ESG Lab Review

ShieldX APEIRO: Agentless Multi-cloud Security

Date: May 2017 **Author:** Kerry Dolan and Tony Palmer, Senior Lab Analysts

Abstract

The report documents hands-on testing of APEIRO, a microservices-based platform designed for agentless, multi-cloud security. Testing focused on ease of use, terabit-scale threat inspection, and centralized management across multi-cloud environments.

The Challenges

Many organizations leverage cloud infrastructures—private and public—for the agility, flexibility, and cost savings they provide. But while the technologies required to build elastic cloud infrastructures have advanced quickly, cloud security technologies have lagged. Among the toughest cloud security challenges organizations face are provisioning security controls for cloud workloads, monitoring cloud security status, and tracking network patterns for suspicious behaviors, all areas that security solutions designed for physical infrastructures are not suited to. In addition, organizations often use different cloud infrastructures for different workloads, complicating the ability to streamline management, minimize risk, and keep costs down. It is no surprise, then, that when asked about specific spending plans for cybersecurity, 41% of ESG research respondents cited an aspect of cloud security, making it the number one selection[1].

Figure 1. Cloud Security Top Cybersecurity Investment in 2017

Source: Enterprise Strategy Group, 2017

Organizations are wary of the potentially greater attack surface areas of the cloud, and of the ability of third-party providers to protect their data. Network perimeter security, role-based management, and access control are no longer sufficient, and

[1] Source: ESG Research Report, *2017 Cybersecurity Spending Trends*, March 2017.

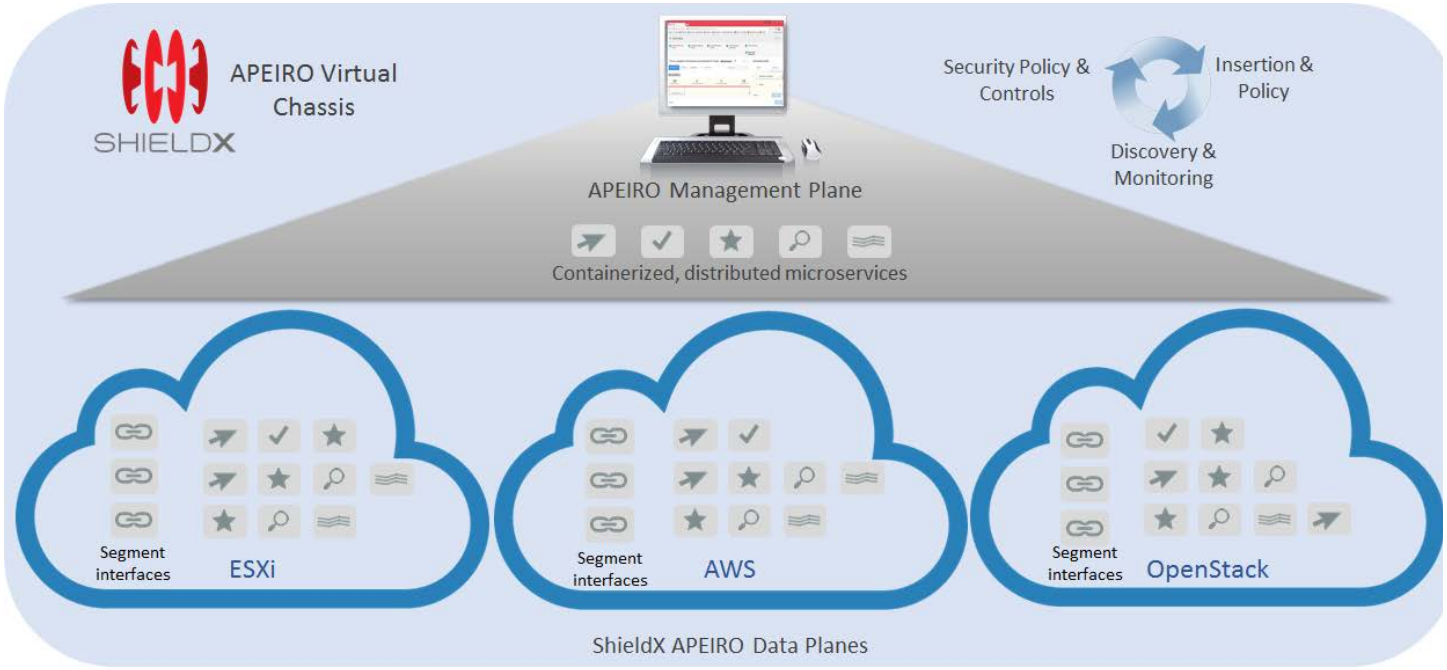
This ESG Lab Review was commissioned by ShieldX and is distributed under license from ESG.
© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

solutions that just offer segmentation get the job only half done—they neglect core security controls such as the ability to detect cyber threats, malware, and abnormal behavior, TLS decryption and termination, and data protection. Organizations require not just full security controls, but also visibility, automation, and orchestration across multi-cloud environments. And if there is a breach, they must be able to detect and stop any lateral movement and its expansion. Security policy must be easy to scale up and down as needed, and without huge costs.

Solution: APEIRO

ShieldX (www.shieldx.com), a security vendor just coming out of stealth, offers APEIRO, a software-defined security solution that uses a container-based, microservices architecture instead of a traditional, monolithic appliance solution to segment and secure terabits of traffic. APEIRO uses microsegmentation to enable security services to be located between applications and within the data center web, database, and application tiers, instead of only at the perimeter; as a result, a breach in one zone will not compromise others.

Figure 2. APEIRO



Source: Enterprise Strategy Group, 2017

APEIRO is fast and easy to deploy over an existing infrastructure (ShieldX boasts 15 minutes), and enables organizations to natively, automatically segment and secure cloud workloads at scale, across both physical and multi-cloud infrastructures. It provides deep packet inspection, visibility, policy management, and enforcement at cloud scale. Organizations can implement security policies on-demand, based on:

- Microsegmentation: Application-aware access control
- Threat detection and prevention: 10,000+ threat definitions to identify threats based on a combination of behavioral, reputation, anomaly, and signature techniques
- Malware detection: Delivered through integration with FireEye appliances or cloud service
- TLS decryption/termination: Network-based, inbound and outbound decryption/termination at customer-defined scale and cost
- URL classification/filtering: Validates safety of external connections, enhances granularity of policy, detection, and enforcement

ShieldX expects to offer network-based Data Loss Prevention (DLP) in a future release.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Because the APEIRO microservices are containerized, they are lightweight and can run on any infrastructure or hypervisor that an organization owns. At launch, APEIRO supports VMware vSphere, OpenStack/KVM, and AWS environments, with additional cloud support on the horizon. Highly available and multi-tenant, APEIRO REST APIs support integration with DevOps-oriented processes.

In addition, as administrators configure APEIRO to secure each environment—such as VMware, AWS, and OpenStack clouds—it automatically packages its containers into the right format for seamless insertion and interconnects them to form a single logical unit, or Virtual Chassis. This Virtual Chassis orchestrates and manages self-inserting security policies that are application traffic-flow-aware; user-awareness is on the roadmap. As new workloads are added, they are automatically included in the security environment; APEIRO scales elastically based on traffic flows, and consumes only the resources it needs, up to a limit as defined by the IT organization. Deep packet inspection and real-time analytics deliver exceptional visibility and enable detection of Indicators of Pivot (IoP) so that any breaches may be tracked, or are stopped in their tracks before proliferating via the east-west axis.

ESG Lab Tested

ESG Lab tested the ease of deploying APEIRO for VMware ESX, AWS, and OpenStack clouds. We also used a simulated environment to demonstrate the ability to automatically scale services and inspect more than a terabit per second of network traffic; identify and block threats; identify Indicators of Pivot to stop attack proliferation; detect malware using FireEye integration; and control access. The test bed included HP ProLiant DL360 servers with Intel Xeon E5 CPUs, 2TB of storage and an AWS VPC.

Ease of Deployment

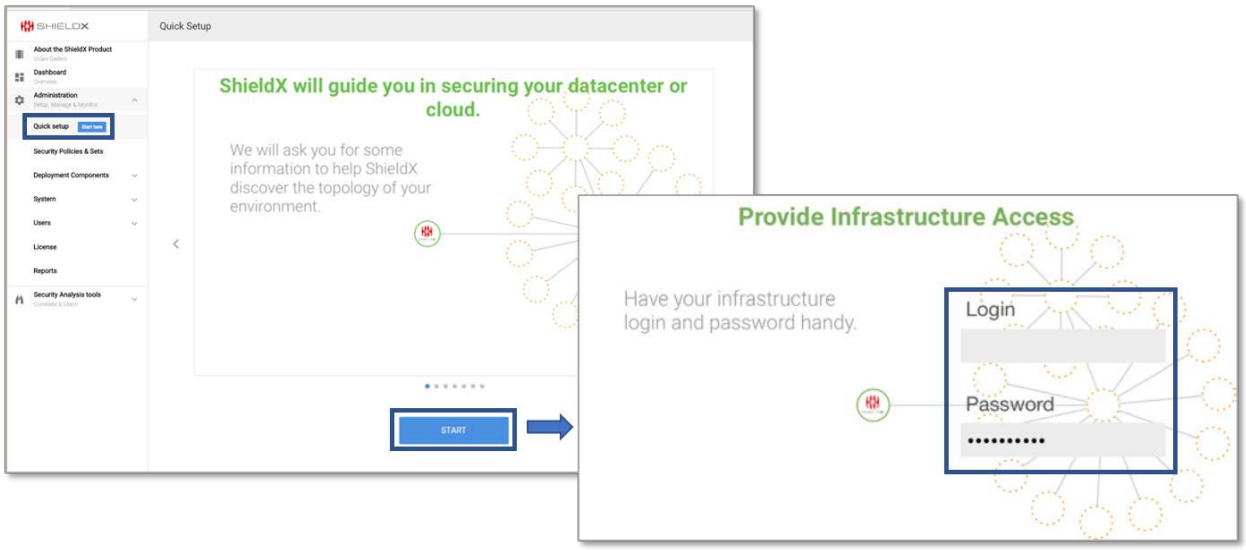
ESG Lab began by deploying the software to the VMware environment, which was extremely simple and fast. We downloaded the licensed OVA file, assigned a host name (*ShieldX-ESG*) and IP address, entered network details, and clicked ***Save***. Next, using administrator credentials, we logged into the APEIRO management UI using the Google Chrome web browser and started the process of creating a Virtual Chassis.

Automatic Discovery

Using the ***Quick Setup*** drop-down option in the Administration menu, we created an Infrastructure Controller Connector to connect to our VMware virtual infrastructure and enable information exchange and security orchestration. We selected VMware ESXi and entered the name ***ESG Infra***, provided a valid IP address, entered administrator credentials for the VMware environment, and clicked ***Next*** to enable APEIRO to automatically discover the infrastructure.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 3. APEIRO Quick Setup



When discovery was complete, we added a management network, which allows communication between APEIRO management and data plane microservices and Segment Interfaces (SIs), and then configured the backplane network (*ShieldX-ESG-Backplane*). The APEIRO backplane network uses a virtualized port group on the vSwitch so that APEIRO microservices may move inspected traffic among themselves.

Configure Deployment Specification

The next step was to create a Deployment Specification, which defines operations as the infrastructure changes. It includes the hosts to which APEIRO can scale out, the storage used by microservices, and IP addresses to be assigned to the microservices. We named the Deployment Specification *ESG-Test-Deployment*, designated the hosts, retained the default storage and network selections, and clicked ***Save***.

Create Data Planes

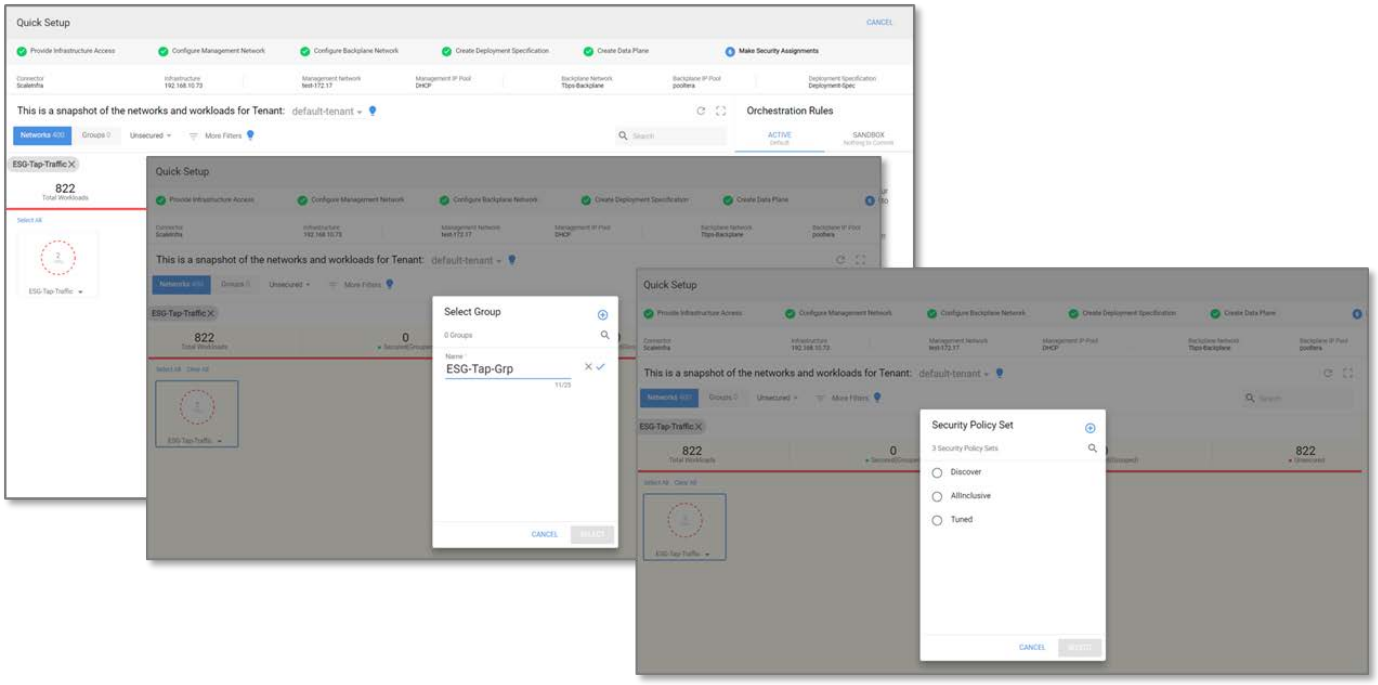
The next step was to create a Data Plane for ESXi. Each Data Plane is self-managing and adaptive, with automatically generated Segment Interfaces and inspection microservices. We named this Data Plane *ESGDP1*, assigned the Infrastructure Connector and Deployment Specification previously created, and clicked ***Next*** to complete the process.

Configure Security Orchestration Policy

Configuring a Security Orchestration Policy defines the security controls for groups of networks or workloads that share similar security requirements. ESG Lab selected the *ESG-Tap-Traffic* network, which was created to demonstrate passive APEIRO tap operation. *ESG-Tap-Traffic* was displayed with a red dashed circle as an unsecured network. The number within the circle displays the number of VMs running. (Green circles indicate grouped and secured networks, while yellow-dashed circles indicate networks that have been grouped but with no security policies bound yet.) We placed it into a group called *ESGGroup1*, assigned a Security Orchestration Policy (*All-Inclusive)* to that group, clicked on ***Create New Rule***, then ***Commit to Active and Save***.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 4. Configuring an APEIRO Security Orchestration Policy

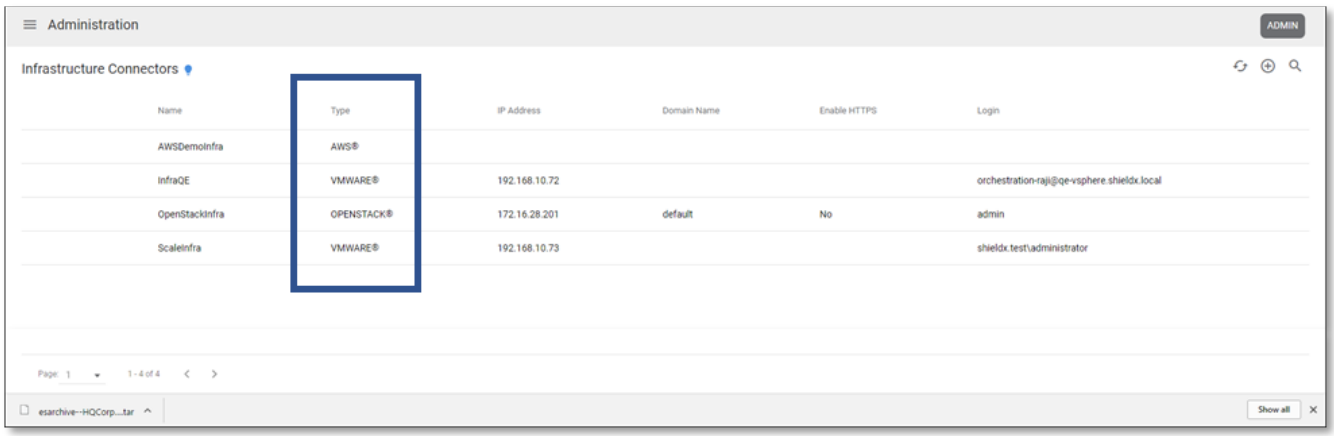


Next, we repeated the steps using the same Infrastructure Controller Connector to create another Data Plane. We created a VLAN pool in the Deployment Specification, and created Client and Server resource groups. This time we selected the Inline configuration, and activated and saved it.

The configuration process was simple and intuitive, and as claimed by ShieldX, in about 15 minutes ESG Lab had deployed a Virtual Chassis with both Tap and Inline operations configured; the former passively visualizes traffic and detects threats but takes no action, while the latter will actively block unwanted or malicious network traffic.

In multi-cloud environments, each infrastructure being protected has its own Data Plane, but all are managed through a single management plane. In order to install APEIRO to our OpenStack and AWS infrastructures, ESG Lab created Data Planes for these using the same procedures. As Figure 5 shows, all three Data Planes were managed from the same management UI.

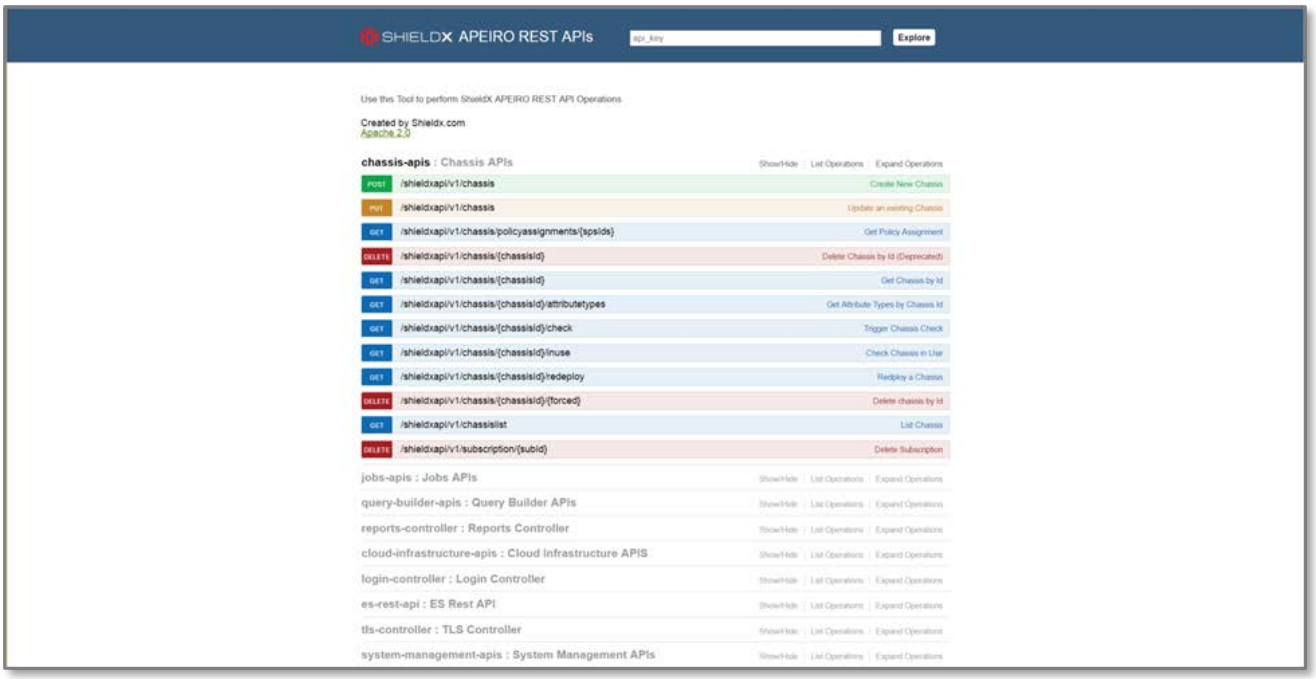
Figure 5. APEIRO Multi-cloud Environment Management



© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Finally, we looked at the APEIRO API documentation to understand how REST APIs can enable complete integration with an organization's existing orchestration frameworks. These APIs expose all configuration and management functionality.

Figure 6. APEIRO REST APIs



Why This Matters

Most organizations have a complex mix of legacy physical and multi-cloud virtual infrastructures. This complicates IT's ability to deliver the secure, agile data services organizations demand. It requires collaboration among infrastructure, security, and DevOps teams, but many times these teams continue to rely on physically focused security technologies and processes that were not built for cloud infrastructures.

ESG Lab validated the ease and speed of deploying APEIRO. In 15 minutes we had installed APEIRO on our VMware cloud, and had configured the Virtual Chassis and the Infrastructure Connector, Deployment Specification, Data Planes, and Security Orchestration Policies required to protect our environment. Once this was complete, APEIRO was ready to automatically scale up and down to deliver the microservices needed for continuous monitoring and cloud security. AWS and OpenStack deployments were equally simple and fast, and we validated the ability to manage all three from a single interface. The simplicity of deployment, management, and scaling enables agility and cost reduction.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Traffic Inspection and Threat Detection

ESG Lab also validated the ability of APEIRO to inspect more than a terabit per second of traffic—automatically scaling microservices up and down as needed to visualize and secure applications, and detect and mitigate threats. We watched in the Dashboard as the primary APEIRO Data Plane microservices elastically scaled out and in:

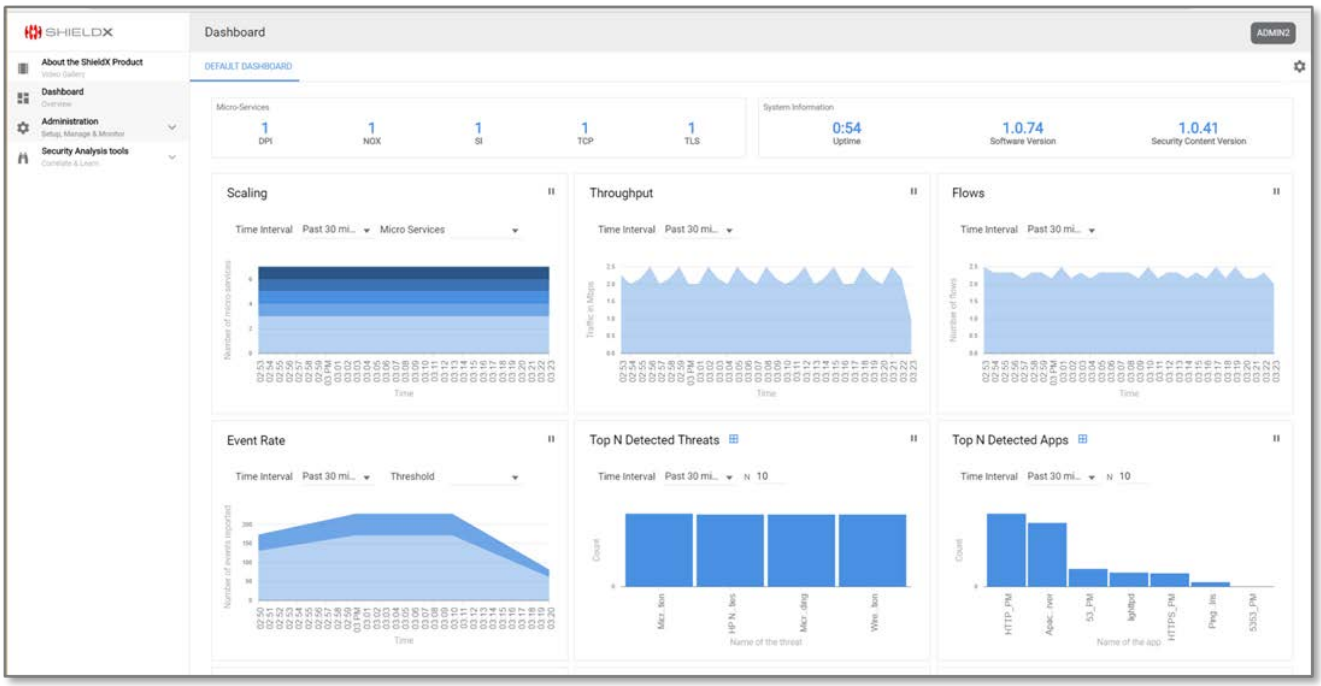
- Flow handling (TCP/UDP/ICMP) for Layer 4
- Deep packet inspection (DPI) of Layer 7 traffic.
- Network Object Extractor (NOX) – delivering integration with established security infrastructure (e.g. supplemental sandbox technologies, such as FireEye). Works in Tap or Inline mode in conjunction with DPI to assemble files from individual packets before handing them to FireEye.
- Transport Layer Security – decrypts/encrypts transport layer connections

Create Dashboard

We began by creating a dashboard in the web-based management UI to monitor the environment. We clicked on the gear icon, chose a display theme and column layout, named our dashboard *ESG-Test*, and configured it to show all widgets: Microservices Inventory, System Information Scaling, Throughput, Flows, Event Rate, Top N Detected Threats, and Top N Detected Apps.

Next, ESG Lab logged into a client machine on our test network, *ShieldX-ESG-Client,* and ran a script that generated financial traffic from finance.yahoo.com. We then logged into the management UI, clicked on ***Dashboard***, enabled ***Auto-refresh***, and within minutes were able to view the microservices activities and Top N Detected Apps, which were shown in the widgets, as seen in Figure 7.

Figure 7. The APEIRO Dashboard

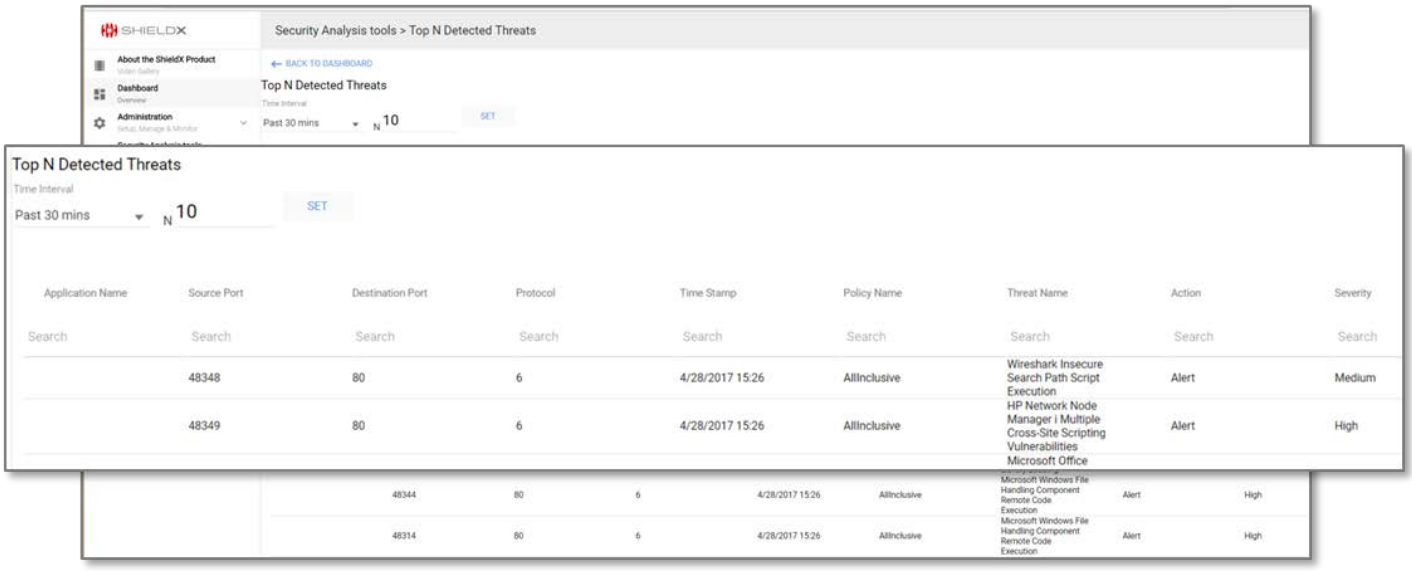


© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Threat Detection

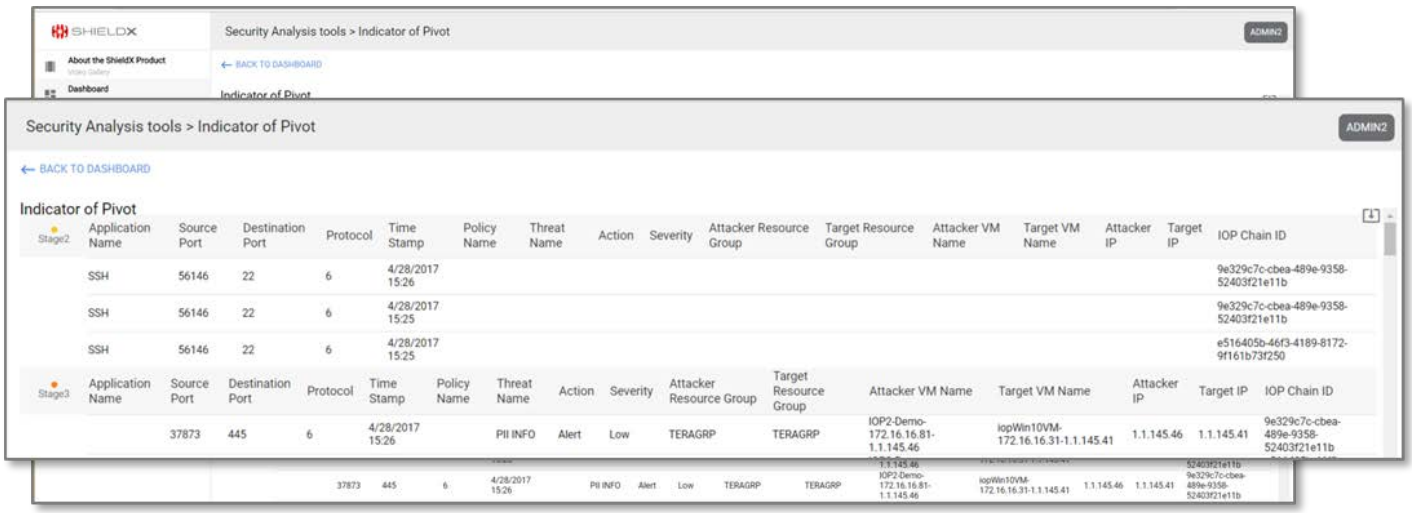
Next, we ran another script designed to simulate multiple attacks. Again, we logged into the management UI with auto-refresh enabled and observed threats being detected, top malware domains, invalid certificates, and others.

Figure 8. APEIRO Security Analysis—Top N Detected Threats



Following this, we ran one more attack script that executed a WordPress attack, followed by a series of lateral movements, data collection, and data exfiltration, and validated that APEIRO correctly identified these threats with Indicators of Pivot (IOP).

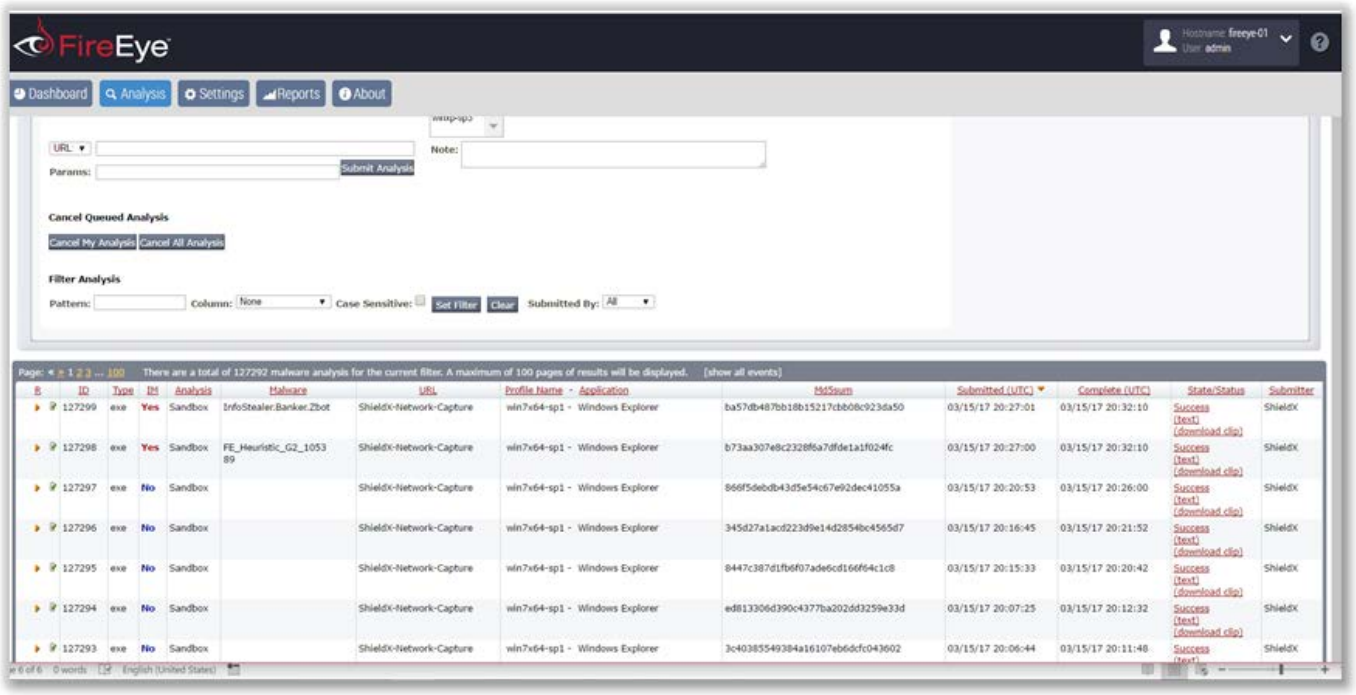
Figure 9. APEIRO Security Analysis—Indicators of Pivot



The next test script demonstrated the ability of APEIRO to detect malware files using its built-in integration with the FireEye AX-series malware analysis appliance. As files requiring inspection were detected, they were redirected to the FireEye appliance where they were placed in a sandbox and analyzed; when analysis was complete, the results were viewable on the APEIRO dashboard.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 10. APEIRO FireEye Integration and Malware Detection/Analysis



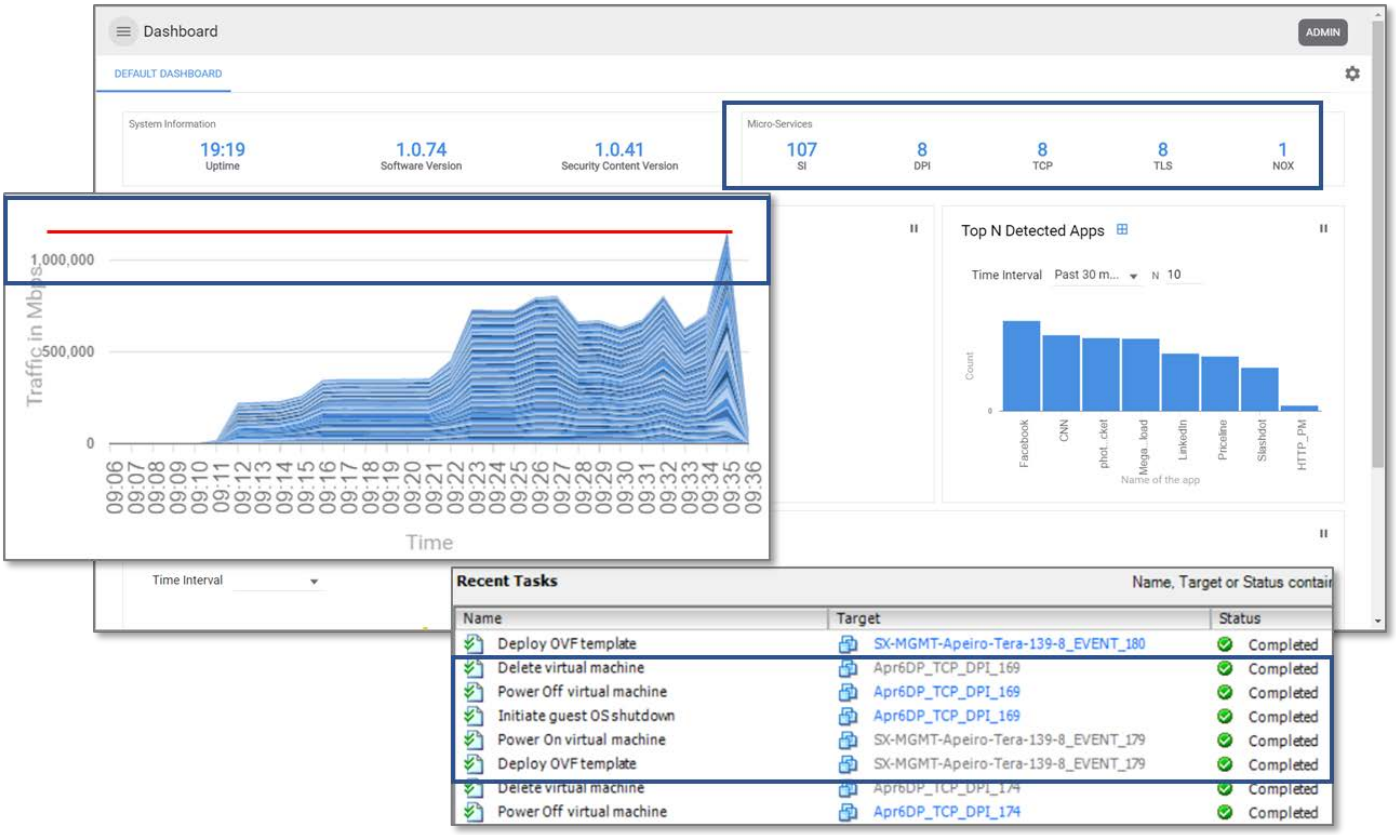
Terabit+ Traffic Inspection

Finally, ESG Lab viewed a demonstration of the ability of APEIRO to scale for inspection of a large amount of data. This test used a simulated environment leveraging 20 hosts to generate more than a terabit per second of traffic; the APEIRO data path test environment included two hosts, each with 256 GB RAM, and an overall total of 40 virtual CPU cores and 4TB of storage.

We ran a script that generated traffic from all 20 hosts. In about 25 minutes, traffic ramped up to more than 1.1 Tb/Sec. APEIRO scaled simultaneously and automatically, spinning up new microservice instances to handle the additional load, and spinning them back down once the traffic subsided. Figure 11 shows a graph demonstrating the terabit scale and timeline, along with the APEIRO dashboard showing the numerous microservices instances. The vSphere view in the bottom of Figure 11 shows microservices scaling back down.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

Figure 11. Terabit-Plus Traffic Inspection



This APEIRO configuration provided sufficient resources to perform application-aware microsegmentation across the full terabit per second of traffic. It should be noted that organization can simply increase the the amount of virtual cores, RAM, and storage in the APEIRO environment to enable additional features and controls, such as Threat Prevention or Malware Detection, without reducing throughput.

Why This Matters

Cyber threats are dynamic, and cyber criminals continue to innovate. Breaches can infiltrate your infrastructure and then spread within, causing serious damage. Perimeter-based security is no longer sufficient, and appliance-based solutions cannot offer the scalability and agility that cloud infrastructures demand. Clouds are designed for change and growth, and cloud security must operate using the same principles.

ESG Lab confirmed that APEIRO provides dynamic discovery and continuous security monitoring at terabit scale. Multiple types of threats were identified, including malware that was analyzed via FireEye integration, and Indicators of Pivot provided the alerts needed to intercept the lateral spread of malicious code. Security microservices automatically scaled up to inspect more than a terabit of data, and then scaled back, enabling full security with efficient resource use.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

The Bigger Truth

While organizations expand their cloud data services, many continue to leverage security solutions built for static, physical infrastructure. This mismatch results in higher risk, higher costs, and less agility. Why is this the case? The cloud security story our colleague Jon Oltsik told in a recent blog sets the scene:

> "A few years ago, ESG (and other) research indicated that security concerns posed the biggest impediment for more pervasive use of cloud computing. What happened next? Business executives and CIOs found that cloud agility, flexibility, and potential cost savings were too good to pass up, creating a "cloud or bust" mentality. Naturally, CISOs had to do their best and go along for the ride whether they were ready or not.[2]"

He goes on to comment that organizations have a hard time getting visibility into cloud-based workloads, and find it difficult to find the right level of automation and orchestration that they need for the cloud. Perimeter-based solutions and monolithic appliances simply cannot keep up with the ever-changing threat landscape, as the onslaught of breaches that cross every industry cost organizations in terms of money, customer loyalty, and reputation. Nor can these solutions provide the agile scalability security professionals know is needed to capture, process, and analyze cloud traffic.

ShieldX is just coming out of stealth to reveal a new approach: APEIRO, 100% cloud-native software, designed with cloud principles, technologies, and economics in mind. Protection is delivered using distributed, self-orchestrating microservices that mirror the agility, flexibility, and scale of cloud infrastructure. This ensures that in ever-changing cloud environments, organizations can be confident that the right traffic is being inspected in the right location and with the right policies applied at the right time.

ESG Lab validated that APEIRO delivers consistent and broad security controls across multi-cloud environments, including VMware ESX, AWS, and OpenStack, ensuring that no workloads are more vulnerable than others, no matter how you scale. It provides visibility and intelligent analysis across your cloud spectrum, the ability to detect a single threat in terabits of traffic, malware integration with FireEye, and the ability to halt the lateral movement of an attack through real-time analysis.

APEIRO is also cost efficient. From a CapEx perspective, it is a lightweight, containerized solution that eliminates the hefty hardware, power, and cooling costs of large, appliance-based solutions—especially when one considers that organizations must purchase enough appliances to handle their potential peak throughput. In terms of OpEx, it is simple to deploy and scale, with consolidated management across multi-cloud environments.

This is a new solution from a new company and there are a few features that ESG Lab looks forward to in the future, including additional cloud support and network-based DLP. However, in our first round of testing, APEIRO demonstrated fast and simple-to-execute, multi-site and multi-cloud deployment and insertion. In our test environment, ESG Lab was able to segment and comprehensively secure a network in less than 15 minutes with built-in controls and integration with FireEye for malware detection and mitigation. Elastic, on-demand scaling was also impressive, with APEIRO dynamically spinning services up and down as needed, automatically. ShieldX may be a new player, but they are definitely worth a closer look.

[2] Source: ESG Blog, *Cloud Security: Still a Work in Progress*, Jon Oltsik, March 21, 2017.

© 2017 by The Enterprise Strategy Group, Inc. All Rights Reserved.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.