EMA Vendor to Watch: ShieldX

Corporate Information

ShieldX is one of a growing number of startups to use microsegmentation as a foundation to deliver more flexible security to protect east/west traffic in virtual and cloud environments. What sets it apart from its rivals is the breadth of security controls the APEIRO platform provides, and APEIRO's quick deployment. Although it trailed some of its rivals to market, ShieldX made up for lost time by quickly signing up well-known reference customers like Alaska Airlines in the U.S. and Park Holidays in the U.K. The fledgling cloud security company also generated significant venture funding in two rounds–an initial $9 million in late 2015 and a $25 million B round in late 2017. The B round added investors with a solid track record of success, including FireEye founder Ashar Aziz, Dimension Data, and Symantec Ventures, who joined existing venture backers Bain Capital, FireEye, and Aspect Ventures.

ShieldX was launched in 2015 by serial entrepreneur Dr. Ratinder Paul Singh Ahuja, who founded and sold four earlier startups to vendors including Cisco, Extreme Networks, and McAfee. At McAfee, he served as CTO and Vice President of its mobile and network security units. At ShieldX, he leads a team of veteran technology executives, including co-founders Harjinder Singh and Manuel Nedbal, the latter of whom led the development of the industry's first 10 Gbps deep packet inspection appliance. Between them, they hold 47 security-related patents. ShieldX itself holds a single patent, with 18 more in the pipeline.

Value Proposition

The road to securing virtual workloads in the cloud against known and zero-day malware is littered with less than successful approaches. Hairpinning traffic from one virtual machine to another through an external physical appliance for inspection is cumbersome, expensive, and slow. Anti-malware agents installed in virtual machines take up precious memory and CPU. While network virtualization can help reduce the potential attack surface in the flat networks used in virtualized data centers, it does not provide protection against the full gamut of malware techniques. Enter APEIRO, which combines a range of detection technologies implemented as microservices, each within its own Docker container. Functions supported within APEIRO's virtual chassis include TLS traffic decryption and termination, IDS/IPS, native sandboxing or integration with FireEye's AX and Helix, secure web gateway functionality, virtual TAP traffic collection and aggregation, full packet capture and logging, DLP, NGFW, and anomaly and lateral movement detection. It combines those functions with automated discovery of assets upon installation and leverages machine learning to assign those assets to multiple groups. Operators then define policies that are applied to the groups. APEIRO also uses orchestration and automation to connect to the various cloud services the customer uses, whether they are private clouds or public clouds. To date, those services include Amazon AWS EC2, Microsoft Azure, OpenStack, and VMware ESXi. APEIRO maintains consistent policies across those different environments.

ShieldX made extensive use of automation within APEIRO to speed deployment and policy definitions across multiple groups. Not only does it automate discovery, profiling, and grouping of workloads, it also automates insertion, automatically provides policy recommendations and updates, and dynamically maintains groups across multiple clouds. The company claims installation takes 30 minutes. Flexible pricing models include pricing by processing capacity or by network traffic volumes.

EMA Perspective

The movement to the cloud is in full swing now, but there's still a lot of confusion about the most effective way to secure those cloud-based workloads since cloud security is still a prime concern. Last year, 90 percent of cybersecurity professionals responding to a LinkedIn Information Security Community survey revealed they are concerned about cloud security, which was an 11 percent increase over the same survey conducted one year earlier. Eighty-four percent of respondents said that traditional security products either don't work in the cloud or are of limited use. The top concern among those respondents was the potential for data loss or leakage.

Adding to the confusion are competing claims by vendors in different camps that take non-traditional approaches to securing virtual workloads. There are traditional security providers, such as Trend Micro, that established a strong beachhead in securing virtual servers. Adding to the cacophony are network function virtualization providers, such as VMware and Cisco, who claim their network-focused micro-segmentation can protect workloads. They primarily do so through access control. Meanwhile, a growing list of security-focused micro-segmentation vendors including Illumio, Guardicore, vArmour, Juniper Networks, and others claim to provide more complete and flexible protection of virtual workloads in the cloud.

It will take some time for the dust to clear, and in the interim there is an opportunity for smaller, innovative startups like ShieldX to gain attention and market share. ShieldX is wise to target specific use cases around lateral east/west protection in the data center and multi-cloud environments, clean pipe services for telcos and ISPs, and multi-tenant consumption-based services from MSSPs. Its support for multiple public cloud services dovetails nicely with a trend among enterprises to adopt a multi-cloud strategy. In January, RightScale conducted its annual State of the Cloud survey among IT professionals and found that 81 percent said their organizations had a multi-cloud strategy. With its flexible architecture and ability to maintain consistent policy enforcement across multiple cloud environments, ShieldX is well positioned to capitalize on that trend.