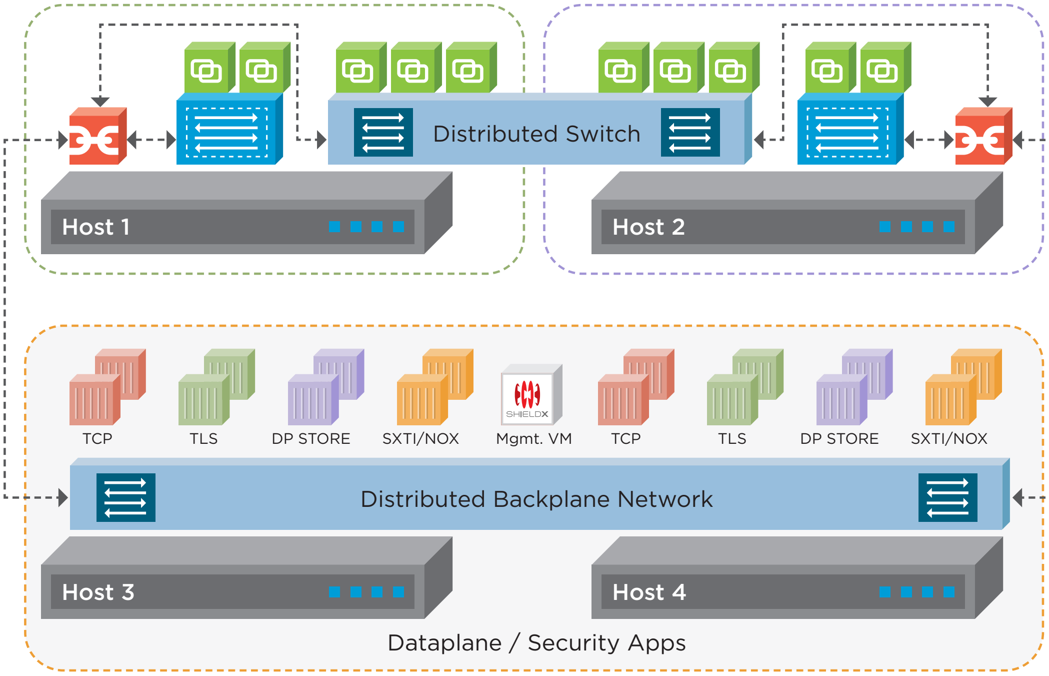
Understanding the dynamic nature of enterprise networks, APEIRO continuously monitors the multi-cloud for new workloads (VMs/Instances), networks/subnets, and load balancers via cloud APIs and recommends changes to the policy, ensuring security adapts as quickly as the environment changes.

Automate

The security policies enforced in the environment by APEIRO factor not only application connectivity models, but also the high-level intent of the connection based on business policies. Thus, policy definition includes both what is happening now (application connectivity maps) and what *should* be happening (business policies). Once the policy is defined, APEIRO inserts the security controls via each cloud provider's orchestration engines to realize security intent automatically, providing a consistent security model regardless of the location of the application and data.

APEIRO automatically inserts security services down to the subnet level via traffic steering or redirection leveraging the cloud provider's native capabilities:

- **VMware vSphere:** APEIRO can utilize a tap, tap trunk, inline or micro-segmentation to access the network traffic and implement/enforce policies.
- **Azure:** APEIRO integrates with Azure to redirect both north/south and east/west traffic to implement/enforce policies.
- **AWS:** APEIRO uses AWS APIs to insert security for north/south connections presently and will provide support for east/west policies by early 2019.



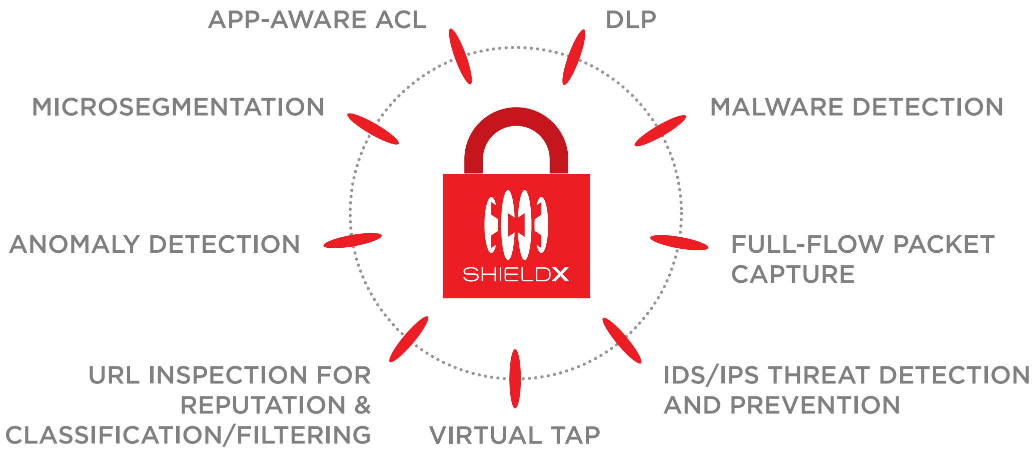
APEIRO's modern architecture adheres to the philosophy of "security as code," which means it integrates natively with infrastructure and security orchestration and automation tools. Featuring simple HTTP-based APIs, as well as a Software Developer's Kit (SDK) for integration, organizations can create sophisticated and reusable workflows representing playbooks, mocking services, etc.

For example, based on a policy trigger APEIRO can kick off an incident response process in a security orchestration and automation tool to accelerate the gathering of forensic information and based upon the workflow the response tool could send a request back to APEIRO to quarantine specific instances identified as part of the attack. This kind of bidirectional integration provides the ability to manage APEIRO in a repeatable and predictable manner.

Secure

To date, network security architected for the cloud consisted of implementing micro-segmentation. As the industry has learned over the past decade, segmentation is necessary, but not sufficient to provide comprehensive security. ShieldX's full flow Deep Packet Inspection (DPI) provides the ability to deliver the following security services at wire speed:

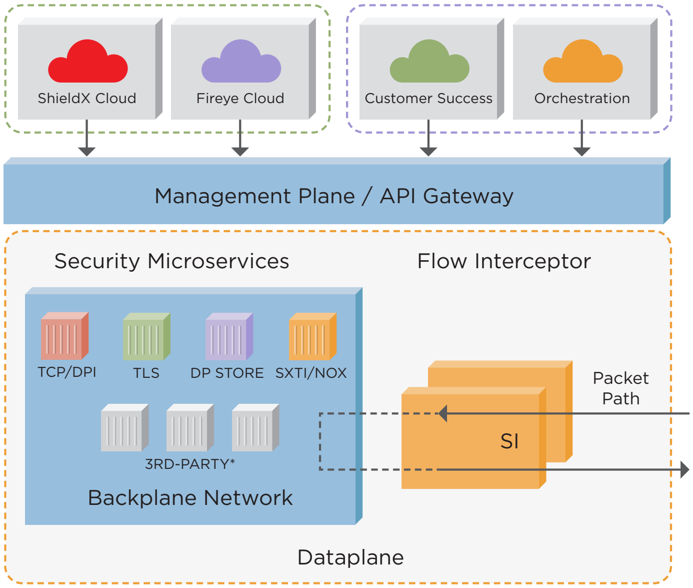
- TLS traffic decryption and termination
- IDS/IPS threat detection and prevention
- Integrated threat intelligence through partnerships with leading vendors including FireEye/Mandiant and Webroot
- Network-based malware detection and detonation via FireEye
- Full packet capture
- Web traffic protection via URL classification, filtering, and reputation
- Anomaly detection to pinpoint attacks in progress
- DLP monitoring and enforcement (at rest and in motion) [available late 2018]
- Application-aware microsegmentation
- Data In Motion Detection for detecting exfiltration of sensitive data



Besides implementing comprehensive security on the network, APEIRO also provides significant value when trying to detect an attack. Visualizing attacker behavior on a threat/malware execution map across multi-cloud networks allows organizations to watch for indicators of pivot to detect lateral movement during an attack campaign. To leverage this unique security data, APEIRO integrates with monitoring technologies including SIEM and security analytics. By aggregating logs, forwarding raw or filtered events, and enriching data and events with observed behavior (exported as JSON/XML), organizations can improve their security monitoring, advanced threat detection, and forensics/incident response.

Infinite Scalability and Flexibility

ShieldX's most significant innovation is its elastic, micro-services based architecture, allowing APEIRO to deploy security services at wire speed, expand and contract as needed, and deploy in any cloud or virtualized environment. In analyzing the architecture at a deeper level, it consists of the following:



- **Management plane:** The management plane can be used either on-prem or within a Public Cloud, orchestrating security across the virtualized data center and multi-cloud.
- **Segment Interface:** The Segment Interface processes network traffic at either ingress/egress or at a defined flow entry point (tap or inline micro-segmentation) and sends to the data plane.
- **Distributed Multi-cloud Dataplane:** The data plane implements security services per environment and security policy. Decoupled from both the management plane, inspection and policy enforcement happens within each non-routable and isolated data plane.
- **Virtual chassis:** A single scalable management plane and multiple distributed data planes together form a virtual chassis.

Each security service can expand and contract as needed due to the implementation as an independent, elastic micro-service on the data plane. For example, if a hundred large files containing potentially sensitive information hit the network destined for different destinations, this would overwhelm traditional security gateways that would need to serially inspect the content in each file, check the destination IP address (to ensure it's not a blacklisted network), and then decide whether to block the connection. APEIRO's full flow DPI engine inspects the traffic and determines each file that needs more in-depth inspection, then initiates a separate content inspection micro-service instantly for each file, while simultaneously checking the destination IP against a variety of threat intel databases, enabling parallel processing and decision making on whether to block the file.

APEIRO's micro-services-based architecture can provide a level of scale and flexibility matched only by the cloud itself.

APEIRO IS THE PLATFORM MULTI-CLOUD SECURITY NEEDS

Microsegmentation with APEIRO

When an adversary surpasses perimeter security controls (and they will), they gain free run of the environment, including access to high-value assets and the ability to exfiltrate sensitive data. Microsegmentation provides a necessary complement to the protection in place at the perimeter by detecting and preventing lateral movement by the attacker. Thus, microsegmentation provides detailed visibility of activities on the East/West axis of the data center or cloud and acts as an early warning system as well as the last line of defense.

APEIRO inserts into the network fabric of the multi-cloud and virtualized data center, first discovering all of the applications running in the datacenter and mapping those connections into a visual map. Using machine learning to determine application connectivity and dependencies provide the basis for a dynamic policy recommendation. Thus, organizations don't need to manually inventory and determine access control policies—APEIRO does that automatically.

APEIRO enforces the segmentation strategy which controls the blast radius of any compromised device. Thus, APEIRO prevents any attempts by the attacker to jump between networks and move laterally towards its target. Additionally, as the networks change, APEIRO connects to the cloud provider's API to determine the changes and adapt the policy.

Interconnect data centers securely and consistently with APEIRO

As enterprises have embraced cloud services, they now have to support both their existing data centers and the new cloud environments. Supporting both requires secure, and cost-effective interconnections, which rely on advanced network security controls not natively available in these cloud environments. Traditional network security vendors have adapted their products for the cloud, yet they are not cost-effective due to historical pricing models and complexity in deployment. More cloud-friendly emerging security products help to solve this problem but typically require a complete rewrite of the policies, procedures, and workflows.

APEIRO provides unmatched flexibility in deploying common, consistent security policies across the virtualized data center and the multi-cloud. Starting by mapping the connectivity required by applications across the entire network, automatically generating and inserting the security policies into the fabric of the network, and then enforcing the security policies at scale provides organizations with the ability to securely and cost-effectively interconnect their networks.

Secure applications deployed in the cloud with APEIRO

Due to the flexibility, agility, and cost inherent to the cloud, migrating critical applications to the cloud (IaaS specifically) has become an IT imperative. These high-profile applications tend to handle sensitive corporate data, requiring a focus on both data security and compliance. This "north/south" security requirement protects Internet-facing applications which connect to data either within the cloud or virtualized data center.

APEIRO provides the ability to clearly define access control policies for a high-profile Internet-facing application and ensure users of the application only connect to authorized data sources via microsegmentation. Additionally, APEIRO inserts security services including SSL decryption, IDS/IPS, and network-based malware detection and detonation to the inbound connections at wire speed via its micro-services-based architecture. Thus, an organization can deploy comprehensive security to Internet-facing applications without having to roll out an entirely different solution for the cloud.

The common thread between these three disparate solutions is the ability to deploy uniform and consistent security policies across the multi-cloud and virtualized datacenter. ShieldX analyzes network activity in all of the environments, determines the appropriate security policy for each situation, and inserts the security services and controls at scale, as needed. No other solution provides the scale and flexibility of ShieldX APEIRO.

SUMMARY

Enterprise security teams struggle in balancing their traditional security controls and providing a scalable and agile platform for the cloud while facing an accelerating migration to the public cloud and a need to continue supporting highly virtualized data centers. ShieldX's APEIRO ends that struggle by providing a scalable and flexible multi-cloud security platform for highly-virtualized data center and IaaS networks. Featuring an elastic micro-services-based technology that doesn't require agents, enterprises can automatically define and enforce a full-stack security strategy and insert those controls into networks of any size.

Key benefits include:

- **Simplification:** APEIRO implements a consolidated set of controls without requiring agents to reduces the operational cost of cloud security and also enforce consistent security policies across multi-cloud and highly virtualized environments.
- **Resilience:** APEIRO future proofs the enterprise ahead of shifting threats through its innovative micro-services-based architecture that flexibly inserts security controls at the necessary scale.
- **Automation:** APEIRO minimizes risk to the organization by using a self-orchestrating system that autonomously provisions at the speed of cloud and DevOps. Because it adapts to the current state of the applications, administrators can focus on troubleshooting issues, not modifying policies based on application changes.
- **Contextual security:** APEIRO identifies suspicious activity by profiling the environment and recommending policies to protect the applications deployed across the environment. APEIRO continuously monitors activity within multi-cloud and virtualized data centers to ensure changes to the applications don't result in security exposures.
- **Expense reduction/TCO:** APEIRO's micro-services-based architecture can expand and contract security as needed to reduce complexity and cost. APEIRO'S comprehensive security platform allows organizations to consolidate tools and reduce FTE's.

Finally, a security platform built for the cloud that provides the agility and flexibility needed by organizations migrating their critical data to the cloud.

SHIELDX

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

+1 408.758.9400
info@shieldx.com
www.shieldx.com

August 2018