SHIELDX

Elastic Security Platform Datasheet

Make security the easiest thing you do in the cloud.

ShieldX is a cloud-native elastic security platform that maintains vigilance and control across all cloud deployment models. ShieldX uses cutting edge analytics modeling to understand the intent of your workflows, and then applies the right policies and controls to create elasticity, drive nimble deployments, and then autonomously apply security. By delivering a full stack of agentless security controls to protect data centers, cloud infrastructure, applications and data, ShieldX unites your security tools into one intelligent, automated solution to help enterprises achieve Elastic Security.

THE IT WORLD HAS EVOLVED. SECURITY HASN'T—UNTIL NOW.

Your network is no longer defined by a border. Instead, its defined by "wherever your data went in the cloud." As workloads and dataflows stretch across all the dynamic deployment models, the security concerns remain consistent. However, your security solutions were designed, engineered and implemented for datacenter operations are obsolete. They are no longer effective in protecting your data—they lack elasticity to enable the business across the cloud—especially the multicloud. In addition, security controls designed on old-school datacenter paradigm all suffer from the same affliction—they detect incidents after the fact, and need to be continually assessed, adjusted and reconfigured manually to adapt with the evolving network and threatscape. This puts IT Security Teams in a continuous state of vigilance, waiting for the next incident. The ShieldX elastic security platform can adapt, expand, contract—while providing all the tools you used in the datacenter—while consolidating visibility and control in multicloud deployments.

By providing micro-segmented environments that automatically adapt with the workflows—infused with all of the mitigations needed to protect those workflows—reaction becomes not just instant, but also comprehensive. Intent is instantly translated into the policy and mitigation enablement. Security is no longer a response—it's autonomous. Using ShieldX, IT Security Teams no longer have to spend all of their time on vigilance and reactive controls. They can focus their precious time and resources on driving modern technology, business growth, and IT advancement.

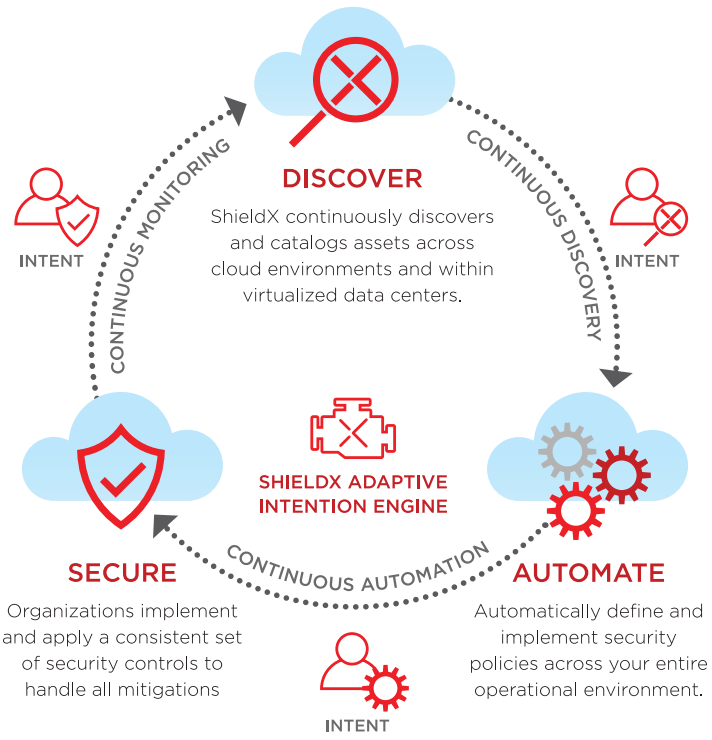
HOW DOES IT WORK?

The ShieldX Elastic Security platform enables dev-ops and security teams to protect their multi-cloud environments.

- **Discover:** Once ShieldX is deployed across your multi-cloud environment, the system will begin to automatically and continuously discover new resources—such as web tiers, or middleware apps, or storage—as they are brought online.

- **Automate:** Upon discovery, ShieldX enables users to automate the insertion process of ShieldX flow inspectors or segment interfaces to properly route network traffic through the ShieldX security microservices.

- **Secure:** Using the security intention that has been applied across these diverse set of cloud networks and workflows, ShieldX instantiates the appropriate microservices that will transform that policy intention into actual controls. This ensures that virtual machines and workloads are continuously



and automatically monitored and secured without the need for human intervention while also providing automated visibility and security pervasively across your multi-cloud environment.

THE SHIELDX ADAPTIVE INTENTION ENGINE

The ShieldX Adaptive Intention Engine allows security teams to apply their security intention through a broad set of ShieldX controls that include application visibility, workload protection, micro segmentation, IPS, firewall, malware detection and more. The security policies enforced by ShieldX not only factor in application connectivity models, but also the high-level intent of the connection based on business policies. Once the policy is defined, ShieldX 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. ShieldX allows you to deploy software-defined Elastic Security in a containerized micro-services overlay to your distributed cloud services and the workflows going across them.

SHIELDX IMPACT

- **Micro-containerization allows for elastic security**. Instead of having to deploy ACLs across network segments using "all or nothing datacenterbased controls" like firewalls, ShieldX gives your workflows the protection when they need it, how they need it, as much as they need it—autonomously.

- **Adaptive threat modelling.** By using ShieldX to autonomously determine which policies to apply to which controls for this a given workflow, ShieldX can "micro-design" each workflow's specific threat model. You don't have to worry anymore about "did we miss something?" because ShieldX will discover issues for you and adjust on the fly.

- **Centralized monitoring, review, and control over cloud environments.** ShieldX provides the flexibility you need to protect each workflow exactly how it needs to be protected—and then comes back together to give your IT Security Team the unified visibility of the overall threat landscape.

- **Do more with less.** ShieldX removes the complexity and overhead by autonomously adapting to the workflows within a microsegment, dynamically adjusting policies to meet security requirements as well as performs proactive threat modeling and attack surface management across all deployment models. Using ShieldX, security teams see immediate operational cost reductions in vigilance, incident management, mitigation correlation, change control processes, initial setup and ongoing maintenance as well as savings in software license.

- **Virtual Firewall.** ShieldX provides a cost-effective, scalable alternative to traditional virtual firewalls. ShieldX access controls are enforced across multi-cloud infrastructures between workloads. Unlike traditional virtual firewalls, ShieldX can scale easily to any size deployment and includes the Adaptive Intention Engine that uses machine learning to automatically generate initial and ongoing policies (patent application #P1010P034).

IDS/IPS Threat Detection & Prevention: Threat actors take advantage of network-based IDS/IPS by knowing that the rule bases must account for everything on the network—and cannot be granular enough to laser focus on specific workflow characteristics. ShieldX provides a new paradigm in micro-service segmentation per workflow couple with tailor-made IDS/IPS string matching to create unparalleled protection models.

Malware Prevention: Malware has become laser targeted on specific data, data formats, and workflow characteristics. Broad signature-based malware solutions have become inefficient and ineffective in preventing and controlling tailor-made attacks designed to compromise specific workload models. ShieldX can proactively protect workflows across the multicloud using a combination of static and dynamic inspection, either on-premise or in the cloud.

Full-Flow Packet Capture:

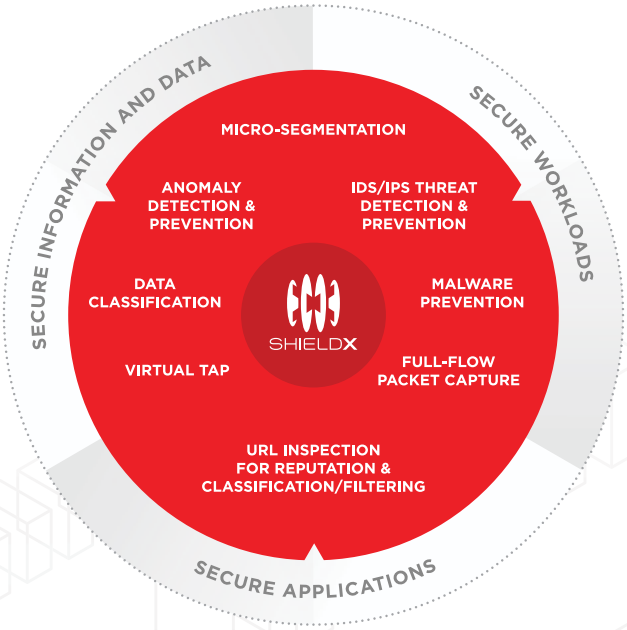
Provides the ability to record traffic that matches a pre-configured filter specification.

Data Classification:

Detects and controls the movement of sensitive data within the multicloud. Also discovers sensitive data at-rest to formulate policies customized to the attack surface.

Intelligence Secure Export API:

Aggregationand mirroring of captured flow data to external inspection and logging products.



URL Inspection for Reputation & Classification/ Filtering:

Inspect HTTP/S traffic for security and acceptable-use policies.

Anomaly Detection & Prevention:

Correlation of individual events to surface in-progress kill chain activities.

Elastic Micro-segmentation:

Prevent unwanted lateral movement in the data center or the cloud, stopping the compromise and exfiltration of sensitive data.

Supported Environments

- Azure
- Amazon AWS
- VMWare ESX

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

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

November 2018